Серия P-2602HW EE

Интернет-центр с модемом ADSL2+, беспроводной точкой доступа 802.11g, коммутатором Fast Ethernet и SIP-адаптером IP-телефонии

Серия P-2602H EE

Интернет-центр с модемом ADSL2+, коммутатором Fast Ethernet и SIP-адаптером IP-телефонии

Руководство пользователя

Версия 3.40
7/2006
Первая редакция

ZyXEL

Авторские права

Отказ от ответственности

Корпорация ZyXEL заявляет об отказе от любой ответственности, возникающей в силу применения или эксплуатации её аппаратных или программных продуктов, описанных в настоящем документе. Корпорация ZyXEL также никому не передает свои или чужие права на патенты. Корпорация ZyXEL оставляет за собой право вносить изменения в описанную в настоящем документе продукцию без предварительного уведомления. Данный документ может быть изменён без уведомления.

Торговые марки

ZyNOS (сетевая операционная система ZyXEL) – зарегистрированная торговая марка корпорации ZyXEL Communications, Inc. Другие торговые марки, перечисленные в настоящем документе, используются исключительно для целей идентификации и могут составлять собственность их владельцев.

Техника безопасности

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

- Чтобы уменьшить риск возгорания, используйте для телекоммуникационной линии провода калибра 26 AWG (American Wire Gauge, американская система классификации проводов по диаметру) или более толстые.
- НЕ открывайте устройства и модули. Открывая или снимая крышку, вы открываете места с высоким напряжением, которое опасно для жизни. Обслуживать устройство должен ТОЛЬКО квалифицированный специалист. За дополнительной информацией обращайтесь к поставщику.
- Подавайте на устройство питание ТОЛЬКО от специально предназначенного для него источника питания. Сетевой шнур должен подключаться к сети переменного тока с соответствующим напряжением (110 В в Северной Америке и 230 В в Европе).
- НЕ пользуйтесь устройством, если источник или кабель питания поврежден, иначе может произойти поражение электрическим током.
- Если кабель питания поврежден, выньте вилку из розетки.
- НЕ пытайтесь починить источник или кабель питания. Обратитесь к местному поставщику и закажите новый кабель или источник питания.
- Размещайте соединительные кабели так, чтобы не наступать на них и не задевать их. НЕ ставьте какие-либо предметы на кабель питания, НЕ размещайте устройство там, где на кабель питания может кто-нибудь наступить.
- Не используйте устройство вне помещений. Убедитесь, что все соединения выполнены внутри помещений. Существует определённая вероятность поражения электрическим током в результате молнии.
- Монтируя устройство на стене, следите за тем, чтобы не повредить электропроводку, газо- или водопроводные трубы.
- НЕ устанавливайте и не эксплуатируйте устройство во время грозы. Существует определённая вероятность поражения электрическим током в результате молнии.
- НЕ подвергайте устройство воздействию влаги, пыли или агрессивных жидкостей.
- НЕ устанавливайте устройство вблизи от воды, например, в сыром подвале или рядом с бассейном.
- Убедитесь, что кабели правильно подключены к клеммам.
- НЕ загораживайте вентиляционные проёмы устройства. Недостаточная вентиляция может повредить устройство.
- НЕ складывайте на устройство никаких предметов.
- Подключайте к устройству ТОЛЬКО годное к применению вспомогательное оборудование.

Изделие допускает возможность переработки. Соблюдайте правила утилизации.

Информация о сертификации P-2602H EE

Модем ZyXEL P-2602H EE одобрен для применения государственными органами по сертификации средств связи..

Система сертификации ГОСТ Р, Госстандарт России

Сертификат соответствия № РОСС TW.АЯ46.В04951. Срок действия с 03.03.2006 по 03.03.2008. Соответствует требованиям: ГОСТ Р МЭК 60950-2002, ГОСТ Р 51318.22-99 (класс Б), ГОСТ Р 51318.24-99 (группа 1), ГОСТ Р 51317.3.2-99, ГОСТ Р 51317.3.3-99.

Система сертификации в области связи

За Сертификат соответствия № ОС-1-СП-0249. Срок действия с 23.03.2006 по 23.03.2009. Соответствует требованиям: РД 45.080-99 "Аппаратура цифровых систем передачи абонентского доступа. Технические требования"; РД 45.038-99 "Технические требования к аппаратуре связи, реализующей функции маршрутизации пакетов протокола межсетевого обмена (аппаратура маршрутизации пакетов IP). Редакция 1-1998"; РД 45.176-2001 "Аппаратура связи, реализующая функции коммутации кадров в локальной сети на уровне звена данных. Технические требования"; Изменение №1. РД 45.176-2001 "Аппаратура связи, реализующая функции коммутации кадров в локальной сети на уровне звена данных. Технические требования"; Изменение №2. РД 45.176-2001 "Аппаратура связи, реализующая функции коммутации кадров в локальной сети на уровне звена данных. Технические требования"; Изменение №2. РД 45.176-2001 "Аппаратура связи, реализующая функции коммутации кадров в локальной сети на уровне звена данных. Технические требования"; РД 45.046-99 "Аппаратура связи, реализующая функции передачи речевой информации по сетям передачи данных с протоколом IP. Технические требования"; "Средства технические телематических служб. Протокол SIP. Общие технические требования. Редакция 1-2002", утв. Минсвязи России 03.07.2002г.

Государственная Санитарно-эпидемиологическая служба РФ

Санитарно-эпидемиологическое заключение № 77.01.09.650.П.13885.06.4. Срок действия с 24.06.2004 по 16.06.2009. Соответствует требованиям: СанПиН 2.2.2./ 2.4.1340-03 "Гигиенические требования к персональным электронно-вычислительным машинам и организации работы", СН 2.2.4./2.1.8.562-96.

Юридический адрес изготовителя

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

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

Гарантийное обслуживание ZyXEL

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

Гарантийные обязательства

1. Настоящая гарантия действует в течение трех лет с даты приобретения изделия ZyXEL и подразумевает гарантийное обслуживание в случае обнаружения дефектов, связанных с материалами и сборкой. В этом случае потребитель имеет право на бесплатный ремонт изделия.

2. При регистрации приобретенного изделия через Интернет на сайте указанном в таблице потребитель получает дополнительный год гарантийного обслуживания.

3. Максимальный срок гарантии, предоставляемой компанией ZyXEL, исчисляется с даты производства изделия и составляет четыре с половиной года. Дата производства определяется по серийному номеру на корпусе изделия: SYYxxWWxxxxxx, где YY - две последние цифры года, а WW - номер недели с начала года.

4. Настоящая гарантия распространяется только на изделия ZyXEL, проданные через официальные каналы дистрибуции ZyXEL.

5. Настоящая гарантия предоставляется компанией ZyXEL в дополнение к правам потребителя, установленным действующим законодательством в стране приобретения.

Условия гарантии

1. Гарантийное обслуживание изделия ZyXEL осуществляется в авторизованных сервисных центрах (АСЦ) ZyXEL на приведенных ниже условиях.

2. Настоящая гарантия действительна только при предъявлении вместе с неисправным изделием правильно заполненного фирменного гарантийного талона с проставленной датой продажи. Компания ZyXEL оставляет за собой право отказать в бесплатном гарантийном обслуживании, если гарантийный талон не будет предоставлен или если содержащаяся в нем информация будет неполной или неразборчивой.

3. Настоящая гарантия недействительна в случаях, если:

3.1 серийный номер на изделии изменен, стерт, удален или неразборчив;

3.2 изделие переделывалось без предварительного письменного согласия ZyXEL;

3.3 изделие неправильно эксплуатировалось, в том числе: а) использовалось не по назначению или не в соответствии с руководством ZyXEL; б) устанавливалось или эксплуатировалось в условиях, не соответствующих стандартам и нормам безопасности, действующим в стране использования;

3.4 изделие ремонтировалось не уполномоченными на то сервисными центрами или дилерами;

3.5 изделие вышло из строя по причине несчастного случая, удара молнии, затопления, пожара, неправильной вентиляции и иных причин, находящихся вне контроля ZyXEL;

3.6 изделие пострадало при транспортировке, за исключением случаев, когда она производится АСЦ;

3.7 изделие использовалось в дефектной системе.

Контактная информация

СПОСОБ СВЯЗИ СТРАНА	E-MAIL СЛУЖБЫ ПОДДЕРЖКИ E-MAIL ОТДЕЛА ПРОДАЖ	ТЕЛЕФОН ФАКС	ВЕБ-САЙТ FTP-СЕРВЕР	ПОЧТОВЫЙ АДРЕС
РОССИЯ	http://zyxel.ru/support	+7-095-542-89-29	www.zyxel.ru	ZyXEL Россия ул. Островитянова, д. 37а 117279 Москва Россия
УКРАИНА	support@ua.zyxel.com	+380-44-247-69-78	www.ua.zyxel.com	ZyXEL Украина Ул. Пимоненко 13 04050 Киев Украина
	sales@ua.zyxel.com	+380-44-494-49-32		
КАЗАХСТАН	http://zyxel.kz/support	+ 7 (3272) 590-689	http://zyxel.kz	ZyXEL Казахстан 050010б, Алматы пр. Достык 43, офис 414

Содержание

Глава 11
Голосовая телефонная связь 163

Список рисунков

Список таблиц

Предисловие

Благодарим за приобретение устройства P-2602H/HW EE (беспроводное интегрированное устройство доступа 802.11g / ADSL2+ / VoIP, далее – “P-2602”). P-2602 отличается простотой в установке и настройке.

О Руководстве пользователя

В этом руководстве содержатся инструкции по настройке P-2602 для различных применений.

Примечание: Для настройки P-2602 следует применять веб-конфигуратор или интерпретатор команд. Оба интерфейса управления различаются по составу настраиваемых параметров.

Другие документы

- Диск с сопроводительными материалами

  На прилагаемом компакт-диске содержится вспомогательная документация.

- Руководстве по быстрому запуску

  Руководстве по быстрому запуску поможет в кратчайшее время подготовить устройство к работе. Оно содержит информацию о подключении и указания по началу работы с устройством.

- Контекстная справка в веб-конфигураторе

  Встроенная гипертекстовая справка с описаниями отдельных экранов и вспомогательными сведениями.

- Веб-сайт ZyXEL

  На сайте http://www.zyxel.ru вы найдете новости о продукции, файлы микропрограмм, обновленную документацию и другие материалы технической поддержки.

Отзывы о руководстве пользователя

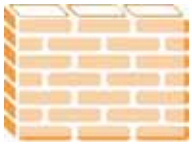
Помогая нам, вы помогаете себе. Любые замечания по этому руководству, вопросы и предложения просим отправлять электронной почтой по адресу techwriters@zyxel.com.tw или обычной почтой по адресу: The Technical Writing Team, ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 300, Taiwan. Спасибо.

Условные обозначения и синтаксис

- “Введите” означает, что следует набрать на клавиатуре один или несколько знаков. “Выберите” или “отметьте” означает, что следует выбрать один из предопределённых вариантов.

- Заголовки экранов и названия экранных полей набраны **жирным шрифтом Times New Roman**. Предопределённые варианты набраны **жирным шрифтом Arial**. Команды и клавиши со стрелками заключены в квадратные скобки. [ENTER] обозначает клавишу Enter или “ввод”, [ESC] обозначает клавишу Escape (Esc), [ПРОБЕЛ] обозначает клавишу для ввода пробела.
- Последовательность действий, выполняемых мышью, отмечается угловыми скобками (>). Например, предложение: “В операционной системе Windows выберите **Start** > **Settings** > **Control Panel**” означает, что сначала следует нажать кнопку **Start**, затем подвести указатель мыши к пункту **Settings** и щелкнуть на позиции **Control Panel**.
- Сокращение “напр.” означает “например”, а “т.е.” означает “то есть” или “говоря другими словами”.
- P-2602H/HW EE может упоминаться в тексте Руководства как P-2602.

Обозначения на рисунках

P-2602 	Компьютер 	Ноутбук 
Сервер 	Коммутатор 	Маршрутизатор 
Телефон 	DSLAM 	Шлюз группообразования 
Сетевой экран 	Беспроводной сигнал 	

Глава 1
Краткое знакомство с P-2602

В этой главе рассмотрены основные возможности и применения устройства.

1.1 Обзор серии P-2602H/HW EE

P-2602H/HW EE – это серия интегрированных устройств доступа (IAD), которые объединяют в себе маршрутизатор ADSL2+ и средства голосовой связи по IP (VoIP), позволяя использовать обычный аналоговый или ISDN-телефон для разговоров по Интернету. Сочетание технологий DSL и NAT позволяет легко настроить совместное использование высокоскоростного Интернет-канала. Серия P-2602H/HW EE также заключает в себе полноценное решение для сетевой безопасности с мощным межсетевым экраном и средствами фильтрации содержания.

В руководстве рассматриваются следующие модели, доступные на момент его подготовки.

Таб. 1 Рассматриваемые модели

Модель	Название	Код
P-2602HW EE (LifeLine, Annex A) Rev. L-D1A	Интернет-центр с модемом ADSL2+, точкой доступа Wi-Fi, коммутатором Ethernet и SIP-адаптером IP-телефонии с резервированием через телефонную сеть общего пользования	P-2602HWL-D1A
P-2602HW EE (Annex A) Rev. D1A	Интернет-центр с модемом ADSL2+, точкой доступа Wi-Fi, коммутатором Ethernet и SIP-адаптером IP-телефонии	P-2602HW-D1A
P-2602H EE (Annex A) Rev. D1A	Интернет-центр с модемом ADSL2+, коммутатором Ethernet и SIP-адаптером IP-телефонии	P-2602H-D1A

Некоторые функции могут быть недоступны в определенных моделях. Формат обозначений продуктов описан ниже.

- “H” означает интегрированный 4-портовый концентратор (коммутатор). Модели “H” также включают в себя поддержку виртуальных частных сетей (VPN).
- “W” означает поддержку беспроводной сети стандарта IEEE 802.11g, реализуемую встроенным модулем формата “mini-PCI”. Все функции беспроводных сетей, описанные в данном руководстве, относятся только к моделям “W”.
- “L” обозначает наличие линии ТфОП (телефонной сети общего пользования), позволяющей одновременно пользоваться услугами VoIP и обычных коммутируемых телефонных сетей. Все функции линии ТфОП, описанные в данном руководстве, относятся только к моделям “L”.

Примечание: Когда P-2602 находится в выключенном состоянии, для вызовов можно использовать только порт **PHONE 1**. Запомните, какой из телефонных аппаратов подключен к этому порту, чтобы в экстренных ситуациях было можно им воспользоваться.

Модели с индексом “3” перед последней буквой названия (например, P-2602HWL-D3A) обозначают устройства, предназначенные для работы по сети ISDN (цифровая телефонная сеть с интегрированными услугами). Модели с индексами “1” или “7” перед последней буквой названия (например, P-2602HWL-D1A или P-2602HWL-D7A) обозначают устройства, предназначенные для работы по сети T-ISDN (UR-2).

Примечание: Используйте только микропрограмму, предназначенную для конкретной модели устройства P-2602. См. ярлык на нижней стороне корпуса P-2602.

Графический интерфейс пользователя (GUI), доступный через веб-браузер, позволяет легко управлять устройством.

Примечание: Все экраны, приведенные в данном руководстве пользователя, относятся к модели P-2602HWL-D1.

1.2 Характеристики

В следующих разделах рассмотрены основные особенности устройства.

Встроенный коммутатор

Четыре Ethernet-порта 10/100 Мбит/с с автоматическим согласованием позволяют P-2602 автоматически определять скорость входящих данных и перенастраиваться без вмешательства пользователя. Благодаря этому обеспечивается передача данных на скорости 10 Мбит/с или 100 Мбит/с в полудуплексном или дуплексном режиме в зависимости от типа сети Ethernet. Порты имеют автоматическое определение полярности (MDI/MDI-X), поэтому для подключения к ним можно применять как перекрестный, так и прямой Ethernet-кабель.

Высокоскоростной доступ к Интернету

P-2602 идеально подходит для работы с высокоскоростным Интернетом и объединения территориально разнесенных локальных сетей. Устройство P-2602 совместимо со стандартами ADSL/ADSL2/ADSL2+. Максимальные скорости передачи данных для каждого стандарта приведены в следующей таблице.

Таб. 2 Стандарты ADSL

СТАНДАРТНЫЕ СКОРОСТИ ПЕРЕДАЧИ ДАННЫХ	ВОСХОДЯЩИЙ КАНАЛ	НИСХОДЯЩИЙ КАНАЛ
ADSL	832 кбит/с	8 Мбит/с
ADSL2	3,5 Мбит/с	12 Мбит/с
ADSL2+	3,5 Мбит/с	24 Мбит/с

Примечание: Если поддержка Annex M в вашем P-2602 отсутствует, максимальная скорость восходящего канала ADSL2/2+ будет составлять 1,2 Мбит/с. Устройства P-2602, предназначенные для работы по ISDN, не поддерживают Annex M.

Максимально возможные скорости нисходящего и восходящего каналов зависят от стандарта, поддерживаемого вашим поставщиком услуг Интернета. Фактически достижимая скорость зависит от удаленности от поставщика услуг, а также от качества линии и ряда других параметров.

Линия ТфОП (только в моделях с индексом “L”)

Устройство позволяет подключить линию коммутируемой телефонной сети общего пользования (ТфОП). При этом можно отвечать на поступающие вызовы ТфОП даже в то время, когда по VoIP ведутся телефонные переговоры. Для того, чтобы осуществить исходящий вызов через ТфОП, можно набрать числовой префикс. Если устройство отключено от сети, можно по-прежнему осуществлять телефонные вызовы по ТфОП.

Примечание: Когда P-2602 находится в выключенном состоянии, для вызовов можно использовать только порт **PHONE 1**. Запомните, какой из телефонных аппаратов подключен к этому порту, чтобы в экстренных ситуациях было можно им воспользоваться.

Доступ в Интернет без настройки

После выполнения физических подключений и включения питания устройство автоматически обнаруживает параметры подключения к Интернету (например, номера VCI/VPI и метод инкапсуляции), используемые поставщиком услуг Интернета, и выполняет необходимую настройку. В тех случаях, когда для подключения требуются дополнительные параметры учетной записи (например, имя пользователя и пароль) или когда P-2602 не может соединиться с поставщиком услуг, устройство направит вас на соответствующие экраны веб-конфигуратора для ввода параметров или диагностики ошибок.

Функция “Any IP”

Функция “Any IP” позволяет выходить с компьютеров в Интернет через P-2602 без перенастройки параметров сети (в частности, IP-адреса и маски подсети), когда IP-адреса компьютера и P-2602 находятся в разных подсетях.

Автоматическая инициализация

Ваш поставщик услуг VoIP может автоматически обновлять конфигурацию вашего устройства через сервер автоматической инициализации (auto-provisioning).

Автоматическое обновление микропрограммы

Если в ходе автоматической инициализации устройство обнаружит новую версию микропрограммы, оно предложит обновить микропрограмму. Для работы этой функции необходимо, чтобы ваш поставщик услуг VoIP имел сервер автоматической инициализации и сервер для хранения микропрограмм.

Межсетевой экран

В устройстве реализован динамический межсетевой экран с защитой от DoS-атак (Denial of Service – отказ в обслуживании). По умолчанию при активном межсетевом экране весь входящий трафик от WAN (глобальной вычислительной сети) к LAN блокируется, если он не инициализирован в LAN. Межсетевой экран поддерживает анализ пакетов TCP/UDP, обнаружение DoS-атак, а также имеет средства информирования в реальном времени, ведения отчетов и журналов.

Поддержка IPSec VPN

Виртуальная частная сеть (VPN) позволяет соединяться с бизнес-партнерами и филиалами через Интернет по защищенному каналу с шифрованием данных, не прибегая к прокладыванию дорогостоящих выделенных линий. Реализация VPN строится на базе стандарта IPSec и совместима с другими продуктами, реализующими VPN на базе IPSec.

P-2602 поддерживает до двух параллельных подключений по IPSec.

Трансляция сетевых адресов (NAT)

Функция трансляции сетевых адресов (NAT) позволяет преобразовывать IP-адрес, используемый в одной сети (например, частный IP-адрес в локальной сети), в другой IP-адрес, известный в другой сети (например, глобальный IP-адрес в Интернете).

Фильтрация содержания

Фильтрация содержания позволяет блокировать доступ к веб-сайтам, URL которых содержит определенные (задаваемые вами) ключевые слова. Дополнительно можно ограничить период времени, в который применяется фильтрация, и задать список доверенных IP-адресов в локальной сети, которым разрешен доступ в Интернет без фильтрации.

Управление полосой пропускания

Функция управления полосой пропускания позволяет задать классы полосы пропускания для различных приложений и/или подсетей. Каждому из классов можно выделить определенную полосу пропускания (“бюджет”).

REN

Эквивалентное число устройств вызова (REN) – это параметр, характеризующий количество устройств (телефонов или факс-аппаратов), которые могут быть подключены к телефонной линии. Для вашего устройства REN=3, т.е. каждый телефонный порт может поддерживать до трех устройств.

Динамический буфер компенсации дрожания фазы

Встроенный адаптивный буфер позволяет сгладить различную задержку поступления голосовых данных (эффект дрожания фазы). Это повышает качество звукового сигнала во время разговора.

Поддержка нескольких учетных записей SIP

Можно одновременно использовать несколько учетных записей голосовой связи (SIP), присвоив их одному или обоим телефонным портам.

Поддержка нескольких голосовых каналов

Устройство может одновременно работать с несколькими каналами голосовой связи (несколькими телефонными вызовами). Кроме того, можно отвечать на входящие телефонные вызовы по учетной записи VoIP, даже если в данный момент кто-то другой использует эту учетную запись для разговора по телефону.

Обнаружение пауз/подавление тишины

Функция обнаружения пауз (VAD) Она позволяет снизить нагрузку на сеть во время вызова за счет исключения пакетов с тишиной, когда разговор на линии отсутствует.

Искусственный фон во время паузы

Чтобы полная тишина не была ошибочно принята за разрыв соединения, устройство может создавать определенный шумовой фон, заполняя паузы в те интервалы, когда абонент на другом конце соединения не говорит и удаленное устройство прекращает передачу.

Подавление эха

Ваше устройство поддерживает G.168, стандарт ITU-T для подавления эха, вызываемого реверберацией вашего голоса в трубке во время разговора.

QoS (качество обслуживания)

Механизмы «качество обслуживания» (QoS, Quality of Service) обеспечивают наилучшее обслуживание в рамках отдельных потоков. Ваше устройство поддерживает маркировку ToS (тип обслуживания) и DiffServ (дифференциация служб). За счет этого устройство может маркировать голосовые кадры, которые будут в приоритетном порядке передаваться по сети.

SIP ALG

Ваше устройство представляет собой шлюз прикладного уровня для SIP (SIP ALG), позволяющий пропускать вызовы VoIP через NAT к устройствам, расположенным за NAT (например, к компьютерам с программами, реализующими VoIP на основе SIP).

Универсальная технология “включи и работай” (UPnP)

Используя стандартный протокол TCP/IP, ваше устройство может динамически включаться в сеть с устройствами, поддерживающими UPnP, получать IP-адрес и сообщать свои возможности другим сетевым устройствам.

Поддержка PPPoE (RFC2516)

Протокол передачи от точки к точке через Ethernet (PPPoE) эмулирует коммутируемое соединение. Он позволяет поставщикам услуг Интернета сохранить существующую конфигурацию сети при переходе к новым технологиям широкополосного доступа, в частности - ADSL. Драйвер PPPoE в составе вашего устройства прозрачен по отношению к компьютерам в локальной сети, которые работают исключительно в сегменте Ethernet и не могут заметить наличия PPPoE. Это исключает необходимость в управлении клиентами PPPoE на отдельных компьютерах.

Другие функции PPPoE

- Завершение PPPoE-сеанса при отсутствии активности
- Автоматическое инициирование PPPoE-сеанса (dial on demand)

Поддержка DNS для динамических адресов

Службы DNS для динамических адресов позволяют использовать фиксированное доменное имя для хоста с динамическим IP-адресом, упрощая доступ к хосту из Интернета. Такая услуга предоставляется поставщиком услуг DNS после соответствующей регистрации.

DHCP

Протокол DHCP (динамический протокол настройки хоста) позволяет отдельным клиентским компьютерам получать при загрузке конфигурацию TCP/IP от центрального DHCP-сервера. Ваше устройство имеет встроенный DCHP-сервер, который по умолчанию активен. Устройство назначает DHCP-клиентам IP-адреса, адрес шлюза по умолчанию и адреса DNS-серверов. Ваше устройство также может выступать в качестве промежуточного DHCP-сервера (сервера ретрансляции) для пересылки назначаемых IP-адресов от фактического DHCP-сервера к клиентам.

Поддержка нескольких PVC (постоянных виртуальных каналов)

Ваше устройство поддерживает до 8 постоянных виртуальных каналов (PVC).

Совмещение IP-адресов

Совмещение IP-адресов (IP aliasing) позволяет разделить физическую сеть на различные логические сети через один и тот же интерфейс Ethernet. Ваше устройство позволяет настроить до трех логических интерфейсов LAN на одном физическом интерфейсе Ethernet, при этом устройство будет выступать в качестве межсетевого шлюза для каждой сети LAN.

Политики маршрутизации IP (IPPR)

Обычно решения о маршрутизации принимаются только по адресу получателя, и маршрутизатор выбирает для отправки пакета кратчайший путь. Политика маршрутизации IP (IPPR) реализует алгоритм, заменяющий стандартный механизм маршрутизации и позволяющий изменить правила пересылки пакетов в зависимости от политики, настраиваемой администратором.

Фильтры пакетов

В устройстве предусмотрена функция фильтрации пакетов для реализации механизмов безопасности и управления сетью.

Простота установки

Устройство обеспечивает возможность быстрой, интуитивно понятной и простой установки.

Корпус

Компактный и вентилируемый корпус устройства занимает минимальную площадь и не потребует высвобождать место в тесном офисном помещении.

1.3 Функции беспроводной связи (только в моделях с индексом “W”)

Беспроводная сеть стандарта IEEE 802.11g

Стандарт IEEE 802.11g сохраняет полную совместимость со стандартом IEEE 802.11b. Это означает, что радиоплата 802.11b может непосредственно взаимодействовать с устройством 802.11g (и наоборот) на скорости 11 Мбит/с или ниже в зависимости от диапазона. Стандарт 802.11g имеет несколько промежуточных скоростей между максимальной и минимальной скоростью передачи данных. Стандарт 802.11g предусматривает следующие скорости передачи данных и типы модуляции:

Таб. 3 IEEE 802.11g

СКОРОСТЬ ПЕРЕДАЧИ ДАННЫХ (МБИТ/С)	МОДУЛЯЦИЯ
1	DBPSK (дифференциальная двухпозиционная фазовая манипуляция)
2	DQPSK (дифференциальная квадратурная фазовая манипуляция)
5.5 / 11	CCK (манипуляция дополнительного кода)
6/9/12/18/24/36/48/54	OFDM (мультиплексирование с ортогональным частотным разделением сигналов)

Примечание: На функционирование устройства могут воздействовать другие источники радиочастоты 2,4 ГГц, например, микроволновые печи, беспроводные телефоны, устройства, в которых используется технология Bluetooth, и другие беспроводные устройства для LAN.

Беспроводная сеть стандарта IEEE 802.11g+

Ваше устройство поддерживает модификацию стандарта IEEE 802.11g+, благодаря чему другие беспроводные устройства ZyXEL с поддержкой IEEE 802.11g+ могут связываться с P-2602 на большей скорости по сравнению с обычным стандартом IEEE 802.11g.

Внешняя антенна

P-2602 оснащается внешней антенной для устойчивой радиосвязи между беспроводными станциями и точками доступа.

Фильтрация MAC-адресов в беспроводной сети

Ваше устройство может проверять MAC-адреса беспроводных станций, сравнивая их со списком разрешенных или запрещенных MAC-адресов.

Протокол шифрования WEP

WEP (Wired Equivalent Privacy – “конфиденциальность, характерная для проводной связи“) обеспечивает шифрование кадров данных при пересылке по беспроводной сети для защиты от перехвата.

Защищенный доступ по Wi-Fi

Защищенный доступ по Wi-Fi (WPA) реализует подмножество функций стандарта информационной безопасности IEEE 802.11i. Ключевым различием между WPA и WEP является аутентификация пользователя и улучшенное шифрование данных.

WPA2

WPA 2 (IEEE 802.11i) – стандарт безопасности для беспроводных сетей, ставящий более жесткие требования к криптостойкости и управлению ключами по сравнению с WPA.

WMM QoS

WMM QoS (механизм качества обслуживания для мультимедийных приложений Wi-Fi) позволяет задать приоритеты беспроводного трафика в соответствии с потребностями отдельных сетевых служб.

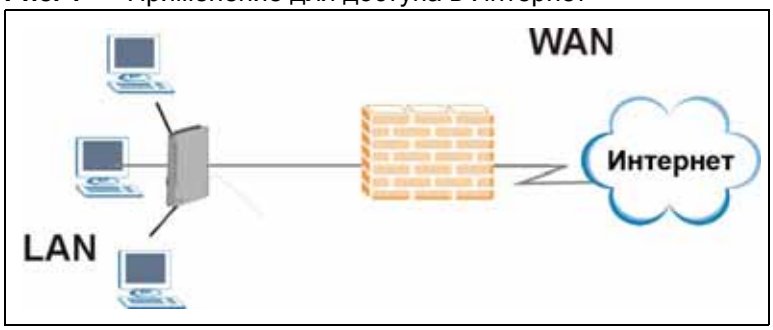
1.4 Области применения P-2602

Ниже рассмотрены примеры применений, для которых P-2602 подходит наилучшим образом.

1.4.1 Доступ к Интернету

Ваше устройство будет идеальным решением для высокоскоростного доступа в Интернет. Оно поддерживает семейство протоколов TCP/IP, используемых в Интернете. Устройство совместимо с оборудованием DSLAM (мультиплексорами ADSL) всех крупных поставщиков. DSLAM представляет собой стойку с линейными платами ADSL, заведенными на магистральный сетевой интерфейс/канал (например, T1, OC3, DS3, ATM или Frame Relay). Для ADSL такое устройство можно считать эквивалентом стойки с ADSL-модемами. Устройство дополнительно позволяет клиентам беспроводной сети обращаться к ресурсам вашей локальной сети и Интернета. Типовой вариант организации доступа в Интернет изображен ниже.

Рис. 1 Применение для доступа в Интернет



1.4.1.1 Доступ в Интернет с одной учетной записью

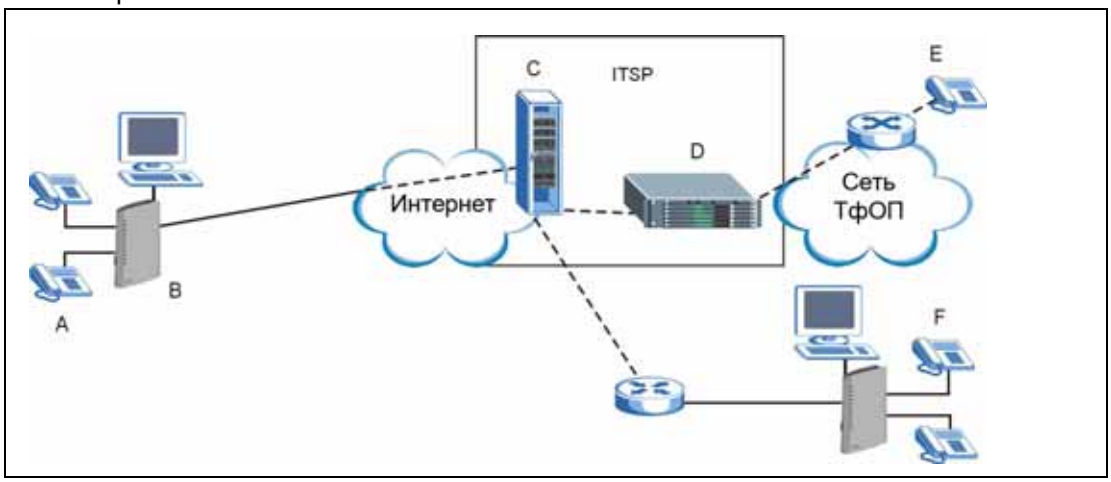
Для сетевых окружений класса SOHO (дом / небольшой офис) устройство предусматривает функцию SUA (Single User Account – учетная запись одного пользователя), позволяющую нескольким пользователям в локальной сети (LAN) одновременно выходить в Интернет, используя один IP-адрес

1.4.2 Телефонная связь через поставщика услуг Интернет-телефонии

В домашней сети или небольшом офисе устройство позволяет делать и принимать телефонные вызовы через поставщика услуг Интернет-телефонии (ITSP).

На следующем рисунке показана примерная схема вызова в режиме VoIP через ITSP. Вы используете аналоговый телефон (A), а ваш маршрутизатор (B) преобразует телефонный вызов в вызов VoIP. После этого устройство передает вызов через Интернет на SIP-сервер ITSP. Сервер вызовов VoIP переадресует вызовы на телефоны ТфОП (E) через шлюз группообразования (D) в сеть ТфОП. Сервер вызовов VoIP направляет вызовы на IP-телефоны (F) через Интернет.

Рис. 2 Применение для телефонной связи через поставщика услуг Интернет-телефонии

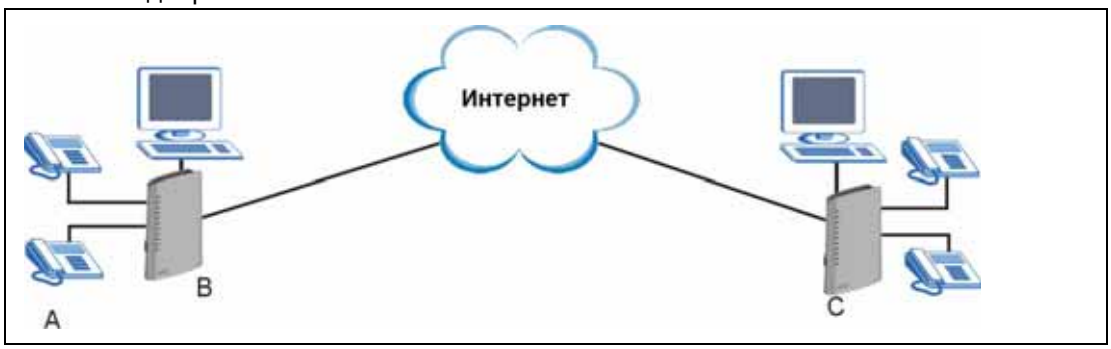


1.4.3 Телефонная связь в одноранговом режиме

Можно устанавливать телефонное соединение напрямую с указанным IP-адресом, не используя прокси-сервер SIP. Такие одноранговые вызовы также называются вызовами по схеме “точка-точка” или “IP-адрес – IP-адрес”. Для них необходимо, чтобы был известен IP-адрес удаленной стороны.

На следующем рисунке показана примерная схема VoIP-вызова в одноранговом режиме. Вы используете аналоговый телефон (A), а ваш маршрутизатор (B) преобразует телефонный вызов в вызов VoIP, передавая его через Интернет удаленному устройству VoIP (C).

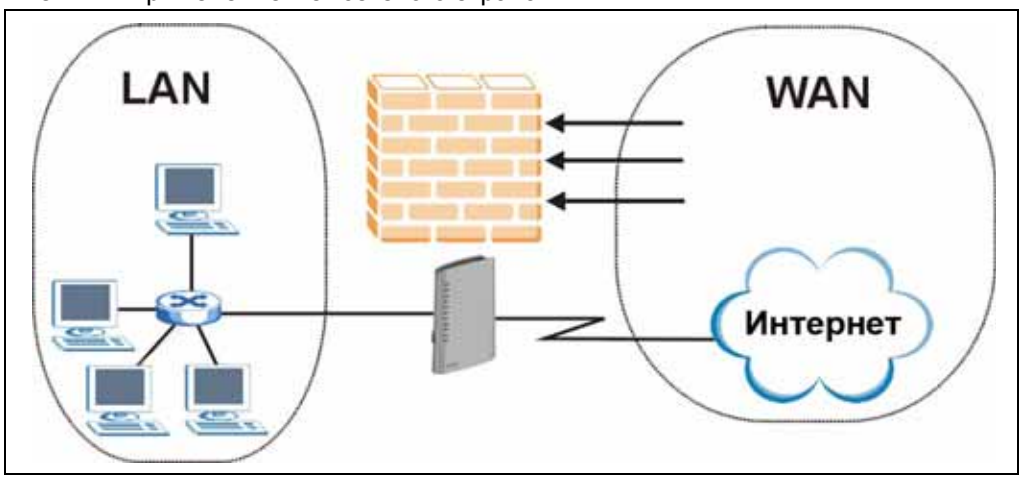
Рис. 3 Одноранговый вызов



1.4.4 Межсетевой экран для безопасного широкополосного доступа в Интернет

Ваше устройство обеспечивает защиту от нападений интернет-хакеров. По умолчанию межсетевой экран блокирует весь входящий трафик со стороны WAN. Межсетевой экран поддерживает анализ пакетов TCP/UDP, обнаружение DoS-атак, а также имеет средства информирования в реальном времени, ведения отчетов и журналов.

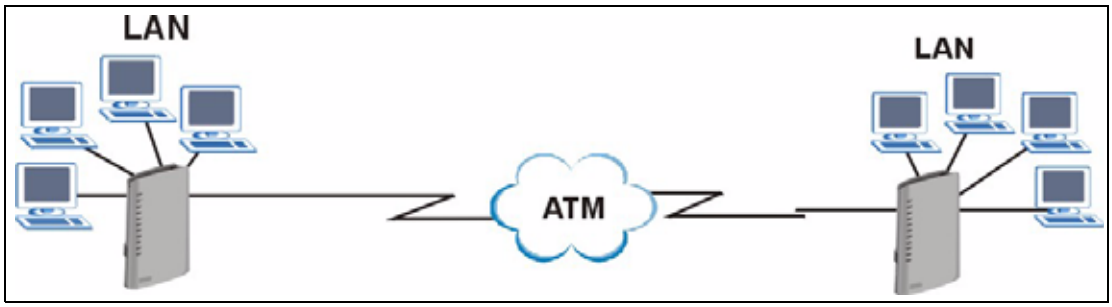
Рис. 4 Применение межсетевого экрана



1.4.5 Объединение локальных сетей

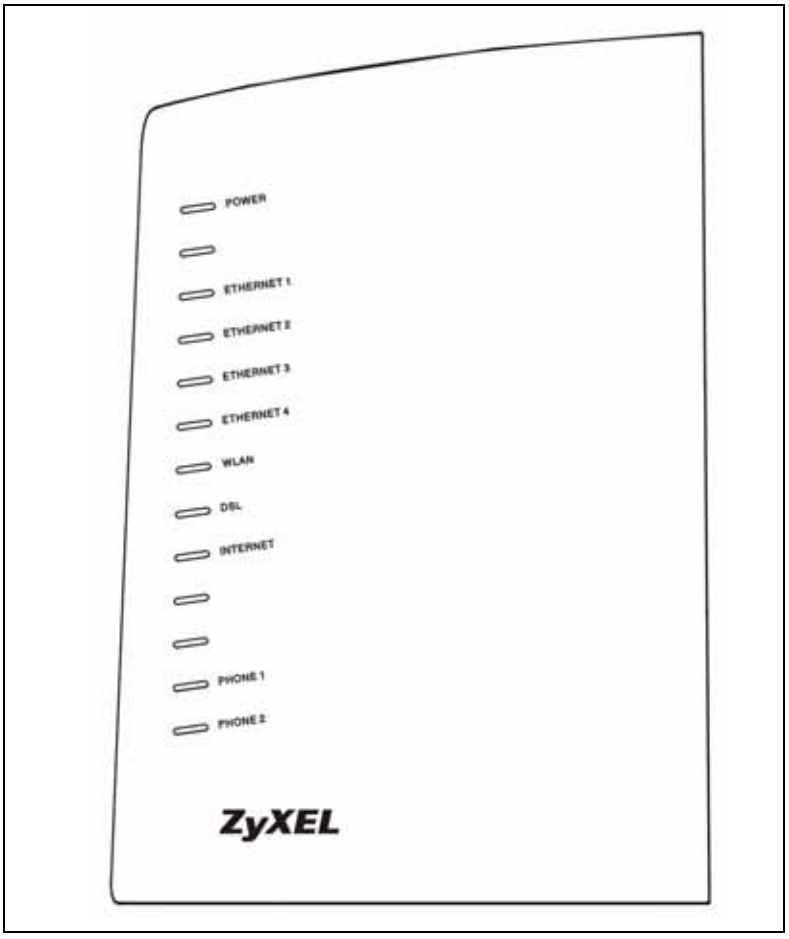
Устройство можно использовать для соединения двух территориально разнесенных сетей по ADSL-линиям. Ниже изображен типовой вариант применения устройства для объединения локальных сетей.

Рис. 5 Объединение локальных сетей



1.4.6 Светодиоды

Рис. 6 Светодиоды



Светодиоды на корпусе устройства описаны в следующей таблице.

Таб. 4 Светодиоды

СВЕТО-ДИОДЫ	ЦВЕТ	СОСТОЯНИЕ	ОПИСАНИЕ
POWER	Зелёный	Вкл.	Устройство включено и работает исправно.
		Мигание	Устройство перезагружается и выполняет самодиагностику.
	Красный	Вкл.	Устройство не готово к работе или находится в состоянии сбоя.
	Нет	Выкл.	Устройство выключено.
ETHERNET 1-4	Зелёный	Вкл.	Устройство подключено к Ethernet-сети.
		Мигание	P-2602 передает/принимает данные.
	Нет	Выкл.	Соединение на Ethernet-порту отсутствует.
WLAN (только в моделях с индексом “W”)	Зелёный	Вкл.	Устройство готово, но не осуществляет передачу/прием данных через беспроводную локальную сеть.
		Мигание	Устройство передает/принимает данные через беспроводную локальную сеть.
	Нет	Выкл.	Беспроводная сеть не готова или находится в состоянии сбоя.
DSL	Зелёный	Вкл.	Устройство подключено к DSL-линии.
		Мигание	Устройство инициализирует DSL-линию.
	Нет	Выкл.	DSL-связь отключена.
INTERNET	Зелёный	Вкл.	Устройство установило IP-соединение, но трафик в данный момент отсутствует. Устройству присвоен IP-адрес (статический или полученный от DHCP-сервера) на стороне WAN, PPP-согласование успешно завершено (если оно применяется), и DSL-соединение находится в активном состоянии.
		Мигание	Устройство передает или принимает IP-трафик.
	Красный	Вкл.	Устройство предприняло неудачную попытку установить IP-соединение. Причиной сбоя может быть отсутствие отклика от DHCP-сервера, отсутствие отклика PPPoE или непрохождение аутентификации PPPoE).
	Нет	Выкл.	IP-соединение не установлено
PHONE 1, 2	Зелёный	Вкл.	Для данного телефонного порта зарегистрирована учетная запись SIP.
		Мигание	На телефоне, подключенном к данному телефонному порту, снята трубка или имеется входящий вызов.
	Оранжевый	Вкл.	Для телефонного порта зарегистрирована учетная запись SIP, и для соответствующей учетной записи SIP есть голосовое сообщение.
		Мигание	На телефоне, подключенном к данному телефонному порту, снята трубка или имеется голосовое сообщение для соответствующей учетной записи SIP.
	Нет	Выкл.	Для телефонного порта не зарегистрирована учетная запись SIP.

Указания по подключению аппаратной части см. в Руководстве по быстрому запуску.

Глава 2
Описание веб-конфигуратора

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

2.1 Обзор веб-конфигуратора

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

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

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

Проверка необходимых настроек Internet Explorer описана в гл. 27 на стр. 347.

2.1.1 Вызов веб-конфигуратора

1. Убедитесь, что все аппаратные подключения P-2602 выполнены правильно (см. *Руководство по быстрому запуску*).
2. Откройте веб-браузер.
3. Введите “192.168.1.1”»в качестве URL.
4. Появится экран Password (“Пароль”). Заводской пароль по умолчанию (“1234”) в поле ввода будет скрыт от просмотра. Если вы еще не изменяли пароль, достаточно будет нажать кнопку **Login**. Чтобы восстановить в поле пароль по умолчанию, нажмите **Cancel**. Если вы сменили пароль, введите пароль и нажмите кнопку **Login**.

Рис. 7 Экран ввода пароля

5 Если вы еще не изменяли пароль, появится следующий экран. Настоятельно рекомендуется сменить заводской пароль. Введите новый пароль, повторно введите его для подтверждения и нажмите **Apply**. Если вы не хотите менять пароль, нажмите **Ignore**, чтобы перейти к главному меню.

Рис. 8 Экран смены пароля

6 Появится экран, предлагающий перейти к мастеру или к экранам расширенной настройки.

- Если вы впервые вошли в систему и хотите выполнить основные настройки, выберите **Go to Wizard setup**. После нажатия кнопки **Apply** появится экран выбора мастера. Дополнительные сведения см. в гл. 3 на стр. 61.
- Чтобы настроить функции, не предусмотренные в мастерах, нажмите **Go to Advanced setup**. Если вы хотите всегда напрямую переходить к расширенным экранам, отметьте флажок. После нажатия кнопки **Apply** появится основной экран. Дополнительные сведения см. в разд. 2.2 на стр. 56.
- Чтобы покинуть веб-конфигуратор, выберите **Exit**.

Примечание: Для защиты от несанкционированного использования P-2602 автоматически завершает сеанс веб-конфигуратора, если он не использовался в течение пяти минут. В этом случае достаточно повторно войти в систему.

Рис. 9 Экран мастера или расширенной настройки

2.1.2 Кнопка сброса

Кнопку **RESET**, расположенную сзади на корпусе устройства, можно использовать для включения или выключения беспроводной локальной сети. Ее также можно использовать для активации OTIST, чтобы присвоить параметры безопасности беспроводным клиентам. Если вы забыли пароль или не можете получить доступ к веб-конфигуратору, с помощью кнопки **RESET** можно загрузить в устройство заводские настройки. При этом будут потеряны все настройки, выполненные ранее, а в качестве пароля будет восстановлен “1234”. Можно также использовать

2.1.2.1 Использование кнопки сброса

1. Убедитесь, что светодиод **POWER** горит (не мигает).
2. Выполните одну из следующих операций.

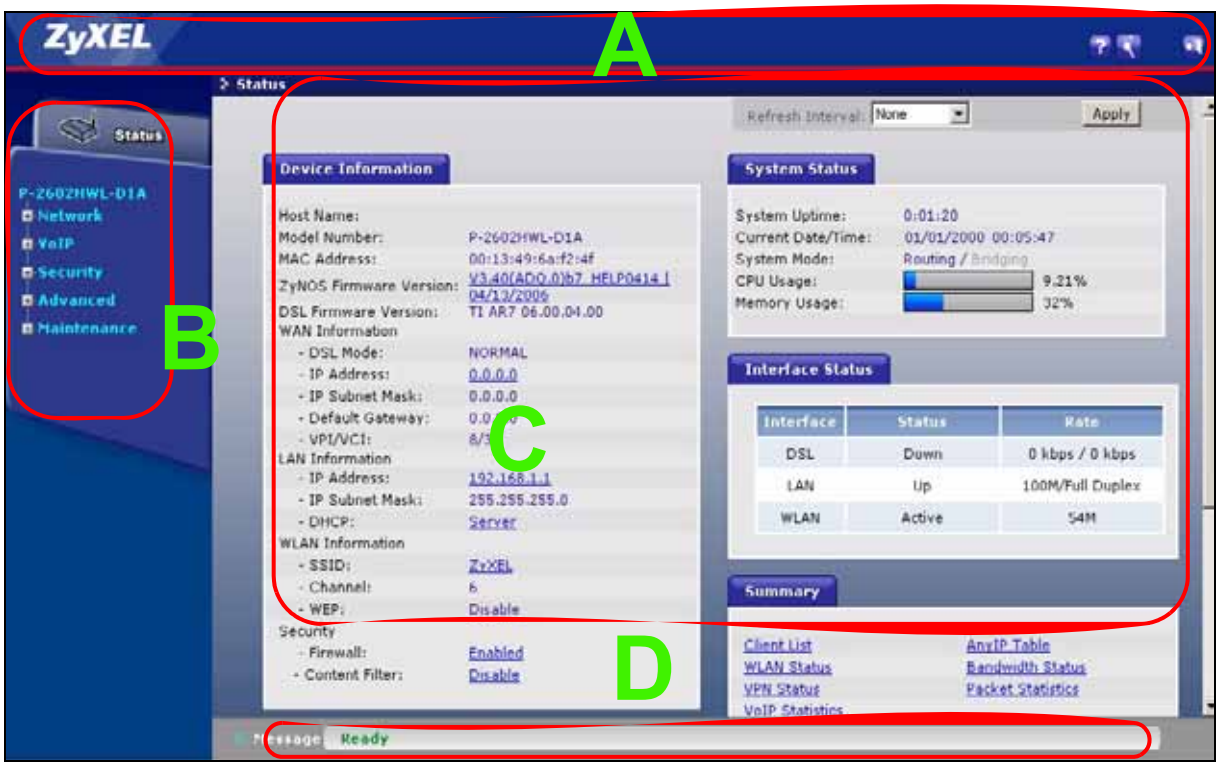
   Чтобы включить или отключить беспроводную сеть, нажмите кнопку **RESET** на одну секунду и отпустите ее. Светодиод **WLAN** должен загореться или погаснуть. (только в моделях с индексом “W”)

   Чтобы активировать OTIST и присвоить параметры безопасности беспроводным клиентам, нажмите кнопку **RESET** на пять секунд и отпустите ее. Светодиод **WLAN** LED будет мигать, пока устройство посредством OTIST рассылает параметры беспроводной сети клиентам OTIST (только в моделях с индексом “W”).

   Чтобы возвратить устройство к заводским настройкам, держите кнопку the **RESET** нажатой десять секунд или пока не начнет мигать СВЕТОДИОД **POWER**, затем отпустите кнопку. Когда светодиод **POWER** начинает мигать, это значит, что значения по умолчанию восстановлены, и устройство перезагружается.

2.2 Основной экран веб-конфигуратора

Рис. 10 Основной экран



Как показано выше на рисунке, основной экран поделен на следующие области:

- **A** - область заголовка
- **B** - панель навигации
- **C** - основное окно
- **D** - строка состояния

2.2.1 Область заголовка

Область заголовка позволяет выбрать язык и содержит в верхнем правом углу несколько значков.

Эти значки вызывают следующие функции.

Таб. 5 Значки в заголовках экранов веб-конфигуратора

ЗНАЧОК	ОПИСАНИЕ
	**Справка**: Этот значок вызывает экраны справки.
	**Мастера**: Этот значок служит для перехода к мастерам настройки. Дополнительные сведения см. в гл. 3 на стр. 61.
	**Завершение сеанса**: Это значок служит для выхода из веб-конфигуратора.

2.2.2 Панель навигации

Пункты меню в навигационной панели открывают экраны для настройки параметров P-2602. Каждый пункт меню описан в следующих таблицах.

Таб. 6 Общая структура панели навигации

ССЫЛКА	ВКЛАДКА	НАЗНАЧЕНИЕ
Status		Это окно содержит административную и относящуюся к системе информацию.
Network		
WAN	Internet Connection	Этот экран служит для настройки параметров поставщика услуг Интернета, присвоения IP-адресов в сети WAN, настройки адресов DNS-серверов и других дополнительных параметров.
LAN	IP	Этот экран служит для настройки параметров TCP/IP локальной сети, включения функции "Any IP" и настройки других дополнительных параметров.
	DHCP Setup	Этот экран служит для настройки параметров DHCP для локальной сети.
	Client List	Этот экран служит для просмотра текущих параметров DHCP-клиентов и привязки постоянных IP-адресов к определенным MAC-адресам (и именам хостов).
	IP Alias	Этот экран служит для разделения интерфейса LAN на подсети.
Wireless LAN (только в моделях с индексом “W”)	General	Это экран служит для настройки общих параметров беспроводной локальной сети (WLAN), а также параметров аутентификации и безопасности WLAN.
	OTIST	Этот экран служит для присвоения параметров беспроводной сети беспроводным клиентам.
	Экран MAC Filter	Этот экран служит для настройки исключительного доступа определенных беспроводных клиентов к P-2602 или ограничения доступа определенных беспроводных клиентов к P-2602.
	QoS	WMM QoS позволяет задать приоритеты беспроводного трафика в соответствии с потребностями отдельных сетевых служб.
	Local User Database	Этот экран служит для настройки встроенных пользовательских профилей для аутентификации станций беспроводной сети.

Таб. 6 Общая структура панели навигации

ССЫЛКА	ВКЛАДКА	НАЗНАЧЕНИЕ
NAT	General	Этот экран служит для активации NAT.
	Port Forwarding	Этот экран позволяет сделать локальные серверы доступными внешнему миру.
	Address Mapping	Этот экран позволяет настроить параметры привязки для трансляции сетевых адресов.
VoIP		
SIP	SIP Settings	Этот экран служит для настройки параметров голосовой связи по IP в P-2602.
	QoS	Это окно служит для настройки параметров качества обслуживания VoIP в P-2602.
Phone	Analog Phone	Этот экран позволяет настроить привязку телефонных портов к учетным записям.
	Common	Этот экран служит для настройки общих параметров телефонного порта.
	Region	Этот экран служит для указания вашего местонахождения и выбора режима обработки вызовов.
Phone Book	Incoming Call Policy	Этот экран служит для настройки переадресации телефонного вызова.
	Speed Dial	Этот раздел служит для добавления, редактирования и удаления часто используемых номеров из телефонной книги SIP.
PSTN Line (“L” models only)	General	Этот экран служит для настройки параметров ТфОП в P-2602.
Security		
Firewall	General	Этот экран служит для включения/отключения межсетевого экрана и выбора действий, выполняемых по умолчанию над сетевым трафиком в определенных направлениях.
	Rules	Этот экран содержит сводку правил межсетевого экрана и позволяет редактировать/добавлять правила.
	Anti Probing	Этот экран позволяет настроить ответ устройства на эхозапросы и запросы сетевых служб, не отмеченных как общедоступные.
	Threshold	Этот экран позволяет задать пороговые значения для разрыва не полностью открытых сеансов.
Content Filter	Keyword	Этот экран служит для блокирования доступа к веб-сайтам по определенным ключевым словам в URL.
	Schedule	Этот экран служит для задания дней и периодов в течение дня, в которые активируется фильтрация содержания.
	Trusted	Этот экран позволяет в исключительном порядке отменить фильтрацию содержания для определенных пользователей в локальной сети.
VPN	Setup	Этот экран служит для настройки туннелей VPN.
	Monitor	Этот экран служит для просмотра текущего состояния каждого туннеля VPN.
	VPN Global Setting	Этот экран позволяет разрешить прохождение трафика NetBIOS через туннели VPN.
Advanced		

Таб. 6 Общая структура панели навигации

ССЫЛКА	ВКЛАДКА	НАЗНАЧЕНИЕ
Static Route	IP Static Route	Этот экран служит для настройки статических маршрутов IP, сообщающих устройству о конфигурации сетей, расположенных за непосредственно подключенными удаленными узлами.
Bandwidth MGMT	Summary	Этот экран служит для настройки управления полосой пропускания интерфейса.
	Rule Setup	Этот экран служит для настройки правила управления полосой пропускания.
	Monitor	Этот экран служит для просмотра текущего использования и распределения полосы пропускания в P-2602.
Dynamic DNS		Этот экран позволяет настроить статическое имя хоста для динамического IP-адреса.
Remote MGMT	WWW	Этот экран позволяет выбрать интерфейсы и IP-адреса, с которых пользователям разрешается управлять P-2602 по протоколу HTTP.
	Telnet	Этот экран позволяет выбрать интерфейсы и пользователей (IP-адреса), которым разрешается управлять устройством P-2602 по протоколу Telnet.
	FTP	Этот экран позволяет выбрать интерфейсы и пользователей (IP-адреса), которым разрешается управлять устройством P-2602 по протоколу FTP.
	SNMP	Этот экран служит для настройки параметров управления P-2602 по упрощенному протоколу управления сетью (SNMP).
	DNS	Этот экран позволяет выбрать интерфейсы и пользователей (IP-адреса), которым разрешается направлять DNS-запросы на P-2602.
	ICMP	На этом экране указывается, должно ли устройство отвечать на эхозапросы и обращения к недоступным службам.
UPnP	General	Этот экран позволяет включить или отключить поддержку UPnP.
Maintenance		
System	General	Этот экран позволяет задать название устройства, доменное имя, период неактивности сеанса управления и пароль.
	Time Setting	Это окно служит для настройки даты и времени в P-2602.
Logs	View Log	Этот экран служит для просмотра журналов устройства.
	Log Settings	Этот экран позволяет выбрать типы журналов и срочных предупреждений, которые должно отмечать устройство . Также можно настроить отправку журналов по электронной почте.
Tools	Firmware	Этот экран служит для загрузки микропрограмм в устройство.
	Configuration	Этот экран служит для резервного копирования и восстановления конфигурации, а также для сброса к заводским настройкам по умолчанию.
	Restart	Этот экран служит для перезагрузки P-2602 без выключения питания.
Диагностика	General	Этот экран служит для проверки соединения с другими устройствами.
	DSL Line	На этом экране отображаются данные, которые могут помочь вам при диагностике проблем с DSL-подключением.

2.2.3 Основное окно

В основном окне отображается информация и поля для настройки. Работа с этим окном будет рассмотрена далее.

Непосредственно после входа в систему появляется экран **Status**. Дополнительные сведения о работе с экраном **Status** см. в гл. 6 на стр. 89.

2.2.4 Строка состояния

После нажатия кнопки **Apply** или **OK** проверяйте строку состояния, чтобы удостовериться, что настройки действительно обновлены.

Глава 3
Экраны мастеров настройки подключения к Интернету и беспроводной сети

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

3.1 Введение

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

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

3.2 Мастер настройки доступа к Интернету

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

Рис. 11 Выбор режима

2 Для настройки доступа в Интернет и беспроводной сети выберите **INTERNET/ WIRELESS SETUP**.

Рис. 12 Экран приветствия мастера

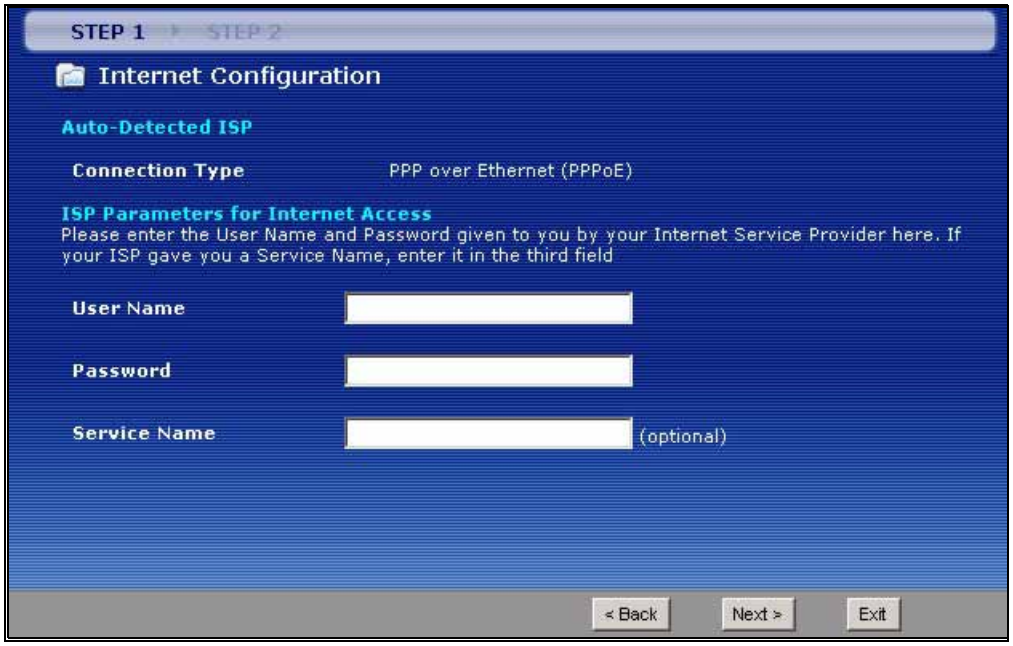
3 Устройство ZyXEL попытается автоматически найти DSL-соединение и обнаружить тип соединения.

a Если подключение не найдено, появится следующий экран. Проверьте, правильно ли подключено оборудование, и выберите **Restart the Internet/Wireless Setup Wizard**, чтобы вернуться на экран приветствия мастера. Если вы по-прежнему не можете соединиться, выберите **Manually configure your Internet connection**. Следуйте указаниям мастера и введите параметры настройки вашего подключения в том виде, в котором они были сообщены вам поставщиком услуг Интернета. Дополнительные сведения см. в разд. 3.2.1 на стр. 64.
Чтобы пропустить настройку Интернета и настроить параметры беспроводной сети, оставьте выбранным вариант **Yes** и нажмите кнопку **Next**.

Рис. 13 Автоматический поиск: DSL-соединение отсутствует

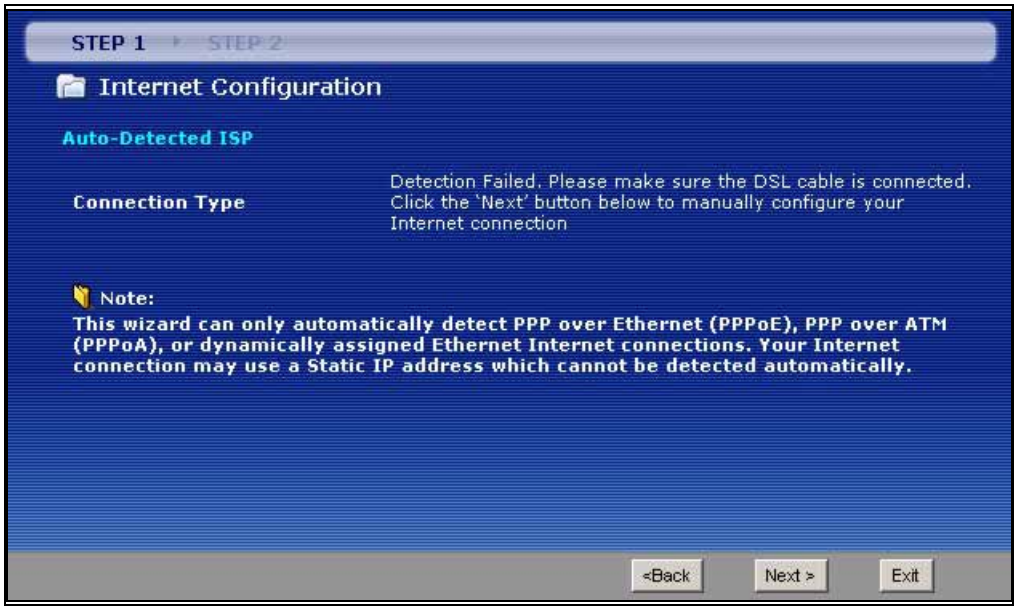
b Если обнаружено соединение по протоколу PPPoE или PPPoA появится следующий экран. Введите параметры вашей учетной записи (имя пользователя, пароль, и/или название службы) в том виде, в котором они сообщены поставщиком услуг Интернета. Затем нажмите **Next** и перейдите к настройке в мастере беспроводного соединения (см. разд. 3.3 на стр. 69).

Рис. 14 Автоматический поиск: PPPoE



c Следующий экран появляется, если устройство ZyXEL обнаруживает наличие соединения, но не определяет его тип. Нажмите **Next**. Указания по ручной настройке P-2602 для доступа в Интернет см. в разд. 3.2.1 на стр. 64.

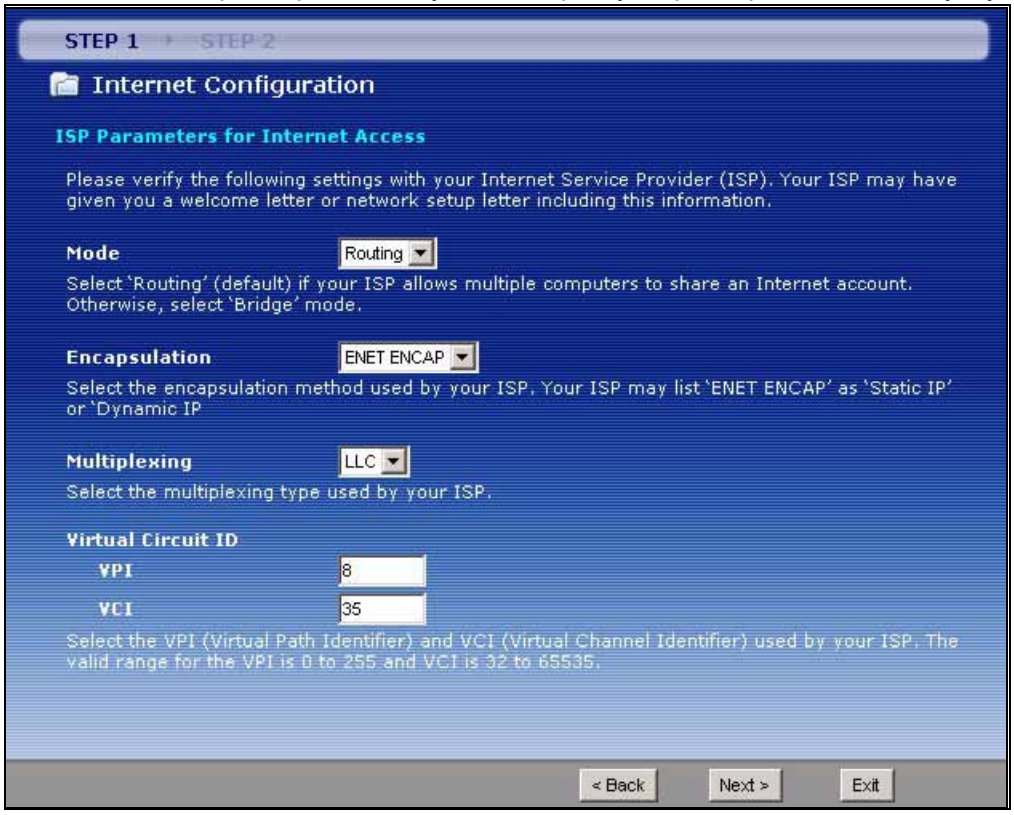
Рис. 15 Автоматический поиск: ошибка



3.2.1 Настройка в ручном режиме

1 Если физическая линия подключена, но P-2602 не может определить тип DSL-соединения, необходимо ввести параметры доступа в Интернет на экране мастера точно в том виде, в котором они сообщены поставщиком услуг. Во всех полях, информация по которым у вас отсутствует, оставьте значения по умолчанию.

Рис. 16 Мастер настройки доступа к Интернету: параметры поставщика услуг



Интернета

Поля изображённого выше экрана описаны в следующей таблице.

Таб. 7 Мастер настройки доступа к Интернету: параметры поставщика услуг Интернета

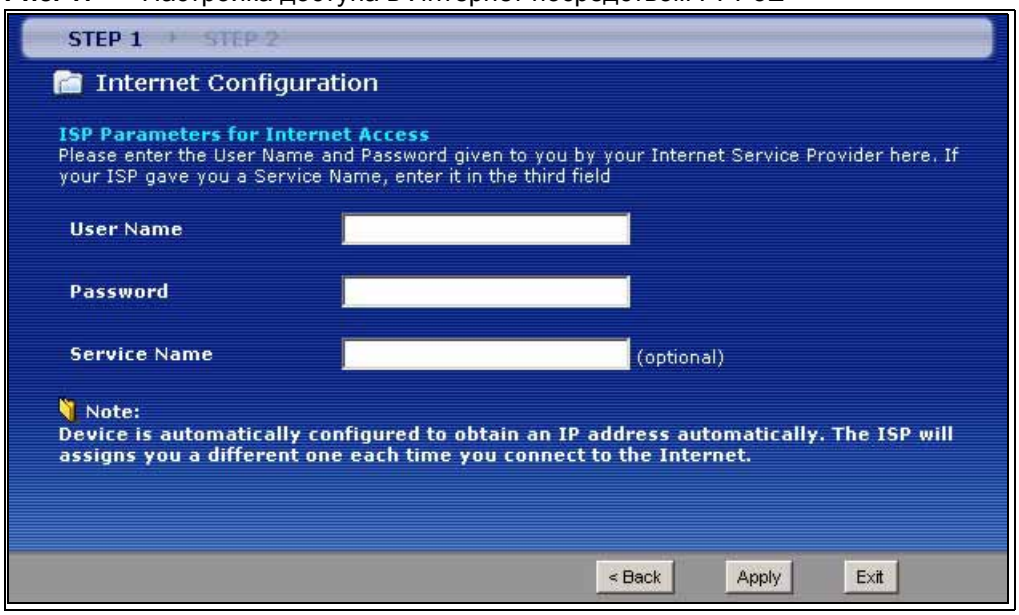
ПОЛЕ	ОПИСАНИЕ
Mode	Если ваш поставщик услуг Интернета позволяет использовать одну учетную запись с нескольких компьютеров, в поле **Mode** выберите **Routing** (этот режим действует по умолчанию). В противном случае выберите режим моста **Bridge**.
Encapsulation	Выберите тип инкапсуляции, используемый поставщиком услуг Интернета, из раскрывающегося списка **Encapsulation**. Доступные варианты зависят от режима, выбранного в поле **Mode**. Если в поле Mode выбран режим **Bridge**, выберите **PPPoA** или **RFC 1483**. Если в поле Mode выбран режим **Routing**, выберите **PPPoA**, **RFC 1483**, **ENET ENCAP** или **PPPoE**.

Таб. 7 Мастер настройки доступа к Интернету: параметры поставщика услуг Интернета

ПОЛЕ	ОПИСАНИЕ
Multiplexing	Выберите тип мультиплексирования, используемый поставщиком услуг Интернета, из раскрывающегося списка **Multiplex**: VC-based (мультиплексирование на основе виртуальных каналов) или LLC-based (мультиплексирование на основе управления логическим каналом связи).
Virtual Circuit ID	Совокупность VPI (идентификатора виртуального пути) и VCI (идентификатора виртуального канала) определяет виртуальную цепь. Подробное описание см. в приложении.
VPI	Введите присвоенный вам VPI. Это поле могло быть настроено заранее.
VCI	Введите присвоенный вам VCI. Это поле могло быть настроено заранее.
Back	Для возврата к предыдущему экрану нажмите кнопку **Back**.
Next	Для перехода к следующему экрану мастера нажмите кнопку **Next**. Экран мастера, который появится следующим, зависит от протокола, выбранного выше.
Exit	Чтобы закрыть экран мастера, не внося изменений, выберите **Exit**.

2 Вид следующего экрана мастера зависит от выбранного режима и типа инкапсуляции. Все экраны приведены для режима маршрутизации. Заполните поля и нажмите кнопку **Next** для продолжения. Описание мастера настройки беспроводного подключения см. в разд. 3.3 на стр. 69.

Рис. 17 Настройка доступа в Интернет посредством PPPoE

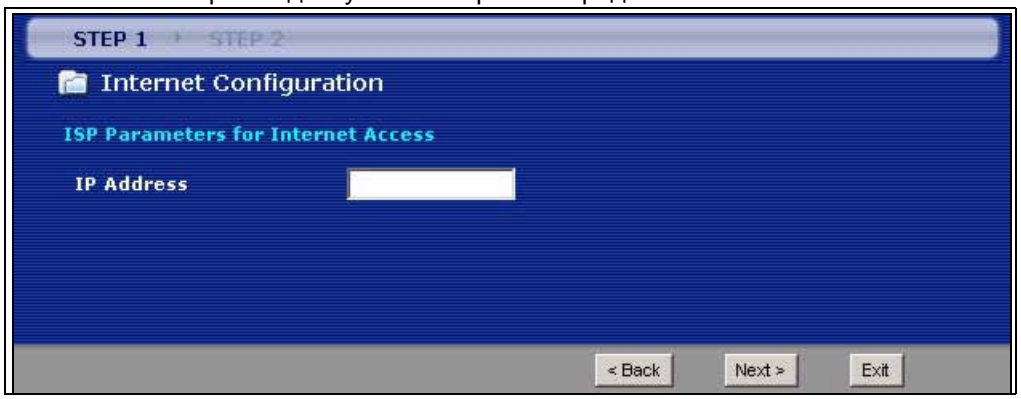


Поля изображённого выше экрана описаны в следующей таблице.

Таб. 8 Настройка доступа в Интернет посредством PPPoE

ПОЛЕ	ОПИСАНИЕ
User Name	Введите имя пользователя в точности так, как оно указано поставщиком услуг. Если поставщик присвоил имя пользователя в формате пользователь@домен, где доменом является название службы, следует ввести оба компонента в точном соответствии с указаниями.
Password	Введите пароль, связанный с указанным выше именем пользователя.
Service Name	Введите название службы PPPoE.
Back	Для возврата к предыдущему экрану нажмите кнопку **Back**.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-2602.
Exit	Чтобы закрыть экран мастера, не внося изменений, выберите **Exit**.

Рис. 18 Настройка доступа в Интернет посредством RFC 1483

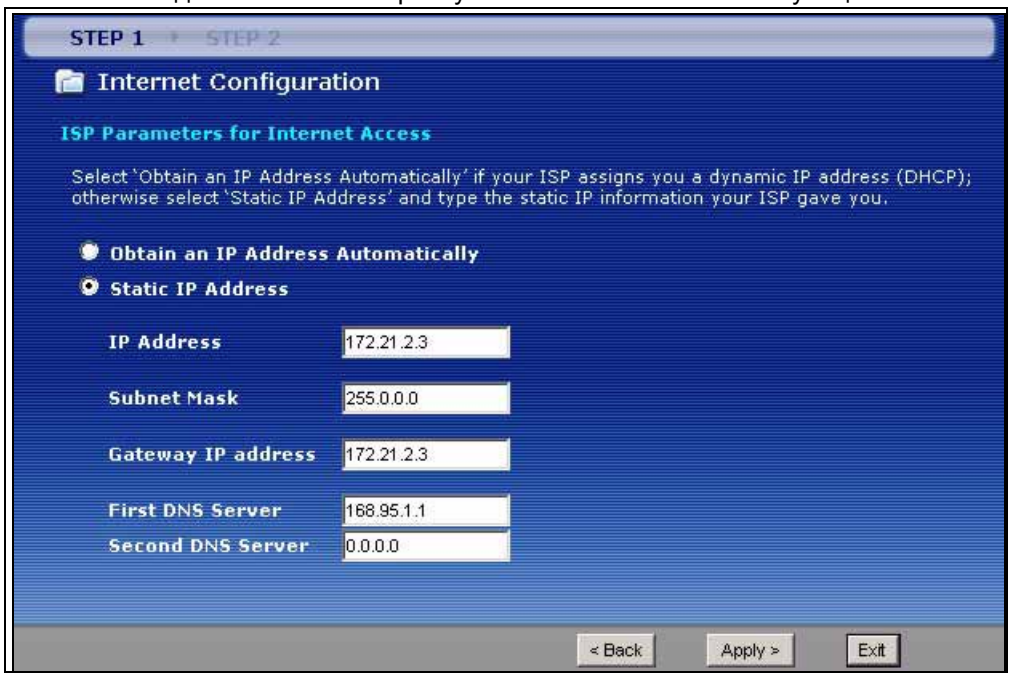


Поля изображённого выше экрана описаны в следующей таблице.

Таб. 9 Настройка доступа в Интернет посредством RFC 1483

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

Рис. 19 Подключение к Интернету с использованием инкапсуляции ENET ENCAP



Поля изображённого выше экрана описаны в следующей таблице.

Таб. 10 Подключение к Интернету с использованием инкапсуляции ENET ENCAP

ПОЛЕ	ОПИСАНИЕ
Obtain an IP Address Automatically	Статический IP-адрес – это фиксированный адрес, выдаваемый поставщиком услуг Интернета. Динамический IP-адрес не имеет постоянного значения; поставщик услуг Интернета для каждого сеанса работы с Интернетом назначает новый адрес. Если вам назначается динамический IP-адрес, выберите **Obtain an IP Address Automatically**.
Static IP Address	Выберите **Static IP Address**, если поставщик услуг Интернета выдал вам статический IP-адрес.
IP Address	Введите IP-адрес, выданный поставщиком услуг Интернета.
Subnet Mask	Введите маску подсети в десятичном виде через точку. Способ расчета маски подсети при делении на подсети описан в приложении.
Gateway IP address	Если на предыдущем экране в поле **Encapsulation** вы выбрали режим **ENET ENCAP**, то здесь необходимо указать IP-адрес шлюза (предоставляемый поставщиком услуг Интернета).
First DNS Server	Введите IP-адреса DNS-серверов. Адреса DNS-серверов передаются клиентским компьютерам вместе с присвоенными им IP-адресами и маской подсети.
Second DNS Server	См. выше.
Back	Для возврата к предыдущему экрану нажмите кнопку **Back**.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-2602.
Exit	Чтобы закрыть экран мастера, не внося изменений, выберите **Exit**.

Рис. 20 Настройка доступа в Интернет посредством PPPoA

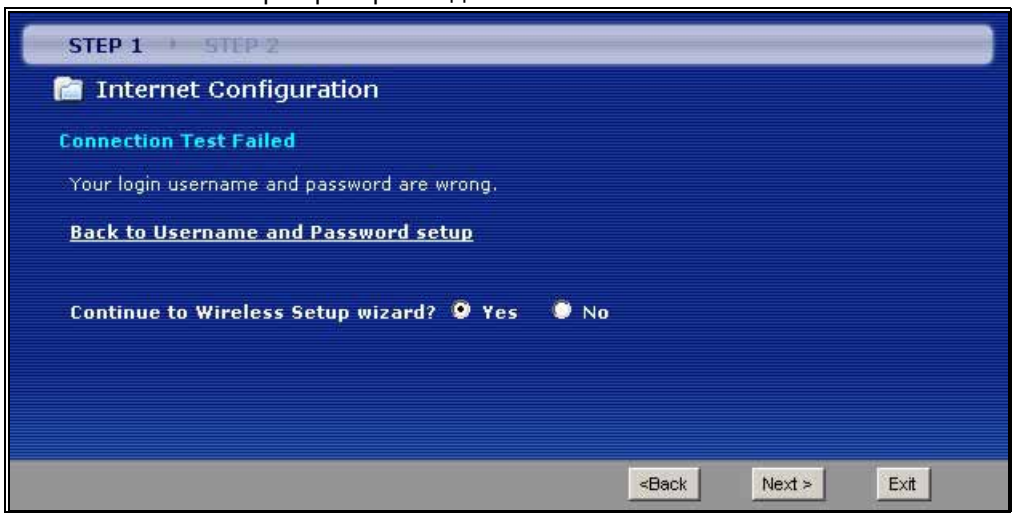
Поля изображённого выше экрана описаны в следующей таблице.

Таб. 11 Настройка доступа в Интернет посредством PPPoA

ПОЛЕ	ОПИСАНИЕ
User Name	Введите имя пользователя, предоставленное поставщиком услуг Интернета.
Password	Введите пароль, связанный с указанным выше именем пользователя.
Back	Для возврата к предыдущему экрану нажмите кнопку **Back**.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-2602.
Exit	Чтобы закрыть экран мастера, не внося изменений, выберите **Exit**.

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

Рис. 21 Ошибка при проверке подключения – 1



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

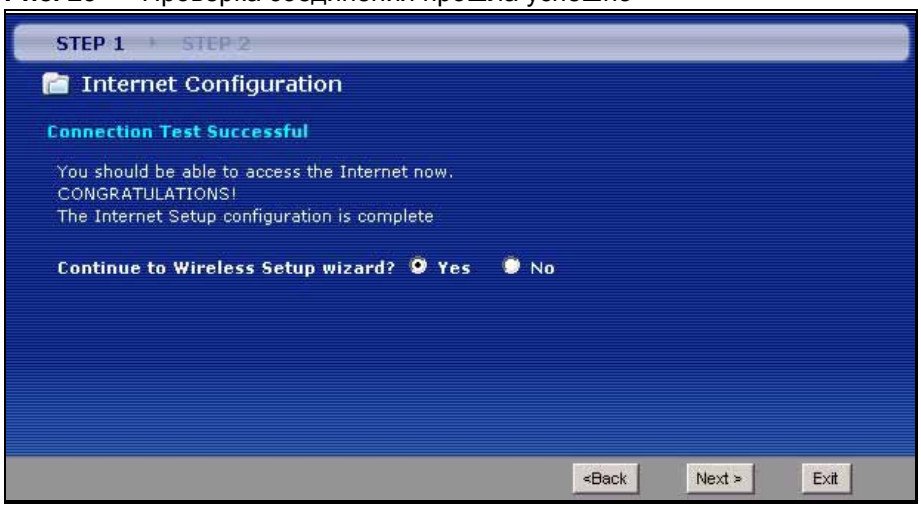
Рис. 22 Ошибка при проверке подключения – 2

3.3 Мастер настройки беспроводного соединения

По завершении настройки параметров доступа в Интернет используйте следующие экраны, чтобы настроить беспроводную локальную сеть.

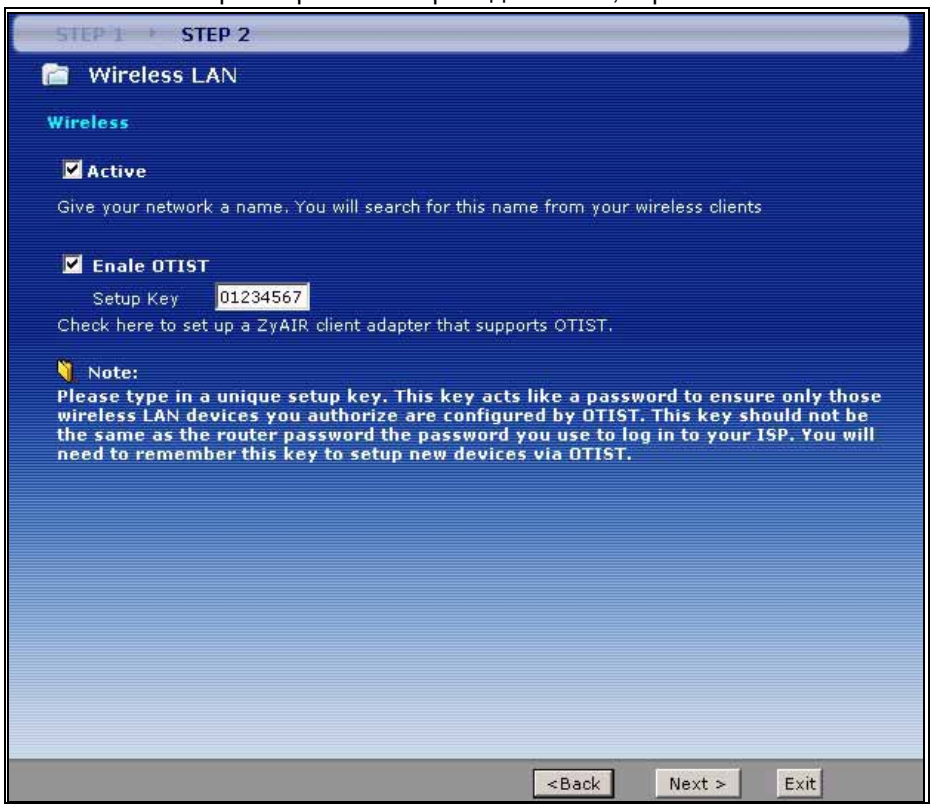
1 Чтобы настроить параметры беспроводной сети, выберите **Yes** и нажмите **Next**. В противном случае выберите **No** и перейдите к шагу 6.

Рис. 23 Проверка соединения прошла успешно



2 Этот экран служит для активации беспроводной сети и OTIST. Чтобы продолжить, нажмите кнопку **Next**

Рис. 24 Мастер настройки беспроводной сети, экран 1



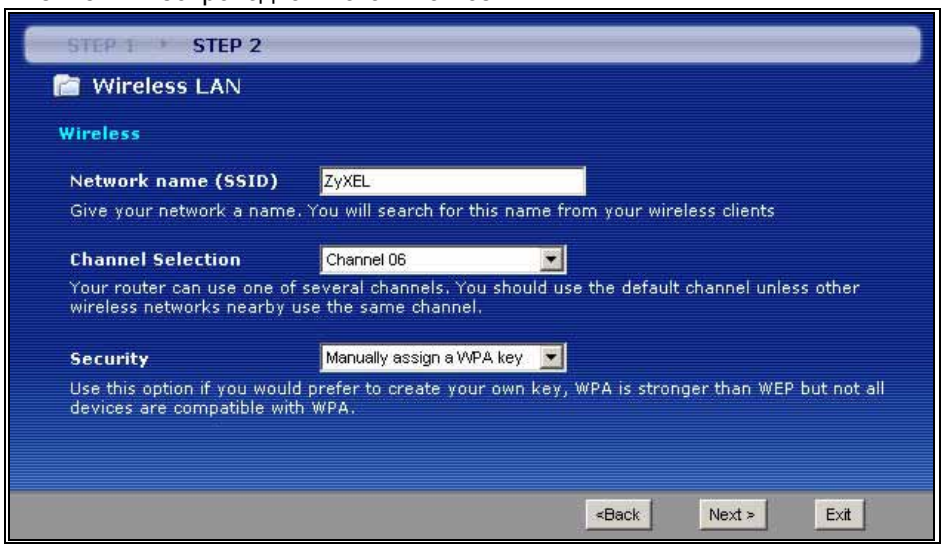
Поля соответствующего экрана описаны в следующей таблице.

Таб. 12 Мастер настройки беспроводной сети, экран 1

ПОЛЕ	ОПИСАНИЕ
Active	Отметьте этот флажок, чтобы включить беспроводную локальную сеть.
Enable OTIST	Отметьте этот флажок, чтобы активировать режим OTIST, позволяющий передать настройки безопасности SSID и WEP/WPA-PSK с P-2602 на беспроводные клиенты, поддерживающие OTIST и находящиеся в зоне покрытия беспроводной сети. OTIST необходимо одновременно активировать и запустить на беспроводном клиенте. Процесс передачи настроек занимает три минуты.
Setup Key	Введите ключ настройки OTIST (**Setup Key**) длиной до восьми знаков ASCII. Помните, что ключ настройки на P-2602 и беспроводных клиентах должен быть одинаковым.
Back	Чтобы перейти на предыдущий экран, выберите **Back**.
Next	Чтобы перейти на следующий экран, выберите **Next**.
Exit	Чтобы закрыть экран мастера, не сохраняя изменений, выберите **Exit**.

3 На этом экране следует указать параметры беспроводной сети. Нажмите **Next**.

Рис. 25 Беспроводная локальная сеть



Поля соответствующего экрана описаны в следующей таблице.

Таб. 13 Мастер настройки беспроводной сети, экран 2

ПОЛЕ	ОПИСАНИЕ
Network Name(SSID)	Введите описательное имя (до 32 символов из 7 бит в кодировке ASCII) для беспроводной LAN. При изменении этого в поля в P-2602 убедитесь в том, что все беспроводные станции используют один и тот же SSID для получения доступа к сети.
Channel Selection	Диапазон радиочастот, используемых беспроводными устройствами IEEE 802.11b/g, называется каналом. Выберите идентификатор канала, не используемый ни одним из находящихся поблизости устройств.
Security	Чтобы настроить ключ WPA посредством OTIST, выберите **Automatically assign a WPA key**. Чтобы задать ключ для предварительного совместного использования (WPA-PSK), выберите **Manually assign a WPA-PSK key**. Выберите этот параметр, если ваши беспроводные клиенты поддерживают WPA. Подробности см. разд. 3.3.1 на стр. 72. Чтобы задать ключ WEP, выберите **Manually assign a WEP key**. Подробности см. разд. 3.3.2 на стр. 73. Чтобы отключить безопасность беспроводной сети и сделать сеть доступной всем устройствам в зоне покрытия, выберите **Disable wireless security**.
Back	Чтобы перейти на предыдущий экран, выберите **Back**.
Next	Чтобы перейти на следующий экран, выберите **Next**.
Exit	Чтобы закрыть экран мастера, не сохраняя изменений, выберите **Exit**.

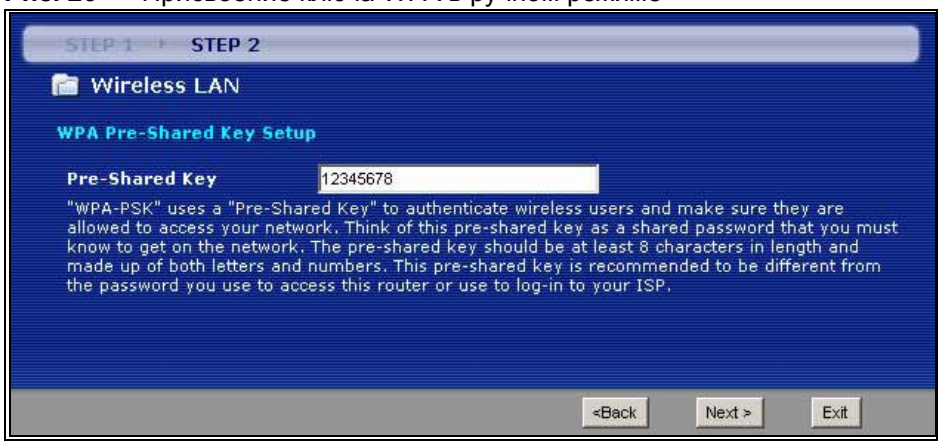
Примечание: Беспроводные станции и P-2602 для установки беспроводной связи должны использовать одно и то же сочетание SSID, идентификатора канала и ключа шифрования (если шифрование включено).

4 Доступные для выбора варианты зависят от режима безопасности, выбранного на предыдущем экране. Заполните соответствующие поля (если это необходимо) и нажмите **Next**.

3.3.1 Присвоение ключа WPA в ручном режиме

Чтобы задать ключ для предварительного совместного использования (**Pre-Shared Key**), на экране настройки беспроводной сети выберите **Manually assign a WPA key**.

Рис. 26 Присвоение ключа WPA в ручном режиме



Поля соответствующего экрана описаны в следующей таблице.

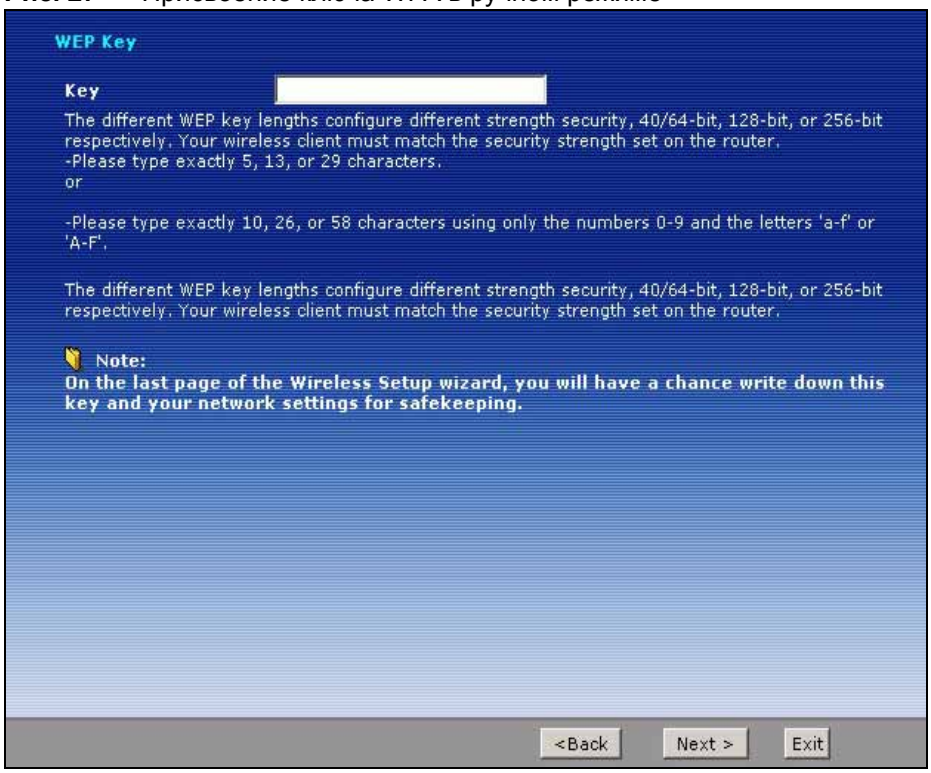
Таб. 14 Присвоение ключа WPA в ручном режиме

ПОЛЕ	ОПИСАНИЕ
Pre-Shared Key	Введите ключ длиной от 8 до 63 символов с учетом регистра в кодировке ASCII. Наибольшую безопасность беспроводного соединения можно обеспечить, настроив WPA на экранах беспроводной сети. Для этого потребуется иметь настроенный сервер аутентификации.
Back	Чтобы перейти на предыдущий экран, выберите **Back**.
Next	Чтобы перейти на следующий экран, выберите **Next**.
Exit	Чтобы закрыть экран мастера, не сохраняя изменений, выберите **Exit**.

3.3.2 Присвоение ключа WPA в ручном режиме

Чтобы настроить параметры шифрования WEP, выберите **Manually assign a WEP key**.

Рис. 27 Присвоение ключа WPA в ручном режиме



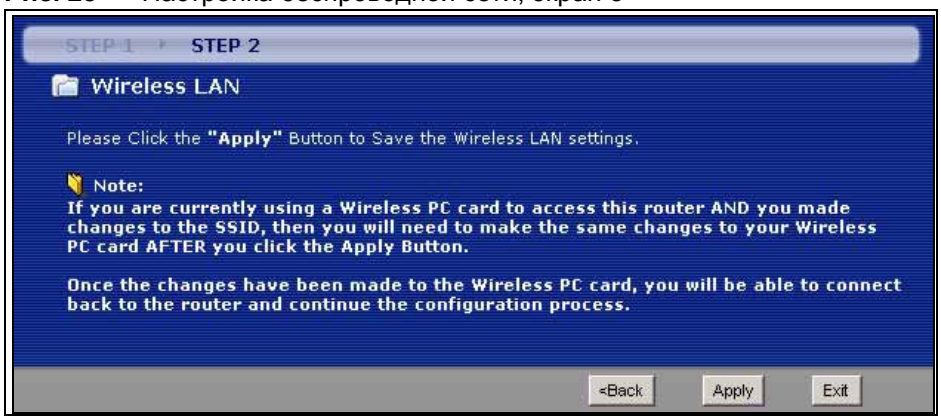
Поля соответствующего экрана описаны в следующей таблице.

Таб. 15 Присвоение ключа WPA в ручном режиме

ПОЛЕ	ОПИСАНИЕ
Key	Ключи WEP используются для шифрования данных. Для передачи данных устройство P-2602 и беспроводные станции должны использовать один и тот же ключ WEP. Введите любые 5, 13 или 29 ASCII-символов или 10, 26 или 58 шестнадцатеричных символов (“0-9”, “A-F”), соответственно, для 64-, 128- или 256-разрядного ключа WEP.
Back	Чтобы перейти на предыдущий экран, выберите **Back**.
Next	Чтобы перейти на следующий экран, выберите **Next**.
Exit	Чтобы закрыть экран мастера, не сохраняя изменений, выберите **Exit**.

5 Чтобы сохранить настройки беспроводной сети, выберите **Apply**.

Рис. 28 Настройка беспроводной сети, экран 3



6 Проверьте правильность ваших настроек по сводной таблице (таблица доступна только для чтения). Нажмите кнопку **Finish**, чтобы завершить работу мастера и сохранить настройки.

Примечание: Если вы отказались от настройки беспроводной сети, экраны параметров беспроводной сети появляться не будут.

Рис. 29 Мастер настройки доступа в Интернет и беспроводной сети – завершение

7 Запустите браузер и перейдите на сайт www.zyxel.com. Доступ в Интернет – это только начало. Ознакомьтесь с остальными главами этого руководства, чтобы подробнее узнать о всех возможностях P-2602. Если вы не можете получить доступ к Интернету, снова откройте веб-конфигуратор и проверьте правильность настроек, указанных вами в мастерах.

Глава 4
Мастер VoIP и пример настройки

В этой главе описана настройка учетных записей SIP и выполнение телефонного вызова VoIP.

4.1 Введение

Устройство P-2602 снабжено средствами голосовой связи по IP-сетям (VoIP), позволяя использовать обычный аналоговый телефон для телефонной связи через Интернет. В P-2602 можно настроить до двух учетных записей SIP для VoIP.

В этом разделе описывается настройка P-2602 для вызова абонента, который также использует VoIP-устройство. Перед выполнением изложенных указаний, убедитесь, что ваш телефон подключен к порту **Phone 1**.

На следующем рисунке ваш телефон обозначен буквой **A**, а телефон вызываемого абонента – буквой **B** .

Рис. 30 Телефонные вызовы VoIP

Для осуществления телефонных вызовов VoIP необходимо настроить на P-2602 как минимум одну учетную запись SIP. Учетную запись SIP можно зарегистрировать в мастере **VOICE OVER INTERNET SETUP**.

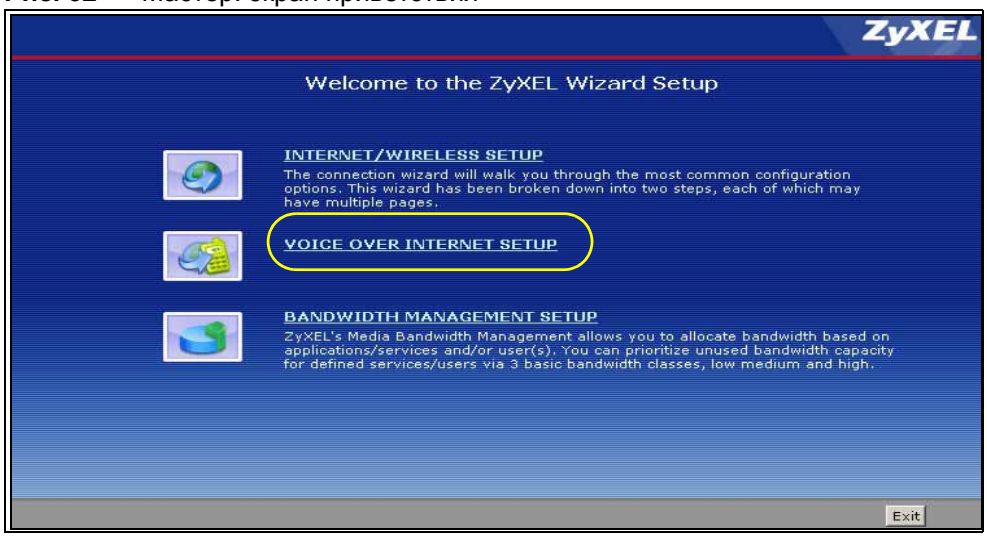
4.2 Настройка в мастере VoIP

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

Рис. 31 Выбор режима

2 Для настройки параметров SIP выберите **VOICE OVER INTERNET SETUP**.

Рис. 32 Мастер: экран приветствия

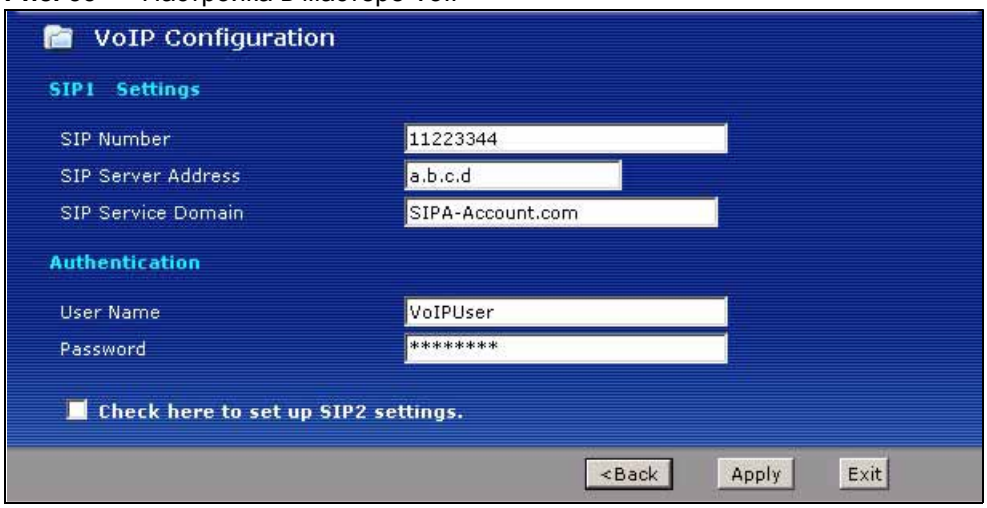


3 На экране **VOICE OVER INTERNET SETUP** введите сведения, предоставленные поставщиком услуг VoIP. Ваш поставщик услуг VoIP должен предоставить вам указанные ниже сведения. По завершении настройки нажмите кнопку **Apply**.

Таб. 16 Пример ввода информации для учетной записи SIP

СВЕДЕНИЯ ОТ ПОСТАВЩИКА УСЛУГ VOIP	ПРИМЕРЫ ЗНАЧЕНИЙ	ОПИСАНИЕ
SIP account address	11223344@SIPA-Account.com	**11223344** – это ваш номер SIP. В учетной записи SIP номер указывается перед символом “@”. **SIPA-Account.com** – это домен сервера SIP.
SIP server address	a.b.c.d	**a.b.c.d** – IP-адрес или доменное имя сервера SIP.
Username	VoIPUser	Это имя пользователя, с которым осуществляется регистрация учетной записи SIP.
Password	Password	Это пароль, с которым осуществляется регистрация учетной записи SIP.

Рис. 33 Настройка в мастере VoIP



Поля изображённого выше экрана описаны в следующей таблице..

Таб. 17 Настройка в мастере VoIP

ПОЛЕ	ОПИСАНИЕ
SIP Number	Введите в этом поле ваш номер SIP. Используйте номер или текст, указанный перед символом “@” в учетной записи SIP. Если ваша учетная запись SIP имеет вид 11223344@SIPA-Account.com, то номером SIP будет “11223344”. Допустимая длина – до 127 знаков ASCII.
SIP Server Address	Введите в этом поле IP-адрес или доменное имя сервера исходящего сервера SIP. Не имеет значения, является ли указанный сервер прокси-сервером, сервером переадресации или сервером регистрации. Допустимая длина – до 95 знаков ASCII.
Домен службы SIP	Введите в этом поле имя домена службы SIP (имя домена в учетной записи SIP следует после символа “@”, например, 11223344@SIPA-Account.com). Допустимая длина – до 127 печатных знаков расширенного набора ASCII.
User Name	В этом поле указывается имя пользователя, используемое для регистрации данной учетной записи SIP на сервере регистрации SIP. Введите имя пользователя в том виде, в котором оно было вам сообщено. Допустимая длина – до 95 знаков ASCII.
Password	Введите пароль, связанный с введенным выше именем пользователя. Допустимая длина – до 95 печатных знаков расширенного набора ASCII.
Check here to set up SIP2 settings.	Этот экран служит для настройки учетной записи SIP 1. Выберите флажок, если вы имеете вторую учетную запись SIP, которую вы хотите использовать. Для второй учетной записи SIP потребуется настроить те же поля. **Примечание:** Если вы настраиваете более одной учетной записи SIP, то необходимо настроить параметры в разделе **Analog Phone** (см. разд. 11.13 на стр. 179), чтобы различать две учетные записи SIP при входящих и исходящих вызовах.
Back	Для возврата к предыдущему экрану нажмите кнопку **Back**.

Таб. 17 Настройка в мастере VoIP

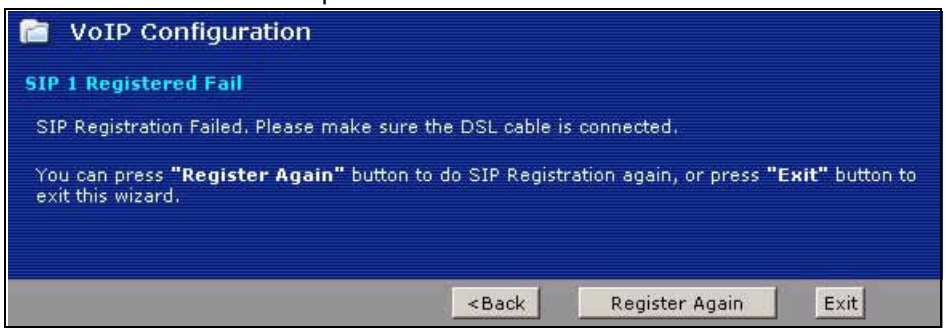
ПОЛЕ	ОПИСАНИЕ
Apply	Нажмите кнопку **Apply**, чтобы завершить работу мастера и сохранить настройки.
Exit	Чтобы закрыть экран мастера, не сохраняя изменений, выберите **Exit**.

4 P-2602 попытается зарегистрировать учетную запись SIP у поставщика услуг VoIP. После регистрации учетной записи загорится светодиод **PHONE 1** и можно будет осуществлять и принимать телефонные вызовы VoIP.

Рис. 34 Проверка регистрации SIP

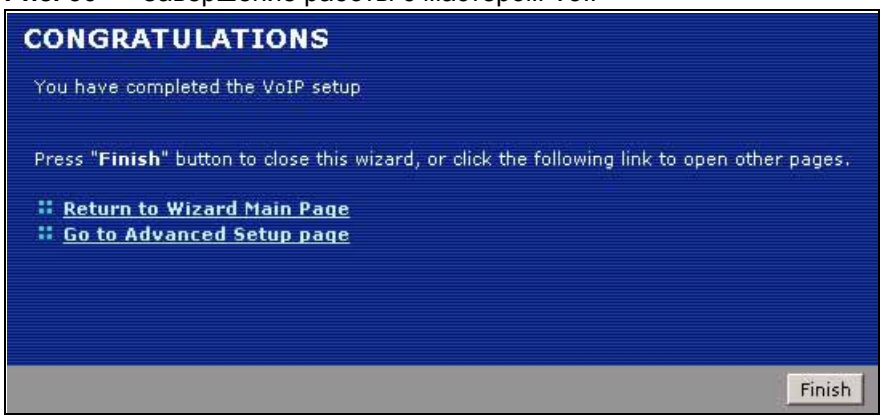
5 Этот экран появляется, если регистрация учетной записи SIP завершается с ошибкой. Если DSL-кабель был отсоединен, подключите его снова. Затем выждите несколько секунд и нажмите **Register Again**. Если ваше интернет-подключение уже работает, нажмите **Back** и попробуйте повторно ввести параметры вашей учетной записи SIP.

Рис. 35 Ошибка мастера VoIP



6 Этот экран появляется, если регистрация учетной записи SIP завершена успешно. Если вы хотите воспользоваться другим мастером настройки, выберите **Return to Wizard Main Page**. Чтобы закрыть мастера и перейти к основным экранам веб-конфигуратора, выберите **Go to Advanced Setup page** или **Finish**.

Рис. 36 Завершение работы с мастером VoIP



7 Другим пользователям VoIP, с которыми вы собираетесь соединяться, также необходимо выполнить подобную последовательность действий, чтобы убедиться, что их учетные записи SIP зарегистрированы и активны. После регистрации они должны предоставить вам свои номера SIP. Для телефонных номеров SIP используйте схему, предлагаемую поставщиком услуг VoIP.

Эту же схему можно использовать и для вызова обычных телефонных номеров. Сначала наберите префикс, указанный поставщиком услуг VoIP, затем – обычный телефонный номер.

Примечание: Подробнее о настройке VoIP и осуществлении вызовов без VoIP см. гл. 11 на стр. 163.

Глава 5
Мастер управления полосой пропускания

В этой главе иллюстрируется настройка управления полосой пропускания с помощью мастеров.

5.1 Введение

Управление полосой пропускания позволяет контролировать суммарную полосу пропускания порта WAN P-2602 и упорядочивать распределение полосы пропускания в соответствии с потребностями сетевых служб. Это помогает исключить ситуации, когда одна служба забирает всю полосу пропускания, блокируя доступ другим пользователям.

5.2 Предопределенные службы для управления полосой пропускания

Ниже описаны службы, которые можно выбрать и к которым можно применять управление полосой пропускания, используя экраны мастера.

Таб. 18 Настройка управления полосой пропускания: службы

СЛУЖБА	ОПИСАНИЕ
WWW	WWW (“веб”, “Всемирная паутина”) – это интернет-система для распространения графической информации с гиперссылками по протоколу передачи гипертекста (HTTP) - клиент-серверному протоколу WWW. Название “Всемирная паутина” не является синонимом Интернета и обозначает только одну из сетевых служб в Интернете. Среди других служб Интернета – чат в реальном времени (IRC) и группы новостей (NNTP). Обращение к WWW осуществляется посредством веб-браузера.
FTP	Протокол передачи файлов используется для пересылки файлов, в особенности – больших объемов данных, которые невозможно передать по электронной почте. Для FTP используется TCP-порт 21.
E-Mail	Электронная почта состоит из сообщений, рассылаемых по компьютерной сети определенным группам или людям. По умолчанию для электронной почты часто используются следующие порты: POP3 - порт 110 IMAP - порт 143 SMTP – порт 25 HTTP - порт 80

Таб. 18 Настройка управления полосой пропускания: службы (продолжение)

СЛУЖБА	ОПИСАНИЕ
Telnet	Telnet – протокол регистрации в системе и эмуляции терминала, распространенный в Интернете и в среде UNIX. Он предназначен для работы по сетям TCP/IP. Его основное назначение – обеспечить дистанционный доступ пользователей к хостам. Для Telnet используется TCP-порт 23.
NetMeeting (H.323)	Продукт мультимедиа-коммуникаций, разработанный Microsoft и обеспечивающий групповой доступ к конференц-связи и видеоконференциям в Интернете. NetMeeting поддерживает VoIP, сеансы текстового чата, виртуальную доску (whiteboard), передачу файлов и совместный доступ к приложениям. NetMeeting основан на протоколе H.323. H.323 - стандартный набор протоколов конференц-связи для передачи аудиовидеопотоков и данных. Он реализует двухточечную и многоточечную связь в реальном времени между клиентскими компьютерами по сети с коммутацией пакетов, не обеспечивающей гарантированного качества обслуживания. Основным транспортом для H.323 является TCP, стандартный номер порта – 1720.
VoIP (SIP)	Передача сигналов речевого диапазона по Интернету называется IP-телефонией (VoIP). Протокол инициирования сеанса (SIP) – международный стандарт реализации VoIP. SIP представляет собой протокол прикладного (сигнального) уровня, отвечающий за подготовку, перенастройку и завершение сеансов голосовой связи и мультимедиа-конференций через Интернет. Основным транспортом для SIP является UDP (также поддерживается TCP), стандартный номер порта – 5060.
VoIP (H.323)	Передача сигналов речевого диапазона по Интернету называется IP-телефонией (VoIP). H.323 - стандартный набор протоколов конференц-связи для передачи аудиовидеопотоков и данных. Он реализует двухточечную и многоточечную связь в реальном времени между клиентскими компьютерами по сети с коммутацией пакетов, не обеспечивающей гарантированного качества обслуживания. Основным транспортом для H.323 является TCP, стандартный номер порта – 1720.
TFTP	TFTP (упрощенный протокол пересылки файлов) – протокол передачи файлов в Интернете, подобный FTP, но использующий UDP (протокол пользовательских датаграмм) вместо TCP (протокол управления передачей).

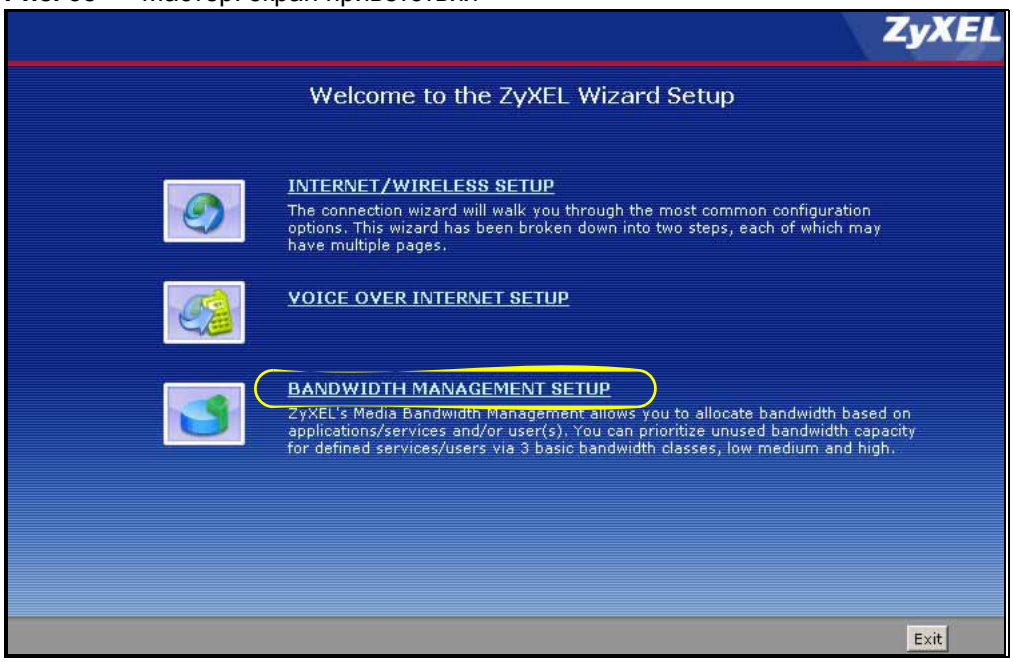
5.3 Настройка в мастере управления полосой пропускания

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

Рис. 37 Выбор режима

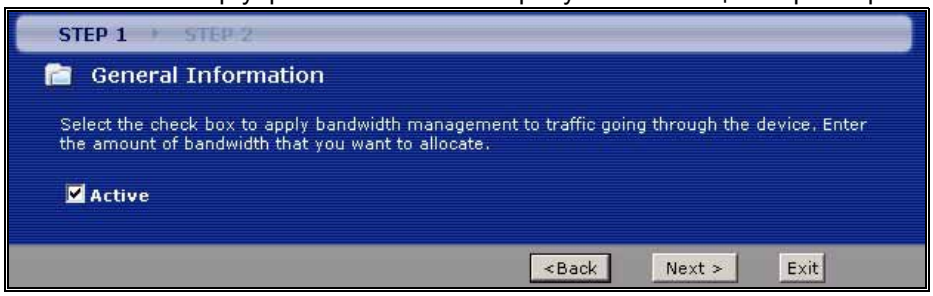
2 Выберите **BANDWIDTH MANAGEMENT SETUP**.

Рис. 38 Мастер: экран приветствия



3 Активируйте управление полосой пропускания и выберите способ выделения полосы пропускания пакетам: по размеру пакета или по типу сетевой службы.

Рис. 39 Мастер управления полосой пропускания: общие параметры



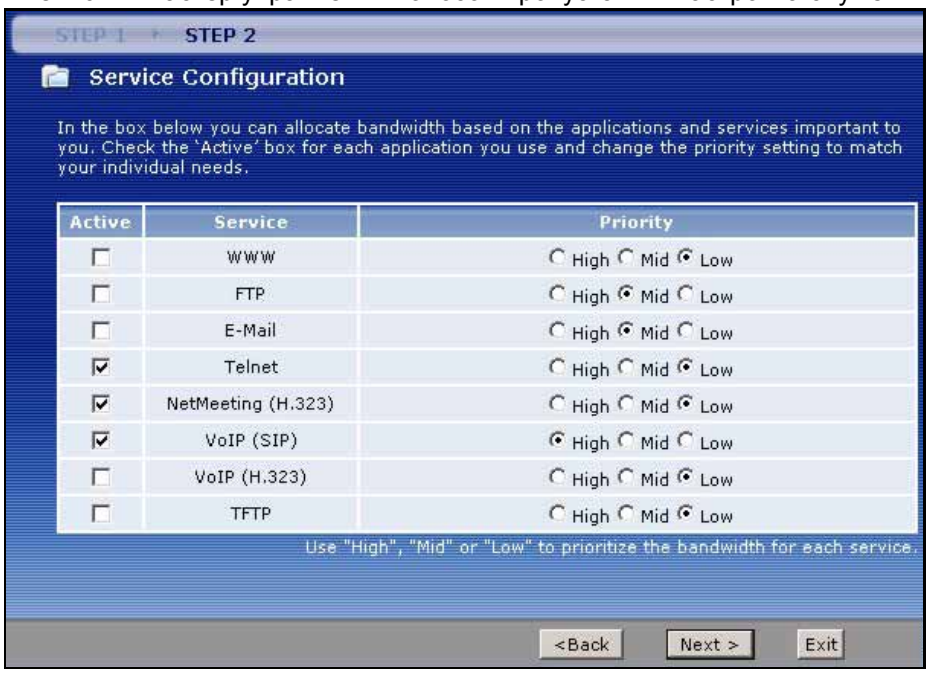
Поля изображённого выше экрана описаны в следующей таблице.

Таб. 19 Мастер управления полосой пропускания: общие параметры

ПОЛЕ	ОПИСАНИЕ
Active	Выберите флажок **Active**, чтобы включить на P-2602 управление полосой пропускания для исходящего трафика на порту WAN, LAN или WLAN. Чтобы автоматически выделять полосу пропускания с учетом размера пакетов, выберите **Auto Classifier**; чтобы распределить полосу пропускания соразмерно потребностям сетевых служб, выберите **Services Setup**.
Back	Для возврата к предыдущему экрану нажмите кнопку **Back**.
Next	Чтобы перейти на следующий экран, выберите **Next**.
Exit	Чтобы закрыть экран мастера, не сохраняя изменений, выберите **Exit**.

4 Если вы выбрали **Service Setup**, на втором экране мастера выберите сетевые службы, к которым следует применять управление полосой пропускания, и отметьте приоритеты, назначаемые перечисленным службам.

Рис. 40 Мастер управления полосой пропускания: настройка служб



Поля соответствующего экрана описаны в следующей таблице.

Таб. 20 Мастер управления полосой пропускания: настройка служб

ПОЛЕ	ОПИСАНИЕ
Active	Выберите **Active**, чтобы включить управление полосой пропускания для трафика, связанного с выбранной службой. Чтобы включить управление полосой пропускания для конкретной службы/ приложения, отметьте флажок **Active**.
Service	В этих полях перечислены названия служб.
Priority	Выберите приоритет, с которым P-2602 будет обрабатывать трафик для каждой из служб (**High** - высокий, **Mid** - средний, **Low** - низкий). Службы с высоким приоритетом (**High**) получают всю необходимую им полосу пропускания. Если нескольким службам назначен одинаковый приоритет, полоса пропускания будет делиться между этими службами поровну. Для служб, не указанных в настройках управления полосой пропускания, полоса выделяется только после того, как она будет выделена всем настроенным службам. Если правила, настроенные в этом мастере, будут изменены на экране **Advanced**, **Bandwidth MGMT**, **Rule Setup**, то переключатель приоритета службы изменит положение на **User Configured** (Настраивается пользователем). Экран **Advanced, Bandwidth MGMT**, **Rule Setup** позволяет отредактировать настройки правил.
Back	Для возврата к предыдущему экрану нажмите кнопку **Back**.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-2602.
Exit	Чтобы закрыть экран мастера, не внося изменений, выберите **Exit**.

5 Следуйте инструкциям на экране, затем нажмите кнопку **Finish** для завершения работы мастера установки и сохранения конфигурации.

Рис. 41 Мастер управления полосой пропускания: завершение работы

Глава 6
Экраны состояния

Экраны состояния (**Status**) позволяют наблюдать за текущим состоянием устройства, системных ресурсов, интерфейсов (LAN и WAN) и учетных записей SIP. Он также позволяет регистрировать и дерегистрировать учетные записи SIP. На экранах **Status** также содержатся подробные сведения о функциях “Any IP” и DHCP, а также статистика по использованию VoIP, управлению полосой пропускания и трафику.

6.1 Экран состояния

Чтобы перейти на этот экран, выберите **Status**.

Рис. 42 Экран состояния

Каждое поле описано в следующей таблице.

Таб. 21 Экран Status

ПОЛЕ	ОПИСАНИЕ
Refresh Interval	Укажите интервал, с которым P-2602 будет обновлять содержимое этого экрана.
Apply	Чтобы немедленно обновить содержимое экрана, нажмите эту кнопку.
Device Information	
Host Name	В этом поле отображается имя системы, используемое для идентификации. Его можно изменить в поле **System Name** на экране **Maintenance > System > General**.
Model Number	В этом поле отображается наименование модели вашего устройства.
MAC Address	В этом поле отображается уникальный MAC или Ethernet-адрес P-2602.
ZyNOS Firmware Version	В этом поле отображается текущая версия микропрограммы в устройстве. Также указывается дата создания этой версии микропрограммы. Щелкните на этом поле, чтобы перейти на экран для смены микропрограммы.
DSL Firmware Version	В этом поле отображается текущая версия микропрограммы DSL-модема в устройстве.
WAN Information	
DSL Mode	В этом поле отображается стандарт DSL, используемый P-2602.
IP Address	В этом поле отображается текущий IP-адрес P-2602 со стороны WAN. Щелкните на этом поле, чтобы перейти на экран для смены IP-адреса.
IP Subnet Mask	В этом поле отображается текущая маска подсети в WAN.
Default Gateway	В этом поле отображается IP-адрес шлюза по умолчанию, если он применим
VPI/VCI	В этом поле отображаются идентификаторы виртуального пути и виртуального канала, введенные на экране **WAN**.
LAN Information	
IP Address	В этом поле отображается текущий IP-адрес P-2602 со стороны LAN. Щелкните на этом поле, чтобы перейти на экран для смены IP-адреса.
IP Subnet Mask	В этом поле отображается текущая маска подсети в LAN.
DHCP	В этом поле отбражаются DHCP-службы, которые P-2602 предоставляет в локальной сети. Возможны следующие варианты: **Server** – P-2602 выступает в локальной сети в качестве DHCP-сервера, присваивая IP-адреса другим компьютерам в локальной сети. **Relay** – устройство действует как заменитель DHCP-сервера и выполняет обмен запросами и откликами между удаленным сервером и клиентами. **None** – P-2602 не предоставляет службу DHCP в локальной сети. Щелкните на этом поле, чтобы перейти на экран для смены микропрограммы.
WLAN Information	(только в моделях с индексом “W”)
SSID	Это описательное название, идентифицирующее P-2602 в беспроводной сети. Щелкните на этом поле, чтобы перейти на экран для смены идентификатора.
Channel	Это номер канала, который P-2602 использует в данный момент.
Security	В этом поле отображается тип режима безопасности, используемого P-2602 в беспроводной сети.

Таб. 21 Экран Status

ПОЛЕ	ОПИСАНИЕ
Security	
Firewall	В этом поле сообщается, активирован ли межсетевой экран P-2602. Щелкните на этом поле, чтобы перейти на экран для смены правил межсетевого экрана.
Content Filter	В этом поле сообщается, активирована ли фильтрация содержания. Щелкните на этом поле, чтобы перейти на экран для смены микропрограммы.
System Status	
System Uptime	В этом поле отображается продолжительность непрерывной работы P-2602 с момента последнего запуска. Запуск P-2602 происходит при включении питания, при перезагрузке (**Maintenance > Tools > Restart**) и при сбросе (см. разд. 2.1.2 на стр. 55).
Current Date/ Time	В этом поле отображается текущая дата и время по часам P-2602. Дату и время можно изменить на экране **Maintenance > System > Time Setting**.
System Mode	В этом поле отображается режим работы P-2602: маршрутизатор (router) или мост (bridge).
CPU Usage	В этом поле отображается текущая загрузка вычислительных мощностей P-2602 в процентах. Когда загрузка приближается к 100%, P-2602 работает при полной нагрузке и пропускная способность используется по максимуму. Чтобы увеличить пропускную способность для одних приложений, необходимо отключить другие (например, с помощью управления полосой пропускания; см. гл. 19 на стр. 277).
Memory Usage	В этом поле отображается текущий объем используемой оперативной памяти P-2602 в процентах. Обычно эта величина не должна достигать больших значений. Если объем используемой памяти приближается к 100%, работа P-2602 может стать нестабильной, и устройство необходимо перезагрузить. См. разд. 25.6 на стр. 335, либо выключите устройство (отключите источник питания) на несколько секунд.
Interface Status	
Interface	В этом столбце перечислены все интерфейсы, имеющиеся в P-2602.
Status	Для DSL-интерфейса в этом поле может отображаться **Down** (канал разъединен), **Up** (канал соединен), если используется инкапсуляция Ethernet, и **Down** (канал разъединен), **Up** (канал соединен), **Idle** (соединение (ppp-сеанс) неактивно), **Dial** (начало вызова) и **Drop** (прерывание вызова), если используется инкапсуляция PPPoE. В этом поле указывается, используется ли сетевой интерфейс устройством P-2602. Для интерфейса LAN в этом поле отображается **Up**, когда P-2602 использует интерфейс, и **Down**, когда P-2602 не использует интерфейс. Для интерфейса WLAN в этом поле отображается **Active**, когда беспроводная сеть включена, и **Inactive**, когда беспроводная сеть отключена.
Rate	Для интерфейса LAN в этом поле отображается скорость порта и используемый режим дуплекса. Для интерфейса DSL отображается скорость передачи по нисходящему и восходящему каналу. Для интерфейса WLAN отображается скорость передачи, когда беспроводная сеть включена, и **N/A**, когда беспроводная сеть отключена.
Summary	
Client List	По этой ссылке можно просмотреть сведения о DHCP-клиенте. См. разд. 8.5 на стр. 125.

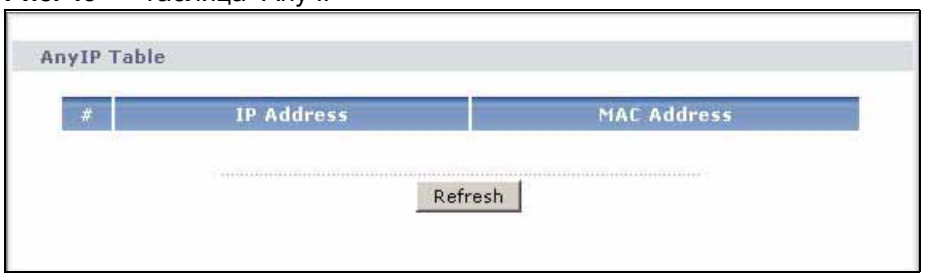
Таб. 21 Экран Status

ПОЛЕ	ОПИСАНИЕ
AnyIP Table	По этой ссылке можно просмотреть список IP-адресов и MAC-адресов компьютеров, находящихся в одной подсети с P-2602. См. разд. 6.2 на стр. 92.
WLAN Status	По этой ссылке можно просмотреть MAC-адреса беспроводных станций, которые в данный момент связаны с P-2602. См. разд. 6.3 на стр. 93.
Bandwidth Status	По этой ссылке можно просмотреть полосу пропускания, используемую P-2602, и объемы выделения полосы пропускания. См. разд. 19.9 на стр. 288.
VPN Status	По этой ссылке можно просмотреть текущие VPN-соединения P-2602. См. разд. 17.16 на стр. 266.
Packet Statistics	По этой ссылке можно просмотреть состояние портов и статистику по пакетам. См. разд. 6.4 на стр. 94.
VoIP Statistics	По этой ссылке можно просмотреть статистику использования VoIP. См. разд. 6.5 на стр. 95.
VoIP Status	
Account	В этом столбце перечислены все учетные записи SIP, настроенные в P-2602.
Registration	В этом поле отображается текущее состояние регистрации учетной записи SIP. Для пользования VoIP необходимо зарегистрировать учетную запись SIP на сервере SIP. Если учетная запись SIP уже зарегистрирована на сервере SIP, • нажмите **Unregister**, чтобы удалить регистрацию учетной записи с сервера SIP. При этом ваша учетная запись не аннулируется, но удаляется привязка идентификатора SIP к вашему IP-адресу или имени домена. • Во втором поле отображается **Registered**. Если учетная запись не зарегистрирована на сервере SIP, • нажмите **Register**, чтобы устройство P-2602 попыталось зарегистрировать учетную запись SIP на сервере SIP. • Во втором поле отображается причина, по которой учетная запись не зарегистрирована. **Inactive** - учетная запись SIP не активна. Ее можно активировать на экране **VoIP > SIP > SIP Settings**. **Register Fail** - последняя попытка регистрации учетной записи SIP на сервере SIP посредством P-2602 завершилась с ошибкой. P-2602 автоматически пытается зарегистрировать учетную запись SIP при включении питания P-2602 или при активации учетной записи.
URI	В этом поле отображается номер счета и домен службы учетной записи SIP. Эти параметры можно изменить на экране **VoIP > SIP > SIP Settings**.

6.2 Таблица адресов для функции “Any IP”

Чтобы перейти на этот экран, выберите **Status > AnyIP Table**. На этом экране можно просмотреть IP-адреса и MAC-адреса всех компьютеров, использующих P-2602, но находящихся в разных подсетях с P-2602.

Рис. 43 Таблица “Any IP”



Каждое поле описано в следующей таблице.

Таб. 22 Таблица адресов для функции “Any IP”

ПОЛЕ	ОПИСАНИЕ
#	В этом поле отображается порядковый номер, не связанный с параметрами какой-либо записи.
IP Address	В этом поле выводятся IP-адреса компьютеров, использующих P-2602, но находящихся в разных подсетях с P-2602.
MAC Address	В этом поле выводятся MAC-адреса компьютеров, использующих P-2602, но находящихся в разных подсетях с P-2602.
Refresh	Нажмите эту кнопку, чтобы обновить содержимое экрана.

6.3 Экран состояния WLAN (только в моделях с индексом “W”)

Чтобы перейти на этот экран, выберите **Status > WLAN Status**. Этот экран позволяет просмотреть состояние беспроводных станций, которые в данный момент соединены с P-2602.

Рис. 44 WLAN Status

Поля соответствующего экрана описаны в следующей таблице.

Таб. 23 Экран состояния WLAN

ПОЛЕ	ОПИСАНИЕ
#	Это порядковый номер подсоединенной беспроводной станции.
MAC Address	В этом поле отображается MAC-адрес подсоединенной беспроводной станции.

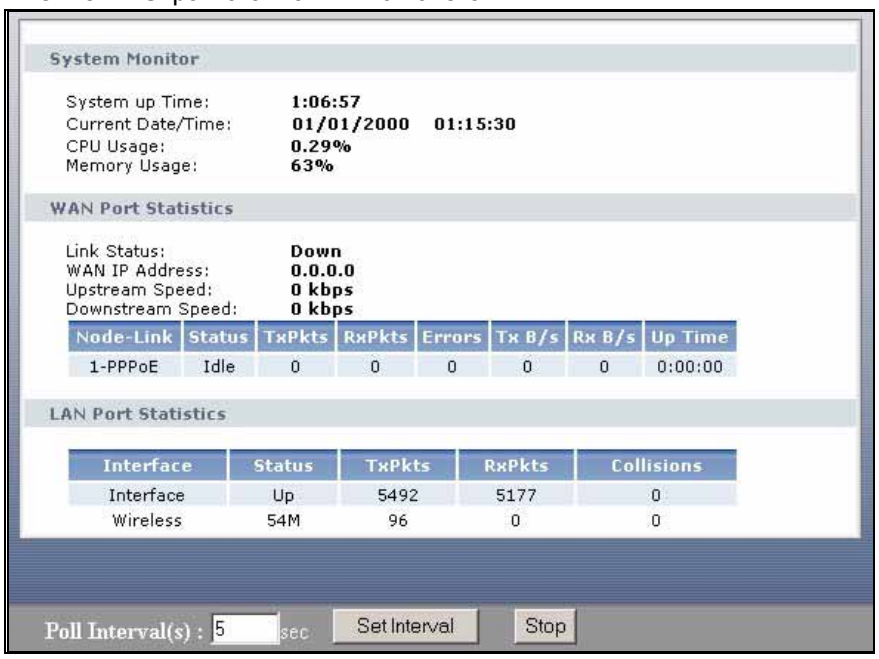
Таб. 23 Экран состояния WLAN (продолжение)

ПОЛЕ	ОПИСАНИЕ
Association Time	В этом поле отображается время, когда беспроводная станция впервые соединилась с P-2602.
Refresh	Нажмите кнопку **Refresh**, чтобы обновить содержимое экрана.

6.4 Статистика по пакетам

Чтобы перейти на этот экран, выберите **Status > Packet Statistics**. Информация, предназначенная только для чтения, касается состояния порта и пакетов. На экране также содержатся поля “system up time” (“время непрерывной работы системы”) и “poll interval(s)” (“интервалы опроса”). Поле **Poll Interval(s)** можно настраивать.

Рис. 45 Экран статистики по пакетам



Поля изображённого выше экрана описаны в следующей таблице.

Таб. 24 Статистика по пакетам

ПОЛЕ	ОПИСАНИЕ
System Monitor	
System up Time	В этом поле отображается суммарная продолжительность работы системы.
Current Date/Time	В этом поле отображается текущая дата и время по часам P-2602.
CPU Usage	В этом поле отображается загрузка ЦП (в процентах).
Memory Usage	В этом поле отображается объем используемой оперативной памяти (в процентах).
WAN Port Statistics	

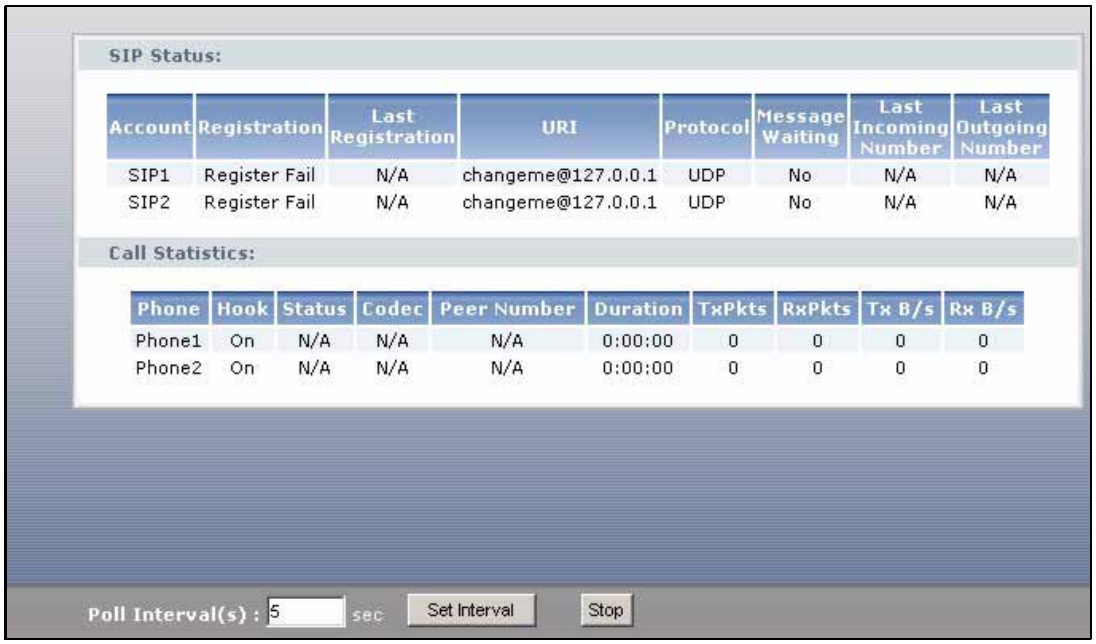
Таб. 24 Статистика по пакетам (продолжение)

ПОЛЕ	ОПИСАНИЕ
Link Status	В этом поле отображается состояние соединения с WAN.
WAN IP Address	В этом поле отображается IP-адрес, соответствующий WAN-порту P-2602.
Upstream Speed	В этом поле отображается скорость восходящего канала P-2602.
Downstream Speed	В этом поле отображается скорость нисходящего канала P-2602.
Node-Link	В этом поле отображается порядковый номер и тип соединения с удаленным узлом. Возможны следующие типы соединений: PPPoA, ENET, RFC 1483 и PPPoE.
Status	В этом поле отображается состояние: **Down** (канал разъединен), **Up** (канал соединен), если используется инкапсуляция Ethernet, и **Down** (канал разъединен), **Up** (канал соединен), **Idle** (соединение (ppp-сеанс) неактивно), **Dial** (начало вызова) и **Drop** (прерывание вызова), если используется инкапсуляция PPPoE.
TxPkts	В этом поле отображается количество пакетов, отправленных через данный порт.
RxPkts	В этом поле отображается количество пакетов, принятых через данный порт.
Errors	В этом поле отображается количество пакетов с ошибками на данном порту.
Tx B/s	В этом поле отображается число байт, отправленных за последнюю секунду.
Rx B/s	В этом поле отображается число байт, принятых за последнюю секунду.
Up Time	В этом поле отображается суммарная продолжительность пребывания данного порта в активном состоянии.
LAN Port Statistics	
Ethernet	В этом поле отображается **Ethernet** (порты LAN) или **Wireless** (порт WLAN).
Status	Для портов LAN в этом поле отображается **Down** (порт разъединен) или **Up** (порт соединен). Для интерфейса WLAN отображается скорость передачи, когда беспроводная сеть включена, и **N/A**, когда беспроводная сеть отключена.
TxPkts	В этом поле отображается количество пакетов, отправленных через данный интерфейс.
RxPkts	В этом поле отображается количество пакетов, полученных через данный интерфейс.
Collisions	В этом поле отображается число коллизий на данном интерфейсе.
Poll Interval(s)	Введите интервал времени для обновления системной статистики в браузере.
Set Interval	Нажмите эту кнопку, чтобы применить новый интервал опроса, введённый выше в поле **Poll Interval**.
Stop	Нажмите эту кнопку, чтобы приостановить обновление системной статистики.

6.5 Статистика VoIP

Чтобы перейти на этот экран, выберите **Status > VoIP Statistics**.

Рис. 46 Статистика VoIP



Каждое поле описано в следующей таблице.

Таб. 25 Статистика VoIP

ПОЛЕ	ОПИСАНИЕ
SIP Status	
Account	В этом столбце перечислены все учетные записи SIP, настроенные в P-2602.
Registration	В этом поле отображается текущее состояние регистрации учетной записи SIP. Его можно изменить на экране **Status**. **Registered** - учетная запись зарегистрирована на сервере SIP. **Register Fail** - последняя попытка регистрации учетной записи SIP на сервере SIP посредством P-2602 завершилась с ошибкой. P-2602 автоматически пытается зарегистрировать учетную запись SIP при включении питания P-2602 или при активации учетной записи. **Inactive** - учетная запись SIP не активна. Ее можно активировать на экране **VoIP > SIP > SIP Settings**.
Last Registration	В этом поле отображается время последней успешной регистрации учетной записи SIP. Если эта запись никогда ранее не была успешно зарегистрироана, поле будет содержать **N/A**.
URI	В этом поле отображается номер счета и домен службы учетной записи SIP. Эти параметры можно изменить на экране **VoIP > SIP > SIP Settings**.
Protocol	В этом поле отображается тип транспортного протокола, применяемого для данной учетной записи SIP. Для учетных записей SIP всегда применяется протокол UDP.
Message Waiting	В этом поле сообщается о наличии сообщений, поступивших (находящихся в состоянии ожидания) для данной учетной записи SIP.
Last Incoming Number	В этом поле отображается последний номер, с которого осуществлялся вызов учетной записи SIP. Если на учетную запись не поступали никакие вызовы, поле будет содержать **N/A**.

Таб. 25 Статистика VoIP

ПОЛЕ	ОПИСАНИЕ
Last Outgoing Number	В этом поле отображается последний номер, на который осуществлялся вызов с данной учетной записи SIP. Если с этой учетной записи не осуществлялось никаких исходящих вызовов, поле будет содержать **N/A**.
Call Statistics	
Phone	В этом поле отображается состояние всех телефонных портов P-2602.
Hook	В этом поле указывается, поднята ли трубка на телефонном аппарате. **On** - Линия разъединяется или уже разъединена. **Off** - На телефоне набирается номер, принимается вызов, или имеется установленное соединение.
Status	В этом поле отображается текущее состояние телефонного вызова. **N/A** - В данный момент вызовы VoIP, входящие или исходящие вызовы отсутствуют. **DIAL** - Звонит телефон на вызываемой стороне. **RING** - Звонит телефон с входящим вызовом VoIP. **Process** - Выполняется вызов VoIP. **DISC** - Вызываемая сторона занята, вызываемый абонент повесил трубку или на вашем телефоне не была повешена трубка.
Codec	В этом поле отображается тип речевого кодека, используемого для вызовов VoIP через данный телефонный порт.
Peer Number	В этом поле отображается номер SIP удаленной стороны, с которой в данный момент установлено VoIP-соединение через телефонный порт.
Duration	В этом поле отображается продолжительность текущего вызова.
Tx Pkts	В этом поле отображается число пакетов, отправленных P-2602 в течение текущего вызова.
Rx Pkts	В этом поле отображается число пакетов, принятых P-2602 в течение текущего вызова.
Tx B/s	В этом поле отображается скорость передачи пакетов P-2602 в течение текущего вызова. Эта величина представляет собой усредненную скорость, выраженную в байтах в секунду.
Rx B/s	В этом поле отображается скорость приема пакетов P-2602 в течение текущего вызова. Эта величина представляет собой усредненную скорость, выраженную в байтах в секунду.
Poll Interval(s)	Укажите интервал, с которым P-2602 будет обновлять содержимое этого экрана, и нажмите кнопку **Set Interval**.
Set Interval	Нажмите эту кнопку, чтобы задать интервал, указанный в поле **Poll Interval**. P-2602 будет обновлять экран с заданным интервалом.
Stop	Нажмите эту кнопку, чтобы устройство P-2602 прекратило обновлять экран.

Глава 7
Настройка WAN

В этой главе описывается настройка параметров глобальной сети.

7.1 Обзор параметров WAN

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

7.1.1 Encapsulation

Необходимо использовать тот метод инкапсуляции, которого требует поставщик услуг Интернета. P-2602 поддерживает следующие методы.

7.1.1.1 ENET ENCAP

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

7.1.1.2 PPP по Ethernet (PPPoE)

P-2602 поддерживает PPPoE (протокол передачи от точки к точке через Ethernet). PPPoE – это проект стандарта IETF (RFC 2516), определяющий способ взаимодействия персонального компьютера (ПК) с модемом (DSL, кабельным, беспроводным и т.д.), обеспечивающим широкополосное соединение. Параметр **PPPoE** служит для настройки коммутируемых соединений с использованием PPPoE.

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

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

Протокол PPPoE позволяет снизить затраты труда как абонента, так и оператора, поскольку для него не требуется производить специальное конфигурирование широкополосного модема на стороне клиента.

Реализация PPPoE непосредственно в P-2602 (а не на отдельных компьютерах) снимает необходимость в установке ПО для PPPoE на компьютерах локальной сети, поскольку эту часть задачи выполняет P-2602. Кроме того, благодаря NAT доступ будут иметь все компьютеры в LAN.

7.1.1.3 PPPoA

PPPoA означает протокол “точка-точка” поверх 5-го уровня адаптации ATM (AAL5). PPPoA функционирует так же, как модемное коммутируемое соединение с Интернетом. P-2602 инкапсулирует PPP-сеанс по стандарту RFC1483 и передает его через постоянный виртуальный канал (ATM PVC) на оборудование DSLAM (мультиплексор цифрового абонентского канала) у поставщика услуг. Подробное описание PPPoA см. в RFC 2364. Подробное описание PPP см. в RFC 1661.

7.1.1.4 RFC 1483

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

7.1.2 Мультиплексирование

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

7.1.2.1 Мультиплексирование VC

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

7.1.2.2 Мультиплексирование LLC

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

7.1.3 VPI и VCI

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

7.1.4 IP Address Assignment (Назначение IP-адреса)

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

7.1.4.1 Назначение IP-адресов при использовании инкапсуляции PPPoA или PPPoE

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

7.1.4.2 Назначение IP-адресов при использовании инкапсуляции RFC 1483

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

7.1.4.3 Назначение IP-адресов при использовании инкапсуляции ENET ENCAP

В этом случае вы можете иметь или статический или динамический IP-адрес. Для статического IP-адреса необходимо заполнить поля **IP Address** и **ENET ENCAP Gateway** сведениями, полученными от поставщика услуг Интернета. Однако в случае динамического IP-адреса устройство P-2602 будет выступать DHCP-клиентом в сети WAN, и поля **IP Address** и **ENET ENCAP Gateway** будут неприменимы, поскольку P-2602 получает соответствующие значения от DHCP-сервера.

7.1.5 Закрепленное соединение (PPP)

Закрепленное соединение (nailed-up connection) – это соединение по коммутируемой линии, которое всегда активно независимо от потребности в передаче трафика. Реализация закрепленного соединения в P-2602 сводится к тому, что отключается время ожидания, а кроме того, при каждом разрыве сеанса P-2602 будет пытаться автоматически восстановить соединение. Закрепленное соединение может оказаться чрезвычайно дорогостоящим по очевидным причинам.

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

7.1.6 NAT

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

7.2 Метрика

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

Метрика устанавливает приоритеты маршрутов, используемых P-2602 для связи с Интернетом. Если два маршрута по умолчанию имеют одно и то же значение метрики, P-2602 использует следующие предопределенные приоритеты:

- обычный маршрут: определяется поставщиком услуг Интернета (см. разд. 7.5 на стр. 105)
- маршрут для переадресации трафика (см. разд. 7.7 на стр. 111)
- резервный маршрут WAN, также называемый маршрутом резервирования через коммутируемый доступ (см. разд. 7.8 на стр. 112)

Например, если обычный маршрут имеет метрику 1, маршрут переадресации трафика – метрику 2, а маршрут резервирования через коммутируемый доступ – метрику 3, то в качестве основного маршрута по умолчанию действует обычный маршрут. Если через обычный маршрут соединение с Интернетом отсутствует, то затем P-2602 пробует маршрут переадресации трафика. Если маршрут переадресации также оказывается неработоспособен, P-2602 использует маршрут резервирования через коммутируемый доступ.

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

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

7.3 Ограничение трафика

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

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

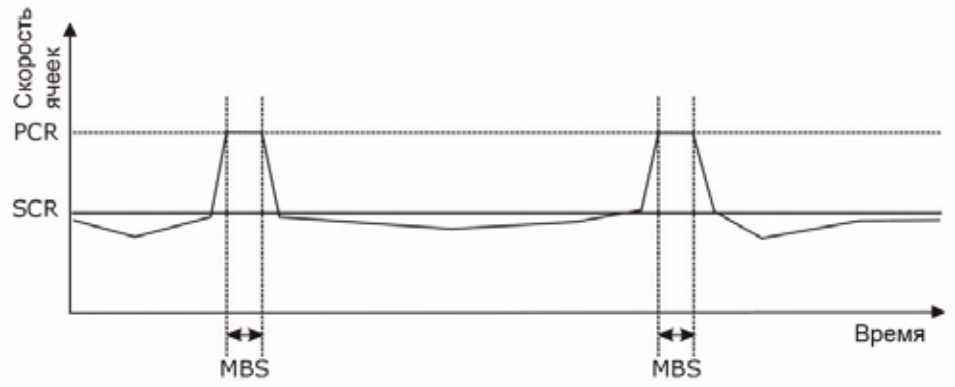
Выдерживаемая скорость ячеек (Sustained Cell Rate, SCR) средняя скорость ячеек для каждого источника пульсирующего трафика. Она задаёт максимальную среднюю скорость, с которой ячейки могут пересылаться по виртуальному соединению. SCR не должна превышать PCR.

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

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

Взаимосвязь PCR, SCR and MBS продемонстрирована на следующем рисунке.

Рис. 47 Пример ограничения трафика



7.3.1 Классы трафика в ATM

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

7.3.1.1 Постоянная скорость (CBR)

Постоянная битовая скорость (CBR) обеспечивает фиксированную полосу пропускания, которая доступна всегда, даже в отсутствие передаваемых данных.
CBR-трафик обычно чувствителен к временным параметрам (не допускает задержек). CBR применяется для соединений, непрерывно требующих определённой полосы пропускания. Устанавливается пиковая скорость передачи ячеек (PCR), при превышении которой ячейки могут отбрасываться. Примерами соединений, требующих CBR, являются видео высокой чёткости и голосовая связь.

7.3.1.2 Переменная скорость (VBR)

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

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

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

7.3.1.3 Неуказанная битовая скорость (UBR)

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

7.4 Доступ в Интернет без настройки

После соединения с телефонной розеткой и включения питания P-2602 автоматически обнаруживает параметры подключения к Интернету (например, номера VCI/VPI и метод инкапсуляции), используемые поставщиком услуг Интернета, и выполняет необходимую настройку. В тех случаях, когда для подключения требуются дополнительные параметры учетной записи (например, имя пользователя и пароль) или когда P-2602 не может соединиться с поставщиком услуг, устройство направит вас на соответствующие экраны веб-конфигуратора для ввода параметров или диагностики ошибок.

В следующих случаях доступ в Интернет без настройки будет отключен:

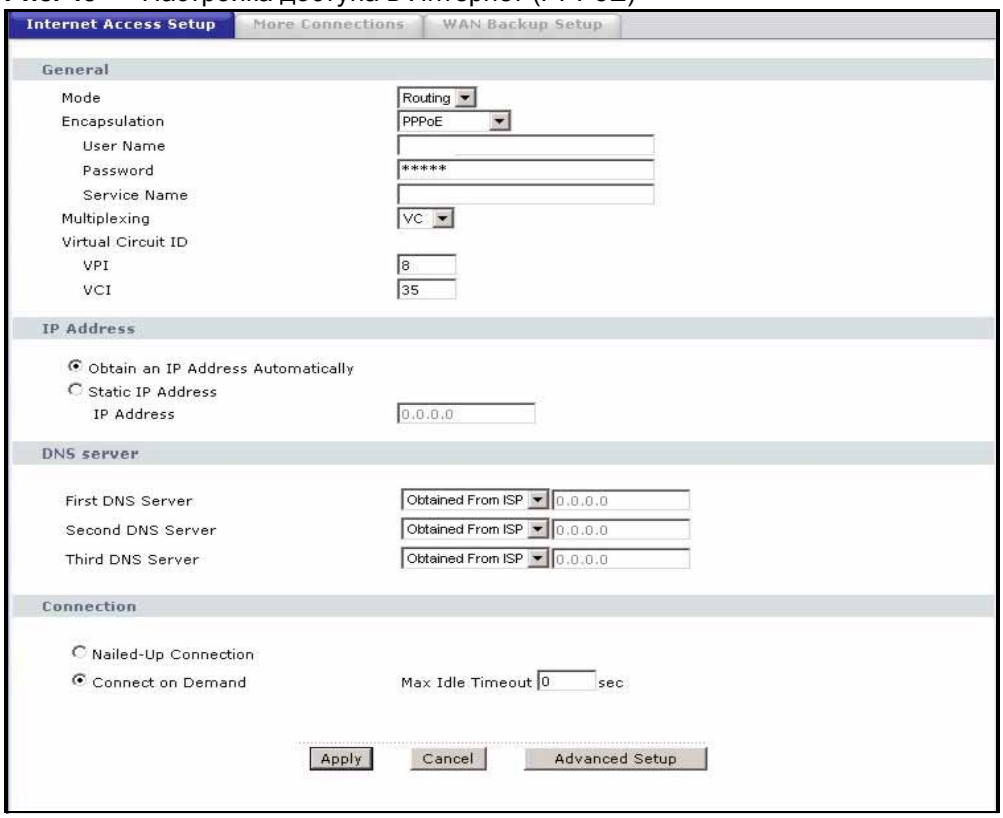
- P-2602 находится в режиме моста
- устройство P-2602 настроено на использование статического (неизменяемого) IP-адреса в сети WAN.

7.5 Настройка доступа к Интернету

Чтобы изменить настройки удаленного узла WAN для P-2602, выберите **Network > WAN > Internet Access Setup**. Данное окно содержит различия в зависимости от инкапсуляции.

Дополнительные сведения см. в разд. 7.1 на стр. 99.

Рис. 48 Настройка доступа в Интернет (PPPoE)



Поля соответствующего экрана описаны в следующей таблице.

Таб. 26 Настройка доступа к Интернету

ПОЛЕ	ОПИСАНИЕ
General	
Mode	Если ваш поставщик услуг Интернета позволяет использовать одну учетную запись с нескольких компьютеров, выберите режим маршрутизации – **Routing** (этот режим действует по умолчанию). В противном случае выберите режим моста – **Bridge**.
Encapsulation	Выберите тип инкапсуляции, используемый поставщиком услуг Интернета, из раскрывающегося списка. Доступные для выбора варианты зависят от режима, выбранного в поле **Mode**. Если в поле **Mode** выбран режим **Bridge**, выберите **PPPoA** или **RFC 1483**. Если в поле **Mode** выбран режим **Routing**, выберите **PPPoA**, **RFC 1483**, **ENET ENCAP** или **PPPoE**.
User Name	(Только для инкапсуляции PPPoA и PPPoE) Введите имя пользователя в точности так, как оно указано поставщиком услуг. Если поставщик присвоил имя пользователя в формате пользователь@домен, где доменом является название службы, следует ввести оба компонента в точном соответствии с указаниями.
Password	(Только для инкапсуляции PPPoA и PPPoE)) Введите пароль, связанный с указанным выше именем пользователя.
Service Name	(Только для инкапсуляции PPPoE) Введите название службы PPPoE.
Мультиплексирование	Выберите тип мультиплексирования, используемый поставщиком услуг Интернета, из раскрывающегося списка. Варианты выбора: **VC** или **LLC**.

Таб. 26 Настройка доступа к Интернету (продолжение)

ПОЛЕ	ОПИСАНИЕ
Virtual Circuit ID	Совокупность VPI (идентификатора виртуального пути) и VCI (идентификатора виртуального канала) определяет виртуальную цепь. Подробное описание см. в приложении.
VPI	Допустимый диапазон значений VPI – от 0 до 255. Введите присвоенный вам VPI.
VCI	Допустимый диапазон значений VCI – от 32 до 65535 (диапазон от 0 до 31 зарезервирован для локального управления трафиком ATM). Введите присвоенный вам VCI.
IP Address	
IP Address	Это поле доступно в том случае, если в поле **Mode** выбран режим **Routing**. Статический IP-адрес – это фиксированный адрес, выдаваемый поставщиком услуг Интернета. Динамический IP-адрес не имеет постоянного значения; поставщик услуг Интернета для каждого сеанса работы с Интернетом назначает новый адрес. Если вам выдается динамический IP-адрес, выберите **Obtain an IP Address Automatically**, в противном случае выберите **Static IP Address** и введите IP-адрес, присвоенный поставщиком услуг Интернета, ниже в поле **IP Address**.
Subnet Mask (Только для инкапсуляции ENET ENCAP)	Введите маску подсети в десятичном виде через точку. Способ расчета маски подсети при делении на подсети описан в приложении.
Gateway IP address (Только для инкапсуляции ENET ENCAP)	Если в поле **Encapsulation** выбран режим **ENET ENCAP**, то необходимо определить IP-адрес шлюза (сообщаемый поставщиком услуг Интернета).
DNS Server	
First DNS Server Second DNS Server Third DNS Server	Если поставщик услуг Интернета автоматически присваивает параметры DNS-сервера (а также адрес P-2602 в сети WAN), выберите **Obtained From ISP**. Выберите **User-Defined**, если вам известен IP-адрес DNS-сервера. Введите IP-адрес DNS-сервера в расположенном справа поле. Если вы выбрали **User-Defined**, но оставили 0.0.0.0 в качестве IP-адреса, то после нажатия **Apply** поле **User-Defined** сменится на **None**. Если во втором поле вы выбрали **User-Defined** и ввели одинаковый IP address, то второе поле **User-Defined** после нажатия кнопки **Apply** сменится **None**. Чтобы использовать P-2602 в качестве прокси-сервера для DNS для тех случаев, когда поставщик услуг Интернета предоставляет информацию о DNS только через расширения IPCP, выберите **DNS Relay**. IP-адрес P-2602 в сети LAN отображается в поле справа (это поле доступно только для чтения). P-2602 сообщает DHCP-клиентам в локальной сети, что само устройство P-2602 является DNS-сервером. Когда компьютер в локальной сети отправляет запрос DNS в P-2602, P-2602 переадресует запрос на DNS-сервер, адрес которого получен в IPCP, и передает отклик обратно компьютеру. Режим ретрансляции (**DNS Relay**) можно выбрать только для одного из трех серверов; если вы выберите **DNS Relay** для второго или третьего DNS-сервера, это значение изменится на **None** после нажатия кнопки **Apply**. Выберите **None**, если DNS-серверы настраивать не требуется. Для этого в локальной сети должен иметься другой DNS-сервер, либо на всех компьютерах адреса DNS-серверов должны быть настроены вручную. Если DNS-сервер не настроен, для получения доступа к машине необходимо знать ее IP-адрес.

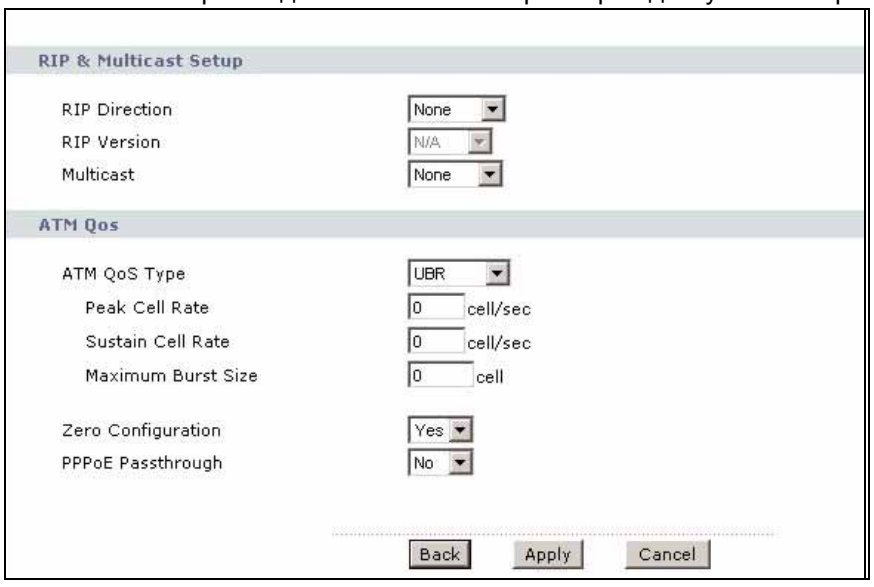
Таб. 26 Настройка доступа к Интернету (продолжение)

ПОЛЕ	ОПИСАНИЕ
Connection (Только для инкапсуляции PPPoA и PPPoE).	
Nailed-Up Connection	Выберите **Nailed-Up Connection**, чтобы использовать закрепленное соединение, которое активно все время. P-2602 будет пытаться автоматически восстановить соединение при разрыве сеанса.
Connect on Demand	Если соединение не требуется поддерживать постоянно, выберите **Connect on Demand** и укажите интервал неактивности в поле **Max Idle Timeout**.
Max Idle Timeout	Если вы выбрали режим **Connect on Demand**, в поле **Max Idle Timeout** укажите интервал неактивности. Значение по умолчанию – 0, при котором сеанс соединения с Интернетом не завершается никогда.
Apply	Чтобы сохранить изменения, выберите **Apply**.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.
Advanced Setup	Нажмите эту кнопку, чтобы перейти на экран **Advanced WAN Setup** для настройки дополнительных параметров глобальной сети.

7.5.1 Настройка дополнительных параметров доступа к Интернету

Для настройки дополнительных параметров глабальной сети в P-2602 нажмите кнопку **Advanced Setup** на экране **Internet Access Setup**. Появится изображенный ниже экран.

Рис. 49 Настройка дополнительных параметров доступа к Интернету



Поля изображённого выше экрана описаны в следующей таблице.

Таб. 27 Настройка дополнительных параметров доступа к Интернету

ПОЛЕ	ОПИСАНИЕ
RIP & Multicast Setup	
RIP Direction	Выберите направление RIP: **None** (нет), **Both** (вход-выход), **In Only** (только вход) или **Out Only** (только выход).
RIP Version	Выберите версию протокола RIP: **RIP-1**, **RIP-2B** или **RIP-2M**.
Multicast	IGMP (широковещательный протокол взаимодействия групп в Интернете) – это протокол сетевого уровня, используемый для установления членства в группе многоадресной рассылки. P-2602 поддерживает IGMP версии 1 (**IGMP-v1**) и **IGMP-v2**. Чтобы отключить этот протокол, выберите **None**.
QoS для ATM	
ATM QoS Type	Выберите **CBR** (постоянная скорость передачи), если нужно задать фиксированную полосу пропускания для передачи голоса или данных. Выберите **UBR** (не заданная скорость передачи), если изменение скорости передачи со временем не имеет большого значения, например, в случае электронной почты. Выберите **VBR-RT** (переменная битовая скорость, работа в режиме реального времени), если соединение характеризуется пульсирующим трафиком с жёсткими ограничениями на задержки и допустимые колебания задержек. Выберите **VBR-nRT** (переменная битовая скорость без требований реального времени), если соединение не требует жесткого контроля задержек и их колебаний.
Peak Cell Rate	Разделите скорость DSL-линии (бит/с) на 424 (размер ATM-ячейки). Получится пиковая скорость передачи ячеек (PCR). Полученное значение будет соответствовать максимальной скорости посылки ячеек отправителем. Введите значение PCR в этом поле.
Sustain Cell Rate	Выдерживаемая скорость ячеек (SCR) задаёт среднюю (долговременную) скорость передачи ячеек. Введите SCR (значение SCR должно быть меньше PCR). Необходимо помнить, что по умолчанию система использует значение 0 ячеек в секунду.
Maximum Burst Size	Максимальный размер пульсации (Maximum Burst Size, MBS) – это максимальное число ячеек, при посылке которого будет соблюдаться PCR. Введите MBS (меньше 65535).
Zero Configuration	Эта функция не применяется, если для P-2602 указывается использовать статический IP-адреса в сети WAN, либо если выбран режим моста. Выберите **Yes**, чтобы устройство P-2602 автоматически обнаружило параметры подключения к Интернету (например, номера VCI/VPI и метод инкапсуляции), используемые поставщиком услуг Интернета, и выполнило необходимую настройку. Выберите **No**, чтобы отключить эту функцию. В этом случае потребуется вручную настроить P-2602 на доступ к Интернету.
PPPoE Passthrough (только для инкапсуляции PPPoE)	Это поле доступно в том случае, если выбран режим инкапсуляции **PPPoE**. В дополнение к встроенному в P-2602 PPPoE-клиенту можно включить режим сквозного прохождения PPPoE, чтобы разрешить использование PPPoE-клиентов на хостах в локальной сети для соединения с поставщиком услуг Интернета через P-2602. Каждый хост может иметь отдельную учетную запись и глобальный IP-адрес на стороне WAN. Сквозной режим PPPoE – альтернатива NAT для тех применений, где использование NAT невозможно. Отключите сквозной режим PPPoE, чтобы запретить хостам в локальной сети с помощью программных клиентов PPPoE соединяться с поставщиком услуг Интернета.

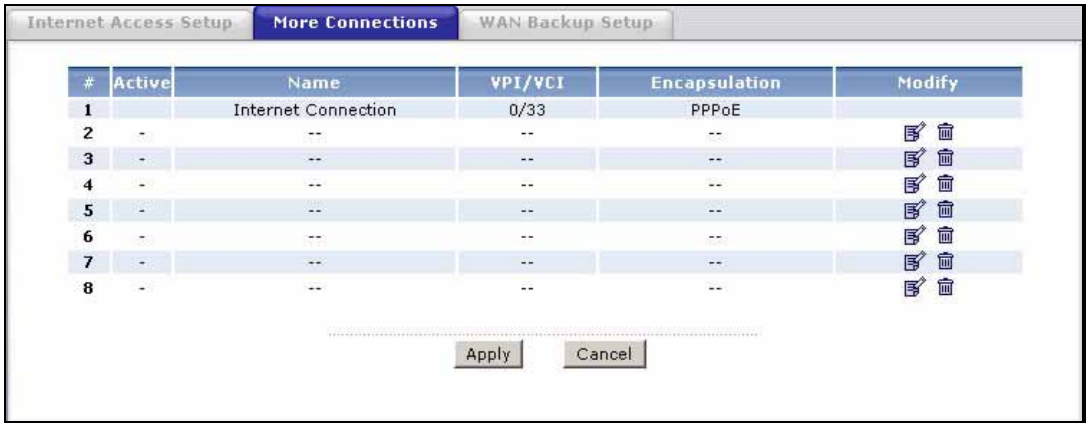
Таб. 27 Настройка дополнительных параметров доступа к Интернету (продолжение)

ПОЛЕ	ОПИСАНИЕ
Back	Для возврата к предыдущему экрану нажмите кнопку **Back**.
Apply	Чтобы сохранить изменения, выберите **Apply**.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

7.6 Несколько соединений с WAN

P-2602 позволяет настроить одновременно несколько соединений для доступа в Интернет. Чтобы настроить дополнительные соединения для доступа в Интернет, выберите **Network > WAN > More Connections**. Данное окно содержит различия в зависимости от инкапсуляции.

Рис. 50 Несколько соединений с WAN



Поля изображённого выше экрана описаны в следующей таблице.

Таб. 28 Настройка дополнительных параметров доступа к Интернету

ПОЛЕ	ОПИСАНИЕ
#	В этом поле отображается порядковый номер соответствующего подключения.
Active	В этом поле отображается, активно ли данное подключение.
Name	В этом поле отображается название, присвоенное подключению.
VPI/VCI	В этом поле отображаются идентификаторы VPI (идентификатор виртуального пути) и VCI (идентификатор виртуальной цепи) для данного WAN-соединения.
Encapsulation	В этом поле отображается метод инкапсуляции, используемый для подключения к Интернету.
Modify	Щелкните на значке редактирования, чтобы отредактировать параметры настройки подключения к Интернету. Щелкните на этом значке, находясь в пустом поле настроек, чтобы добавить новую настройку доступа в Интернет. Щелкните на значке удаления, чтобы удалить настройку доступа в Интернет из списка подключений.

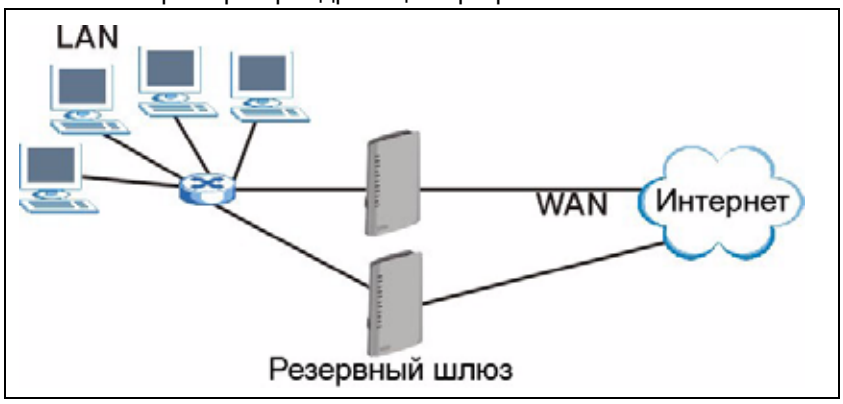
Таб. 28 Настройка дополнительных параметров доступа к Интернету (продолжение)

ПОЛЕ	ОПИСАНИЕ
Apply	Чтобы сохранить изменения, выберите **Apply**.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

7.7 Переадресация трафика

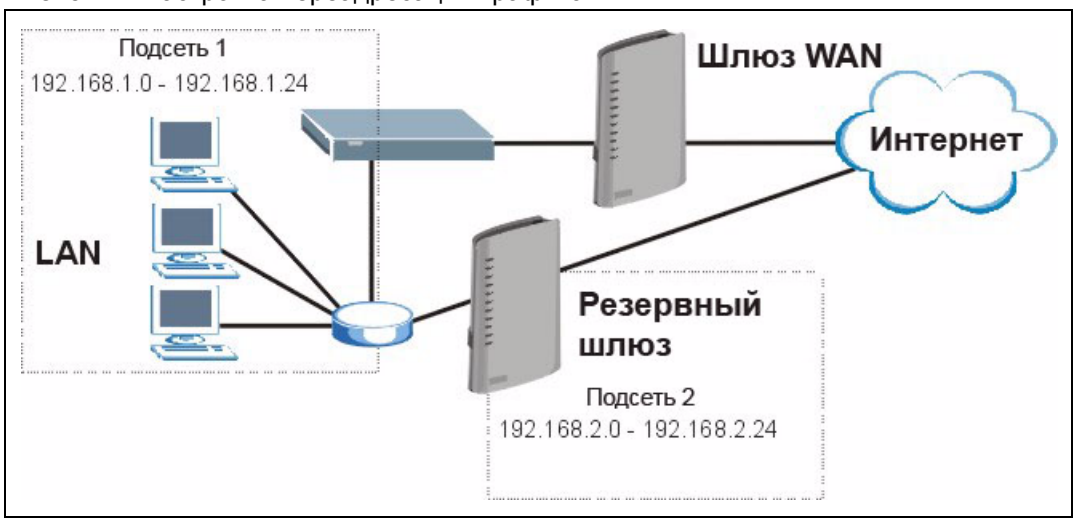
Переадресация трафика направляет трафик к резервному шлюзу, когда P-2602 не может подключиться к Интернету. Пример приведён на следующем рисунке.

Рис. 51 Пример переадресации трафика



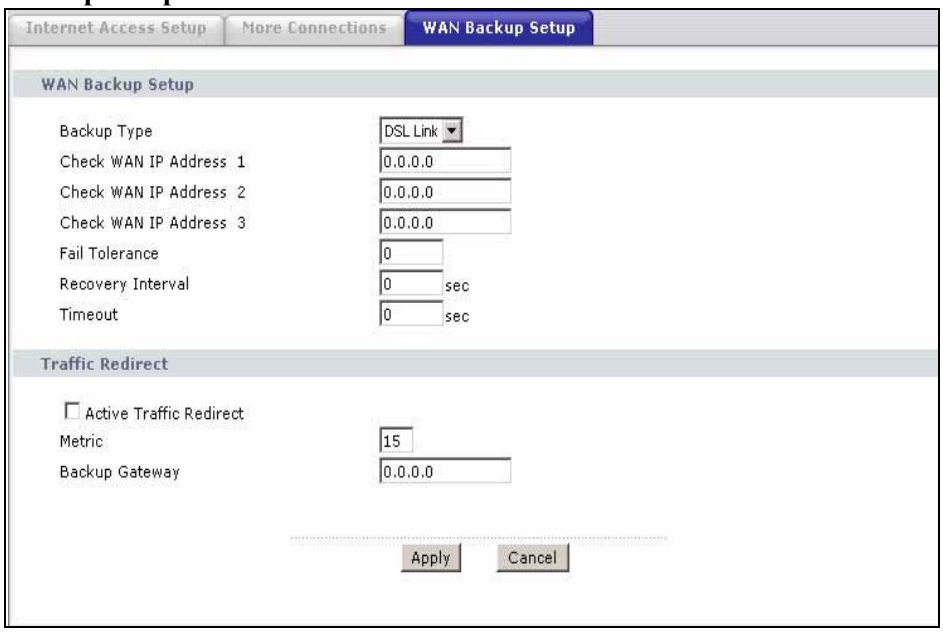
Следующая топология сети позволяет избежать проблем безопасности, свойственных треугольному маршруту, когда резервный шлюз связан с LAN. Используйте совмещение IP-адресов использования, чтобы организовать в составе LAN две или три логических сети, шлюзом между которыми будет являться P-2602. Поместите защищенную LAN в одну подсеть (подсеть 1 на следующем рисунке), а резервный шлюз – в другую подсеть (подсеть 2). Настройте фильтры, разрешающие прохождение пакетов из защищенной LAN (подсеть 1) к резервному шлюзу (подсеть 2).

Рис. 52 Настройка переадресации трафика



7.8 Настройка резервирования WAN

Чтобы настроить резервирование WAN в P-2602, выберите **Network > WAN > WAN Backup Setup**.



Поля соответствующего экрана описаны в следующей таблице.

Таб. 29 Настройка резервирования WAN

ПОЛЕ	ОПИСАНИЕ
Backup Type	Выберите метод, которым P-2602 будет проверять наличие DSL-соединения. Выберите **DSL Link**, чтобы устройство P-2602 проверяло наличие физического соединения с DSLAM. Выберите **ICMP**, чтобы периодически отправлять эхозапросы с P-2602 на IP-адреса, заданные в полях **Check WAN IP Address**.
Check WAN IP Address1-3	Это поле задает адреса, с помощью которых P-2602 будет проверять доступность WAN. Введите IP-адрес ближайшего надежного компьютера (например, адрес DNS-сервера поставщика услуг). **Примечание:** Если вы активируете переадресацию трафика или резервирование через коммутируемый доступ, здесь необходимо указать по крайней мере один IP-адрес. При использовании резервирования WAN P-2602 периодически отправляет эхозапросы на указанные здесь адреса и при неполучении ответа переключается на резервное соединение с WAN (если оно настроено).
Fail Tolerance	Укажите число раз (рекомендуемое значение – 2), которое P-2602 может отправить эхозапросы на указанные в поле **Check WAN IP Address** IP-адреса без получения отклика, прежде чем переключится на резервное соединение с WAN (или на другой вид резервного соединения с WAN).

Таб. 29 Настройка резервирования WAN (продолжение)

ПОЛЕ	ОПИСАНИЕ
Recovery Interval	Когда P-2602 использует соединение с меньшим приоритетом (обычно – резервное соединение с WAN), устройство периодически проверяет возможность перехода на более приоритетное соединение. Введите длительность интервала в секундах (рекомендуется 30), выдерживаемого P-2602 между проверками доступности сети. Увеличьте интервал, если целевой IP-адрес обрабатывает много трафика.
Timeout	Введите число секунд (рекомендуется 3), в течение которого P-2602 будет ожидать отклика на один из эхозапросов, отправленных по указанным в поле **Check WAN IP Address** адресам, прежде чем запрос будет сочтен превысившим время ожидания. Соединение с WAN будет признано недоступным после того, как P-2602 обнаружит истечение времени ожидания указанное в поле **Fail Tolerance** число раз. Если ваша сеть занята или переполнена, введите в этом поле более высокое значение.
Traffic Redirect	Переадресация трафика направляет трафик к резервному шлюзу, когда P-2602 не может подключиться к Интернету.
Active Traffic Redirect	Отметьте этот флажок, чтобы устройство P-2602 использовало переадресацию трафика при недоступности обычного соединения с WAN. **Примечание:** Чтобы активировать переадресацию трафика, необходимо настроить как минимум один проверяемый IP-адрес в разделе “Check WAN IP Address”.
Metric	Это поле задает приоритет маршрута среди других маршрутов, используемых P-2602. Метрика обозначает “стоимость” передачи пакета. Маршрутизатор определяет оптимальный маршрут передачи, выбирая путь с самой низкой “стоимостью”. Для маршрутизации на основе RIP мерой стоимости является число переходов между сетевыми сегментами, минимальное значение – 1 – соответствует напрямую подключённым сетям. Значение метрики должно быть в диапазоне от 1 до 15; значения больше 15 означают, что соединение не функционирует. Чем меньше значение, тем ниже “стоимость”.
Backup Gateway	Введите IP-адрес резервного межсетевого шлюза в десятичном виде через точку. P-2602 автоматически переадресует трафик на этот IP-адрес, если разрывается соединение P-2602 с Интернетом.
Apply	Чтобы сохранить изменения, выберите **Apply**.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

Глава 8
Настройка LAN

В этой главе описывается настройка параметров локальной сети.

8.1 Обзор LAN

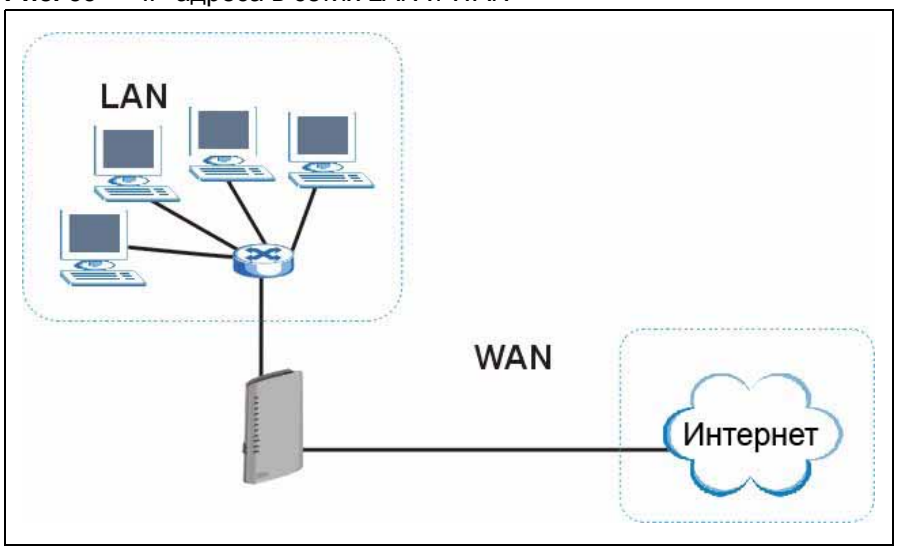
Локальная вычислительная сеть (LAN, ЛВС) - общедоступная система связи, к которой подключено множество компьютеров. Локальная сеть объединяет компьютеры, сосредоточенные на определённой площади, обычно – находящиеся в одном здании или на одном этаже. Экраны LAN помогают настраивать DHCP-сервер для локальной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

Выполнение настроек на экранах **LAN** описано в разд. 8.3 на стр. 121.

8.1.1 Сети LAN, WAN и устройство ZyXEL

Непосредственное физическое подключение определяет, являются ли порты P-2602 портами WAN или LAN. Как показано ниже, существуют две раздельных IP-сети: внутренняя (сеть LAN) и внешняя (сеть WAN).

Рис. 53 IP-адреса в сетях LAN и WAN



8.1.2 Настройка DHCP

DHCP (протокол динамической настройки хоста, RFC 2131 и RFC 2132) позволяет клиентам в момент запуска получать настройки TCP/IP с сервера. P-2602 позволяет включить или отключить встроенный DHCP-сервер. Когда устройство P-2602 настроено в качестве DHCP-сервера, оно сообщает настройки TCP/IP клиентам. Если служба DHCP отключена, необходимо иметь в своей LAN другой DHCP-сервер или настраивать компьютеры вручную.

8.1.2.1 Установка IP-пула

В P-2602 имеется предварительно настроенный диапазон IP-адресов для клиентов DHCP (пул DHCP). См. техническое описание в приложениях. Не назначайте компьютерам в локальной сети статические адреса, принадлежащие пулу DHCP.

8.1.3 Адрес DNS-сервера

DNS (служба доменных имён) обеспечивает преобразование доменных имён в соответствующие им IP-адреса и наоборот. DNS-сервер крайне важен, потому что без него для получения доступа к компьютеру пришлось бы выяснять его IP-адрес. Адреса DNS-серверов, указанные в настройках DHCP, передаются клиентским компьютерам вместе с присвоенными им IP-адресами и маской подсети.

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

Некоторые поставщики услуг Интернета передают информацию о DNS-серверах посредством специальных расширений управляющего протокола IP (IPCP) после установки PPP-соединения. Если ваш поставщик услуг Интернета не сообщил адреса DNS-серверов в явном виде, возможно, что эти адреса будут переданы во время согласования IPCP. P-2602 поддерживает расширения IPCP для передачи информации о DNS-серверах посредством функции прокси-сервера для DNS.

Если маршрутизатор настроен в качестве сервера ретрансляции DNS, он сообщает DHCP-клиентам, что DNS-сервером является он сам. Когда компьютер в сети LAN отправляет запрос DNS в P-2602, P-2602 переадресует запрос на DNS-сервер, адрес которого получен в IPCP, и передает отклик обратно компьютеру.

Необходимо отметить, что функция прокси-сервера для DNS работает только тогда, когда поставщик услуг Интернета использует расширения управляющего протокола IP (IPCP) для передачи информации о DNS-серверах. Это не означает, что во всех случаях можно не указывать DNS-серверы в настройках DHCP. Если ваш поставщик услуг

Интернета сообщил вам IP-адреса DNS-серверов в явном виде, не забудьте ввести эти адреса на экране **DHCP Setup**. Это позволит P-2602 передавать DNS-серверы на компьютеры, которые в свою очередь смогут выполнять запрос DNS-сервера непосредственно без участия P-2602.

8.1.4 Присвоение адресов DNS-серверов

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

Поставщик услуг Интернета может распространять адреса серверов DNS двумя способами.

- Первый способ – адреса DNS-серверов сообщаются абоненту в информационном бюллетене при подключении к услугам. Если ваш поставщик услуг Интернета сообщил вам адреса DNS-серверов, введите их на экране **DHCP Setup**.
- P-2602 выступает в роли прокси-сервера для DNS, когда поле **DNS Server** на экране **DHCP Setup** установлено в значение **DNS Relay**.

8.2 TCP/IP LAN

P-2602 имеет встроенный DHCP-сервер, который назначает IP-адреса и сообщает адреса DNS-серверов системам с функцией DHCP-клиента.

8.2.1 IP-адрес и маска подсети

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

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

Если поставщик услуг Интернета не сообщил вам номер IP-подсети в явном виде, то наиболее вероятно, что вы используете единственную учетную запись пользователя, и поставщик услуг Интернета назначит вам динамический IP-адрес при установлении соединения. В этом случае рекомендуется выбрать номер сети от 192.168.0.0 до 192.168.255.0. Также потребуется разрешить в P-2602 функцию трансляции сетевых адресов (NAT). Комитет по цифровым адресам в Интернете (Internet Assigned Number Authority, IANA) зарезервировал определённые диапазоны адресов специально для частных применений; все адреса, которые не принадлежат этим диапазонам, не должны использоваться без специальных на то указаний. Предположим, что в качестве номера

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

После выбора номера сети выберите для P-2602 легкозапоминающийся IP-адрес, например, 192.168.1.1, но этот адрес не должен использоваться никаким другим устройством в вашей сети.

Маска подсети указывает на долю номеров IP-адресов в сети. P-2602 автоматически вычисляет маску подсети на основе назначаемого пользователем IP-адреса. В отсутствие специальных указаний изменять маску подсети, предлагаемую P-2602, не следует.

8.2.1.1 Частные IP-адреса

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

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

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

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

8.2.2 Настройка RIP

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

- **Both -** P-2602 будет периодически распространять таблицу маршрутизации по широковещательному запросу и объединять принимаемые параметры RIP.

- **In Only -** P-2602 не будет отправлять RIP-пакеты, но будет обрабатывать все принимаемые RIP-пакеты.
- **Out Only -** P-2602 будет отправлять RIP-пакеты, но не будет обрабатывать поступающие RIP-пакеты.
- **None -** P-2602 не будет отправлять RIP-пакеты и будет игнорировать все поступающие RIP-пакеты.

Поле **Version** управляет форматом и способом широковещательной рассылки RIP-пакетов с P-2602 (устройство принимает пакеты обоих форматов). **RIP-1** поддерживается всеми устройствами, а RIP-2 позволяет передавать больше информации. RIP-1 обычно достаточен для большинства сетей, кроме сетей со сложной топологией.

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

8.2.3 Многоадресная рассылка

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

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

P-2602 поддерживает версию 1 IGMP (**IGMP-v1**) и версию 2 (**IGMP-v2**). При запуске P-2602 опрашивает все непосредственно связанные с ним сети, чтобы собрать информацию о принадлежности к группам. Впоследствии P-2602 периодически обновляет эту информацию. Многоадресную рассылку IP на LAN- и/или WAN-интерфейсах P-2602 можно разрешить/запретить с помощью веб-конфигуратора (**LAN**; **WAN**). Чтобы отключить многоадресную рассылку на этих интерфейсах, выберите **None**.

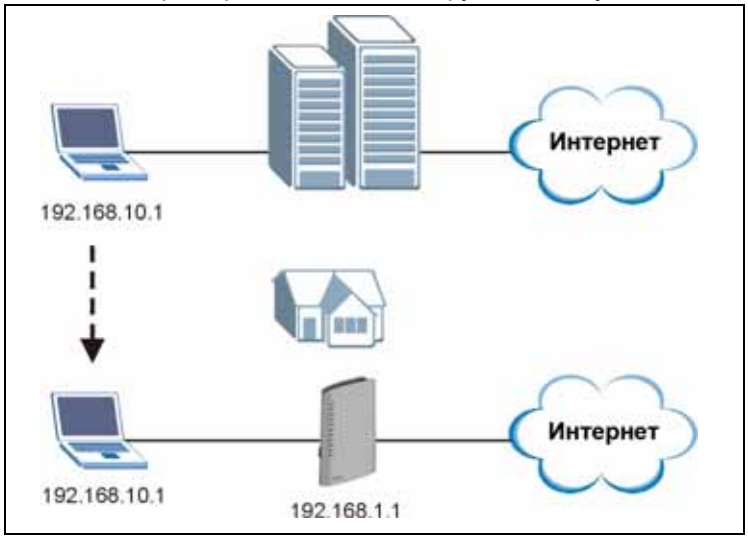
8.2.4 Any IP

Традиционно было необходимо устанавливать IP-адреса и маски подсетей компьютера и P-2602 так, чтобы они находились в той же самой подсети, благодаря чему компьютер мог получать доступ к Интернету через P-2602. В тех случаях, когда компьютеру необходимо иметь статический IP-адрес в другой сети, потребовалось бы вручную настраивать сетевые параметры компьютера каждый раз, когда вам требуется доступ к Интернету через P-2602.

Функция “Any IP” позволяет выходить с компьютеров в Интернет через P-2602 без перенастройки параметров сети (в частности, IP-адреса и маски подсети), когда IP-адреса компьютера и P-2602 находятся в разных подсетях. Собирается ли компьютер использовать динамический или статический (фиксированный) IP-адрес, можно просто подключить компьютер к P-2602 и пользоваться Интернетом.

На следующем рисунке представлен сценарий, в котором компьютер настроен на использование статического частного IP-адреса в корпоративной среде. Дома, где имеется P-2602, компьютер также можно использовать для выхода в Интернет, не изменяя сетевые настройки, даже когда IP-адреса компьютера и P-2602 не находятся в одной и той же подсети.

Рис. 54 Пример использования функции “Any IP”



Функция “Any IP” не распространяется на компьютеры, использующие динамический или статический IP-адрес, который находится в одной подсети с P-2602.

Примечание: Для использования функции “Any IP” в P-2602 *необходимо* разрешить NAT/SUA.

8.2.4.1 Принцип работы функции “Any IP”

ARP (Address Resolution Protocol) – это протокол для установления соответствия между IP-адресом и физическим адресом устройства в локальной сети. Физический адрес устройства называется MAC-адресом. Таблица маршрутизации IP задается на Ethernet-устройствах с поддержкой IP (P-2602) и определяет, через какие сегменты данные пересылаются к указанному адресату.

Ниже перечислены операции, которые происходят, когда компьютер впервые обращается к Интернету через P-2602.

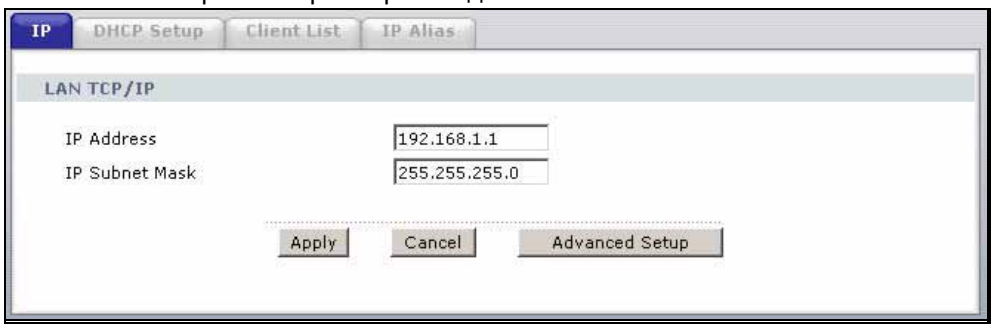
1. Когда компьютер (находящийся в другой подсети) в первый раз обращается к Интернету, он отправляет пакеты на шлюз по умолчанию (которым P-2602 не является), руководствуясь MAC-адресом в своей таблице ARP.
2. Когда компьютер не может найти шлюз по умолчанию, он отправляет широковещательный запрос ARP по локальной сети.
3. P-2602 принимает широковещательный запрос ARP от компьютера и отвечает на него, подставляя свой MAC-адрес.
4. Компьютер обновляет MAC-адрес шлюза по умолчанию в таблице ARP. После обновления таблицы ARP компьютер может обращаться к Интернету через P-2602.
5. Принимая пакеты от компьютера, P-2602 создает запись в таблице маршрутизации IP, что позволяет в дальнейшем правильно пересылать пакеты, предназначенные этому компьютеру.

После обновления всех параметров маршрутизации компьютер может получить доступ к P-2602 и Интернету, как если бы он находился в одной подсети с P-2602.

8.3 Настройка параметров IP для локальной сети

Чтобы перейти на экран **IP,** выберите **Network > LAN**. Дополнительные сведения см. в разд. 8.1 на стр. 115.

Рис. 55 Настройка параметров IP для LAN



Поля изображённого выше экрана описаны в следующей таблице.

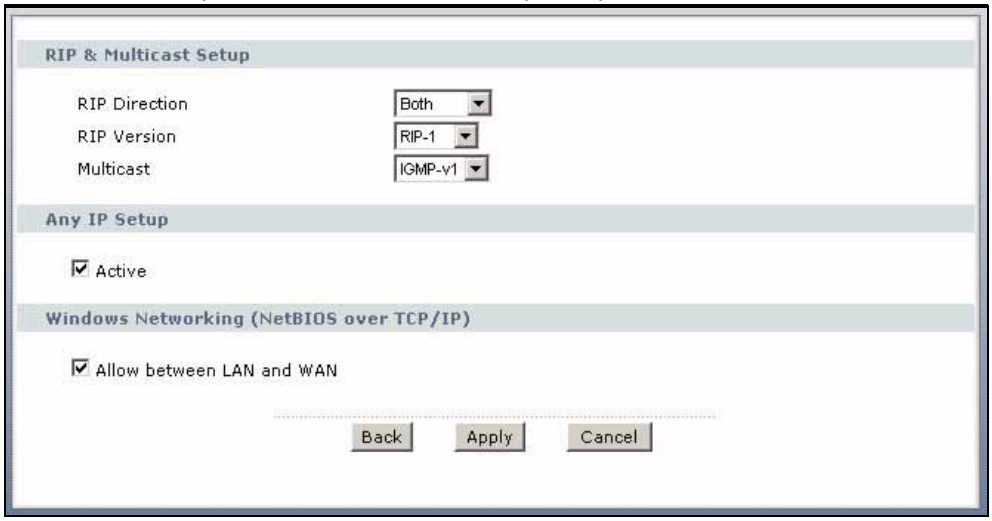
Таб. 30 Настройка параметров IP для LAN

ПОЛЕ	ОПИСАНИЕ
TCP/IP LAN	
IP Address	Введите IP-адрес P-2602 в виде десятичных чисел через точку, например: 192.168.1.1 (заводская настройка по умолчанию).
IP Subnet Mask	Введите маску подсети, назначенную поставщиком услуг Интернета (если она предоставлена).
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-2602.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.
Advanced Setup	Нажмите эту кнопку, чтобы перейти на экран **Advanced LAN Setup** для настройки дополнительных параметров локальной сети.

8.3.1 Настройка дополнительных параметров локальной сети

Для настройки дополнительных параметров локальной сети в P-2602 нажмите кнопку **Advanced Setup** на экране **LAN IP**. Появится изображенный ниже экран.

Рис. 56 Настройка дополнительных параметров локальной сети



Поля изображённого выше экрана описаны в следующей таблице.

Таб. 31 Настройка дополнительных параметров локальной сети

ПОЛЕ	ОПИСАНИЕ
RIP & Multicast Setup	
RIP Direction	Выберите направление RIP: **None** (нет), **Both** (вход-выход), **In Only** (только вход) или **Out Only** (только выход).
RIP Version	Выберите версию протокола RIP: **RIP-1**, **RIP-2B** или **RIP-2M**.

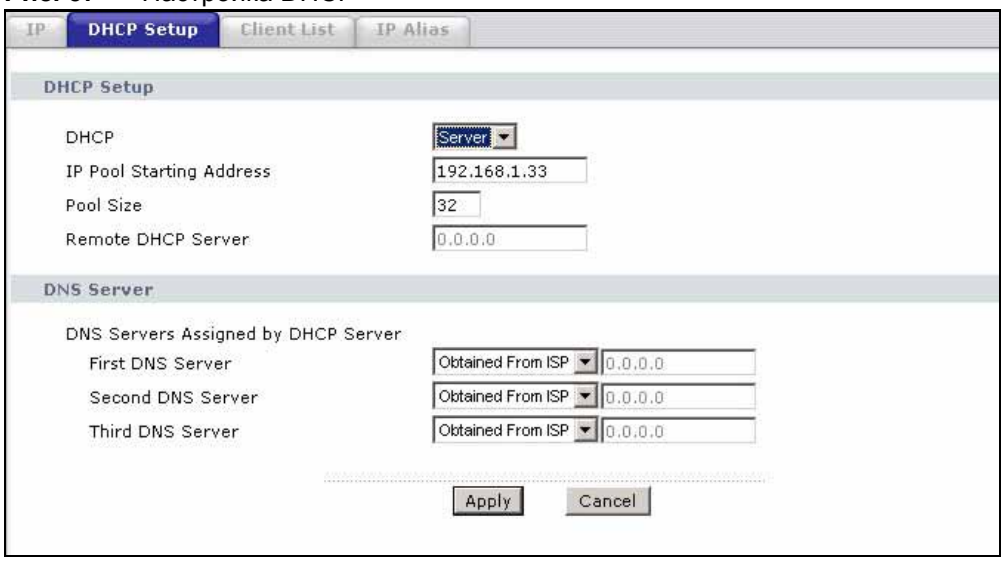
Таб. 31 Настройка дополнительных параметров локальной сети (продолжение)

ПОЛЕ	ОПИСАНИЕ
Multicast	IGMP (широковещательный протокол взаимодействия групп в Интернете) – это протокол сетевого уровня, используемый для установления членства в группе многоадресной рассылки. P-2602 поддерживает IGMP версии 1 (**IGMP-v1**) и **IGMP-v2**. Чтобы отключить этот протокол, выберите **None**.
Any IP Setup	Чтобы включить поддержку “Any IP”, отметьте флажок **Active**. Эта функция позволяет компьютерам получать доступ к Интернету без изменения сетевых настроек (IP-адреса и маски подсети), даже когда IP-адреса компьютера и P-2602 находятся в разных подсетях. Если функция “Any IP” отключена, соединяться с P-2602 и получать доступ в Интернет через P-2602 могут только компьютеры с динамическими или статическими IP-адресами в одной подсети с P-2602.
Windows Networking (NetBIOS over TCP/IP)	NetBIOS (базовая сетевая система ввода-вывода) представляет собой широковещательные пакеты TCP или UDP, позволяющие компьютеру подключаться и взаимодействовать с локальной сетью. Пакеты NetBIOS могут приводить к вызову служб коммутируемого доступа посредством PPPoE или PPTP, даже если эти службы не были запрошены пользователем. В других случаях требуется разрешить пакетам NetBIOS проходить в сеть WAN, чтобы найти компьютер на стороне WAN.
Allow between LAN and WAN	Отметьте этот флажок, чтобы разрешить пересылку пакетов NetBIOS из LAN в WAN и из WAN в LAN. Если в межсетевом экране политика по умолчанию блокирует трафик из WAN в LAN, то необходимо также включить в межсетевом экране правило, разрешающее по умолчанию пересылать трафик NetBIOS из WAN в LAN. Снимите этот флажок, чтобы блокировать пакеты NetBIOS, пересылаемые из LAN в WAN и из WAN в LAN.
Back	Для возврата к предыдущему экрану нажмите кнопку **Back**.
Apply	Чтобы сохранить изменения, выберите **Apply**.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

8.4 Настройка DHCP

Чтобы перейти на показанный ниже экран, выберите **Network > DHCP Setup**. Этот экран служит для настройки параметров DNS-сервера, которые P-2602 сообщает DHCP-клиентам в локальной сети.

Рис. 57 Настройка DHCP



Поля изображённого выше экрана описаны в следующей таблице.

Таб. 32 Настройка DHCP

ПОЛЕ	ОПИСАНИЕ
DHCP Setup	
DHCP	Если это поле установлено в значение **Server**, P-2602 может присваивать IP-адреса, адрес шлюза по умолчанию и адреса DNS-серверов DHCP-клиентам на базе Windows 95, Windows NT и других ОС. При выборе значения **None** сервер будет выключен. При выборе значения **Relay** P-2602 действует как заменитель DHCP-сервера и выполняет обмен запросами и откликами 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 настроить следующие параметры:
IP Pool Starting Address	В этом поле указывается первый адрес в непрерывном пуле IP-адресов.
Pool Size	В этом поле указывается размер или общая численность пула IP-адресов.
Remote DHCP Server	Если выше в поле **DHCP** был выбран режим **Relay**, введите в этом поле IP-адрес непосредственного удаленного DHCP-сервера.
DNS Server	
DNS Servers Assigned by DHCP Server	P-2602 передает IP-адрес сервера DNS (системы доменных имен) клиентам DHCP.

Таб. 32 Настройка DHCP

ПОЛЕ	ОПИСАНИЕ
First DNS Server Second DNS Server Third DNS Server	Если поставщик услуг Интернета автоматически присваивает параметры DNS-сервера (а также адрес P-2602 в сети WAN), выберите **Obtained From ISP**. Выберите **User-Defined**, если вам известен IP-адрес DNS-сервера. Введите IP-адрес DNS-сервера в расположенном справа поле. Если вы выбрали **User-Defined**, но оставили 0.0.0.0 в качестве IP-адреса, то после нажатия **Apply** поле **User-Defined** сменится на **None**. Если во втором поле вы выбрали **User-Defined** и ввели одинаковый IP address, то второе поле **User-Defined** после нажатия кнопки **Apply** сменится **None**. Чтобы использовать P-2602 в качестве прокси-сервера для DNS для тех случаев, когда поставщик услуг Интернета предоставляет информацию о DNS только через расширения IPCP, выберите **DNS Relay**. IP-адрес P-2602 в сети LAN отображается в поле справа (это поле доступно только для чтения). P-2602 сообщает DHCP-клиентам в локальной сети, что само устройство P-2602 является DNS-сервером. Когда компьютер в локальной сети отправляет запрос DNS в P-2602, P-2602 переадресует запрос на DNS-сервер, адрес которого получен в IPCP, и передает отклик обратно компьютеру. Режим ретрансляции (**DNS Relay**) можно выбрать только для одного из трех серверов; если вы выберите **DNS Relay** для второго или третьего DNS-сервера, это значение изменится на **None** после нажатия кнопки **Apply**. Выберите **None**, если DNS-серверы настраивать не требуется. Для этого в локальной сети должен иметься другой DHCP-сервер, либо на всех компьютерах адреса DNS-серверов должны быть настроены вручную. Если DNS-сервер не настроен, для получения доступа к машине необходимо знать ее IP-адрес.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-2602.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

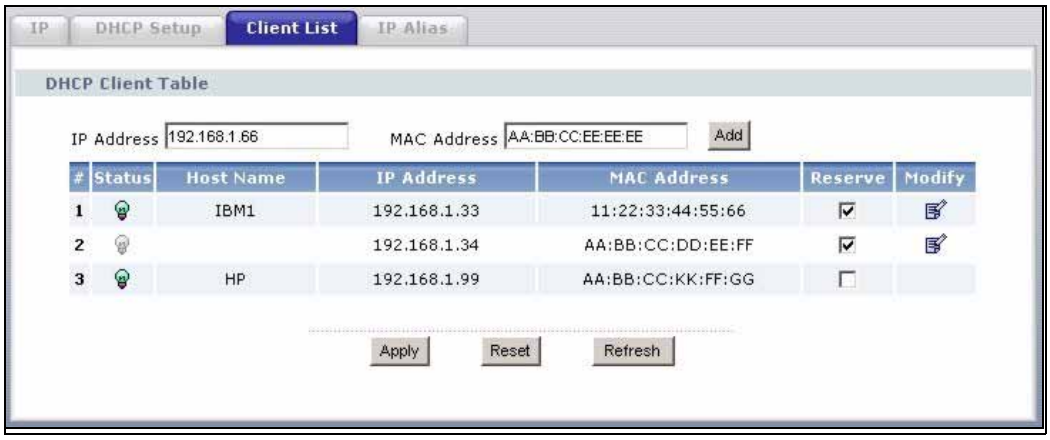
8.5 Список клиентов в локальной сети

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

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

Чтобы перейти на показанный ниже экран, выберите **Network > LAN > Client List**. Этот экран служит для изменения статических настроек DHCP в P-2602.

Рис. 58 Список клиентов в локальной сети



Поля изображённого выше экрана описаны в следующей таблице.

Таб. 33 Список клиентов в локальной сети

ПОЛЕ	ОПИСАНИЕ
IP Address	Введите IP-адрес, который требуется присвоить компьютеру в локальной сети с указанным ниже MAC-адресом.
MAC Address	Введите MAC-адрес компьютера в локальной сети.
Add	Нажмите **Add**, чтобы добавить статическую запись DHCP.
#	В данном поле отображается порядковый номер (строка) в статической таблице IP-адресов.
Status	В данном поле отображается состояние соединения клиента с P-2602.
Host Name	В данном поле отображается имя - хост компьютера.
IP Address	В данном поле отображается IP-адрес, соответствующий полю #, указанному в списке выше.
MAC Address	MAC-адрес, также называемый Ethernet-адресом локальной сети, уникален для каждого компьютера (адрес состоит из шести пар шестнадцатеричных символов). Плата сетевого интерфейса, например, Ethernet-адаптер, имеет жёстко запрограммированный заводской адрес. Порядок присвоения таких адресов является промышленным стандартом и позволяет исключить появление двух адаптеров с одинаковым адресом.
Reserve	Отметьте флажками записи (щелкните флажок в заголовке, чтобы автоматически отметить все записи), для которых P-2602 всегда должен присваивать выбранные IP-адреса в соответствии с указанными MAC-адресами (и именами хостов). В таблице можно выбрать до 128 записей. После нажатия кнопки **Apply** MAC-адрес и IP-адрес также появятся на экране **LAN Static DHCP** (где они будут доступны для редактирования).
Modify	Щелкните на значке редактирования, чтобы сделать поле IP-адреса доступным для редактирования и изменить адрес.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-2602.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.
Refresh	Чтобы повторно загрузить таблицу DHCP, нажмите кнопку **Refresh**.

8.6 Совмещение IP-адресов в локальной сети

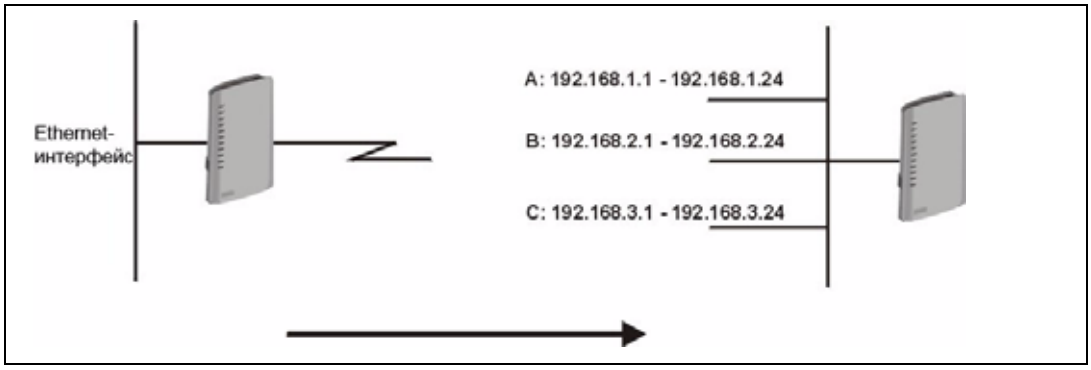
Функция совмещения IP-адресов (IP aliasing) позволяет разделить физическую сеть на различные логические сети, использующие один и тот же интерфейс Ethernet. P-2602 поддерживает до трех логических интерфейсов LAN на одном физическом интерфейсе Ethernet, при этом P-2602 будет выступать в качестве межсетевого шлюза для каждой сети LAN.

Используя совмещение IP-адресов, можно также настроить правила межсетевого экрана для управления доступом между логическими сетями (подсетями) в локальной сети.

Примечание: Следите за тем, чтобы подсети логических сетей не перекрывались.

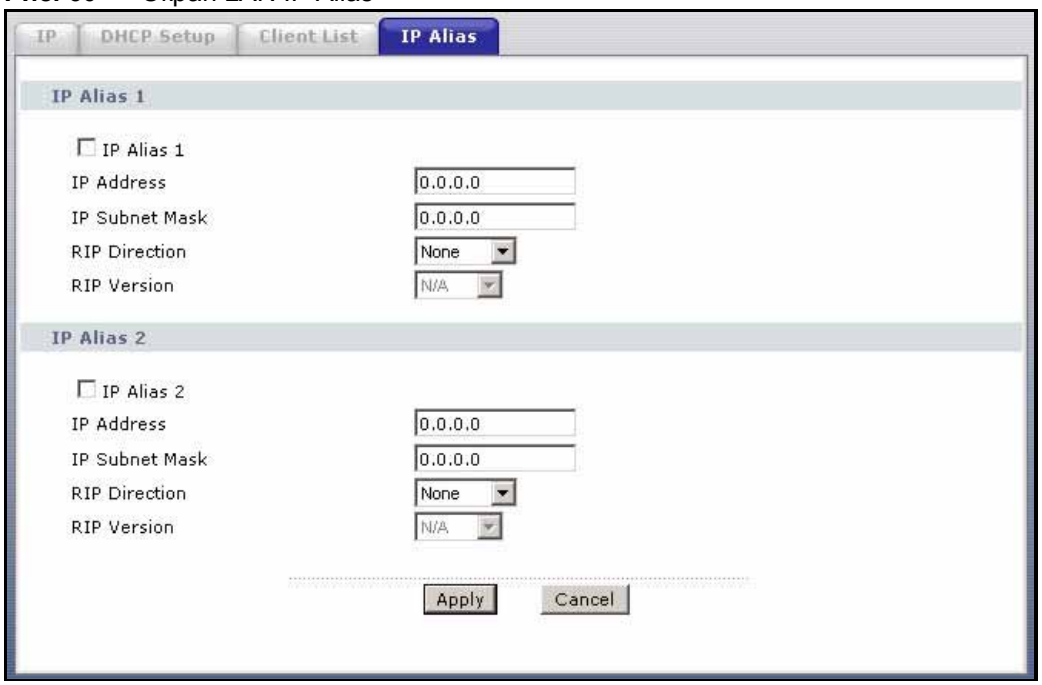
На следующем рисунке показана сеть LAN, разделенная на подсети A, B, и C.

Рис. 59 Физическая сеть и отдельные логические сети



Чтобы перейти на показанный ниже экран, выберите **Network** > **LAN** > **IP Alias**. Этот экран служит для изменения параметров совмещения IP-адресов в P-2602.

Рис. 60 Экран LAN IP Alias



Поля изображённого выше экрана описаны в следующей таблице.

Таб. 34 Экран LAN IP Alias

ПОЛЕ	ОПИСАНИЕ
IP Alias 1, 2	Отметьте флажок, чтобы настроить другую сеть LAN для P-2602.
IP Address	Введите IP-адрес вашего P-2602 в десятичном виде через точку. Вместо этого можно щелкнуть правой кнопкой мыши, чтобы скопировать и/или вставить IP-адрес.
IP Subnet Mask	P-2602 автоматически вычисляет маску подсети на основе назначаемого пользователем IP-адреса. Если вам не требуется деление на подсети, используйте маску подсети, рассчитанную P-2602.
RIP Direction	RIP (информационный протокол маршрутизации, стандарты RFC 1058 и RFC 1389) позволяет маршрутизатору обмениваться параметрами маршрутизации с другими маршрутизаторами. Поле **RIP Direction** управляет процессом отправки и приема RIP-пакетов. Выберите направление RIP: **Both** (вход-выход), **In Only** (только вход) или **Out Only** (только выход), **None** (нет). Если выбраны значения **Both** или **Out Only**, P-2602 будет периодически рассылать таблицу маршрутизации посредством широковещательного сообщения. Если выбраны значения **Both** или **In Only**, устройство будет объединять получаемые параметры RIP; если выбрано значение **None**, устройство не будет рассылать RIP-пакеты и будет игнорировать поступающие RIP-пакеты.

Таб. 34 Экран LAN IP Alias

ПОЛЕ	ОПИСАНИЕ
RIP Version	Поле **RIP Version** управляет форматом и способом широковещательной рассылки RIP-пакетов с P-2602 (устройство принимает пакеты обоих форматов). **RIP-1** поддерживается всеми устройствами, а RIP-2 позволяет передавать больше информации. RIP-1 обычно достаточен для большинства сетей, кроме сетей со сложной топологией. Модификации **RIP-2B** и **RIP-2M** передают сведения о маршрутизации в формате RIP-2; различие между ними состоит в том, что в **RIP-2B** используется широковещательная рассылка по подсетям, а в **RIP-2M** – многоадресная рассылка. Многоадресная рассылка может уменьшить загрузку на машинах, не являющихся маршрутизаторами, поскольку они обычно не откликаются по адресу многоадресной рассылки RIP и в этом случае просто не будут получать пакеты RIP. Однако если один маршрутизатор использует многоадресную рассылку, то все маршрутизаторы в вашей сети также должны использовать многоадресную рассылку. По умолчанию для протокола RIP выбрано направление **Both** (вход-выход), а поле Version установлено в значение **RIP-1**.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-2602.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

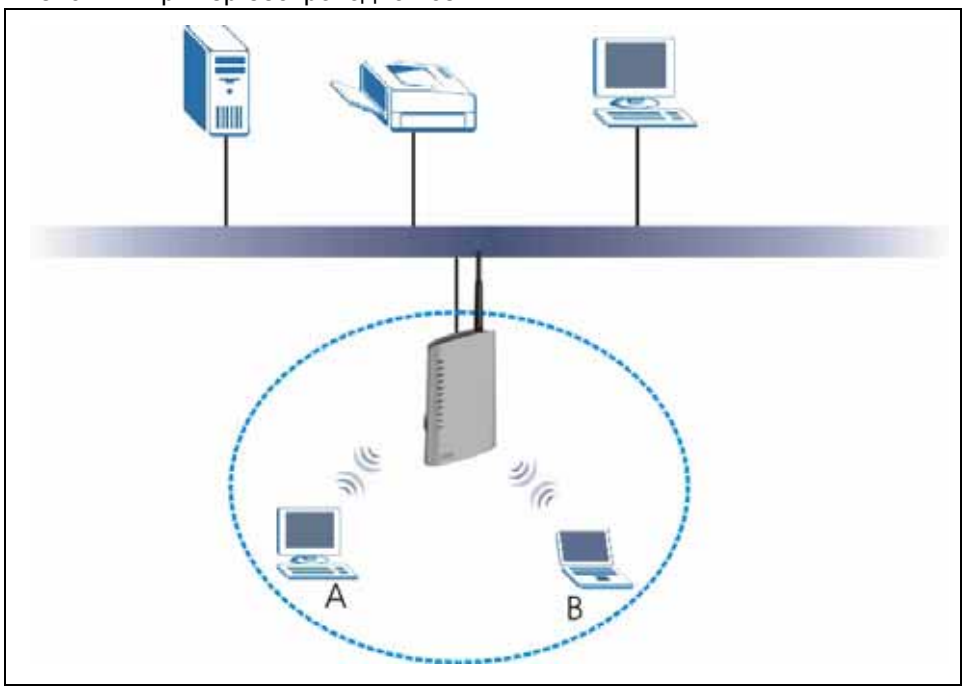
Глава 9
Беспроводная локальная сеть

В этой главе рассматривается настройка параметров беспроводной сети в P-2602. Более подробные сведения о беспроводных сетях см. в приложениях. Данная глава относится только к моделям с индексом “W”.

9.1 Общие сведения о беспроводных сетях

На следующем рисунке изображен пример беспроводной сети.

Рис. 61 Пример беспроводной сети



Беспроводная сеть обведена синим кругом. В беспроводной сети устройства **A** и **B** через точку доступа (**AP**) взаимодействуют с другими устройствами (например, с принтером) и с Интернетом. Точкой доступа является ваше устройство P-2602.

Каждая беспроводная сеть должна соответствовать следующим основным принциам.

- Все устройства в одной беспроводной сети должны использовать одинаковый идентификатор SSID.

  SSID – это имя беспроводной сети. Аббревиатура SSID означает “идентификатор набора сетевых служб” (Service Set IDentity).

- Две территориально перекрывающиеся беспроводные сети должны использовать разные частотные каналы.

  В каждой беспроводной сети для передачи и приема информации используется определенный частотный канал, аналогичный радиостанции или телевизионному каналу.

- Все устройства в одной беспроводной сети должны использовать средства безопасности, совместимые с точкой доступа.

  Средства безопасности предотвращают несанкционированный доступ к сети. Они также защищают информацию, передаваемую по беспроводной сети.

9.2 Общие сведения о безопасности беспроводных сетей

В следующих подразделах рассматриваются основные средства безопасности беспроводных сетей.

9.2.1 SSID

Обычно P-2602 выступает в качестве радиомаяка, регулярно передавая в эфир идентификаторы SSID. Можно скрыть эти идентификаторы, отключив их рассылку на P-2602. Кроме того, необходимо сменить заводской SSID на выбранное вами значение, которое не может быть легко угадано.

Защита, обеспечиваемая этими мерами, малоэффективна, поскольку для беспроводных устройств остаются способы несанкционированного получения SSID. Кроме того, беспроводные устройства по-прежнему могут следить за информацией, передаваемой по беспроводной сети.

9.2.2 Фильтр MAC-адресов

Каждое устройство в беспроводной сети имеет уникальный идентификационный номер – MAC-адрес.[1] MAC-адрес обычно записывается в виде двенадцати шестнадцатеричных символов[2]: например, 00A0C5000002 или 00:A0:C5:00:00:02. Чтобы узнать MAC-адрес для каждого устройства беспроводной сети, обратитесь к руководству пользователя на соответствующее устройство или к другой документации.

1. Некоторые беспроводные устройства (например, сканеры) могут только обнаруживать присутствие беспроводных сетей, не имея возможности в них работать. MAC-адреса у таких беспроводных устройств могут отсутствовать.
2. Шестнадцатеричными являются знаки из набора: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F.

Фильтр MAC-адресов позволяет задать для P-2602 список устройств, которым разрешено или не разрешено использовать беспроводную сеть. Если устройству разрешено использовать беспроводную сеть, оно также должно иметь правильные настройки (SSID, частотный канал и параметры безопасности). Если устройству не разрешено использовать беспроводную сеть, наличие у него необходимых настроек не имеет значения.

Этот вид защиты не защищает информацию, передаваемую по беспроводной сети. Кроме того, беспроводные устройства могут несанкционированным образом присвоить себе MAC-адрес разрешенного устройства, посредством которого они будут использовать беспроводную сеть.

9.2.3 Аутентификация пользователя

Аутентификация – это процесс, при котором проверяется право беспроводного устройства на использование беспроводной сети. Аутентификацию можно настроить так, чтобы каждый пользователь должен был регистрироваться перед входом в беспроводную сеть. Однако для этого каждое устройство в беспроводной сети должно поддержать IEEE 802.1x.

Для беспроводных сетей можно хранить имена и пароли каждого пользователя на RADIUS-сервере. Этот сервер чаще применяется в корпоративных сетях, чем в домашних. При отсутствии RADIUS-сервера настройка имен пользователей и паролей невозможна.

Для беспроводных устройств сохраняется возможность несанкционированного просмотра информации, пересылаемой по беспроводной сети, даже если они не могут использовать сеть. Кроме того, беспроводные устройства могут несанкционированным образом узнать имя пользователя и пароль, чтобы использовать эти реквизиты для получения доступа к сети.

9.2.4 Шифрование

Для защиты данных, пересылаемых по беспроводной сети, применяется шифрование. Шифрование равносильно применению некоторого секретного кода, не зная который, невозможно получить доступ к зашифрованной информации.

В зависимости от типа аутентификации могут применяться два типа шифрования. (Дополнительные сведения см. в разд. 9.2.3 на стр. 133.)

Таб. 35 Типы шифрования для различных типов аутентификации

	Без аутентификации	RADIUS-сервер
Наименьший уровень безопасности	Без средств безопасности	
↕	Статическое шифрование WEP	
	WPA-PSK	WPA
Наибольший уровень безопасности	WPA2-PSK	WPA2

Например, если для беспроводной сети предусмотрен RADIUS-сервер, можно выбрать **WPA** или **WPA2**. Если пользователи не регистрируются для входа в беспроводную сеть, можно выбрать отсутствие шифрования, **статическое шифрование WEP**, **WPA-PSK** или **WPA2-PSK2**.

Обычно рекомендуется выбирать наиболее стойкий метод шифрования из числа поддерживаемых всеми устройствами беспроводной сети. Для примера рассмотрим построение беспроводной сети с P-2602. Сеть не имеет RADIUS-сервера, поэтому аутентификация отсутствует. Предположим, что в беспроводной сети находятся два устройства. Устройство A поддерживает только WEP, а устройство B поддерживает WEP и WPA. Поэтому для беспроводной сети следует выбрать **статическое шифрование WEP**.

Примечание: В беспроводных сетях рекомендуется применять **WPA-PSK**, **WPA** или более стойкие методы шифрования. Другие типы шифрования лучше, чем полное его отсутствие, но они содержат ряд уязвимостей, позволяющих несанкционированно дешифровать информацию за относительно короткое время.

При выборе методов шифрования **WPA2** или **WPA2-PSK** в P-2602 можно также включить дополнительную поддержку WPA, выбрав параметр **WPA compatible**. В этом случае, если одни устройства поддерживают WPA, а другие – WPA2, в P-2602 нужно установить метод **WPA2-PSK** или **WPA2** (в зависимости от способа входа в беспроводную сеть) и выбрать параметр **WPA Compatible**.

Во многих типах шифрования для беспроводных сетей для защиты информации используется ключ. Чем длиннее ключ, тем сильнее шифрование. Каждое устройство в беспроводной сети должно иметь один и тот же ключ.

9.2.5 Технология OTIST

Фирменная технология ZyXEL OTIST (One-Touch Intelligent Security Technology) позволяет задать в P-2602 идентификатор SSID и тип шифрования (WEP или WPA-PSK) и распространить эти параметры с P-2602 по устройствам в беспроводных сетях. В результате снимается необходимость установки SSID и метода шифрования на каждом устройстве в беспроводной сети.

Устройства в беспроводной сети должны поддерживать OTIST и должны находиться в диапазоне покрытия P-2602 во время активации этой функции. Дополнительные сведения см. в разд. 9.6 на стр. 144.

9.3 Основные аспекты производительности

В следующих подразделах рассмотрены различные способы улучшения производительности беспроводной сети.

9.3.1 Качество обслуживания (QoS)

Для улучшения передачи голосовых и видеоданных по беспроводной сети можно включить QoS для мультимедийных приложений Wi-Fi (WMM) . QoS назначит высокий приоритет голосовым и видеоданным, что обеспечит более равномерную их передачу. Точно так же многопоточной загрузке крупных файлов будет назначен низкий приоритет, чтобы передача этих данных не ухудшала качество работы других приложений.

9.4 Специальная терминология беспроводной связи

В следующей таблице перечислены термины и сокращения из области беспроводных сетей, используемые в P-2602.

ТЕРМИН	ОПИСАНИЕ
Внутренний трафик в системе базовой станции (Intra-BSS Traffic)	Этот термин относится к прямому обмену данными (в обход P-2602) между двумя устройствами беспроводной сети. Для повышения безопасности беспроводной сети можно отключить этот способ связи.
Порог квитирования RTS/CTS (RTS/CTS Threshold)	В беспроводной сети, охватывающей большую площадь, беспроводные устройства могут не знать о присутствии друг друга. В результате они могут одновременно передавать информацию на точку доступа, вызывая коллизии и препятствуя прохождению информации. Если это значение ниже значения по умолчанию, беспроводным устройствам в определенных случаях потребуется запрашивать разрешение у P-2602. Чем ниже значение, тем чаще устройства должны запрашивать разрешение. Если это значение больше порога фрагментации (см. ниже), беспроводным устройствам никогда не требуется запрашивать разрешение у P-2602.

ТЕРМИН	ОПИСАНИЕ
Преамбула (Preamble)	Преамбула используется для синхронизации передачи в беспроводной сети. Существует 2 режима преамбулы: длинный и короткий. Если режим преамбулы, используемый устройством, не совпадает с режимом P-2602, обмен данными с P-2602 невозможен.
Аутентификация (Authentication)	Аутентификация – это процесс, при котором проверяется право беспроводного устройства на использование беспроводной сети.
Максимальная пиковая скорость кадров (Max. Frame Burst)	Включите этот параметр, чтобы улучшить производительность сетей, использующих только IEEE 802.11g или сочетание IEEE 802.11b/g. Максимальная пиковая скорость кадров устанавливает максимальное время, в течение которого P-2602 передает только беспроводный трафик IEEE 802.11g.
Порог фрагментации (Fragmentation Threshold)	Для загруженных сетей рекомендуется небольшой порог фрагментации. Увеличение порога повышает быстродействие, если сеть загружена слабо.
Роуминг (Roaming)	При наличии в вашей беспроводной сети двух или более P-2602 (или других точек беспроводного доступа) можно включить этот параметр, чтобы беспроводные устройства могли перемещаться в другую сеть без повторной регистрации. Это полезно для таких устройств, как ноутбуки, которые часто меняют местоположение.

9.5 Экран общей настройки WLAN

Примечание: При настройке P-2602 с использованием компьютера, подключенного к беспроводной LAN, и изменении настроек SSID или WEP в P-2602 беспроводная связь разрывается после подтверждения настроек кнопкой **Apply**. Затем нужно изменить настройки беспроводного соединения своего компьютера, чтобы они соответствовали новым настройкам P-2602.

Чтобы перейти на экран **Wireless LAN General** , выберите **Network > Wireless LAN**.

Рис. 62 Беспроводная сеть: общие настройки

Поля для настройки общих параметров беспроводной сети описаны в следующей таблице.

Таб. 36 Беспроводная сеть: общие настройки

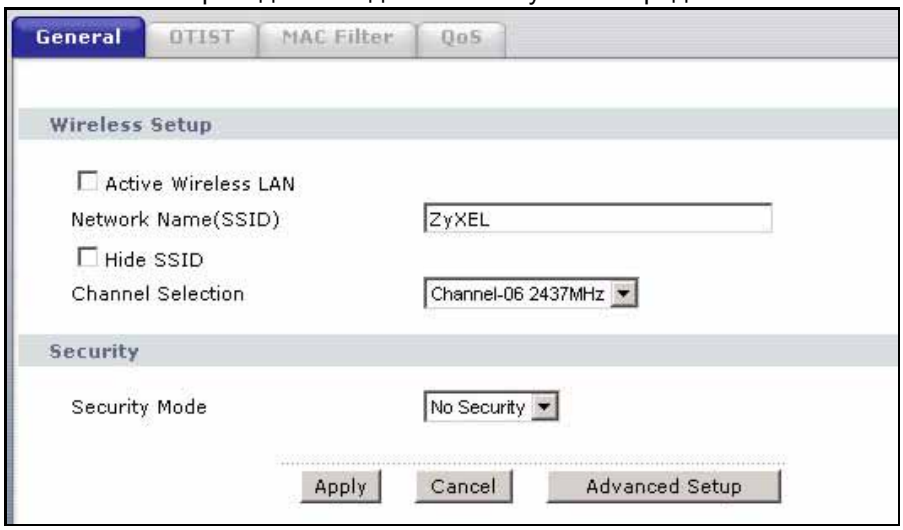
ПОЛЕ	ОПИСАНИЕ
Active Wireless LAN	Отметьте этот флажок Active, чтобы активировать беспроводную сеть.
Network Name(SSID)	(Идентификатор набора услуг) SSID определяет Service Set (Набор услуг), с которым связана беспроводная станция. Беспроводные станции, связанные с точкой доступа (AP), должны иметь одну и ту же SSID. Введите описательное имя (до 32 символов из 7 бит в кодировке ASCII) для беспроводной сети. **Примечание:** При настройке P-2602 с использованием компьютера, подключенного к беспроводной LAN, и изменении настроек SSID или WEP в P-2602 беспроводная связь разрывается после подтверждения настроек кнопкой Apply. Затем нужно изменить настройки беспроводного соединения своего компьютера, чтобы они соответствовали новым настройкам P-2602.
Hide SSID	Отметьте этот флажок, чтобы скрывать SSID в исходящих кадрах радиомаяка, при этом получить SSID с помощью инструментов пассивного сканирования будет невозможно.
Channel Selection	Выберите рабочую частоту/канал из числа разрешенных в вашем регионе. Выберите номер канала из раскрывающегося списка.
Security Mode	Подробное описание этого поля см. в следующих разделах.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-2602.
Cancel	Чтобы возвратить настройки на этом экране в их прежнее состояние, нажмите **Cancel**.
Advanced Setup	Чтобы перейти на экран **Wireless Advanced Setup** для редактирования дополнительных параметров WLAN, нажмите **Advanced Setup**.

9.5.1 Без средств безопасности

Выберите **No Security**, чтобы разрешить беспроводным станциям устанавливать связь с точками доступа без какого-либо шифрования данных.

Примечание: Если средства безопасности при беспроводной передаче данных через P-2602 не используются, сеть доступна любому беспроводному устройству, находящемуся в зоне покрытия.

Рис. 63 Беспроводное соединение: отсутствие средств безопасности



Поля изображённого выше экрана описаны в следующей таблице.

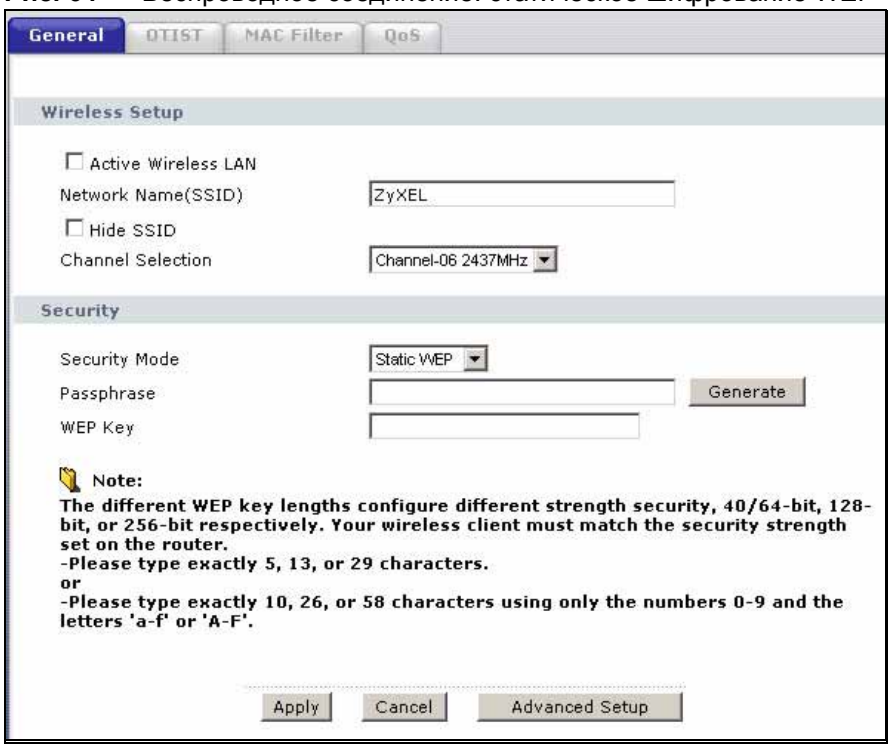
Таб. 37 Беспроводное соединение с отсутствием средств безопасности

ПОЛЕ	ОПИСАНИЕ
Security Mode	Выберите **No Security** в раскрывающемся списке.

9.5.2 Экран WEP Encryption

Для настройки и включения шифрования WEP перейдите на экран **General** , выбрав **Network > Wireless LAN**. В списке **Security Mode** выберите **Static WEP**.

Рис. 64 Беспроводное соединение: статическое шифрование WEP



Поля для настройки безопасности беспроводной сети описаны в следующей таблице.

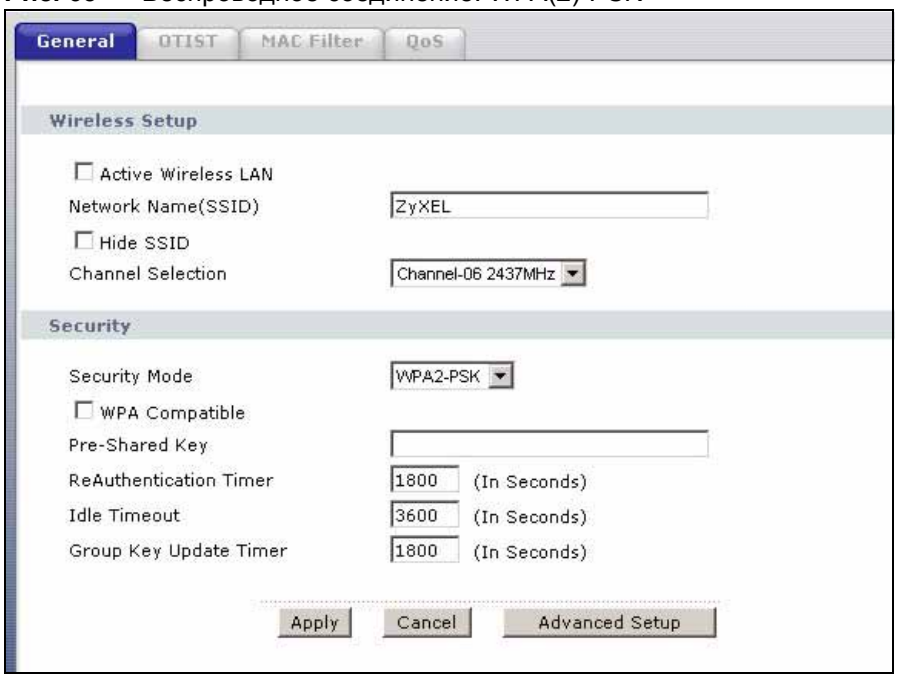
Таб. 38 Беспроводное соединение: статическое шифрование WEP

ПОЛЕ	ОПИСАНИЕ
Security Mode	В раскрывающемся списке выберите **Static WEP**.
Passphrase	Введите идентификационную фразу (до 32 печатных символов) и щелкните **Generate**. P-2602 автоматически генерирует ключ WEP.
WEP Key	Ключи WEP используются для шифрования данных. Для передачи данных P-2602 и беспроводные станции должны использовать один и тот же ключ WEP. Чтобы вручную задать ключ WEP, введите любые 5, 13 или 29 символов (строка ASCII) или 10, 26 или 58 шестнадцатеричных символов (“0-9”, “A-F”), соответственно, для 64-битового, 128-битового или 256-битового ключа WEP.

9.5.3 WPA(2)-PSK

Для настройки и включения аутентификации WPA-PSK перейдите на экран **General** , выбрав **Network > Wireless LAN** . В списке **Security Mode** выберите **WPA-PSK** или **WPA2-PSK**.

Рис. 65 Беспроводное соединение: WPA(2)-PSK



Поля для настройки безопасности беспроводной сети описаны в следующей таблице.

Таб. 39 Беспроводное соединение: WPA(2)-PSK

ПОЛЕ	ОПИСАНИЕ
Security Mode	В раскрывающемся списке выберите **WPA-PSK** или **WPA2-PSK**.
WPA Compatible	Это поле доступно только для WPA2-PSK. Отметьте этот флажок, чтобы включить в P-2602 одновременную поддержку WPA-PSK и WPA2-PSK.
Pre-Shared Key	Механизмы шифрования, используемые для **WPA(2)** и **WPA(2)-PSK**, одинаковы. Единственное различие между ними состоит в том, что в **WPA(2)-PSK** используется простой общий пароль вместо реквизитов конкретных пользователей. Введите ключ для предварительного совместного использования – от 8 до 63 символов ASCII с учетом регистра (включая пробелы и специальные символы) или 64 шестнадцатеричных символа.
ReAuthentication Timer	Укажите число секунд, по истечении которого беспроводные станции должны повторно отправлять имя пользователя и пароль для продолжения соединения. Допустимые интервалы – от 10 до 9999 секунд. По умолчанию принят интервал 1800 секунд (30 минут). **Примечание:** Если аутентификация станций беспроводной сети производится посредством RADIUS-сервера, будет иметь приоритет таймер повторной аутентификации на RADIUS-сервере.

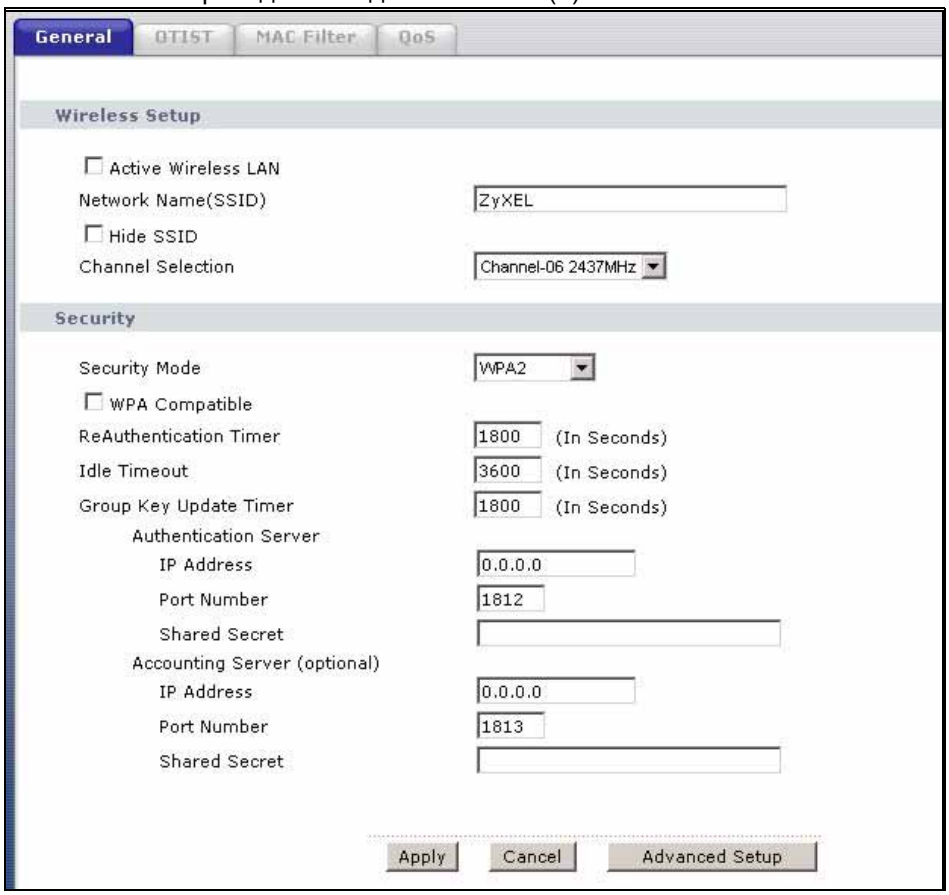
Таб. 39 Беспроводное соединение: WPA(2)-PSK

ПОЛЕ	ОПИСАНИЕ
Idle Timeout	P-2602 автоматически отключает клиента от беспроводной сети после периода неактивности. Клиенту придется снова вводить имя пользователя и пароль для получения доступа к проводной сети. Интервал времени по умолчанию 3600 секунд (или 1 час).
Group Key Update Timer	**Таймер обновления ключа группы WPA** – это скорость, с которой точка доступа (при использовании управления ключом **WPA(2)-PSK**) или сервер **RADIUS** (при использовании управления ключом WPA) отсылает новый ключ группы всем клиентам. Процесс повторного назначения ключа является эквивалентом WPA автоматического изменения ключа WEP для AP и всех станций в беспроводной LAN на периодической основе. Параметр **WPA Group Key Update Timer** (таймер обновления ключа группы WPA) также поддерживается в режиме**WPA-PSK**. По умолчанию P-2602 использует интервал **1800** секунд (30 минут).

9.5.4 Экран настройки аутентификации WPA(2)

Для настройки и включения аутентификации WPA вызовите экран **Wireless**, щелкнув на ссылке **Wireless LAN** в разделе **Network**. В списке **Security** выберите **WPA** или **WPA2**.

Рис. 66 Беспроводное соединение: WPA(2)



Поля для настройки безопасности беспроводной сети описаны в следующей таблице.

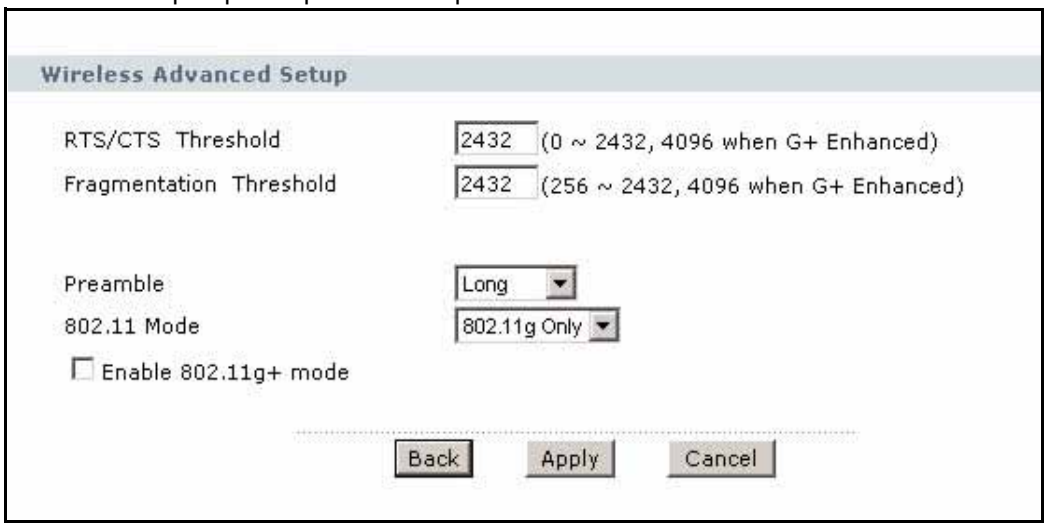
Таб. 40 Беспроводное соединение: WPA(2)

ПОЛЕ	ОПИСАНИЕ
Security Mode	В раскрывающемся списке выберите **WPA** или **WPA2**.
WPA Compatible	Это поле доступно только для WPA2. Отметьте этот флажок, чтобы включить в P-2602 одновременную поддержку WPA и WPA2.
ReAuthentication Timer	Укажите число секунд, по истечении которого беспроводные станции должны повторно отправлять имя пользователя и пароль для продолжения соединения. Допустимые интервалы – от 10 до 9999 секунд. По умолчанию принят интервал 1800 секунд (30 минут). **Примечание:** Если аутентификация станций беспроводной сети производится посредством RADIUS-сервера, будет иметь приоритет таймер повторной аутентификации на RADIUS-сервере.
Idle Timeout	P-2602 автоматически отключает клиента от беспроводной сети после периода неактивности. Клиенту придется снова вводить имя пользователя и пароль для получения доступа к проводной сети. Интервал времени по умолчанию 3600 секунд (или 1 час).
WPA Group Key Update Timer	**Таймер обновления ключа группы WPA** – это скорость, с которой точка доступа (при использовании управления ключом**WPA- PSK**) или сервер **RADIUS** (при использовании управления ключом WPA) отсылает новый ключ группы всем клиентам. Процесс повторного назначения ключа является эквивалентом WPA автоматического изменения ключа WEP для AP и всех станций в беспроводной LAN на периодической основе. Установка **WPA Group Key Update Timer (Таймера обновления ключа группы WPA)** также поддерживается в режиме**WPA- PSK**. По умолчанию P-2602 использует интервал **1800** секунд (30 минут).
Authentication Server	
IP Address	Введите IP-адрес внешнего сервера аутентификации в десятичном виде через точку.
Port Number	Введите номер порта внешнего сервера аутентификации. Номер порта по умолчанию – **1812**. Это значение можно изменить только с разрешения администратора сети.
Shared Secret	Укажите пароль (длиной до 31 алфавитно-цифрового знака), который будет служить ключом для совместного использования внешним сервером учета и P-2602. Он должен быть одинаковым у внешнего сервера учета и P-2602. Этот ключ не пересылается по сети.
Accounting Server	
IP Address	Введите IP-адрес внешнего сервера учета в десятичном виде через точку.
Port Number	Введите номер порта внешнего сервера учета. Номер порта по умолчанию – **1813**. Это значение можно изменить только с разрешения администратора сети.
Shared Secret	Укажите пароль (длиной до 31 алфавитно-цифрового знака), который будет служить ключом для совместного использования внешним сервером учета и P-2602. Он должен быть одинаковым у внешнего сервера учета и P-2602. Этот ключ не пересылается по сети.

9.5.5 Расширенная настройка беспроводной сети

Для настройки расширенных параметров беспроводной сети нажмите кнопку **Advanced Setup** на экране **General** . Появится изображенный ниже экран.

Рис. 67 Экран расширенной настройки



Поля изображённого выше экрана описаны в следующей таблице.

Таб. 41 Беспроводная сеть: расширенная настройка

ПОЛЕ	ОПИСАНИЕ
Wireless Advanced Setup	
RTS/CTS Threshold	Введите число от 0 до 2432. Если выбран флажок “G+ Enhanced”, появится значение 4096.
Fragmentation Threshold	Это максимальный размер фрагмента данных, который можно отправить. Введите число от 256 до 2432. Если выбран флажок “G+ Enhanced”, появится значение 4096.
Preamble	Выберите тип преамбулы в раскрывающемся списке: **Long** (длинный), **Short** (короткий) или **Dynamic** (динамический). Значение по умолчанию – **Long**. Подробности см. в приложении.
802.11 Mode	Чтобы разрешить соединяться с P-2602 только устройствам, отвечающим стандарту IEEE 802.11b, выберите **802.11b Only**. Чтобы разрешить соединяться с P-2602 только устройствам, отвечающим стандарту IEEE 802.11g, выберите **802.11g Only**. Чтобы разрешить соединяться с P-2602 устройствам, отвечающим любому стандартов: IEEE 802.11b или IEEE 802.11g, выберите **Mixed**. Скорость передачи у вашего устройства P-2602 может несколько снизиться.
Enable 802.11g+ mode	Отметьте флажок **Enable 802.11g+ mode**, чтобы разрешить всем WLAN-устройствам ZyXEL, поддерживающим эту функцию, соединяться с P-2602 на более высокой скорости. P-2602 при этом будет передавать данные на скорости выше, чем в режиме **802.11g Only**.
Back	Выберите эту ссылку, чтобы вернуться к предыдущему экрану без сохранения изменений.

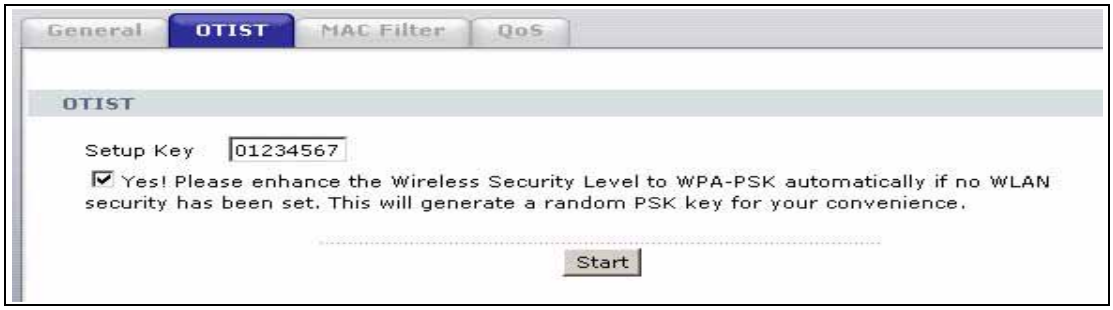
Таб. 41 Беспроводная сеть: расширенная настройка

ПОЛЕ	ОПИСАНИЕ
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-2602.
Cancel	Чтобы возвратить настройки на этом экране в их прежнее состояние, нажмите **Cancel**.

9.6 Экран OTIST

Этот экран служит для настройки и запуска функции OTIST в P-2602 для вашей беспроводной сети. Чтобы перейти на этот экран, выберите **Network > Wireless LAN > OTIST**.

Рис. 68 Network > Wireless LAN > OTIST



Поля изображённого выше экрана описаны в следующей таблице.

Таб. 42 Экран Network > Wireless LAN > OTIST

ПОЛЕ	ОПИСАНИЕ
Setup Key	Введите ключ (пароль) длиной 8 символов ASCII. **Примечание:** Изменив ключ настройки OTIST в P-2602, его также необходимо изменить в беспроводных устройствах.

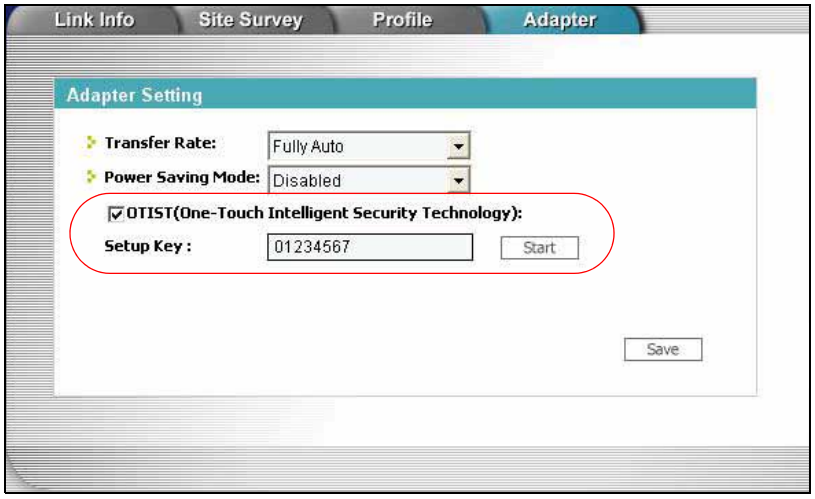
Таб. 42 Экран Network > Wireless LAN > OTIST (продолжение)

ПОЛЕ	ОПИСАНИЕ
Yes!	Выберите это поле, чтобы устройство P-2602 автоматически сгенерировало для беспроводной сети ключ для предварительного совместного использования. Перед этим пройдите по ссылке **Network > Wireless LAN > General** и установите **Security Mode** в значение **No Security**. Снимите этот флажок, чтобы устройство P-2602 применяло введенный вами ключ для предварительного совместного использования. Перед этим выберите **Network > Wireless LAN > General**, установите параметр **Security Mode** в значение **WPA-PSK** и введите ключ в поле **Pre-Shared Key**.
Start	Нажмите **Start**, чтобы активировать OTIST и распространить по сети параметры настройки. Этот процесс занимает три минуты. **Примечание:** Кнопку **Start** в настройках P-2602 и аналогичные кнопки в настройках других устройств необходимо нажать в течение трех минут. Запускать настройку OTIST в беспроводных устройствах и P-2602 можно в любом порядке.

Перед нажатием кнопки **Start** необходимо включить OTIST во всех устройствах беспроводной сети, поддерживающих эту технологию OTIST. Для большинства устройств достаточно следующих операций.

1. Запустите утилиту ZyXEL
2. Перейдите на закладку **Adapter**.
3. Отметьте флажок **OTIST** и введите в поле **Setup Key** тот же ключ настройки, что и в P-2602.
4. Нажмите кнопку **Save** (Сохранить).

Рис. 69 Пример: экран OTIST беспроводного клиента



Чтобы запустить OTIST в устройстве, нажмите на этом экране кнопку **Start**.

Примечание: Кнопку **Start** в настройках P-2602 и аналогичные кнопки в настройках других устройств необходимо нажать в течение трех минут. Запускать настройку OTIST в беспроводных устройствах и P-2602 можно в любом порядке.

После нажатия кнопки **Start** в настройках P-2602 откроется следующий экран (на P-2602).

Рис. 70 OTIST: параметры

Ключ, указанный на этом экране, можно использовать для ручной настройки шифрования WPA-PSK для устройств беспроводной сети, не поддерживающих OTIST.

Проверьте настройки и нажмите **OK**. P-2602 начнет передавать параметры OTIST. В конфигураторах P-2602 и беспроводных устройств откроются следующие экраны.

Рис. 71 OTIST: ход выполнения на P-2602

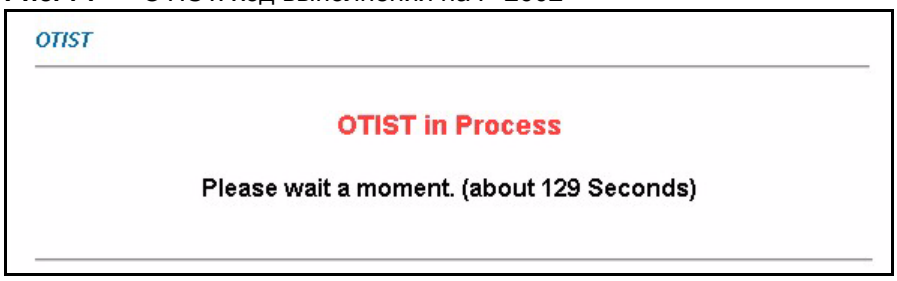


Рис. 72 OTIST: ход выполнения на беспроводном устройстве

Эти экраны закроются по завершении передачи.

9.6.1 Замечания по использованию OTIST

1 Если вы включили OTIST в беспроводном устройстве, этот экран будет появляться каждый раз, когда вы запускаете утилиту. Для поиска точки доступа с поддержкой OTIST (т.е. для отыскания P-2602) нажмите **Yes**.

Рис. 73 Запрос подтверждения на запуск OTIST

2 Если беспроводное устройство с поддержкой OTIST теряет связь по беспроводной сети более чем на десять секунд, оно будет искать точку доступа с поддержкой OTIST в течение одной минуты. (Если поиск точки доступа с поддержкой OTIST запускается вручную, продолжительность поиска не ограничивается; чтобы остановить поиск, нажмите **Cancel** на экране хода выполнения OTIST).

3 Чтобы повторно передать настройки после того, как беспроводное устройство найдет точку доступа с поддержкой OTIST, необходимо нажать **Start** на экране **Network > Wireless LAN > OTIST** для P-2602 или нажать и держать нажатой кнопку **Reset** на P-2602 в течение одной или двух секунд.

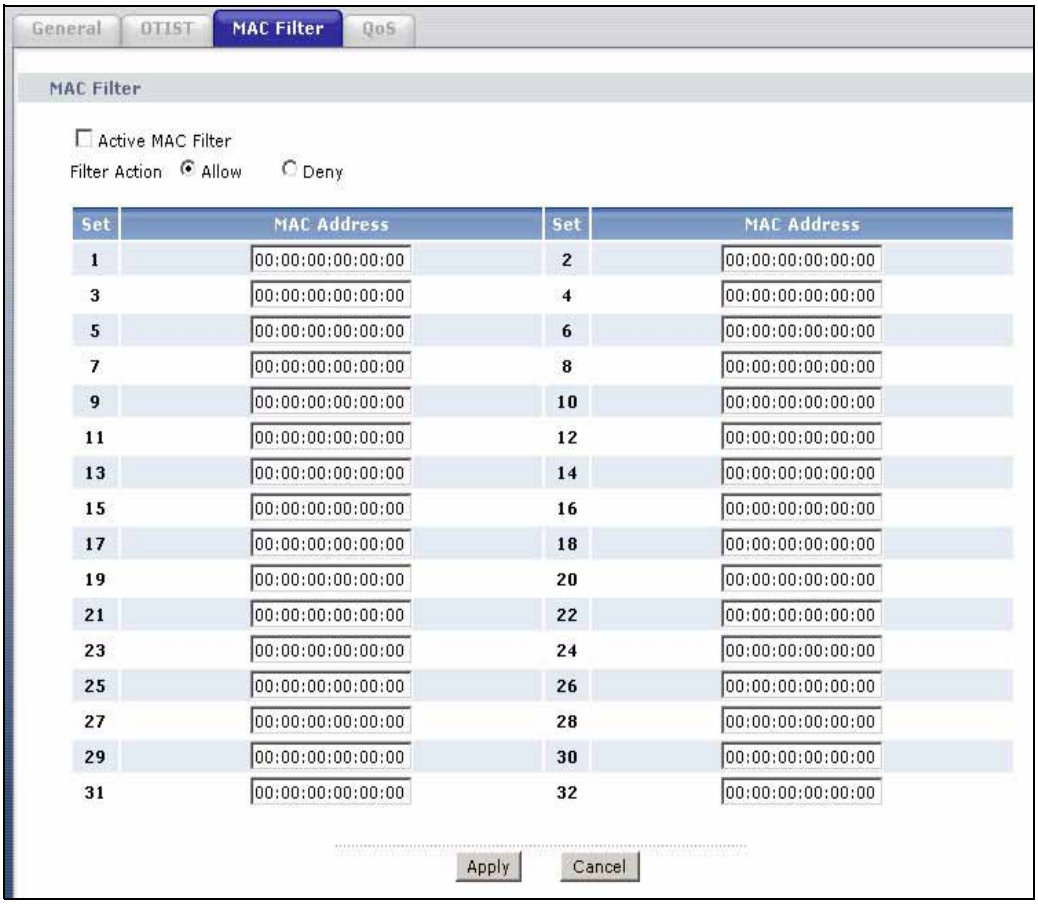
4 Если после использования OTIST вы измените SSID или ключи на P-2602, необходимо будет снова запустить OTIST или ввести соответствующие параметры вручную на беспроводных устройствах.

5 Если вы настроили OTIST для генерации ключа WPA-PSK, этот ключ будет меняться каждый раз, когда вы выполняете OTIST. Поэтому при подключении нового устройства к вашей беспроводной сети вы должны повторно выполнить OTIST на точке доступа и ВСЕХ беспроводных устройствах.

9.7 Экран MAC Filter

Чтобы изменить настройки фильтрации MAC-адресов в P-2602, выберите **Network > Wireless LAN** > **MAC Filter**. Появится изображенный ниже экран.

Рис. 74 Фильтр MAC-адресов



Поля этого меню описаны в следующей таблице.

Таб. 43 Фильтр MAC-адресов

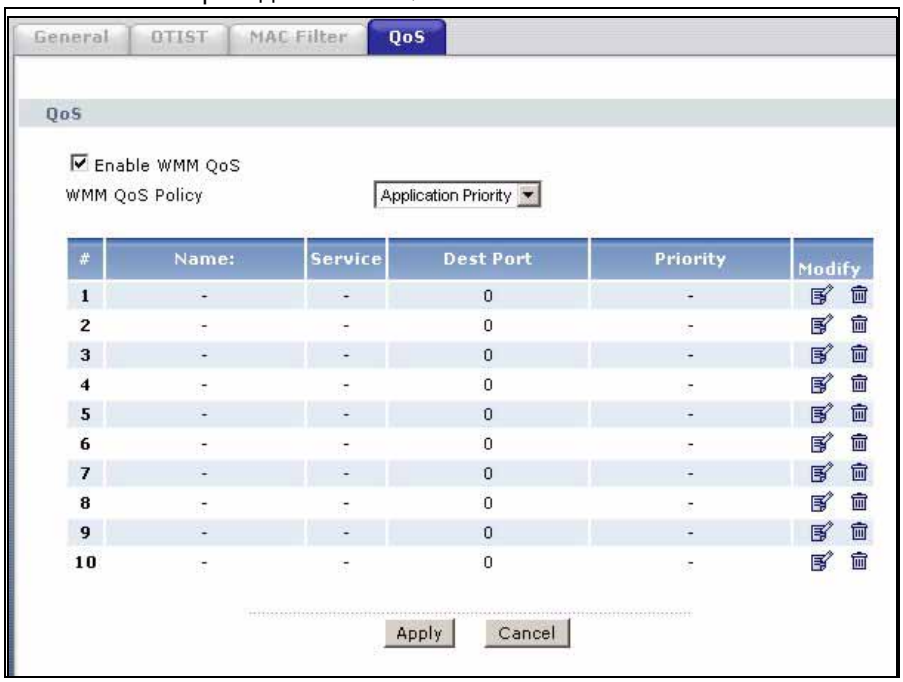
ПОЛЕ	ОПИСАНИЕ
Active MAC Filter	Чтобы активировать фильтрацию по MAC-адресам, отметьте этот флажок.
Filter Action	Определите действие фильтра для списка MAC-адресов в таблице **MAC Address**. Выберите **Deny**, чтобы блокировать доступ к P-2602. С MAC-адресов, не перечисленных в таблице, будет разрешено обращаться к P-2602. Выберите **Allow**, чтобы разрешить доступ к P-2602. С MAC-адресов, не перечисленных в таблице, будет запрещено обращаться к P-2602.
Запрос Set	В этом поле отображается порядковый номер MAC-адреса.
MAC Address	Введите MAC-адреса станций беспроводной сети, которым разрешен или запрещен доступ к P-2602. Введите MAC-адреса в правильном формате MAC-адреса, то есть, шесть шестнадцатеричных пар символов, например, 12:34:56:78:9a:bc.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-2602.
Cancel	Чтобы возвратить настройки на этом экране в их прежнее состояние, нажмите **Cancel**.

9.8 Экран QoS

Экран QoS по умолчанию позволяет автоматически назначать приоритет услуге.

Выберите **Network > Wireless LAN** > **QoS**. Появится изображенный ниже экран.

Рис. 75 Беспроводная сеть: QoS



Поля изображённого выше экрана описаны в следующей таблице.

Таб. 44 Беспроводная сеть: QoS

ПОЛЕ	ОПИСАНИЕ
QoS Setup	
Enable WMM QoS	Отметьте этот флажок, чтобы активировать WMM QoS в P-2602.
WMM QoS Policy	Выберите **Default**, чтобы устройство P-2602 автоматически присваивало сетевой службе уровень приоритета в соответствии со значением ToS в IP-заголовках отправлямых пакетов. Выберите **Application Priority** из раскрывающегося списка, чтобы просмотреть таблицу названий приложений, служб, портов и приоритетов, к которым может применяться WMM QoS.
	Эта таблица появляется только в том случае, если в поле **WMM QoS Policy** выбрано **Application Priority**.
#	В этом поле отображается номер записи в таблице приложений.
Name	В этом поле отображается описание записи в таблице приложений.
Service	В этом поле отображается тип службы, к которой применяется WMM QoS: **FTP**, **WWW**, **E-mail** или **User Defined** (служба, настроенная пользователем).
Dest Port	В этом поле отображается номер порта, на который приложение передает трафик.

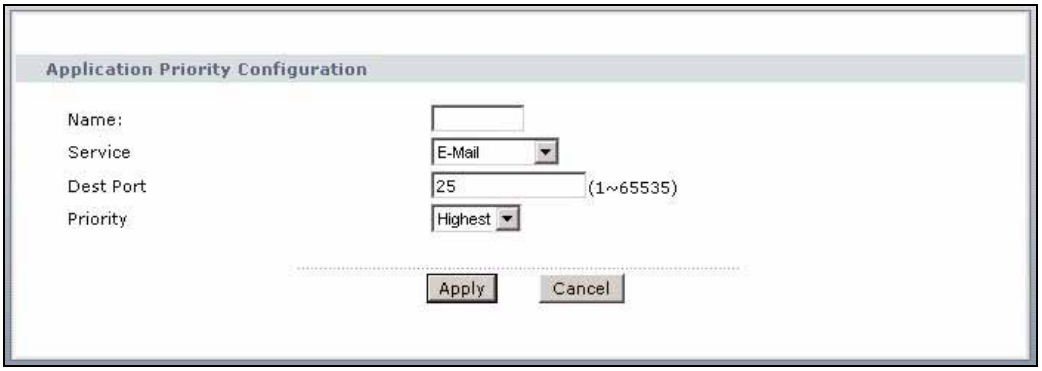
Таб. 44 Беспроводная сеть: QoS

ПОЛЕ	ОПИСАНИЕ
Priority	Выберите приоритет приложения. **Highest** – наивысший приоритет, обычно используемый для голосовых и видеоданных со строгими требованиями к качеству. **High** – высокий приоритет, обычно применяется для голосовых и видеоданных, для которых допускается среднее качество. **Mid** - средний приоритет, обычно используемый для приложений, не относящихся к другим уровням приоритета, например, для веб-серфинга. **Low** – низкий приоритет, обычно применяется для некритичных “фоновых” приложений, например, для неконтролируемой передачи данных или печати заданий, наличие которых не должно никоим образом сказываться на других приложениях.
Modify	Перейдите на экран **Application Priority Configuration**, нажав значок **Edit**. Измените существующую запись приложения или создайте новую запись на экране **Application Priority Configuration**. Щелкинте **Remove**, чтобы удалить запись приложения.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-2602.

9.8.1 Экран Application Priority Configuration

Чтобы отредактировать запись с параметрами WMM QoS для приложения, щелкните на значке редактирования под заголовком **Modify**. Появится изображенный ниже экран.

Рис. 76 Экран Application Priority Configuration



Перечень часто используемых типов служб и входных портов см. в прилож.31 на стр. 403. Поля изображённого выше экрана описаны в следующей таблице.

Таб. 45 Экран Application Priority Configuration

ПОЛЕ	ОПИСАНИЕ
Application Priority Configuration	
Name	Введите описание приоритета приложения.

Таб. 45 Экран Application Priority Configuration

ПОЛЕ	ОПИСАНИЕ
Service	Ниже описаны приложения, для которых могут применяться приоритеты WMM QoS. Выберите сетевую службу из раскрывающегося списка. • **FTP** Протокол передачи файлов используется для пересылки файлов, в особенности – больших объемов данных, которые невозможно передать по электронной почте. Для FTP используется порт 21. • **E-Mail** Электронная почта состоит из сообщений, рассылаемых по компьютерной сети определенным группам или людям. По умолчанию для электронной почты часто используются следующие порты: POP3 - порт 110 IMAP - порт 143 SMTP – порт 25 HTTP - порт 80 • **WWW** WWW (“веб”, “Всемирная паутина”) – это интернет-система для распространения графической информации с гиперссылками по протоколу передачи гипертекста (HTTP) - клиент-серверному протоколу WWW. Название “Всемирная паутина” не является синонимом Интернета и обозначает только одну из сетевых служб в Интернете. Среди других служб Интернета – чат в реальном времени (IRC) и группы новостей (NNTP). Обращение к WWW осуществляется посредством веб-браузера. • **User-Defined** Пользователь может задавать собственные сетевые службы, указывая соответствующие им порты и приложения.
Dest Port	В этом поле отображается список портов, используемых выбранной службой. Введите номер порта в предоставленном поле, если вы хотите по умолчанию использовать другой порт.
Priority	Выберите приоритет из раскрывающегося списка.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-2602.
Cancel	Для возврата к предыдущему экрану нажмите кнопку **Cancel**.

Глава 10
Экраны трансляции сетевых адресов (NAT)

В этой главе поясняется способ настройки NAT в P-2602.

10.1 Краткий обзор NAT

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

10.1.1 Определения NAT

Термины "внешний" и "внутренний" определяют положение хоста относительно P-2602, например, компьютеры абонентов - это внутренние хосты, а веб-серверы в Интернете являются внешними хостами.

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

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

Таб. 46 Определения, относящиеся к NAT

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

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

10.1.2 Назначение NAT

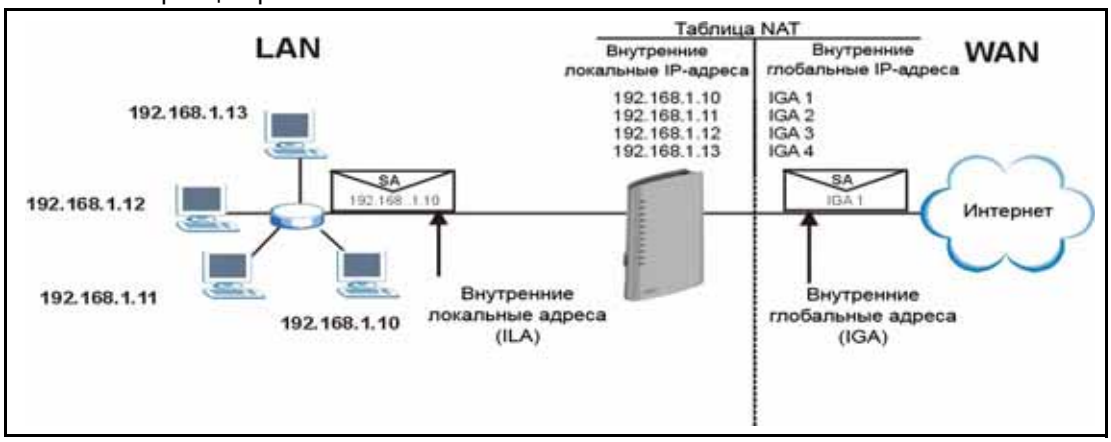
В самой простой форме NAT заменяет исходный IP-адрес в пакете, полученном от абонента (внутреннего локального адреса), на другой адрес (внутренний глобальный адрес) перед отправлением пакета на сторону WAN. Когда ответ возвращается, NAT преобразовывает адрес получателя (внутренний глобальный адрес) обратно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

Глобальные IP-адреса для внутренних хостов могут назначаться ISP статически или динамически. Кроме того, можно определять серверы (например, веб-сервер и telnet-сервер) в локальной сети и делать их доступными для внешнего мира. Если серверы не определены (для схем трансляции “многие к одному” и “многие ко многим с перегрузкой” – см. таб. 47 на стр. 156), NAT обеспечивает дополнительную защиту, играя роль сетевого экрана. Если серверы не определены, P-2602 отфильтровывает все поступающие запросы, таким образом препятствуя проникновению в сеть злоумышленников. Для получения дополнительной информации о преобразовании IP-адреса обращайтесь к *RFC 1631*, *Преобразователь IP- адресов сети (NAT)*.

10.1.3 Принцип работы NAT

Каждый пакет имеет два адреса – адрес источника и адрес получателя. Для исходящих пакетов ILA (Внутренний локальный адрес) – исходный адрес в LAN, а IGA (Внутренний глобальный адрес) – исходный адрес в WAN. Для поступающих пакетов ILA - адрес места назначения в LAN, а IGA - в WAN. NAT привязывает частные (локальные) IP-адреса к глобальным уникальным, требуемым для обмена данными с хостами в других сетях. В каждом пакете заменяется исходный IP-адрес (а в режимах “многие к одному” и “многие ко многим с перегрузкой” – также и номер исходного порта TCP/UDP), после чего пакет пересылается в Интернет. P-2602 отслеживает оригинальные адреса и номера портов, чтобы в поступающих ответных пакетах восстанавливались исходные значения. Это проиллюстрировано на следующем рисунке.

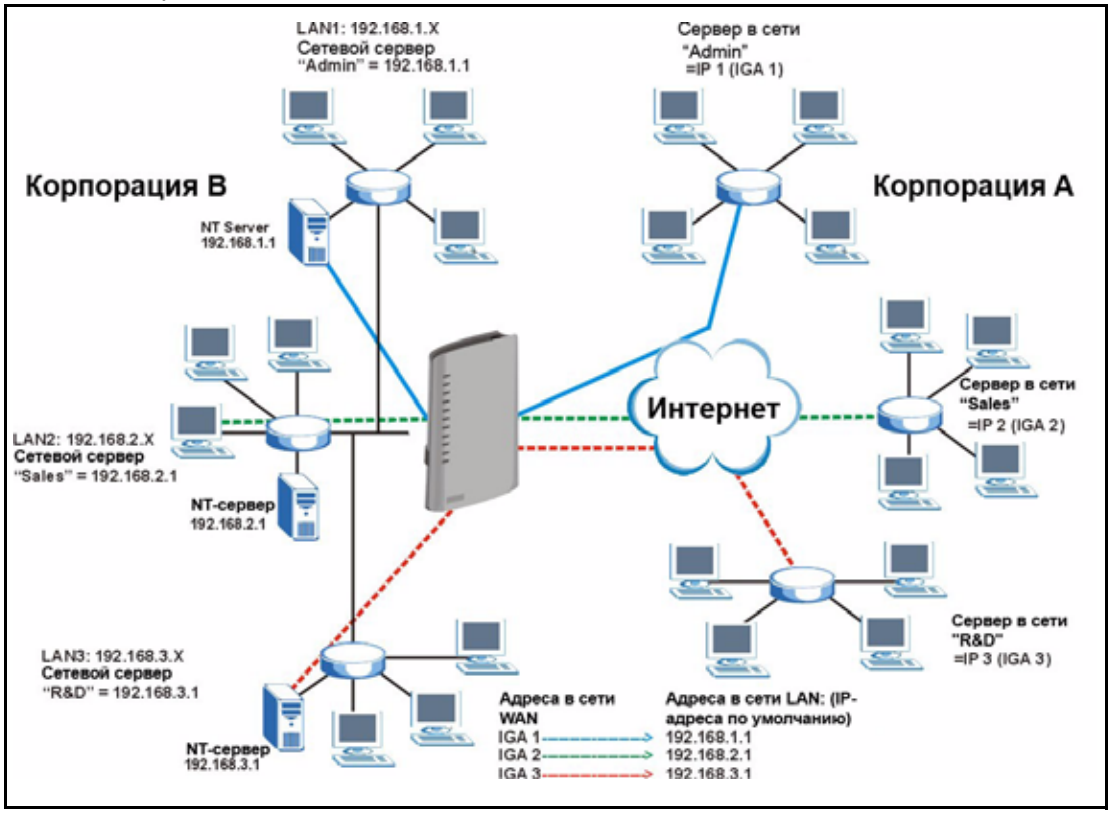
Рис. 77 Принцип работы NAT



10.1.4 Применение NAT

На следующем рисунке иллюстрируется возможное применение NAT, в котором три внутренние сети LAN (логические LAN, использующие совмещение IP-адресов) за P-2602 могут обмениваться данными с тремя раздельными сетями WAN.

Рис. 78 Применение NAT с IP-псевдонимом



10.1.5 Типы привязки NAT

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

- **Один - один**: В режиме “один к одному” P-2602 привязывает один локальный IP-адрес к одному глобальному IP-адресу.
- **Многие к одному**: в режиме “многие к одному” P-2602 привязывает несколько локальных IP-адресов к одному глобальному IP-адресу. Этот режим эквивалентен режиму SUA (Single User Account), использовавшемуся в прежних маршрутизаторах ZyXEL (в текущих моделях ему соответствует параметр **SUA Only**). Фактически данный режим представляет собой PAT – трансляцию адресов портов.
- **Многие ко многим с перегрузкой**: в режиме “многие ко многим с перегрузкой” P-2602 привязывает несколько локальных IP-адресов к общим глобальным IP-адресам.
- **Многие ко многим без перегрузки**: в режиме “многие ко многим без перегрузки” P-2602 привязывает каждый локальный IP-адрес к уникальному глобальному IP-адресу.
- **Server (Сервер)**: Этот тип позволяет указывать внутренние серверы различных служб в NAT, которые должны быть доступными для внешнего мира.

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

В следующей таблице дается сводная информация об этих типах.

Таб. 47 Типы привязки NAT

ТИП	ПРИВЯЗКА IP
One-to-One (один к одному)	ILA1←→ IGA1
Many-to-One (многие к одному) (SUA/PAT)	ILA1←→ IGA1 ILA2←→ IGA1 …
Many-to-Many Overload (многие ко многим с перегрузкой)	ILA1←→ IGA1 ILA2←→ IGA2 ILA3←→ IGA1 ILA4←→ IGA2 …
Many-to-Many No Overload (многие ко многим без перегрузки)	ILA1←→ IGA1 ILA2←→ IGA2 ILA3←→ IGA3 …
Server (сервер)	Сервер 1 IP←→ IGA1 Сервер 2 IP←→ IGA1 Сервер 3 IP←→ IGA1

10.2 Сравнение SUA (Учетная запись отдельного пользователя) и NAT

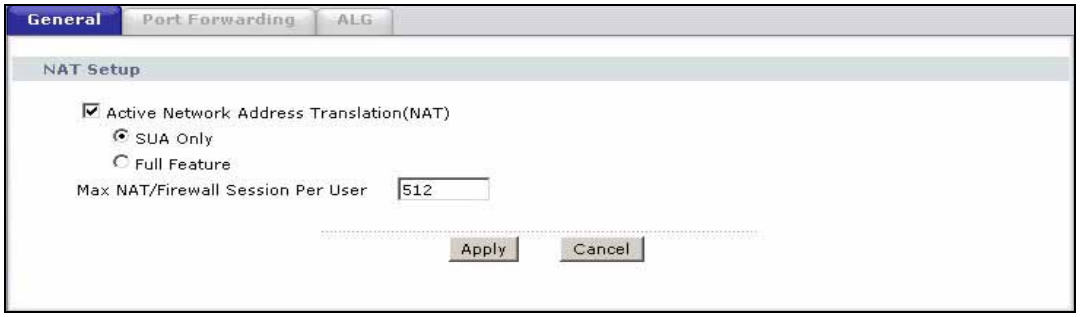
SUA (Single User Account – одна учетная запись) представляет собой подмножество NAT, реализуемое операционной системой ZyNOS и включающее два типа привязки: “**многие к одному**” и “**сервер**”. P-2602 также поддерживает полноценный режим NAT (**Full Feature**), в котором несколько глобальных IP-адресов привязываются к нескольким IP-адресам клиентов или серверов в частных сетях LAN с помощью одного из способов, перечисленных в таб. 47 на стр. 156.

- Если для P-2602 выделен только один глобальный IP-адрес в сети WAN, выберите **SUA Only**.
- Если для P-2602 выделено несколько глобальных IP-адресов в сети WAN, выберите **Full Feature**.

10.3 Общая настройка NAT

Чтобы разрешить пересылку трафика из WAN через P-2602, в дополнение к настройке SUA/NAT необходимо создать правило для сетевого экрана. Выберите **Network > NAT**, чтобы открыть следующий экран.

Рис. 79 Общие настройки NAT



Поля изображённого выше экрана описаны в следующей таблице.

Таб. 48 Общие настройки NAT

ПОЛЕ	ОПИСАНИЕ
Active Network Address Translation (NAT)	Установите этот флажок, чтобы активировать NAT.
SUA Only	Выберите этот переключатель, если для P-2602 выделен только один глобальный IP-адрес в сети WAN.
Full Feature	Выберите этот переключатель, если для P-2602 выделено несколько глобальных IP-адресов в сети WAN.

Таб. 48 Общие настройки NAT (продолжение)

ПОЛЕ	ОПИСАНИЕ
Max NAT/ Firewall Session Per User	Для компьютеров, работающих в одноранговых (P2P) сетях, например, в файлообменных сетях, необходимо устанавливать сеансы через NAT. В отсутствие ограничения на число сеансов NAT, открываемых одним клиентом, все сеансы NAT могут оказаться исчерпаны. В этом случае невозможно установить новые сеансы NAT, и пользователи не могут выходить в Интернете. Для каждого сеанса NAT устанавливается соответствующий сеанс сетевого экрана. Это поле позволяет ограничить число сеансов NAT/сетевого экрана, открываемых клиентскими компьютерами в P-2602. Если в вашей сети P2P-приложениями пользуется мало клиентов, можно увеличить это значение, чтобы ограничение числа устанавливаемых сеансов NAT не ухудшало производительность. Если в вашей сети P2P-приложениями пользуется большое число клиентов, можно уменьшить это число, чтобы исключить перерасходование набора сеансов NAT отдельными клиентами.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-2602.
Cancel	Чтобы возвратить настройки на этом экране в их прежнее состояние, нажмите **Cancel**.

10.4 Переадресация портов

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

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

Многие поставщики услуг Интернета для жилого сектора запрещают своим абонентам устанавливать серверы (в частности, веб- и FTP-серверы). Оператор может периодически проверять серверы и приостановить действие учетной записи, если обнаружит какие-нибудь работающие службы в данном местоположении. Для получения дополнительной информации следует обращаться к оператору.

10.4.1 Default Server IP Address

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

Примечание: Если IP-адрес сервера по умолчанию (**Default Server**) не указан, P-2602 будет отбрасывать все пакеты для портов, не указанных на этом экране или в настройке дистанционного управления.

10.4.2 Переадресация портов: сетевые службы и номера портов

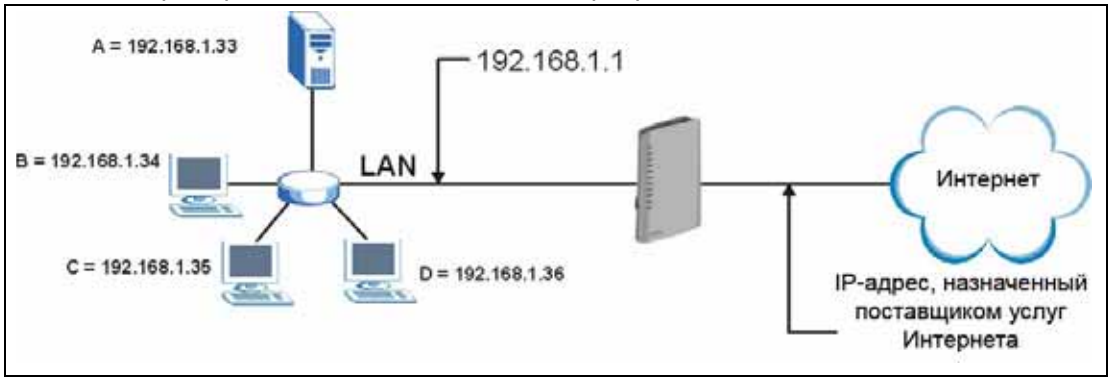
Экран **Port Forwarding** служит для переадресации входящих обращений к сетевым службам на серверы в локальной сети.

Наиболее часто используемые номера портов приведены в прилож. F на стр. 403. Обращайтесь к RFC 1700 для получения дополнительной информации о номерах портов.

10.4.3 Настройка серверов с переадресацией портов (пример)

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

Рис. 80 Пример подключения нескольких серверов к NAT



10.5 Настройка переадресации портов

Примечание: Если IP-адрес сервера по умолчанию (**Default Server**) не указан, P-2602 будет отбрасывать все пакеты для портов, не указанных на этом экране или в настройке дистанционного управления.

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

Номера портов для ряда распространенных сетевых служб см. в прилож. F на стр. 403.

Рис. 81 Переадресация портов

Поля изображённого выше экрана описаны в следующей таблице.

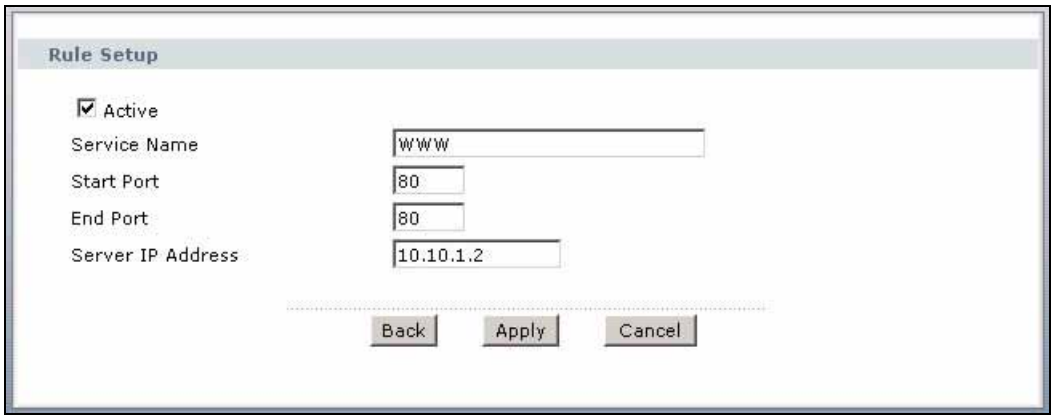
Таб. 49 Переадресация портов

ПОЛЕ	ОПИСАНИЕ
Default Server Setup	
Default Server	В дополнение к серверам для заданных типов сетевых служб NAT поддерживает сервер по умолчанию. Сервер по умолчанию получает пакеты для портов, не указанных на этом экране. Если IP-адрес сервера по умолчанию (**Default Server**) не указан, P-2602 будет отбрасывать все пакеты для портов, не указанных на этом экране или в настройке дистанционного управления.
Port Forwarding	
Service Name	Выберите сетевую службу из раскрывающегося списка.
Server IP Address	Введите IP-адрес сервера для указанной сетевой службы.
Add	Нажмите эту кнопку, чтобы добавить правило в расположенную ниже таблицу.
#	В этом поле отображается порядковый номер правила (только для чтения).
Active	Отметьте этот флажок, чтобы активировать правило.
Service Name	В этом поле отображается название сетевой службы.
Start Port	В этом поле отображается первый номер порта, соответствующий данной службе.
End Port	В этом поле отображается последний номер порта, соответствующий данной службе.
Server IP Address	В этом поле отображается IP-адрес сервера.
Modify	Чтобы перейти на экран для редактирования правила переадресации портов, щелкните на значке редактирования. Для удаления существующего правила переадресации портов щелкните на значке удаления. При удалении одного правила все последующие правила смещаются вверх.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-2602.
Cancel	Нажмите **Cancel**, чтобы вернуться к прежнему состоянию настроек.

10.5.1 Редактирование правил переадресации портов

Чтобы отредактировать правило переадресации портов, щелкните на значке редактирования для соответствующего правила на экране **Port Forwarding**. Появится экран, показанный ниже.

Рис. 82 Редактирование правил переадресации портов



Поля изображённого выше экрана описаны в следующей таблице.

Таб. 50 Настройка правил переадресации портов

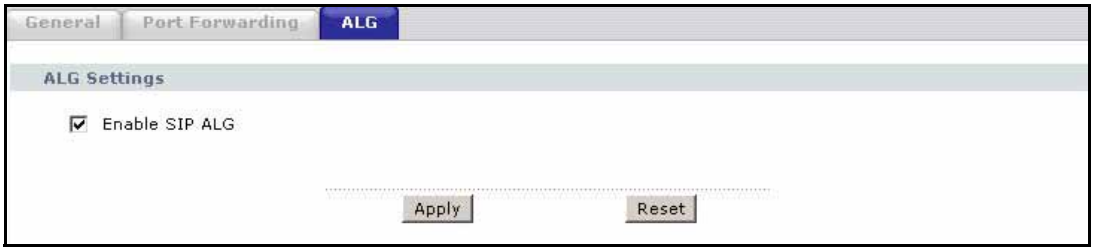
ПОЛЕ	ОПИСАНИЕ
Active	Отметьте этот флажок, чтобы активировать правило.
Service Name	Введите название для идентификации данного правила переадресации портов.
Start Port	Введите номер порта. Если переадресация требуется только для одного порта, введите его номер повторно в поле **End Port**. Чтобы включить переадресацию для диапазона портов, введите в данном поле номер первого порта, а в поле **End Port** – номер последнего порта.
End Port	Введите номер порта. Если переадресация требуется только для одного порта, в поле **Start Port** и в этом поле укажите один и тот же номер порта. Чтобы включить переадресацию для нескольких портов, введите номер последнего порта в диапазоне. Началом диапазона будет порт, введенный выше в поле **Start Port**.
Server IP Address	Здесь вводится внутренний IP-адрес сервера.
Back	Для возврата к предыдущему экрану нажмите кнопку **Back**.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-2602.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

10.5.2 SIP ALG

Некоторые NAT-маршрутизаторы могут поддерживать шлюз для прикладного уровня SIP (SIP ALG). SIP ALG позволяет пропускать вызовы SIP через NAT, проверяя и преобразуя IP-адреса в составе потока данных. Когда P-2602 регистрируется на сервере регистрации SIP, SIP ALG преобразует частный IP-адрес P-2602 в потоке данных в глобальный IP-адрес. Если P-2602 располагается за SIP ALG, использовать STUN или прокси-сервер для исходящих запросов не требуется.

Этот экран позволяет включать и отключать SIP (VoIP) ALG в P-2602. Чтобы перейти на этот экран, выберите **Network > NAT > ALG**.

Рис. 83 Экран Network > NAT > ALG



Каждое поле описано в следующей таблице.

Таб. 51 Экран Network > NAT > ALG

ПОЛЕ	ОПИСАНИЕ
Enable SIP ALG	Выберите этот флажок, если необходима корректная работа SIP (VoIP) с переадресацией портов и правилами привязки адресов.
Apply	Нажмите эту кнопку, чтобы сохранить изменения в P-2602 и ввести их в действие.
Reset	Нажмите эту кнопку, чтобы вернуться к прежнему состоянию настроек.

Глава 11
Голосовая телефонная связь

В этой главе представлены общие сведения о VoIP и SIP, а также поясняется порядок настройки параметров голосовой связи в устройстве.

11.1 Введение в VoIP

VoIP – это пересылка сигналов голосовой телефонной связи с помощью межсетевого протокола (IP). VoIP позволяет делать телефонные звонки и отправлять факсы через Интернет с затратами во много раз меньше, чем при использовании обычных телефонных сетей с коммутацией каналов. Также можно использовать серверы для различных приложений телефонии, таких как АТС и голосовая почта. Услуги IP-телефонии (VoIP) предоставляются поставщиками услуг Интернет-телефонии (ITSP).

Для телефонных сетей с коммутацией каналов требуется полоса пропускания 64 килобита в секунду (кбит/с) в каждом направлении. Благодаря применению особых технологий кодирования голоса со сжатием VoIP позволяет уменьшить требуемую полосу пропускания.

11.2 SIP

Протокол инициации сеанса (SIP) представляет собой протокол прикладного (сигнального) уровня, отвечающий за подготовку, перенастройку и завершение сеансов голосовой связи и мультимедиа-конференций через Интернет.

Сигнальные данные SIP передаются отдельно от среды, в которой обрабатываются сеансы. В одном сеансе для передающей среды и сигналов могут использоваться различные маршруты. SIP обрабатывает телефонные вызовы и обеспечивает взаимодействие с традиционными телефонными сетями с коммутацией каналов.

11.2.1 Идентификаторы, используемые в SIP

Для учетной записи SIP используется идентификатор (также именуемый адресом SIP). В своем полном формате идентификатор SIP называется SIP URI (универсальный идентификатор ресурса). URI, принадлежащий учетной записи SIP, идентифицирует эту учетную запись аналогично тому, как адрес e-mail идентифицирует учетную запись электронной почты. Идентификатор SIP имеет следующий формат: номер_SIP@домен_службы_SIP.

11.2.1.1 Номер SIP

Номер SIP представляет собой часть SIP URI, находящуюся до символа “@”. В номере SIP могут использоваться буквы, как в адресе электронной почты (например, johndoe@your-ITSP.com), или цифры, как в телефонном номере (например, 1122334455@VoIP-provider.com).

11.2.1.2 Домен службы SIP

Имя домена в SIP URI – это домен службы SIP, идентифицирующий поставщика услуг VoIP. Например, в адресе SIP 1122334455@VoIP-provider.com доменом службы SIP является “VoIP-provider.com”.

11.2.2 Структура вызова с использованием SIP

На следующем рисунке показаны основные этапы подготовки и завершения вызова посредством SIP. “A” вызывает “B”.

Таб. 52 Структура вызова с использованием SIP

A		B
1. INVITE	→	
	←	2. Звонок
	←	3. OK
4. ACK	→	
	5. Диалог (голосовой трафик)	
6. BYE	→	
	←	7. OK

“A” посылает “B” запрос SIP INVITE. Это “приглашение” предлагает “B” подключиться к телефонному вызову по протоколу SIP.

6 “B” направляет отклик, означающий, что телефон звонит.

7 После ответа “B” выдает отклик OK.

8 Затем “A” направляет сообщение ACK, подтверждающее, что “B” ответил на вызов.

9 Затем “A” и “B” обмениваются голосовыми данными (находятся в режиме разговора).

10 По завершении разговора “A” разрывает соединение, направляя запрос BYE.

11 “B” выдает отклик OK, подтверждая получение запроса BYE. Вызов считается завершенным.

11.2.3 Серверы SIP

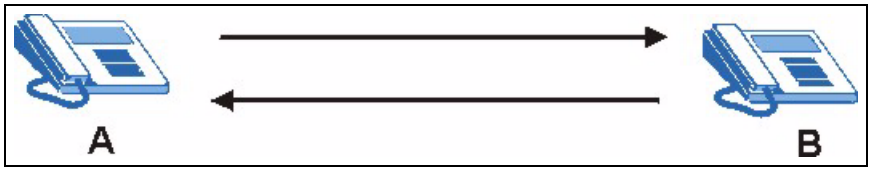
SIP представляет собой протокол “клиент-сервер”. Клиент SIP – это прикладная программа или устройство, отправляющее запросы SIP. Сервер SIP отвечает на запросы SIP.

VoIP-вызов с использованием SIP начинается на стороне клиента и завершается на стороне сервера. Клиентом SIP может являться компьютер или SIP-телефон. Одно устройство может выступать как в качестве клиента, так и в качестве сервера SIP.

11.2.3.1 Пользовательский агент SIP

Пользовательский агент SIP может осуществлять и принимать телефонные вызовы посредством VoIP. Это означает, что SIP может применяться для одноранговой коммуникации, несмотря на то, что он является клиент-серверным протоколом. На следующем рисунке любая из сторон, “A” или “B”, может выступать пользовательским агентом SIP для осуществления вызова. “A” и “B” также могут одновременно являться пользовательскими агентами SIP для приема вызова.

Рис. 84 Пользовательский агент SIP



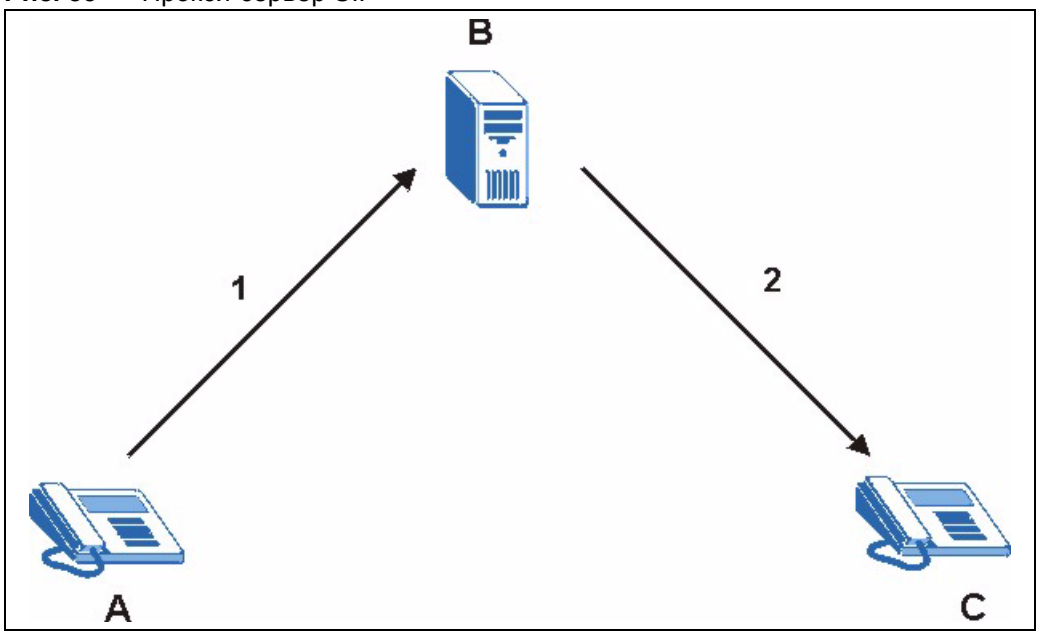
11.2.3.2 Прокси-сервер SIP

Прокси-сервер SIP принимает запросы от клиентов и пересылает их другому серверу.

Для примера предположим, что с клиентского устройства “A” требуется осуществить вызов абонента, использующего клиентское устройство “C”.

1. Клиентское устройство (“A” на рисунке) направляет прокси-серверу SIP (“B”) приглашение на вызов.
2. Прокси-сервер SIP передает приглашение на вызов устройству “C”.

Рис. 85 Прокси-сервер SIP



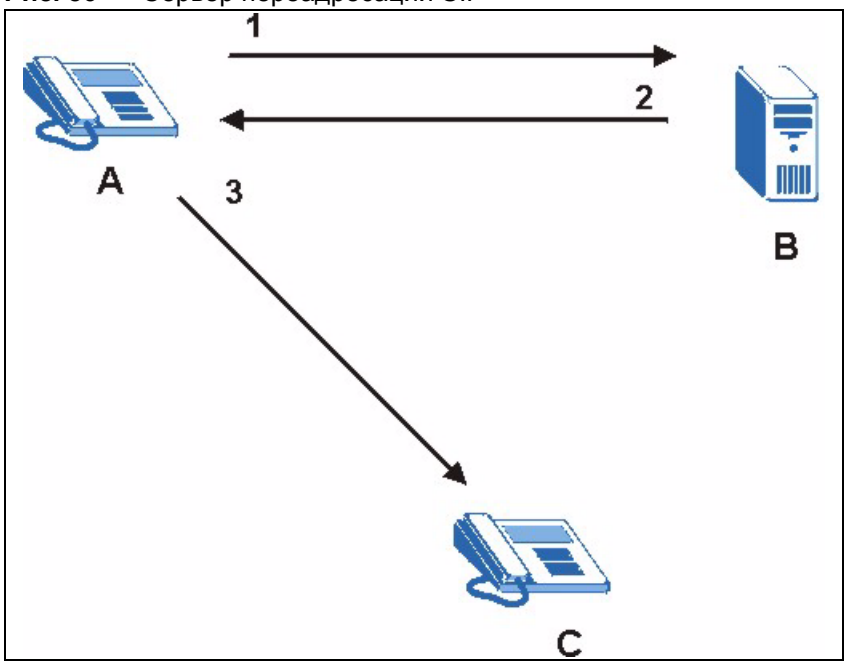
11.2.3.3 Сервер переадресации SIP

Сервер переадресации SIP принимает запросы SIP, преобразует адрес места назначения в IP-адрес и возвращает преобразованный адрес устройству, отправившему запрос. После этого клиентское устройство, отправившее исходный запрос, может направлять запросы на IP-адрес, полученный от сервера переадресации. Сами серверы переадресации не инициируют запросы SIP.

Для примера предположим, что с клиентского устройства “A” требуется осуществить вызов абонента, использующего клиентское устройство “C”.

1. Клиентское устройство “A” отправляет приглашение на вызов устройства “C” серверу переадресации SIP (“B”).
2. Сервер переадресации SIP возвращает приглашение устройству “A” с IP-адресом (или доменным именем) устройства “C”.
3. Затем клиентское устройство “A” направляет приглашение на вызов клиентскому устройству “C”.

Рис. 86 Сервер переадресации SIP



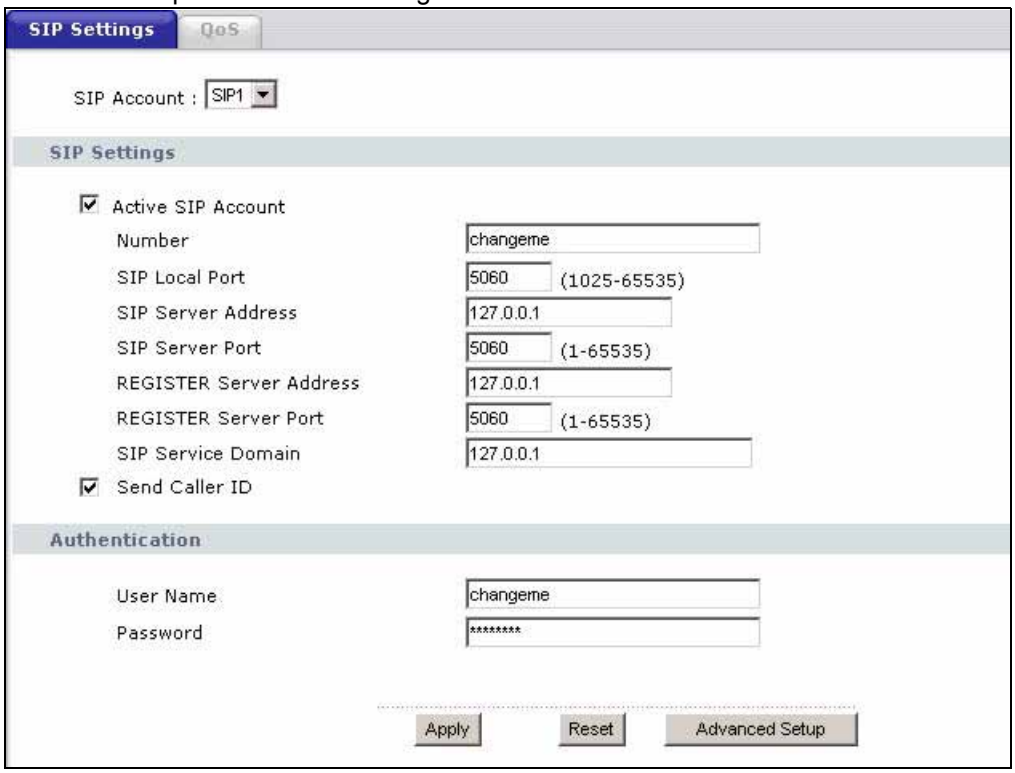
11.2.3.4 Сервер регистрации SIP

Сервер регистрации SIP ведет базу данных с привязкой идентификаторов SIP к IP-адресам или доменным именам. Когда вы регистрируетесь, сервер регистрации проверяет ваше имя пользователя и пароль.

11.3 Экран SIP Settings

Этот экран служит для управления основными параметрами отдельных учетных записей SIP. Он также позволяет активировать или деактивировать каждую учетную запись. Чтобы перейти на этот экран, выберите **VoIP > SIP > SIP Settings**.

Рис. 87 Экран SIP > SIP Settings



Каждое поле описано в следующей таблице.

Таб. 53 Экран SIP > SIP Settings

ПОЛЕ	ОПИСАНИЕ
SIP Account	Выберите учетную запись SIP для просмотра на этом экране. При изменении этого поля содержимое экрана автоматически обновляется.
SIP Settings	
Active SIP Account	Отметьте этот флажок, чтобы использовать данную учетную запись в P-2602. Снимите флажок, если необходимо, чтобы отключить использование данной учетной записи в P-2602.
Number	Введите ваш номер SIP. Это часть полного идентификатора SIP URI до знака “@”. Допустимая длина – до 127 печатных знаков ASCII.
SIP Local Port	Если ваш поставщик услуг VoIP сообщил вам номер входного порта, введите номер порта, который будет открыт на P-2602. В противном случае следует оставить значение по умолчанию.
SIP Server Address	Введите IP-адрес или доменное имя сервера SIP, сообщенное поставщиком услуг VoIP. Допустимая длина – до 95 печатных знаков ASCII. Не имеет значения, является ли указанный сервер прокси-сервером, сервером переадресации или сервером регистрации.
SIP Server Port	Если ваш поставщик услуг VoIP сообщил вам номер входного порта, введите номер порта, открытого на сервере SIP. В противном случае следует оставить значение по умолчанию.
REGISTER Server Address	Введите IP-адрес или доменное имя сервера регистрации SIP, сообщенное поставщиком услуг VoIP. Если поставщик услуг не указал адрес сервера, введите тот же адрес, что и в поле **SIP Server Address**. Допустимая длина – до 95 печатных знаков ASCII.

Таб. 53 Экран SIP > SIP Settings

ПОЛЕ	ОПИСАНИЕ
REGISTER Server Port	Если поставщик услуг VoIP сообщил вам номер входного порта на сервере регистрации SIP, введите этот номер. В противном случае введите тот же номер порта, что и в поле **SIP Server Port**.
SIP Service Domain	Введите имя домена, в котором находится служба SIP. В полном идентификаторе SIP URI имя домена находится после знака “@”. Допустимая длина – до 127 печатных знаков расширенного набора ASCII.
Send Caller ID	Отметьте этот флажок, чтобы разрешить передачу идентификационных данных при исходящих вызовах VoIP. Снимите флажок, чтобы запретить передачу идентификационных данных.
Authentication	
User Name	Введите имя пользователя для регистрации данной учетной записи SIP. Имя пользователя должно быть введено в точности так, как оно было вам сообщено. Допустимая длина – до 95 печатных знаков ASCII.
Password	Введите пароль для регистрации данной учетной записи SIP. Пароль должен быть введен в точности так, как он был вам сообщен. Допустимая длина – до 95 печатных знаков расширенного набора ASCII.
Apply	Нажмите эту кнопку, чтобы сохранить изменения в P-2602 и ввести их в действие.
Cancel	Нажмите эту кнопку, чтобы возвратить все поля на этом экране к последним сохраненным значениям.
Advanced Setup	Нажмите эту кнопку, чтобы отредактировать специальные настройки для данной учетной записи SIP. Появится экран расширенной настройки SIP (**Advanced SIP Setup**).

11.3.1 RTP

В вызовах VoIP, осуществляемых посредством SIP, передача голосовых данных осуществляется по протоколу RTP (Real time Transport Protocol – транспортный протокол для режима реального времени). Подробное описание RTP см. в документе RFC 1889.

11.4 Импульсно-кодовая модуляция

Импульсно-кодовая модуляция (ИКМ, PCM) реализуется путем измерения амплитуды аналогового сигнала с регулярными интервалами и преобразования измеренных значений в битовые последовательности.

11.5 Кодирование речи

Кодек (кодер-декодер) кодирует аналоговые сигналы голосовой связи в цифровые сигналы, а также декодирует цифровые сигналы обратно в аналоговые. P-2602 поддерживает следующие кодеки.

11.5.1 G.711

G.711 представляет собой кодек формы сигнала на основе импульсно-кодовой модуляции (ИКМ). G.711 обеспечивает очень высокое качество звука, но требует полосы пропускания не менее 64 кбит/с.

11.5.2 G.729

G.729 представляет собой гибридный кодек формы сигнала, реализующий метод анализа через синтез (AbS). В этом кодеке используется фильтр, учитывающий свойства речевого тракта человека. G.729 обеспечивает высокое качество звука, одновременно позволяя уменьшить требуемую полосу пропускания до 8 кбит/с.

11.6 Сигналы, используемые для вызовов в ТфОП

При двухтональном многочастотном (DTMF) способе кодирования сигналов для осуществления вызовов используется совокупность двух частот (низкой и высокой). Этот способ также именуется Touch Tone®. Каждая кнопка на DTMF-телефоне соответствует различной паре частот.

При импульсном наборе номера на местную АТС подается последовательность коротких импульсов (щелчков).[1]

11.7 MWI (индикация наличия сообщений)

Функцию индикации наличия сообщений (MWI) можно использовать для того, чтобы телефон оповещал о поступивших голосовых сообщениях с помощью звукового сигнала. Система обмена сообщениями, используемая вашим поставщиком услуг VoIP, должна поддерживать отправку пакетов SIP о состоянии ожидания сообщений согласно стандарту RFC 3842.

1. На момент подготовки настоящего документа P-2602 не поддерживает импульсный набор.

11.8 Индивидуальная настройка сигналов (IVR)

Функция IVR (Interactive Voice Response интерактивный голосовой ответ) обеспечивает управление устройством P-2602 с помощью телефона. P-2602 позволяет записать собственные звуковые сигналы для функций входящего звонка (**Caller Ringing Tone**) и ожидания (**On Hold Tone**). Записанные сигналы будут применяться для входящих звонков и режима ожидания.

Таб. 54 Параметры настройки собственных сигналов

ПАРАМЕТР	ОПИСАНИЕ
Суммарная длительность всех сигналов	120 секунд в сумме для всех самостоятельно записанных сигналов.
Продолжительность одного сигнала	20 секунд.
Общее допустимое число записываемых сигналов	Десять Можно записать до десяти собственных сигналов общей длительностью не более 120 секунд. Например, можно записать до десяти 12-секундных сигналов или до шести 20-секундных сигналов.

11.8.0.1 Запись собственных сигналов

Для создания новых или изменения существующих сигналов выполните следующие действия:

1. Снимите на телефоне трубку и наберите на клавиатуре телефона последовательность “****”. Дождитесь сообщения о том, что вы вошли в меню настройки.
2. Наберите номер в диапазоне 1101~1108 и нажмите кнопку “#”.
3. Через микрофон телефонной трубки запишите необходимую мелодию или сообщение. Нажмите кнопку “#”.
4. Завершив настройку, можно продолжить работу с записанными сигналами (добавление, прослушивание и удаление), либо повесить трубку.

11.8.0.2 Прослушивание собственных сигналов

Для прослушивания ранее записанного сигнала выполните следующие действия:

1. Снимите на телефоне трубку и наберите на клавиатуре телефона последовательность “****”. Дождитесь сообщения о том, что вы вошли в меню настройки.
2. Чтобы прослушать записанный сигнал, наберите номер в диапазоне 1201~1208 и нажмите кнопку “#”.
3. Завершив настройку, можно продолжить работу с записанными сигналами (добавление, прослушивание и удаление), либо повесить трубку.

11.8.0.3 Удаление собственных сигналов

Для удаления записанного сигнала выполните следующие действия:

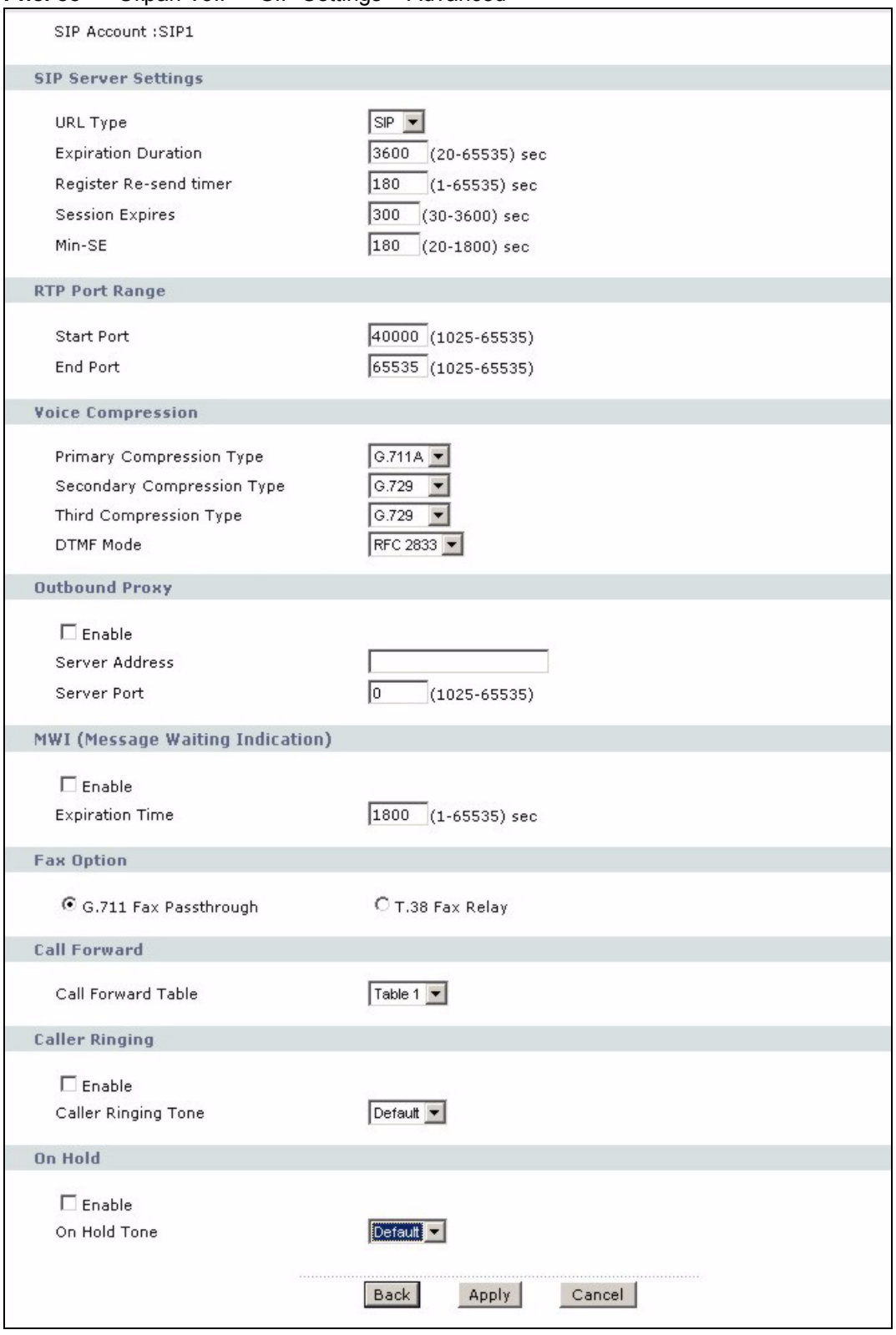
1. Снимите на телефоне трубку и наберите на клавиатуре телефона последовательность “****”. Дождитесь сообщения о том, что вы вошли в меню настройки.
2. Чтобы удалить соответствующий сигнал, наберите номер в диапазоне 1301~1308 и нажмите кнопку “#”. Чтобы удалить все записанные сигналы, наберите 14 и нажмите кнопку “#”.

Завершив настройку, можно продолжить работу с записанными сигналами (добавление, прослушивание и удаление), либо повесить трубку.

11.9 Экран расширенной настройки SIP

Вызовите экран **SIP Settings** , выбрав **VoIP > SIP > SIP Settings**. Чтобы открыть экран **Advanced Setup**, выберите учетную запись SIP и нажмите **Advanced SIP Setup** . Этот экран служит для управления дополнительными параметрами учетной записи SIP.

Рис. 88 Экран VoIP > SIP Settings > Advanced



Каждое поле описано в следующей таблице.

Таб. 55 Экран VoIP > SIP Settings > Advanced

ПОЛЕ	ОПИСАНИЕ
SIP Account	В этом поле отображается наименование учетной записи SIP, просматриваемой на данном экране.
SIP Server Settings	
URL Type	Выберите, должно ли имя домена службы SIP включаться в номер SIP, отправляемый устройством P-2602. **SIP** – включать имя домена службы SIP. **TEL** – не включать имя домена службы SIP.
Expiration Duration	Введите число секунд, по истечении которого запись, зарегистрированная на сервере регистрации SIP, удаляется. По истечении этого времени P-2602 автоматически попытается повторно зарегистрировать учетную запись SIP. (На сервере регистрации SIP может быть настроен другой интервал истечения учетных записей.)
Register Re-send timer	Введите длительность паузы (в секундах), которую P-2602 будет выдерживать перед повторной регистрацией учетной записи SIP, если предыдущая попытка окажется неудачной или не будет получен отклик.
Session Expires	Введите число секунд, в течение которого P-2602 позволит сеансу SIP находиться в режиме простоя (без обмена данными), прежде чем сеанс будет автоматически разъединен.
Min-SE	Введите число секунд, в течение которого P-2602 позволит сеансу SIP находиться в режиме простоя (без обмена данными), прежде чем сеанс будет автоматически разъединен. Устанавливая сеанс SIP, оба устройства должны согласовать время истечения неактивных сеансов. Это поле задает минимальное время истечения, которое может быть принято P-2602.
RTP Port Range	
Start Port End Port	Если ваш поставщик услуг VoIP сообщил вам номер входного порта для RTP-трафика, введите этот номер. В противном случае следует оставить значения по умолчанию. Чтобы указать один номер порта, введите один и тот же номер в полях **Start Port** и **End Port**. Чтобы ввести диапазон номеров портов, • введите номер первого порта в поле **Start Port**. • введите номер последнего порта в поле **End Port**.
Voice Compression	Выберите тип речевого кодека (кодера-декодера), который будет использоваться P-2602. G.711 обеспечивает более высокое качество речи, но требует большей полосы пропускания (64 кбит/с). • В Европе обычно применяется **G.711A**. • В североамериканских странах и Японии обычно применяется **G.711u**. Отличием кодека **G.729** является то, что ему достаточно полосы 8 кбит/с. Типы кодеков, используемые P-2602 и удаленной стороной, должны совпадать. Устанавливая сеанс SIP, оба устройства должны согласовать тип кодека.
Primary Compression Type	Выберите предпочтительный тип речевого кодека для P-2602, который будет использоваться в первую очередь.
Secondary Compression Type	Выберите тип кодека, который будет использоваться P-2602 во вторую очередь. Чтобы разрешить устройству P-2602 использовать только первый выбранный кодек, выберите **None**.

Таб. 55 Экран VoIP > SIP Settings > Advanced

ПОЛЕ	ОПИСАНИЕ
Third Compression Type	Выберите тип речевого кодека, который будет использоваться P-2602 в третью очередь. Чтобы разрешить устройству P-2602 использовать только первый или второй выбранный кодек, выберите **None**.
DTMF Mode	Этот параметр определяет, как P-2602 будет обрабатывать тональные сигналы, генерируемые при нажатии кнопок на телефоне. Необходимо выбрать тот режим, который используется поставщиком услуг VoIP. **RFC 2833** - DTMF-сигналы передаются в пакетах RTP. **PCM** - DTMF-сигналы передаются в потоке голосовых данных. Этот метод наиболее целесообразен, если выбранный кодек не использует сжатие (как G.711). Кодеки, использующие сжатие (например, G.729) могут искажать тональные сигналы. **SIP INFO** - DTMF-сигналы передаются в сообщениях SIP.
Outbound Proxy	
Active	Выберите этот вариант, если ваш поставщик услуг VoIP имеет исходящий SIP-сервер для обработки голосовых вызовов. Это позволяет P-2602 работать с любым типом NAT-маршрутизатора и устранять потребность в STUN или SIP ALG. Во всех NAT-маршрутизаторах, расположенных перед P-2602, необходимо отключить SIP ALG, чтобы эти устройства не преобразовывали IP-адрес (уже обработанный исходящим прокси-сервером).
Server Address	Введите IP-адрес или доменное имя сервера исходящего прокси-сервера SIP.
Server Port	Если ваш поставщик услуг VoIP сообщил вам номер входного порта на исходящем сервере SIP, введите этот номер. В противном случае следует оставить значение по умолчанию.
MWI (Message Waiting Indication)	
Enable	Функцию индикации наличия сообщений (MWI) можно использовать для того, чтобы телефон оповещал о поступивших голосовых сообщениях с помощью звукового сигнала. Ваш поставщик услуг VoIP должен поддерживать эту функцию.
Expiration Time	Оставьте значение по умолчанию, если от поставщика услуг VoIP не поступало указаний его изменить. Введите число секунд, в течение которого сервер SIP будет предоставлять службу ожидания сообщений при каждом подключении к ней устройства P-2602. До истечения этого времени P-2602 произведет автоматическое переподключение.
Fax Option	Это поле определяет режим работы P-2602 с факсимильными сообщениями.
G.711 Fax Passthrough	Выберите этот параметр, чтобы устройство P-2602 использовало для пересылки факсов протокол G.711. Устройства на удаленной стороне также должны использовать G.711.
T.38 Fax Relay	Выберите этот параметр, чтобы устройство P-2602 отправляло факсы через IP-сеть в виде пакетов UDP или TCP. Это обеспечивает лучшее качество, но может привести к проблемам с совместимостью. Устройства на удаленной стороне также должны использовать T.38.
Call Forward	
Call Forward Table	Выберите таблицу переадресации вызовов, которую требуется P-2602 использовать для входящих вызовов. Эти таблицы настраиваются на экране **VoIP > Phone Book > Incoming Call Policy**.
Caller Ringing	

Таб. 55 Экран VoIP > SIP Settings > Advanced

ПОЛЕ	ОПИСАНИЕ
Enable	Установите флажок, чтобы выбрать тональный сигнал, который будет выдаваться звонящим абонентам. В P-2602 предусмотрен сигнал по умолчанию, но можно добавить дополнительные сигналы с помощью IVR. Дополнительные сведения см. в разд. 11.8 на стр. 171.
Caller Ringing Tone	Выберите сигнал, который будет слышать звонящий вам абонент. Эти сигналы необходимо предварительно настроить с помощью IVR. Подробности см. в разд. 11.8 на стр. 171.
On Hold	
Enable	Установите флажок, чтобы выбрать тональный сигнал, который будет выдаваться в линию при помещении вызова в режим ожидания. В P-2602 предусмотрен сигнал по умолчанию, но можно добавить дополнительные сигналы с помощью IVR. Дополнительные сведения см. в разд. 11.8 на стр. 171.
On Hold Tone	Выберите сигнал, который будет слышать абонент, переведенный в режим ожидания. Эти сигналы необходимо предварительно настроить с помощью IVR. Дополнительные сведения см. в разд. 11.8 на стр. 171.
Back	Нажмите эту кнопку, чтобы возвратиться на экран **SIP Settings** без сохранения изменений.
Apply	Нажмите эту кнопку, чтобы сохранить изменения в P-2602 и ввести их в действие.
Cancel	Нажмите эту кнопку, чтобы возвратить все поля на этом экране к последним сохраненным значениям.

11.10 Качество обслуживания (QoS)

Понятие “качество обслуживания” (QoS) характеризует способность самой сети передавать данные с минимальной задержкой, а также обозначает способы организации сети, обеспечивающие требуемую ширину полосы пропускания для мультимедиа-приложений реального времени.

11.10.1 Тип службы (ToS)

Для классификации сетевого трафика в источнике данных (например, в P-2602) могут быть заданы значения ToS (Type Of Service – тип службы), на основании которых сервер может принимать решение о наилучшем способе доставки, т.е. наименьшей стоимости, кратчайшем маршруте и т.п.

11.10.2 DiffServ

DiffServ - это модель классов обслуживания (CoS), в которой пакеты снабжаются специальными маркерами. В каждой точке маршрута через сеть с поддержкой DiffServ такие пакеты могут обрабатываться по особым правилам. Пакеты помечаются числовыми кодами DiffServ (DSCP), которые указывают требуемый уровень обслуживания. Это позволяет промежуточным сетевым устройствам, поддерживающим

DiffServ, реализовывать индивидуальную обработку пакетов по числовым кодам, не согласовывая маршруты и не запоминая информацию о состоянии каждого потока. Кроме того, приложениям не требуется запрашивать особый способ обслуживания или заранее уведомлять промежуточные узлы о направлении трафика.[1]

11.10.2.1 DSCP и индивидуальная обработка в каждой точке маршрута

DiffServ предусматривает новое поле DS (Differentiated Services – дифференциация служб), заменяющее поле “тип службы” (ToS) в заголовке IP. Поле DS содержит двухбитовое неиспользуемое поле и шестибитовое поле 6-bit DSCP, позволяющее определить до 64 уровней обслуживания. Структура поля DS приведена на следующем рисунке.

DSCP имеет обратную совместимость с тремя старшими битами в октете ToS, что позволяет несовместимым с DiffServ, но поддерживающим ToS устройствам обрабатывать DSCP без конфликтов.

Рис. 89 DiffServ: поле дифференциации служб

DSCP (6-битовое)	Не используется (2-битовое)

Значение DSCP определяет механизм пересылки PHB (Per-Hop Behavior – индивидуальная обработка в каждой точке маршрута), по которому пакет обрабатывается в сети DiffServ. Правила маркировки задают порядок маркировки различных видов трафика для различных направлений пересылки. После этого ресурсы могут распределяться согласно значениям DSCP и настроенным политикам.

11.10.3 Виртуальная локальная сеть

VLAN (виртуальная локальная вычислительная сеть) позволяет разделить физическую сеть на несколько логических сетей. Взаимодействовать друг с другом могут только станции в составе одной и той же группы.

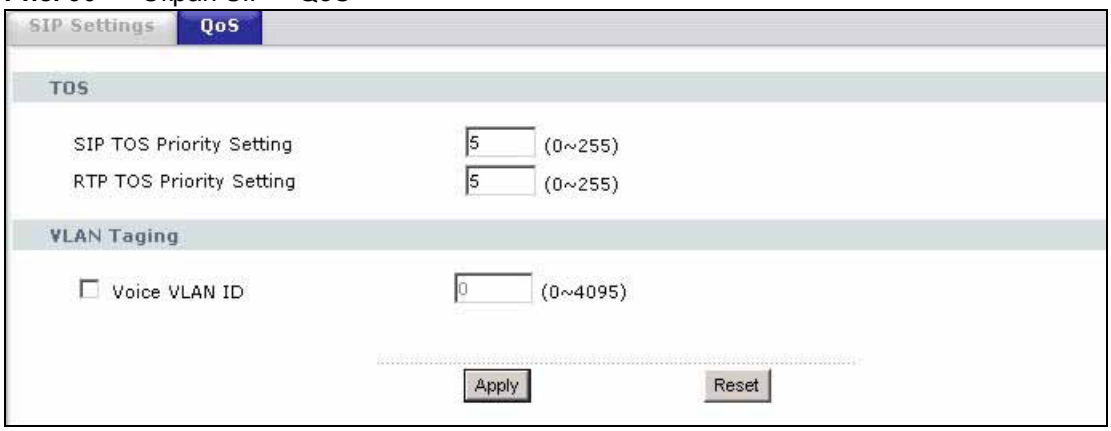
Ваше устройство P-2602 может добавлять маркеры идентификатора VLAN IEEE 802.1Q к речевым кадрам, пересылаемым по сети. Это позволяет P-2602 общаться с сервером SIP, который является участником одной и той же группы VLAN. Некоторые поставщики услуг Интернета используют идентификатор VLAN для обнаружения голосового трафика, которому дается приоритет над обычным трафиком.

11.10.4 Экран SIP QoS

Этот экран служит для управления параметрами ToS и VLAN в P-2602. Чтобы перейти на этот экран, выберите **VoIP > SIP > QoS**.

1. На момент подготовки настоящего документа P-2602 не поддерживает DiffServ.

Рис. 90 Экран SIP > QoS



Каждое поле описано в следующей таблице.

Таб. 56 Экран SIP > QoS

ПОЛЕ	ОПИСАНИЕ
SIP TOS Priority Setting	Введите приоритет для голосового трафика SIP. Для передаваемого голосового трафика P-2602 будет создавать маркеры приоритета ToS с указанным приоритетом.
RTP TOS Priority Setting	Введите приоритет для голосового трафика RTP. Для передаваемого RTP-трафика P-2602 будет создавать маркеры приоритета ToS с указанным приоритетом.
Voice VLAN ID	Отметьте этот флажок, если устройство P-2602 для обмена данными с SIP-сервером должно входить в состав VLAN. Уточнить необходимые настройки можно у системного администратора. В правом поле введите идентификатор VLAN, предоставленный системным администратором. Ваша LAN и шлюз должны быть настроены на использование маркеров VLAN. В противном случае это поле необходимо очистить.
Apply	Нажмите эту кнопку, чтобы сохранить изменения в P-2602 и ввести их в действие.
Cancel	Нажмите эту кнопку, чтобы возвратить все поля на этом экране к последним сохраненным значениям.

11.11 Телефон

Для каждого телефонного порта P-2602 можно по отдельности настроить громкость, подавление эха и параметры VAD (обнаружения пауз). Можно также выбрать учетную запись SIP, которая будет использоваться для исходящих вызовов.

11.12 Линия ТфОП (только в моделях с индексом “L”)

Наличие линии для телефонной сети общего пользования (ТфОП) позволяет осуществлять вызовы через обычную коммутируемую телефонную сеть. Для осуществления обычного вызова необходимо набрать префикс. Когда устройство выключено, можно делать вызовы через обычную сеть, не набирая префикс.

Примечание: Когда P-2602 находится в выключенном состоянии, для вызовов можно использовать только порт **PHONE 1**. Запомните, какой из телефонных аппаратов подключен к этому порту, чтобы в экстренных ситуациях было можно им воспользоваться.

На экране **PSTN Line** можно также указать список телефонных номеров, для которых всегда (без набора префикса) будет использоваться обычная телефонная сеть. В этот список рекомендуется внести телефоны экстренных служб (пожарная часть, милиция, скорая помощь).

11.12.1 Обнаружение пауз/подавление тишины

Функция обнаружения пауз (VAD) позволяет контролировать наличие разговора. Она позволяет P-2602 снизить нагрузку на сеть во время вызова за счет исключения пакетов с тишиной, когда разговор на линии отсутствует.

11.12.2 Искусственный фон во время паузы

Когда используется функция VAD, P-2602 генерирует фоновый сигнал в интервалы, когда абонент на удаленном конце не говорит. Этот сигнал сообщает, что линия не разъединена, поскольку полная тишина может быть ошибочно принята за разрыв соединения.

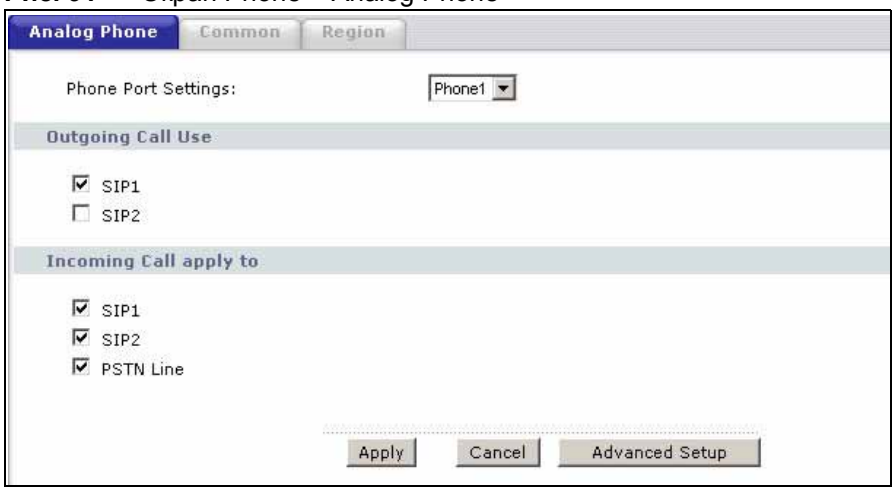
11.12.3 Подавление эха

G.168 – стандарт ITU-T на подавление эха, возникающего в результате реверберации голоса в телефонной трубке во время разговора.

11.13 Экран Analog Phone

Этот экран позволяет выбрать учетные записи SIP и PSTN-линии, используемые каждым телефоном. Чтобы перейти на этот экран, выберите **VoIP > Phone > Analog Phone**.

Рис. 91 Экран Phone > Analog Phone



Каждое поле описано в следующей таблице.

Таб. 57 Экран Phone > Analog Phone

ПОЛЕ	ОПИСАНИЕ
Phone Port Settings	Выберите телефонный порт, настройки которого требуется просмотреть в этом экране. При изменении этого поля содержимое экрана автоматически обновляется.
Outgoing Call Use	
SIP1	Отметьте этот флажок, чтобы при исходящих вызовах через данный телефонный порт использовалась учетная запись SIP1. Если выбраны обе учетные записи SIP, P-2602 сначала попытается использовать SIP2.
SIP2	Отметьте этот флажок, чтобы при исходящих вызовах через данный телефонный порт использовалась учетная запись SIP2. Если выбраны обе учетные записи SIP, P-2602 сначала попытается использовать SIP2.
Incoming Call apply to	
SIP1	Отметьте этот флажок, чтобы для входящих вызовов через данный телефонный порт использовалась учетная запись SIP1. Если для входящих вызовов выбрано несколько источников, различить их во время звонка будет невозможно.
SIP2	Отметьте этот флажок, чтобы для входящих вызовов через данный телефонный порт использовалась учетная запись SIP2. Если для входящих вызовов выбрано несколько источников, различить их во время звонка будет невозможно.

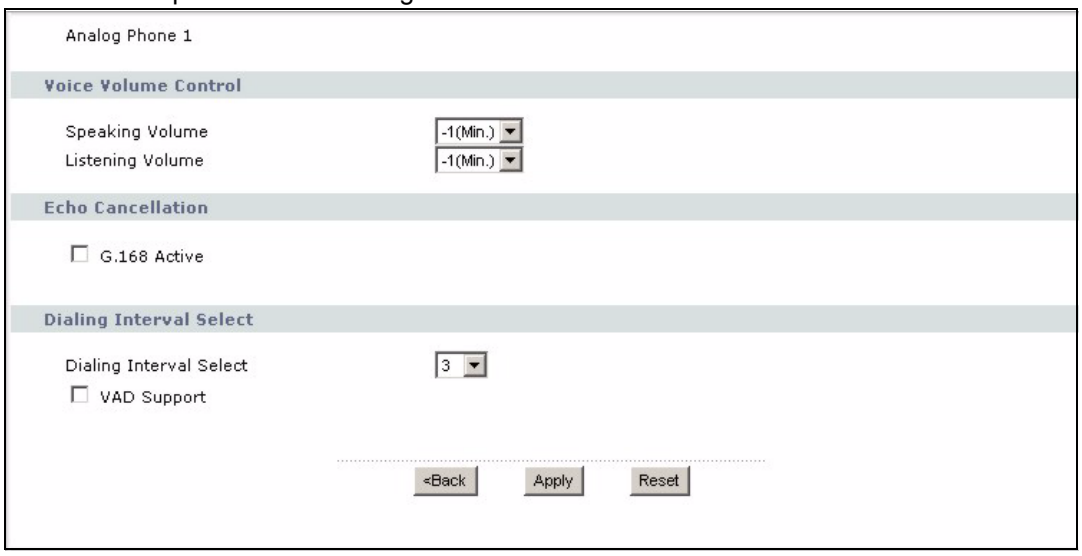
Таб. 57 Экран Phone > Analog Phone

ПОЛЕ	ОПИСАНИЕ
PSTN Line (только в моделях с индексом “L”)	Выберите это значение, чтобы принимать через данный телефонный порт вызовы, осуществляемые по обычной линии ТфОП (не через Интернет). Если для входящих вызовов выбрано несколько источников, различить их во время звонка будет невозможно. **Примечание:** Когда устройство P-2602 находится в выключенном состоянии, независимо от выполненных настроек для вызовов может использоваться только телефон, подключенный к порту **PHONE 1**. Запомните, какой из телефонных аппаратов подключен к этому порту, чтобы в экстренных ситуациях было можно им воспользоваться.
Apply	Нажмите эту кнопку, чтобы сохранить изменения в P-2602 и ввести их в действие.
Cancel	Нажмите эту кнопку, чтобы возвратить все поля на этом экране к последним сохраненным значениям.
Advanced Setup	Щелкните здесь, чтобы изменить расширенные параметры настройки для данного телефонного порта. Появится экран **Advanced Analog Phone Setup**.

11.14 Экран Advanced Analog Phone Setup

Этот экран служит для расширенной настройки отдельных телефонных портов. Чтобы перейти на этот экран, на экране **VoIP > Phone > Analog Phone** выберите **Advanced Setup**.

Рис. 92 Экран Phone > Analog Phone > Advanced



Каждое поле описано в следующей таблице.

Таб. 58 Экран Phone > Analog Phone > Advanced

ПОЛЕ	ОПИСАНИЕ
Analog Phone	В этом поле отображается телефонный порт, выбранный для просмотра на этом экране.
Voice Volume Control	
Speaking Volume	Введите уровень громкости, с которым P-2602 будет отправлять речевые данные удаленной стороне. -1 соответствует наименьшей громкости, а 1 – наибольшей.
Listening Volume	Введите уровень громкости, который P-2602 будет использовать для речевых данных, получаемых от удаленной стороны. -1 соответствует наименьшей громкости, а 1 – наибольшей.
Echo Cancellation	
G.168 Active	Выберите этот флажок, чтобы включить подавление эха, возникающего от реверберации вашего голоса в телефонной трубке во время разговора.
Dialing Interval Select	
Dialing Interval Select	Введите длительность паузы (в секундах), которую P-2602 будет выдерживать после прекращения набора номера, прежде чем осуществлять вызов. Значение зависит от того, как быстро вы можете набирать телефонные номера. Если на экране **VoIP > Phone > Common** выбрано **Active Immediate Dial**, можно немедленно начинать вызов нажатием кнопки “номер” (#), и в этом случае P-2602 не будет учитывать значение данного параметра.
VAD Support	Выберите этот параметр, чтобы P-2602 прекращало передачу данных в те интервалы времени, когда вы не говорите. Это снижает объем трафика, создаваемый P-2602.
Back	Нажмите эту кнопку, чтобы возвратиться на экран **Analog Phone** без сохранения изменений.
Apply	Нажмите эту кнопку, чтобы сохранить изменения в P-2602 и ввести их в действие.
Cancel	Нажмите эту кнопку, чтобы возвратить все поля на этом экране к последним сохраненным значениям.

11.14.1 Экран Common Phone Settings

Этот экран служит для активации и деактивации непосредственного начала вызова. Чтобы перейти на этот экран, выберите **VoIP > Phone > Common**.

Рис. 93 Экран Phone > Common

Каждое поле описано в следующей таблице.

Таб. 59 Экран Phone > Common

ПОЛЕ	ОПИСАНИЕ
Active Immediate Dial	Установите этот флажок, чтобы при нажатии кнопки “номер” (#) устройство P-2602 сразу начинало набирать номер, не выдерживая паузу, заданную в поле **Dialing Interval Select** на экране **VoIP > Phone > Analog Phone**. Если выбран этот параметр, достаточно набрать телефонный номер и нажать кнопку “номер”. P-2602 начинает набирать номер сразу, без ожидания. Вместо нажатия кнопки также можно подождать указанное число секунд.
Apply	Нажмите эту кнопку, чтобы сохранить изменения в P-2602 и ввести их в действие.
Cancel	Нажмите эту кнопку, чтобы возвратить все поля на этом экране к последним сохраненным значениям.

11.15 Обзор дополнительных телефонных услуг

Многие поставщики услуг VoIP предоставляют так называемые дополнительные услуги:, удержание вызова, ожидание вызова, передача вызова другому абоненту и т.п. P-2602 поддерживает следующие виды услуг:

- Удержание вызова
- Ожидание вызова
- Второй вызов в параллельном режиме
- Передача вызова на другого абонента
- Переадресация вызова (см. разд. 11.19 на стр. 190)
- Трехсторонняя конференц-связь
- Внутренние вызовы (см. разд. 12.3 на стр. 195)

Примечание: Чтобы использовать все дополнительные услуги, доступные через порты P-2602, может быть необходимо заказать их у поставщика услуг VoIP.

11.15.1 Кнопка сброса

Операция сброса (“flash”) состоит в том, что рычаг телефонного аппарата нажимается на короткое время (десятые доли секунды) и снова отпускается. В новых телефонных аппаратах обычно предусмотрена кнопка “сброс”, которая генерирует этот сигнал с помощью электроники. Если кнопка сброса в вашем телефонном аппарате отсутствует, операцию сброса можно выполнить, нажав рукой на рычаг и сразу же его отпустив. Однако рекомендуется всегда пользоваться кнопкой сброса, которая строго выдерживает необходимое время. При ручном сбросе, если держать рычаг нажатым слишком долго, P-2602 может воспринять это как разъединение.

Все дополнительные услуги можно вызывать с помощью кнопки сброса.

11.15.2 Дополнительные телефонные услуги европейского стандарта

В этом разделе описано использование дополнительных телефонных услуг при установке параметра **Call Service Mode** в значение **Europe Type**. Команды для дополнительных услуг перечислены ниже в таблице.

Если после нажатия кнопки сброса вы не набираете номер подкоманды до истечения стандартного интервала приема подкоманды (2 секунды) или набираете неверный номер подкоманды, текущая операция прерывается.

Таб. 60 Команды европейского стандарта, вызываемые кнопкой сброса

КОМАНДА	ПОДКОМАНДА	ОПИСАНИЕ
Сброс		Помещение текущего вызова в режим ожидания для осуществления второго вызова. Возврат к вызову (если нет второго вызова).
Сброс	0	Разъединение вызова, находящегося в режиме ожидания, или отклонение входящего вызова, ожидающего ответа.
Сброс	1	Завершение текущего соединения и ответ на входящий вызов или возобновление разговора с абонентом, находящимся в режиме ожидания.
Сброс	2	1. Переключение между двумя вызовами. 2. Помещение текущего вызова в режим ожидания для ответа на входящий вызов. 3. Разделение трехсторонней конференц-связи на два индивидуальных вызова (один – на связи, другой – в режиме ожидания).
Сброс	3	Установление трехсторонней конференц-связи.
Сброс	*98#	Передача вызова на другой телефон.

11.15.2.1 Удержание вызова в сетях европейского стандарта

Функция удержания вызова позволяет нажатием кнопки сброса поместить вызов (**A**) в режим ожидания.

Если существует другой вызов, для переключения между вызывающими абонентами **A** и **B** следует нажать кнопку сброса и затем “2”. Другой абонент при этом переводится в режим ожидания.

Чтобы разъединить вызов, находящийся в режиме ожидания, и сохранить связь с текущим абонентом, нажмите кнопку сброса и затем “0”.

Чтобы разъединить текущий вызов и возобновить вызов из режима ожидания, нажмите кнопку сброса и затем “1”.

Если вы повесите трубку, когда один из абонентов будет находиться в режиме ожидания, телефон предупредит об этом звонком.

11.15.2.2 Ожидание вызова в сетях европейского стандарта

Эта функция позволяет помещать вызов в режим ожидания, пока вы отвечаете на другой входящий вызов по одному и тому же телефону.

Если на ваш номер поступил другой вызов, то вы услышите сигнал предупреждения о поступившем вызове. В этом случае можно предпринять одно из следующих действий:

- Отклонить второй вызов.

  Нажмите кнопку сброса, затем нажмите “0”.
- Разъединить первый вызов и ответить на второй вызов.

  Либо нажмите кнопку сброса и “1”, либо повесьте трубку и ответьте, когда телефон зазвонит.
- Поместить первый вызов в ожидание и ответить на второй вызов.

  Нажмите кнопку сброса, затем нажмите “2”.

11.15.2.3 Передача вызова в сетях европейского стандарта

Чтобы передать входящий вызов (на который вы ответили) на другой телефон, выполните следующие действия.

1. Нажмите кнопку сброса, чтобы поместить абонента в режим ожидания.
2. Когда вы услышите гудок, наберите “*98#” для обращения к селекторной связи, затем наберите номер, на который вы хотите передать вызов.
3. После того, как вы услышите сигнал вызова или ответ второй стороны, повесьте трубку.

11.15.2.4 Трехсторонняя конференц-связь в сетях европейского стандарта

Для установления трехсторонней конференц-связи выполните следующие операции.

1. Во время разговора нажмите кнопку сброса, чтобы перевести абонента в режим ожидания и услышать гудок.

2 Чтобы сделать другой вызов, наберите непосредственно требуемый номер.

3 После ответа на второй вызов нажмите кнопку сброса, затем нажмите “3”, чтобы установить трехстороннюю связь.

4 Чтобы завершить соединение, повесьте трубку.

5 Чтобы разделить трехстороннюю конференц-связь на два отдельных вызова (один – на связи, другой – в режиме ожидания), нажмите кнопку сброса и “2”.

11.15.3 Дополнительные телефонные услуги американского стандарта

В этом разделе описано использование дополнительных телефонных услуг при установке параметра **Call Service Mode** в значение **USA Type**. Команды для дополнительных услуг перечислены ниже в таблице.

Если после нажатия кнопки сброса вы не набираете номер подкоманды до истечения стандартного интервала приема подкоманды (2 секунды) или набираете неверный номер подкоманды, текущая операция прерывается.

Таб. 61 Команды американского стандарта, вызываемые кнопкой сброса

КОМАНДА	ПОДКОМАНДА	ОПИСАНИЕ
Сброс		Помещение текущего вызова в режим ожидания для осуществления второго вызова. После успешного установления второго вызова снова нажмите кнопку сброса, чтобы установить трехстороннюю связь. Помещение текущего вызова в режим ожидания для ответа на входящий вызов.
Сброс	*98#	Передача вызова на другой телефон.

11.15.3.1 Удержание вызова в сетях американского стандарта

Функция удержания вызова позволяет нажатием кнопки сброса поместить вызов (**A**) в режим ожидания.

Если существует другой вызов, то для переключения между вызывающими абонентами **A** и **B** можно использовать кнопку сброса. Другой абонент при этом переводится в режим ожидания.

Если вы повесите трубку, когда один из абонентов будет находиться в режиме ожидания, телефон предупредит об этом звонком.

11.15.3.2 Ожидание вызова в сетях американского стандарта

Эта функция позволяет помещать вызов в режим ожидания, пока вы отвечаете на другой входящий вызов по одному и тому же телефону.

Если на ваш номер поступил другой вызов, вы услышите сигнал предупреждения о поступившем вызове.

Чтобы поместить первый вызов в ожидание и ответить на второй вызов, нажмите кнопку сброса.

11.15.3.3 Передача вызова в сетях американского стандарта

Чтобы передать входящий вызов (на который вы ответили) на другой телефон, выполните следующие действия.

1. Нажмите кнопку сброса, чтобы поместить абонента в режим ожидания.
2. Когда вы услышите гудок, наберите “*98#” для обращения к селекторной связи, затем наберите номер, на который вы хотите передать вызов.
3. После того, как вы услышите сигнал вызова или ответ второй стороны, повесьте трубку.

11.15.3.4 Трехсторонняя конференц-связь в сетях американского стандарта

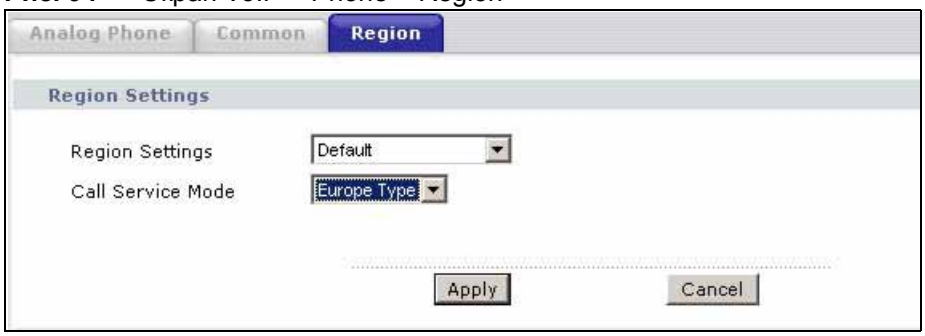
Для установления трехсторонней конференц-связи выполните следующие операции.

1. Во время разговора нажмите кнопку сброса, чтобы перевести абонента (A) в режим ожидания и услышать гудок.
2. Чтобы сделать другой вызов (с абонентом B), наберите непосредственно требуемый номер.
3. После ответа абонента B на второй вызов нажмите кнопку сброса, чтобы установить трехстороннюю связь.
4. Чтобы завершить соединение, повесьте трубку.
5. Чтобы разделить трехстороннюю конференц-связь на два отдельных вызова (абонент A – на связи, абонент B – в режиме ожидания), нажмите кнопку сброса.
6. Чтобы возвратиться к трехстороннему соединению, снова нажмите кнопку сброса.
7. Чтобы снова разделить трехстороннюю конференц-связь на два отдельных вызова, нажмите кнопку сброса. Теперь абонент B будет находиться на связи, а абонент A – в режиме ожидания.

11.16 Экран Phone Region

Этот экран служит для управления настройками, зависящими от того, в каком регионе мира используется P-2602. Чтобы перейти на этот экран, выберите **VoIP > Phone > Region**.

Рис. 94 Экран VoIP > Phone > Region



Каждое поле описано в следующей таблице.

Таб. 62 Экран VoIP > Phone > Region

ПОЛЕ	ОПИСАНИЕ
Region Settings	Выберите местонахождение P-2602.
Call Service Mode	Выберите режим вызова дополнительных телефонных услуг (удержание вызова, ожидание вызова, передача вызова другому абоненту и трехсторонняя конференц-связь), поддерживаемый вашим поставщиком услуг VoIP. **Europe Type** - европейский стандарт дополнительных телефонных услуг **USA Type** - американский стандарт дополнительных телефонных услуг Для пользования услугами может потребоваться подписка на них. Обратитесь к поставщику услуг VoIP.
Apply	Нажмите эту кнопку, чтобы сохранить изменения в P-2602 и ввести их в действие.
Cancel	Нажмите эту кнопку, чтобы возвратить все поля на этом экране к последним сохраненным значениям.

11.17 Ускоренный вызов

Функция ускоренного вызова позволяет быстро набирать часто используемые номера телефонов VoIP.

11.17.1 Одноранговые вызовы

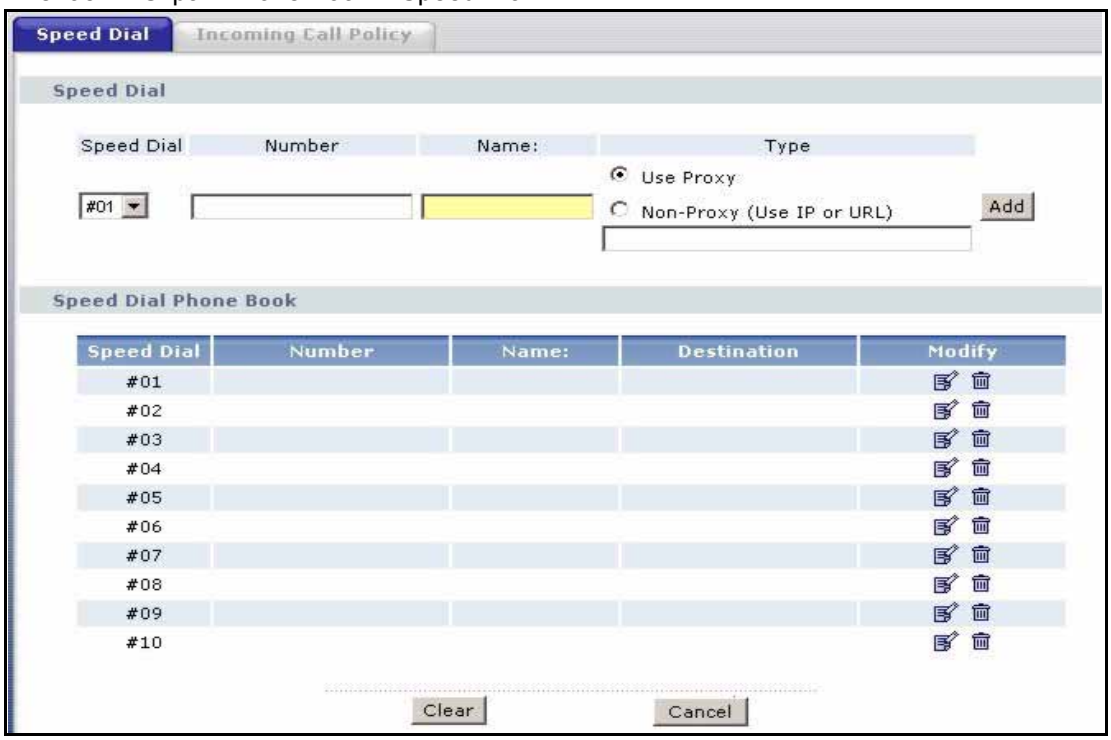
Можно вызывать другое устройство VoIP непосредственно, минуя сервер SIP. Для этого необходимо настроить запись в телефонной книге ускоренного вызова. В графе **Type** выберите **Non-Proxy (Use IP or URL)** и укажите IP-адрес или доменное имя вызываемой стороны. При вызове через запись в книге ускоренных вызовов устройство P-2602 направит удаленному VoIP-устройству запрос SIP INVITE.

Для осуществления одноранговых вызовов VoIP настройка учетной записи SIP в P-2602 не требуется.

11.18 Экран Speed Dial

Для осуществления одноранговых вызовов или набора номеров, содержащих буквы, необходимо настроить записи в телефонной книге ускоренного вызова. Такие записи можно также создать для часто используемых телефонных номеров SIP. Этот раздел служит для добавления, редактирования и удаления записей в телефонной книге ускоренных вызовов для исходящих вызовов. Чтобы перейти на этот экран, выберите **VoIP > Phone Book > Speed Dial**.

Рис. 95 Экран Phone Book > Speed Dial



Каждое поле описано в следующей таблице.

Таб. 63 Экран Phone Book > Speed Dial

ПОЛЕ	ОПИСАНИЕ
Speed Dial	Этот раздел служит для создания и редактирования записей в телефонной книге ускоренного вызова.
Speed Dial	Выберите номер ускоренного вызова, который вы хотите использовать для данного телефонного номера.
Number	Введите номер SIP, который P-2602 будет набирать при использовании данного номера ускоренного вызова.
Name	Введите имя абонента, вызываемого с помощью данного номера ускоренного вызова. Допустимая длина – до 127 печатных знаков ASCII.

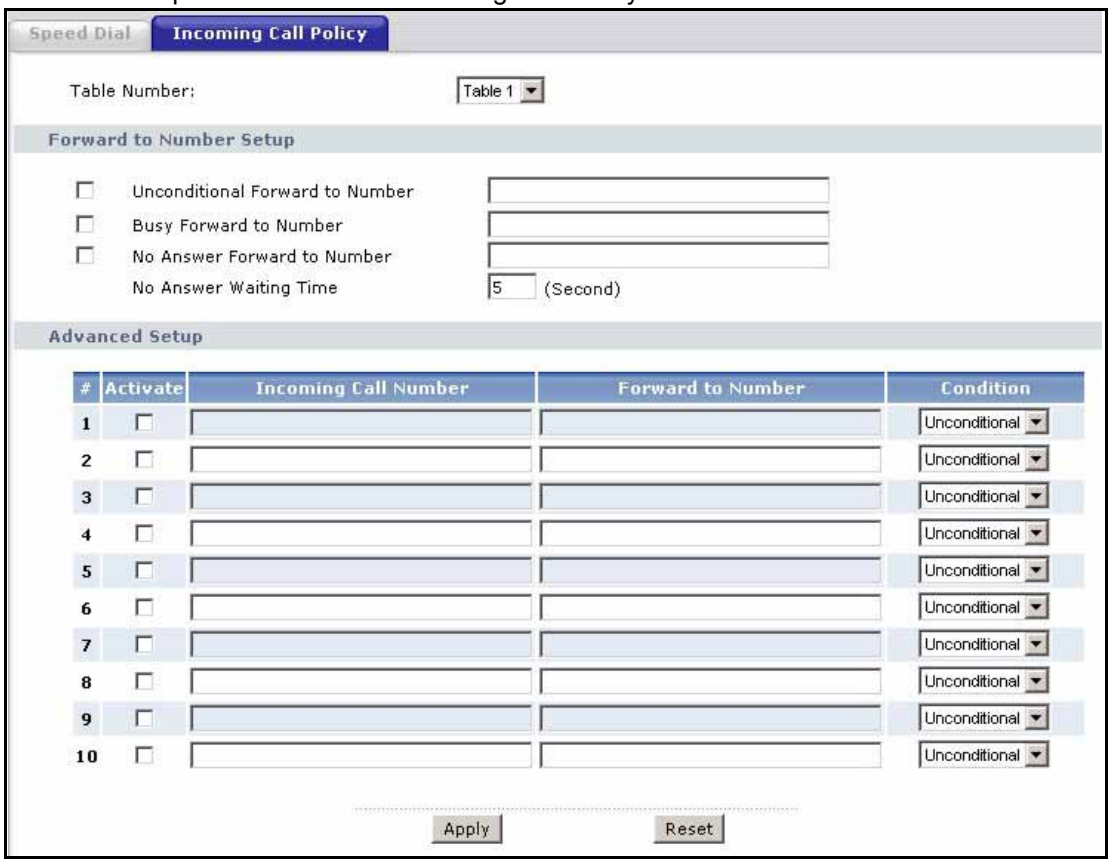
Таб. 63 Экран Phone Book > Speed Dial

ПОЛЕ	ОПИСАНИЕ
Type	Выберите **Use Proxy**, чтобы для набора этого номера использовать одну из учетных записей SIP. Выберите **Non-Proxy (Use IP or URL)**, чтобы использовать другой сервер SIP или осуществлять вызов в одноранговом режиме. В этом случае в расположенном ниже поле нужно указать IP-адрес или доменное имя сервера SIP или удаленной стороны соединения.
Add	Щелкните здесь, чтобы обновить раздел **Speed Dial Phone Book** сведениями из раздела **Speed Dial**.
Speed Dial Phone Book	Этот раздел служит для просмотра и удаления всех записей в телефонной книге ускоренного вызова.
Speed Dial	В этом поле отображается номер ускоренного вызова, который набирается для вызова соответствующего абонента.
Number	В этом поле отображается номер SIP, который P-2602 будет набираться вместо данного номера ускоренного вызова.
Name	В этом поле отображается имя абонента, вызываемого с помощью данного номера ускоренного вызова.
Destination	Это поле будет пустым, если для ускоренного вызова используется одна из существующих учетных записей SIP. В противном случае в нем будет указан IP-адрес или доменное имя сервера SIP или удаленной стороны соединения. (Это поле соответствует полю **Type** в разделе **Speed Dial**.)
Modify	Это поле служит для редактирования или удаления записи из телефонной книги ускоренного вызова. Щелкните на значке **Edit**, чтобы скопировать информацию из данной записи ускоренного вызова в раздел **Speed Dial**, где ее можно изменить. Щелкните значок **Remove**, чтобы удалить данную запись ускоренного вызова.
Clear	Щелкните здесь, чтобы удалить все записи ускоренного вызова.
Cancel	Нажмите эту кнопку, чтобы возвратить все поля на этом экране к последним сохраненным значениям.

11.19 Экран Incoming Call Policy

На этом экране настраиваются правила обработки входящих вызовов. Можно блокировать, переадресовывать, или принимать входящие вызовы. Чтобы перейти на этот экран, выберите **VoIP > Phone Book > Incoming Call Policy**.

Рис. 96 Экран Phone Book > Incoming Call Policy



Можно создать два набора правил переадресации вызовов. Каждый набор хранится в таблице переадресации вызовов. Каждое поле описано в следующей таблице.

Таб. 64 Экран Phone Book > Incoming Call Policy

ПОЛЕ	ОПИСАНИЕ
Table Number	Выберите таблицу переадресации вызовов, которую требуется просмотреть на этом экране. При изменении этого поля содержимое экрана автоматически обновляется.
Forward to Number Setup	P-2602 проверяет эти правила в том порядке, в котором они перечислены, после проверки правил в разделе **Advanced Setup**.
Unconditional Forward to Number	Выберите этот режим, чтобы указать P-2602 переадресовывать все входящие вызовы на указанный номер телефона независимо от других правил на экране **Forward to Number**. Введите телефонный номер в поле справа.
Busy Forward to Number	Выберите этот режим, чтобы указать P-2602 переадресовывать все входящие вызовы на указанный номер телефона, если телефонный порт занят. Введите телефонный номер в поле справа. При наличии вызова, находящегося в режиме ожидания, входящий вызов будет переадресован на указанный телефонный номер, если вы отклоните или проигнорируете второй входящий вызов.
No Answer Forward to Number	Выберите этот режим, чтобы указать P-2602 переадресовывать неотвеченные входящие вызовы на указанный телефонный номер. (См. **No Answer Waiting Time**.) Введите телефонный номер в поле справа.

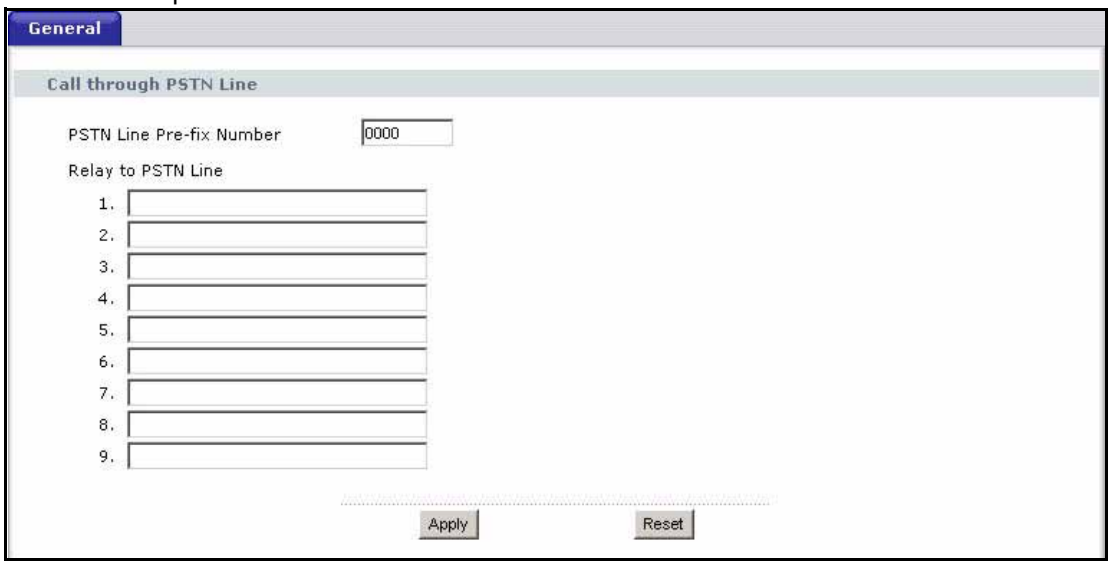
Таб. 64 Экран Phone Book > Incoming Call Policy

ПОЛЕ	ОПИСАНИЕ
No Answer Waiting Time	Это поле используется для описанных ниже событий: **No Answer Forward to Number** (нет ответа, переадресация на указанный номер) и **No Answer** (нет ответа). Введите время (в секундах), в течение которого P-2602 будет ожидать ответа на входящий вызов, прежде он будет помечен как неотвеченный.
Advanced Setup	P-2602 проверяет эти правила до проверки правил в разделе **Forward to Number**.
#	Это поле содержит порядковый номер и не связано с каким-либо правилом. Однако сам порядок также имеет значение. P-2602 последовательно проверяет каждое правило и применяет только первое найденное правило, для которого выполняются условия.
Activate	Установите этот флажок, чтобы включить данное правило. Снимите этот флажок, чтобы отключить данное правило.
Incoming Call Number	Введите телефонный номер, к которому применяется это правило.
Forward to Number	Введите телефонный номер, на который будут переадресовываться входящие вызовы с номера **Incoming Call Number**. В зависимости от условия (**Condition**) это поле можно оставить пустым.
Condition	Выберите ситуации, в которых входящие вызовы будут переадресовываться с номера **Incoming Call Number**, или выберите альтернативное действие. **Unconditional** - P-2602 немедленно переадресует все вызовы с номера **Incoming Call Number** на номер **Forward to Number**. **Busy -** P-2602 переадресует все вызовы с номера **Incoming Call Number** на номер **Forward to Number**, когда с вашей учетной записью SIP уже имеется установленный вызов. **No Answer -** P-2602 переадресует все неотвеченные вызовы с номера **Incoming Call Number** на номер **Forward to Number**. (См. **No Answer Waiting Time**.) **Block -** P-2602 отклоняет вызовы с номера **Incoming Call Number**. **Accept -** P-2602 принимает вызовы с номера **Incoming Call Number**. Правило с этим условием позволяет запретить переадресацию входящих вызовов от определенных абонентов по правилам раздела **Forward to Number**.
Apply	Нажмите эту кнопку, чтобы сохранить изменения в P-2602 и ввести их в действие.
Cancel	Нажмите эту кнопку, чтобы возвратить все поля на этом экране к последним сохраненным значениям.

11.20 Экран PSTN Line (только в моделях с индексом “L”)

Этот экран позволяет настроить линию ТфОП для обычных телефонных вызовов. Чтобы перейти на этот экран, выберите **VoIP > PSTN Line > General**.

Рис. 97 Экран PSTN Line > General



Каждое поле описано в следующей таблице.

Таб. 65 Экран PSTN Line > General

ПОЛЕ	ОПИСАНИЕ
PSTN Line Pre-fix Number	Введите префикс длиной 1 – 7 цифр, который потребуется набирать перед телефонным номером, чтобы осуществлять обычные телефонные вызовы в то время, когда зарегистрирована одна из ваших учетных записей SIP. По этой последовательности цифр P-2602 определит, что вы хотите сделать вызов через обычную телефонную сеть.
Relay to PSTN Line	Введите телефонные номера (для обычных вызовов, не вызовов VoIP), которые вы хотите набирать без префикса. Например, можно ввести телефоны экстренных служб. Номер (1 – 9) не является номером ускоренного вызова. Это обычный порядковый номер, не связанный с конкретными телефонными номерами.
Apply	Нажмите эту кнопку, чтобы сохранить изменения в P-2602 и ввести их в действие.
Cancel	Нажмите эту кнопку, чтобы возвратить все поля на этом экране к последним сохраненным значениям.

Глава 12
Использование телефона

В этой главе описывается, как выполнять основные операции с телефоном, подключенным к P-2602.

12.1 Набор номера

При наличии зарегистрированной учетной записи SIP светодиод **PHONE** горит зеленым светом. Наберите номер SIP на клавиатуре вашего телефона (например, “12345”).

разд. 11.17 на стр. 188Одноранговые вызовы и набор номеров, содержащих буквы, осуществляются только через телефонную книгу ускоренного вызова. Наберите номер ускоренного вызова на клавиатуре вашего телефона.

Для набора обычных телефонных номеров используйте схему, предусмотренную поставщиком услуг VoIP.

12.2 Набор номера в режиме ускоренного вызова

После настройки записи ускоренного вызова и внесения ее в телефонную книгу наберите последовательность, соответствующую номеру ускоренного вызова, на клавиатуре вашего телефона.

12.3 Внутренние вызовы

Чтобы позвонить на телефон, подключенный к другому порту P-2602, наберите на клавиатуер вашего телефона “####”.

12.4 Проверка IP-адреса устройства

Чтобы прослушать текущий IP-адрес P-2602 в виде сообщения, выполните следующие действия.

1. Снимите трубку на телефоне.
2. Наберите на клавиатуре телефона последовательность “****”. Дождитесь сообщения о том, что вы вошли в меню настройки.
3. Нажмите “5”, затем нажмите кнопку “#”.
4. Прослушайте и запишите IP-адрес.
5. Повесьте трубку.

12.5 Автоматическое обновление микропрограммы

Во время автоматической инициализации P-2602 проверяет наличие новой версии микропрограммы. При обнаружении новой вышедшей микропрограммы P-2602 проинформирует об этом особым сообщением, когда вы снимите трубку.

Чтобы обновить микропрограмму P-2602, наберите “*99#”.

Чтобы отказаться от обновления микропрограммы P-2602, наберите “#99#”.

Глава 13
Межсетевые экраны

В этой главе даны основные сведения о межсетевых экранах и кратко рассмотрен межсетевой экран в P-2602.

13.1 Общие сведения о межсетевых экранах

Первоначально английский термин “*firewall*” (“брандмауэр”) возник в строительстве и обозначал перегородку, предназначенную для предотвращения распространения огня из одной комнаты в другую. В компьютерных сетях термин “firewall” (переводимый как “межсетевой экран”) обозначает систему или группу систем, обеспечивающую выполнение политики контроля над доступом из одной сети в другую. Его также можно определить как механизм, используемый для защиты надёжной сети от ненадёжной. Конечно, межсетевые экраны не могут решить все проблемы безопасности и являются *лишь одним из множества* механизмов, используемых для создания периметра безопасности согласно политике сетевой безопасности. Межсетевой экран не должен оставаться *единственным* используемым механизмом или приемом. Чтобы межсетевой экран эффективно выполнял защитные функции, необходимо соответствующим образом его спроектировать и установить. Для этого требуется интегрировать межсетевой экран в более широкую политику информационной безопасности. Кроме того, следует реализовать определенные политики в самом межсетевом экране.

Настройки межсетевого экрана по умолчанию описаны в разд. 14.5 на стр. 216.

Просмотр правил межсетевого экрана описан в разд. 14.6 на стр. 218.

Настройка правил межсетевого экрана описана в разд. 14.6.1 на стр. 220.

Настройка собственных типов сетевых служб описана в разд. 14.6.2 на стр. 222.

Настройка пороговых значений для межсетевых экранов описана в разд. 14.8.3 на стр. 229.

13.2 Типы межсетевых экранов

Существует три основных типа межсетевых экранов:

- межсетевые экраны с фильтрацией пакетов
- межсетевые экраны прикладного уровня
- динамические межсетевые экраны

13.2.1 Межсетевые экраны с фильтрацией пакетов

Межсетевые экраны с фильтрацией пакетов ограничивают доступ, исходя из содержащихся в пакете данных о сетевом адресе источника/получателя и о типе приложения.

13.2.2 Межсетевые экраны прикладного уровня

Межсетевые экраны прикладного уровня ограничивают доступ, выступая в качестве промежуточных (прокси) серверов по отношению к внешним серверам. Используя программы, написанные для определенных интернет-служб, например, HTTP, FTP и telnet, они могут проверять корректность содержимого пакета с точки зрения конкретных приложений. Шлюзы прикладного уровня в целом имеют много преимуществ по сравнению с непосредственным пропусканием трафика на внутренние хосты:

Сокрытие информации не позволяет извне находить имена внутренних систем посредством DNS, поскольку шлюз прикладного уровня – единственный хост, название которого сообщается внешним системам.

Мощный механизм аутентификации позволяет проверять подлинность трафика на прикладном уровне до его поступления на внутренние хосты, а средства ведения журналов обеспечивают большую эффективность, чем если бы эта операция выполнялась на самом хосте. Правила фильтрации в маршрутизаторе с фильтрацией пакетов могут быть менее сложными по сравнению с тем случаем, когда маршрутизатор должен фильтровать трафик на прикладном уровне, пересылая его нескольким системам. Маршрутизатору требуется только пересылать трафик прикладного уровня, предназначенный для шлюза прикладного уровня, а остальной трафик не пропускать.

13.2.3 Межсетевые экраны с инспекцией пакетов с учетом состояния

Динамические (stateful) межсетевые экраны ограничивают доступ, применяя к пакетам с данными определенные правила доступа. Решения об управлении доступом принимаются с учетом IP-адреса и протокола. Они также следят за потоком данных в сеансе, проверяя целостность соединения и адаптируясь к динамическим протоколам. Такие межсетевые экраны в целом обеспечивают наилучшую пропускную способность и прозрачность, однако они могут иметь недостаточно развитые средства управления доступом на прикладном уровне и средства кэширования, поддерживаемые многими прокси-серверами. Более подробные сведения о динамическом анализе пакетов см. в разд. 13.5 на стр. 204.

Межсетевые экраны различных типов стали неотъемлемой частью стандартных систем безопасности на предприятиях.

13.3 Краткий обзор межсетевого экрана ZyXEL

Межсетевой экран P-2602 представляет собой динамический межсетевой экран, который может быть активирован для защиты от атак, провоцирующих отказ в обслуживании (DoS). Назначение P-2602 состоит в том, чтобы частная локальная сеть (LAN) была надежно подключена к Интернету. P-2602 может использоваться для предотвращения хищения, разрушения и модификации данных, а также операций по регистрации, которые могут иметь важное значение для безопасности сети. P-2602 также имеет средства фильтрации пакетов.

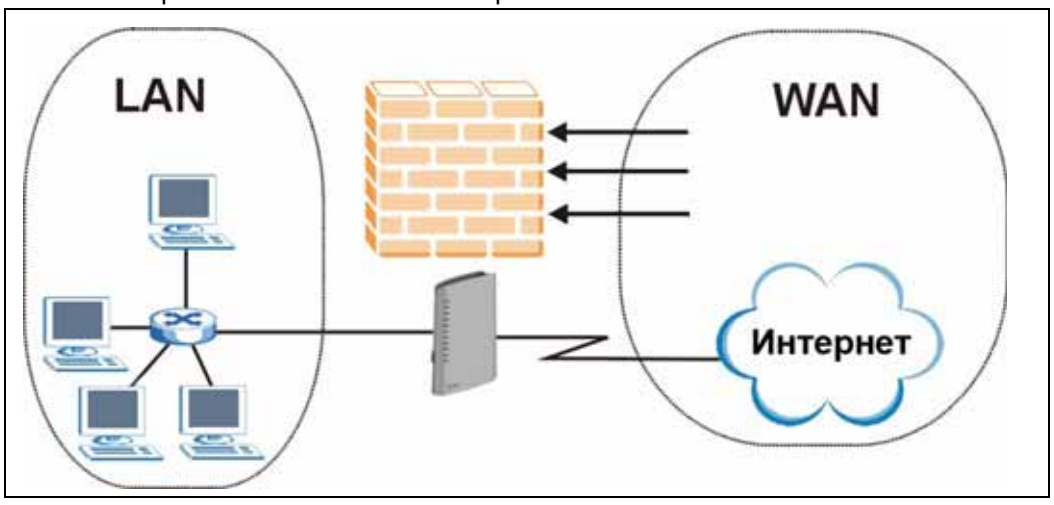
P-2602 размещается между LAN и Интернетом. Благодаря этому он функционирует как безопасный интернет-центр для всех данных, пересылаемых между Интернетом и LAN.

P-2602 имеет один порт DSL/ISDN и один Ethernet-порт LAN. Эти порты физически разделяют сеть на две области.

- Порт DSL/ISDN служит для подключения к Интернету.
- Порт LAN (локальной сети) подключается к компьютерной сети, для которой необходимо обеспечить защиту от внешнего мира. Эти компьютеры должны иметь доступ к Интернет-службам, таким как электронная почта, FTP и WWW. Однако доступ извне будет закрыт, пока вы не настроите дистанционное управление или не создадите правило межсетевого экрана, разрешающие удаленным хостам обращаться к определенным сетевым службам.

13.3.1 Атаки, вызывающие отказ в обслуживании

Рис. 98 Применение межсетевого экрана



13.4 Отказ в обслуживании

Атаки, приводящие к отказу в обслуживании (DoS), нацелены на устройства и сети, подключенные к Интернету. Их цель состоит не в добыче конфиденциальной информации, а в блокировании работы устройства или сети, в результате чего сетевые ресурсы становятся недоступны пользователям. В заводской конфигурации P-2602 предусмотрено обнаружение и нейтрализация всех известных видов DoS-атак.

13.4.1 Основы

Для совместного доступа к информации в Интернете все компьютеры используют общий язык, называемый протоколом TCP/IP. TCP/IP, в свою очередь, подразделяется на ряд прикладных протоколов, которые выполняют конкретные функции. Эти протоколы различаются по своеобразным “добавочным номерам” – номерам TCP- и UDP-портов, к которым привязаны такие протоколы, как HTTP (веб), FTP (протокол передачи файлов), POP3 (электронная почта) и т.д. Например, для веб-трафика по умолчанию используется TCP-порт 80.

Для взаимодействия компьютеров в Интернете используется модель “клиент-сервер”, в которой сервер “дежурит” на определенном порту TCP/UDP, ожидая запроса информации удаленными клиентскими компьютерами, находящимися в сети. В частности, веб-сервер обычно работает на порту 80. Следует отметить, что даже если к компьютеру предполагается обращаться только через один порт, например, через веб-сервер на порту 80, другие порты также будут активны. Неосторожность в настройке или управлении компьютером может создать возможности для хакерского нападения через незащищенный порт.

Самые распространённые порты IP:

Таб. 66 Часто используемые порты IP

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

13.4.2 Типы DoS-атак

Существует четыре типа DoS-атак:

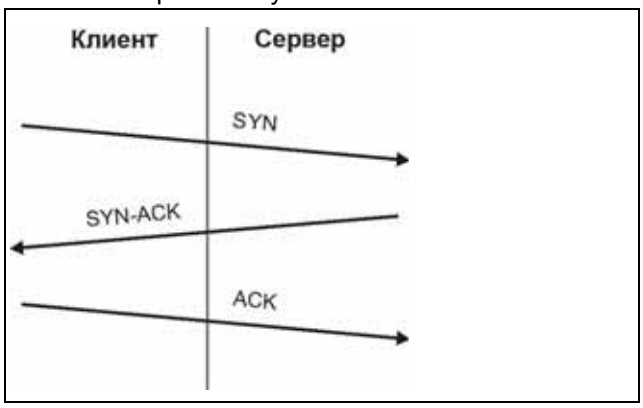
1. Атаки, эксплуатирующие дефекты конкретной реализации TCP/IP.
2. Атаки, эксплуатирующие недосмотры в спецификациях TCP/IP.
3. Нападения методом “грубой силы”, заполняющие сеть бесполезными данными.
4. Подмена IP-адреса.

5 “Атаки типа “**Ping of Death**” и “**Teardrop**”, эксплуатирующие распространенные ошибки в реализациях TCP/IP, присутствующие на разных компьютерах и хост-системах.

- Для атаки “Ping of Death” с помощью утилиты “ping” создается IP-пакет, длина которого превышает допустимую длину 65 536 байт, предусмотренную спецификацией IP. Пакет недопустимо большого размера отправляется на незащищенную систему, в результате чего она может дать сбой, зависнуть или перезагрузиться.
- Атака “Teardrop” нацелена на ошибки в механизме повторной сборки IP-пакетов. При передаче данных через сеть IP-пакеты часто разбиваются на фрагменты меньшего размера. Каждый фрагмент имеет тот же формат, что и исходный IP-пакет, но отличается наличием особого поля смещения, которое указывает: этот фрагмент содержит байты 200 – 400 из исходного (нефрагментированного) IP-пакета. Программа “Teardrop” создает множество фрагментов IP-пакетов с перекрывающимися значениями в поле смещения. При повторной сборке этих фрагментов на компьютере-получателе некоторые системы дают сбои, зависают или перезагружаются.

6 Недостаточная проработка спецификаций TCP/IP создала возможности для атак, известных как “**SYN Flood**” и “**LAND**”. Эти атаки производятся на этапе установления связи, при подготовке сеанса обмена данными между двумя приложениями.

Рис. 99 Три этапа установления сеанса

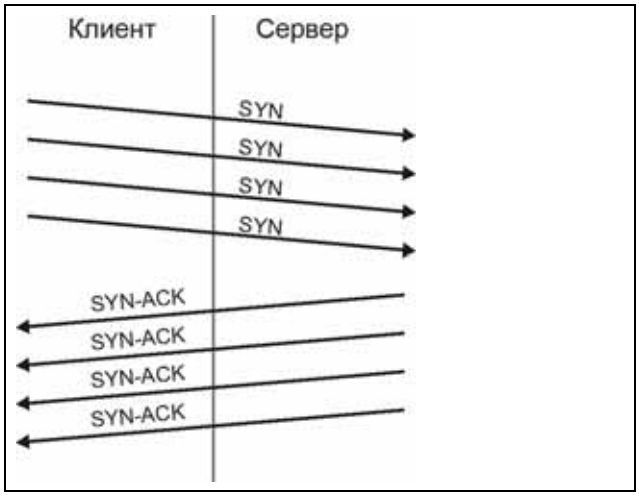


Обычно приложение, открывающее сеанс, направляет серверу-получателю пакет SYN (синхронизация). Получатель отвечает пакетом ACK (подтверждение) и посылает собственный SYN, на который инициатор также должен ответить пакетом ACK. После этого подготовительного этапа соединение считается установленным.

- Атака “**SYN Flood**” выводит из строя жертву с помощью большого числа пакетов SYN. Каждый пакет заставляет систему-жертву направлять отклик SYN-ACK. Пока жертва ожидает подтверждения, которое должно прийти в ответ на SYN-ACK, она накапливает в так называемой невыполненной очереди все текущие запросы SYN-ACK. SYN-ACK удаляются из этой очереди только после прихода подтверждения или в результате отмены трехэтапной операции установления связи по

срабатыванию внутреннего таймера (который рассчитан на относительно долгий интервал). Когда очередь переполнена, система начинает игнорировать все поступающие запросы SYN, и система перестает быть доступна правомочным пользователям.

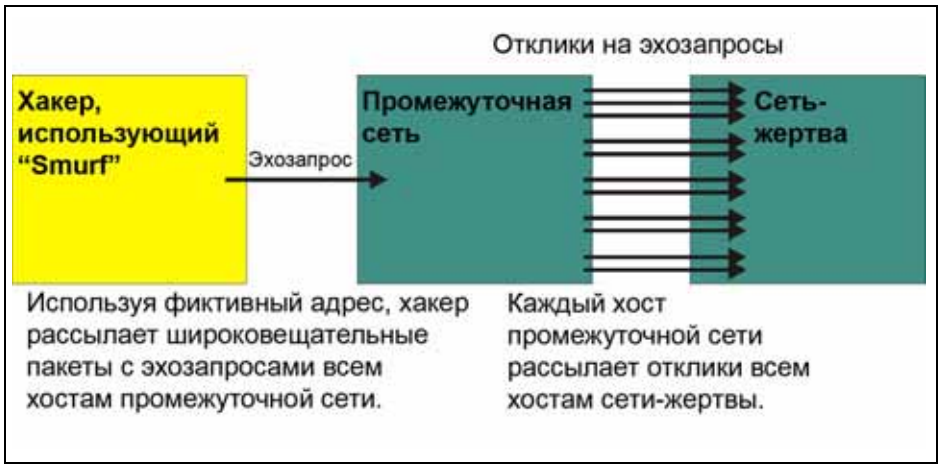
Рис. 100 SYN Flood



- В атаке **“LAND”** хакеры направляют в сеть пакеты SYN, в которых IP-адрес источника подменен на адрес жертвы. В результате имитируется ситуация, при которой хост посылает пакеты сам себе, и система, пытающаяся ответить самой себе, перестает быть доступна.

7 В атаке методом грубой силы **(“brute-force”)**, например, в атаке “Smurf”, используется функция прямого широковещательного запроса для подсети, предусмотренная спецификацией IP, при этом сеть, на которую направлена атака, переполняется бесполезными данными. Применяя Smurf, хакер переполняет маршрутизатор эхозапросами ICMP (Internet Control Message Protocol – межсетевой протокол контрольных сообщений), известными как “ping”. Поскольку IP-адрес адресата каждого пакета представляет собой широковещательный адрес подсети, маршрутизатор передает пакет эхозапроса ICMP всем хостам в сети. При большом числе хостов эхозапросы и отклики ICMP порождают значительный трафик. Если хакер подменит IP-адрес источника в пакете эхозапроса ICMP, то результирующий ICMP-трафик не только переполнит “промежуточную” сеть, но и распространится в сети-жертве с подмененным IP-адресом источника. Такое переполнение широковещательным трафиком расходует всю доступную полосу пропускания, парализуя обмен данными.

Рис. 101 Атака Smurf



13.4.2.1 Уязвимость ICMP

ICMP – это протокол сообщений об ошибках, работающий совместно с IP. Следующие типы ICMP-запросов вызывают предупреждение:

Таб. 67 Команды ICMP, вызывающие предупреждения

5	REDIRECT
13	TIMESTAMP_REQUEST
14	TIMESTAMP_REPLY
17	ADDRESS_MASK_REQUEST
18	ADDRESS_MASK_REPLY

13.4.2.2 Недопустимые команды (NetBIOS и SMTP)

Допустимыми являются только следующие команды NetBIOS, все другие команды не разрешены.

Таб. 68 Допустимые команды NetBIOS

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

Любые команды SMTP, кроме перечисленных в следующих таблицах, являются недопустимыми.

Таб. 69 Допустимые команды SMTP

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

13.4.2.3 Traceroute

Traceroute – это утилита для определения маршрута пакета между двумя конечными точками. В ряде случаев, когда фильтрация пакетов в межсетевом экране настроена неправильно, хакер может преодолеть межсетевой экран с помощью “traceroute” и узнать топологию сети за межсетевым экраном.

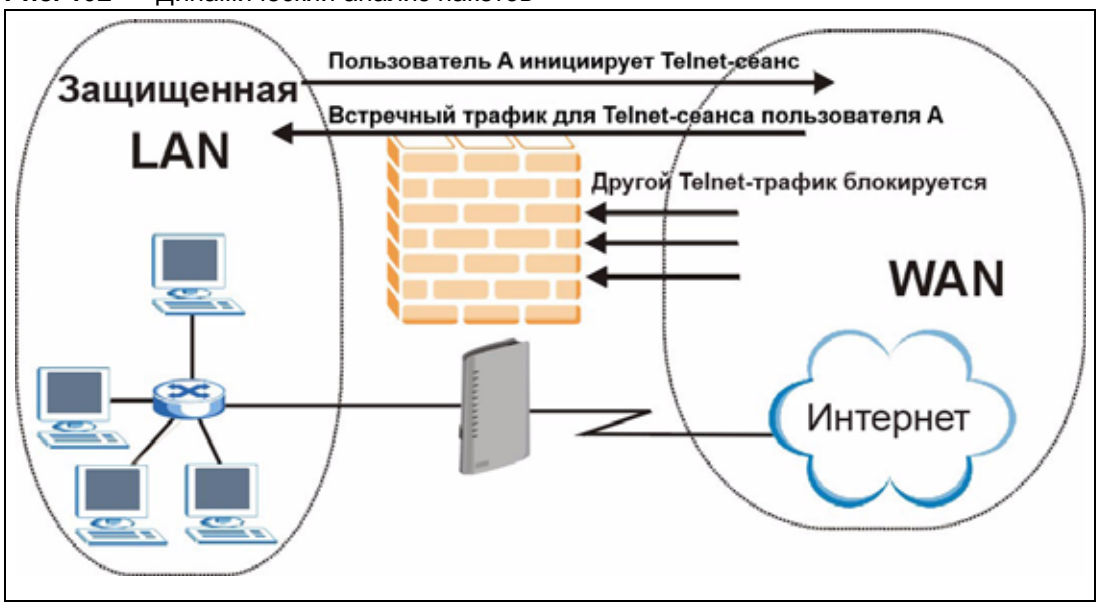
Часто для DoS-атак также используется прием, известный как **подмена IP-адреса**. Целью подмены может быть проникновение в системы, сокрытие истинного местонахождения хакера или увеличение эффекта DoS-атаки. Подмена IP-адреса используется для несанкционированного доступа на компьютеры, при этом маршрутизатор или межсетевой экран вводится в заблуждение тем, что сеанс якобы устанавливается изнутри доверенной сети. Реализуя подмену IP-адреса, хакер должен изменить заголовки пакета так, чтобы казалось, что пакеты происходят от доверенного хоста и должны свободно пропускаться маршрутизатором или межсетевым экраном. P-2602 блокирует все попытки подмены IP-адреса.

13.5 Динамический анализ пакетов

Динамический анализ пакетов состоит в том, что содержимое полей в пакетах сравнивается с пакетами, которые ранее были признаны доверенными. Например, если вы обращаетесь к какой-либо внешней сетевой службе, прокси-сервер запоминает такие параметры вашего исходного запроса, как номер порта и адреса источника и получателя. Это “запоминание” называется *сохранением состояния.* Когда внешняя система отвечает на ваш запрос, межсетевой экран сравнивает полученные пакеты с сохраненным состоянием, решая, нужно ли разрешить или запретить их прохождение. Используя динамический анализ пакетов, P-2602 защищает частные LAN от хакеров и вандалов в Интернете. По умолчанию механизм динамического анализа пакетов в P-2602 разрешает установление всех соединений с Интернетом со стороны LAN, и блокирует весь трафик по направлению к LAN, исходящий из Интернета. В первом приближении динамический анализ пакетов:

- Разрешает все сеансы, устанавливаемые со стороны LAN (локальная сеть) в направлении WAN (Интернет).
- Запрещает установление любых сеансов со стороны WAN в направлении LAN.

Рис. 102 Динамический анализ пакетов



На приведенном выше рисунке показано действие правил межсетевого экрана P-2602 по умолчанию, а также проиллюстрирован принцип работы динамического анализа пакетов. Пользователь “A” инициализирует сеанс Telnet изнутри LAN, и ответы на этот запрос разрешаются. Однако любой другой трафик Telnet, исходящий от WAN, блокируется.

13.5.1 Процедура динамического анализа пакетов

В рассмотренном примере при выходе TCP-пакета из локальной сети через интерфейс WAN межсетевого экрана происходит следующая последовательность событий. TCP-пакет является первым в сеансе, протокол прикладного уровня, к которому относится данный пакет, выбран для проверки по правилам межсетевого экрана:

1. Направление движения пакета – из LAN межсетевого экрана в WAN.
2. Пакет проверяется по имеющемуся списку доступа на выходе интерфейса, и его прохождение разрешается (запрещенный пакет был бы на этом этапе попросту отброшен).
3. Пакет проверяется по правилу межсетевого экрана. Устанавливается и отмечается состояние соединения для данного пакета. Эти сведения отмечаются в новой записи таблицы состояний, создаваемой для нового соединения. Если правило межсетевого экрана для этого пакета отсутствует и не имеет место атака, то действие, выполняемое над данным пакетом, определяется параметрами, заданными на экране **Firewall General**.
4. Исходя из полученной информации о состоянии, правило межсетевого экрана создает временную запись в списке доступа, вставляя ее в начало расширенного списка доступа на входе интерфейса WAN. Эта временная запись в списке доступа служит для того, чтобы разрешить входящие пакеты на том соединении, для которого только что был проверен исходящий пакет.

5 Исходящий пакет выходит через интерфейс.

6 Позднее на интерфейс поступает входящий пакет. Этот пакет относится к соединению, ранее установленному с помощью исходящего пакета. Входящий пакет проверяется по списку контроля доступа на входе интерфейса, и его прохождение разрешается благодаря наличию ранее созданной временной записи в списке доступа.

7 Пакет проверяется по правилу межсетевого экрана; запись в таблице состояния соединения при необходимости обновляется. С учетом обновленной информации о состоянии могут быть изменены временные записи во входном расширенном списке доступа, чтобы разрешались только пакеты, соответствующие текущему состоянию соединения.

8 Все другие входящие или исходящие пакеты, относящиеся к данному соединению, проходят проверку с необходимым обновлением записей в таблице состояний и изменением временных записей во входном списке доступа, после чего пакеты отправляются через интерфейс.

9 При завершении сеанса или разрыве неактивного сеанса по таймеру соответствующая запись исключается из таблицы состояний, а временные записи во входном списке доступа – удаляются.

13.5.2 Динамический анализ пакетов в устройствах ZyXEL

Могут быть определены дополнительные правила, расширяющие или заменяющие правила по умолчанию. В качестве примера можно создать правило, которое будет:

- Блокировать весь трафик определенного типа, например, IRC (чат в реальном времени), отправляемый из LAN в Интернет.
- Разрешать определенные виды трафика из Интернета к определенным хостам в LAN.
- Разрешать доступ к Web-серверу всем, кроме конкурентов.
- Разрешать использование определенных протоколов, например, Telnet, только авторизованным пользователям в LAN.

Логика работы таких правил заключается в проверке IP-адреса источника, места назначения и типа протокола IP в проходящих пакетах и сравнении этих значений с правилами, установленными администратором.

Примечание: Возможность задавать правила для межсетевого экрана – весьма мощное средство, при помощи которого можно снять защиту, обеспечиваемую межсетевым экраном, либо полностью заблокировать доступ в Интернет. При создании и удалении правил межсетевого экрана необходима чрезвычайная осторожность. Внося любое изменение, необходимо сразу же его проверить, чтобы удостовериться в правильности его работы.

Ниже приведено краткое техническое описание алгоритмов, по которым межсетевой экран следит за соединениями. Соединения могут присутствовать в явном виде, обусловленном протоколами верхнего уровня (например, TCP), или формироваться P-2602 (как в случае с “виртуальными соединениями”, создаваемыми для UDP и ICMP).

13.5.3 Безопасность TCP

P-2602 использует информацию о состоянии, входящую в пакеты TCP. Первый пакет в любом новом соединении имеет установленный флажок SYN и сброшенный флажок ACK, такой пакет называется начальным. Все пакеты, которые не имеют такой структуры флажков, называются последующими – они представляют данные, которые встречаются далее в потоке TCP.

Если начальный пакет приходит из WAN, это означает, что кто-то пытается установить соединение из Интернета в LAN. За исключением ряда особых случаев (см. далее раздел “Протоколы верхнего уровня”) эти пакеты запрещаются и отмечаются в журнале.

Если начальный пакет приходит из LAN, это означает, что кто-то пытается установить соединение из LAN в Интернет. Соединение будет разрешено или запрещено исходя из политики безопасности (политика безопасности по умолчанию разрешает подобные виды соединений). Создается запись в кэше с информацией о соединении: IP-адреса, порты TCP, порядковые номера и т.д.

Получая последующие пакеты (из Интернета или из LAN), P-2602 извлекает из них информацию о соединении, которая сверяется с содержимым кэша. Прохождение пакета разрешается только в том случае, если он соответствует действительному соединению (т.е. поступает в ответ на соединение, установленное из LAN).

13.5.4 Безопасность UDP/ICMP

Пакеты UDP и ICMP сами по себе не содержат никакой информации о соединении (в частности, порядковых номеров). Однако они как минимум содержат два IP-адреса (источник и адресат). В пакете UDP также указывается пара номеров портов, а в ICMP – тип и код пакета. Все эти данные анализируются для построения “виртуальных соединений” в кэше.

В частности, поступление любого пакета UDP со стороны LAN приводит к созданию записи в кэше. Запоминаются IP-адреса и пары номеров портов. В течение короткого промежутка времени пакеты UDP, приходящие со стороны WAN и имеющие соответствующий IP-адрес и информацию UDP, будут пропускаться в обратном направлении через межсетевой экран.

Подобная схема имеет место и для ICMP, за исключением того, что P-2602 применяет более строгие ограничения: входящие отклики на эхозапрос принимаются только для ранее отправленных эхозапросов, прием откликов с маской адреса разрешен только для отправленных запросов маски адреса, а прием откликов с меткой времени – только для отправленных запросов метки времени. Никакие другие ICMP-пакеты не пропускаются

через межсетевой экран, поскольку они потенциально опасны и содержат недостаточно информации, которая бы позволяла их отследить. В частности, никогда не впускаются пакеты переадресации ICMP, которые могут использоваться для изменения маршрута с целью проведения трафика через машины злоумышленников.

13.5.5 Протоколы верхнего уровня

Некоторые протоколы высших уровней (например, FTP и RealAudio) одновременно используют несколько сетевых соединений. В общем виде они обычно имеют управляющее соединение (control connection), которое используется для пересылки команд между оконечными точками, и соединение для передачи данных (data connection), по которому передается основной объем информации.

Рассмотрим протокол FTP. Пользователь в LAN открывает управляющее соединение с сервером в Интернете и запрашивает файл. В этот момент удаленный сервер со стороны Интернета открывает встречное соединение для передачи данных. Для того, чтобы протокол FTP был работоспособен, этому соединению необходимо разрешить прохождение в LAN, даже если обычные соединения из Интернета запрещены.

Для этой цели P-2602 просматривает данные FTP на уровне приложения. В частности производится поиск исходящих команд “PORT”, при обнаружении которых создается запись в кэше под ожидаемое соединения для передачи данных. При этом не возникает какой-либо опасности, так как команда PORT содержит сведения об адресах и портах, однозначно идентифицирующие соединение.

Поддержка любого протокола с подобным принципом работы должна вводиться в индивидуальном порядке. Для этого можно использовать функцию настраиваемых портов (Custom Ports) в веб-конфигураторе.

13.6 Рекомендации по усилению безопасности с помощью межсетевого экрана

- Смените пароль по умолчанию.
- Ограничьте круг лиц, имеющих доступ к маршрутизатору по telnet.
- Не включайте какие-либо неиспользуемые локальные службы, такие как SNMP или NTP. Любая подключенная служба может нести в себе потенциальную угрозу системе безопасности. Настойчивый хакер может творчески подойти к задаче поиска способов использования включенных служб для получения доступа к межсетевому экрану или сети.
- Защитите включенные локальные службы от неправильного использования. Защиту можно установить, сконфигурировав службы так, чтобы они взаимодействовали только с определенными узлами, и, настроив правила так, чтобы для служб в конкретных интерфейсах пакеты блокировались.
- Установите защиту от подмены IP-адреса, убедившись в том, что межсетевой экран включен.
- Разместите межсетевой экран в защищенной (запираемой) комнате.

13.6.1 Общие правила безопасности

Осторожность не бывает излишней! Не обязательно любая брешь, возникшая в системе безопасности, будет связана с межсетевым экраном, фильтрацией или NAT. Ниже даны общие рекомендации, позволяющие свести риск к минимуму.

- Предложите вашему предприятию или учреждению проработать всесторонний план безопасности. Добросовестная работа сетевого администратора означает необходимость предугадывать стратегии хакеров и быть к ним готовым. Лучшая защита против хакеров и взломщиков – осведомленность. Разъясните всем работникам, насколько важна безопасность и как оградиться от риска. Разработайте свой список наподобие этого!
- DSL и кабельные модемы – это постоянные соединения, которые особенно уязвимы, поскольку они предоставляют больше возможностей хакеру для проникновения в вашу систему. Выключайте компьютер, когда он не используется.
- Никогда не сообщайте пароли и другую конфиденциальную информацию при случайных телефонных звонках или обращениях по электронной почте.
- Никогда не рассылайте конфиденциальную информацию (пароли, реквизиты кредитных карт и т.п.) по электронной почте в незашифрованном виде.
- Никогда не сообщайте конфиденциальную информацию через веб-страницу, если веб-сайт не использует защищенные сеансы. О наличии защищенного сеанса можно узнать по значку ключа в строке состояния вашего браузера (Internet Explorer 3.02 или выше, Netscape 3.0 или выше). Если веб-сайт использует защищенный сеанс, информация может быть передана безопасно. Защищенные операции в сети чрезвычайно сложны для взлома.
- Никогда не сообщайте ваш IP-адрес или другую информацию об устройстве сети людям, не относящимся к вашей организации. Будьте особенно осторожны с файлами, полученными по электронной почте от незнакомых лиц. Весьма распространенный способ внедрения программ для дистанционного управления (BackOrifice) в чужие системы состоит в их отправке в качестве “троянского коня” с другими файлами.
- Регулярно меняйте используемые пароли. Всегда используйте пароли, которые не могут быть легко разгаданы. Самыми трудными с точки зрения взлома являются пароли со смесью символов верхнего и нижнего регистра, чисел и служебных знаков типа % или #.
- Регулярно обновляйте ваше программное обеспечение. Старые версии многих программ, в особенности браузеров, имеют широко известные уязвимости. При обновлении до текущих версий вы получаете самые новые исправления ошибок.
- Общаясь в веб- или IRC-чатах, отдавайте себе отчет в том, какую информацию вы сообщаете посторонним лицам.
- Если ваша система начала вести себя непредсказуемо, обратитесь к поставщику услуг Интернета. Иногда хакеры приводят в действие механизмы, постепенно нарушающие стабильность системы или приводящие к ее неработоспособности.
- Всегда измельчайте конфиденциальные документы, особенно относящиеся к вашему компьютеру, прежде чем их выбросить. Хакеры раскапывают мусор организаций или частных лиц, чтобы отыскать информацию, которая могла бы помочь им в нападении.

13.7 Сравнение фильтрации пакетов и межсетевого экрана

Ниже проведено краткое сравнение функций фильтрации пакетов и межсетевого экрана, реализованных в P-2602.

13.7.1 Фильтрация пакетов:

- Маршрутизатор фильтрует пакеты при их прохождении через интерфейс маршрутизатора согласно заданным правилам фильтра.
- Фильтрация пакетов – весьма мощный инструмент, но при этом достаточно трудоемкий в настройке и обслуживании, особенно если для определенных сетевых служб требуется цепь из нескольких правил.
- Фильтрация пакетов ограничивается проверкой части заголовка IP-пакета.

13.7.1.1 Когда следует использовать фильтрацию

- Для запрета/разрешения пакетов в LAN по их MAC-адресам.
- Для запрета/разрешения особых пакетов IP, не относящихся к протоколам TCP, UDP или ICMP.
- Для запрета/разрешения одновременно входящего (из WAN в LAN) и исходящего (из LAN в WAN) трафика между определенным внутренним хостом/сетью “A” и внешним хостом/сетью “B”. Если фильтр блокирует трафик от “A” до “B”, он также блокирует трафик от “B” до “A”. Фильтры не могут различать трафик, исходящий от внутреннего или внешнего хоста, по IP-адресу.
- Для запрета/разрешения трассировки маршрута IP (traceroute).

13.7.2 Межсетевой экран

- Межсетевой экран просматривает содержимое пакета, а также адреса источника и получателя. В межсетевых экранах подобного типа используется модуль-инспектор, применяемый для всех протоколов и различающий другие уровни, для которых предназначены данные в пакете, от сетевого уровня (заголовки IP) до прикладного уровня.
- Межсетевой экран выполняет динамический анализ пакетов. Он учитывает состояние обрабатываемых соединений, чтобы, например, разрешенный входящий пакет мог быть связан с соответствующим исходящим запросом и пропущен через экран. И наоборот, входящие замаскированные пакеты, являющиеся ответом на несуществующий исходящий запрос, будут блокироваться.
- Межсетевой экран использует фильтрацию в масштабе сеанса, применяя интеллектуальные правила, которые дополняют процесс фильтрации и позволяют управлять сетевым сеансом в целом, а не отдельными пакетами в его составе.
- Межсетевой экран предусматривает функцию информирования по электронной почте с отправкой регулярных отчетов и предупреждений.

13.7.2.1 Когда следует использовать межсетевой экран

- Для предотвращения DoS-атак и проникновения хакеров в сеть.
- В одном правиле межсетевого экрана может быть указан диапазон IP-адресов источников и адресатов, а также номеров портов. Это делает межсетевой экран наилучшим вариантом в тех случаях, когда требуются сложные правила.
- Для выборочного запрета/разрешения входящего или исходящего трафика между внутренним хостом/сетями и внешним хостом/сетями. Необходимо помнить, что фильтры не различают трафик, исходящий от внутреннего хоста или внешнего хоста, по IP-адресу.
- Если требуется проверка большого набора правил, межсетевой экран работает лучше, чем фильтрование.
- Используйте межсетевой экран, если вам необходимы регулярные отчеты по электронной почте о состоянии вашей системы или предупреждения об атаках на систему.
- Межсетевой экран позволяет заранее запретить трафик на определенные URL. URL сохраняются в базе данных списков управления доступом (ACL).

Глава 14
Настройка межсетевого экрана

В этой главе описывается активация и настройка межсетевого экрана в P-2602.

14.1 Методы доступа

Веб-конфигуратор является наиболее универсальным инструментом настройки межсетевого экрана, имеющимся в устройстве P-2602. Поэтому рекомендуется настраивать межсетевой экран с помощью веб-конфигуратора. Команды CLI (интерфейса командной строки) предлагают ограниченные возможности настройки, и пользоваться ими рекомендуется только опытным пользователям.

14.2 Общие сведения о политиках межсетевого экрана

Правила межсетевого экрана сгруппированы по направлению прохождения пакетов, к которым они применяются:

- Из LAN в LAN/маршрутизатор
- Из LAN в WAN
- Из WAN в LAN
- Из WAN в WAN/маршрутизатор

Примечание: LAN включает как порты LAN, так и беспроводную сеть (WLAN).

По умолчанию функция динамического анализа пакетов в P-2602 разрешает прохождение пакетов в следующих направлениях:

- Из LAN в LAN/маршрутизатор (LAN to LAN/Router)

  Это позволяет компьютерам в составе LAN управлять P-2602 и обмениваться данными с сетями или подсетями, связанными с интерфейсом LAN.
- Из LAN в WAN (LAN to WAN)

По умолчанию функция динамического анализа пакетов в P-2602 запрещает прохождение пакетов в следующих направлениях:

- Из WAN в LAN (WAN to LAN)
- Из WAN в WAN/маршрутизатор (WAN to WAN/Router)

  Тем самым компьютеры в WAN теряют возможность использовать P-2602 как шлюз для связи с другими компьютерами в WAN и/или для управления P-2602.

Можно также определить дополнительные наборы правил или модифицировать существующие, но при этом необходимо соблюдать крайнюю осторожность.

Примечание: Настраивая правила межсетевого экрана без четкого понимания принципа их работы, можно по неосторожности ослабить безопасность межсетевого экрана и защищенной сети. После настройки правил всегда проверяйте их работу.

Например, можно создать следующие виды правил:

- Блокирование определенных типов трафика из LAN в Интернет, например, IRC (чат в реальном времени).
- Разрешение определенных видов трафика из Интернета к определенным хостам в LAN, например, синхронизация базы данных Lotus Notes.
- Разрешение доступа к веб-серверу всем, кроме ваших конкурентов.
- Разрешать использование определенных протоколов, например, Telnet, только авторизованным пользователям в LAN.

Логика работы таких правил заключается в сравнении IP-адреса источника, места назначения и типа протокола IP в проходящих пакетах с условиями, установленными администратором. Самостоятельно настраиваемые правила имеют приоритет и заменяют собой правила, действующие в P-2602 по умолчанию.

14.3 Логика правил

Примечание: Прежде чем приступить к настройке правил, тщательно ознакомьтесь со следующими подразделами.

14.3.1 Самоконтроль при создании правила

Сформулируйте назначение правила. Например: “это правило ограничивает все обращения по протоколу IRC из LAN в Интернет.” Или: “это правило позволяет удаленному серверу Lotus Notes синхронизироваться по Интернету с внутренним сервером Notes.”

1. В чем состоит назначение правила: разрешение или запрет трафика?
2. К какому направлению трафика применяется правило?
3. На какие службы IP оно распространяется?
4. К каким компьютерам в LAN (если это необходимо) должно применяться правило?
5. К каким компьютерам в Интернете должно применяться правило? Чем конкретнее изложено правило, тем лучше. Например, если трафик разрешается из Интернета в LAN, лучше разрешить доступ в LAN только с определенных машин в Интернете.

14.3.2 Аспекты безопасности

1. После того, как сформулирована логика правила, чрезвычайно важно рассмотреть аспекты безопасности, с которыми оно сопряжено:
2. Мешает ли это правило обращению пользователей из LAN к критически важным ресурсам в Интернете? Например, если блокируется IRC, нет ли пользователей, которым необходим этот вид сетевой службы?
3. Можно ли изменить правило так, чтобы оно было более определенным? Например, если IRC блокируется для всех пользователей, не окажется ли более эффективным правило, которое блокирует доступ только для определенных пользователей?
4. Если правило разрешает пользователям из Интернета обращаться к ресурсам в LAN, не создает ли оно уязвимости? Например, если разрешено обращаться из Интернета к портам FTP (TCP 20, 21) на компьютерах в LAN, пользователи из Интернета смогут соединяться с компьютерами, на которых работают FTP-серверы.
5. Не конфликтует ли данное правило с существующими правилами?
6. После проработки всех этих вопросов добавление правила сводится лишь к указанию необходимых параметров в соответствующих полях на экране веб-конфигуратора.

14.3.3 Основные поля для настройки правил

14.3.3.1 Action

Какое действие должно выполняться: **Drop** (отброс), **Reject** (запрет) или **Permit** (разрешение)?

Примечание: “Drop” означает, что межсетевой экран попросту отбрасывает пакет. “Reject” означает, что межсетевой экран отбрасывает пакет, возвращая отправителю ICMP-сообщение о недоступности адресата.

14.3.3.2 Service (Служба)

Выберите сетевую службу из списка **Service**. Если требуемая служба в списке отсутствует, необходимо сначала ее определить. Подробнее о предопределенных типах служб см. прилож. F на стр. 403 .

14.3.3.3 Source Address (Адрес источника)

Где находится источник соединения: в LAN или в WAN? Является ли он одиночным IP-адресом, диапазоном IP-адресов или подсетью?

14.3.3.4 Destination Address (Адрес получателя)

Где находится адресат соединения: в LAN или в WAN? Является ли он одиночным IP-адресом, диапазоном IP-адресов или подсетью?

14.4 Connection Direction (Направление соединения)

В этом разделе описаны примеры правил межсетевого экрана для соединений в направлении из LAN в WAN и из WAN в LAN.

Правила “LAN to LAN/Router”, “WAN to WAN/Router” и “DMZ to DMZ/Router” относятся к пакетам, входящим с соответствующего интерфейса (LAN, WAN или DMZ в указанном порядке). “LAN to LAN/Router” обозначает политики для пакетов, следующих из LAN на P-2602 (т.е. политики управления P-2602 через интерфейс LAN), и политики для пакетов, следующих из LAN в LAN (т.е. политики управления маршрутизацией между двумя подсетями в рамках LAN). Аналогичным образом политики “WAN to WAN/ Router” и “DMZ to DMZ/ Router” применяются к портам DMZ и WAN.

14.4.1 Правила для трафика из LAN в WAN

По умолчанию для трафика из LAN в WAN действует правило, разрешающее всем пользователям из LAN неограниченный доступ к WAN. Правила для трафика из LAN в WAN настраиваются для того, чтобы ограничить отдельным пользователям доступ к определенным службам в WAN. Правила для трафика из WAN в LAN

Правило по умолчанию для трафика из WAN в LAN блокирует все входящие соединения (из WAN в LAN). Если требуется разрешить определенным пользователям, находящимся в WAN, обращаться к вашей LAN, то для этого потребуется настроить собственные правила.

14.4.2 Предупреждения

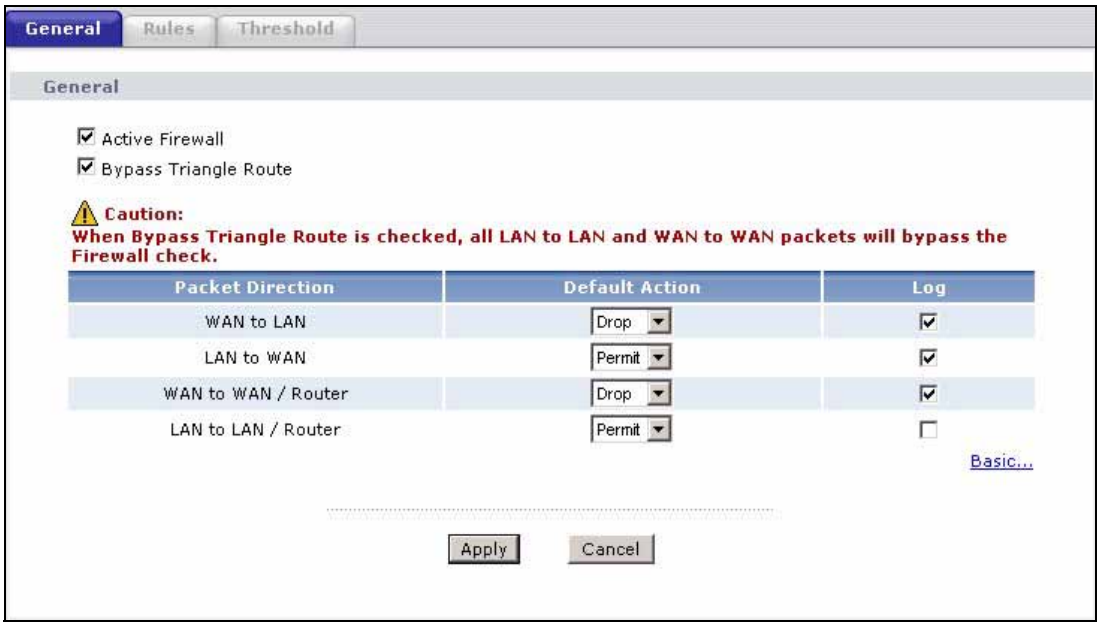
Предупреждения – это сообщения о событиях (например, об атаках), требующие немедленного внимания. На экране **Edit Rule** (см. рис. 105 на стр. 220). можно настроить генерацию предупреждений при выполнении определенных правил. Когда событие приводит к генерации предупреждения, на адрес электронной почты, указанный на экране **Log Settings**, немедленно высылается сообщение. Подробные указания см. в гл. 24 на стр. 323.

14.5 Общая политика межсетевого экрана

Чтобы перейти на следующий экран, выберите **Security > Firewall**. Активируйте межсетевой экран, установив флажок **Active Firewall**, как показано на следующем экране.

Подробное описание см. в разд. 13.1 на стр. 197.

Рис. 103 Межсетевой экран: общая политика



Поля изображённого выше экрана описаны в следующей таблице.

Таб. 70 Межсетевой экран: общая политика

ПОЛЕ	ОПИСАНИЕ
Active Firewall	Установите этот флажок, чтобы активировать межсетевой экран. Когда межсетевой экран активирован, P-2602 выполняет управление доступом и обеспечивает защиту от атак DoS (Denial of Service – отказ в обслуживании).
Bypass Triangle Route	Установите этот флажок, чтобы межсетевой экран P-2602 разрешал использование треугольной топологии маршрутизации в сети. См. приложение для дополнительной информации о топологии треугольного маршрута. **Примечание:** Разрешение асимметричных маршрутов позволяет пропускать трафик из WAN непосредственно к компьютерам в LAN, минуя маршрутизатор. прилож. H на стр. 409 содержит подробные сведения о треугольной топологии маршрутизации и способах решения связанных с ней проблем.
Packet Direction	В этом поле выбирается направление движения пакетов (**LAN to LAN / Router**, **LAN to WAN**, **WAN to WAN / Router**, **WAN to LAN)**. Правила межсетевого экрана сгруппированы по направлению прохождения пакетов, к которым они применяются. Например, **LAN to LAN / Router** означает пакеты, проходящие от компьютера/подсети в составе LAN к другому компьютеру/подсети на интерфейсе LAN P-2602 или к самому устройству P-2602.

Таб. 70 Межсетевой экран: общая политика (продолжение)

ПОЛЕ	ОПИСАНИЕ
Default Action	В раскрывающихся списках выберите действие по умолчанию, которое межсетевой экран должен выполнять над пакетами, проходящими в выбранном направлении и не подпадающими ни под одно из правил. Выберите **Drop**, чтобы отбрасывать пакеты, не возвращая отправителю пакет сброса TCP или ICMP-сообщение о недоступности адресата. Выберите **Reject**, чтобы отбрасывать пакеты и возвращать отправителю пакет сброса TCP (для TCP-пакетов) или ICMP-сообщение о недоступности адресата (для UDP-пакетов). Выберите **Permit**, чтобы разрешить прохождение пакетов.
Log	Отметьте этот флажок, чтобы оставлять запись в журнале (при выполнении вышеуказанного действия) для пакетов, проходящих в выбранном направлении и не соответствующих ни одному из настроенных вами правил.
Expand...	Нажмите эту кнопку, чтобы просмотреть дополнительную информацию.
Basic...	Нажмите эту кнопку, чтобы скрыть дополнительную информацию.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-2602.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

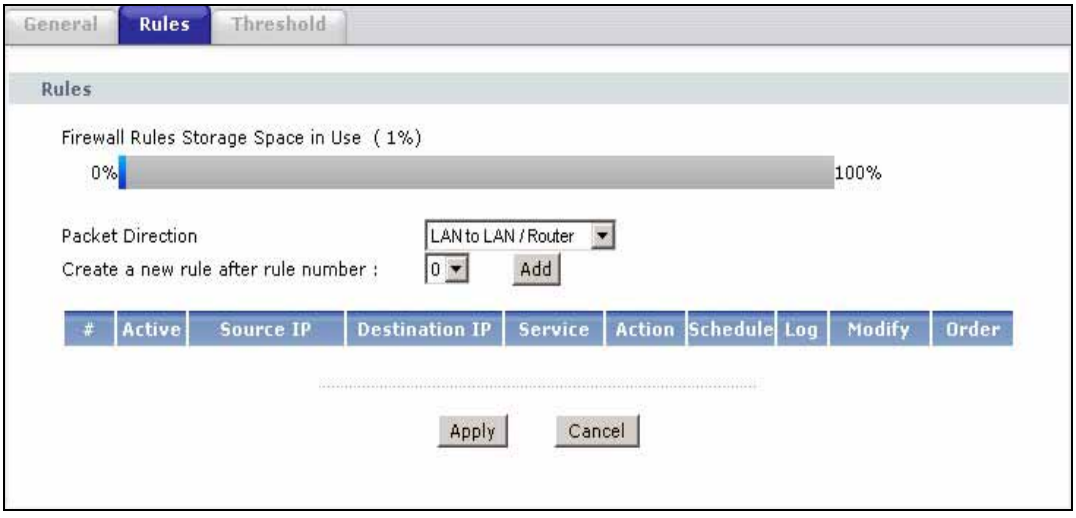
14.6 Сводка правил сетевого экрана

Примечание: Порядок следования правил имеет большое значение, поскольку правила применяются по очереди.

Для дополнительной информации см. разд. 13.1 на стр. 197.

Чтобы открыть следующий экран, выберите **Security > Firewall > Rules**. На нем приведен список настроенных правил сетевого экрана. Обратите внимание на порядок, в котором перечислены правила.

Рис. 104 Сводка правил сетевого экрана



Поля изображённого выше экрана описаны в следующей таблице.

Таб. 71 Сводка правил сетевого экрана

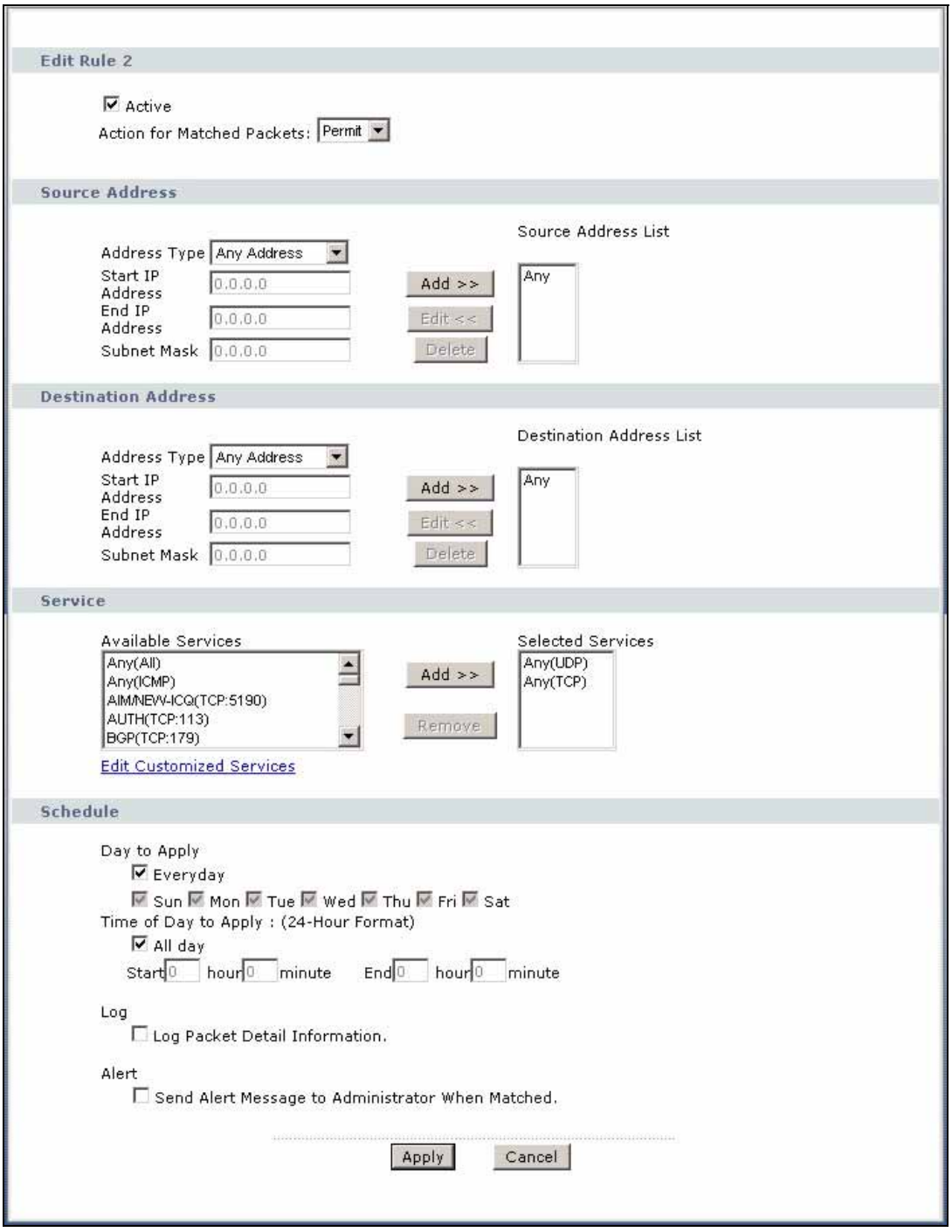
ПОЛЕ	ОПИСАНИЕ
Firewall Rules Storage Space in Use	Этот неизменяемый индикатор сообщает, сколько из объема памяти P-2602, отведенного под правила межсетевого экрана, используется в настоящий момент. Когда используется не более 80% объема, индикатор имеет зеленый цвет. При превышении 80% объема индикатор становится красным.
Packet Direction	Этот раскрывающийся список позволяет выбрать направление прохождения пакетов для настройки правил сетевого экрана.
Create a new rule after rule number	Выберите порядковый номер и нажмите **Add**, чтобы добавить новое правило под выбранным правилом. Например, если выбран номер 6, новое правило получит номер 7, а прежнее правило №7 (если оно существует) станет правилом №8.
	Следующие поля доступны только для чтения и содержат сводный перечень созданных правил, относящихся к трафику в выбранном направлении. Настроенные правила межсетевого экрана (приведенные ниже) имеют приоритет над общими настройками межсетевого экрана, выполненными на экране **General**.
#	В этом поле указан порядковый номер правила. Порядок следования правил имеет большое значение, поскольку правила применяются по очереди.
Active	В этом поле отображается состояние межсетевого экрана (активен / неактивен). Чтобы активировать правило, отметьте флажок. Чтобы деактивировать правило, снимите флажок.
Source IP	В этом раскрывающемся списке отображаются адреса или диапазоны адресов источников, к которым применяется данное правило межсетевого экрана. Следует помнить, что пустой адрес источника или получателя соответствует **любому** адресу.
Destination IP	В этом раскрывающемся списке отображаются адреса или диапазоны адресов получателей, к которым применяется данное правило межсетевого экрана. Следует помнить, что пустой адрес источника или получателя соответствует **любому** адресу.
Service	В этом раскрывающемся списке отображаются сетевые службы, к которым применяется данное правило межсетевого экрана. Дополнительные сведения см. в прилож.31 на стр. 403.
Action	В этом поле указывается действие, выполняемое межсетевым экраном: простое удаление пакетов (**Drop**), удаление пакетов с уведомлением отправителя посредством TCP-пакета “сброс” или ICMP-сообщения “адресат недоступен” (**Reject**) или разрешение пересылки пакета (**Permit**).
Schedule	В этом поле отображается наличие расписания: да (**Yes**) или нет (**No**).
Log	Это поле показывает, должен ли создаваться журнал для пакетов, подпадающих под данное правило: да (**Yes**) или нет (**No**).
Modify	Чтобы перейти на экран для редактирования правила, щелкните на значке редактирования. Для удаления существующего правила щелкните на значке удаления. Появится окно с просьбой подтвердить удаление. При удалении одного правила все последующие правила смещаются вверх.
Order	Щелкните на значке перемещения, чтобы вызвать поле **Move the rule to**. В поле **Move the rule to** введите номер, который должен быть присвоен правилу, и нажмите кнопку **Move**. Порядок следования правил имеет большое значение, поскольку правила применяются по очереди.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-2602.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

14.6.1 Настройка правил межсетевого экрана

Для дополнительной информации см. разд. 13.1 на стр. 197.

Чтобы вызвать показанный ниже экран, на экране **Rules** выберите порядковый номер правила и нажмите **Add**, либо щелкните на значке редактирования правила (**Edit**). Описание полей экрана см. в следующей таблице.

Рис. 105 Межсетевой экран: редактирование правила



Поля изображённого выше экрана описаны в следующей таблице.

Таб. 72 Межсетевой экран: редактирование правила

ПОЛЕ	ОПИСАНИЕ
Active	Выберите этот параметр, чтобы включить данное правило межсетевого экрана.
Action for Matched Packet	Этот раскрывающийся список позволяет выбрать действие, выполняемое над пакетами, подпадающими под правило: **Drop** – пакет удаляется, **Reject** – пакет удаляется с уведомлением отправителя посредством ICMP-сообщения “адресат недоступен”, **Permit** – пакет пропускается.
Source/Destination Address	
Address Type	Должно ли выбранное правило распространяться на один конкретный IP-адрес, на диапазон IP-адресов (например, с 192.168.1.10 по 192.169.1.50), на подсеть или на любые IP-адреса? Выберите вариант из раскрывающегося списка: **Single Address** (один адрес), **Range Address** (диапазон адресов), **Subnet Address** (адрес подсети) и **Any Address** (любой адрес).
Start IP Address	Введите в этом поле один IP-адрес или начальный IP-адрес диапазона.
End IP Address	Введите в этом поле конечный IP-адрес диапазона.
Subnet Mask	Введите в этом поле маску подсети, если это необходимо.
Add>>	Нажмите **Add >>**, чтобы добавить новый адрес в список **Source Address** или **Destination Address**. Можно добавить несколько адресов, диапазонов и/или подсетей.
Edit <<	Чтобы отредактировать существующий адрес источника или получателя, выберите его в списке и нажмите **Edit<<**.
Delete	Чтобы удалить существующий адрес источника или получателя, выберите его из расположенного выше списка **Source Address** или **Destination Address** и нажмите кнопку **Delete**.
Services	
Available/ Selected Services	Подробное описание доступных служб см. в прилож. F на стр. 403. Чтобы добавить службу в расположенный справа список выбранных служб (**Selected Services**), выберите ее слева в списке **Available Services** и нажмите кнопку **Add >>**. Чтобы удалить службу, выберите ее справа в списке **Selected Services**, затем нажмите **Remove**.
Edit Customized Service	Чтобы открыть экран для настройки новой службы, отсутствующей в предопределенном списке служб, пройдите по ссылке **Edit Customized Services**.
Schedule	
Day to Apply	Выберите, должно ли правило применяться каждый день (Everyday) или только в определенные дни недели.
Time of Day to Apply (24-Hour Format)	Выберите **All Day** (круглосуточно) или укажите время начала и окончания действия правила в формате “часы:минуты”.
Log	
Log Packet Detail Information	Этот флажок указывает, следует ли оставлять отметку в журнале для пакетов, соответствующих правилу. Чтобы настроить ведение соответствующих журналов в P-2602, перейдите на страницу **Log Settings** и выберите категорию журналов **Access Control**.
Alert	

Таб. 72 Межсетевой экран: редактирование правила (продолжение)

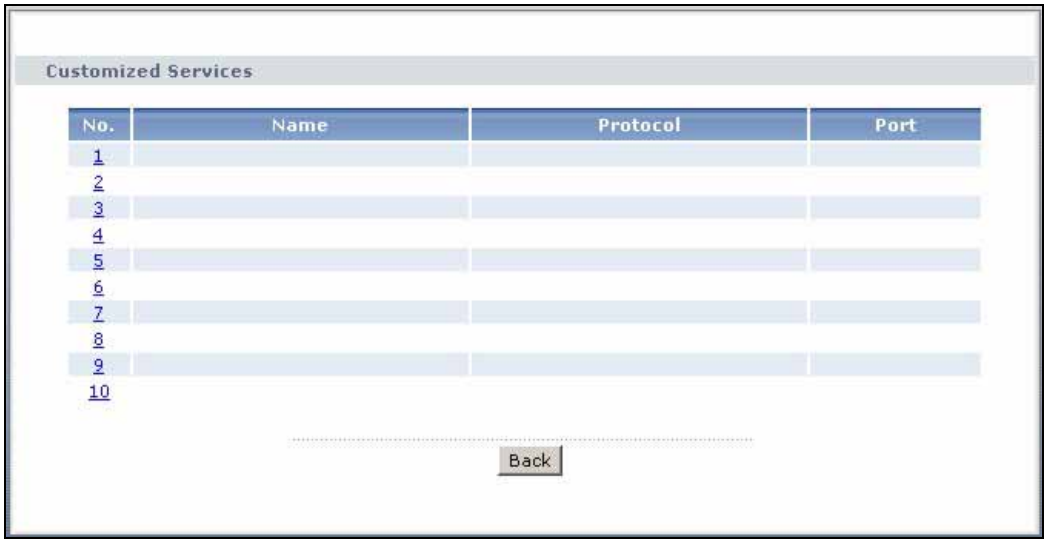
ПОЛЕ	ОПИСАНИЕ
Send Alert Message to Administrator When Matched	Отметьте этот флажок, чтобы устройство P-2602 генерировало предупреждение для пакетов, соответствующих правилу.
Back	Для возврата к предыдущему экрану нажмите кнопку **Back**.
Apply	Нажмите кнопку **Apply** для сохранения настроек и выхода из данного экрана.
Cancel	Чтобы закрыть экран, не сохраняя изменений, выберите **Cancel**.

14.6.2 Настройка собственных портов для сетевых служб

Настройка собственных сетевых служб и номеров портов, не предусмотренных в заводской конфигурации P-2602. Подробный перечень номеров портов и сетевых служб см. на сайте IANA (Комитета по цифровым адресам в Интернете). Примеры см. в прилож. F на стр. 403. Чтобы задать собственный номер порта для сетевой службы, во время редактирования правила сетевого экрана пройдите по ссылке **Edit Customized Services**. Откроется следующий экран.

Подробное описание см. в разд. 13.1 на стр. 197.

Рис. 106 Межсетевой экран: задание собственных сетевых служб



Поля изображённого выше экрана описаны в следующей таблице.

Таб. 73 Задание собственных сетевых служб

ПОЛЕ	ОПИСАНИЕ
No.	В этом поле отображается порядковый номер настроенной вами сетевой службы. Щелкните на номере службы, чтобы перейти на экран **Firewall Customized Services Config** для настройки или редактирования собственных сетевых служб.
Name	В этом поле отображается наименование настроенной вами сетевой службы.

Таб. 73 Задание собственных сетевых служб

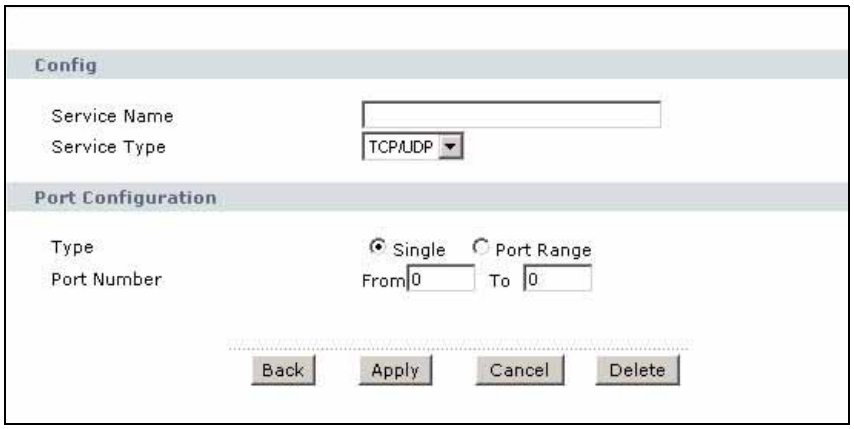
ПОЛЕ	ОПИСАНИЕ
Protocol	В этом поле отображается тип протокола IP (**TCP**, **UDP** или **TCP/UDP**), который соответствует настроенной вами сетевой службе.
Port	В этом поле отображается номер порта или диапазон портов, соответствующий настроенной вами сетевой службе.
Back	Нажмите кнопку **Back**, чтобы вернуться к экрану **Firewall Edit Rule**.

14.6.3 Задание собственной сетевой службы

Чтобы создать новый порт или отредактировать существующий, на экране **Firewall Customized Services** щелкните на порядковом номере порта. Откроется следующий экран.

Подробное описание см. в разд. 13.1 на стр. 197.

Рис. 107 Межсетевой экран: собственные сетевые службы



Поля изображённого выше экрана описаны в следующей таблице.

Таб. 74 Межсетевой экран: собственные сетевые службы

ПОЛЕ	ОПИСАНИЕ
Service Name	Укажите уникальное название для данного порта.
Service Type	Выберите IP-порт (**TCP**, **UDP** или **TCP/UDP**), который соответствует настроенному порту, выбранному в раскрывающемся списке.
Port Configuration	
Type	Выберите **Single**, чтобы указать только один порт, или **Range**, чтобы указать диапазон портов, соответствующих настраиваемой сетевой службе.
Port Number	Введите номер порта или диапазон портов, соответствующий настраиваемой сетевой службе.
Apply	Нажмите кнопку **Apply** для сохранения настроек и выхода из данного экрана.

Таб. 74 Межсетевой экран: собственные сетевые службы (продолжение)

ПОЛЕ	ОПИСАНИЕ
Cancel	Чтобы вернуться к прежним настройкам, нажмите **Cancel**.
Delete	Чтобы удалить существующее правило, нажмите **Delete**.

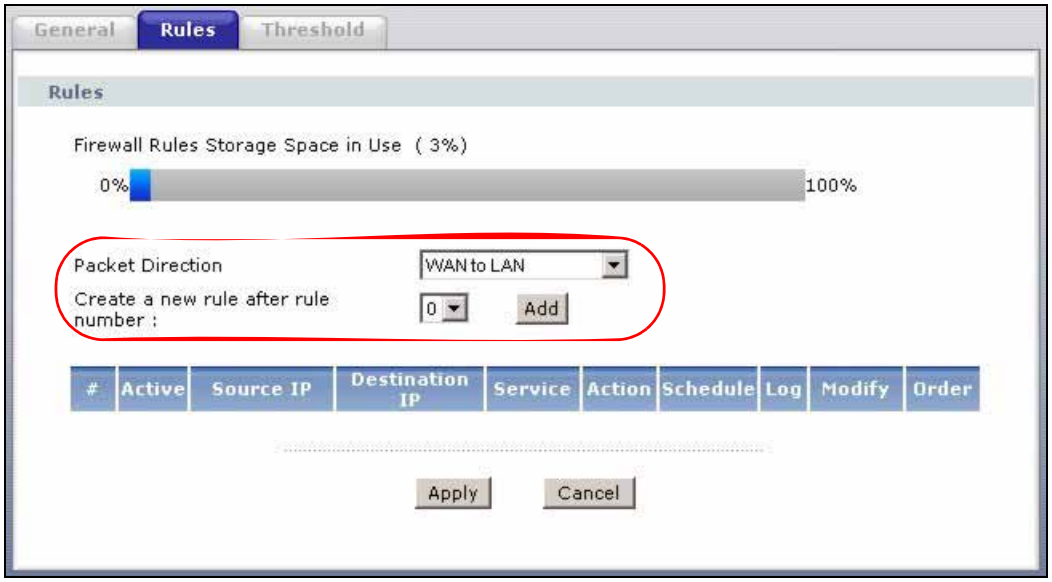
14.7 Пример правила для межсетевого экрана

Следующее правило межсетевого экрана разрешает соединения из Интернета посредством вымышленной службы “MyService”.

1 Выберите **Security > Firewall** > **Rules**.

2 В поле **Packet Direction** выберите **WAN to LAN**.

Рис. 108 Пример настройки межсетевого экрана: правила



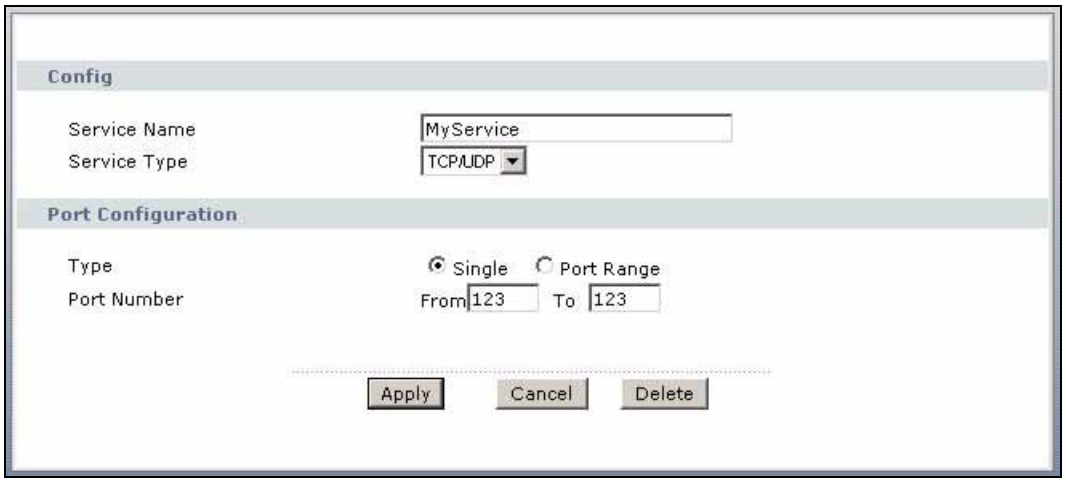
3 На экране **Rules** выберите порядковый номер правила, за которым должно следовать вновь добавляемое правило. Например, если выбран номер 6, новое правило получит номер 7, а прежнее правило №7 (если оно существует) станет правилом №8.

4 Нажмите кнопку **Add**, чтобы вызвать экран настройки правила межсетевого экрана.

5 На экране **Edit Rule** перейдите по ссылке **Edit Customized Services** на экран **Customized Service**.

6 Вызовите экран **Customized Services Config**, щелкнув на порядковом номере, выполните на нем настройки, показанные ниже, и нажмите **Apply**.

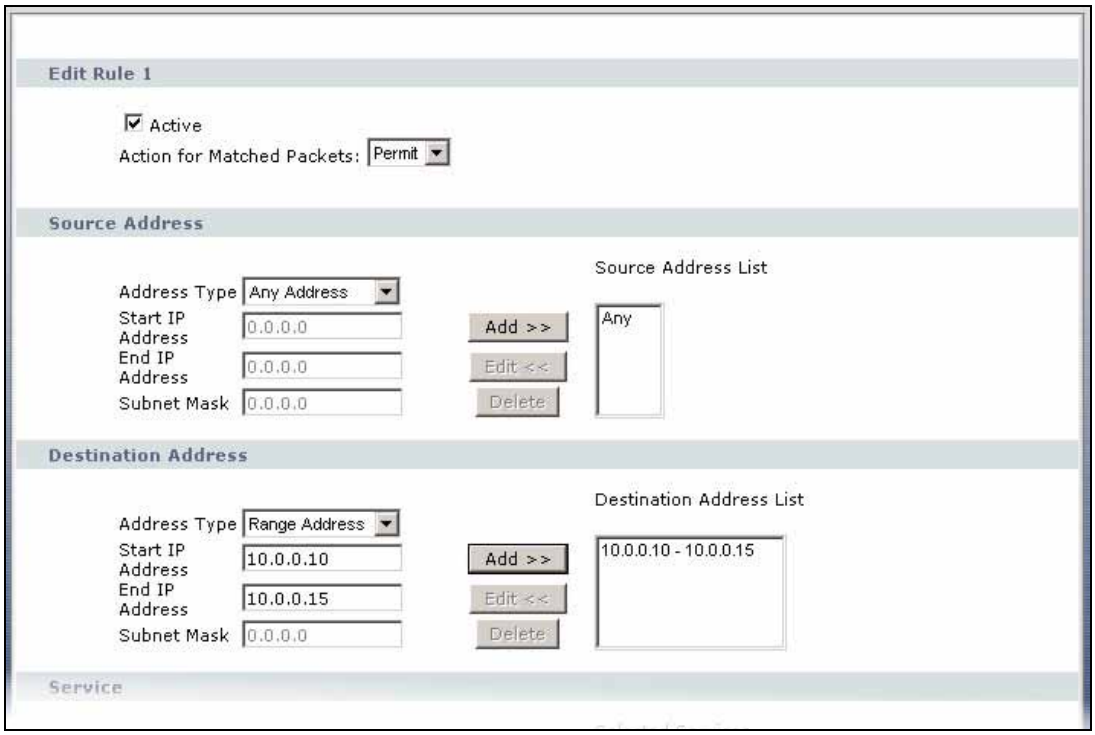
Рис. 109 Пример редактирования собственного номера порта



7 В поле **Destination Address** выберите **Any** и нажмите **Delete**.

8 Руководствуясь приведенным ниже образцом, настройте поля для получателя пакетов, и нажмите **Add**.

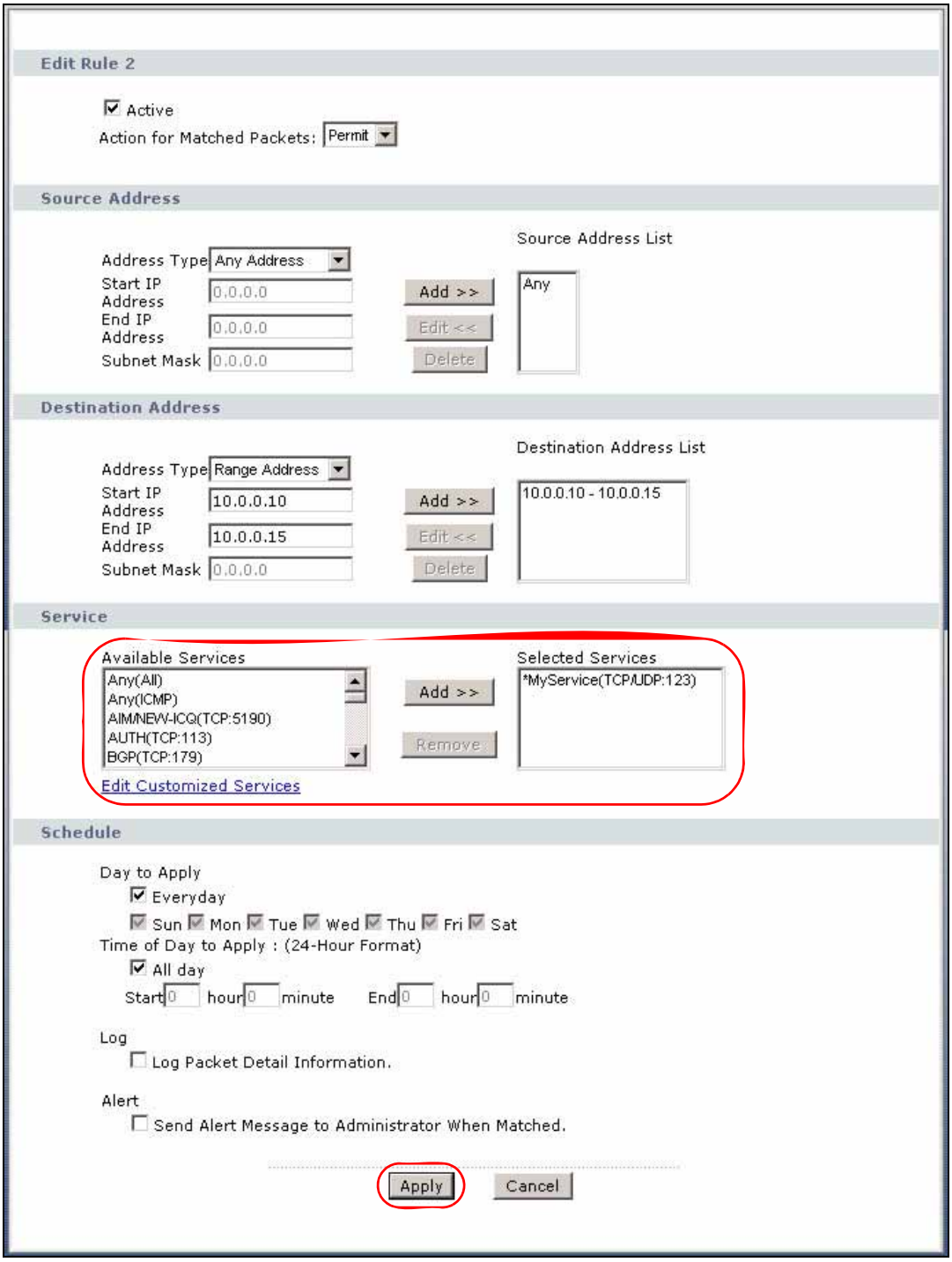
Рис. 110 Пример настройки межсетевого экрана. Редактирование правил: адрес получателя



9 Настройте сетевые службы, перемещая их между списками **Available Services** и **Selected Services** с помощью кнопок **Add >>** и **Remove**. Закончив настройку, нажмите **Apply**.

Примечание: В списках **Services** и **Rules** перед названиями сетевых служб, заданных пользователями, стоит знак “*”.

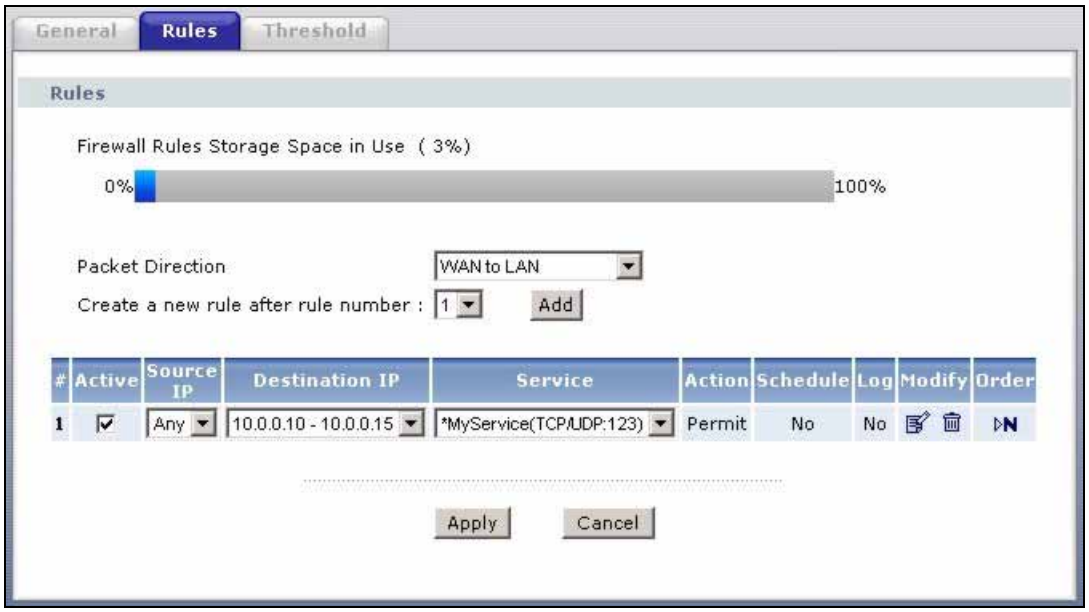
Рис. 111 Пример настройки межсетевого экрана. Редактирование правил: выбор собственных сетевых служб



По завершении настройки данного правила межсетевого экрана экран **Rules** будет иметь следующий вид.

Правило 1 позволяет посредством службы “MyService” подключаться из WAN к IP-адресам в LAN в диапазоне от 10.0.0.10 до 10.0.0.15.

Рис. 112 Пример настройки межсетевого экрана: правила: MyService



14.8 Пороговые значения для защиты от DoS

Для защиты от DoS-атак P-2602 в используется принцип пороговых уровней, определяющих предел, по превышении которого частично открытые сеансы отменяются. Эти пороговые значения действуют глобально для всех сеансов.

Можно использовать значения по умолчанию или изменить их в соответствии с собственными требованиями к безопасности.

Настройка пороговых значений описана в разд. 14.8.3 на стр. 229.

14.8.1 Пороговые значения

Эти параметры следует корректировать, если сеть не работает должным образом. Предварительно следует проверить счетчики межсетевого экрана. Значения по умолчанию подходят для большинства небольших офисов. Пороговые значения выбираются с учетом следующих факторов:

- Максимальное число открытых сеансов.
- Минимальный резерв серверов в вашей локальной сети.
- Вычислительная мощность серверов в вашей локальной сети.
- Пропускная способность сети.
- Типы трафика для определенных серверов.

Если в свете любого из этих факторов ваша сеть оказывается медленнее, чем среднестатистическая (особенно если имеются серверы с малой производительностью или высокой загруженностью), то значения по умолчанию следует уменьшить.

Прежде чем продолжить настройку правил межсетевого экрана, необходимо завершить изменения пороговых значений.

14.8.2 Частично открытые сеансы

Необычно высокое число частично открытых сеансов (как абсолютное число, так и частота поступления) может говорить об имеющей место атаке с целью спровоцировать отказ в обслуживании. Для TCP, понятие “частично открытый” означает, что сеанс не достиг установленного состояния – трехэтапное установление соединения TCP еще не было завершено (см. рис. 99 на стр. 201). Для UDP частично открытыми сеансами считаются те, в которых межсетевой экран не обнаружил встречного трафика.

P-2602 измеряет как общее число частично открытых сеансов в данный момент времени, так и частоту попыток установления сеанса. Для обоих протоколов отслеживается общее число и частота возникновения частично открытых сеансов. Измерения производятся раз в минуту.

Когда число существующих частично открытых сеансов превышает порог (**max-incomplete high**), P-2602 начинает удалять частично открытые сеансы, освобождая ресурсы для новых запросов на соединение. P-2602 продолжает удалять частично открытые сеансы, пока это необходимо, т.е. пока число существующих частично открытых сеансов не опустится ниже другого порога (**max-incomplete low**).

Когда частота накопления частично открытых сеансов превышает порог (**one-minute high**), P-2602 начинает удалять частично открытые сеансы, освобождая ресурсы для новых запросов на соединение. P-2602 продолжает удалять частично открытые сеансы, пока это необходимо, т.е. пока частота накопления частично открытых сеансов не опустится ниже другого порога (**one-minute low**). Частота – это число новых попыток, выявленных в последнем одноминутном периоде измерений.

14.8.2.1 Задание верхнего порога частично открытых сеансов TCP и времени блокирования

Необычно высокое число частично открытых сеансов с одним и тем же адресатом может говорить об имеющей место атаке с целью спровоцировать отказ в обслуживании.

Когда число существующих частично открытых сеансов превышает порог (**TCP Maximum Incomplete**), P-2602 начинает удалять частично открытые сеансы, руководствуясь одним из следующих методов.

- Если величина **Blocking Time** равна 0 (значение по умолчанию), P-2602 при каждом новом запросе на подключение к хосту будет удалять самый старый из частично открытых сеансов. Это позволяет гарантировать, что число частично открытых сеансов с конкретным хостом никогда не превысит порог.

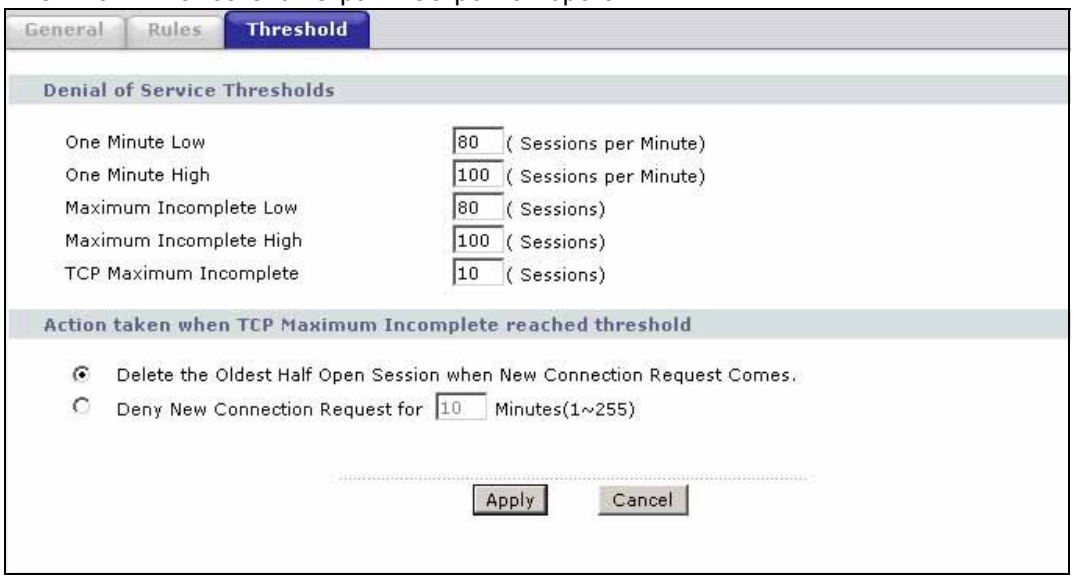
- Если величина **Blocking Time** больше 0, P-2602 блокирует все новые запросы на подключение к данному хосту, оставляя серверу время для обработки существующих соединений. P-2602 продолжает блокировать все вновь поступающие запросы на подключение, пока не истечет задержка **Blocking Time** .

14.8.3 Настройка пороговых значений для межсетевого экрана

При превышении порога **TCP Maximum Incomplete** P-2602 также направляет предупреждения. Глобальные значения порога и времени блокировки применяются ко всем TCP-соединениям.

Чтобы открыть следующий экран, выберите **Firewall**, затем – **Threshold**.

Рис. 113 Межсетевой экран: настройка порогов



Поля изображённого выше экрана описаны в следующей таблице.

Таб. 75 Межсетевой экран: настройка порогов

ПОЛЕ	ОПИСАНИЕ	ЗНАЧЕНИЯ ПО УМОЛЧАНИЮ
Denial of Service Thresholds		
One Minute Low	Это частота накопления частично открытых сеансов, при которой межсетевой экран прекращает удалять частично открытые сеансы. P-2602 продолжает удалять частично открытые сеансы, пока это необходимо, т.е. пока частота накопления частично открытых сеансов не опустится ниже этого порога.	80 существующих частично открытых сеансов.

Таб. 75 Межсетевой экран: настройка порогов (продолжение)

ПОЛЕ	ОПИСАНИЕ	ЗНАЧЕНИЯ ПО УМОЛЧАНИЮ
One Minute High	Это частота накопления частично открытых сеансов, при которой межсетевой экран начинает удалять частично открытые сеансы. Когда частота накопления частично открытых сеансов превышает этот порог, P-2602 начинает удалять частично открытые сеансы, освобождая ресурсы для новых запросов на соединение.	100 частично открытых сеансов в минуту. При указанных выше значениях параметров P-2602 начинает удалять частично открытые сеансы, когда за последнюю минуту обнаруживается более 100 попыток установки сеанса, и прекращает удалять частично открытые сеансы, если за последнюю минуту число обнаруженных попыток установления сеанса не превышает 80.
Maximum Incomplete Low	Это число существующих частично открытых сеансов, при котором межсетевой экран прекращает удалять частично открытые сеансы. P-2602 продолжает удалять частично открытые сеансы, пока это необходимо, т.е. пока число существующих частично открытых сеансов не опустится ниже данного порога.	80 существующих частично открытых сеансов.
Maximum Incomplete High	Это число существующих частично открытых сеансов, при котором межсетевой экран начинает удалять частично открытые сеансы. Когда число существующих частично открытых сеансов превышает этот порог, P-2602 начинает удалять частично открытые сеансы, освобождая ресурсы для новых запросов на соединение. Выбранное значение **Maximum Incomplete High** не должно быть ниже текущего значения **Maximum Incomplete Low**.	100 существующих частично открытых сеансов. С приведенными выше значениями параметров P-2602 начинает удалять частично открытые сеансы, когда число существующих частично открытых сеансов превышает 100, и прекращает их удалять, когда число существующих частично открытых сеансов падает ниже 80.
TCP Maximum Incomplete	Это число существующих частично открытых сеансов TCP с одинаковым IP-адресом адресата, при котором межсетевой экран начинать удалять частично открытые сеансы с данным хостом. Введите число от 1 до 256. При небольших сетях, медленных системах или ограниченной пропускной способности следует выбирать меньшие значения.	30 существующих частично открытых сеансов TCP.
Action taken when the TCP Maximum Incomplete reached threshold		
Delete the Oldest Half Open Session when New Connection Request Comes.	Выберите этот переключатель, чтобы при поступлении нового запроса на подключения удалять наиболее старый частично открытый сеанс.	
Deny New Connection Request for	Выберите этот переключатель и укажите период, в течение которого P-2602 будет блокировать новые запросы на подключение, если превышен порог **TCP Maximum Incomplete**. Продолжительность блокировки указывается в минутах (от 1 до 256).	
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-2602.	
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.	

Глава 15
Фильтрация содержания

В этой главе описывается настройка фильтрации содержания.

15.1 Общие сведения о фильтрации содержания

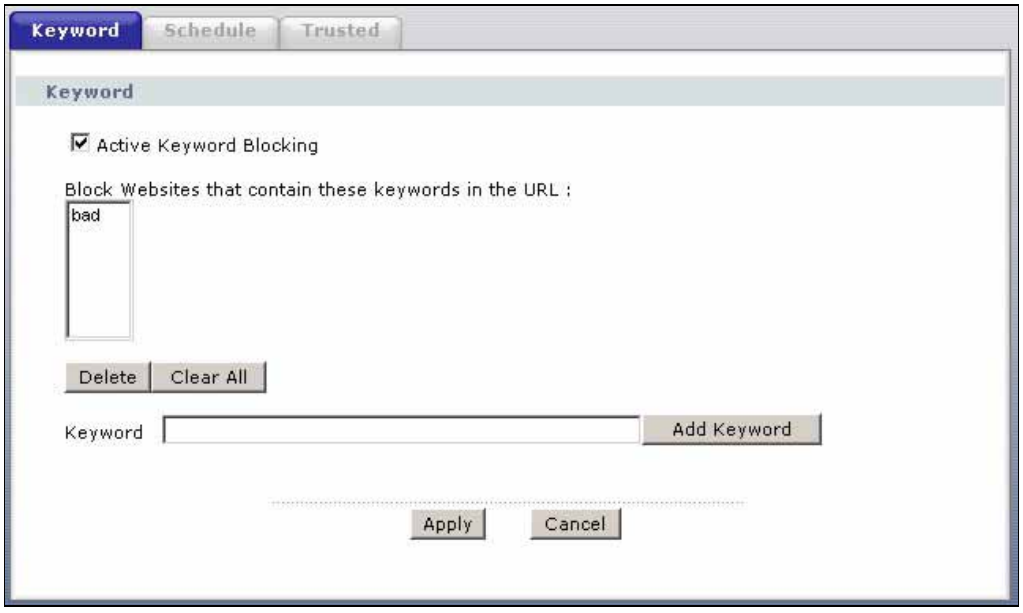
Фильтрация содержания позволяет задать и применять политику доступа к Интернету, отвечающую вашим задачам. Фильтрация содержания дает возможность блокировать доступ к веб-сайтам, URL которых содержит определенные (задаваемые вами) ключевые слова. Можно задать расписание, по которому P-2602 будет применять фильтрацию содержания. Также можно указать доверенные IP-адреса в локальной сети, для которых P-2602 не будет применять фильтрацию содержания.

15.2 Настройка блокирования по ключевым словам

Этот экран служит для блокирования доступа к сайтам по определенным ключевым словам в URL. Например, если вы задали ключевое слово “bad”, P-2602 блокирует все сайты, в URL которых содержится это слово (например, http://www.website.com/bad.html), даже если сайт отсутствует в списке фильтров.

Чтобы разрешить P-2602 блокировать веб-сайты по ключевым словам в URL, выберите **Security > Content Filter**. Появится изображенный ниже экран.

Рис. 114 Фильтрация содержания: настройка ключевых слов



Поля соответствующего экрана описаны в следующей таблице.

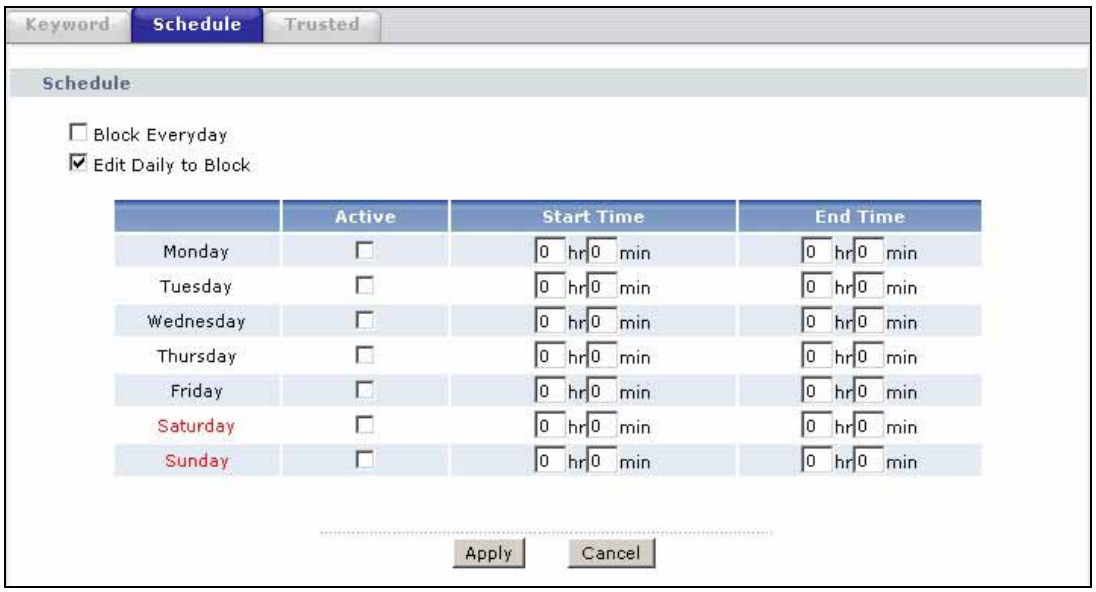
Таб. 76 Фильтрация содержания: настройка ключевых слов

ПОЛЕ	ОПИСАНИЕ
Active Keyword Blocking	Установите этот флажок, чтобы включить данную функцию.
Block Websites that contain these keywords in the URL:	В этом поле содержится список всех ключевых слов, по которым в P-2602 настроено блокирование.
Delete	Чтобы удалить ключевое слово, выделите его в списке и нажмите кнопку **Delete**.
Clear All	Нажмите кнопку **Clear All**, чтобы удалить все ключевые слова из списка.
Keyword	Введите ключевое слово в этом поле. Можно использовать любые символы, допустимая длина – до 127 знаков ASCII. Использование символов групповых подстановок (wildcard) не допускается.
Add Keyword	Введя ключевое слово, нажмите **Add Keyword**, чтобы его добавить. Повторите эту операцию для добавления других ключевых слов. Максимально допустимое число ключевых слов – 64. При попытке обращения к веб-странице, содержащей ключевое слово, вы получите сообщение о том, что фильтр содержания заблокировал ваш запрос.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-2602.
Cancel	Чтобы вернуться к прежним настройкам, нажмите **Cancel**.

15.3 Настройка графика

Чтобы ограничить дни и периоды суток, в которые P-2602 будет выполнять фильтрацию содержания, выберите **Security > Content Filter** > **Schedule**. Появится изображенный ниже экран.

Рис. 115 Фильтрация содержания: график



Поля изображённого выше экрана описаны в следующей таблице.

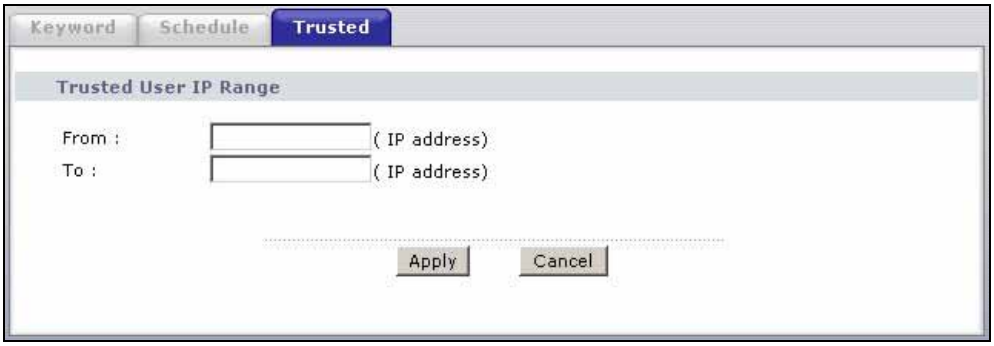
Таб. 77 Фильтрация содержания: график

ПОЛЕ	ОПИСАНИЕ
Schedule	Выберите **Block Everyday**, чтобы применять фильтрацию содержания каждый день. В противном случае выберите **Edit Daily to Block** и укажите дни недели (или выберите все дни), а также время суток, в которое должна действовать фильтрация.
Active	Отметьте этот флажок, чтобы активировать фильтрацию содержания в выбранный день.
Start TIme	Введите время начала фильтрации содержания в формате “часы-минуты”.
End Time	Введите время окончания фильтрации содержания в формате “часы-минуты”.
Apply	Нажмите **Apply (Применить)** для сохранения изменений.
Cancel	Чтобы вернуться к прежним настройкам, нажмите **Cancel**.

15.4 Настройка адресов доверенных компьютеров

Чтобы устройство P-2602 не применяло фильтрацию содержания к определенным пользователям, выберите **Security > Content Filter** > **Trusted**. Появится изображенный ниже экран.

Рис. 116 Фильтрация содержания: доверенный компьютер



Поля изображённого выше экрана описаны в следующей таблице.

Таб. 78 Фильтрация содержания: доверенный компьютер

ПОЛЕ	ОПИСАНИЕ
Trusted User IP Range	
From	Введите IP-адрес компьютера в локальной сети (или начальный адрес в диапазоне IP-адресов), который будет освобожден от действия фильтрации содержания.
To	Введите конечный адрес в диапазоне IP-адресов локальной сети, освобождаемых от действия фильтрации содержания. Если исключение делается только для одного компьютера, оставьте это поле пустым.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-2602.
Cancel	Чтобы вернуться к прежним настройкам, нажмите **Cancel**.

Глава 16
Введение в IPSec

В этой главе рассматриваются основы построения VPN-сетей по технологии IPSec.

16.1 Краткий обзор VPN

VPN (виртуальная частная сеть) реализует защищённый обмен данными между двумя физическими объектами, не требуя затрат на организацию между ними выделенной линии. Защищённая VPN сочетает в себе сетевые туннели, средства шифрования, аутентификации, контроля доступа и аудита, обеспечивая пересылку трафика через Интернет или другую незащищённую сеть, в которой для обмена данными используется семейство протоколов TCP/IP.

16.1.1 IPSec

IPSec (Internet Protocol Security) это реализация VPN, построенная на основе стандартов и предлагающая гибкие решения для защищенной передачи данных по сети общего пользования, такой как Интернет. В IPSec применяется ряд стандартизированных криптографических технологий, обеспечивающих конфиденциальность, целостность информации и аутентификацию на уровне IP.

16.1.2 Ассоциация безопасности

Ассоциация безопасности (SA) представляет собой соглашение между двумя сторонами, указывающее, какие параметры безопасности (ключи, алгоритмы) будут ими использоваться.

16.1.3 Другие термины

16.1.3.1 Шифрование

Шифрование – это математическая операция, которая преобразует данные из “открытого” (читаемого) текста в зашифрованный (скремблированный) текст посредством т.н. ключа. Ключ и открытый текст подаются процедуре шифрования, которая выполняет скремблирование, формируя защищенное зашифрованное сообщение. Расшифровка противоположна операции шифрования: она представляет собой математическую операцию, которая преобразует зашифрованный текст в открытый. Для расшифровки также требуется ключ.

Рис. 117 Шифрование и расшифровка

16.1.3.2 Конфиденциальность данных

Отправитель IPSec может зашифровать пакеты перед их передачей по сети.

16.1.3.3 Целостность информации

Получатель IPSec может проверять достоверность пакетов, получаемых от отправителя, чтобы удостовериться, что данные не были изменены в процессе передачи.

16.1.3.4 Аутентификация источника данных

Получатель IPSec может проверять источник пакетов IPSec. Это операция реализована на базе контроля целостности информации.

16.1.4 Применения VPN

P-2602 поддерживает следующие применения VPN.

- Объединение двух или нескольких частных сетей

  Возможность подключения филиалов и деловых партнеров через Интернет с существенной экономией и большей производительностью по сравнению с прокладыванием выделенных каналов между объектами.

- Доступ к сетевым ресурсам при включенной трансляции сетевых адресов (NAT)

  При включении NAT удаленные пользователи не имеют возможности обращаться к хостам в сети LAN, если конкретный хост с конкретным протоколом не указан в качестве общедоступного сервера. Поскольку туннель VPN заканчивается в сети LAN, отдаленные пользователи смогут получить доступ ко всем компьютерам, использующим частные IP-адреса в LAN.

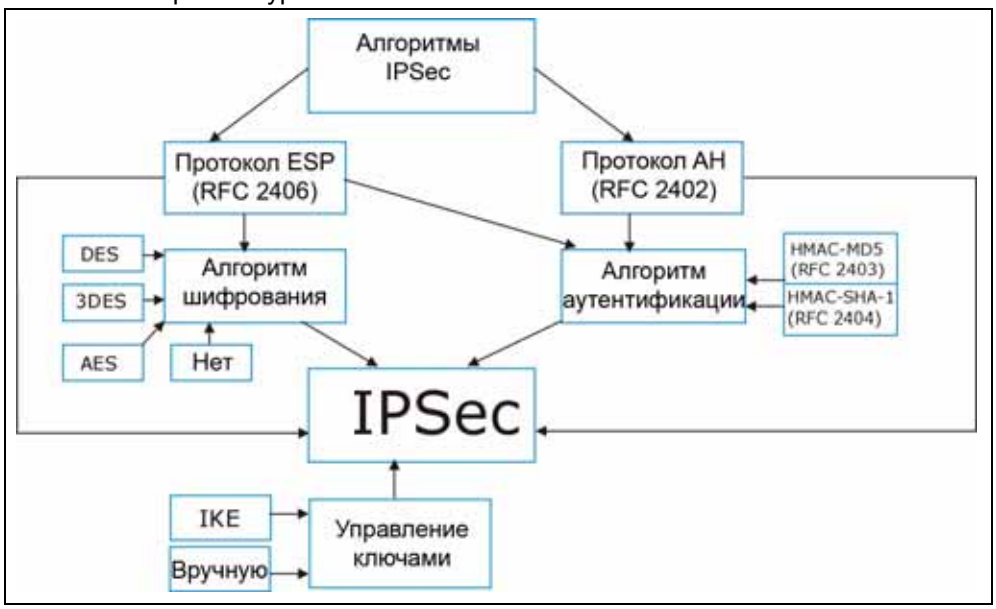
- Неподдерживаемые IP-приложения

  VPN-туннель позволяет обеспечить поддержку для новых, неподдерживаемых IP-приложений. Пример применения VPN см. в гл. 1 на стр. 39.

16.2 Архитектура IPSec

Ниже представлена общая схема архитектуры IPSec.

Рис. 118 Архитектура IPSec



16.2.1 Алгоритмы IPSec

Протоколы **ESP** (защищенное сокрытие содержания, RFC 2406) и **AH** (заголовок аутентификации, RFC 2402) описывают форматы пакетов и устанавливают общие стандарты в отношении структуры пакета (включая алгоритмы реализации).

Алгоритм шифрования описывает использование методик шифрования, в частности DES (стандарт шифрования данных – Data Encryption Standard) и Triple DES (тройной DES).

Алгоритмы аутентификации, HMAC-MD5 (RFC 2403) и HMAC-SHA-1 (RFC 2404), обеспечивают механизм аутентификации для протоколов **AH** и **ESP**. Подробности см. в разд. 17.2 на стр. 241.

16.2.2 Управление ключами

Управление ключами позволяет выбрать механизм работы с ключами для построения VPN: IKE (ISAKMP) или ручная настройка ключей.

16.3 Инкапсуляция

VPN на основе IPSec поддерживают два режима работы: **транспортный** и **туннельный**.

Рис. 119 Инкапсуляция IPSec в транспортном и туннельном режимах

16.3.1 Транспортный режим

Транспортный режим используется для защиты протоколов верхнего уровня и касается только данных в пакете IP. В **транспортном** режиме пакет IP содержит тип протокола безопасности (**AH** или **ESP**), указываемый после исходного заголовка IP и дополнительных полей, но перед любыми протоколами верхнего уровня, содержавшимися в пакете (TCP или UDP).

В случае **ESP** защита применяется только к протоколам верхнего уровня, содержащимся в пакете. Информация в заголовке IP и дополнительные поля в процессе аутентификации не используются, поэтому исходный IP-адрес не может быть проверен при контроле целостности данных.

Если в качестве протокола безопасности используется **AH**, то защита распространяется на остальные поля заголовка IP, а использование фрагментов оригинального заголовка IP в процессе хеширования позволяет проверить целостность всего пакета.

16.3.2 Туннельный режим

В **туннельном** режиме инкапсулируется весь пакет IP, что обеспечивает его защищенную передачу. **Туннельный** режим необходим для шлюзов, обеспечивающих доступ к внутренним системам. **Туннельный** режим фактически представляет собой IP-туннель, дополненный средствами аутентификации и шифрования. Этот режим используется наиболее часто. **Туннельный** режим требуется для соединений между шлюзами и между хостом и шлюзом. При связи в **туннельном** режиме используются два набора заголовков IP:

- **Внешний заголовок** : Внешний заголовок IP содержит IP-адрес целевого шлюза VPN.
- **Внутренний заголовок** : Внутренний заголовок IP содержит IP-адрес конечного получателя, находящегося за шлюзом VPN. Протокол безопасности указывается после внешнего заголовка IP и перед внутренним заголовком IP.

16.4 IPSec и NAT

Ознакомьтесь с этим разделом, если вы используете IPSec на хосте, находящимся за P-2602.

NAT несовместим с протоколом **AH** как в **транспортном**, так и в **туннельном** режиме. В VPN-сетях на основе IPSec, использующих протокол **AH**, исходящий пакет снабжается цифровой подписью, которая рассчитывается для заголовка и полезной нагрузки, и приписывается к пакету в виде хеш-значения. При использовании протокола **AH** содержимое пакета (полезная нагрузка) не шифруется.

NAT-устройство между оконечными точками IPSec заменит адрес источника или получателя самостоятельно выбранным адресом. VPN-устройство на принимающей стороне для проверки целостности поступающего пакета вычислит собственное хеш-значение и сообщит о том, что оно не совпало со значением, приложенным к полученному пакету. Поскольку VPN-устройству на принимающей стороне неизвестно о наличии промежуточного NAT, оно действует так, как если бы была выявлена попытка злонамеренного изменения данных.

При использовании IPSec с **ESP** в **туннельном** режиме весь оригинальный пакет (включая заголовки) инкапсулируется в новый пакет IP. Адресом источника нового пакета IP является выходной адрес шлюза-отправителя VPN, а адресом получателя пакета – входной адрес устройства VPN на принимающей стороне. При использовании протокола **ESP** с аутентификацией производится шифрование содержимого пакета (в данном случае шифруется весь исходный пакет). Зашифрованное содержимое, но не новые заголовки, снабжается электронной подписью, дополняемой к пакету.

ESP в **туннельном** режиме с аутентификацией совместим с NAT, так как проверка целостности производится для совокупности исходного заголовка и исходной полезной нагрузки, а оба этих параметра не изменяются при прохождении NAT-устройства.

ESP в **транспортном** режиме с аутентификацией несовместим с NAT.

Таб. 79 Взаимодействие VPN и NAT

ПРОТОКОЛ БЕЗОПАСНОСТИ	РЕЖИМ	NAT
AH	Транспортный	Нет
AH	Туннельный	Нет
ESP	Транспортный	Нет
ESP	Туннельный	Да

Глава 17
Экраны VPN

В этой главе рассмотрены экраны VPN. В гл. 24 на стр. 323 описан просмотр журналов, а в приложении описан формат журналов IPSec.

17.1 Обзор VPN/IPSec

Экраны, описанные в этой главе, служат для настройки правил для VPN-соединений, а также для управления VPN-соединениями.

17.2 Алгоритмы IPSec

Протоколы **ESP** и **AH** необходимы для создания ассоциаций безопасности (SA), лежащих в основе VPN на базе IPSec. SA строится на аутентификации, обеспечиваемой протоколами **AH** и **ESP**. Основная задача управления ключами – установление и поддержание SA между различными системами. После установления SA может начинаться транспортировка данных.

17.2.1 Протокол AH (заголовок аутентификации)

Протокол **AH** (RFC 2402) отвечает требованиям целостности, аутентификации, контроля последовательности (защиты от внедрения посторонних данных), и однозначной идентификации отправителя, но не предназначен обеспечивать конфиденциальность – эту задачу выполняет **ESP**.

В тех применениях, где конфиденциальность не требуется или не санкционирована государственными ограничениями в области криптографии, **AH** может использоваться для контроля целостности. Такая реализация не защищает информацию от разглашения, но позволит реализовать проверку целостности информации и аутентификацию отправителя.

17.2.2 Протокол ESP (Encapsulating Security Payload – защищенное сокрытие содержания)

Протокол **ESP** (RFC 2406) реализует шифрование в дополнение к функциям, обеспечиваемым **AH**. Возможности **ESP** по аутентификации ограничены по сравнению с **AH** из-за того, что в процессе аутентификации не участвуют сведения из заголовка IP. Тем не менее, **ESP** будет достаточен, если аутентификация необходима только для протоколов верхнего уровня.

Дополнительная возможность **ESP** – дополнение полезной нагрузки фиктивными данными, за счет чего скрывается истинный размер передаваемого пакета и обеспечивается повышенная защищенность.

Таб. 80 Сравнение AH и ESP

	ESP	**AH**
ШИФРОВАНИЕ		
	DES (по умолчанию) Стандарт шифрования данных (DES) – широко используемый метод шифрования данных с помощью секретного ключа. В стандарте DES к каждому 64-битному блоку данных применяется 56-битный ключ.	**MD5** (по умолчанию) В алгоритме MD5 (Message Digest 5) для аутентификации пакетов используется 128-битная свёртка.
	3DES Тройной DES (3DES) – это модифицированный алгоритм DES, реализуемый в три прохода с тремя отдельными ключами (3 x 56 = 168 битов), и обладающий вдвое большей криптостойкостью по сравнению с DES.	**SHA1** В алгоритме SHA1 (Secure Hash Algorithm) для аутентификации пакетов используется 160-битная свёртка.
	AES Усовершенствованный стандарт шифрования (AES) - более новый алгоритм, также использующий секретный ключ. В данной реализации AES к каждому 128-битному блоку данных применяется 128-битный ключ. AES обладает большим быстродействием, чем 3DES.	
	Чтобы настроить туннель 2-й фазы без шифрования, выберите **NULL**.	
АУТЕНТИФИКАЦИЯ	**MD5** (по умолчанию) В алгоритме MD5 (Message Digest 5) для аутентификации пакетов используется 128-битная свёртка.	**MD5** (по умолчанию) В алгоритме MD5 (Message Digest 5) для аутентификации пакетов используется 128-битная свёртка.
	SHA1 В алгоритме SHA1 (Secure Hash Algorithm) для аутентификации пакетов используется 160-битная свёртка.	**SHA1** В алгоритме SHA1 (Secure Hash Algorithm) для аутентификации пакетов используется 160-битная свёртка.
	Для минимальной защиты можно применять метод **MD5**, а для наибольшей безопасности следует использовать **SHA1**.	

17.3 Поле “My IP Address”

В поле “My IP Address” указывается IP-адрес P-2602 на стороне WAN. Если значение этого поля будет изменено, устройство P-2602 должно будет перестроить VPN-туннель.

Если в этом поле введен адрес **0.0.0.0**, действует следующий алгоритм:

- Для настройки VPN-туннеля P-2602 использует текущий IP-адрес (статический или динамический), присвоенный P-2602 в сети WAN (static or dynamic).
- При обрыве соединения с WAN P-2602 использует для туннеля VPN IP-адрес резервирования через коммутируемый доступ или IP-адрес в LAN, если используется переадресация трафика. Подробнее о резервировании через коммутируемый доступ и переадресации трафика см. гл. 7 на стр. 99 .

17.4 Адрес защищенного шлюза

Адрес защищенного шлюза – это IP-адрес или доменное имя удаленного шлюза IPSec на стороне WAN.

Если удаленный защищенный шлюз имеет статический IP-адрес в сети WAN, введите его в поле **Secure Gateway Address**. В поле **Secure Gateway Address** также можно указать доменное имя удаленного защищенного шлюза, если оно имеется.

Доменное имя отдаленного безопасного шлюза можно также указывать в поле **Secure Gateway Address** в тех случаях, когда удаленный защищенный шлюз имеет динамический IP-адрес в сети WAN и использует службу DDNS. Устройство P-2602 должно перестраивать VPN-туннель при каждом изменении IP-адреса удаленного безопасного шлюза в сети WAN (возможно возникновение задержки, пока на серверы DDNS не поступит новый IP-адрес удаленного шлюза в сети WAN).

17.4.1 Динамический адрес защищенного шлюза

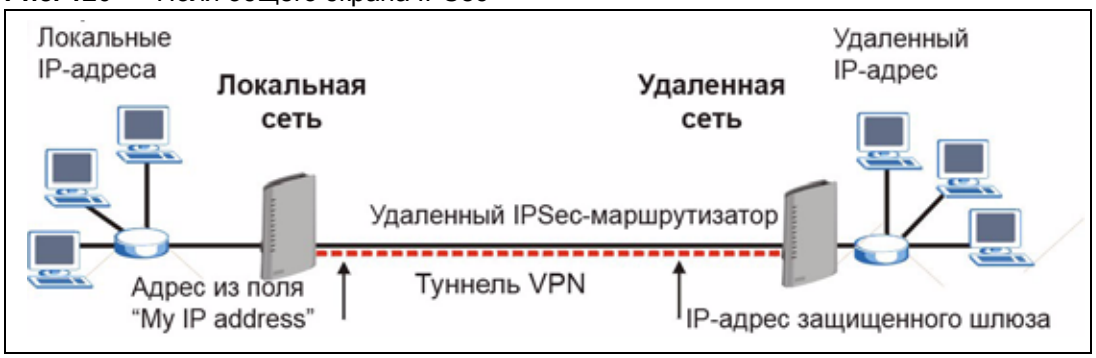
Если удаленный защищенный шлюз имеет динамический IP-адрес в сети WAN и не использует DDNS, в поле Secure Gateway Address введите адрес 0.0.0.0. В этом случае SA могут инициироваться только удаленным защищенным шлюзом, такая конфигурация полезна для дистанционных (надомных) сотрудников, обращающихся через туннель VPN к корпоративной сети (примеры настройки см. в разд. 17.18 на стр. 268).

Адрес 0.0.0.0 может быть задан как IP-адрес защищенного шлюза только в том случае, если используется протокол управления ключами **IKE**, а не ручной режим **Manual**.

17.5 Экран VPN Setup

На следующем рисунке поясняется назначение основных полей в веб-конфигураторе.

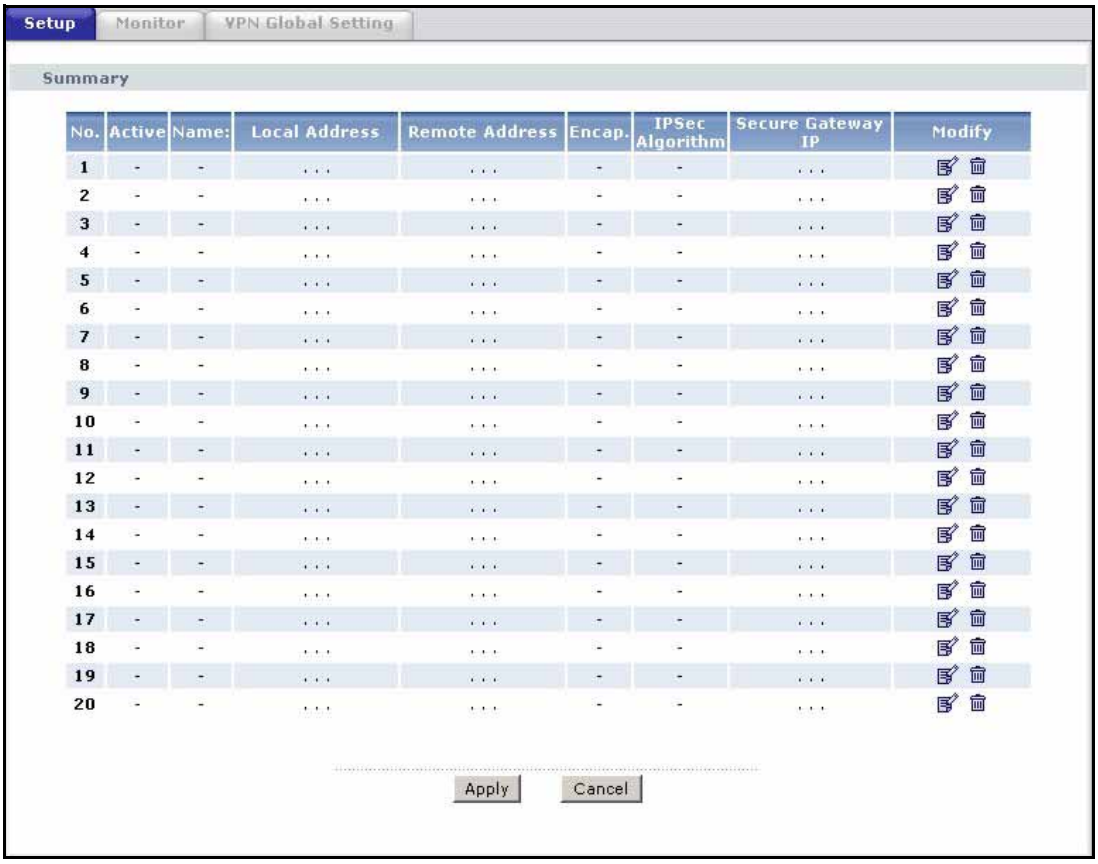
Рис. 120 Поля общего экрана IPSec



Локальные и удаленные IP-адреса должны быть статическими.

Чтобы перейти на экран **VPN Setup**, выберите **Security**, затем – **VPN** . На этом экране представлено меню настроенных вами правил (туннелей) IPSec. Информация в меню доступна только для чтения. Для редактирования или создания правила IPSec выберите порядковый номер и выполните настройку в соответствующих подменю.

Рис. 121 Экран VPN Setup



Поля изображённого выше экрана описаны в следующей таблице.

Таб. 81 Экран VPN Setup

ПОЛЕ	ОПИСАНИЕ
No.	В этом поле указан порядковый номер VPN. Чтобы отредактировать политику VPN, щелкните мышью на ее номере.
Active	В этом поле отображается состояние политики VPN (активна / неактивна). **Yes** обозначает, что соответствующая политика VPN активна. **No** обозначает, что соответствующая политика VPN неактивна.
Name	В данном поле отображается идентификационное имя для данной политики VPN.
Local Address	В этом поле указываются IP-адреса компьютеров в вашей локальной сети за устройством P-2602. Если поле **Local Address Type** на экране **VPN-IKE** (или **VPN-Manual Key**) установлено в значение **Single**, дважды будет отображаться один и тот же (статический) IP-адрес. Если поле **Local Address Type** на экране **VPN-IKE** (или **VPN-Manual Key**) установлено в значение **Range**, будут отображаться начальные и конечные (статические) IP-адреса в диапазоне. Если поле **Local Address Type** на экране **VPN-IKE** (или **VPN-Manual Key**) установлено в значение **Subnet**, будет отображаться (статический) IP-адрес и маска подсети.
Remote Address	В этом поле указываются IP-адреса компьютеров в удаленной локальной сети за удаленным маршрутизатором IPSec. Если в поле **Secure Gateway Address** введен адрес **0.0.0.0**, то в данном поле будет указано **N/A** (“неприменимо”). В этом случае VPN-соединение может инициироваться только удаленным защищенным шлюзом, Если поле **Remote Address Type** на экране **VPN-IKE** (или **VPN-Manual Key**) установлено в значение **Single**, дважды будет отображаться один и тот же (статический) IP-адрес. Если поле **Remote Address Type** на экране **VPN-IKE** (или **VPN-Manual Key**) установлено в значение **Range**, будут отображаться начальные и конечные (статические) IP-адреса в диапазоне. Если поле **Remote Address Type** на экране **VPN-IKE** (или **VPN-Manual Key**) установлено в значение **Subnet**, будет отображаться (статический) IP-адрес и маска подсети.
Encap.	В этом поле отображается выбранный режим: **Tunnel** или **Transport** mode (по умолчанию – **Tunnel**).
IPSec Algorithm	В данном поле отображаются протоколы безопасности, используемые для SA. Использование **AH** и **ESP** приводит к повышению требований к производительности вычислений P-2602 и задержке обмена данными (запаздыванию).
Secure Gateway IP	В этом поле указывается статический IP-адрес WAN или URL удаленного маршрутизатора IPSec. Если в поле **Secure Gateway Address** на экране **VPN-IKE** был указан адрес **0.0.0.0**, то в данном поле будет также отображаться адрес **0.0.0.0**.
Modify	Чтобы перейти на экран для редактирования конфигурации VPN, щелкните на значке **Edit**. Для удаления существующей конфигурации VPN щелкните на значке **Remove**.
Apply	Нажмите эту кнопку, чтобы сохранить изменения в P-2602.
Cancel	Нажмите эту кнопку, чтобы возвратить настройки к их последним сохраненным значениям.

17.6 Keep Alive

При установлении туннеля IPSec с включенной функцией поддержания активности (Keep Alive), P-2602 автоматически восстанавливает туннель по истечении периода действия IPSec SA (подробнее о периоде действия SA см. разд. 17.12 на стр. 256). Фактически один раз установленный туннель IPSec становится постоянно действующим. Чтобы эта функция работала, оба маршрутизатора IPSec должны иметь функцию поддержания активности, совместимую с P-2602.

Если с устройством P-2602 уже установлено максимально допустимое число одновременно открытых туннелей IPSec, для каждого из которых включено поддержание активности, то установить новые туннели с P-2602 будет невозможно, поскольку P-2602 никогда не разрывает ранее установленных туннелей.

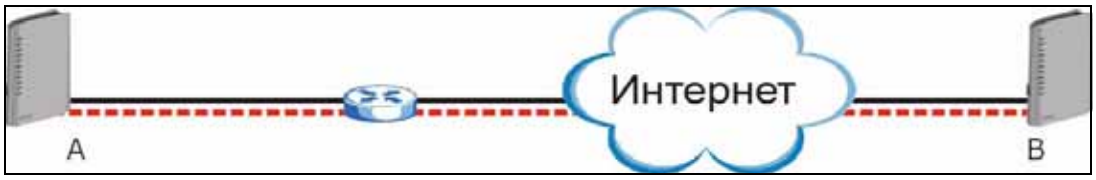
Если в туннеле пересылается только исходящий трафик без входящего трафика, P-2602 автоматически разрывает туннель по истечении двух минут.

17.7 VPN, NAT, и прослеживание NAT

NAT несовместим с протоколом AH ни в **транспортном**, ни в **туннельном** режиме. В VPN-сетях на основе IPSec, использующих протокол AH, исходящий пакет снабжается цифровой подписью, которая рассчитывается для заголовка и полезной нагрузки, и приписывается к пакету в виде хеш-значения. В результате устройство VPN на принимающей стороне обнаруживает несовпадение хеш-значения и полученных данных и предполагает, что данные были злонамеренно изменены.

Кроме того, NAT обычно также несовместим с ESP в транспортном режиме, но функция прослеживания NAT (**NAT Traversal**) в P-2602 позволяет устранить эту несовместимость. Прослеживание NAT позволяет устанавливать IKE SA при наличии NAT-маршрутизаторов между двумя маршрутизаторами IPSec.

Рис. 122 NAT-маршрутизатор между IPSec-маршрутизаторами



Обычно установить IKE SA при нахождении маршрутизатора NAT между двумя маршрутизаторами IPSec невозможно, поскольку маршрутизатор NAT изменяет заголовок пакета IPSec. Функция прослеживания NAT решает эту проблему, добавляя порт к пакету IPSec заголовок с номером UDP-порта 500. NAT-маршрутизатор пересылает пакет IPSec, не изменяя заголовок для UDP-порта 500. Как показано на рис. 122 на стр. 246, когда маршрутизатор IPSec пытается установить IKE SA, маршрутизатор IPSec B проверяет порт заголовок с UDP-портом 500, и маршрутизаторы A IPSec A и B устанавливают IKE SA.

Чтобы использовать прослеживание NAT, необходимо:

- Использовать протокол ESP (в транспортном или в туннельном режиме).
- Использовать протокол ключей IKE.
- Включить прослеживание NAT в обеих оконечных точках туннеля IPSec.
- Настроить NAT-маршрутизатор, разрешив пересылку пакетов для UDP-порта 500 на IPSec-маршрутизатор A.

В результате обеспечивается совместимость NAT и ESP в туннельном режиме, так как проверка целостности производится для совокупности исходного заголовка и исходной полезной нагрузки, а оба этих параметра не изменяются при прохождении NAT-устройства. Совместимость AH и ESP с NAT в туннельных и транспортных режимах отражена в следующей таблице.

Таб. 82 Взаимодействие VPN и NAT

ПРОТОКОЛ БЕЗОПАСНОСТИ	РЕЖИМ	NAT
AH	Транспортный	Нет
AH	Туннельный	Нет
ESP	Транспортный	Да*
ESP	Туннельный	Да

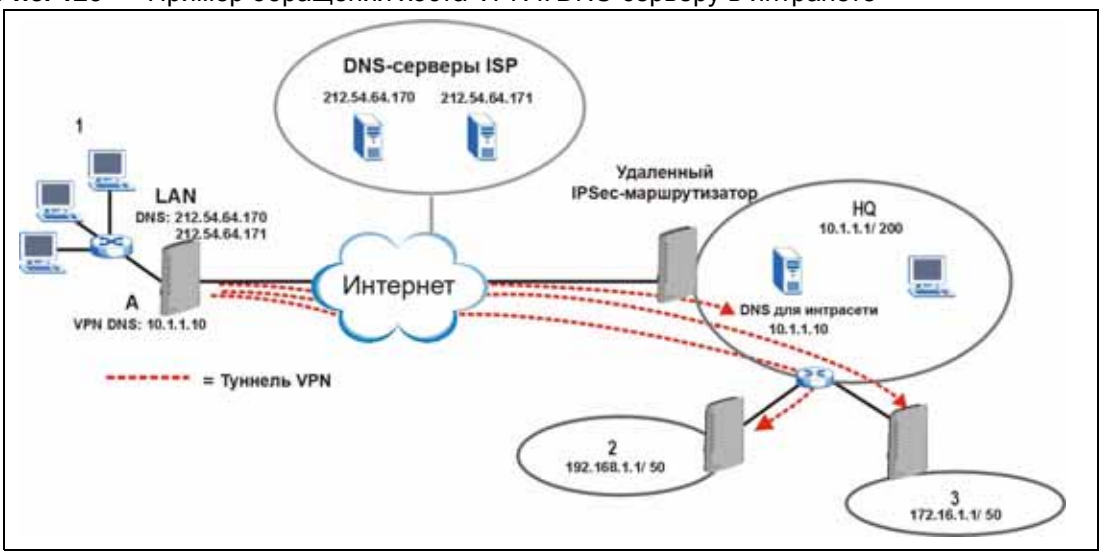
Да* - этот режим поддерживается в P-2602, если включено прослеживание NAT.

17.8 Удаленный DNS-сервер

В тех случаях, когда обращение к интранет-серверам в удаленной сети с DNS-сервером осуществляется по доменным именам, необходимо указать адрес этого DNS-сервера. DNS-серверы локальной сети или поставщика услуг Интернета (ISP) использовать нельзя, поскольку они не могут преобразовывать доменные имена к частным IP-адресам в удаленной сети

На следующем рисунке приведен пример создания трех туннелей VPN из сети P-2602 A: к филиалу 2, к филиалу 3 и к штаб-квартире. Чтобы получить доступ к компьютерам, которые используют частные доменные имена сети штаб-квартиры (HQ), P-2602 в филиале 1 использует DNS-сервер в интранете штаб-квартиры. Функция DNS-сервера для VPN не работает с Windows 2000 и Windows XP.

Рис. 123 Пример обращения хоста VPN к DNS-серверу в интранете



Если DNS-сервер интранета в удаленной сети не указан, то хост VPN сможет обращаться к компьютерам удаленной сети только по IP-адресам.

17.9 Тип и содержание идентификатора

В агрессивном режимоме согласования (см. разд. 17.12.1 на стр. 257), P-2602 идентифицирует поступающие SA по типу и содержанию идентификатора, так как эти идентификационные данные не шифруются. Таким образом P-2602 получает возможность различать несколько правил для SA, устанавливаемых удаленными маршрутизаторами IPSec с динамическими IP-адресами в сети WAN. Дистанционные сотрудники могут использовать отдельные пароли для одновременного подключения к P-2602 через маршрутизаторы IPSec с динамическими IP-адресами (пример конфигурации для дистанционного сотрудника см. в разд. 17.18 на стр. 268).

Независимо от настроенного типа и содержания идентификатора P-2602 не позволяет сохранять несколько активных правил с перекрывающимися локальными и удаленными IP-адресами.

В основном режиме (см. разд. 17.12.1 на стр. 257) тип и содержание идентификатора зашифрованы, что обеспечивает защиту подлинности. При этом P-2602 может различать не более 12 типов SA, поступающих от удаленных маршрутизаторов IPSec с динамическими IP-адресами в сети WAN. Возможность различать 12 типов входящих SA на P-2602 обусловлена тем, что при настройке правила VPN могут быть выбраны три разных алгоритма шифрования (DES, 3DES и AES), два алгоритма аутентификации (MD5 и SHA1) и две группы ключей (DH1 и DH2). См. разд. 17.13 на стр. 258. Тип и содержание идентификатора играют роль дополнительного уровня идентификации для поступающих SA.

Тип идентификатора может быть доменным именем, IP-адресом или почтовым адресом. Содержание – это IP-адрес, доменное имя или почтовый адрес.

Таб. 83 Поля типа и содержания для локальных идентификаторов

LOCAL ID TYPE=	CONTENT=
IP	Введите IP-адрес вашего компьютера или оставьте это поле пустым, чтобы автоматически использовать собственный IP-адрес P-2602.
DNS	Введите доменное имя (длиной до 31 знака), идентифицирующее данное устройство P-2602.
E-mail	Введите адрес электронной почты (длиной до 31 знака), идентифицирующий данное устройство P-2602.
	Имя домена или адрес электронной почты, введённый в поле **Content**, используется только для идентификации и не должен быть реальным именем домена или адресом электронной почты.

Таб. 84 Поля типа и содержания для удаленных идентификаторов

PEER ID TYPE=	CONTENT=
IP	Введите IP-адрес компьютера, с которым будет устанавливаться VPN-соединение, или оставьте это поле пустым, чтобы устройство P-2602 автоматически использовало значение из поля **Secure Gateway**.
DNS	Введите доменное имя (длиной до 31 знака), идентифицирующее удаленный IPSec-маршрутизатор.
E-mail	Введите адрес электронной почты (длиной до 31 знака), идентифицирующий удаленный IPSec-маршрутизатор.
	Имя домена или адрес электронной почты, введённый в поле **Content**, используется только для идентификации и не должен быть реальным именем домена или адресом электронной почты. Имя домена может не соответствовать IP-адресу удалённого маршрутизатора или настройкам в поле **Secure Gateway Address** ниже.

17.9.1 Примеры типов и содержаний идентификатора

Для установления VPN-туннеля два маршрутизатора IPSec должны иметь одинаковые настройки типа и содержания идентификатора.

В данном примере два P-2602 могут завершить согласование и установить туннель VPN.

Таб. 85 Примеры совпадающих типов и содержаний идентификаторов

P-2602 A	P-2602 B
Тип локального идентификатора: E-mail	Тип локального идентификатора: IP
Содержание локального идентификатора: tom@yourcompany.com	Содержание локального идентификатора: 1.1.1.2
Тип удалённого идентификатора: IP	Тип удалённого идентификатора: E-mail
Содержание удалённого идентификатора: 1.1.1.2	Содержание удалённого идентификатора: tom@yourcompany.com

В этом примере два устройства P-2602 не могут завершить согласование, поскольку на P-2602 B **выбран тип локального идентификатора IP**, а на P-2602 A **выбран тип удаленного идентификатора E-mail**. В журнале IPSEC появится сообщение о несовпадающем идентификаторе (“ID mismatched”).

Таб. 86 Примеры несовпадающих типов и содержаний идентификаторов

P-2602 A	P-2602 B
Тип локального идентификатора: IP	Тип локального идентификатора: IP
Содержание локального идентификатора: 1.1.1.10	Содержание локального идентификатора: 1.1.1.10
Тип удалённого идентификатора: E-mail	Тип удалённого идентификатора: IP
Содержание удалённого идентификатора: aa@yahoo.com	Содержание удалённого идентификатора: неприменимо

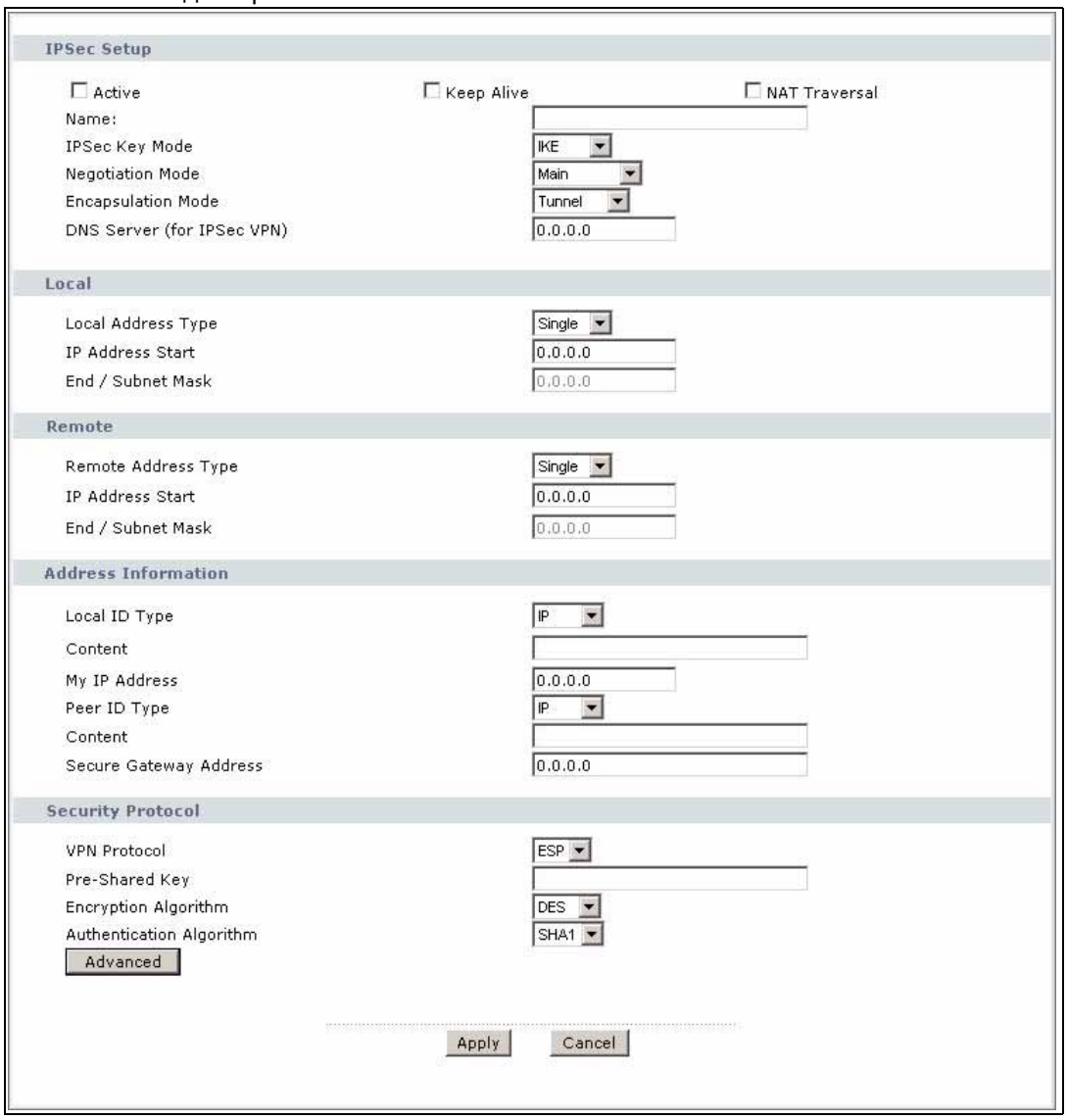
17.10 Ключ для предварительного совместного использования

Ключ для предварительного совместного использования идентифицирует стороны соединения во время согласования в 1-й фазе IKE (подробнее о фазах IKE см. разд. 17.12 на стр. 256). Термин “предварительное совместное использование” означает, что этот ключ должен быть сообщен другой стороне прежде чем с ней может быть установлен защищенный сеанс.

17.11 Редактирование политик VPN

Для редактирования политик VPN перейдите на Экран VPN Setup и щелкните на значке **Edit**.

Рис. 124 Редактирование политик VPN



Поля изображённого выше экрана описаны в следующей таблице.

Таб. 87 Редактирование политик VPN

ПОЛЕ	ОПИСАНИЕ
IPSec Setup	
Active	Установите этот флажок, чтобы активировать данную политику VPN. В этом поле определяется, применяется ли правило VPN перед тем, как пакет покидает межсетевой экран.
Keep Alive	В раскрывающемся списке выберите **Yes** (да) или **No** (нет). Выберите **Yes** и нажмите [ENTER], чтобы устройство P-2602 автоматически запустило SA повторно после истечения срока действия, даже если трафика нет. Чтобы использовать эту возможность, на удалённом IPSec-маршрутизаторе должна быть включена функция поддержки активности.

Таб. 87 Редактирование политик VPN

ПОЛЕ	ОПИСАНИЕ
NAT Traversal	Эта функция доступна, если в поле **VPN protocol** выбран протокол **ESP**. Прослеживание NAT позволяет настроить соединение VPN, когда между P-2602 и удаленным IPSec-маршрутизатором имеются NAT-маршрутизаторы. На удаленном IPSec-маршрутизаторе также должно быть разрешено прослеживание NAT, и NAT-маршрутизаторы должны отправлять пакеты UDP 500 удаленному IPSec-маршрутизатору за NAT-маршрутизатором.
Name	Введите идентификатор данной политики длиной до 32 символов. Можно использовать любые символы, включая пробелы, но конечные пробелы отсекаются P-2602.
IPSec Key Mode	В раскрывающемся списке выберите **IKE** или **Manual**. Рекомендуется выбрать режим **IKE**, обеспечивающий повышенную защиту. Режим **Manual** (ручной) используется для устранения неисправностей, если возникают проблемы с использованием режима управления ключами **IKE**.
Negotiation Mode	В раскрывающемся списке выберите **Main** (основной) или **Aggressive** (агрессивный). Несколько SA, соединяющихся через защищённый межсетевой шлюз, должны иметь одинаковый режим согласования.
Encapsulation Mode	Выберите режим в раскрывающемся списке: **Tunnel** (туннельный) или **Transport** (транспортный).
DNS Server (for IPSec VPN)	Если для данной VPN-сети существует частный DNS-сервер, введите его IP-адрес в этом поле. P-2602 будет назначать этот дополнительный DNS-сервер DHCP-клиентам P-2602, IP-адреса которых находятся в диапазоне локальных адресов данного правила. DNS-сервер позволяет клиентам в сети VPN находить другие компьютеры и серверы в VPN по их (частным) доменным именам.
Local	Локальные IP-адреса должны быть статическими и соответствовать настроенным удалённым IP-адресам удалённого IPSec-маршрутизатора. Две активных SA могут иметь одинаковый локальный или удалённый IP-адрес, но не оба сразу. Можно настроить несколько SA между одинаковыми локальными и удалёнными IP-адресами, при условии, что в конкретный момент времени активным будет только одна. Несколько правил, в которых поле **Secure Gateway Address** установлено в значение **0.0.0.0**, могут быть одновременно активны только в том случае, если ни в одном из них диапазон IP-адресов не пересекается с другими правилами. Если настроено активное правило, для которого в поле **Secure Gateway Address** указан адрес **0.0.0.0**, а полный IP-адрес LAN совпадает с локальным IP-адресом, то настроить другие активные правила, в которых **Secure Gateway Address = 0.0.0.0**, будет невозможно.
Local Address Type	В раскрывающемся меню выберите **Single** (единичный адрес), **Range** (диапазон) или **Subnet** (подсеть). Чтобы задать один IP-адрес, выберите **Single**. Чтобы задать определенный диапазон IP-адресов, выберите **Range**. Чтобы задать подсеть IP-адресов по маске подсети, выберите **Subnet**.
IP Address Start	Если в поле **Local Address Type** выбрано значение **Single**, введите (статический) IP в вашей сети LAN за устройством P-2602. Если в поле **Local Address Type** выбрано **Range**, введите начальный (статический) IP диапазона адресов компьютеров в вашей сети LAN за устройством P-2602. Если в поле **Local Address Type** выбрано **Subnet**, введите (статический) IP-адрес в вашей сети LAN за устройством P-2602.

Таб. 87 Редактирование политик VPN

ПОЛЕ	ОПИСАНИЕ
End / Subnet Mask	Если в поле **Local Address Type** выбрано **Single**, то данное поле не действует. Если в поле **Local Address Type** выбрано **Range**, введите конечный (статический) IP-адрес диапазона IP-адресов компьютеров в вашей сети LAN за устройством P-2602. Если в поле **Local Address Type** выбрано **Subnet**, введите маску подсети, которая соответствует вашей сети LAN за устройством P-2602.
Remote	Удаленные IP-адреса должны быть статическими и соответствовать настроенным локальным IP-адресам удалённого маршрутизатора IPSec. Поля удаленных адресов не применяются, если в поле **Secure Gateway IP Address** выбран адрес **0.0.0.0**. В этом случае VPN-соединение может инициироваться только удаленным защищенным шлюзом, У двух активных SA не может быть одинаковых локальных и удалённых IP-адресов. Две активных SA могут иметь одинаковый локальный или удалённый IP-адрес, но не оба сразу. Можно настроить несколько SA между одинаковыми локальными и удалёнными IP-адресами, при условии, что в конкретный момент времени активным будет только одна.
Remote Address Type	В раскрывающемся меню выберите **Single** (единичный адрес), **Range** (диапазон) или **Subnet** (подсеть). Выберите **Single**, чтобы указать единичный IP-адрес. Чтобы задать определенный диапазон IP-адресов, выберите **Range**. Чтобы задать подсеть IP-адресов по маске подсети, выберите **Subnet**.
IP Address Start	Если в поле **Remote Address Type** выбрано значение **Single**, введите (статический) IP-адрес в сети за удаленным IPSec-маршрутизатором. Если в поле **Remote Address Type** выбрано **Range**, введите начальный (статический) IP диапазона адресов компьютеров в сети за удаленным IPSec-маршрутизатором. Если в поле **Remote Address Type** выбрано значение **Subnet**, введите (статический) IP-адрес в сети за удаленным IPSec-маршрутизатором.
End / Subnet Mask	Если в поле **Remote Address Type** выбрано **Single**, то данное поле не действует. Если в поле **Remote Address Type** выбрано **Range**, введите конечный (статический) IP-адрес диапазона IP-адресов компьютеров в сети за удаленным IPSec-маршрутизатором. Если в поле **Remote Address Type** выбрано значение **Subnet**, введите маску подсети, которая соответствует сети за удаленным IPSec-маршрутизатором.
Address Information	
Local ID Type	Выберите **IP** для идентификации данного P-2602 по его IP-адресу. Выберите **DNS** для идентификации P-2602 по доменному имени. Выберите **E-mail** для идентификации P-2602 по адресу электронной почты.

Таб. 87 Редактирование политик VPN

ПОЛЕ	ОПИСАНИЕ
Content	Если в поле **Local ID Type** выбрано **IP**, введите IP-адрес своего компьютера в поле **Content** локального идентификатора. Если в поле **Content** выбран адрес **0.0.0.0** или это поле оставлено пустым, P-2602 будет автоматически использовать IP-адрес из поля **My IP Address** (см. описание поля **My IP Address**). В следующих ситуациях рекомендуется указывать в поле **Content** локального идентификатора адрес, отличный от **0.0.0.0**, или использовать типы идентификаторов **DNS** или **E-mail**. Между двумя маршрутизаторами IPSec имеется NAT-маршрутизатор . Необходимо, чтобы удаленный маршрутизатор IPSec различал VPN-соединения от разных IPSec-маршрутизаторов с динамическими IP-адресами в сети WAN. Если в поле **Local ID Type** выбран тип идентификатора **DNS** или **E-mail**, в поле **Content** для локального идентификатора введите доменное имя или адрес электронной почты, идентифицирующие данное устройство P-2602. Допустимая длина – до 31 символа ASCII с пробелами, но конечные пробелы отсекаются. Доменное имя или почтовый адрес служат только для идентификации и могут представлять собой абсолютно произвольные строки.
My IP Address	Введите IP-адрес вашего устройства P-2602 в сети WAN. Туннель VPN необходимо построить заново в случае изменения этого IP-адреса. Если в этом поле введен адрес **0.0.0.0**, действует следующий алгоритм: Для настройки VPN-туннеля P-2602 использует текущий IP-адрес (статический или динамический), присвоенный P-2602 в сети WAN (static or dynamic). При обрыве соединения с WAN P-2602 использует для туннеля VPN IP-адрес резервирования через коммутируемый доступ или IP-адрес в LAN, если используется переадресация трафика. Подробнее о резервировании через коммутируемый доступ и переадресации трафика см. гл. 7 на стр. 99 .
Peer ID Type	Выберите **IP** для идентификации удалённого IPSec-маршрутизатора по его IP-адресу. Выберите **DNS** для идентификации удаленного IPSec-маршрутизатора по доменному имени. Выберите **E-mail** для идентификации удаленного IPSec-маршрутизатора по адресу электронной почты.
Content	Содержание удаленной идентификатора настраивается в зависимости от его типа. Если выбран тип идентификатора **IP**, укажите IP-адрес компьютера, к которому вы подключаетесь через VPN. Если в этом поле указан адрес **0.0.0.0** или поле оставлено пустым, P-2602 будет использовать адрес, указанный в поле **Secure Gateway Address** (см. описание поля **Secure Gateway Address**). Если выбран тип идентификатора **DNS** или **E-mail**, введите доменное имя или адрес электронной почты, идентифицирующий IPSec-маршрутизатор. Допустимая длина – до 31 символа ASCII с пробелами, но конечные пробелы отсекаются. Доменное имя или почтовый адрес служат только для идентификации и могут представлять собой абсолютно произвольные строки. В следующих ситуациях рекомендуется указывать IP-адрес, отличный от **0.0.0.0**, или использовать типы идентификаторов **DNS** или **E-mail**: Между двумя маршрутизаторами IPSec имеется NAT-маршрутизатор. Необходимо, чтобы устройство P-2602 различало VPN-соединения от разных IPSec-маршрутизаторов с динамическими IP-адресами в сети WAN.

Таб. 87 Редактирование политик VPN

ПОЛЕ	ОПИСАНИЕ
Secure Gateway Address	Введите IP-адрес в сети WAN или URL (до 31 символа) маршрутизатора IPSec, к которому производится подключение по VPN. Установите значение **0.0.0.0** в этом поле, если удалённый IPSec-маршрутизатор имеет динамический IP-адрес WAN (в поле **Key Management** должно быть установлено значение **IKE**). Несколько правил, в которых поле **Secure Gateway Address** установлено в значение **0.0.0.0**, могут быть одновременно активны только в том случае, если ни в одном из них диапазон IP-адресов не пересекается с другими правилами. Если настроено активное правило, для которого в поле **Secure Gateway Address** указан адрес **0.0.0.0**, а полный IP-адрес LAN совпадает с локальным IP-адресом, то настроить другие активные правила, в которых **Secure Gateway Address** = **0.0.0.0**, будет невозможно.
Security Protocol	
VPN Protocol	Выберите **ESP**, чтобы использовать протокол ESP (Encapsulation Security Payload). Протокол ESP (RFC 2406) реализует шифрование в дополнение к функциям, обеспечиваемым **AH**. Если в этом поле выбран протокол **ESP**, необходимо также настроить параметры в полях **Encryption Algorithm** и **Authentication Algorithm** (см. ниже).
Pre-Shared Key	Введите ваш ключ для предварительного совместного использования в этом поле. Ключ для предварительного совместного использования идентифицирует стороны соединения во время согласования в 1-й фазе IKE. Термин “предварительное совместное использование” означает, что этот ключ должен быть сообщен другой стороне прежде чем с ней может быть установлен защищенный сеанс. Введите от 8 до 31 символа ASCII (регистр, в котором набраны символы, учитывается) или от 16 до 62 шестнадцатеричных символов (“0-9”, “A-F”). Перед шестнадцатеричным кодом необходимо ставить приставку “0x” (ноль икс). Длина этой приставки не входит в длину ключа (от 16 до 62 символа). Например, в строке “0x0123456789ABCDEF” приставка “0x” означает, что ключ указан в шестнадцатеричном виде, а последовательность “0123456789ABCDEF” является непосредственным ключом. На обоих концах туннеля VPN должен использоваться один и тот же ключ для предварительного совместного использования. Если на обоих концах не используется ключ для предварительного совместного использования, будет получен пакет “PYLD_MALFORMED” (полезная нагрузка плохо сформирована).
Encryption Algorithm	В раскрывающемся списке выберите алгоритм шифрования: **DES**, **3DES**, **AES** или **NULL**. При использовании любого из этих алгоритмов шифрования отправитель и получатель должны использовать один и тот же секретный ключ, который может применяться для шифрования и расшифровки сообщений или для создания и проверки кода аутентификации сообщений. В алгоритме шифрования DES используется 56-битный ключ. Тройной DES (**3DES**) – разновидность **DES**, где используется 168- битовый ключ. Поэтому **3DES** более защищен по сравнению с **DES**. Для него также требуется больше вычислительных мощностей, что увеличивает задержки и снижает производительность. В данной реализации **AES** используется 128-битный ключ. **AES** обладает большим быстродействием, чем **3DES**. Чтобы настроить туннель без шифрования, выберите значение **NULL**. Если выбран режим **NULL**, ключ шифрования вводить не требуется.

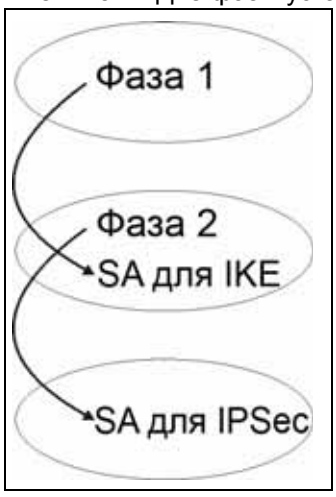
Таб. 87 Редактирование политик VPN

ПОЛЕ	ОПИСАНИЕ
Authentication Algorithm	В раскрывающемся списке выберите **SHA1** или **MD5**. **MD5** (свертка сообщения, реализация 5) и **SHA1** (защищенный алгоритм хеширования) – это алгоритмы хеширования, используемые для аутентификации данных в пакете. Алгоритм **SHA1** обычно считается более надёжным, чем **MD5**, но он несколько медленнее. Для минимальной защиты можно применять метод **MD5**, а для наибольшей безопасности следует использовать **SHA1**.
Advanced	Для более подробной настройки параметров управления ключами IKE нажмите кнопку **Advanced**.
Back	Для возврата к предыдущему экрану нажмите кнопку **Back**.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-2602.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

17.12 Фазы IKE

Согласование IKE (Internet Key Exchange – протокол обмена ключами для Интернета) подразделяется на два этапа: фаза 1 (аутентификация) и фаза 2 (обмен ключами). В ходе обмена в 1-й фазе устанавливается IKE SA, а во 2-й фазе с помощью созданной SA согласуется SA для IPSec.

Рис. 125 Две фазы установления SA для IPSec



Для фазы 1 необходимо:

- Выбрать режим согласования.
- Осуществить аутентификацию соединения, введя ключ для предварительного совместного использования.
- Выбрать алгоритм шифрования.
- Выбрать алгоритм аутентификации.
- Выбрать группу ключей для криптографического алгоритма Диффи-Хелмана с открытым ключом (**DH1** или **DH2**).

- Задать период действия IKE SA (SA Life Time). Это поле позволяет определить срок действия IKE SA, по истечении которого IKE SA прекращает действовать. Если истечение IKE SA наступит после того, как будет установлена IPSec SA, то IPSec SA не будет признана истекшей.

Для фазы 2 необходимо:

- Выбрать протокол (**ESP** или **AH**) для обмена ключами IKE.
- Выбрать алгоритм шифрования.
- Выбрать алгоритм аутентификации
- Указать, требуется ли использовать механизм PFS (Perfect Forward Secrecy – защита от разглашения использованных ключей), реализуемый с помощью криптографического алгоритма Диффи-Хелмана с открытым ключом – см. разд. 17.12.3 на стр. 258. Чтобы отключить PFS, выберите **None** (это значение выбрано по умолчанию).
- Выбрать режим: **Tunnel** (туннельный) или **Transport** (транспортный).
- Задать период действия IPSec SA (SA Life Time). Это поле позволяет определить срок действия IKE SA, по истечении которого P-2602 автоматически согласует новую IPSec SA, если в соединении имеется трафик. P-2602 будет автоматически согласовывать новую IPSec SA и в том случае, если трафик отсутствует, но на обоих IPSec-маршрутизаторах включена функция поддержания активности. При истечении срока действия IPSec SA маршрутизатор IPSec должен будет повторно согласовать SA перед очередной пересылкой трафика.

17.12.1 Режим согласования

Режим согласования (**Negotiation Mode**), выбранный для 1-й фазы, определяет способ формирования ассоциации безопасности (SA) для каждого соединения посредством согласований IKE.

- В основном режиме (**Main Mode**) обеспечивается наибольший уровень безопасности при согласовании аутентификации между сторонами соединения (фаза 1). В нем используются 6 сообщений и 3 двухсторонних цикла передачи: согласование SA, обмен ключами Диффи-Хелмана и обмен случайными числами (“nonce”). Этот режим обеспечивает защиту идентификационных данных (параметры, позволяющие вас идентифицировать, во время согласования не раскрываются).
- Агрессивный режим (**Aggressive Mode**) обладает большим быстродействием по сравнению с основным режимом (**Main Mode**) за счет исключения некоторых этапов согласования идентификации (на фазе 1). Его недостаток состоит в том, что ускоренная процедура ограничивает эффективность согласования и не обеспечивает защиту идентификационных данных. Он полезен в условиях удаленного доступа, где адрес инициатора неизвестен отвечающей стороне, и обе стороны реализуют аутентификацию посредством ключей для предварительного совместного использования.

17.12.2 Группы ключей Диффи-Хелмана (DH)

Протокол Диффи-Хелмана (DH) представляет собой криптографический протокол с открытым ключом, позволяющий двум сторонам согласовать секретный ключ по незащищенному каналу связи. Протокол Диффи-Хелмана используется во время подготовки IKE SA для формирования ключей сеанса. Поддерживаются две группы ключей Диффи-Хелмана: 768-битная (группа 1 - **DH1**) и 1024-битная (группа 2 – **DH2**). По завершении обмена ключами Диффи-Хелмана обе удаленные стороны получают общий секретный ключ, но IKE SA не аутентифицируется. Если необходима аутентификация, следует применять ключи для предварительного совместного использования.

17.12.3 Защита от разглашения использованных ключей (PFS)

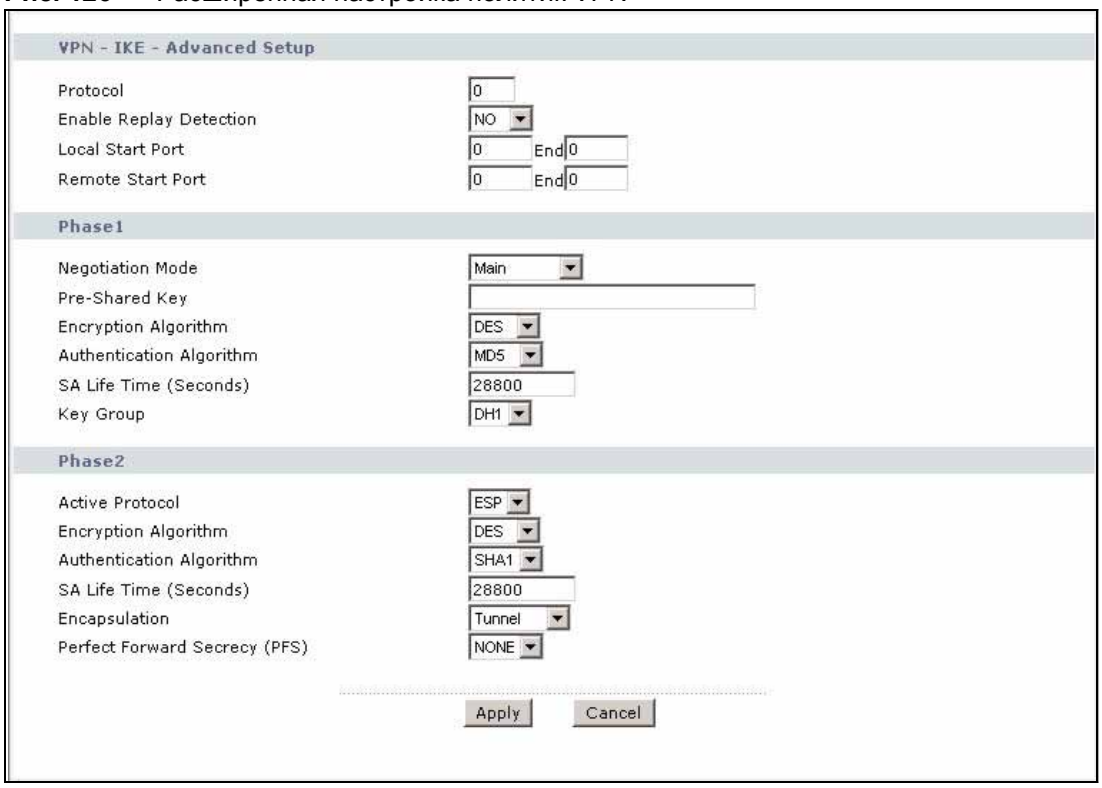
Включение режима PFS делает ключ временным. В каждом очередном согласовании IPSec SA участвует новый ключ, для чего обмен ключами Диффи-Хелмана выполняется заново. Если при включенном режиме PFS один ключ случайно станет известен, это не поставит под угрозу предыдущие и последующие ключи, поскольку каждый последующий ключ не может быть получен из предыдущего. Недостатком этой дополнительной меры защиты является длительный обмен ключами Диффи-Хелмана.

Для данных, не требующих подобной степени защиты, это может оказаться нежелательным, поэтому по умолчанию в P-2602 режим PFS отключен (**None**). Отключение PFS означает, что ключи шифрования для каждой очередной аутентификации получаются из одного и того же корневого секретного ключа (что и является причиной меньшей защищенности этой схемы), но формирование SA осуществляется быстрее за счет того, что обмен ключами Диффи-Хелмана пропускается.

17.13 Настройка расширенных параметров IKE

Чтобы перейти на показанный ниже экран, на экране Редактирование политик VPN выберите **Advanced**.

Рис. 126 Расширенная настройка политик VPN



Поля изображённого выше экрана описаны в следующей таблице.

Таб. 88 Расширенная настройка политик VPN

ПОЛЕ	ОПИСАНИЕ
VPN - IKE	
Protocol	Введите 1 для ICMP, 6 для TCP, 17 для UDP и т.д. 0 – значение по умолчанию, обозначающее любой протокол.
Enable Replay Detection	Поскольку для настройки VPN требуются большие вычислительные ресурсы, система может подвергнуться атакам, провоцирующим отказ в обслуживании (DoS). Приемник IPSec может обнаруживать и удалять старые и дублируемые пакеты для защиты от атак воспроизведения (replay). Чтобы включить защиту от атак воспроизведения, в раскрывающемся меню выберите **YES**; чтобы отключите защиту, выберите **NO**.
Local Start Port	0 – значение по умолчанию, обозначающее любой порт. Введите номер порта от 0 до 65535. Самые распространённые порты IP: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
End	В этом поле введите номер порта для определения диапазона портов. Этот номер порта должен быть больше, чем тот, что указан в предыдущем поле. Если в поле **Local Start Port** оставлено значение 0, поле **End** также останется с нулевым значением.
Remote Start Port	0 – значение по умолчанию, обозначающее любой порт. Введите номер порта от 0 до 65535. Самые распространённые порты IP: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.

Таб. 88 Расширенная настройка политик VPN

ПОЛЕ	ОПИСАНИЕ
End	В этом поле введите номер порта для определения диапазона портов. Этот номер порта должен быть больше, чем тот, что указан в предыдущем поле. Если в поле **Local Start Port** оставлено значение 0, поле **End** также примет значение 0.
Phase 1	
Negotiation Mode	В раскрывающемся списке выберите **Main** (основной) или **Aggressive** (агрессивный). Несколько SA, соединяющихся через защищённый межсетевой шлюз, должны иметь одинаковый режим согласования.
Pre-Shared Key	Введите ваш ключ для предварительного совместного использования в этом поле. Ключ для предварительного совместного использования идентифицирует стороны соединения во время согласования в 1-й фазе IKE. Термин “предварительное совместное использование” означает, что этот ключ должен быть сообщен другой стороне прежде чем с ней может быть установлен защищенный сеанс. Введите от 8 до 31 символа ASCII (регистр, в котором набраны символы, учитывается) или от 16 до 62 шестнадцатеричных символов (“0-9”, “A-F”). Перед шестнадцатеричным кодом необходимо ставить приставку “0x” (ноль икс). Длина этой приставки не входит в длину ключа (от 16 до 62 символов). Например, в строке “0x0123456789ABCDEF” приставка “0x” означает, что ключ указан в шестнадцатеричном виде, а последовательность “0123456789ABCDEF” является непосредственным ключом. На обоих концах туннеля VPN должен использоваться один и тот же ключ для предварительного совместного использования. Если на обоих концах не используется ключ для предварительного совместного использования, будет получен пакет “PYLD_MALFORMED” (полезная нагрузка плохо сформирована).
Encryption Algorithm	В раскрывающемся списке выберите алгоритм шифрования: **DES**, **3DES** или **AES**. При использовании любого из этих алгоритмов шифрования отправитель и получатель должны использовать один и тот же секретный ключ, который может применяться для шифрования и расшифровки сообщений или для создания и проверки кода аутентификации сообщений. В алгоритме шифрования DES используется 56-битный ключ. Тройной DES (**3DES**) – разновидность **DES**, где используется 168- битовый ключ. Поэтому**3DES** более защищен по сравнению с **DES**. Для него также требуется больше вычислительных мощностей, что увеличивает задержки и снижает производительность. В данной реализации AES используется 128-битный ключ. **AES** обладает большим быстродействием, чем **3DES**.
Authentication Algorithm	В раскрывающемся списке выберите **SHA1** или **MD5**. **MD5** (свертка сообщения, реализация 5) и **SHA1** (защищенный алгоритм хеширования) – это алгоритмы хеширования, используемые для аутентификации данных в пакете. Алгоритм **SHA1** обычно считается более надёжным, чем **MD5**, но он несколько медленнее. Для минимальной защиты можно применять метод **MD5**, а для наибольшей безопасности следует использовать **SHA1**.
SA Life Time (Seconds)	Укажите в этом поле период времени, по истечении которого будет автоматически производиться повторное согласование IKE SA. Допустимый диапазон – от 60 до 3 000 000 секунд (почти 35 дней). Короткий период действия SA позволяет усилить безопасность, давая команду двум межсетевым шлюзам VPN обновлять ключи шифрования и аутентификации. Однако каждый раз при повторном согласовании туннеля VPN все пользователи, получающие доступ к удалённым ресурсам, временно отключаются.

Таб. 88 Расширенная настройка политик VPN

ПОЛЕ	ОПИСАНИЕ
Key Group	Для фазы настройки 1 IKE необходимо выбрать группу ключей. **DH1** (значение по умолчанию) соответствует 1-й группе ключей Диффи-Хелмана, 768-битному случайному числу. **DH2** соответствует 2-й группе ключей Диффи-Хелмана 2, 1024-битному (1K бит) случайному числу.
Phase 2	
Active Protocol	В раскрывающемся списке выберите **ESP** или **AH**.
Encryption Algorithm	Это поле доступно в том случае, если в поле **Active Protocol** выбран протокол **ESP**. В раскрывающемся списке выберите алгоритм шифрования: **DES**, **3DES**, **AES** или **NULL**. При использовании любого из этих алгоритмов шифрования отправитель и получатель должны использовать один и тот же секретный ключ, который может применяться для шифрования и расшифровки сообщений или для создания и проверки кода аутентификации сообщений. В алгоритме шифрования DES используется 56-битный ключ. Тройной DES (**3DES**) – разновидность DES, использующая 168-битный ключ. Поэтому**3DES** более защищен по сравнению с **DES**. Для него также требуется больше вычислительных мощностей, что увеличивает задержки и снижает производительность. В данной реализации AES используется 128-битный ключ. **AES** обладает большим быстродействием, чем **3DES**. Чтобы настроить туннель без шифрования, выберите значение **NULL**. Если выбран режим **NULL**, ключ шифрования вводить не требуется.
Authentication Algorithm	В раскрывающемся списке выберите **SHA1** или **MD5**. MD5 (свертка сообщения, реализация 5) и SHA1 (защищенный алгоритм хеширования) – это алгоритмы хеширования, используемые для аутентификации данных в пакете. Алгоритм SHA1 обычно считается более надёжным, чем MD5, но он несколько медленнее. Для минимальной защиты можно применять метод **MD5**, а для наибольшей безопасности следует использовать **SHA1**.
SA Life Time (Seconds)	Укажите в этом поле период времени, по истечении которого будет автоматически производиться повторное согласование IKE SA. Допустимый диапазон – от 60 до 3 000 000 секунд (почти 35 дней). Короткий период действия SA позволяет усилить безопасность, давая команду двум межсетевым шлюзам VPN обновлять ключи шифрования и аутентификации. Однако каждый раз при повторном согласовании туннеля VPN все пользователи, получающие доступ к удалённым ресурсам, временно отключаются.
Encapsulation	Выберите режим в раскрывающемся списке: **Tunnel** (туннельный) или **Transport** (транспортный).
Perfect Forward Secrecy (PFS)	По умолчанию режим PFS (защита от разглашения использованных ключей) для 2-й фазы согласования SA отключен (**NONE**). Это обеспечивает ускорение настройки IPSec, но снижает уровень безопасности. Чтобы включить PFS, в раскрывающемся списке выберите **DH1** или **DH2**. **DH1** – группа Диффи-Хелмана 1, случайное число 768 бит. **DH2** – группа Диффи-Хелмана 2, случайное число 1024 бит (1 Кбит) (безопасность повышается, производительность снижается).
Back	Для возврата к предыдущему экрану нажмите кнопку **Back**.
Apply	Выберите **Apply** , чтобы сохранить изменения в P-2602 и возвратиться на экран **VPN-IKE**.
Cancel	Нажмите кнопку **Cancel**, чтобы возвратиться на экран **VPN-IKE** без сохранения изменений.

17.14 Ручная настройка ключей

Управление ключами в ручном режиме может применяться при возникновении проблем с управлением ключами посредством **IKE**.

17.14.1 Индекс параметров безопасности (SPI)

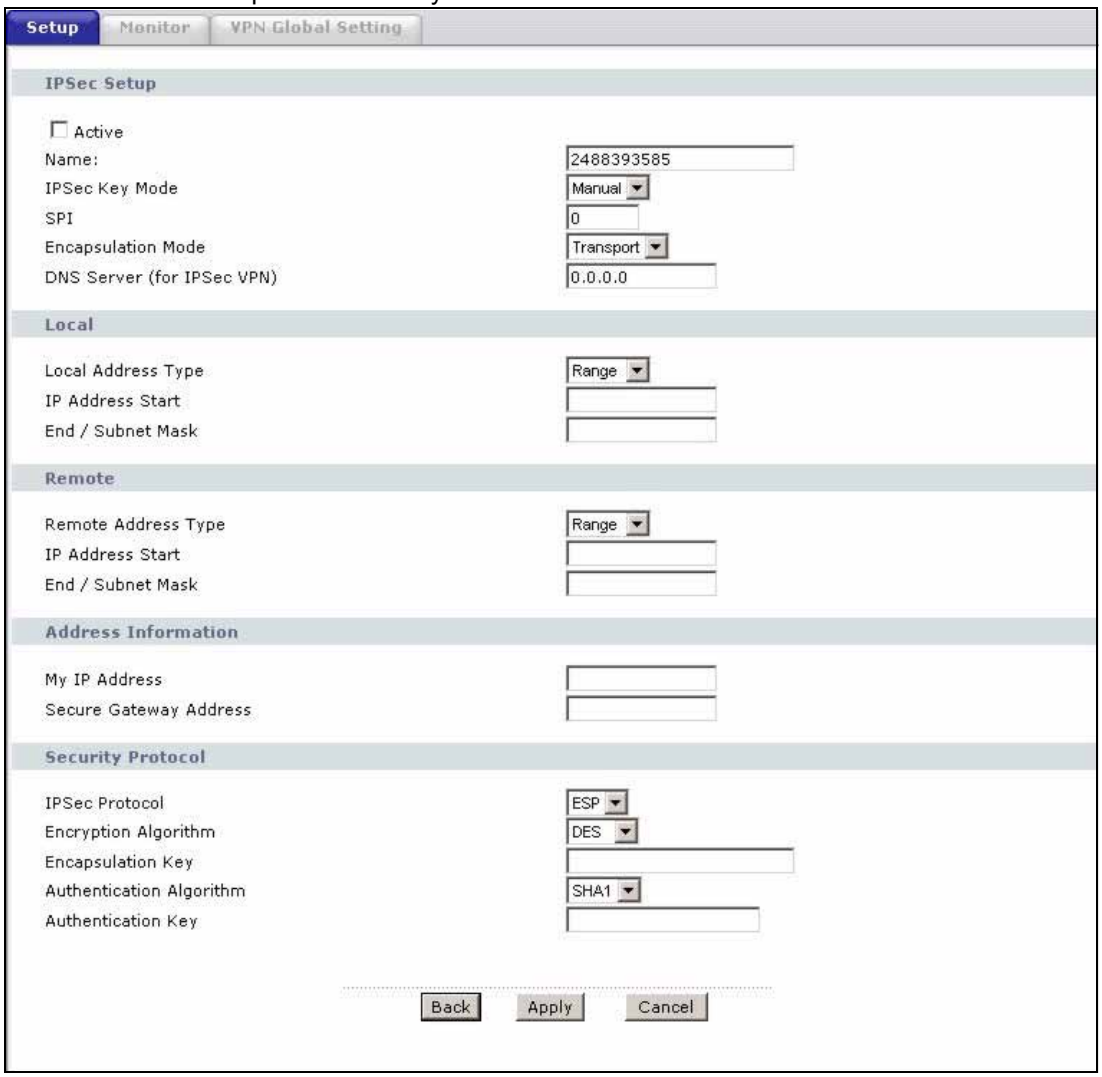
SPI позволяет различать различные SA, имеющие одно место назначения и использующие один и тот же протокол IPSec. Эта информация позволяет мультиплексировать несколько SA в одном шлюзе. Совокупность **SPI** (индекса параметров безопасности) и IP-адреса получателя однозначным образом идентифицирует ассоциацию безопасности (SA). **SPI** передается с удаленного VPN-шлюза на локальный. Локальный VPN-шлюз в этом случае для построения туннеля использует параметры сети, шифрования и ключей, которые администратор связал с индексом SPI.

Текущая реализация ZyXEL предполагает, что входящие и исходящие SPI одинаковы.

17.15 Ввод ключа вручную

Настройка на экране **VPN Manual Key** выполняется только в том случае, если в поле **IPSec Key Mode** на экране **VPN IKE** был выбран режим **Manual**. Экран **VPN Manual Key** показан ниже.

Рис. 127 VPN: экран Manual Key



Поля изображённого выше экрана описаны в следующей таблице.

Таб. 89 VPN: экран Manual Key

ПОЛЕ	ОПИСАНИЕ
IPSec Setup	
Active	Установите этот флажок, чтобы активировать данную политику VPN.
Name	Введите идентификатор данной политики длиной до 32 символов. Можно использовать любые символы, включая пробелы, но конечные пробелы отсекаются P-2602.
IPSec Key Mode	В раскрывающемся списке выберите **IKE** или **Manual**. Режим **Manual** (ручной) используется для устранения неисправностей, если возникают проблемы с использованием режима управления ключами **IKE**.
SPI	Введите десятичное число от 1 до 999999, присваиваемое индексу параметров безопасности.

Таб. 89 VPN: экран Manual Key (продолжение)

ПОЛЕ	ОПИСАНИЕ
Encapsulation Mode	Выберите режим в раскрывающемся списке: **Tunnel** (туннельный) или **Transport** (транспортный).
DNS Server (for IPSec VPN)	Если для данной VPN-сети существует частный DNS-сервер, введите его IP-адрес в этом поле. P-2602 будет назначать этот дополнительный DNS-сервер DHCP-клиентам P-2602, IP-адреса которых находятся в диапазоне локальных адресов данного правила. DNS-сервер позволяет клиентам в сети VPN находить другие компьютеры и серверы в VPN по их (частным) доменным именам.
Local	Локальные IP-адреса должны быть статическими и соответствовать настроенным удалённым IP-адресам удалённого IPSec-маршрутизатора. У двух активных SA не может быть одинаковых локальных и удалённых IP-адресов. Две активных SA могут иметь одинаковый локальный или удалённый IP-адрес, но не оба сразу. Можно настроить несколько SA между одинаковыми локальными и удалёнными IP-адресами, при условии, что в конкретный момент времени активным будет только одна.
Local Address Type	В раскрывающемся меню выберите **Single** (единичный адрес), **Range** (диапазон) или **Subnet** (подсеть). Чтобы задать один IP-адрес, выберите **Single**. Чтобы задать определенный диапазон IP-адресов, выберите **Range**. Чтобы задать подсеть IP-адресов по маске подсети, выберите **Subnet**.
IP Address Start	Если в поле **Local Address Type** выбрано значение **Single**, введите (статический) IP в вашей сети LAN за устройством P-2602. Если в поле **Local Address Type** выбрано **Range**, введите начальный (статический) IP диапазона адресов компьютеров в вашей сети LAN за устройством P-2602. Если в поле **Local Address Type** выбрано **Subnet**, введите (статический) IP-адрес в вашей сети LAN за устройством P-2602.
End / Subnet Mask	Если в поле **Local Address Type** выбрано **Single**, то данное поле не действует. Если в поле **Local Address Type** выбрано **Range**, введите конечный (статический) IP-адрес диапазона IP-адресов компьютеров в вашей сети LAN за устройством P-2602. Если в поле **Local Address Type** выбрано **Subnet**, введите маску подсети, которая соответствует вашей сети LAN за устройством P-2602.
Remote	Удаленные IP-адреса должны быть статическими и соответствовать настроенным локальным IP-адресам удалённого маршрутизатора IPSec. У двух активных SA не может быть одинаковых локальных и удалённых IP-адресов. Две активных SA могут иметь одинаковый локальный или удалённый IP-адрес, но не оба сразу. Можно настроить несколько SA между одинаковыми локальными и удалёнными IP-адресами, при условии, что в конкретный момент времени активным будет только одна.
Remote Address Type	В раскрывающемся меню выберите **Single** (единичный адрес), **Range** (диапазон) или **Subnet** (подсеть). Выберите **Single**, чтобы указать единичный IP-адрес. Чтобы задать определенный диапазон IP-адресов, выберите **Range**. Чтобы задать подсеть IP-адресов по маске подсети, выберите **Subnet**.
IP Address Start	Если в поле **Remote Address Type** выбрано значение Single, введите (статический) IP-адрес в сети за удаленным IPSec-маршрутизатором. Если в поле **Remote Address Type** выбрано **Range**, введите начальный (статический) IP диапазона адресов компьютеров в сети за удаленным IPSec-маршрутизатором. Если в поле **Remote Address Type** выбрано значение **Subnet**, введите (статический) IP-адрес в сети за удаленным IPSec-маршрутизатором.

Таб. 89 VPN: экран Manual Key (продолжение)

ПОЛЕ	ОПИСАНИЕ
End / Subnet Mask	Если в поле **Remote Address Type** выбрано **Single**, то данное поле не действует. Если в поле **Remote Address Type** выбрано **Range**, введите конечный (статический) IP-адрес диапазона IP-адресов компьютеров в сети за удаленным IPSec-маршрутизатором. Если в поле **Remote Address Type** выбрано значение **Subnet**, введите маску подсети, которая соответствует сети за удаленным IPSec-маршрутизатором.
Address Information	
My IP Address	Введите IP-адрес вашего устройства P-2602 в сети WAN. Туннель VPN необходимо построить заново в случае изменения этого IP-адреса. Если в этом поле введен адрес **0.0.0.0**, действует следующий алгоритм: Для настройки VPN-туннеля P-2602 использует текущий IP-адрес (статический или динамический), присвоенный P-2602 в сети WAN (static or dynamic). При обрыве соединения с WAN P-2602 использует для туннеля VPN IP-адрес резервирования через коммутируемый доступ или IP-адрес в LAN, если используется переадресация трафика. Подробнее о резервировании через коммутируемый доступ и переадресации трафика см. гл. 7 на стр. 99.
Secure Gateway Address	Введите IP-адрес в сети WAN или URL (до 31 символа) маршрутизатора IPSec, к которому производится подключение по VPN.
Security Protocol	
IPSec Protocol	Выберите **ESP**, чтобы использовать протокол ESP (Encapsulation Security Payload). Протокол ESP (RFC 2406) реализует шифрование в дополнение к функциям, обеспечиваемым **AH**. Если в этом поле выбран протокол ESP, необходимо также настроить параметры в полях **Encryption Algorithm** и**Authentication Algorithm** (см. ниже).
Encryption Algorithm	В раскрывающемся списке выберите алгоритм шифрования: **DES**, **3DES** или **NULL**. При использовании **DES** для обмена данными отправитель и получатель должны знать один и тот же секретный ключ, который может использоваться для шифрования и дешифровки сообщений или для создания и проверки кода аутентификации сообщений. В алгоритме шифрования **DES** используется 56-битный ключ. Тройной DES (**3DES**) – разновидность **DES**, где используется 168- битовый ключ. Поэтому**3DES** более защищен по сравнению с **DES**. Для него также требуется больше вычислительных мощностей, что увеличивает задержки и снижает производительность. Чтобы настроить туннель без шифрования, выберите значение **NULL**. Если выбран режим **NULL**, ключ шифрования вводить не требуется.
Encapsulation Key (only with ESP)	Если используется алгоритм **DES**, введите уникальный ключ длиной 8 символов. Если используется алгоритм **3DES**, введите уникальный ключ длиной 24 символа. Могут использоваться любые символы, включая пробелы, но конечные пробелы отсекаются.
Authentication Algorithm	В раскрывающемся списке выберите **SHA1** или **MD5**. **MD5** (свертка сообщения, реализация 5) и **SHA1** (защищенный алгоритм хеширования) – это алгоритмы хеширования, используемые для аутентификации данных в пакете. Алгоритм **SHA1** обычно считается более надёжным, чем **MD5**, но он несколько медленнее. Для минимальной защиты можно применять метод **MD5**, а для наибольшей безопасности следует использовать **SHA1**.
Authentication Key	Введите уникальный ключ аутентификации, который должен использоваться IPSec, если он необходим. Для аутентификации **MD5** введите ключ длиной 16 символов, для аутентификации **SHA-1** – 20 символов. Можно использовать любые символы, включая пробелы, но конечные пробелы отсекаются.

Таб. 89 VPN: экран Manual Key (продолжение)

ПОЛЕ	ОПИСАНИЕ
Back	Для возврата к предыдущему экрану нажмите кнопку **Back**.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-2602.

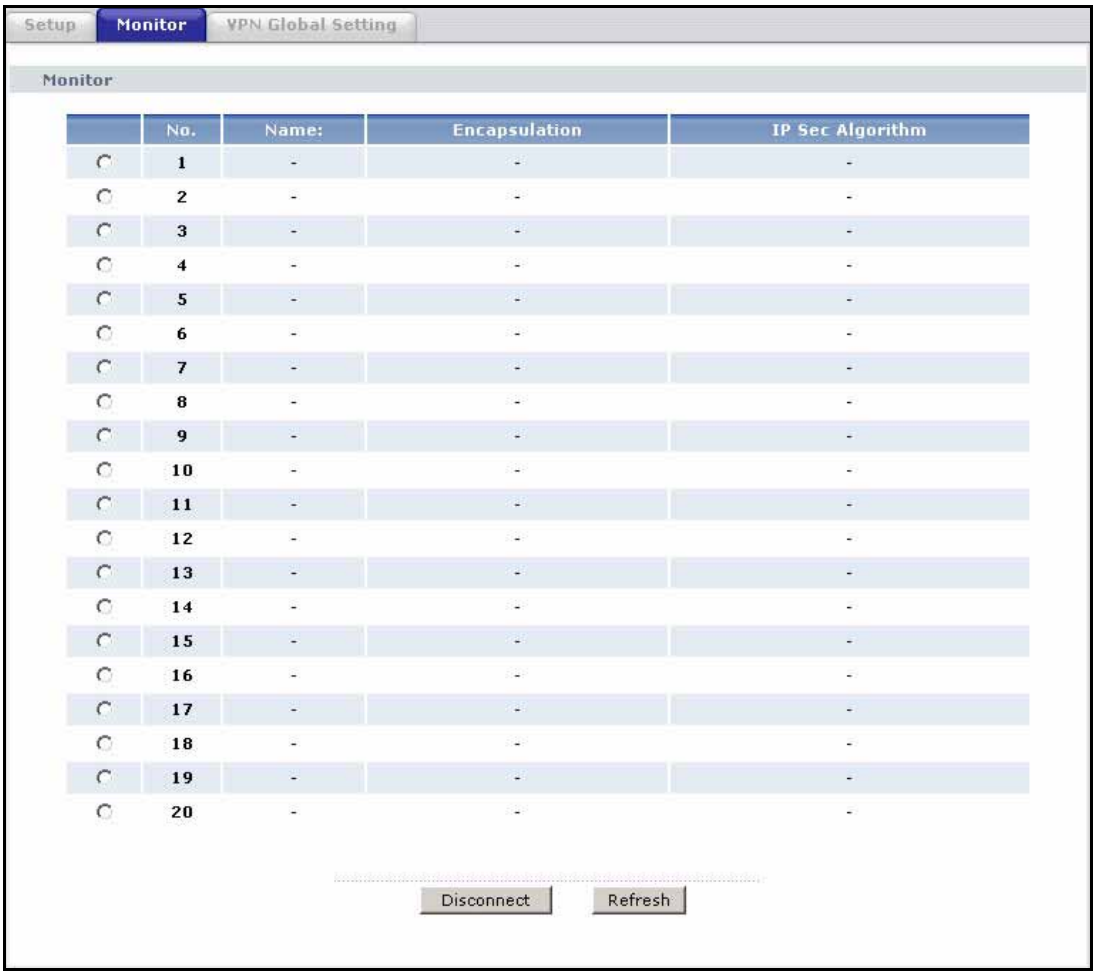
17.16 Использование монитора SA

Чтобы перейти на показанный ниже экран **SA Monitor**, выберите **Security**, **VPN**, затем – **Monitor**. Этот экран служит для просмотра активных соединений VPN и управления ими.

Ассоциация безопасности (SA) – это группа настроек безопасности, относящаяся к конкретному туннелю VPN. На этом экране приведен список активных соединений VPN. Чтобы просмотреть соединения, активные в данный момент, нажмите **Refresh**. Этот экран доступен только для чтения. Поля на вкладке описаны в следующей таблице.

Если есть исходящий трафик, но нет входящего, время ожидания SA автоматически заканчивается через 2 минуты. Туннель без исходящего или входящего трафика считается “бездействующим”, и его время ожидания заканчивается тогда, когда заканчивается время существования SA. В разд. 17.6 на стр. 246описаны настройки, при которых P-2602 будет по истечении срока действия IPSec SA повторно согласовывать даже если трафик отсутствует.

Рис. 128 VPN: Монитор SA



Поля изображённого выше экрана описаны в следующей таблице.

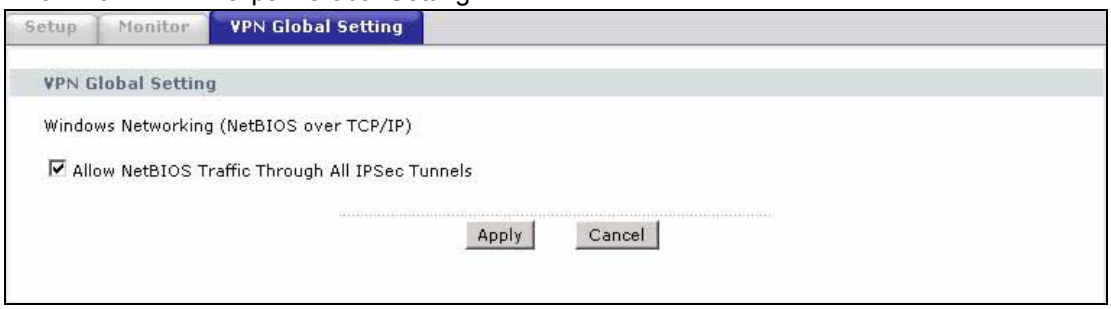
Таб. 90 VPN: монитор SA

ПОЛЕ	ОПИСАНИЕ
No	В этом поле указан порядковый номер ассоциации безопасности.
Name	В данном поле отображается идентификационное имя для данной политики VPN.
Encapsulation	В этом поле отображается режим: **Tunnel** (туннельный) или **Transport** (транспортный).
IPSec Algorithm	В этом поле отображается протокол безопасности, алгоритм шифрования и алгоритм аутентификации, используемый каждым туннелем VPN.
Disconnect	Чтобы прекратить действие одной из ассоциаций безопасности, выберите ее и нажмите **Disconnect**.
Refresh	Нажмите **Refresh**, чтобы на экране отобразились VPN-соединения, активные в данный момент.

17.17 Настройка глобальных параметров

Для настройки глобальных параметров P-2602, относящихся к VPN, выберите **VPN**, затем – **Global Setting**. Появится изображенный ниже экран.

Рис. 129 VPN: экран Global Setting



Поля изображённого выше экрана описаны в следующей таблице.

Таб. 91 VPN: экран Global Setting

ПОЛЕ	ОПИСАНИЕ
Windows Networking (NetBIOS over TCP/IP)	Пакеты NetBIOS (Network Basic Input/Output System) - это TCP- или UDP-пакеты, которые позволяют компьютеру обнаруживать другие компьютеры. Иногда требуется разрешить пакетам NetBIOS проходить через туннели VPN, чтобы компьютеры в локальной сети находили компьютеры в удаленной сети и наоборот.
Allow NetBIOS Traffic Through All IPSec Tunnels	Отметьте этот флажок, чтобы разрешить пересылку пакетов NetBIOS через VPN-соединение.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-2602.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

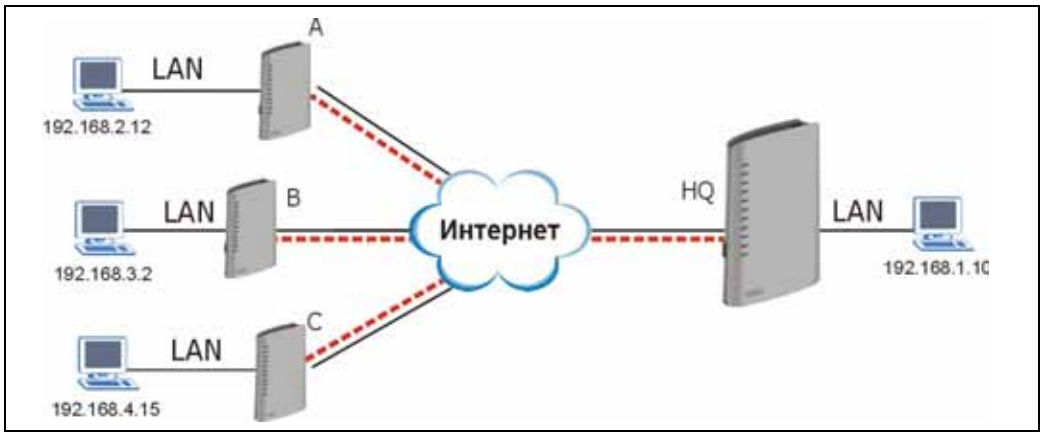
17.18 Примеры настройки VPN/IPSec для дистанционных сотрудников

В следующих примерах рассматривается установление нескольких VPN-соединений между дистанционными сотрудниками и одним устройством P-2602 в штаб-квартире. Дистанционные сотрудники используют IPSec-маршрутизаторы с динамическими IP-адресами в сети WAN. Устройству P-2602 в штаб-квартире присвоен статический глобальный IP-адрес.

17.18.1 Пример совместного использования одного правила VPN несколькими дистанционными сотрудниками

На следующем рисунке и в таблице приведен пример конфигурации, позволяющей нескольким дистанционным сотрудникам (A, B и C) использовать одно правило VPN для одновременного доступа к P-2602 в штаб-квартире (на рисунке – “HQ”). IP-адресам IPSec-маршрутизаторов дистанционных сотрудников в сети WAN не присвоены доменные имена. Все дистанционные сотрудники должны одинаковые параметры IPSec, но локальные IP-адреса (или диапазоны адресов) не должны перекрываться.

Рис. 130 Пример совместного использования одного правила VPN несколькими дистанционными сотрудниками



Таб. 92 Пример совместного использованием одного правила VPN несколькими дистанционными сотрудниками

ПОЛЯ	ДИСТАНЦИОННЫЕ СОТРУДНИКИ	ШТАБ-КВАРТИРА
My IP Address:	0.0.0.0 (динамический IP-адрес, назначенный поставщиком услуг Интернета)	Глобальный статический IP-адрес
Secure Gateway IP Address:	Глобальный статический IP-адрес	0.0.0.0 Если указан этот IP-адрес, то туннель IPSec может инициироваться только дистанционным сотрудником.
Local IP Address:	Сотрудник A: 192.168.2.12 Сотрудник B: 192.168.3.2 Сотрудник C: 192.168.4.15	192.168.1.10
Remote IP Address:	192.168.1.10	0.0.0.0 (не применяется)

17.18.2 Пример использования уникальных правил VPN различными дистанционными сотрудниками

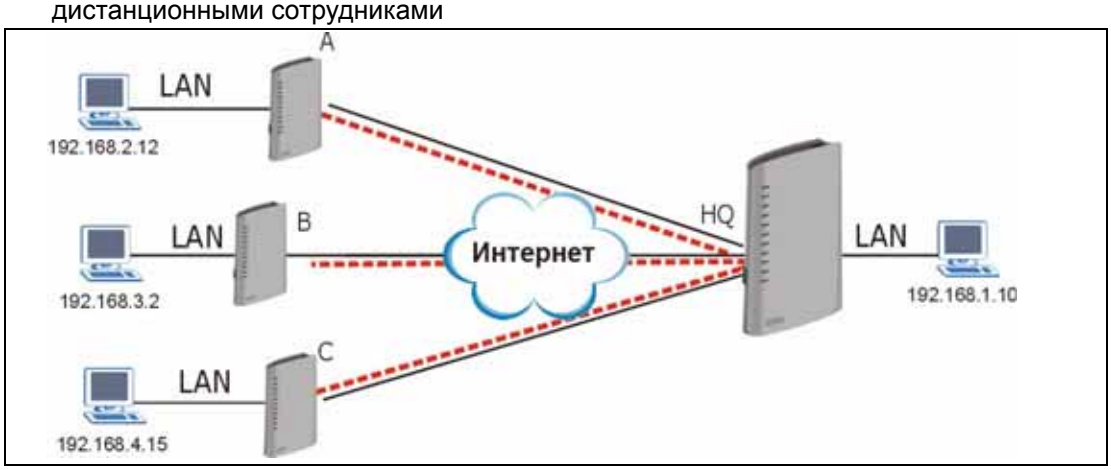
В этом примере дистанционные сотрудники (A, B и C) используют маршрутизаторы IPSec. Динамическим IP-адресам маршрутизаторов в сети WAN присвоены доменные имена (для этого используется динамическая служба DNS).

В режиме агрессивного согласования (см. разд. 17.12.1 на стр. 257) P-2602 может различать правила VPN по типам и содержанию идентификаторов. Дистанционные сотрудники могут использовать отдельные правила VPN для одновременного доступа к P-2602 в штаб-квартире. Они могут использовать различные параметры IPSec. Локальные IP-адреса (или диапазоны адресов) в правилах, настроенных на P-2602 в штаб-квартире, могут перекрываться. Локальные IP-адреса правил, настроенных на IPSec-маршрутизаторах дистанционных сотрудников, перекрываться не должны.

В следующей таблице и на рисунке рассмотрен пример, в котором каждый из трех дистанционных сотрудников использует отдельное VPN-правило для VPN-соединения с P-2602, расположенным в штаб-квартире. P-2602 в штаб-квартире (на рисунке – “HQ”) идентифицирует каждый поступающий SA по типу и содержанию его идентификатора и устанавливает VPN-соединение, используя соответствующее правило VPN.

P-2602 в штаб-квартире может также инициировать VPN-соединения с дистанционными сотрудниками, находя их по доменным именам.

Рис. 131 Пример использования уникальных правил VPN различными дистанционными сотрудниками



Таб. 93 Пример использования уникальных правил VPN различными дистанционными сотрудниками

ДИСТАНЦИОННЫЕ СОТРУДНИКИ	ШТАБ-КВАРТИРА
Правила для всех дистанционных сотрудников:	Все правила для штаб-квартиры:
My IP Address 0.0.0.0	My IP Address: bigcompanyhq.com
Secure Gateway Address: bigcompanyhq.com	Local IP Address: 192.168.1.10
Remote IP Address: 192.168.1.10	Local ID Type: E-mail
Peer ID Type: E-mail	Local ID Content: bob@bigcompanyhq.com
Peer ID Content: bob@bigcompanyhq.com	
Сотрудник A (telecommutera.dydns.org)	Правило 1 для P-2602 в штаб-квартире:

Таб. 93 Пример использования уникальных правил VPN различными дистанционными сотрудниками (продолжение)

ДИСТАНЦИОННЫЕ СОТРУДНИКИ	ШТАБ-КВАРТИРА
Local ID Type: IP	Peer ID Type: IP
Local ID Content: 192.168.2.12	Peer ID Content: 192.168.2.12
Local IP Address: 192.168.2.12	Secure Gateway Address: telecommuter1.com
	Remote Address 192.168.2.12
Сотрудник B (telecommuterb.dydns.org)	Правило 2 для P-2602 в штаб-квартире:
Local ID Type: DNS	Peer ID Type: DNS
Local ID Content: telecommuterb.com	Peer ID Content: telecommuterb.com
Local IP Address: 192.168.3.2	Secure Gateway Address: telecommuterb.com
	Remote Address 192.168.3.2
Сотрудник C (telecommuterc.dydns.org)	Правило 3 для P-2602 в штаб-квартире:
Local ID Type: E-mail	Peer ID Type: E-mail
Local ID Content: myVPN@myplace.com	Peer ID Content: myVPN@myplace.com
Local IP Address: 192.168.4.15	Secure Gateway Address: telecommuterc.com
	Remote Address 192.168.4.15

17.19 VPN и удаленное управление

Если VPN-туннель использует Telnet, FTP или WWW, то для доступа к соответствующей службе необходимо настроить удаленное управление (**Remote Management**).

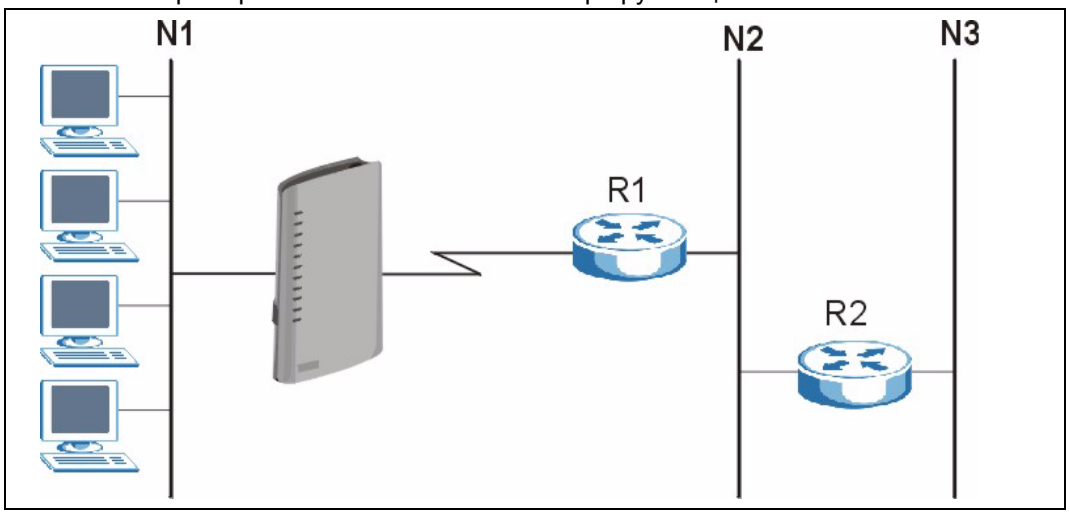
Глава 18
Статическая маршрутизация

В этой главе описывается настройка статических маршрутов для P-2602.

18.1 Статическая маршрутизация

Каждый удаленный узел определяет только ту сеть, к которой непосредственно подключен маршрутизатор, и P-2602 не имеет информации о сетях, расположенных за ее пределами. Например, на следующем рисунке P-2602 получает сведения о сети N2 через удалённый маршрутизатор R1. Однако P-2602 не имеет возможности отправить пакет в сеть N3, поскольку ему неизвестно о существовании маршрута через удалённый маршрутизатор R1 (и далее через R2). Статические маршруты позволяют сообщать P-2602 о сетях, находящихся за пределами удаленных узлов.

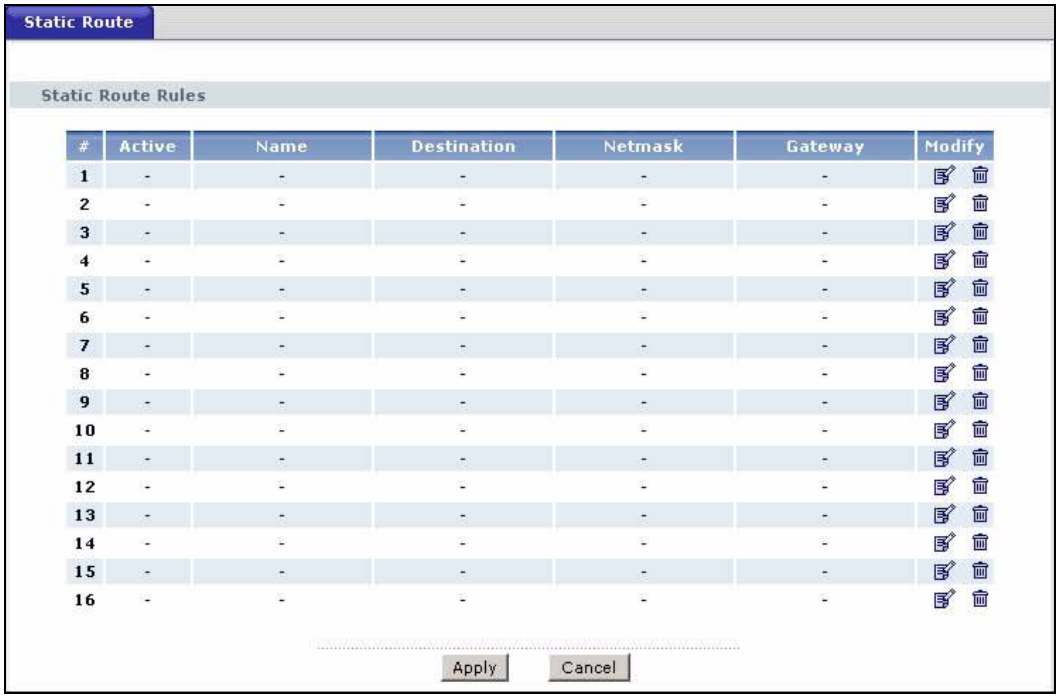
Рис. 132 Пример топологии статической маршрутизации



18.2 Настройка статической маршрутизации

Чтобы перейти на экран **Static Route**, выберите **Advanced > Static Route**.

Рис. 133 Статическая маршрутизация



Поля изображённого выше экрана описаны в следующей таблице.

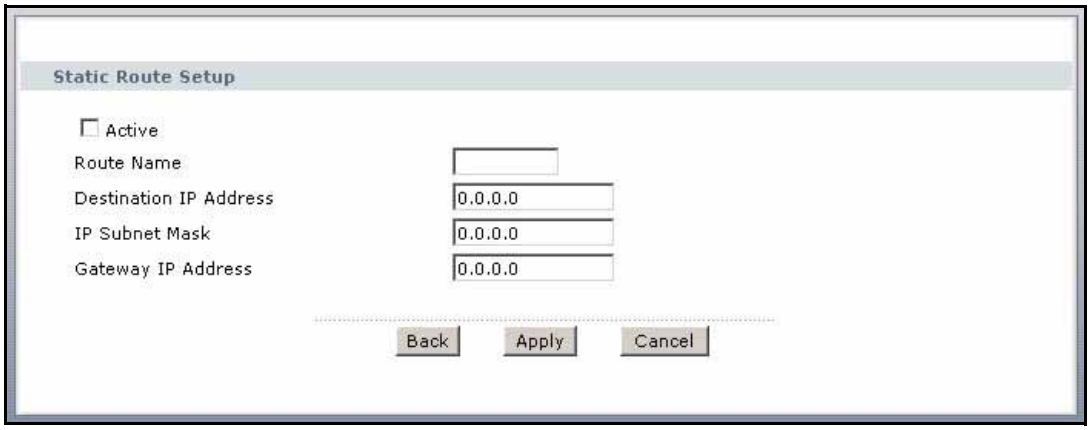
Таб. 94 Статическая маршрутизация

ПОЛЕ	ОПИСАНИЕ
#	В этом поле отображается номер статического маршрута.
Active	Это поле показывает, активен ли данный статический маршрут: **Yes (Да)** или **No (Нет)**.
Name	В этом поле выводится описание или идентификация данного машрута.
Destination	Этот параметр указывает IP-адрес конечной точки маршрута. Маршрутизация всегда подразумевает диапазон сетевых адресов.
Netmask	Этот параметр указывает маску подсети конечной точки маршрута.
Gateway	Это – IP-адрес интернет-центра. Шлюз - это маршрутизатор или коммутатор, расположенный в одном сегменте с LAN- или WAN-портом устройства. Шлюз пересылает пакеты к месту назначения.
Modify	Чтобы перейти на экран задания статических маршрутов для P-2602, щелкните на значке редактирования. Щелкните на значке удаления, чтобы удалить статический маршрут из P-2602. Появится окно с просьбой подтвердить удаление маршрута.
Apply	Нажмите эту кнопку, чтобы сохранить изменения в P-2602.
Cancel	Нажмите эту кнопку, чтобы вернуться к прежнему состоянию настроек.

18.2.1 Редактирование статического маршрута

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

Рис. 134 Редактирование статического маршрута



Поля соответствующего экрана описаны в следующей таблице.

Таб. 95 Редактирование статического маршрута

ПОЛЕ	ОПИСАНИЕ
Active	Это поле позволяет активировать/деактивировать данный статический маршрут.
Route Name	Введите имя статического IP-маршрута. Для удаления данного статического маршрута оставьте это поле пустым.
Destination IP Address	Этот параметр указывает IP-адрес конечной точки маршрута. Маршрутизация всегда подразумевает диапазон сетевых адресов. Если требуется указать маршрут до отдельного хоста, в поле “IP Subnet Mask” введите маску подсети 255.255.255.255 – при этом диапазон сетевых адресов будет ограничен до адреса хоста.
IP Subnet Mask	Введите маску подсети IP.
Gateway IP Address	Введите IP-адрес интернет-центра. Шлюз - это маршрутизатор или коммутатор, расположенный в одном сегменте с LAN- или WAN-портом устройства. Шлюз пересылает пакеты к месту назначения.
Back	Для возврата к предыдущему экрану без сохранения настроек нажмите кнопку **Back**.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-2602.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

Глава 19
Управление полосой пропускания

В этой главе описывается настройка управления полосой пропускания, редактирование правил и просмотр журналов управления полосой пропускания в P-2602.

19.1 Обзор средств управления полосой пропускания

Средства управления полосой пропускания в устройствах ZyXEL позволяют задать правила управления полосой пропускания для различных приложений и/или подсетей. Каждое из правил предусматривает выделение определенной полосы пропускания (“бюджета”).

P-2602 применяет правила управления полосой пропускания к трафику, проходящему через интерфейс. P-2602 не контролирует полосу пропускания для входящего трафика на интерфейсе.

Управление полосой пропускания применяется ко всему трафику, выходящему из маршрутизатора, независимо от источника трафика.

Переадресация трафика или совмещение IP-адресов могут вызывать прохождение трафика из LAN в LAN через P-2602, в результате чего на трафик также будут распространяться правила управления полосой пропускания.

- Сумма выделяемых долей полосы пропускания для интерфейса WAN (трафик из LAN в WAN, из WLAN в WAN) должна быть меньше или равна скорости интерфейса WAN, настроенной на экране **Bandwidth Management Summary**.
- Сумма выделяемых долей полосы пропускания для порта LAN (трафик из WAN в LAN, из WLAN в LAN) должна быть меньше или равна скорости интерфейса LAN, настроенной на экране **Bandwidth Management Summary**.
- Сумма выделяемых долей полосы пропускания для интерфейса WLAN (трафик из LAN в WLAN, из WAN в WLAN) должна быть меньше или равна скорости интерфейса WLAN, настроенной на экране **Bandwidth Management Summary**.

19.2 Управление полосой пропускания с учетом приложений

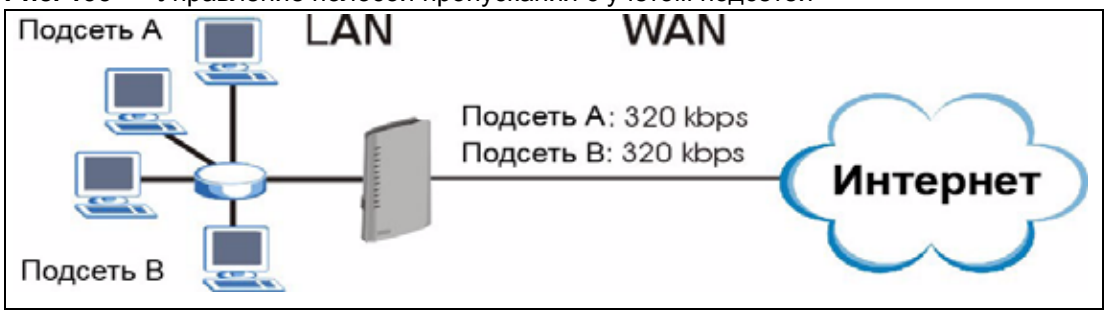
Можно настроить классы полосы пропускания для различных приложений (например, VoIP, WWW, FTP, электронная почта и потоковое видео).

19.3 Управление полосой пропускания с учетом подсетей

Можно определить классы полосы пропускания в зависимости от подсетей.

Пример подсетей LAN приведён на следующем рисунке. Для подсети **A** можно настроить один класс полосы пропускания, а для подсети **B** – другой.

Рис. 135 Управление полосой пропускания с учетом подсетей



19.4 Управление полосой пропускания с учетом приложений и подсетей

Классы полосы пропускания можно также создавать для сочетания подсети и типа приложения. В следующей таблице иллюстрируется пример распределения полосы пропускания для трафика определенноых приложений от отдельных подсетей LAN.

Таб. 96 Пример управления полосой пропускания с учетом приложений и подсетей

ТИП ТРАФИКА	ОТ ПОДСЕТИ A	ОТ 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
Видеоданные	64 кбит/с	64 кбит/с

19.5 Планировщик

Планировщик распределяет полосу пропускания интерфейса по классам полосы пропускания. В P-2602 реализованы планировщики двух типов: на основе равнодоступности и на основе приоритета.

19.5.1 Планировщик на основе приоритета

С планировщиком на основе приоритета P-2602 передает трафик от различных классов полосы пропускания согласно приоритетам, назначенным для классов полосы пропускания. Чем больше номер приоритета, тем выше приоритет класса полосы пропускания. Повышение приоритета позволяет добиться более равномерной работы приложений реального времени (например, использующих аудио или видеоданные).

19.5.2 Планировщик на основе равнодоступности

С планировщиком на основе равнодоступности P-2602 одинаково делит полосу пропускания среди классов полосы пропускания и не позволяет одному классу полосы пропускания использовать всю полосу пропускания интерфейса.

19.6 Максимизация использования полосы пропускания

Параметр максимизации использования полосы пропускания (см. рис. 136 на стр. 283) позволяет P-2602 поделить доступную полосу пропускания интерфейса (включая невыделенную полосу пропускания и неиспользуемую выделенную полосу пропускания в конкретном классе) между классами, требующими большей полосы пропускания.

При максимизации использования полосы пропускания P-2602 сначала проверяется, получает ли каждый класс полосы пропускания необходимую долю полосы. Далее P-2602 делит “доступную” полосу пропускания интерфейса (не присвоенную бюджетам или неиспользуемую классами) в зависимости от того, скольким классам полосы пропускания и с каким приоритетом требуется расширить полосу. Когда только одному классу требуется увеличенная полоса, P-2602 выделяет дополнительную полосу пропускания только этому классу.

Когда расширить полосу требуется нескольким классам P-2602 сначала выделяет доступную полосу классам с наибольшим приоритетом (полностью удовлетворяя требования класса, если имеется достаточная полоса пропускания), а затем распределяет остаток полосы, если он имеется, между менее приоритетными классами. P-2602 равномерно распределяет доступную полосу пропускания между классами с одинаковым уровнем приоритета.

19.6.1 Резервирование полосы пропускания для трафика, не отнесенного к классам

Чтобы разрешить P-2602 выделять полосу пропускания трафику, не указанному в фильтре полосы пропускания, выполните следующие действия.

1. Не включайте для интерфейса параметр **Maximize Bandwidth Usage**.
2. Оставьте некоторую часть полосы пропускания интерфейса, не внося ее в бюджет. Удостоверьтесь, что корневой класс интерфейса имеет большую полосу, чем сумма полос в относящихся к нему правилах.

19.6.2 Пример максимизации использования полосы пропускания

Рассмотрим пример настройки P-2602 с максимизацией использования полосы пропускания на одном из интерфейсов. В следующей таблице представлен бюджет полосы пропускания для каждого класса. Классы настроены для различных подсетей. Суммарная полоса для интерфейса – 10240 кбит/с. Каждой подсети выделено 2048 кбит/с. Оставшиеся вне бюджета 2048 кбит/с используются для исходящего трафика, не определенного ни в одном из фильтров полосы пропускания, если флажок максимизации используемой полосы снят.

Таб. 97 Пример максимизации использования полосы пропускания

КЛАССЫ И РАСПРЕДЕЛЯЕМЫЕ ДОЛИ ПОЛОСЫ ПРОПУСКАНИЯ	
Корневой класс: 10240 кбит/с	Администрация: 2048 кбит/с
	Отдел продаж: 2048 кбит/с
	Маркетинговый отдел: 2048 кбит/с
	Исследовательский сектор: 2048 кбит/с

P-2602 делит неиспользуемые 2048 кбит/с между классами, требующими большей полосы пропускания. Если администрация только использует 1024 кбит/с из выделенных 2048 кбит/с, P-2602 также делит оставшиеся 1024 кбит/с среди классов, которым требуется большая полоса пропускания. Таким образом, P-2602 делит 3072 кбит/с невыделенной и неиспользованной полосы пропускания между классами, которым требуется увеличенная полоса пропускания.

19.6.2.1 Распределение неиспользованной и невыделенной полосы пропускания на основе приоритетов

В следующей таблице указаны приоритеты классов полосы пропускания и доля полосы пропускания, выделяемая каждому классу.

Таб. 98 Пример распределения неиспользованной и невыделенной полосы пропускания на основе приоритетов

КЛАССЫ, ПРИОРИТЕТЫ И РАСПРЕДЕЛЯЕМЫЕ ДОЛИ	
Корневой класс: 10240 кбит/с	Администрация: Приоритет 4, 1024 кбит/с
	Отдел продаж: Приоритет 6, 3584 кбит/с
	Маркетинговый отдел: Приоритет 6, 3584 кбит/с
	Исследовательский сектор: Приоритет 5, 2048 кбит/с

Предположим, что все классы за исключением администрации нуждаются в увеличенной полосе пропускания.

- Каждый класс использует выделенную ему полосу пропускания. Класс “Администрация” получает только 1024 кбит/с вместо выделенных 2048 кбит/с.
- Отделы продаж и маркетинга первыми получают дополнительную полосу пропускания, потому что они имеют самый высокий приоритет (6). Если каждому из них требуется не менее 1536 кбит/с дополнительной полосы пропускания, P-2602 делит общие 3072 кбит/с невыделенной и неиспользованной полосы пропускания равномерно между отделами продаж и маркетинга (каждому – дополнительно по 1536 кбит/с, т.е. в общей сложности каждый класс получает по 3584 кбит/с), потому что оба класса имеют самый высокий приоритет.
- Исследовательскому сектору также требуется увеличенная полоса, но он получает только выделенные для него 2048 кбит/с, потому что вся невыделенная и неиспользованная полоса пропускания распределяется между отделами продаж и маркетинга, имеющими более высокий приоритет.

19.6.2.2 Распределение неиспользованной и невыделенной полосы пропускания на основе приоритетов

В следующей таблице представлен бюджет полосы пропускания для каждого класса.

Таб. 99 Распределение неиспользованной и невыделенной полосы пропускания на основе приоритетов

КЛАССЫ И РАСПРЕДЕЛЯЕМЫЕ ДОЛИ ПОЛОСЫ ПРОПУСКАНИЯ	
Корневой класс: 10240 кбит/с	Администрация: 1024 кбит/с
	Отдел продаж: 3072 кбит/с
	Маркетинговый отдел: 3072 кбит/с
	Исследовательский сектор: 3072 кбит/с

Предположим, что все классы за исключением администрации нуждаются в увеличенной полосе пропускания.

- Каждый класс использует выделенную ему полосу пропускания. Класс “Администрация” получает только 1024 кбит/с вместо выделенных 2048 кбит/с.
- Таким образом, P-2602 делит 3072 кбит/с невыделенной и неиспользованной полосы пропускания между классами, которым требуется увеличенная полоса пропускания. Каждому дополнительно достается по 1024 кбит/с, т.е. все остальные классы получают в общей сложности 3072 кбит/с.

19.6.3 Приоритеты для управления полосой пропускания

Трафик с более высоким приоритетом проходит быстрее, в то время как трафик с более низким приоритетом отбрасывается, если сеть переполнена. В следующей таблице описаны приоритеты, которые можно применять к трафику, отправляемому P-2602 через интерфейс.

Таб. 100 Приоритеты для управления полосой пропускания

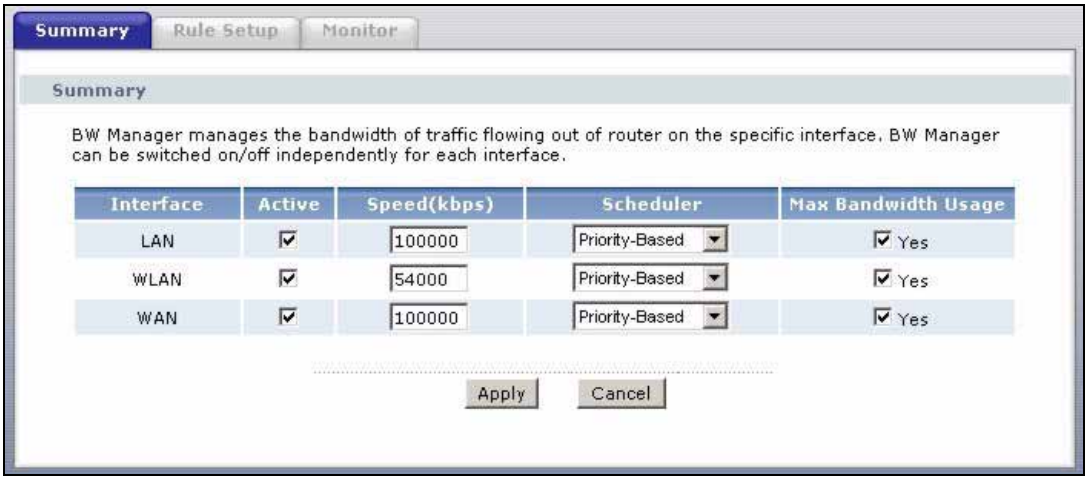
ПРИОРИТЕТ	ОПИСАНИЕ
Высокий (High)	Обычно применяется для голосового или видеотрафика, особенно чувствительного к неустойчивой синхронизации (т.е. к изменчивости задержек).
Средний (Mid)	Обычно применяется для трафика, требующего передачи при первой возможности или с преимуществом относительно других видов трафика – например, для важного рабочего трафика, допускающего некоторую задержку.
Низкий (Low)	Обычно применяется для некритичного “фонового” трафика, например, для неконтролируемой передачи данных, наличие которой допускается, но не должно никоим образом сказываться на других задачах и пользователях.

19.7 Настройка на сводном экране

Чтобы перейти на показанный ниже экран, выберите **Advanced > Bandwidth MGMT** .

Включите управление полосой пропускания на интерфейсе и установите максимальную разрешенную полосу пропускания для этого интерфейса.

Рис. 136 Управление полосой пропускания: сводный экран



Поля изображённого выше экрана описаны в следующей таблице.

Таб. 101 Управление полосой пропускания: сводный экран

ПОЛЕ	ОПИСАНИЕ
Interface	В этих нередактируемых полях отображаются физические интерфейсы. Чтобы включить для интерфейса управление полосой пропускания, отметьте флажок. Управление полосой пропускания применяется ко всему трафику, выходящему через интерфейс, независимо от источника трафика. Переадресация трафика или совмещение IP-адресов могут вызывать прохождение трафика из LAN в LAN через P-2602, в результате чего на трафик также будут распространяться правила управления полосой пропускания.
Active	Чтобы включить для интерфейса управление полосой пропускания, отметьте флажок.
Speed (kbps)	Введите величину полосы пропускания для этого интерфейса, которую вы хотите распределить через управление полосой пропускания. Эта величина станет бюджетом для корневого класса интерфейса. Рекомендуется установить здесь фактическую скорость передачи данных через интерфейс. Например, если ваше интернет-подключение имеет скорость восходящего канала 1 Мбит/с, установите скорость интерфейса WAN 1000 кбит/с. Если это число выше чем фактическая скорость передачи интерфейса, и вы настроили правила для всей ширины полосы пропускания, то более приоритетный трафик может использовать всю полосу пропускания, и в этом случае трафик с низким приоритетом не пропускается. **Примечание:** Если не включен флажок **Max Bandwidth Usage**, P-2602 примет в качестве полосы пропускания значение, заданное в этом поле. P-2602 не будет использовать дополнительную полосу пропускания для соединений через этот интерфейс, даже если исходящая полоса пропускания у этого интерфейса выше.

Таб. 101 Управление полосой пропускания: сводный экран (продолжение)

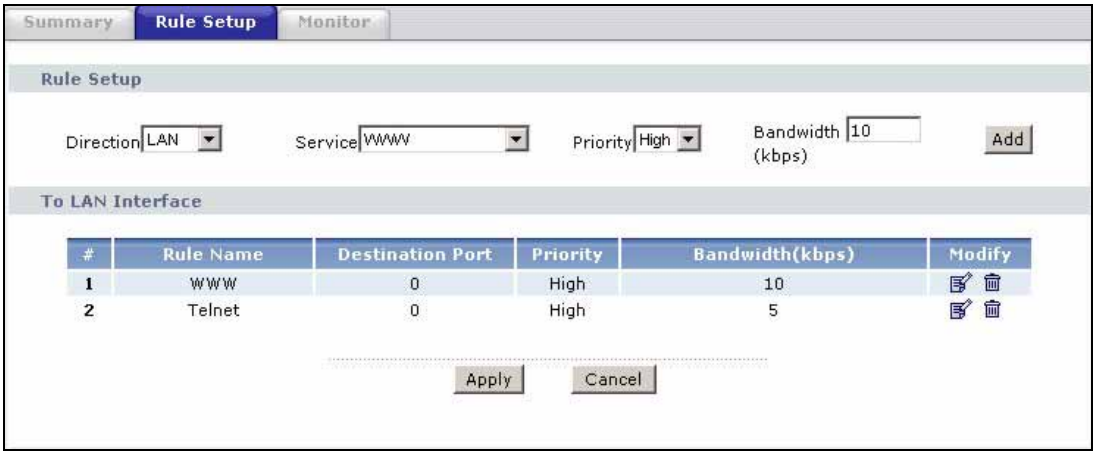
ПОЛЕ	ОПИСАНИЕ
Scheduler	В раскрывающемся меню выберите тип планировщика для трафика: **Priority-Based** (на осное приоритета) или **Fairness-Based** (на основе равнодоступности). Выберите **Priority-Based**, чтобы обслуживать в первую очередь более приоритетные классы. Выберите **Fairness-Based**, чтобы применять одинаковые условия для всех классов приоритета.
Max Bandwidth Usage	Отметьте этот флажок, чтобы указать P-2602 делить всю невыделенную и/или неиспользованную полосу пропускания интерфейса среди классов, которым требуется дополнительная полоса. Снимите этот флажок, если вы хотите зарезервировать полосу пропускания для трафика, который не относится ни к одному из классов, или если требуется ограничить скорость передачи через этот интерфейс (см. описание поля **Speed**).
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-2602.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

19.8 Настройка правил управления полосой пропускания

Прежде чем настраивать правила для интерфейса, необходимо отметить этот интерфейс флажком на экране **Bandwidth Management Summary**.

Выберите **Advanced > Bandwidth MGMT > Rule Setup**, чтобы перейти на показанный ниже экран.

Рис. 137 Управление полосой пропускания: настройка правил



Поля изображённого выше экрана описаны в следующей таблице.

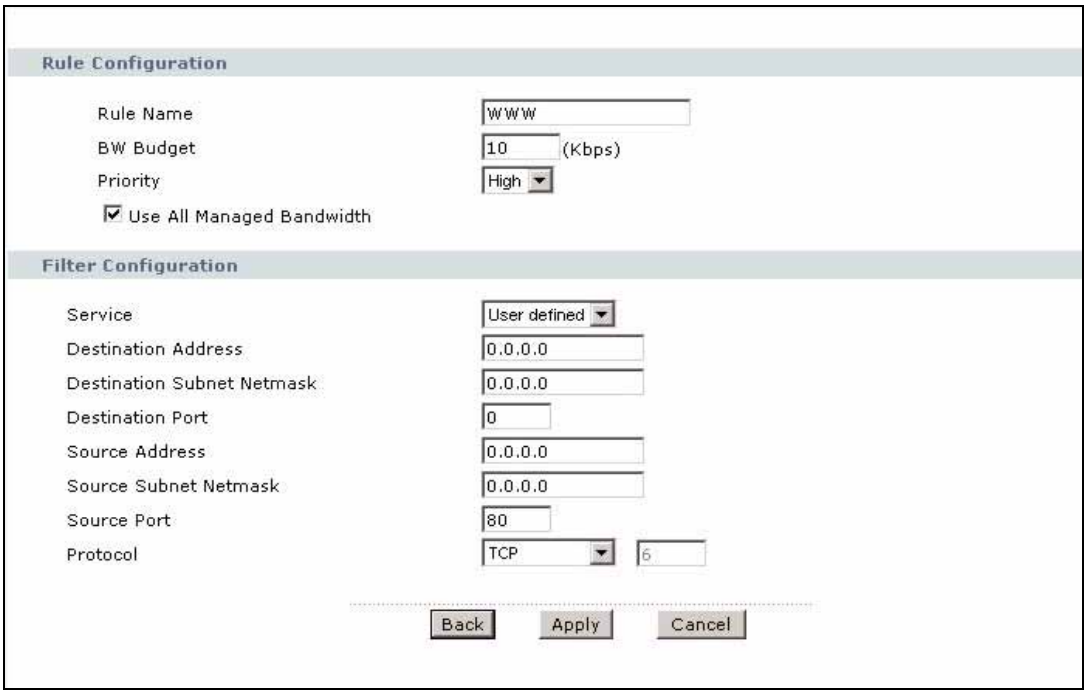
Таб. 102 Управление полосой пропускания: настройка правил

ПОЛЕ	ОПИСАНИЕ
Direction	Выберите **LAN**, чтобы применять управление полосой пропускания к трафику, входящему в LAN через P-2602. Выберите **WAN**, чтобы применять управление полосой пропускания к трафику, выходящему в WAN через P-2602. Выберите **WLAN**, чтобы применять управление полосой пропускания к трафику, выходящему в WLAN через P-2602.
Service	Выберите тип сетевой службы для данного правила. Выберите **User define**, чтобы перейти на экран для задания собственных типов служб.
Priority	Выберите приоритет из раскрывающегося списка: **High** (высокий), **Mid** (средний) или **Low** (низкий).
Bandwidth (kbps)	Укажите максимальную разрешенную полосу пропускания для данного правила в кбит/с. Рекомендуется для отдельных правил устанавливать полосу в диапазоне от 20 кбит/с до 20000 кбит/с. Если вы хотите оставить некоторую полосу для трафика, не соответствующего фильтрам полосы пропускания, убедитесь, что корневой класс интерфейса имеет большую полосу, чем сумма полос в приписанных к нему правилах.
Add	Выберите эту кнопку, чтобы сохранить правило. Правило появится в следующей таблице.
#	В этом поле отображается номер правила управления полосой пропускания.
Rule Name	В этом поле отображается наименование правила.
Destination Port	В этом поле отображается номер порта на стороне получателя. 0 означает любой порт.
Priority	В этом поле отображается приоритет правила.
Bandwidth (kbps)	В этом поле отображается максимальная разрешенная полосу пропускания для данного правила в кбит/с.
Modify	Чтобы перейти на экран для редактирования правила, щелкните на значке редактирования. Для удаления существующего правила щелкните на значке удаления.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-2602.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

19.8.1 Настройка правила

Для настройки правила управления полосой пропускания щелкните на значке **Edit** или выберите **User define** в поле **Service**. Правила управления полосой пропускания служат для распределения определенных долей полосы пропускания (бюджетов) между различными приложениями и/или подсетями.

Рис. 138 Настройка правила управления полосой пропускания



Перечень часто используемых сетевых служб см. в прилож. F на стр. 403. Поля изображённого выше экрана описаны в следующей таблице.

Таб. 103 Настройка правила управления полосой пропускания

ПОЛЕ	ОПИСАНИЕ
Rule Configuration	
Rule Name	Используйте автоматически сгенерированное название или введите название длиной до 20 алфавитно-цифровых символов с пробелами.
BW Budget	Укажите максимальную разрешенную полосу пропускания для данного правила в кбит/с. Рекомендуется для отдельных правил устанавливать полосу в диапазоне от 20 кбит/с до 20000 кбит/с.
Priority	Выберите приоритет из раскрывающегося списка: **High** (высокий), **Mid** (средний) или **Low** (низкий).
Use All Managed Bandwidth	Выберите этот параметр, чтобы разрешить правилу заимствовать неиспользованную полосу пропускания интерфейса. Процесс заимствования полосы пропускания управляется приоритетом правил: полоса заимствуется в первую очередь для правил с самым высоким приоритетом. Не выбирайте этот параметр, если вы хотите оставить полосу пропускания доступной для других типов трафика или ограничить объем полосы пропускания, который может использоваться для трафика, соответствующего этому правилу.
Filter Configuration	

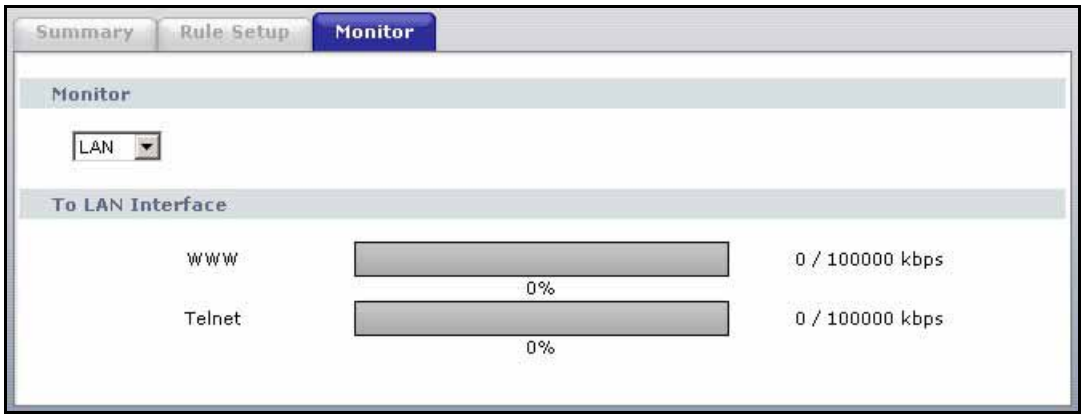
Таб. 103 Настройка правила управления полосой пропускания (продолжение)

ПОЛЕ	ОПИСАНИЕ
Service	Это поле упрощает настройку класса полосы пропускания, позволяя выбрать одно из предопределенных приложений. Если вы выбрали предопределенное приложение, вам не требуется настраивать остальные поля фильтра полосы пропускания (кроме активации или деактивации фильтра). SIP (протокол инициирования сеанса) – это сигнальный протокол, используемый для телефонной связи через Интернет, мгновенного обмена сообщениями и других приложений голосовой связи по IP (VoIP). Чтобы настроить данный фильтр для трафика, использующего SIP, выберите **SIP** в раскрывающемся списке. Протокол передачи файлов (FTP) – это служба передачи файлов, которая работает в Интернете и в сетях TCP/IP. Система, на которой работает сервер FTP, принимает команды от системы-клиента FTP. Служба позволяет пользователям посылать команды серверу для отправки и получения файлов. Чтобы настроить данный фильтр для FTP-трафика, выберите **FTP** в раскрывающемся списке. H.323 - стандартный набор протоколов конференц-связи для передачи аудиовидеопотоков и данных. Он реализует двухточечную и многоточечную связь в реальном времени между клиентскими компьютерами по сети с коммутацией пакетов, не обеспечивающей гарантированного качества обслуживания. Чтобы настроить данный фильтр для трафика, использующего H.323, выберите **H.323** в раскрывающемся списке. Если вы не хотите использовать предопределенные настройки приложений для класса полосы пропускания, выберите **User defined** в раскрывающемся списке. Если выбрано значение **User defined**, необходимо настроить одно из следующих полей (помимо полей **Subnet Mask**, котоыре заполняются только если указывается соответствующий IP-адрес источника или получателя).
Destination Address	Введите IP-адрес получателя в десятичном виде через точку.
Destination Subnet Netmask	Введите маску подсети источника. Это поле не имеет значения, если не указан адрес в поле **Destination Address**. Подробнее о подсетях IP см. в приложении.
Destination Port	Укажите номер порта на стороне получателя. Номера портов для распространенных сетевых служб см. в прилож.31 на стр. 403. Пустое поле IP-адреса получателя означает любой IP-адрес.
Source Address	Введите IP-адрес источника в десятичном виде через точку. Пустое поле IP-адреса источника означает любой IP-адрес.
Source Subnet Netmask	Введите маску подсети источника. Это поле не имеет значения, если не указан адрес в поле **Source Address**. Подробнее о подсетях IP см. в приложении. Пустое поле означает любой номер порта.
Source Port	Укажите номер порта на стороне источника. Номера портов для распространенных сетевых служб см. в прилож.31 на стр. 403 .
Protocol	Выберите протокол (**TCP** или **UDP**) или выберите **User defined** и укажите номер протокола (тип службы). 0 означает любой номер протокола.
Back	Для возврата к предыдущему экрану нажмите кнопку **Back**.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-2602.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

19.9 Монитор полосы пропускания

Чтобы просмотреть использование полосы пропускания в P-2602, выберите **Advanced > Bandwidth MGMT > Monitor**. Появится изображенный ниже экран. Чтобы просмотреть полосу пропускания, используемую интерфейсом и его правила, выберите интерфейс из раскрывающегося списка. Серый участок столбца показывает процент неиспользованной полосы пропускания, а синий участок – используемую полосу пропускания.

Рис. 139 Управление полосой пропускания: Монитор



Глава 20
Настройка DNS для динамических адресов

В этой главе поясняется способ настройки DNS для динамических адресов в P-2602.

20.1 Обзор поддержки DNS для динамических адресов

Динамическая DNS позволяет обновлять текущий динамический IP-адрес с использованием одной или нескольких служб DNS так, чтобы можно было связаться с любым пользователем (в NetMeeting, CU-SeeMe и т.д.). Доступ к FTP-серверу или веб-сайту на собственном компьютере можно получить с использованием доменного имени (например, myhost.dhs.org, где myhost – выбранное имя), которое никогда не будет изменяться, вместо использования IP-адреса, который изменяется при каждом новом подключении. Друзья или родственники всегда смогут вас вызвать, даже если не будут знать ваш IP-адрес.

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

20.1.1 Шаблон DYNDNS

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

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

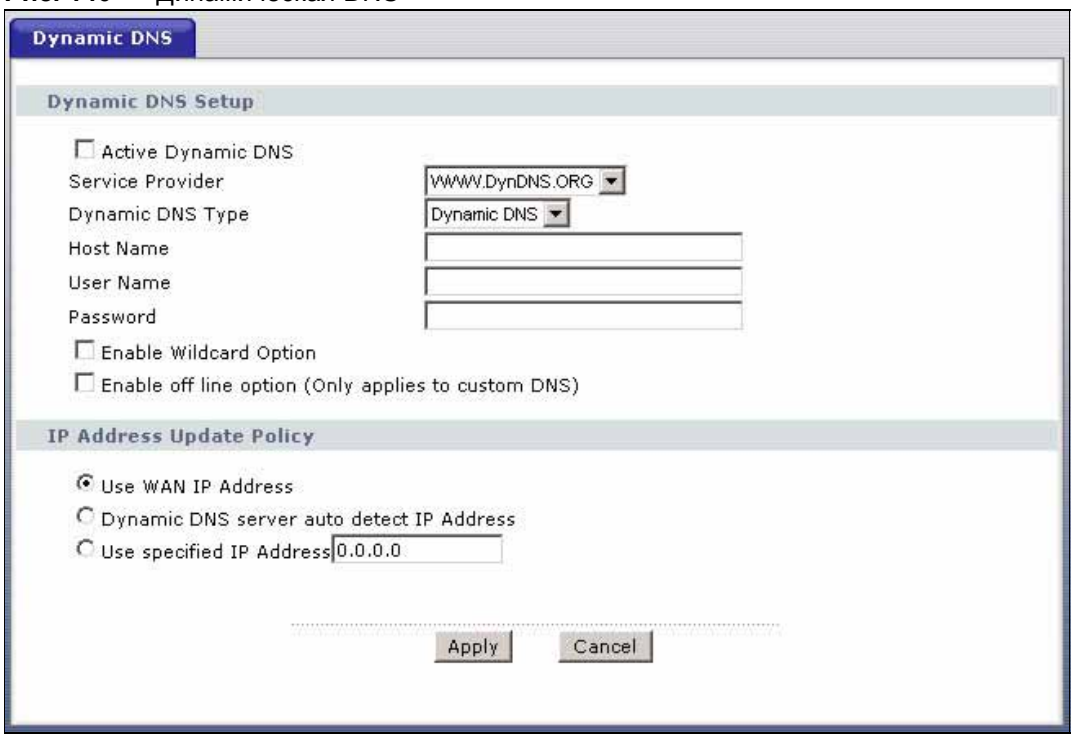
Указания по настройке см. в разд. 20.2 на стр. 289.

20.2 Настройка динамической DNS

Для изменения настроек DDNS в P-2602 выберите **Advanced > Dynamic DNS**. Появится изображенный ниже экран.

Дополнительные сведения см. в разд. 20.1 на стр. 289.

Рис. 140 Динамическая DNS



Поля изображённого выше экрана описаны в следующей таблице.

Таб. 104 Динамическая DNS

ПОЛЕ	ОПИСАНИЕ
Dynamic DNS Setup	
Active Dynamic DNS	Установите этот флажок, чтобы использовать динамическую DNS.
Service Provider	Это название поставщика услуг динамической DNS.
Dynamic DNS Type	Выберите тип услуги, зарегистрированной у поставщика услуг DDNS.
Host Name	Введите доменное имя, присвоенное вашему P-2602 поставщиком услуг DDNS. В каждом поле можно указать до двух имен хостов, отделенных запятыми.
User Name	Введите имя пользователя.
Password	Введите присвоенный вам пароль.
Enable Wildcard Option	Чтобы активировать шаблон DynDNS, отметьте флажок.
Enable off line option	Это поле доступно только в том случае, когда в поле **DDNS Type** выбрано значение **CustomDNS** (Настраиваемая DNS). Узнайте у поставщика услуг динамической DNS о возможности переадресации трафика на указанный вами URL в то время, когда вы не подключены к сети.
IP Address Update Policy	
Use WAN IP Address	Выберите этот параметр, чтобы использовать для обновленрия IP-адресов указанных имен хостов IP-адрес со стороны WAN.

Таб. 104 Динамическая DNS (продолжение)

ПОЛЕ	ОПИСАНИЕ
Dynamic DNS server auto detect IP Address	Этот параметр следует выбирать только в том случае, если между P-2602 и сервером DDNS присутствуют один или несколько маршрутизаторов с поддержкой NAT. Эта функция указывает DDNS-серверу автоматически определять и использовать IP-адрес NAT-маршрутизатора, имеющего глобальный IP-адрес. **Примечание:** DDNS-сервер может неверно определить IP-адрес, если между P-2602 и DDNS-сервером присутствует прокси-сервер HTTP.
Use specified IP Address	Введите IP-адреса для имен хостов. Используйте эту функцию, если вам выделен статический IP-адрес.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-2602.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

Глава 21
Настройка удаленного управления

В этой главе содержится информация о настройке удаленного управления.

21.1 Обзор удаленного управления

Удаленное управление позволяет определять, какие службы/протоколы могут получать доступ к определенному интерфейсу P-2602 (если это возможно) и с каких компьютеров.

Примечание: При настройке удаленного управления с целью управления из WAN необходимо настроить правило межсетевого экрана, разрешающее доступ.

Устройством P-2602 можно управлять удаленно через:

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

Примечание: Если выбран режим **WAN** или **LAN & WAN**, то для разрешения доступа извне потребуется также настроить правило межсетевого экрана.

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

В каждый момент времени может выполняться только один сеанс удаленного управления. P-2602 автоматически разъединяет менее приоритетный сеанс удаленного управления, когда начинается выполнение другого сеанса удаленного управления с более высоким приоритетом. Существуют следующие приоритеты для различных типов сеансов удаленного управления.

1. Telnet
2. HTTP

21.1.1 Ограничения удаленного управления

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

- Пользователь отключил данную службу на одном из экранов удаленного управления.
- IP-адрес в поле **Secured Client IP** не соответствует IP-адресу клиента. При таком несоответствии P-2602 немедленно прерывает сеанс.
- Уже выполняется другой сеанс удаленного управления с равным или более высоким приоритетом. В каждый момент времени может выполняться только один сеанс удаленного управления.
- Правило межсетевого экрана блокирует удаленное управление.

21.1.2 Удаленное управление и NAT

При включенной системе NAT:

- Если настройка выполняется через WAN, укажите IP-адрес P-2602 на стороне WAN.
- Если настройка выполняется через LAN, укажите IP-адрес P-2602 на стороне LAN.

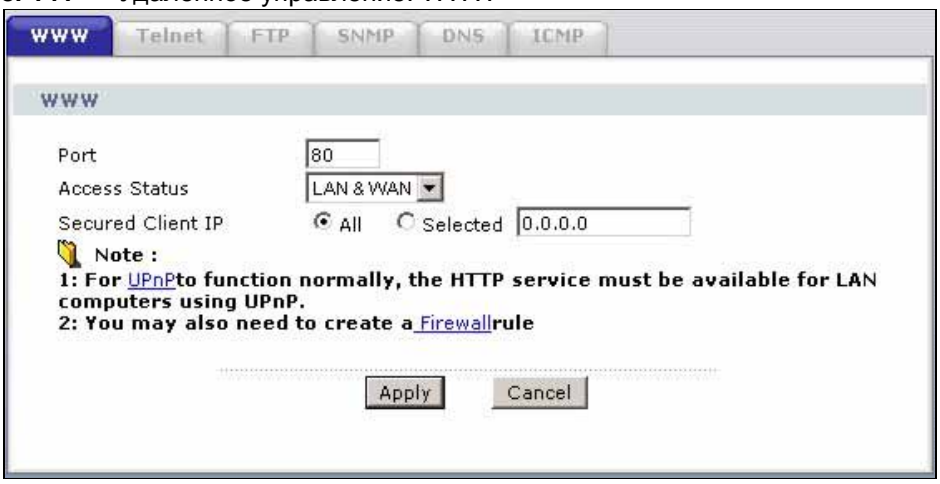
21.1.3 Системный таймер неактивности

По умолчанию системный таймер неактивности установлен на пять минут (триста секунд). P-2602 автоматически отменяет регистрацию пользователя, если сеанс управления остается бездействующим дольше этого периода времени ожидания. Сеанс управления не прерывается при выполнении опроса на экране статистики.

21.2 WWW

Чтобы изменить параметры WWW в P-2602, выберите **Advanced > Remote MGMT**. Откроется экран **WWW**.

Рис. 141 Удаленное управление: WWW



Поля изображённого выше экрана описаны в следующей таблице.

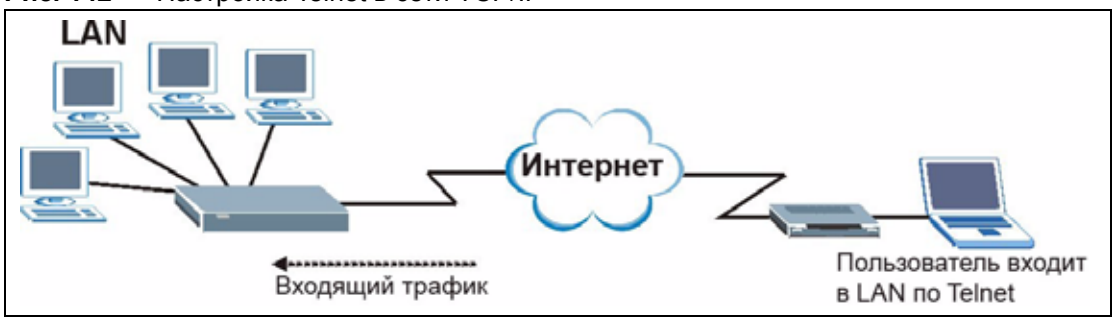
Таб. 105 Удаленное управление: WWW

ПОЛЕ	ОПИСАНИЕ
Port	При необходимости можно изменить номер порта сервера для службы, однако следует использовать тот же самый номер порта для применения данной службы в целях удаленного управления.
Access Status	Выберите интерфейсы, через которые компьютер может получать доступ к P-2602 с использованием данной службы.
Secured Client IP	Защищенный клиент – это “доверенный” компьютер, которому разрешается обмениваться данными с P-2602, используя эту службу. Выберите **All**, чтобы разрешить любому компьютеру получать доступ к P-2602 посредством этой службы. Выберите **Selected**, чтобы доступ к P-2602 посредством данной службы был разрешен только компьютеру с указанным IP- адресом.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-2602.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

21.3 Telnet

P-2602 можно настроить для удаленного доступа по Telnet, как показано ниже. Администратор использует Telnet с компьютера в удаленной сети для получения доступа к P-2602.

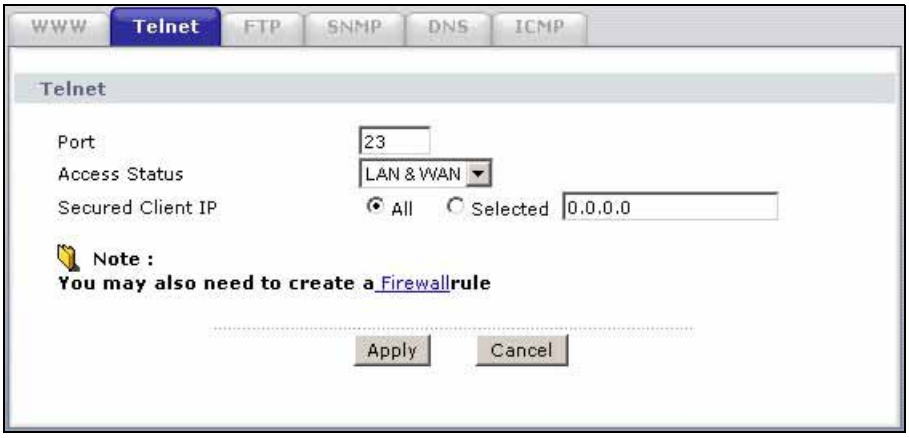
Рис. 142 Настройка Telnet в сети TCP/IP



21.4 Настройка Telnet

Чтобы перейти на показанный ниже экран, выберите **Advanced > Remote MGMT** > закладка **Telnet** .

Рис. 143 Удаленное управление: Telnet



Поля изображённого выше экрана описаны в следующей таблице.

Таб. 106 Удаленное управление: Telnet

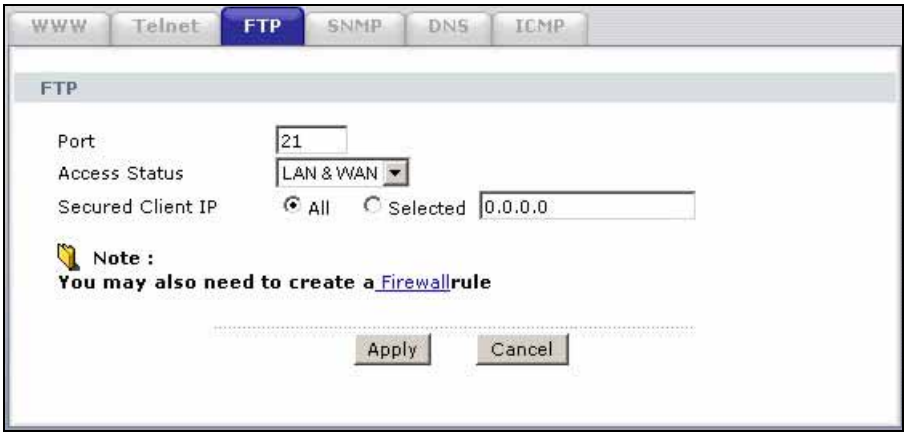
ПОЛЕ	ОПИСАНИЕ
Port	При необходимости можно изменить номер порта сервера для службы, однако следует использовать тот же самый номер порта для применения данной службы в целях удаленного управления.
Access Status	Выберите интерфейсы, через которые компьютер может получать доступ к P-2602 с использованием данной службы.
Secured Client IP	Защищенный клиент – это “доверенный” компьютер, которому разрешается обмениваться данными с P-2602, используя эту службу. Выберите **All**, чтобы разрешить любому компьютеру получать доступ к P-2602 посредством этой службы. Выберите **Selected**, чтобы доступ к P-2602 посредством данной службы был разрешен только компьютеру с указанным IP- адресом.
Apply	Нажмите кнопку **Apply** для сохранения настроек и выхода из данного экрана.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

21.5 Настройка FTP

По протоколу FTP можно загружать в P-2602 файлы микропрограмм и настроек. Подробности см. в разд. 25.7 на стр. 336. Для пользования этой функцией на вашем компьютере должен иметься FTP-клиент.

Чтобы изменить параметры FTP для P-2602, выберите **Advanced > Remote MGMT** > закладка **FTP**. Появится изображенный ниже экран.

Рис. 144 Удаленное управление: FTP



Поля изображённого выше экрана описаны в следующей таблице.

Таб. 107 Удаленное управление: FTP

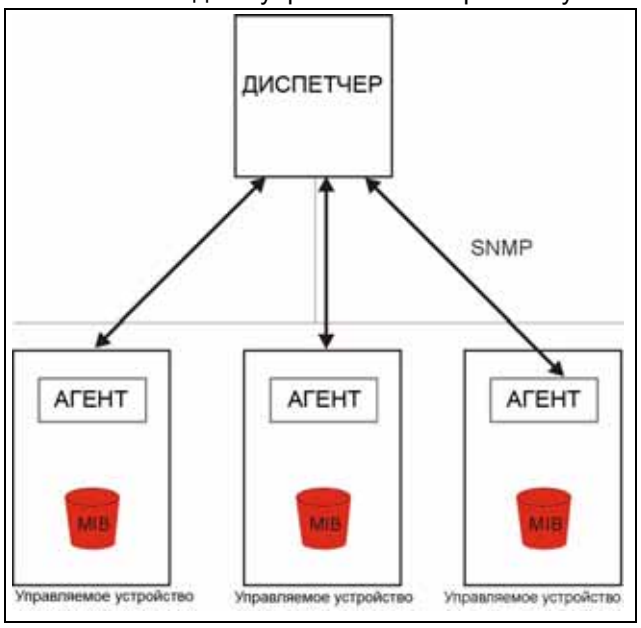
ПОЛЕ	ОПИСАНИЕ
Port	При необходимости можно изменить номер порта сервера для службы, однако следует использовать тот же самый номер порта для применения данной службы в целях удаленного управления.
Access Status	Выберите интерфейсы, через которые компьютер может получать доступ к P-2602 с использованием данной службы.
Secured Client IP	Защищенный клиент – это “доверенный” компьютер, которому разрешается обмениваться данными с P-2602, используя эту службу. Выберите **All**, чтобы разрешить любому компьютеру получать доступ к P-2602 посредством этой службы. Выберите **Selected**, чтобы доступ к P-2602 посредством данной службы был разрешен только компьютеру с указанным IP- адресом.
Apply	Нажмите кнопку **Apply** для сохранения настроек и выхода из данного экрана.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

21.6 SNMP

Протокол SNMP (Simple Network Management Protocol – простой протокол сетевого управления) используется для обмена управляющей информацией между сетевыми устройствами. SNMP входит в семейство протоколов TCP/IP. P-2602 поддерживает функциональные возможности агента SNMP, что позволяет управляющей станции выполнять управление и мониторинг P-2602 через сеть. P-2602 поддерживает версию первую (SNMPv1) и вторую (SNMPv2) версии SNMP. На следующем рисунке показана схема управления на основе SNMP.

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

Рис. 145 Модель управления по протоколу SNMP



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

Агент – это программа, которая выполняется на управляемом устройстве (P-2602). Агент преобразует локальные параметры управления, используемые в управляемом устройстве, в формат, совместимый с SNMP. Диспетчер представляет собой консоль, с которой системные администраторы осуществляют управление сетью. Диспетчер выполняет ПО для управления и мониторинга управляемых устройств.

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

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

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

21.6.1 Поддерживаемые базы MIB

P-2602 поддерживает базу MIB II, которая определена в RFC-1213 и RFC-1215. Основная задача баз MIB – дать администраторам возможность сбора статистических данных и мониторинга состояния и производительности.

21.6.2 Прерывания SNMP

P-2602 направляет прерывания диспетчеру SNMP при наступлении одного из следующих событий:

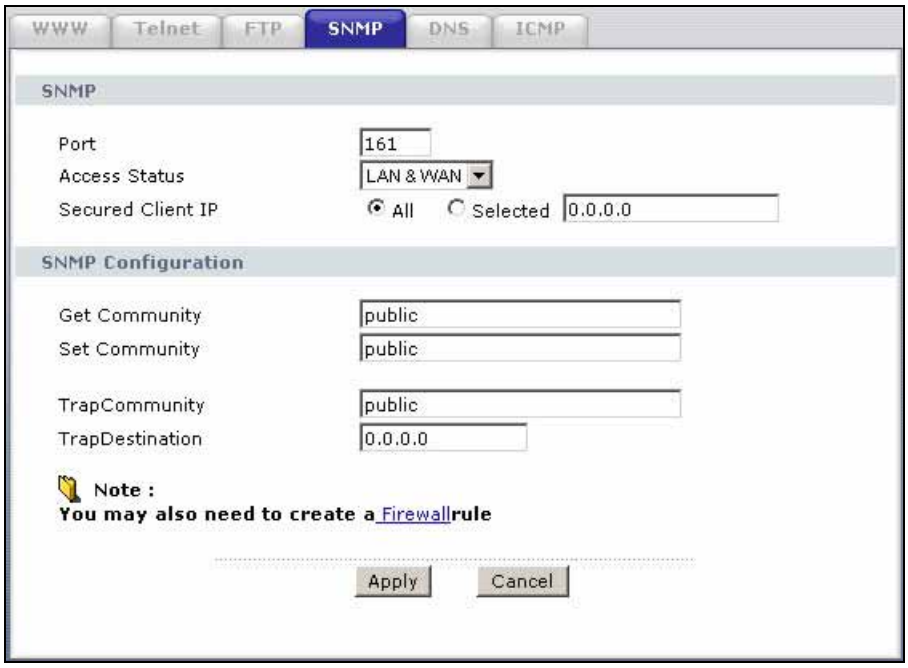
Таб. 108 Прерывания SNMP

ПРЕРЫВАНИЕ №	ИМЯ ПРЕРЫВАНИЯ	ОПИСАНИЕ
0	coldStart (определяется в *RFC-1215*)	Прерывание отправляется после загрузки (включения питания).
1	warmStart (определяется в *RFC-1215*)	Прерывание отправляется после загрузки (программной перезагрузки).
4	authenticationFailure (определяется в *RFC-1215*)	Прерывание отправляется диспетчеру при получении любых запросов SNMP “Get” или “Set” с неверным сообществом (паролем).
6	whyReboot (определяется в ZYXEL-MIB)	Прерывание направляется по причине перезапуска перед перезагрузкой, когда система готовится к перезапуску (“теплая перезагрузка”).
6a	Для перезагрузки, запрошенной пользователем:	Прерывание отправляется с сообщением “Перезагрузка системы пользователем!”, если перезагрузка выполняется по явному запросу, (например, после загрузки новых файлов, получения команды CI “перезагрузка системы” и т.д.).
6b	Из-за неустранимой ошибки:	Прерывание отправляется с сообщением о фатальном коде, если система перезагружается из-за неустранимых ошибок.

21.6.3 Настройка SNMP

Чтобы изменить параметры SNMP для P-2602, выберите **Advanced > Remote MGMT** > **SNMP**. Появится изображенный ниже экран.

Рис. 146 Удаленное управление: SNMP



Поля изображённого выше экрана описаны в следующей таблице.

Таб. 109 Удаленное управление: SNMP

ПОЛЕ	ОПИСАНИЕ
SNMP	
Port	При необходимости можно изменить номер порта сервера для службы, однако следует использовать тот же самый номер порта для применения данной службы в целях удаленного управления.
Access Status	Выберите интерфейсы, через которые компьютер может получать доступ к P-2602 с использованием данной службы.
Secured Client IP	Защищенный клиент – это “доверенный” компьютер, которому разрешается обмениваться данными с P-2602, используя эту службу. Выберите **All**, чтобы разрешить любому компьютеру получать доступ к P-2602 посредством этой службы. Выберите **Selected**, чтобы доступ к P-2602 посредством данной службы был разрешен только компьютеру с указанным IP- адресом.
SNMP Configuration	
Get Community	Введите **Get Community** (“получить сообщество”) – пароль для всех входящих запросов Get и GetNext от диспетчерской станции. Значение по умолчанию – “общедоступно”, все запросы разрешены.
Set Community	Введите **Set community** (“задать сообщество”) – пароль для входящих запросов Set от диспетчерской станции. Значение по умолчанию – “общедоступно”, все запросы разрешены.

Таб. 109 Удаленное управление: SNMP

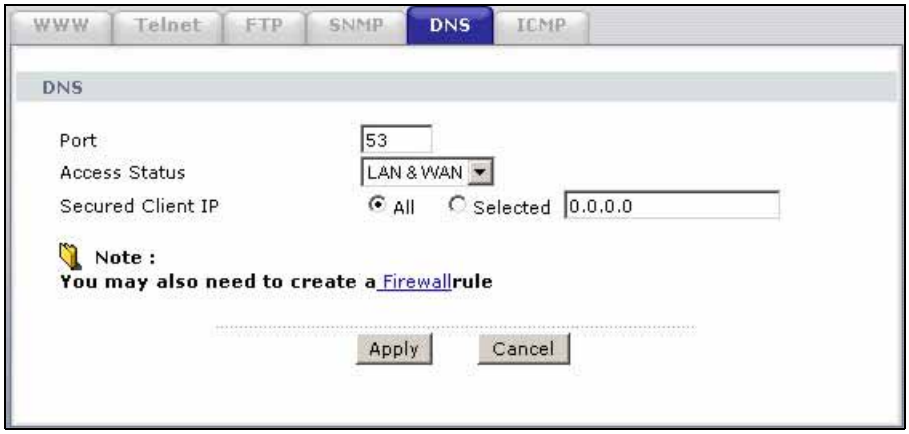
ПОЛЕ	ОПИСАНИЕ
Прерывание	
Community	Введите сообщество для прерываний, которое будет выступать в качестве пароля при отправке прерываний диспетчеру SNMP. Значение по умолчанию – “общедоступно”, все запросы разрешены.
Destination	Введите IP-адрес станции, которой следует направлять прерывания SNMP.
Apply	Нажмите кнопку **Apply** для сохранения настроек и выхода из данного экрана.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

21.7 Настройка DNS

DNS (служба доменных имён) обеспечивает преобразование доменных имён в соответствующие им IP-адреса и наоборот. Дополнительную информацию см. в гл. 8 на стр. 115.

Чтобы изменить параметры DNS для P-2602, выберите **Advanced > Remote MGMT** > **DNS**. Появится изображенный ниже экран. Этот экран позволяет задать IP-адреса, от которых P-2602 будет принимать DNS-запросы, и указать интерфейс, через который P-2602 будет рассылать параметры DNS на эти адреса.

Рис. 147 Удаленное управление: DNS



Поля изображённого выше экрана описаны в следующей таблице.

Таб. 110 Удаленное управление: DNS

ПОЛЕ	ОПИСАНИЕ
Port	Номер порта службы DNS – 53, его нельзя здесь изменить.
Access Status	Выберите интерфейсы, через которые компьютер может отправлять запросы DNS на P-2602.

Таб. 110 Удаленное управление: DNS

ПОЛЕ	ОПИСАНИЕ
Secured Client IP	Защищенный клиент – это “доверенный” компьютер, которому разрешается отправлять запросы DNS на P-2602. Выберите переключатель **All**, чтобы разрешить любому компьютеру отправлять запросы DNS на P-2602. Выберите переключатель **Selected**, чтобы разрешить только компьютеру с указанным IP-адресом отправлять запросы DNS на P-2602.
Apply	Нажмите кнопку **Apply** для сохранения настроек и выхода из данного экрана.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

21.8 Настройка ICMP

Чтобы изменить параметры безопасности P-2602, выберите **Advanced > Remote MGMT** > **ICMP**. Появится изображенный ниже экран.

Если внешний пользователь попытается прозондировать неподдерживаемый порт P-2602, автоматически будет возвращен пакет с откликом ICMP (протокол управляющих сообщений в Интернете). Это позволяет внешнему пользователю узнать о том, что P-2602 существует. P-2602 предусматривает защиту от зондирования, отключающую отправку пакета с откликом ICMP. Это препятствует обнаружению P-2602 посторонними при зондировании неподдерживаемых портов.

Примечание: Если вам необходимо, чтобы устройство отвечало на эхозапросы и обращения к неавторизованным службам, может потребоваться настройка соответствующих параметров защиты от зондирования в межсетевом экране.

Рис. 148 Удаленное управление: ICMP

Поля изображённого выше экрана описаны в следующей таблице.

Таб. 111 Удаленное управление: ICMP

ПОЛЕ	ОПИСАНИЕ
ICMP	Internet Control Message Protocol (Протокол управляющих сообщений в Интернете) является протоколом управлением сообщениями и предоставления отчетов об ошибках при взаимодействии между сервером хоста и интернет-центром. В ICMP используются датаграммы межсетевого протокола (IP), но сообщения обрабатываются программным обеспечением TCP/IP и отображаются в понятном виде для пользователя приложения.
Respond to Ping on	Если выбрано значение **Disable**, P-2602 не будет реагировать на входящие запросы. Выберите **LAN**, чтобы разрешить ответ на поступающие через локальную сеть эхозапросы. Выберите **WAN** , чтобы разрешить ответ на эхозапросы из WAN. В противном случае выберите **LAN & WAN (LAN и WAN)** для передачи ответов на поступающие эхозапросы LAN и WAN.
Do not respond to requests for unauthorized services	Выберите этот параметр, чтобы предотвратить обнаружение P-2602 хакерами путем зондирования неиспользуемых портов. В этом случае P-2602 не будет отвечать на запросы неиспользуемых портов, что позволит скрыть неиспользуемые порты и P-2602. По умолчанию этот параметр не выбран, и P-2602 отправляет пакет ICMP Port Unreachable (“порт недоступен”) при зондировании портов на незадействованных портах UDP, и пакет TCP Reset (“сброс”) при зондировании портов на незадействованных портах TCP. Примечание: пакеты для зондирования сначала должны пройти через межсетевой экран P-2602, прежде чем они будут обрабатываться механизмом противодействия зондированию. Поэтому если межсетевой экран заблокирует пакет с попыткой зондирования, то действие, предпринимаемое P-2602, будет зависеть от политики межсетевого экрана: отправка TCP-пакета сброса для заблокированных TCP-пакетов, ICMP-пакета “порт недоступен” для заблокированных UDP-пакетов, или простое удаление пакета без отправки отклика.
Apply	Нажмите кнопку **Apply** для сохранения настроек и выхода из данного экрана.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

Глава 22
Универсальная технология “включи и работай” (UPnP)

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

22.1 Обзор технологии UPnP

Универсальная технология “включай и работай” (UPnP) является открытым стандартом построения распределенных сетей, в которых используется TCP/IP для простого одноранговой сетевого соединения между устройствами. Устройство UPnP может динамически присоединяться к сети, получать IP-адрес, сообщать свои возможности и получать данные о других устройствах в сети. А когда в устройстве больше нет необходимости, оно может беспрепятственно покинуть сеть в автоматическом режиме.

Указания по настройке см. в разд. 22.2.1 на стр. 306.

22.1.1 Как определить, используется ли UPnP?

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

22.1.2 Прослеживание NAT

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

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

Windows Messenger – пример приложения, поддерживающего прослеживание NAT и UPnP.

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

22.1.3 Предостережения по отношению к UPnP

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

Подключаясь к сети, UPnP-устройство объявляет о своем присутствии многоадресным сообщением. По соображениям безопасности P-2602 допускает передачу многоадресных сообщений только в сети LAN.

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

22.2 UPnP и ZyXEL

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

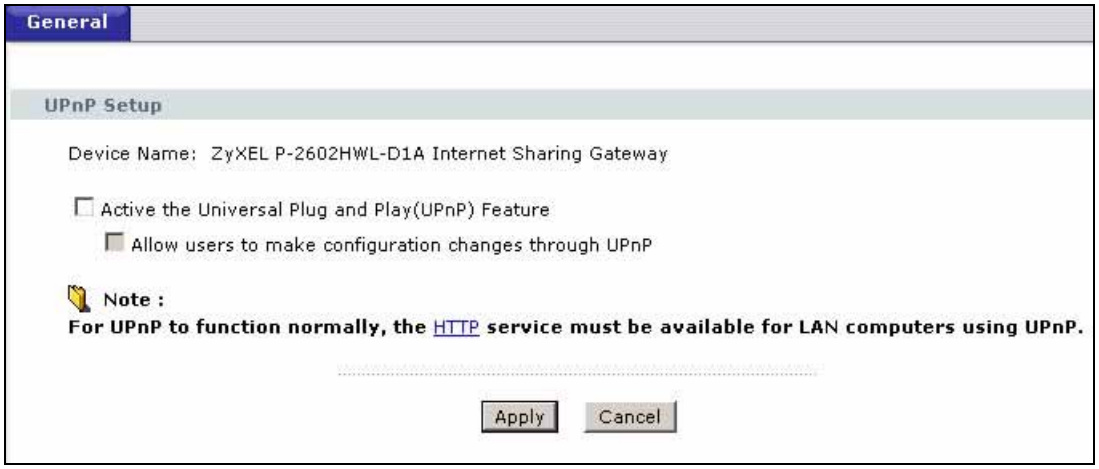
В следующих разделах рассмотрены примеры установки и использования UPnP.

22.2.1 Настройка UPnP

Чтобы перейти на показанный ниже экран, выберите **Advanced > UPnP**.

Дополнительные сведения см. в разд. 22.1 на стр. 305.

Рис. 149 Настройка UPnP



Поля изображённого выше экрана описаны в следующей таблице.

Таб. 112 Настройка UPnP

ПОЛЕ	ОПИСАНИЕ
Active the Universal Plug and Play (UPnP) Feature	Отметьте этот флажок, чтобы активировать UPnP. Помните, что любой пользователь сможет посредством приложения UPnP перейти на экран регистрации веб-конфигуратора, не вводя IP-адрес P-2602 (хотя для доступа к веб-конфигуратору по-прежнему потребуется вводить имя пользователя и пароль).
Allow users to make configuration changes through UPnP	Установите этот флажок, чтобы разрешить приложениям с поддержкой UPnP автоматически конфигурировать P-2602 так, чтобы они могли взаимодействовать через P-2602; например, используя прослеживание NAT, приложения UPnP автоматически резервируют порт для адресации NAT, чтобы взаимодействовать с другим устройством с поддержкой UPnP; это устраняет необходимость ручной настройки переадресации портов для приложения с поддержкой UPnP.
Allow UPnP to pass through Firewall	Отметьте этот флажок, чтобы разрешить прохождение трафика от приложений с поддержкой UPnP в обход межсетевого экрана. Снимите этот флажок, чтобы межсетевой экран блокировал все пакеты приложеий UPnP (например, пакеты MSN).
Apply	Нажмите кнопку **Apply**, чтобы сохранить настройки в P-2602.
Cancel	Чтобы вернуться к прежним настройкам, нажмите **Cancel**.

22.3 Пример установки UPnP в Windows

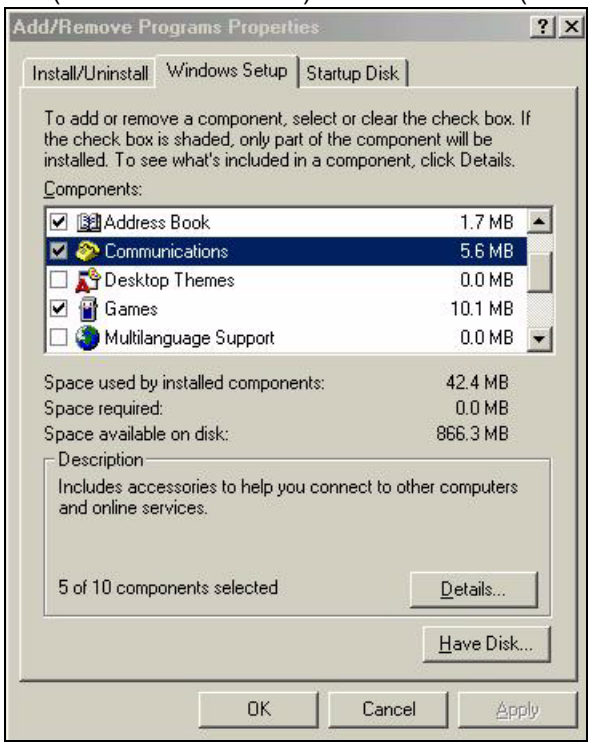
В этом разделе описана установка UPnP в Windows Me и Windows XP.

Установка UPnP в Windows Me

Для установки UPnP в Windows Me выполните указанные ниже действия.

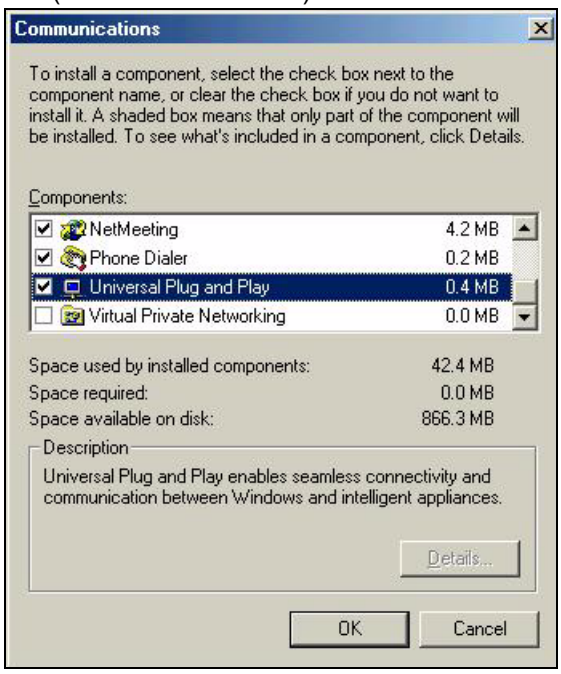
1. Нажмите кнопку **Start (Пуск)** и **Control Panel (Панель управления)**. Выполните двойной щелчок на значке **Add/Remove Programs (Установка и удаление программ)**.
2. Щелкните вкладку **Windows Setup (Установка Windows)** и выберите строку **Communication (Связь)** в поле выбора **Components (Компоненты)**.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

Рис. 150 Add/Remove Programs (Установка и удаление программ): Windows Setup (Установка Windows): Communication (Связь)



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

Рис. 151 Add/Remove Programs (Установка и удаление программ): Windows Setup (Установка Windows): Связь: Компоненты



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

5 Перезапустите компьютер, когда это будет предложено.

Установка UPnP в Windows XP

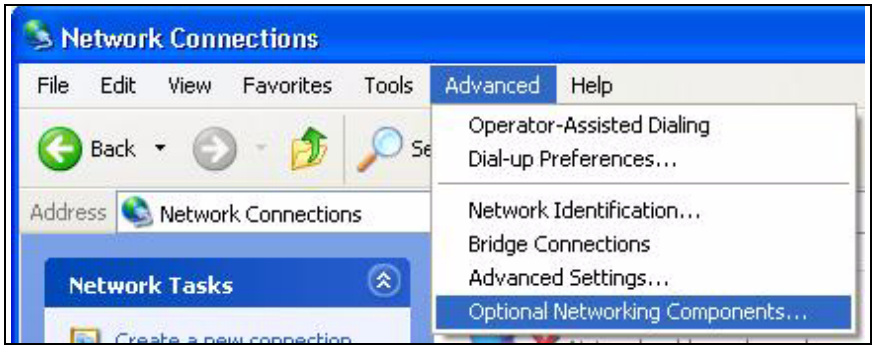
Для установки UPnP в Windows XP выполните указанные ниже действия.

1 Нажмите кнопку **Start (Пуск)** и выберите **Control Panel (Панель управления)**.

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

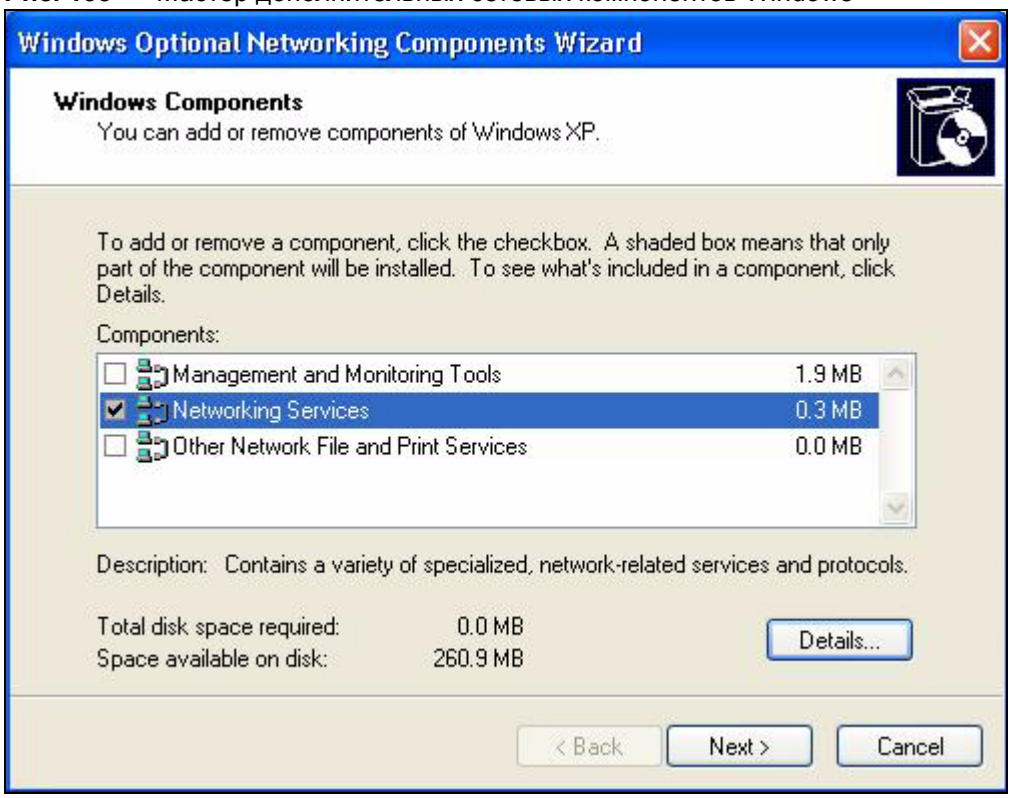
3 В окне **Network Connections (Сетевые подключения)** щелкните кнопку **Advanced (Дополнительно)** в главном меню и выберите пункт **Optional Networking Components … (Дополнительные сетевые компоненты)**.

Рис. 152 Сетевые подключения



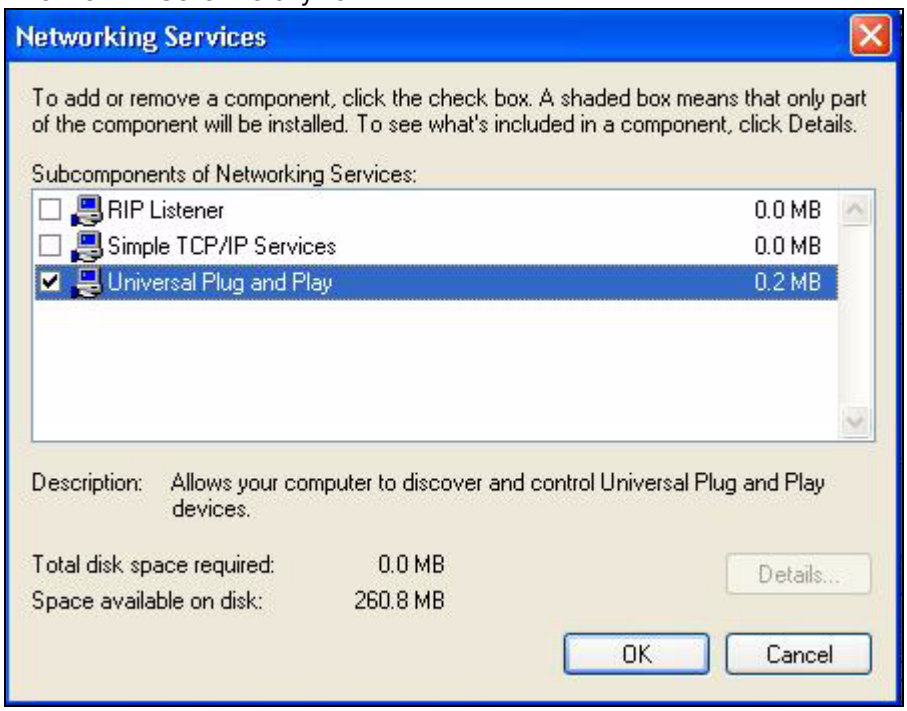
4 Появится окно **Windows Optional Networking Components Wizard (Мастер дополнительных сетевых компонентов Windows)**. Выберите **Networking Service (Сетевые службы)** в окне выбора **Components (Компоненты)** и щелкните кнопку **Details (Состав)**.

Рис. 153 Мастер дополнительных сетевых компонентов Windows



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

Рис. 154 Сетевые службы



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

22.4 Пример использования UPnP в Windows XP

В данном разделе описано использование функции UPnP в Windows XP. Система UPnP уже должна быть установлена в Windows XP и активирована в P-2602.

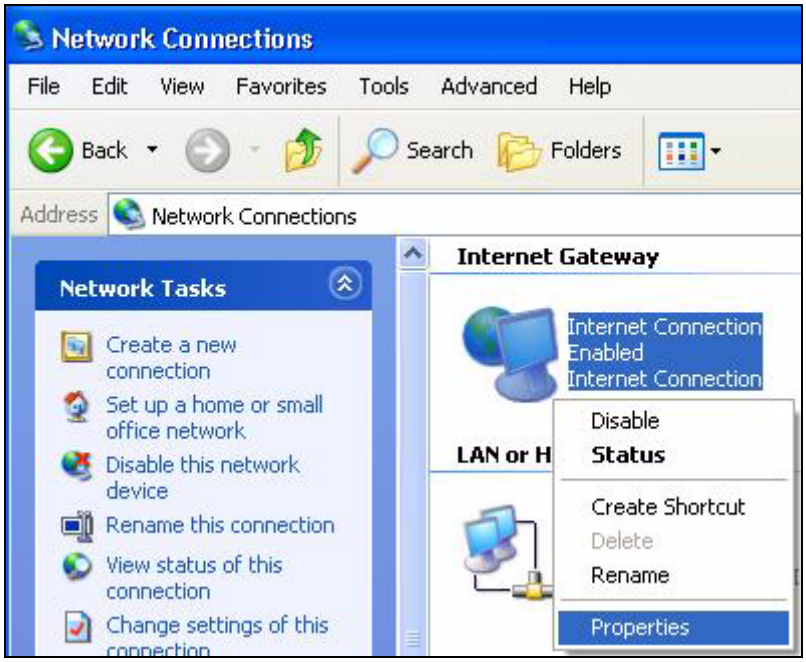
Убедитесь в том, что компьютер подключен к порту LAN на P-2602. Включите компьютер и P-2602.

Автоматическое обнаружение сетевого устройства с поддержкой UPnP

1 Нажмите кнопку **Start (Пуск)** и выберите **Control Panel (Панель управления)**. Дважды щелкните на значке **Network Connections (Сетевые подключения)**. Значок отображается под Internet Gateway (интернет-центром).

2 Щелкните правой кнопкой мыши по этому значку и выберите **Properties (Свойства)**.

Рис. 155 Сетевые подключения



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

Рис. 156 Свойства подключения к Интернету

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

Рис. 157 Свойства подключения к Интернету: расширенные параметры

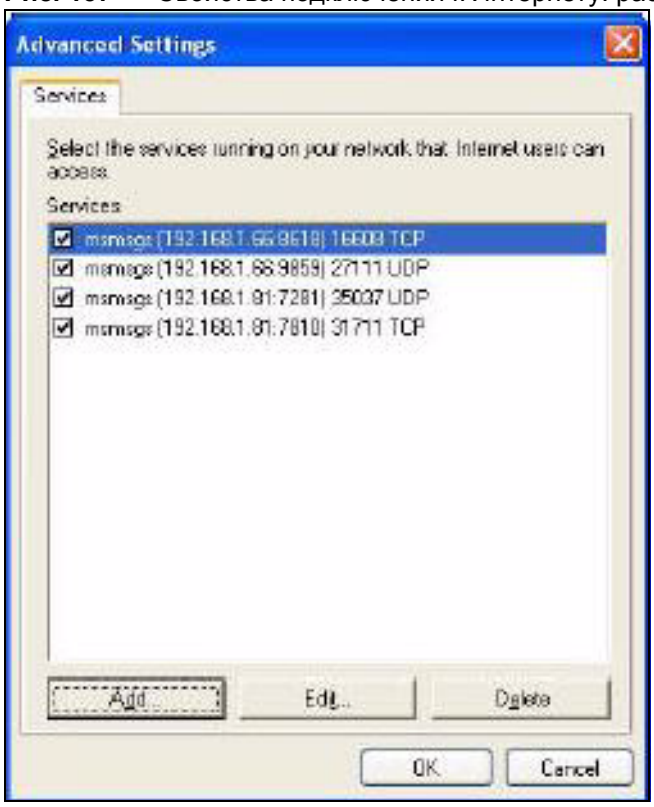
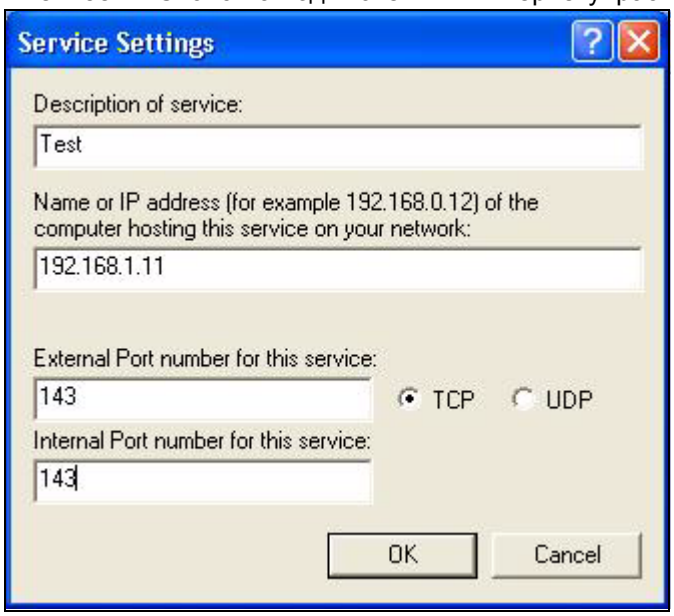


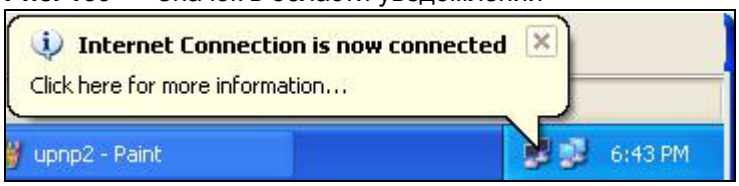
Рис. 158 Свойства подключения к Интернету: расширенные параметры: Add



5 Когда устройство с поддержкой UPnP отключено от компьютера, все привязки порта удаляются автоматически.

6 Установите флажок **Show icon in notification area when connected (Показать значок в области уведомлений при наличии подключения)** и щелкните **OK**. Значок отображается в области уведомлений на панели задач.

Рис. 159 Значок в области уведомлений



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

Рис. 160 Состояние подключения к Интернету

Упрощенный доступ к веб-конфигуратору

Благодаря системе UPnP можно получать доступ к веб-конфигуратору в P-2602 без выяснения IP-адреса P-2602. Это полезно, если неизвестен IP-адрес P-2602.

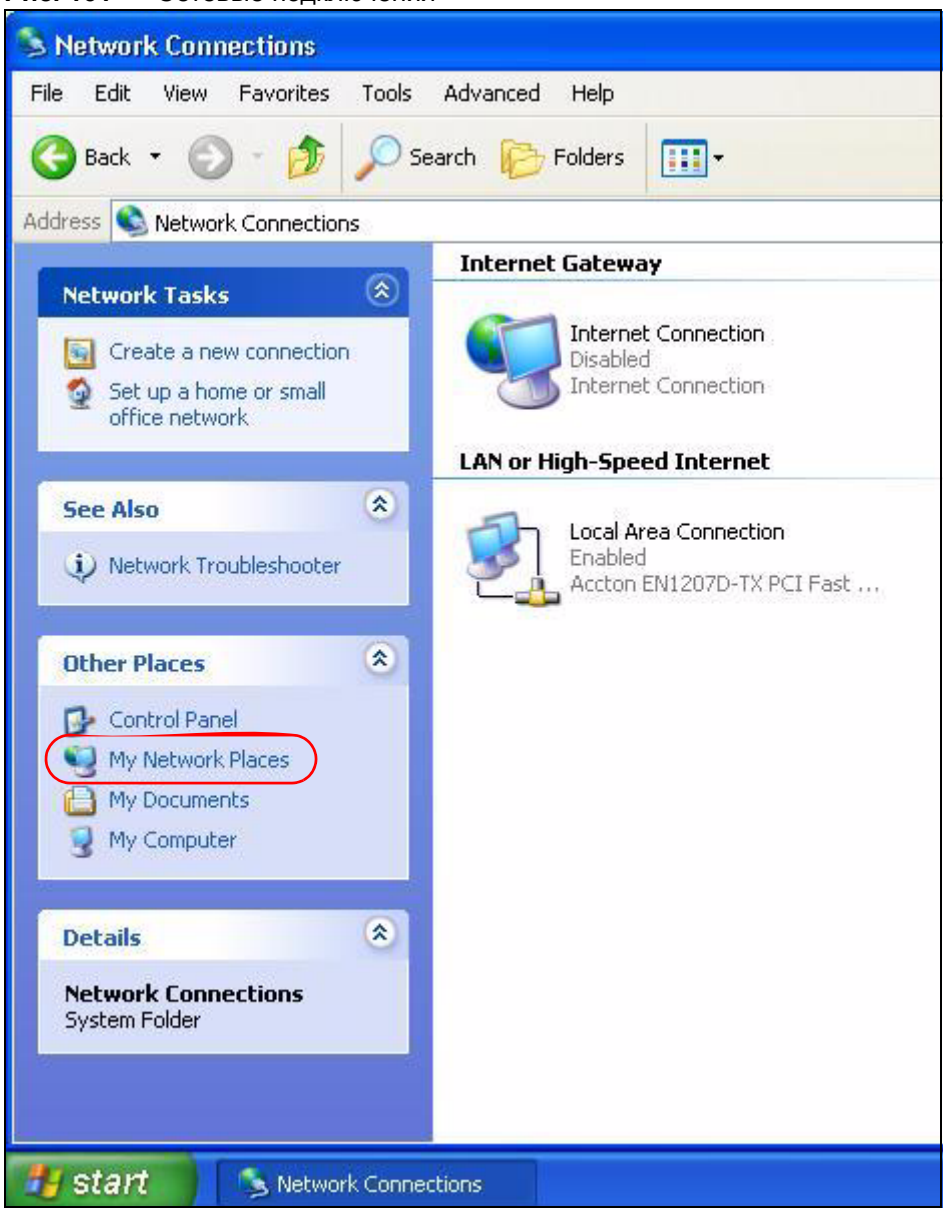
Чтобы вызвать веб-конфигуратор, выполните указанные ниже действия.

1 Нажмите кнопку **Start (Пуск)**, а затем – **Control Panel (Панель управления)**.

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

3 Выберите **My Network Places (Мои местоположения в сети)** под **Other Places**.

Рис. 161 Сетевые подключения



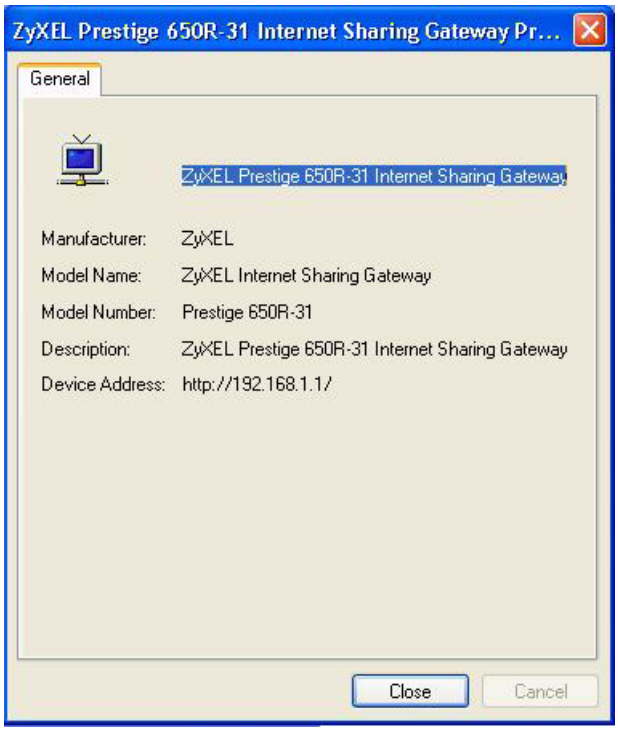
4 Под заголовком **Local Network** отображается значок с описанием каждого устройства с поддержкой UPnP.

5 Щелкните правой кнопкой мыши по значку P-2602 и выберите **Invoke** (Вызвать). Отображается экран регистрации веб-конфигуратора.

Рис. 162 Сетевые подключения: сетевое окружение

6 Щелкните правой кнопкой мыши по значку P-2602 и выберите **Properties** (Свойства). Отображается окно свойств с основной информацией о P-2602.

Рис. 163 Сетевые подключения: Сетевое окружение: свойства: пример



Глава 23
Экран System

Этот экран служит для настройки даты и времени в P-2602.

23.1 Разделы General Setup и System Name

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

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

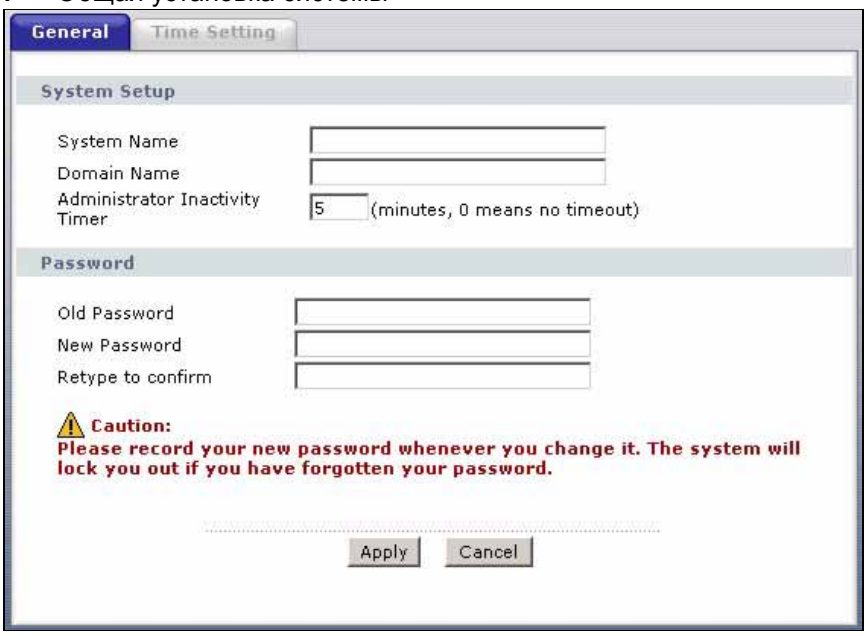
- P-2602.

23.1.1 Раздел General Setup

В поле **Domain Name** указывается информация, распространяемая DHCP-клиентам в локальной сети. Если оставить это поле пустым, используется имя домена, полученное DHCP от ISP. В то время как имя хоста (System Name – Имя системы) следует вводить на каждом отдельном компьютере, доменное имя назначается из P-2602 через DHCP.

Чтобы перейти на экран **General**, выберите **Maintenance > System**.

Рис. 164 Общая установка системы



Поля изображённого выше экрана описаны в следующей таблице.

Таб. 113 Общая установка системы

ПОЛЕ	ОПИСАНИЕ
General Setup	
System Name	Выберите описательное название, позволяющее идентифицировать оборудование. Рекомендуется ввести в этом поле то же значение, что и в поле “Computer name” (“Имя компьютера”). Это имя может быть длиной до 30 буквенно-цифровых символов. Пробелы недопустимы, но тире “-” и символ подчеркивания “_”приемлемы.
Domain Name	Введите здесь имя домена (если оно известно). Если оставить это поле пустым, ISP может назначить имя домена через DHCP. Имя домена, введенное пользователем, получает приоритет над назначенным ISP именем домена.
Administrator Inactivity Timer	Укажите число минут неактивности сеанса управления (через веб-конфигуратор или telnet), по истечении которого сеанс разрывается. Значение по умолчанию - 5 минут. После истечения сеанса потребуется повторно войти в веб-конфигуратор и ввести пароль. Большая длительность периода неактивности является фактором риска для безопасности системы. Значение “0” означает, что сеанс никогда не разрывается, независимо от периода неактивности (использовать данное значение не рекомендуется).
Password	
Old Password	Введите пароль по умолчанию или существующий пароль, который Вы используете, чтобы получить доступ к системе в этом поле.
New Password	Введите новый системный пароль (до 30 символов). Обратите внимание, что при вводе пароля вместо вводимых символов на экране отображаются звездочки “*”. После смены пароля для обращения к P-2602 нужно использовать новый пароль.
Retype to Confirm	Снова введите новый пароль для подтверждения.

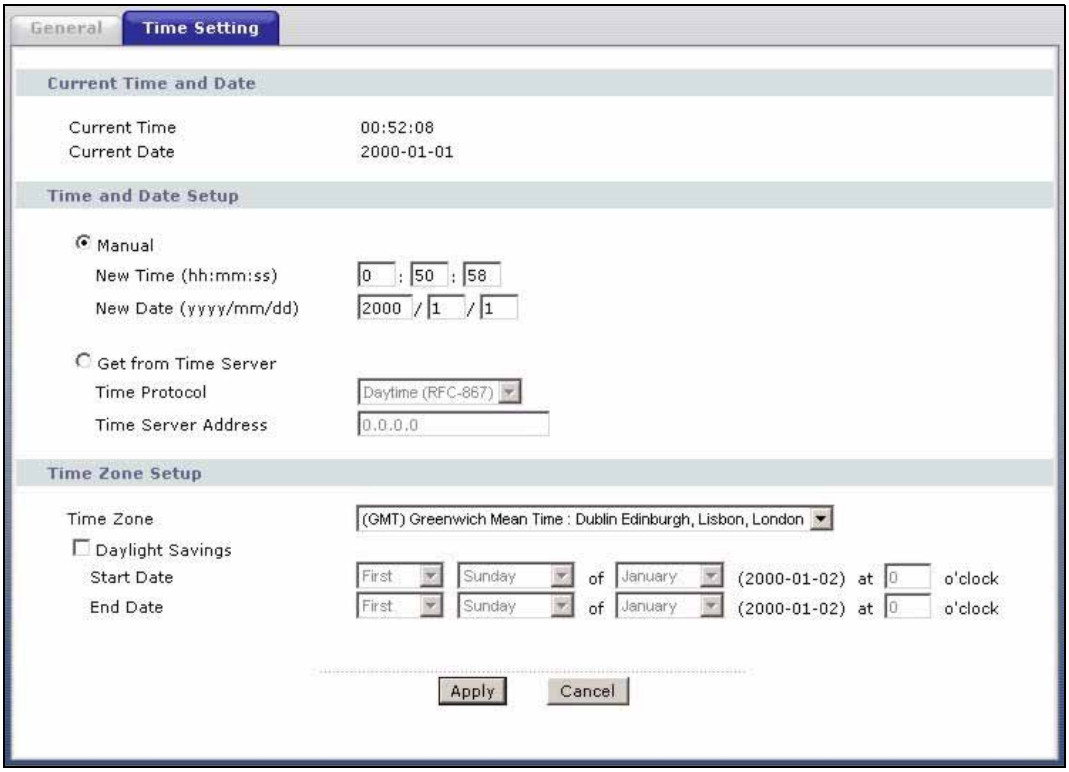
Таб. 113 Общая установка системы

ПОЛЕ	ОПИСАНИЕ
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-2602.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

23.2 Установка часов

Для изменения даты и времени в P-2602 выберите **Maintenance > System > Time Setting**. Появится изображенный ниже экран. Используйте это окно для настройки времени P-2602 с учетом вашего часового пояса.

Рис. 165 Настройка системных часов



Поля изображённого выше экрана описаны в следующей таблице.

Таб. 114 Настройка системных часов

ПОЛЕ	ОПИСАНИЕ
Current Time and Date	
Current Time	В этом поле отображается текущее время по часам P-2602. При каждом обновлении этой страницы в браузере P-2602 синхронизирует часы с сервером точного времени.

Таб. 114 Настройка системных часов (продолжение)

ПОЛЕ	ОПИСАНИЕ
Current Date	В этом поле отображается текущая дата по часам P-2602. При каждом обновлении этой страницы в браузере P-2602 синхронизирует дату с сервером точного времени.
Time and Date Setup	
Manual	Выберите этот переключатель, чтобы ввести время и дату вручную. Елсли вы одновременно настроили новое время, дату, часовой пояс и режим летнего/зимнего времени, введенные вами время и дата имеют приоритет, а настройки часового пояса и летнего/зимнего времени на заданные значения не действуют.
New Time (hh:mm:ss)	В этом поле отображаются последние показания времени, полученные с сервера точного времени или настроенные вручную. Если вы установили параметр **Time and Date Setup** в значение **Manual**, введите в этом поле новое время и нажмите **Apply**.
New Date (yyyy/mm/dd)	В этом поле отображается последняя дата, полученная с сервера точного времени или настроенная вручную. Если вы установили параметр **Time and Date Setup** в значение **Manual**, введите в этом поле новую дату и нажмите **Apply**.
Get from Time Server	Чтобы устройство P-2602 получало показания даты и времени с указанного ниже сервера точного времени, выберите этот параметр.
Time Protocol	Выберите протокол службы точного времени, по которому P-2602 будет обращаться к серверу при включении питания. Не все серверы точного времени поддерживают полный набор протоколов; обратитесь к оператору/ администратору сети или подберите работающий протокол методом проб и ошибок. Основные различия между ними заключаются в формате сообщаемого времени. Формат **Daytime (RFC 867)**: день/месяц/год/часовой пояс, в котором находится сервер. Формат **Time (RFC868)**: целое число длиной 4 байта, означающее количество секунд, прошедшее с 0:0:0 01.01.1970 (1970/1/1 в 0:0:0). Формат **NTP (RFC 1305)** похож на Time (RFC 868).
Time Server Address	Введите IP-адрес или URL (до 20 знаков расширенного набора ASCII) сервера точного времени. Если вы не уверены в том, какие значения требуется ввести, обратитесь к оператору / администратору сети.
Time Zone Setup	
Time Zone	Выберите часовой пояс для данной местности. Это поле задает разницу во времени между местной временной зоной и гринвичским временем (GMT).
Daylight Saving	Летнее время – это период между поздней весной и началом осени, когда во многих странах стрелки переводятся вперед на 1 час по отношению к обычному местному времени, чтобы продлить светлое время в конце дня. Выберите этот параметр, если в вашем часовом поясе действует переход на зимнее/летнее время.

Таб. 114 Настройка системных часов (продолжение)

ПОЛЕ	ОПИСАНИЕ
Start Date	Укажите месяц и день перехода на летнее время, если был отмечен флажок **Enable Daylight Saving**. В поле **o'clock** используется 24-часовой формат. Примеры: На большей части территории США летнее время начинается в первое воскресенье апреля. Для каждого часового пояса летнее время в США начинает действовать с 2:00 по местному времени. Поэтому для США необходимо выбрать **First**, **Sunday**, **April** и ввести 2 в поле **o'clock**. В Европейском союзе и в России летнее время начинается в последнее воскресенье марта. Во всех часовых поясах на территории Евросоюза летнее время начинается одновременно (в 1:00 по Гринвичу или UTC). Поэтому для Евросоюза необходимо выбрать **Last**, **Sunday**, **March**. Время, вводимое в поле **o'clock**, зависит от вашего часового пояса. Например, для Германии, где время на один час опережает гринвичское (GMT+1), следует ввести 2.
End Date	Укажите месяц и день перехода на зимнее время, если был отмечен флажок **Enable Daylight Saving**. В поле **o'clock** используется 24-часовой формат. Примеры: В США летнее время заканчивается в последнее воскресенье октября. Для каждого часового пояса летнее время в США заканчивает действовать в 2:00 по местному времени. Поэтому для США необходимо выбрать **Last**, **Sunday**, **October** и ввести 2 в поле **o'clock**. В Европейском союзе и в России летнее время заканчивается в последнее воскресенье октября. Во всех часовых поясах на территории Евросоюза летнее время заканчивается одновременно (в 1:00 по Гринвичу или UTC). Поэтому для Евросоюза необходимо выбрать **Last**, **Sunday**, **October**. Время, вводимое в поле **o'clock**, зависит от вашего часового пояса. Например, для Германии, где время на один час опережает гринвичское (GMT+1), следует ввести 2.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-2602.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

Глава 24
Журналы

В данной главе описывается настройка общих параметров ведения журналов и просмотр журналов P-2602. Пояснения по сообщениям, оставляемым в журналах, приведены в приложении.

24.1 Обзор средств ведения журналов

Веб-конфигуратор P-2602 позволяет указать, какие категории событий и/или предупреждений должны отмечаться в журнале, и затем просмотреть журналы или переслать их с P-2602 администратору (по электронной почте) или на SYSLOG-сервер.

24.1.1 Журналы и предупреждения

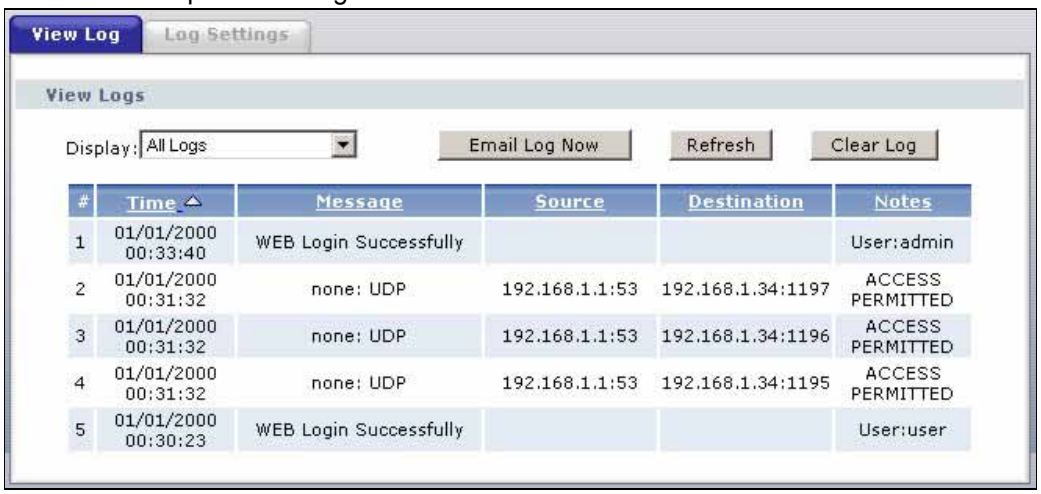
Предупреждение – это журнальное сообщение, требующее более серьёзного внимания. К предупреждениям относятся системные ошибки, атаки и попытки доступа к заблокированным веб-сайтам. Некоторые категории, такие как **системные ошибки**, состоят одновременно из простых журнальных сообщений и предупреждений.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

24.2 Просмотр журналов

Чтобы перейти на экран **View Log**, выберите **Maintenance > Logs**. Экран **View Log** позволяет просмотреть журналы для категорий, выбранных на экране **Log Settings** (см. разд. 24.3 на стр. 324).

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

Рис. 166 Экран View Log



Поля изображённого выше экрана описаны в следующей таблице.

Таб. 115 Экран View Log

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

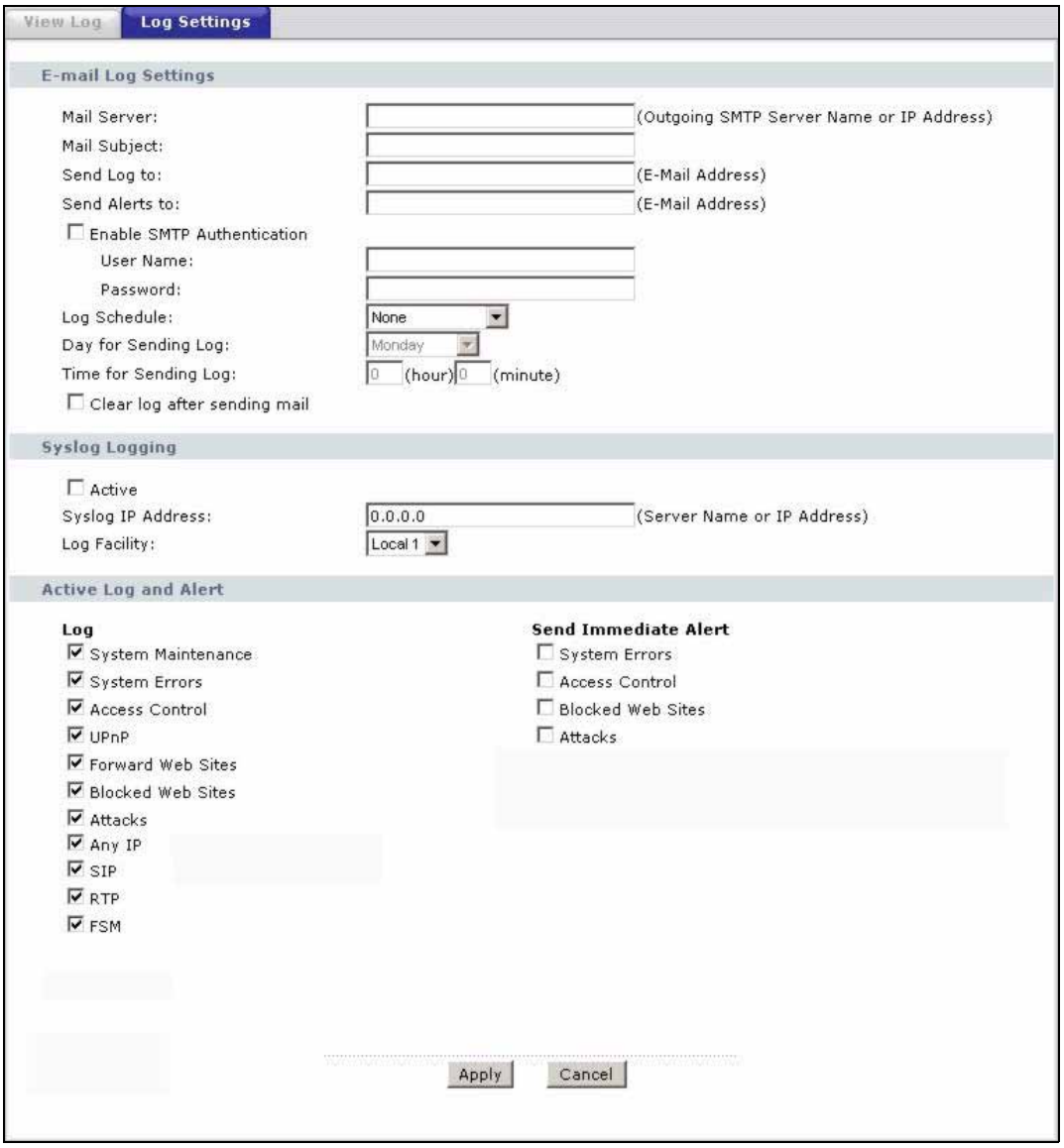
24.3 Настройка параметров ведения журналов

Экран **Log Settings** служит для настройки содержания журналов P-2602, графика отправки сообщений в журналы P-2602 и состава регистрируемых журнальных сообщений и экстренных предупреждений P-2602. Дополнительные сведения см. в разд. 24.1 на стр. 323.

Чтобы изменить параметры ведения журналов P-2602, выберите **Maintenance > Logs** > **Log Settings**. Появится изображенный ниже экран.

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

Рис. 167 Настройки журнала



Поля изображённого выше экрана описаны в следующей таблице.

Таб. 116 Log Settings

ПОЛЕ	ОПИСАНИЕ
E-mail Log Settings	
Mail Server	Введите имя сервера или IP-адрес почтового сервера для адресов электронной почты, указанных ниже. Если это поле оставить пустым, журналы и сообщения с предупреждениями не будут отправляться по электронной почте.
Mail Subject	Введите тему, которая будет указываться в заголовке журнальных сообщений, отправляемых P-2602 по электронной почте. Это поле имеется не у всех моделей P-2602.
Send Log to	P-2602 отправляет журналы по адресу электронной почты, указанному в данном поле. Если это поле оставить пустым, P-2602 не будет отправлять журналы по электронной почте.
Send Alerts to	Оповещения - это уведомления, отправляемые в режиме реального времени, как только происходит событие, такое как атака DoS, ошибка системы или попытка доступа к запрещённому веб-узлу. Введите адрес электронной почты, по которому должны отправляться сообщения с предупреждениями. Оповещения содержат ошибки системы, атаки и попытки доступа к заблокированным веб-сайтам. Если это поле оставить пустым, сообщения с предупреждениями не будут отправляться по электронной почте.
Enable SMTP Authentication	SMTP (простой протокол передачи почты) – стандарт обмена почтовыми сообщениями в Интернете. SMTP позволяет передавать сообщения от одного почтового сервера к другому. Установите этот флажок, чтобы активировать аутентификацию SMTP. Если почтовый сервер требует аутентификацию, но эта функция в устройстве отключена, вы не будете получать журнальные сообщения по электронной почте.
User Name	Введите имя пользователя (длиной до 31 знака; обычно это имя соответствует имени учетной записи электронной почты).
Password	Введите пароль, связанный с указанным выше именем пользователя.
Log Schedule	Это раскрывающееся меню используется для настройки периодичности отправки журнальных сообщений по электронной почте: • **Daily (ежедневно)** • **Weekly (еженедельно)** • **Hourly (ежечасно)** • **When Log is Full (когда журнал полон)** • **None (никогда)**. При выборе **Weekly** или **Daily** укажите время суток, когда должны отправляться сообщения по электронной почте. При выборе варианта **Weekly** укажите также день недели, когда должно отправляться сообщение. При выборе **When Log is Full** предупреждение отправляется, когда заполнен журнал. При выборе варианта **None** журнальные сообщения не отправляются.
Day for Sending Log	В раскрывающемся списке выберите день недели для отправки журналов.
Time for Sending Log	Введите время дня в 24-часовом формате (например, 23:00 соответствует 11:00 вечера) для отправки журналов.
Clear log after sending mail	Установите этот флажок для удаления всех журналов после того, как P-2602 отправит их по электронной почте.
Syslog Logging	P-2602 отправляет журнальное сообщение на внешний сервер системного журнала (SYSLOG).

Таб. 116 Log Settings

ПОЛЕ	ОПИСАНИЕ
Active	Щёлкните **Active (Активный)** для включения регистрации системных журналов.
Syslog IP Address	Введите имя сервера или IP-адрес сервера системных журналов, который должен регистрировать выбранные категории журналов.
Log Facility	Выберите местоположение из раскрывающегося списка. Распределение по журнальным объектам (“log facility”) позволяет записывать сообщения на сервере в различные файлы. Обращайтесь к руководству сервера системных журналов для получения дополнительной информации.
Active Log and Alert	
Log	Выберите категории журналов, которые необходимо записать.
Send Immediate Alert	Выберите категории журналов, предупреждения по которым должны немедленно отправляться P-2602 по электронной почте.
Apply	Нажмите кнопку **Apply** для сохранения настроек и выхода из данного экрана.
Cancel	Чтобы вернуться к прежним настройкам, нажмите **Cancel**.

24.4 Сообщения об ошибках SMTP

При возникновении затруднений с отправкой электронной почты появится следующее сообщение об ошибке.

“SMTP action request failed. ret= ??”. Коды “??” описаны в следующей таблице.

Таб. 117 Сообщения об ошибках SMTP

-1 означает, что у P-2602 отсутствуют свободные сокеты
-2 означает сбой TCP SYN
-3 означает, что невозможно получить ответ “OK” от SMTP-сервера
-4 означает сбой при обработке команды “HELO”
-5 означает сбой при обработке команды “MAIL FROM”
-6 означает сбой при обработке команды “RCPT TO”
-7 означает сбой при обработке команды “DATA”
-8 означает сбой при отправке текста сообщения

24.4.1 Пример журнального сообщения в электронной почте

В каждом сообщении, содержащем полный журнал, присутствует отметка “End of Log” (“Конец журнала”). Ниже приведен пример журнала, отправляемого по электронной почте.

- Содержание строки с темой сообщения можно изменить.
- Дата представляется в формате “день-месяц-год”.
- Здесь дата приведена в формате “месяц-день-год”, время – в формате “часы-минуты-секунды”.
- “Отметка `End of Log`” подтверждает, что журнал отправлен полностью.

Рис. 168 Пример журнального сообщения в электронной почте

```
Тема:
        Firewall Alert From
   Дата:
        пятница, 7 апреля 2000 г. 10:05:42
   Отправитель:
        user@zyxel.com
     Адресат:
        user@zyxel.com
  1|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |default policy  |forward
   | 09:54:03 |UDP     src port:00520 dest port:00520  |<1,00>          |
  2|Apr  7 00 |From:192.168.1.131   To:192.168.1.255   |default policy  |forward
   | 09:54:17 |UDP     src port:00520 dest port:00520  |<1,00>          |
  3|Apr  7 00 |From:192.168.1.6     To:10.10.10.10 |match           |forward
   | 09:54:19 |UDP     src port:03516 dest port:00053  |<1,01>          |
……..{и т.д.}……..
……..{и т.д.}……..
126|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |match           |forward
   | 10:05:00 |UDP     src port:00520 dest port:00520  |<1,02>          |
127|Apr  7 00 |From:192.168.1.131   To:192.168.1.255   |match           |forward
   | 10:05:17 |UDP     src port:00520 dest port:00520  |<1,02>          |
128|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |match           |forward
   | 10:05:30 |UDP     src port:00520 dest port:00520  |<1,02>          |
End of Firewall Log
```

Глава 25
Системные инструменты

В этой главе описывается загрузка новых версий микропрограммы, управление файлами настроек и перезапуск P-2602.

Примечание: Не прерывайте процесс передачи файлов, иначе P-2602 может НЕОБРАТИМО ВЫЙТИ ИЗ СТРОЯ.

25.1 Введение

Для изменения файла настроек устройства или обновления его микропрограммы следуйте указаниям в этой главе. После выполнения настройки можно сделать резервную копию файла настроек на компьютере. Это позволяет впоследствии, если настройки будут ошибочно изменены, восстановить сохраненные значения из резервной копии файла настроек. Можно также загрузить файл с заводскими настройками, если требуется возвратить устройство к заводским настройкам. Все функции и возможности устройства реализуются микропрограммой. Обновления микропрограмм для улучшения работы устройства можно загрузить с FTP-сайта компании ZyXEL (либо www.zyxel.ru).

Примечание: Используйте только микропрограмму, предназначенную для конкретной модели устройства. См. ярлык на нижней стороне корпуса P-2602.

25.2 Имена и расширения файлов

Файл настроек (часто называемый romfile или rom-0) содержит заводские настройки по умолчанию в меню, такие как пароль, настройка DHCP, настройка TCP/IP и т.д. Поставляется ZyXEL с расширением в имени файла “rom”. После настройки параметров устройства P-2602 их можно сохранить на своем компьютере, присвоив имя файла по своему усмотрению.

ZyNOS (сетевая операционная система ZyXEL, часто именуемая “ras-файлом”) представляет собой микропрограмму системы и имеет расширение “bin”. Эту микропрограмму можно найти на www.zyxel.ru. Для многих FTP- и TFTP-клиентов имена файлов будут аналогичны показанным ниже.

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

Это примерный фрагмент FTP-сеанса для передачи файла “firmware.bin” с компьютера в P-2602.

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

Это пример FTP-сеанса для сохранения текущих настроек в файле “`config.cfg`” на компьютере.

Если ваш (T)FTP-клиент не позволяет указать целевое имя файла, отличное от исходного, то файлы потребуется переименовать, поскольку P-2602 принимает только файлы с именами “rom-0” и “ras”. Для использования в дальнейшем сохраните неизменённые копии обоих файлов.

Общее описание файлов дано в следующей таблице. Внутренним именем файла называется имя файла в P-2602, а внешним именем файла называется имя файла вне P-2602, например, на диске компьютера, в локальной сети или на FTP-сервере, где оно может быть другим (не изменяется только расширение файла). Загрузив новую микропрограмму, с помощью экрана **Status** убедитесь, что загружена нужная версия микропрограммы.

Таб. 118 Принятая схема именования файлов

ТИП ФАЙЛА	ВНУТРЕННЕЕ ИМЯ	ВНЕШНЕЕ ИМЯ	ОПИСАНИЕ
Файл настроек	Rom-0	Это имя файла настроек в P-2602. При загрузке файла rom-0 замещается вся файловая система в ПЗУ устройства, включая настройки P-2602, системные данные (в т.ч. пароль по умолчанию), журнал ошибок и журнал трассировки.	*.rom
Микро-программа	Ras	Это имя файла микропрограммы ZyNOS в P-2602.	*.bin

25.3 Управление файлами через WAN

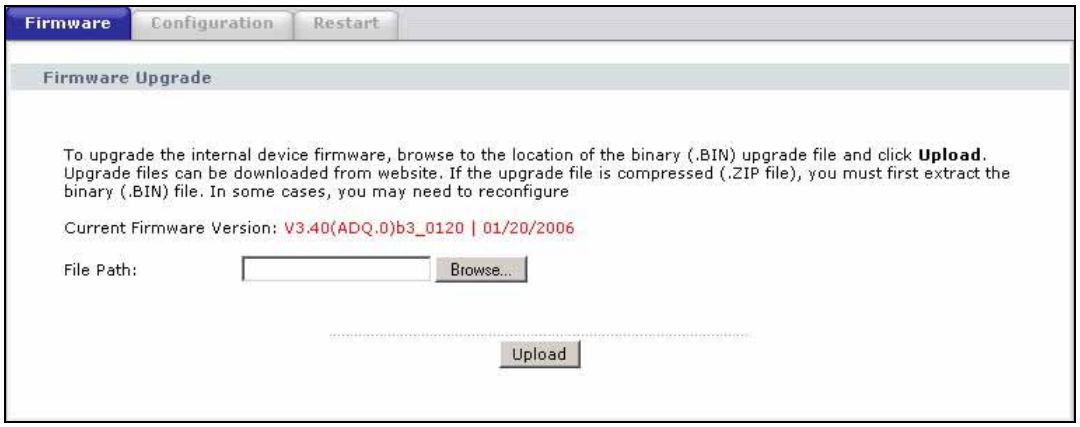
В следующих случаях управление со стороны WAN по протоколам TFTP, FTP невозможно:

1. Активирован сетевой экран (отключите сетевой экран или создайте в нем правило, разрешающее доступ из сети WAN).
2. Служба Telnet отключена в меню 24.11.
3. Применен фильтр в меню 3.1 (LAN) или в меню 11.5 (WAN) для блокирования службы Telnet.
4. IP-адрес в поле **Secured Client IP** (IP-адрес защищенного клиента) в меню 24.11 не соответствует IP-адресу клиента. При таком несоответствии устройство немедленно прерывает сессию Telnet.

25.4 Экран обновления микропрограммы

Чтобы перейти на экран **Firmware**, выберите **Maintenance > Tools**. Для загрузки микропрограммы в P-2602 следуйте указаниям на экране. Для загрузки используется HTTP (протокол передачи гипертекста); процесс может занять до 2 минут. После успешной загрузки система перезапускается. Указания по загрузке микропрограммы посредством протоколов FTP/TFTP см. в разд. 25.9 на стр. 340.

Рис. 169 Экран Firmware Upgrade



Поля изображённого выше экрана описаны в следующей таблице.

Таб. 119 Firmware Upgrade

ПОЛЕ	ОПИСАНИЕ
Current Firmware Version	В этом поле отображается версия и дата создания используемой микропрограммы.
File Path	Введите местоположение файла, который необходимо выгрузить, в этом поле, или щелкните **Browse ... (Найти …)** для его поиска.
Browse...	Щелкните кнопку **Browse... (Найти…)** для поиска файла .bin , который необходимо выгрузить. Помните о том, что необходимо распаковать сжатые файлы (.zip) перед их загрузкой в устройство.
Upload	Нажмите кнопку **Upload**, чтобы начать процесс загрузки. Этот процесс может занять до двух минут.

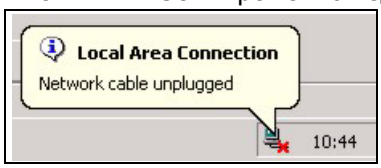
Примечание: НЕ выключайте P-2602, пока идет загрузка микропрограммы!

После того, как появится экран **Firmware Upload in Progress**, подождите две минуты, прежде чем снова обращаться к P-2602.

Рис. 170 Выполнение загрузки микропрограммы

По окончании загрузки микропрограммы P-2602 автоматически перезапускается, что приводит к временному отключению от сети. В некоторых операционных системах на рабочем столе может находиться следующий значок.

Рис. 171 Сеть временно недоступна



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

Если загрузку не удалось выполнить, появится следующее окно. Нажмите **Return**, если нужно вернуться к экрану **Firmware**.

Рис. 172 Сообщение об ошибке

25.5 Резервное копирование и восстановление

Команды FTP/TFTP для передачи файлов настроек описаны в разд. 25.7 на стр. 336 и разд. 25.8 на стр. 339.

Выберите **Maintenance > Tools > Configuration**. Ниже рассматривается возврат к заводским настройам, резервное копирование и восстановление настроек.

Рис. 173 Настройки

25.5.1 Резервное копирование настроек

Функция резервного копирования настроек позволяет скопировать (сохранить) текущие настройки P-2602 в файл на компьютере. После того, как устройство P-2602 будет настроено и начнет работать в штатном режиме, рекомендуется перед любым изменением настроек делать резервную копию файла настроек. Резервный файл настроек будет полезен в том случае, если потребуется вернуться к предыдущим настройкам.

Для сохранения текущих настроек P-2602 на компьютере выберите **Backup**.

25.5.2 Восстановление настроек

Функция восстановления настроек позволяет загрузить новый или ранее сохраненный файл настроек с компьютера в P-2602.

Таб. 120 Восстановление настроек

ПОЛЕ	ОПИСАНИЕ
File Path	Введите местоположение файла, который необходимо загрузить, в этом поле, или щелкните **Browse ...** (Найти …) для поиска этого файла.

Таб. 120 Восстановление настроек

ПОЛЕ	ОПИСАНИЕ
Browse...	Щелкните **Browse...** для поиска файла, который необходимо загрузить. Помните, что необходимо распаковывать сжатые файлы (.ZIP) перед их загрузкой в устройство.
Upload	Нажмите кнопку **Upload**, чтобы начать процесс загрузки.

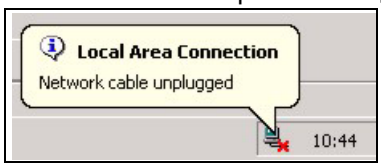
Примечание: Не выключайте P-2602 во время загрузки файла настроек.

При появлении экрана “configuration upload successful” (“загрузка настроек выполнена успешно”) следует подождать одну минуту перед повторной регистрацией в P-2602.

Рис. 174 Загрузка настроек выполнена успешно

По окончании загрузки настроек P-2602 автоматически перезапускается, что приводит к временному отключению от сети. В некоторых операционных системах на рабочем столе может находиться следующий значок.

Рис. 175 Сеть временно недоступна



После загрузки файла заводских настроек необходимо изменить IP-адрес компьютера, чтобы он находился в одной подсети с устройством, имеющим IP-адрес по умолчанию 192.168.1.1. Указания по настройки IP-адреса компьютера см. в прилож. C на стр. 369.

Если загрузку не удалось выполнить, появится следующее окно. Выберите ссылку **Return**, если нужно вернуться к экрану **Configuration**.

Рис. 176 Ошибка при загрузке настроек

25.5.3 Возврат к заводским настройкам

Нажмите кнопку **Reset**, чтобы удалить все выполненные пользователем настройки и возвратить P-2602 к заводским настройкам по умолчанию. Появится следующий экран с предупреждением.

Рис. 177 Предупреждение о сбросе настроек

Рис. 178 Предупреждение о сбросе настроек

Для сброса к заводским настройкам также можно нажать кнопку **RESET** на задней панели P-2602. Подробное описание кнопки **RESET** см. в разд. 2.1.2 на стр. 55.

25.6 Перезапуск

Этот экран служит для перезагрузки P-2602 без выключения питания.

Выберите **Maintenance > Tools** > **Restart**. Чтобы перезагрузить P-2602, выберите **Restart**. Эта операция не влияет на настройки P-2602.

Рис. 179 Экран перезапуска

25.7 Использование команд FTP/TFTP для резервного копирования настроек

В этом разделе описано использование FTP или TFTP для сохранения файла настроек на компьютере.

25.7.1 Использование команд FTP для резервного копирования настроек

1. Запустите FTP-клиент на своем компьютере.
2. Введите команду “`open`”, набрав после нее пробел и IP-адрес P-2602.
3. Нажмите [ENTER] ([ВВОД]) , когда потребуется имя пользователя.
4. Введите пароль (по умолчанию – “1234”).
5. Введите “`bin`”, чтобы установить режим передачи для двоичных файлов.
6. Для передачи файлов с P-2602 на компьютер используйте команду “`get`”, например, “`get rom-0 config.rom`” передает файл настроек с P-2602 на компьютер, где он переименовывается в “`config.rom`”. Подробнее о принятой схеме именования файлов см. выше в данной главе.
7. Введите “`quit`” для выхода из приглашения FTP.

25.7.2 Пример резервного копирования настроек с помощью команд FTP

На рисунке приведен пример использования команд FTP из приглашения DOS для сохранения настроек устройства на компьютере.

Рис. 180 Пример сеанса FTP

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

25.7.3 Резервное копирование настроек с помощью FTP-клиентов с графическим интерфейсом

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

Таб. 121 Общие команды для клиентов FTP на основе GUI.

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

25.7.4 Резервное копирование настроек с использованием TFTP

P-2602 поддерживает загрузку / выгрузку микропрограмм и файла настроек с использованием TFTP (упрощенный протокол передачи файлов) через LAN. Хотя TFTP тоже должен работать через WAN, это не рекомендуется.

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

1. Используйте telnet со своего компьютера для подключения к устройству P-2602 и зарегистрируйтесь. Поскольку TFTP не имеет системы проверки безопасности, P-2602 записывает IP-адрес клиента telnet и принимает запросы TFTP только с этого адреса.
2. Введите команду "`sys stdio 0`" для отключения времени ожидания SMT, чтобы пересылка TFTP не прерывалась. Введите команду "`sys stdio 5`" для восстановления пятиминутного времени ожидания SMT (по умолчанию), когда завершится передача файлов.
3. Запустите клиент TFTP на своем компьютере и подключитесь к P-2602. Установите бинарный режим передачи перед тем, как начинать пересылку данных.
4. Используйте клиент TFTP (смотрите пример ниже) для передачи файлов между P-2602 и компьютером. Имя файла настроек – "`rom-0`" (rom-нуль, а не заглавная буква "O").

Обратите внимание на то, что соединение telnet должно оставаться активным до и во время передачи по TFTP. Для дополнительной информации о командах TFTP (смотрите следующий пример) обращайтесь к документации о программе-клиенте TFTP. При работе в системе UNIX используйте команду "`get`" для передачи от P-2602 к компьютеру и "binary" для установки режима бинарной передачи.

25.7.5 Пример команды TFTP для резервного копирования настроек

Ниже дан пример команды TFTP:

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

где "`i`" указывает на передачу в режиме двоичных файлов (используйте этот режим для передачи нетекстовых файлов), "`host`" – IP-адрес P-2602, "`get`" передает исходный файл в P-2602 (`rom-0`, имя файла настроек в P-2602) в целевой файл компьютере и переименовывает его в config.rom.

25.7.6 Резервное копирование настроек с помощью TFTP-клиентов с графическим интерфейсом

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

Таб. 122 Общие команды для клиентов TFTP на основе GUI

КОМАНДА	ОПИСАНИЕ
Host	Введите IP-адрес P-2602. 192.168.1.1 – заводской IP-адрес P-2602.
Send/Fetch	"Send" ("Отправить") используется для выгрузки файла на P-2602, а "Fetch" ("Получить") – для резервного копирования файла на компьютере.
Local File	Введите путь и имя файла микропрограммы (расширение *.bin) или файл настроек (расширение *.rom) в своем компьютере.

Таб. 122 Общие команды для клиентов TFTP на основе GUI (продолжение)

КОМАНДА	ОПИСАНИЕ
Remote File	Это имя файла настроек в P-2602. Имя файла микропрограммы - “ras”, а для файла настроек – “rom-0”.
Binary	Передача в режиме двоичных файлов.
Abort	Остановка передачи файла.

Подробнее о настройках, запрещающих доступ по TFTP или FTP из WAN, см. разд. 25.3 на стр. 330.

25.8 Использование команд FTP/TFTP для восстановления настроек

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

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

Примечание: ВНИМАНИЕ!
Не прерывайте процесс передачи файлов, иначе устройство может НЕОБРАТИМО ВЫЙТИ ИЗ СТРОЯ. После завершения восстановления настроек устройство автоматически перезагрузится.

25.8.1 Пример восстановления с использованием сеанса FTP

Рис. 181 Пример восстановления с использованием сеанса FTP

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

Настройки, запрещающие доступ по TFTP или FTP через WAN, описаны в разд. 25.3 на стр. 330.

25.9 Загрузка файлов микропрограмм и настроек по FTP и TFTP

В этом разделе описано, как выгружать микропрограмму и файлы настроек.

Примечание: ВНИМАНИЕ!
Не прерывайте процесс передачи файлов, иначе устройство может НЕОБРАТИМО ВЫЙТИ ИЗ СТРОЯ.

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

25.9.1 Пример загрузки файла по FTP из приглашения DOS

1. Запустите FTP-клиент на своем компьютере.
2. Введите команду “open”, набрав после нее пробел и IP-адрес устройства.
3. Нажмите [ENTER] ([ВВОД]) , когда потребуется имя пользователя.
4. Введите пароль (по умолчанию – “1234”).
5. Введите “bin”, чтобы установить режим передачи двоичных файлов.
6. Используйте команду “put” для передачи файлов с компьютера в устройство, например, “put firmware.bin ras” осуществляет передачу микропрограммы с компьютера (firmware.bin) в устройство, где файл переименовывается в “ras”. Подобным образом команда “put config.rom rom-0” передает файл настроек с компьютера (config.rom) в устройство, переименовывая его в “rom-0”. Аналогичным образом “get rom-0 config.rom” обеспечивает передачу файла настроек с устройства в компьютер и переименование его в ““config.rom”. Подробнее о схеме именования файлов см. выше в этой главе.
7. Введите “quit” для выхода из приглашения FTP.

25.9.2 Пример сеанса FTP для загрузки файла микропрограммы

Рис. 182 Пример сеанса FTP для загрузки файла микропрограммы

```
331 Enter PASS command
Password:
230 Logged in
ftp>bin
200 Type I OK
ftp> put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 1103936 bytes sent in 1.10Seconds
297.89Kbytes/sec.
ftp> quit
```

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

Настройки, запрещающие доступ по TFTP или FTP через WAN, описаны в разд. 25.3 на стр. 330.

25.9.3 Загрузка файла по протоколу TFTP

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

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

1. Используйте telnet со своего компьютера для подключения к устройству и зарегистрируйтесь. Поскольку TFTP не имеет системы проверки безопасности, устройство записывает IP-адрес клиента telnet и принимает запросы TFTP только с этого адреса.
2. Введите команду “sys stdio 0” для отключения отслеживания неактивности управляющего интерфейса, чтобы пересылка TFTP не прерывалась. Когда передача файлов завершится, введите команду “command sys stdio 5” для восстановления пятиминутного интервала неактивности управляющего интерфейса (по умолчанию).
3. Запустите клиент TFTP на своем компьютере и подключитесь к устройству. Установите бинарный режим передачи перед тем, как начинать пересылку данных.
4. Используйте клиент TFTP (смотрите пример ниже) для передачи файлов между устройством и компьютером. Имя файла микропрограммы – “ras”.

Обратите внимание, что до и во время передачи по TFTP Telnet-соединение должно быть активным, а устройство должно находиться в режиме командной строки. Для дополнительной информации о командах TFTP (смотрите следующий пример) обращайтесь к документации о программе-клиенте TFTP. При работе в системе UNIX используйте команду “get” для передачи от устройства к компьютеру, “put” – в обратном направлении и “binary” для установки режима бинарной передачи.

25.9.4 Пример команды загрузки по TFTP

Ниже дан пример команды TFTP:

```
tftp [-i] host put firmware.bin ras
```

где “i” указывает на двоичный режим передачи образа (используйте этот режим при передаче нетекстовых файлов), “host” является IP-адресом устройства, а “put” обеспечивает передачу источника файла в компьютере (firmware.bin – имя микропрограммы в компьютере) в место назначения файла на удаленном хосте (ras - имя микропрограммы в устройстве).

Команды, имеющиеся в клиентах TFTP на основе GUI, перечислены выше в данной главе.

Глава 26
Диагностика

На этих экранах (доступных только для чтения) отображаются данные, которые могут помочь вам при диагностике проблем с P-2602.

26.1 Общая диагностика

Чтобы перейти на показанный ниже экран, выберите **Maintenance > Diagnostic**.

Рис. 183 Диагностика: общий экран

Поля изображённого выше экрана описаны в следующей таблице.

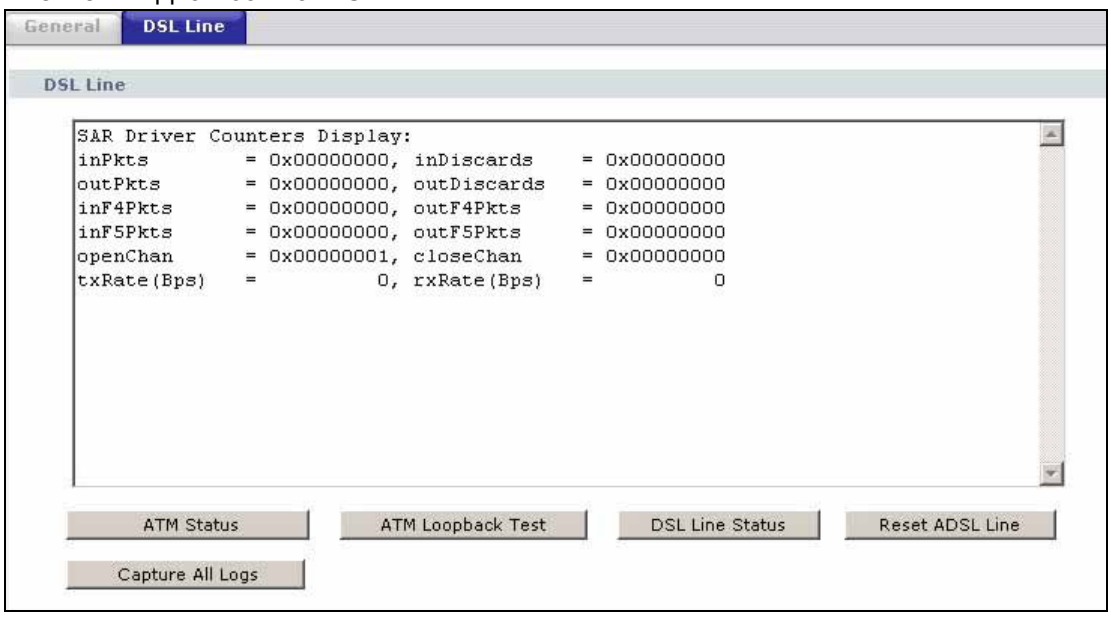
Таб. 123 Диагностика: общий экран

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

26.2 Экран DSL Line Diagnostic

Чтобы перейти на показанный ниже экран, выберите **Maintenance > Diagnostic** > **DSL Line**.

Рис. 184 Диагностика: DSL-линия



Поля изображённого выше экрана описаны в следующей таблице.

Таб. 124 Диагностика: DSL-линия

ПОЛЕ	ОПИСАНИЕ
ATM Status	Нажмите эту кнопку, чтобы просмотреть статистику асинхронного режима передачи (ATM) для вашего DSL-соединения. ATM – это технология построения сетей с высокой пропускной способностью. В ATM-сетях применяются информационные пакеты фиксированного размера, называемые ячейками. Применение ATM позволяет с хорошим результатом реализовать QoS (качество обслуживания). Драйвер SAR (сегментации и повторной сборки) преобразует пакеты в ATM-ячейки. Он также принимает ATM-ячейки и собирает из них пакеты. Счетчики в этом поле обнуляются при запуске устройства. **inPkts** – это число принятых корректных ячеек ATM. **inDiscards** – это число отбракованных полученных ячеек ATM. **outPkts** – это число отправленных ячеек ATM. **outDiscards** – это число отбракованных отправленных ячеек ATM. **inF4Pkts** – это число принятых ячеек OAM F4 (функция 4 эксплуатации, администрирования и управления ATM). Подробнее об OAM для ATM см. в рекомендации ITU I.610. **outF4Pkts** – это число отправленных ячеек ATM OAM F4. **inF5Pkts** – это число принятых ячеек ATM OAM F5. **outF5Pkts** – это число отправленных ячеек ATM OAM F5. **openChan** – это число открытий логического DSL-канала, выполненных P-2602. **closeChan** – это число закрытий логического DSL-канала, выполненных P-2602. **txRate** – скорость передачи (в байтах в секунду). **rxRate** – скорость приёма (в байтах в секунду).
ATM Loopback Test	Нажмите эту кнопку, чтобы запустить тест ATM “обратная петля”. Перед выполнением теста убедитесь, что вы настроили как минимум один PVC с соответствующими VPI/VCI. P-2602 отправляет пакет OAM F5 на DSLAM/ATM-коммутатор, который затем возвращается на P-2602. Кольцевой тест ATM полезен для отыскания проблем, связанных с DSLAM и ATM-сетью.

Таб. 124 Диагностика: DSL-линия (продолжение)

ПОЛЕ	ОПИСАНИЕ
DSL Line Status	Нажмите эту кнопку, чтобы просмотреть статистику по DSL-соединениям. **noise margin downstream** – это соотношение “сигнал-шум” для нисходящей части соединения (к P-2602 от поставщика услуг Интернета), измеряемое в децибелах. Чем выше это число – тем больше амплитуда сигнала по отношению к шуму. **output power upstream** – это уровень мощности (в децибелах), используемый P-2602 для передачи в сторону поставщика услуг Интернета. **attentuation downstream** – это уменьшение амплитуды (в децибелах) DSL-сигнала, поступающего на P-2602 от поставщика услуг Интернета. Модуляция DMT (Discrete Multi-Tone, дискретная многотоновая) делит полосу пропускания линии на поднесущие полосы (подканалы или тональные диапазоны) шириной 4,312 КГц каждая. На остальной части экрана показано распределение битовых полос для линии. Оно отображается в виде шестнадцатеричного числа битов, передаваемых в каждом тональном диапазоне. Эти данные позволяют сделать вывод о качестве соединения и достаточности ширины поднесущей для поддержки скоростей передачи ADSL, а также могут указать на наличие определённых видов помех или затуханий. Дополнительная информация о DMT содержится в рекомендациях ITU-T G.992.1. Чем лучшие характеристики (меньшую протяжённость) имеет линия, тем выше число битов, передаваемых в каждом тональном диапазоне DMT. В каждом тональном диапазоне DMT может передаваться не более 15 битов. Некоторые тональные диапазоны вообще не несут битов, поскольку между восходящим и нисходящим каналами должно иметься разделение частот.

Reset ADSL Line	Нажмите эту кнопку, чтобы переинициализировать ADSL-линию. После этого в крупном текстовом поле над этой кнопкой будет высвечиваться ход выполнения и результат операции, например:
	`Start to reset ADSL (Начало сброса ADSL-линии)`
	`Loading ADSL modem F/W... (Загрузка микропрограммы ADSL-модема)`
	`Reset ADSL Line Successfully! (Сброс ADSL-линии произведен успешно)`

Capture All Logs	Нажмите эту кнопку, чтобы просмотреть сведения и статистику по всем параметрам P-2602, связанным с ATM, DSL-соединением, настройками DHCP, версией микропрограммы, IP-адресами WAN и шлюза по умолчанию, VPI/VCI и IP-адресом в LAN.

Глава 27
Поиск и устранение неполадок

В этой главе рассмотрены вероятные проблемы и соответствующие способы их решения.

27.1 Проблемы, связанные с подготовкой P-2602 к работе

Таб. 125 Устранение проблем, связанных с подготовкой устройства к работе

ПРОБЛЕМА	МЕРЫ ПО УСТРАНЕНИЮ
При включении питания P-2602 не один светодиод не загорается.	Убедитесь, что блок питания P-2602 соединен с P-2602 и включен в соответствующую розетку. Убедитесь, что P-2602 и источник питания включены. Выключите P-2602 и включите его снова. Если проблему не удается устранить, может иметь место неисправность оборудования. В этом случае необходимо обратиться к поставщику.

27.2 Проблемы, связанные с локальной сетью

Таб. 126 Устранение проблем, связанных с локальной сетью

ПРОБЛЕМА	МЕРЫ ПО УСТРАНЕНИЮ
Не горят светодиоды **ETHERNET**.	Проверьте подключения Ethernet-кабелей (подробности см. в *Руководстве по быстрому запуску*). Проверьте, исправны ли Ethernet-кабели
	Убедитесь, что Ethernet-адаптер в вашем компьютере работает исправно.
Невозможно обращаться к P-2602 из локальной сети.	Если функция **Any IP** не включена, убедитесь, что IP-адрес и маска подсети P-2602 и вашего компьютера относятся к одной подсети.

27.3 Проблемы, связанные с WAN

Таб. 127 Устранение проблем, связанных с WAN

ПРОБЛЕМА	МЕРЫ ПО УСТРАНЕНИЮ
Светодиод **DSL** не горит.	Проверьте телефонные провода и соединения между портом **DSL** на P-2602 и телефонной розеткой.
	Убедитесь, что телефонная компания протестировала вашу телефонную линию и подключила к ней DSL-канал.
	Произведите сброс линии DSL, чтобы заново проинициализировать канал связи с DSLAM. Подробности см. в разд. 26.2 на стр. 344.
Не удается получить IP-адрес WAN от поставщика услуг Интернета. (Светодиод **INTERNET** горит красным светом.)	Поставщик услуг Интернета обеспечивает IP-адрес в сети WAN после прохождения аутентификации. Аутентификация может производиться по имени пользователя и паролю, по MAC-адресу или имени хоста. Имя пользователя и пароль применяются только при инкапсуляции PPPoE и PPPoA. Убедитесь, что вы правильно выбрали тип службы (**Service Type**), имя пользователя (**User Name**) и пароль (**Password**); следите за тем, чтобы точно соблюдался регистр символов. См. разд. 7.5 на стр. 105.
Не удается выйти в Интернет.	Убедитесь, что устройство P-2602 находится во включенном состоянии и подключено к сети. Проверите настройки WAN. См. гл. 7 на стр. 99. Убедитесь, что имя пользователя и пароль введены правильно. Если вы используете PPPoE, убедитесь, что режим моста включен.
Соединение с Интернетом прерывается.	Если вы используете инкапсуляцию PPPoA или PPPoE, проверьте настройку интервала неактивности. См. разд. 7.5 на стр. 105. Обратитесь к поставщику услуг Интернета.

27.4 Проблемы, связанные с доступом к устройству ZyXEL

Таб. 128 Устранение проблем, связанных с доступом к устройству

ПРОБЛЕМА	МЕРЫ ПО УСТРАНЕНИЮ
Не удается получить доступ к P-2602.	Имя пользователя – “admin”. Пароль по умолчанию – “1234”. Поля **Password** (имя пользователя) и **Username** (пароль) чувствительны к регистру символов. Убедитесь, что имя пользователя и пароль введены в правильном регистре. Если вы сменили пароль и впоследствии его забыли, вам потребуется загрузить файл настроек по умолчанию. При этом восстанавливаются все заводские настройки, включая пароль.
Невозможно войти в веб-конфигуратор.	Проверьте, нет ли активного сеанса Telnet. Если настройка выполняется через WAN, укажите IP-адрес P-2602 на стороне WAN. См. указания по проверке соединения с WAN. Если настройка выполняется через LAN, укажите IP-адрес P-2602 на стороне LAN. См. указания по проверке соединения с LAN. Проверьте, разрешен ли доступ к службе WWW. Если вы настроили IP-адрес защищенного клиента, IP-адрес вашего компьютера должен с ним совпадать. Подробные указания см. в гл. 21 на стр. 293. Чтобы устройство было доступно через LAN, IP-адреса вашего компьютера и P-2602 должны находиться в одной подсети. Если вы изменили IP-адрес P-2602 на стороне LAN, введите в качестве URL новый адрес. Проверьте, разрешены ли всплывающие окна, сценарии JavaScripts и апплеты Java (см. указания в следующем подразделе).
	Также может потребоваться очистить кэш вашего браузера. В Internet Explorer выберите **Tools** (Сервис), **Internet Options** (Свойства обозревателя). Откроется экран **Internet Options** (Свойства обозревателя). На закладке **General** (Общие) выберите **Delete Files** (Удалить файлы). В появившемся окне отметьте флажок **Delete all offline content** (Удалить это содержимое) и нажмите **OK**. На экране **Internet Options** (Свойства обозревателя) выберите **OK**, чтобы закрыть этот экран. Если вы отсоединили ваш компьютер от одного устройства и подключили его к другому устройству, которое имеет тот же самый IP-адрес, в таблице ARP (протокола разрешения адресов) на вашем компьютере могла остаться запись, в которой IP-адрес управляющего интерфейса связан с MAC-адресом предыдущего устройства). В командной строке Windows наберите **arp -d**, чтобы удалить все записи из таблицы ARP вашего компьютера.
Не работает дистанционное управление P-2602 из LAN или WAN.	В гл. 21 на стр. 293 описаны сценарии, при которых дистанционное управление невозможно.
	Если настройка выполняется через WAN, укажите IP-адрес P-2602 на стороне WAN. Если настройка выполняется через LAN, укажите IP-адрес P-2602 на стороне LAN.

27.4.1 Разрешение всплывающих окон, сценариев JavaScript и апплетов Java

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

- На компьютере в веб-браузере нужно разрешить всплывающие окна.
- Сценарии JavaScript (их выполнение разрешено по умолчанию).
- Разрешения на выполнение Java-кода (включены по умолчанию).

Примечание: Здесь рассмотрены экраны Internet Explorer 6. Экраны в других версиях Internet Explorer могут отличаться.

27.4.1.1 Блокирование всплывающих окон в Internet Explorer

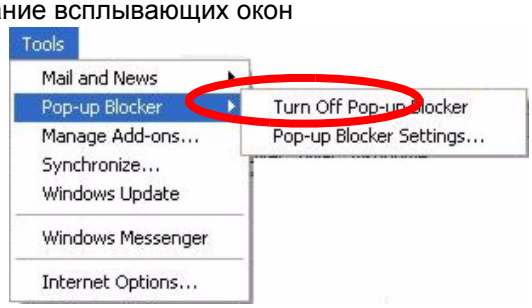
Для входа в устройство может потребоваться отключить блокирование всплывающих окон.

Для этого следует либо полностью отключить блокирование (которое по умолчанию включено Windows XP с пакетом исправлений Service Pack 2), либо включить блокирование, создав исключение для IP-адреса вашего устройства.

27.4.1.1.1 Отключение блокирования всплывающих окон

1 В Internet Explorer выберите **Tools** (Сервис), **Pop-up Blocker** (Блокирование всплывающих окон) и выберите **Turn Off Pop-up Blocker** (Отключить блокирование всплывающих окон).

Рис. 185 Блокирование всплывающих окон

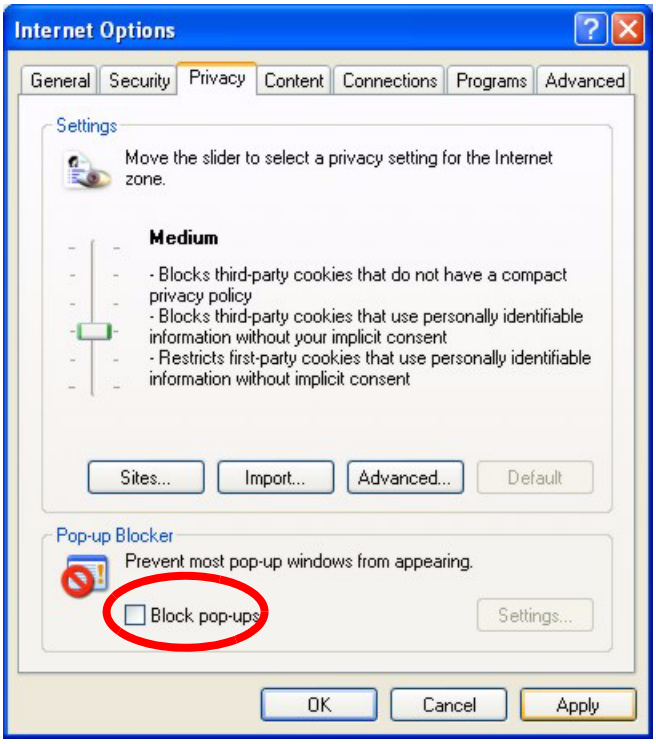


Проверить, включено ли блокирование всплывающих окон, можно в разделе **Pop-up Blocker** (Блокирование всплывающих окон) на закладке **Privacy** (Конфиденциальность).

1 В Internet Explorer выберите **Tools** (Сервис), **Internet Options** (Свойства обозревателя), **Privacy** (Конфиденциальность).

2 Снимите флажок **Block pop-ups** (Блокировать всплывающие окна) в разделе **Pop-up Blocker** (Блокирование всплывающих окон). При этом отключаются все средства блокирования всплывающих окон, которые могли быть активированы.

Рис. 186 Свойства обозревателя



3 Чтобы сохранить настройки, нажмите кнопку **Apply**.

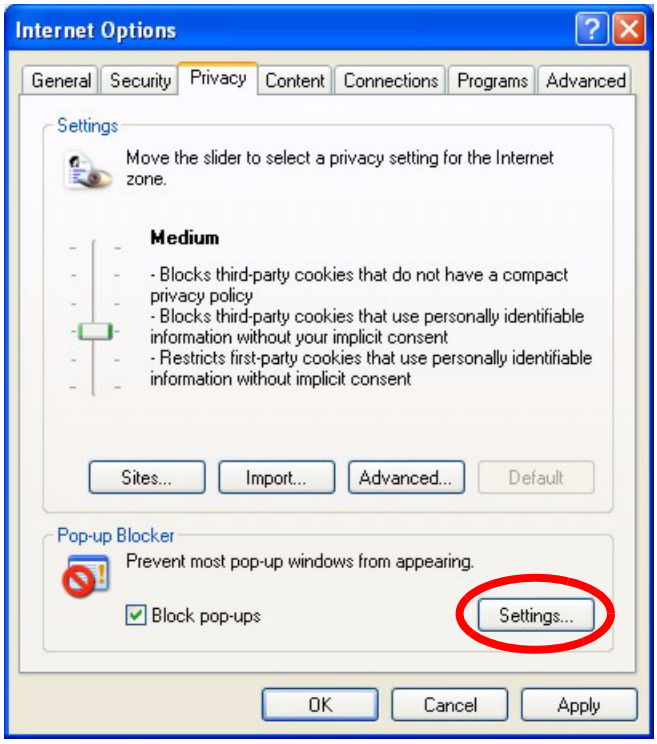
27.4.1.1.2 Разрешение всплывающих окон в исключительном порядке

Вместо полного снятия блокирования можно разрешить всплывающие окна только от вашего устройства. Для этого выполните описанные ниже операции.

1 В Internet Explorer выберите **Tools** (Сервис), **Internet Options** (Свойства обозревателя) и перейдите на закладку **Privacy** (Конфиденциальность).

2 Выберите **Settings…** (Параметры), чтобы открыть экран **Pop-up Blocker Settings** (Параметры блокирования всплывающих окон).

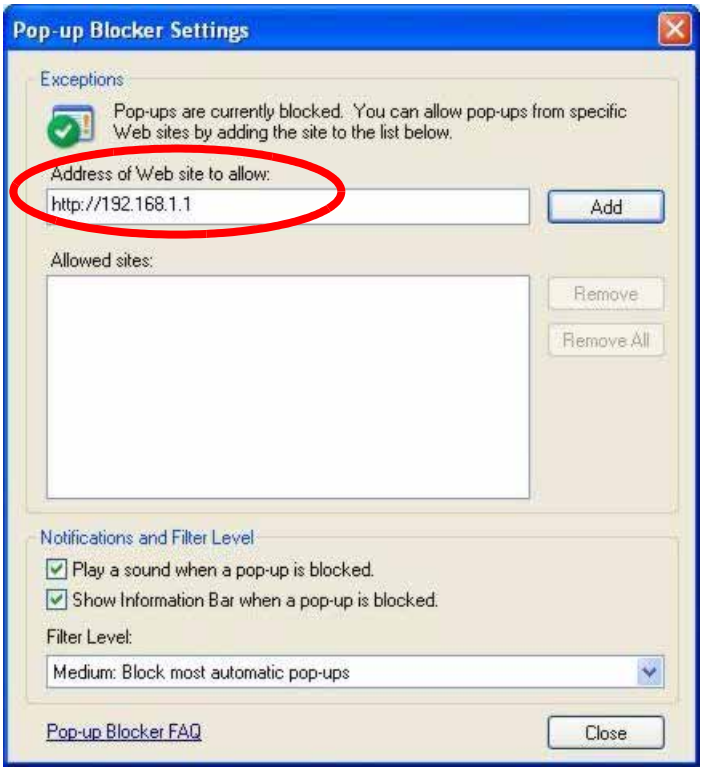
Рис. 187 Свойства обозревателя



3 Введите IP-адрес вашего устройства (web-страница, которую Вы не хотите блокировать) с префиксом “http: //”. Пример: http://192.168.1.1.

4 Нажмите **Add** (Добавить), чтобы внести IP-адрес в список **Allowed sites** (Разрешенные узлы).

Рис. 188 Параметры блокирования всплывающих окон



5 Нажмите **Close** (Закрыть), чтобы вернуться на экран **Privacy** (Конфиденциальность).

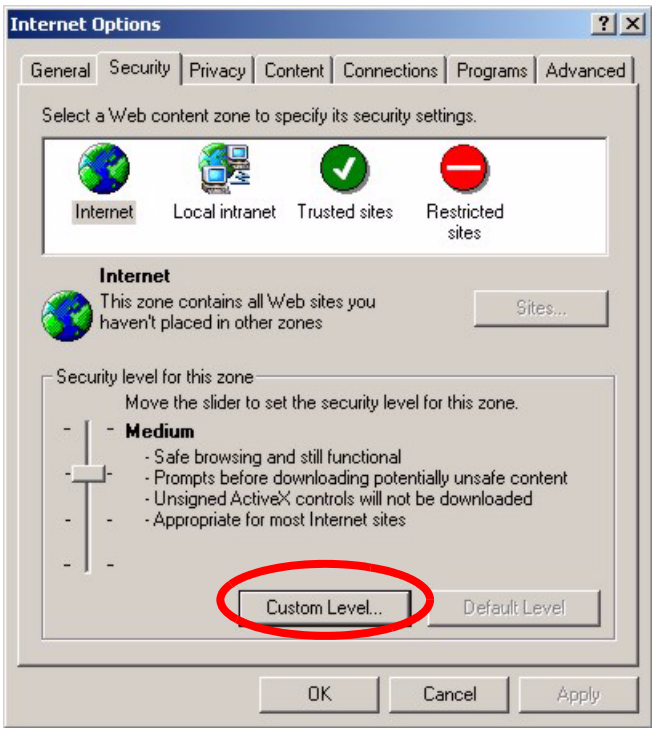
6 Чтобы сохранить настройки, нажмите кнопку **Apply**.

27.4.1.2 Сценарии JavaScript

Если страницы веб-конфигуратора в Internet Explorer отображаются неправильно, проверьте, разрешено ли выполнение сценариев JavaScript.

1 В Internet Explorer выберите **Tools** (Сервис), **Internet Options** (Свойства обозревателя) и перейдите на закладку **Security** (Безопасность).

Рис. 189 Свойства обозревателя



2 Нажмите кнопку **Custom Level...** (Другой).

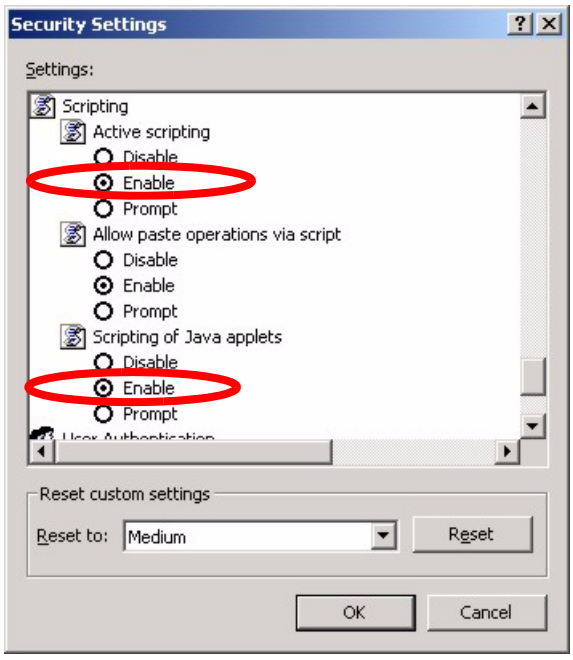
3 Пролистайте список до раздела **Scripting** (Сценарии).

4 В подразделе **Active scripting** (Активные сценарии) проверьте, выбран ли переключатель **Enable** (Разрешить; этот вариант выбран по умолчанию).

5 В подразделе **Scripting of Java applets** (Выполнять сценарии приложений Java) проверьте, выбран ли переключатель **Enable** (Разрешить; этот вариант выбран по умолчанию).

6 Нажмите кнопку **OK**, чтобы закрыть окно.

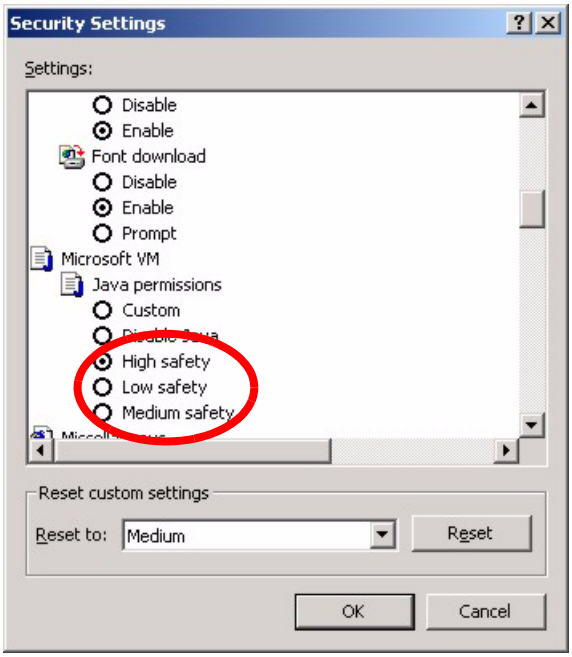
Рис. 190 Параметры безопасности – сценарии JavaScript



27.4.1.3 Разрешения на выполнение Java-апплетов

1. В Internet Explorer выберите **Tools** (Сервис), **Internet Options** (Свойства обозревателя) и перейдите на закладку **Security** (Безопасность).
2. Нажмите кнопку **Custom Level...** (Другой).
3. Пролистайте список до раздела **Microsoft VM** (Виртуальная машина Microsoft).
4. В подразделе **Java permissions** (Разрешения Java) проверьте, выбран ли уровень безопасности.
5. Нажмите кнопку **OK**, чтобы закрыть окно.

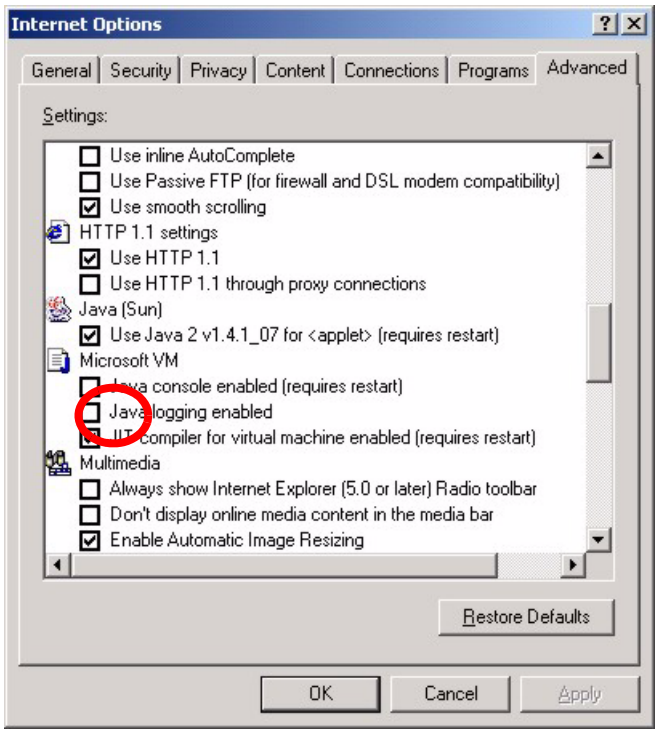
Рис. 191 Параметры безопасности – Java-апплеты



27.4.1.3.1 JAVA (Sun)

1. В Internet Explorer выберите **Tools** (Сервис), **Internet Options** (Свойства обозревателя) и перейдите на закладку **Advanced** (Дополнительно).
2. Убедитесь, что в подразделе **Java (Sun)** выбран пункт **Use Java 2 for <applet>**.
3. Нажмите кнопку **OK**, чтобы закрыть окно.

Рис. 192 Java (Sun)



27.5 Проблемы, связанные с телефонной связью

Таб. 129 Устранение проблем, связанных с телефонной связью

ПРОБЛЕМА	МЕРЫ ПО УСТРАНЕНИЮ
Телефонный порт работает или в телефонной трубке отсутствует гудок.	Проверьте подключение телефона и телефонный провод. Удостоверьтесь, что настройки на экране **VoIP SIP Settings** выполнены правильно.

Таб. 129 Устранение проблем, связанных с телефонной связью (продолжение)

ПРОБЛЕМА	МЕРЫ ПО УСТРАНЕНИЮ
Доступ в Интернет имеется, но осуществлять вызовы VoIP невозможно.	Удостоверьтесь, что настройки на экране **VoIP SIP Settings** выполнены правильно. Должен загореться один из светодиодов **PHONE**. Убедитесь, что телефон подключен к правильному порту **PHONE**. Состояние VoIP можно также проверить на экране **Status**. Если настройки VoIP верны, проверьте работоспособность одноранговых вызовов с помощью функции ускоренного вызова. Если связь через ускоренный вызов работает, возможны неполадки с сервером SIP, обратитесь к вашему поставщику услуг VoIP.
Невозможно осуществить вызов с одного телефонного порта P-2602 на другой порт.	Нельзя позвонить на номер SIP, принадлежащий учетной записи SIP, с помощью которой вы осуществляете вызов. P-2602 генерирует сигнал “занято” и не устанавливает вызов, если набираемый номер SIP соответствует исходящему номеру SIP для используемого телефонного порта. Например, если для порта **Phone 1** используется учетная запись SIP 1, а для порта **Phone 2** – учетная запись SIP 2, то можно звонить с порта **Phone 1** на номер учетной записи SIP 2, а с порта **Phone 2** – на номер учетной записи SIP 1.

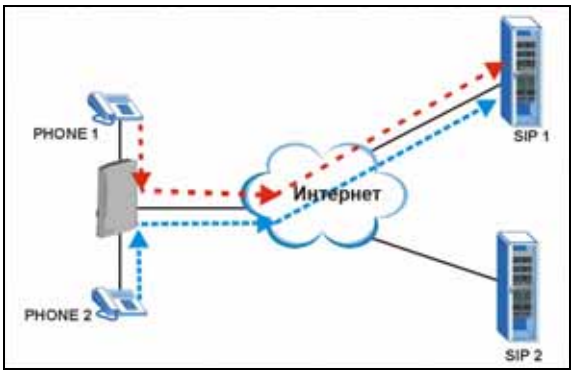
27.6 Проблемы, связанные с использованием нескольких учетных записей SIP

P-2602 имеет два телефонных порта, и на P-2602 можно настроить две учетные записи SIP. По умолчанию P-2602 использует для исходящих вызовов через оба телефонных порта учетную запись SIP 1, а для входящих вызовов – учетные записи SIP 1 и 2. При таких настройках вы всегда используете для исходящих вызовов учетную запись SIP 1 и не можете различать, через какую учетную запись SIP к вам поступают вызовы. Если вы хотите использовать различные схемы набора номера для учета или по другим соображениям, можно настроить телефонные порты так, чтобы при наборе номера или ответе на входящий вызов самостоятельно указывать, какую учетную запись SIP требуется использовать.

27.6.1 Исходящие вызовы

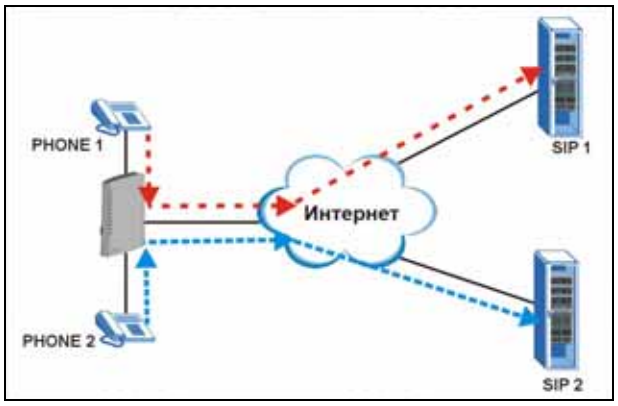
На следующем рисунке показана работа P-2602 в режиме по умолчанию, когда настроены две учетные записи SIP и вы используете два телефона. Когда вы осуществляете вызов с телефона 1 или 2, P-2602 использует учетную запись SIP 1.

Рис. 193 Исходящие вызовы: настройка по умолчанию



В следующем примере телефонный порт 1 настроен на учетную запись SIP 1, а телефонный порт 2 – на учетную запись SIP 2. В этом случае каждый раз, когда вы набираете номер с телефона на порту 1, используется учетная запись SIP 1. Точно так же, когда вы набираете номер с телефона на порту 2, используется учетная запись SIP 2. Для изменения соответствующих настроек служит экран **Analog Phone**. См. **разд. 11.3 на стр. 167**.

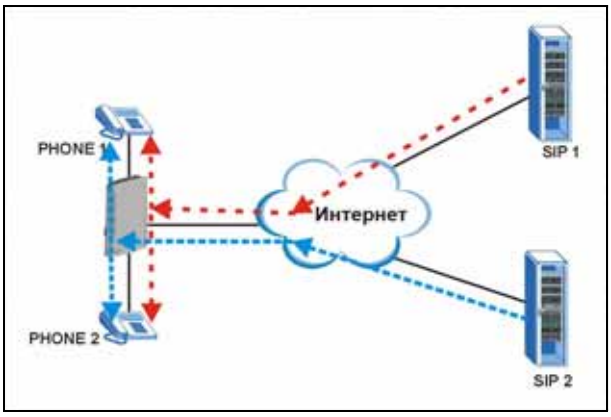
Рис. 194 Исходящие вызовы: индивидуальная настройка



27.6.2 Входящие вызовы

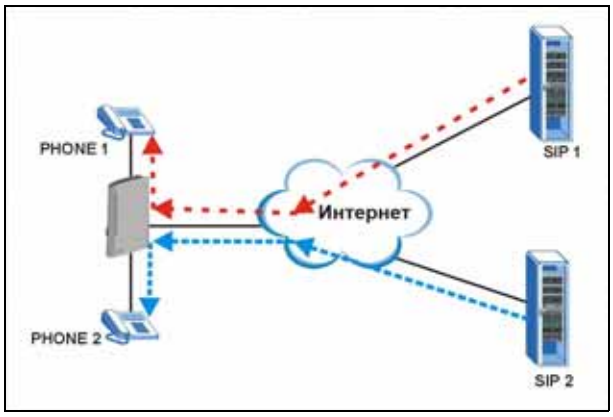
В следующем примере рассмотрена работа P-2602 по умолчанию при наличии двух учетных записей SIP и двух телефонов. Когда вызов поступает на учетную запись SIP 1, звонят телефоны на порту 1 и порту 2. Точно так же, когда вызов поступает на учетную запись SIP 2, звонят телефоны на обоих портах. В обоих случаях нельзя быть уверенным, с какой учетной записи SIP поступает вызов.

Рис. 195 Входящие вызовы: настройка по умолчанию



В следующем примере телефонный порт 1 использует для входящих вызовов учетную запись SIP 1, а телефонный порт 2 – учетную запись SIP 2. При этом каждый раз, когда поступает вызов учетной записи SIP 1, звонит телефон, подключенный к телефонному порту 1. Аналогично, каждый раз, когда поступает вызов учетной записи SIP 2, звонит телефон, подключенный к телефонному порту 2. Соответствующие изменения в настройках можно выполнить на экран **Analog Phone**. См. **разд. 11.3 на стр. 167**.

Рис. 196 Входящие вызовы: индивидуальная настройка



Приложение A
Технические характеристики

Обзор основных характеристик см. в гл. 1 на стр. 39.

Таблицы характеристик

Таб. 130 Технические характеристики устройства

IP-адрес по умолчанию	192.168.1.1
Маска подсети по умолчанию	255.255.255.0 (24 бита)
Пароль по умолчанию	1234
Пул IP-адресов DHCP-сервера	192.168.1.32 – 192.168.1.64
Число статических адресов DHCP	10
Габариты	168 (Ш) x 37 (Г) x 248 (В) мм
Масса	390 г
Электропитание	18 В перем. тока, 1 А
Встроенный коммутатор	Четыре Ethernet-порта RJ-45 с автоматическим согласованием MDI/MDI-X 10/100 Мбит/с
Телефонные порты	2 аналоговых телефонных порта типа RJ-11 FXS
Порт линии ТфОП (только в моделях с индексом “L”)	Один аналоговый телефонный порт RJ-11 FXS для осуществления вызовов по линии ТфОП.
Кнопка сброса	Восстанавливает заводские настройки
Антенна	Одна внешняя симметричная антенна, 2dBi
Рабочая температура	0° C ~ 50° C
Температура хранения	-30° ~ 60° C
Рабочая влажность	10% ~ 85% относительной влажности
Влажность при хранении	10% ~ 90% относительной влажности

Таб. 131 Характеристики микропрограммы

Стандарты ADSL	Поддержка ITU G.992.1 G.dmt (Annex B, U-R2) Встроенный канал операций (EOC) согласно ITU-T G.992.1 ADSL2 G.dmt.bis (G.992.3) ADSL2 G.lite.bis (G.992.4) ADSL 2/2+ AnnexM ADSL2+ (G.992.5) Reach-Extended ADSL (RE ADSL) SRA (плавное регулирование скорости) Автоматическое согласование скорости Физическое соединение ADSL – ATM AAL5 (5-й уровень адаптации ATM) Многопротокольная передача поверх AAL5 (RFC 2684/1483) Многопротокольная передача поверх ATM AAL5 (RFC 2364) PPP поверх Ethernet (RFC 2516) Поддержка нескольких сеансов PPPoE Мультиплексирование VC и LLC До восьми PVC (постоянных виртуальных цепей) I.610 F4/F5 OAM (функции эксплуатации, администрирования и обслуживания) Доступ в Интернет без предварительной настройки
Поддержка других протоколов	Канальный уровень PPP (протокол “точка-точка”) Прозрачный мост для неподдерживаемых протоколов сетевого уровня DHCP-сервер/клиент/агент ретрансляции RIP I/RIP II ICMP QoS для ATM SNMP v1 и v2c с поддержкой MIB II (RFC 1213) Многоадресная рассылка IP, протокол IGMP v1 и v2 Прокси-сервер для IGMP UPnP
Управление	Встроенный веб-конфигуратор Интерпретатор командной строки (CLI) SNMP v1 и v2c с базой данных MIB II Встроенный FTP/TFTP-сервер для обновления микропрограмм и резервного копирования/восстановления файлов настроек Telnet для дистанционного управления Средства дистанционного управления: Telnet, FTP, веб-интерфейс, SNMP и DNS. Автоматическое резервирование VoIP по TFTP / HTTP / HTTPS Дистанционное обновление микропрограммы Syslog

Таб. 131 Характеристики микропрограммы (продолжение)

Беспроводная сеть (только в моделях с индексом “W”)	Соответствие IEEE 802.11g Частотный диапазон: полоса 2.4 ГГц в международном нелицензируемом диапазоне ISM Расширенное мультиплексирование с ортогональным частотным разделением сигналов (OFDM) Скорости передачи данных: 54 Мбит/с, 11 Мбит/с, 5,5 Мбит/с, 2 Мбит/с и 1 Мбит/с с автоматическим снижением Отключение беспроводной сети кнопкой сброса (нажатие на 1 секунду – включение или выключение беспроводной локальной сети; 5 секунд – OTIST; 10 секунд – возврат к заводским настройкам) WPA2 WMM IEEE 802.11i IEEE 802.11e Шифрование WEP (“конфиденциальность, свойственная проводной связи”) 64/128/256 бит. Мост WLAN – LAN До 32 фильтров по MAC-адресам IEEE 802.1x Хранение до 32 встроенных пользовательских профилей в локальной базе данных посредством EAP-MD5 Внешний RADIUS-сервер с использованием EAP-MD5, TLS, TTLS Технология ZyXEL OTIST (мгновенной интеллектуальной настройки безопасности) Антенна: 2dBi, несъемная
Межсетевой экран	Динамический анализ пакетов Предотвращение атак, провоцирующих отказ в обслуживании (DoS): “Ping of Death”, “SYN Flood”, “LAND”, “Smurf” и т.д. Управление доступом для сетевых служб Фильтрация содержания Фильтрация IP и общая фильтрация пакетов Предупреждение об атаках и ведение журналов в реальном времени Отчеты и журналы Сквозной режим SIP ALG
NAT/SUA	Переадресация портов 1024 Сеансы NAT Мультимедиа-приложения PPTP по NAT/SUA Сквозной режим IPSec Сквозной режим SIP ALG
VPN	20 туннелей IPSec IKE и управление ключами в ручном режиме Протоколы AH и ESP Шифрование DES, 3DES и AES Аутентификация SHA-1 и MD5 Инкапсуляция в туннельном и транспортном режиме Прослеживание NAT IPSec Сквозной режим NETBIOS для IPSec

Таб. 131 Характеристики микропрограммы (продолжение)

Фильтрация содержания	Блокирование Web-страниц по ключевым словам в URL.
Статические маршруты	16 IP
Характеристики голосовой связи	SIP версии 2 (протокол инициирования сеанса, RFC 3261) SDP (протокол описания сеанса, RFC 2327) RTP (RFC 1889) RTCP (RFC 1890) Речевые кодеки (кодеры-декодеры) G.711, G.729 Подавление эха G.168 (8 мс ~ 16 мс) Различение сигналов факса и модема Подавление тишины / обнаружение пауз (VAD) Искусственный фон во время паузы (CNG) Динамический (адаптивный) буфер компенсации дрожания фазы Распознавание и генерация DTMF DTMF: внутриполосная и внеполосная передача (RFC 2833),(PCM), (SIP INFO) Установление вызова по схеме “точка-точка” между двумя IAD Быстрый набор номера по телефонной книге с привязкой коротких набираемых номеров к URL. Регистрация нескольких номеров SIP и возможность обработки нескольких сигнальных соединений (для каждого аналогового телефонного порта) Поддержка определителя номера (CID) Гибкая схема набора номера (RFC3525, разд. 7.1.14) Поддержка нескольких учетных записей/телефонных номеров SIP – свободное назначение номеров для каждого телефонного порта
Другие возможности	Any IP Доступ в Интернет без настройки (автоматический поиск VC) Перенаправление трафика Динамическая DNS IP Alias Политики маршрутизации IP SPTGEN QoS

Параметры адаптера питания серии P-2602HWL

Таб. 132 Параметры адаптера питания серии P-2602HWL

ШТЕПСЕЛЬ СЕВЕРОАМЕРИКАНСКОГО СТАНДАРТА	**Поставщик оборудования (OEM)**	**LEI (LEADER ELECTRONICS INC.)**
Модель адаптера питания переменного тока	ADS18B-W 180100	MU18-2180100-A1
Вход питания	Перем. ток 100~240 В / 50/60 Гц / 0,5 А	Перем. ток 100~240 В / 50/60 Гц / 0,6 А

Таб. 132 Параметры адаптера питания серии P-2602HWL (продолжение)

Выход питания	Пост. ток 18 В / 1 А	Пост. ток 18 В / 1 А
Энергопотребление	12 Вт (макс.)	12 Вт (макс.)
Стандарты безопасности	UL,CUL(UL 60950-1)	UL,CUL(UL 60950-1)
ШТЕПСЕЛЬ ЕВРОПЕЙСКОГО СТАНДАРТА		
Модель адаптера питания переменного тока	ADS18B-B 180100	MU18-2180100-C5
Вход питания	Перем. ток 100~240 В / 50/60 Гц / 0,5 А	Перем. ток 100~240 В / 50/60 Гц / 0,6 А
Выход питания	Пост. ток 18 В / 1 А	Пост. ток 18 В / 1 А
Энергопотребление	12 Вт (макс.)	12 Вт (макс.)
Стандарты безопасности	TUV, CE(EN 60950 -1)	TUV, CE(EN 60950-1)
ШТЕПСЕЛЬ БРИТАНСКОГО СТАНДАРТА		
Модель адаптера питания переменного тока	ADS18B-D 180100	MU18-2180100-B2
Вход питания	Перем. ток 100~240 В / 50/60 Гц / 0,5 А	Перем. ток 100~240 В / 50/60 Гц / 0,6 А
Выход питания	Пост. ток 18 В / 1 А	Пост. ток 18 В / 1 А
Энергопотребление	12 Вт (макс.)	12 Вт (макс.)
Стандарты безопасности	TUV, CE(EN 60950 -1)	TUV, CE(EN 60950-1)

Приложение B
Сплиттеры и микрофильтры

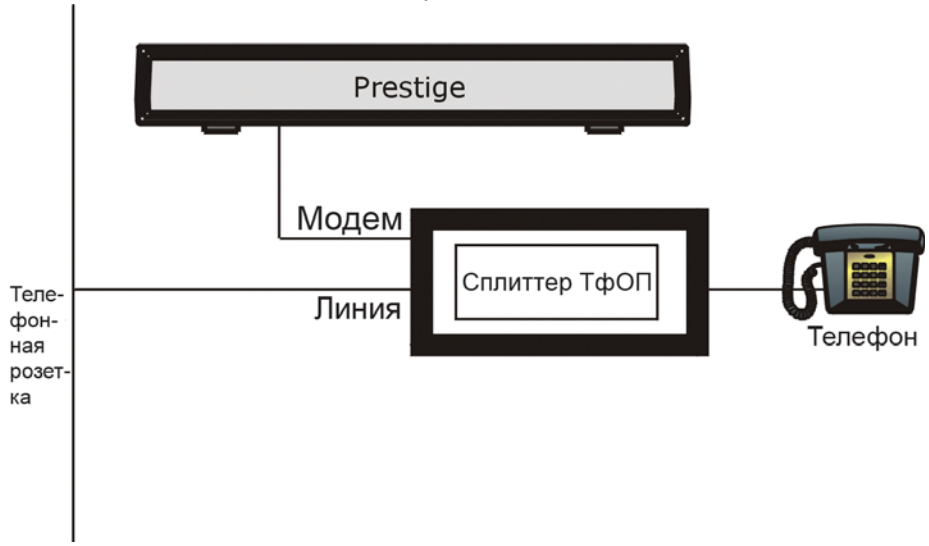
В этом приложении описывается подключение сплиттера аналоговой линии и телефонного микрофильтра.

Подключение сплиттера аналоговой линии

При использовании полноскоростного стандарта (G.dmt) ADSL для разделения телефонного сигнала и ADSL-сигнала необходим сплиттер аналоговой линии. Сплиттер позволяет одновременно пользоваться Интернетом и телефонной связью по одной линии. Сплиттер также блокирует помехи от телефонных трубок.

Сплиттер аналоговой линии целесообразно устанавливать в той точке, где телефонная линия вводится в дом или помещение, как показано на следующем рисунке.

Рис. 197 Подключение сплиттера аналоговой линии



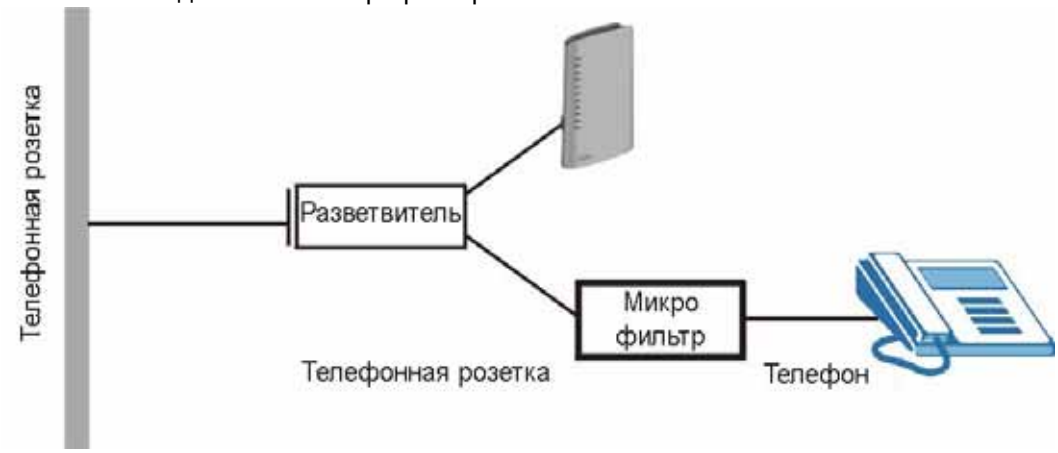
1. К выходу, помеченному “Phone”, подключите телефонный аппарат.
2. К выходу, помеченному “Modem” или DSL, подключите P-2602.
3. Ко входу, помеченному “Line”, подключите линию от телефонной розетки.

Телефонные микрофильтры

Для голосовой телефонной связи используется диапазон низких частот 0 – 4 кГц, а для передачи по ADSL – диапазон более высоких частот, выше 4 кГц. Микрофильтр представляет собой фильтр низких частот, изолирующий телефон от высокочастотных сигналов ADSL. Телефонный микрофильтр требуется не во всех случаях.

1. Соедините телефонную розетку кабелем с одинарным входом разветвителя.
1. Соедините кабелем двойной выход разветвителя со входом “от телефонной розетки” на микрофильтре.
1. Другим кабелем соедините двойной выход разветвителя с P-2602.
1. К выходу “телефон” на микрофильтре подключите ваш телефонный аппарат, как показано на следующем рисунке.

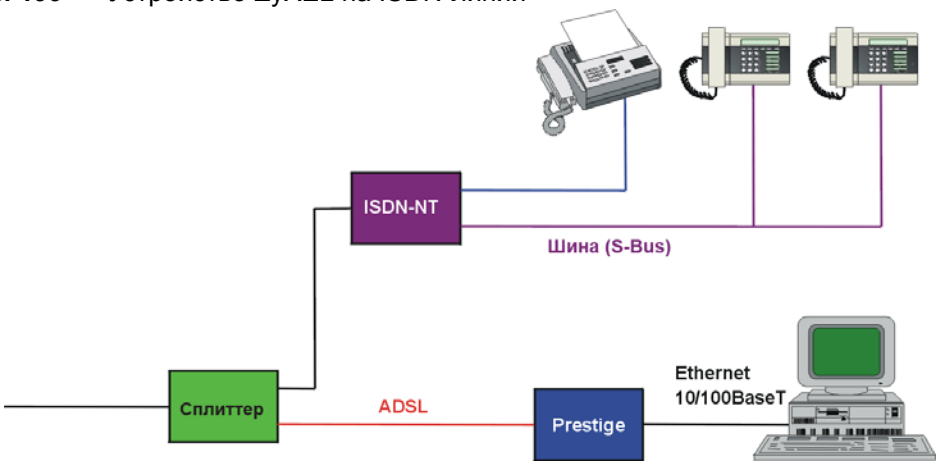
Рис. 198 Подключение микрофильтра



Использование P-2602 с ISDN-линиями

Этот раздел касается только пользователей, применяющих P-2602 с ADSL-каналом по линии ISDN (цифровой сети с интегрированными услугами). Ниже приведен пример установки P-2602 на ISDN-линии.

Рис. 199 Устройство ZyXEL на ISDN-линии



Приложение C
Настройка IP-адреса компьютера

Во всех компьютерах должен быть сетевой адаптер Ethernet 10 Мбит или 100 Мбит и обеспечиваться поддержка протокола TCP/IP.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 и более новые версии этих операционных систем, а также все версии UNIX/LINUX содержат программные компоненты, которые нужны для установки и использования протокола TCP/IP на компьютере. При работе с Windows 3.1 требуется приобретение пакета приложений TCP/IP сторонних производителей.

TCP/IP должен быть установлен на компьютерах, работающих под управлением Windows NT/2000/XP, Macintosh OS 7 и более поздних версий этих операционных систем.

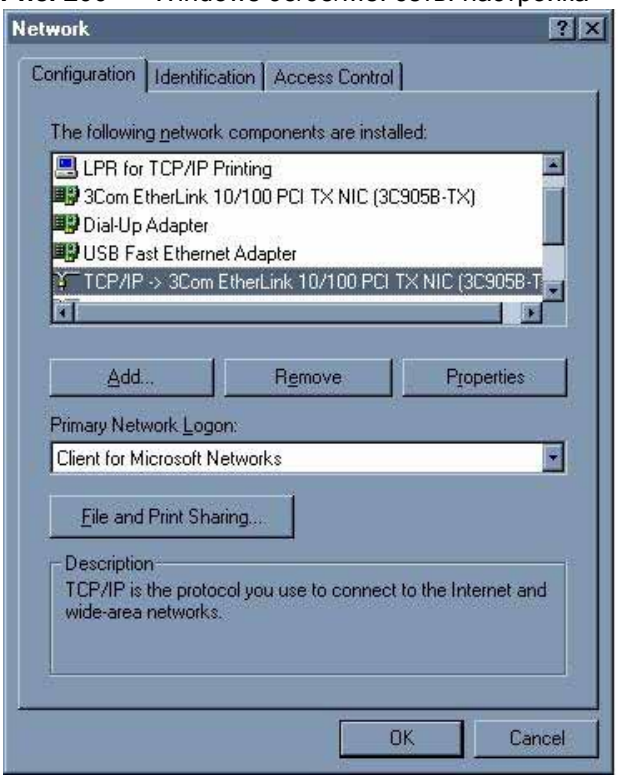
После установки необходимых компонентов TCP/IP настройте параметры TCP/IP для обмена данными через сеть.

Если вместо динамического назначения параметры IP присваиваются в ручном режиме, убедитесь в том, что компьютеры имеют IP-адреса, относящиеся к той же подсети, в которой находится LAN-порт P-2602.

Windows 95/98/Me

Щёлкните кнопку **Start (Пуск)**, **Settings (Настройки)**, **Control Panel (Панель управления)** и выберите двойным щелчком значок **Network (Сеть)** для открытия окна **Network (Сеть)**.

Рис. 200 Windows 95/98/Me: сеть: настройка



Установка компонентов

На вкладке **Configuration (Конфигурация)** окна **Network (Сеть)** отображается список установленных компонентов. Потребуется сетевой адаптер, протокол TCP/IP и клиент для сетей Microsoft.

Если необходим адаптер, выполните следующие действия:

1. В окне **Network (Сеть)** щёлкните кнопку **Add (Добавить)**.
2. Выберите **Adapter (Адаптер)** и щёлкните кнопку **Add (Добавить)**.
3. Выберите производителя и модель сетевого адаптера, затем щёлкните кнопку **OK**.

Если необходимо установить протокол TCP/IP, выполните следующие действия:

1. В окне **Network (Сеть)** щёлкните кнопку **Add (Добавить)**.
2. Выберите **Protocol (Протокол)** и щёлкните кнопку **Add (Добавить)**.
3. Выберите **Microsoft** в списке производителей – **manufacturers**.
4. Выберите **TCP/IP** в списке сетевых протоколов и щёлкните кнопку **OK**.

Если нужен клиент для сетей Microsoft, выполните следующие действия:

1. Щелкните кнопку **Add (Добавить)**.

2 Выберите **Client (Клиент)** и щёлкните кнопку **Add (Добавить)**.

3 Выберите **Microsoft** в списке производителей.

4 Выберите **Client for Microsoft Networks (Клиент для сетей Microsoft)** в списке сетевых клиентов и щёлкните кнопку **OK**.

5 Перезапустите компьютер, чтобы изменения вступили в силу.

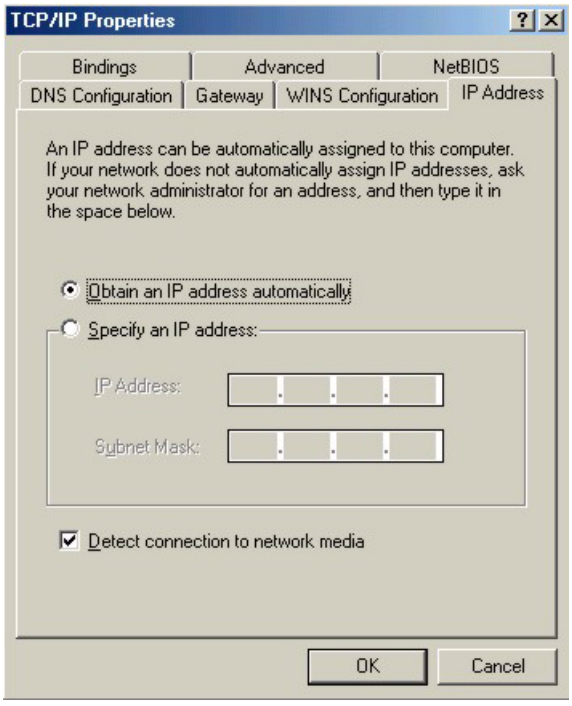
Настройка

1 На вкладке **Configuration (Конфигурация)** окна **Network (Сеть)** выберите запись TCP/IP своего сетевого адаптера и щёлкните **Properties (Свойства)**.

2 Щёлкните вкладку **IP Address (IP-адрес)**.

- Если IP-адрес динамический, выберите переключатель **Obtain an IP address automatically (Получить IP-адрес автоматически)**.
- Если имеется статический IP-адрес, выберите переключатель **Specify an IP address (Указать IP-адрес)** и введите информацию в поля **IP Address (IP-адрес)** и **Subnet Mask (Маска подсети)**.

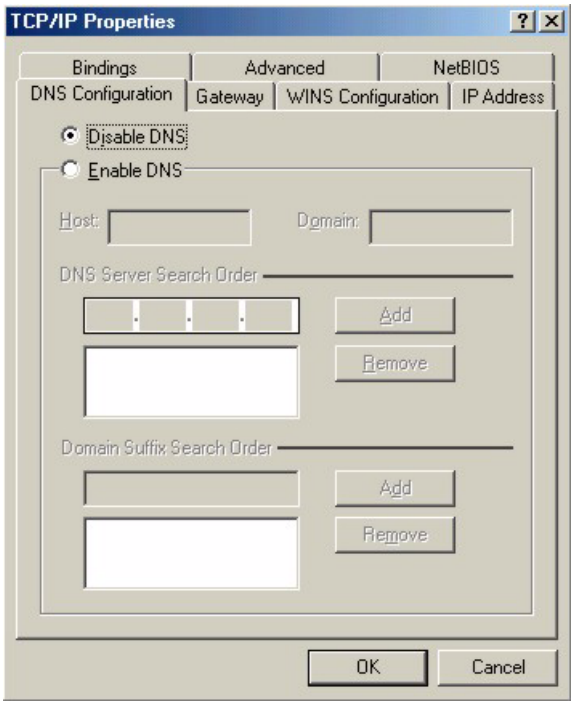
Рис. 201 Windows 95/98/Me: свойства TCP/IP: IP-адрес



3 Щёлкните вкладку **DNS Configuration (Конфигурация DNS)**.

- Если информация о DNS неизвестна, выберите переключатель **Disable DNS (ОтключитьDNS)**.
- Если информация о DNS известна, выберите переключатель **Enable DNS (Включить DNS)** и введите информацию в полях внизу (необязательно заполнять их все).

Рис. 202 Windows 95/98/Me: свойства TCP/IP: конфигурация DNS



4 Щёлкните вкладку **Gateway (Межсетевой шлюз)**.

- Если IP-адрес межсетевого шлюза неизвестен, удалите ранее установленные межсетевые шлюзы.
- Если IP-адрес межсетевого шлюза известен, введите его в поле **New gateway (Новый межсетевой шлюз)** и щёлкните кнопку **Add (Добавить)**.

5 Нажмите кнопку **OK** для сохранения изменений и закройте окно **TCP/IP Properties (СвойстваTCP/IP)**.

6 Нажмите кнопку **OK** для закрытия окна **Network (Сеть)**. При появлении приглашения вставьте компакт-диск Windows.

7 Включите P-2602 и перезапустите компьютер, когда это будет предложено.

Проверка настроек

1 Нажмите кнопку **Start (Пуск)**, **Run (Выполнить)**.

2 В окне **Run (Выполнить)** введите “winipcfg” и щёлкните **OK** для открытия окна **IP Configuration (КонфигурацияIP)**.

3 Выберите свой сетевой адаптер. Вы должны увидеть IP-адрес, маску подсети и межсетевой шлюз по умолчанию своего компьютера.

Windows 2000/NT/XP

1 При работе в Windows XP щёлкните кнопку **start (Пуск)**, **Control Panel (Панель Управления)**. В Windows 2000/ NT щелкните кнопку **Start (Пуск)**, **Settings (Настройки)**, **Control Panel (Панель управления)**.

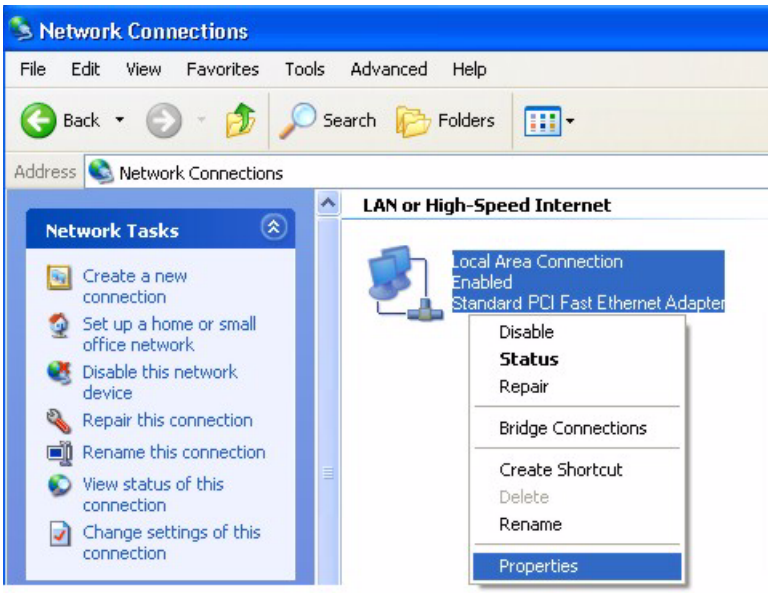
Рис. 203 Windows XP: меню Пуск

2 При работе в Windows XP щёлкните команду **Network Connections (Сетевые подключения)** При работе в Windows 2000/NT щелкните команду **Network and Dial-up Connections (Сеть и коммутируемые подключения)**.

Рис. 204 Windows XP: панель управления

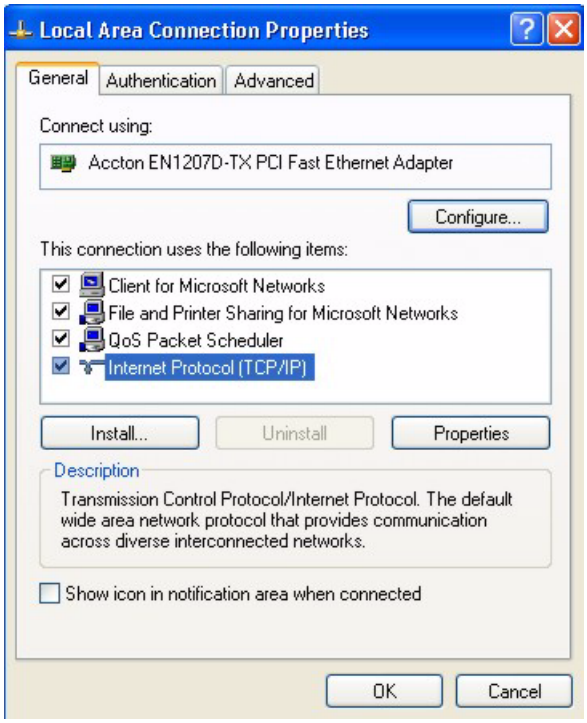
3 Выберите правой кнопкой мыши **Local Area Connection (Подключение по локальной сети)**, затем щёлкните **Properties (Свойства)**.

Рис. 205 Windows XP: панель управления: сетевые подключения: свойства



4 Выберите **Internet Protocol (TCP/IP) (Протокол Интернета (TCP/IP))** (под вкладкой **General (Общие)**) в Win XP) и щёлкните **Properties (Свойства)**.

Рис. 206 Windows XP: Local Area Connection Properties (Подключение по локальной

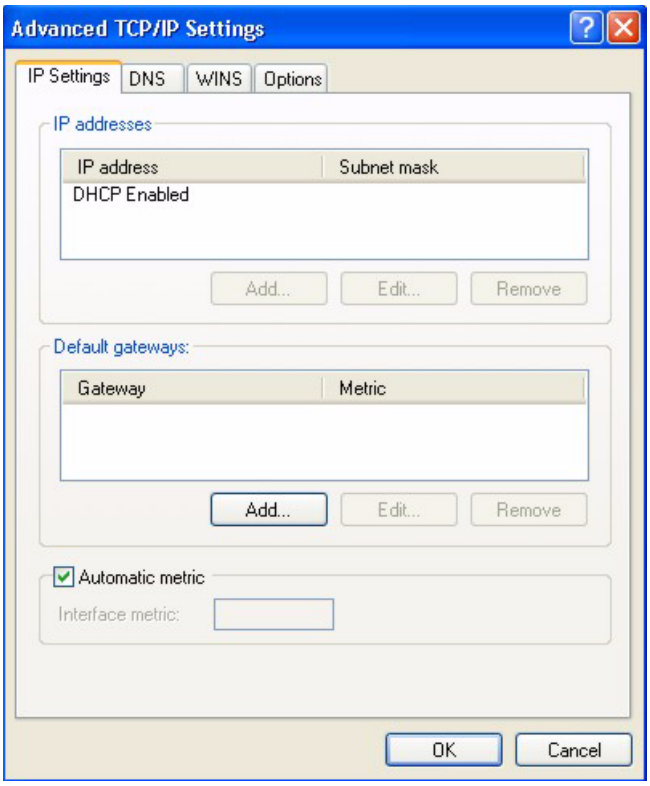


сети – свойства)

5 Открывается окно **Internet Protocol TCP/IP Properties (Свойства: протокол Интернета TCP/IP)** (вкладка **General (Общие)** в Windows XP).

- Если имеется динамический IP-адрес, щёлкните переключатель **Obtain an IP address automatically (Получить IP-адрес автоматически)**.
- Если имеется статический IP-адрес, щёлкните переключатель **Use the following IP Address (Использовать следующий IP-адрес)** и заполните поля **IP address (IP-адрес)**, **Subnet mask (Маска подсети)** и **Default gateway (Основной шлюз)**. Щёлкните кнопку **Advanced (Дополнительно)**.

Рис. 207 Windows XP: дополнительные параметры TCP/IP



6 Если IP-адрес межсетевого шлюза неизвестен, удалите все ранее установленные межсетевые шлюзы на вкладке **IP Settings (Параметры IP)** и щёлкните**OK**.

Если необходимо настроить дополнительные IP-адреса, выполните одно или несколько из следующих действий:

- На вкладке **IP Settings (Параметры IP)**, в разделе IP addresses (IP-адреса), щёлкните кнопку **Add (Добавить)**.
- В окне **TCP/IP Address (Адрес TCP/IP)** введите IP-адрес в поле **IP address (IP-адрес)** и маску подсети в поле **Subnet mask (Маска подсети)**, затем щёлкните кнопку **Add (Добавить)**.
- Выполните два вышеописанных действия для ввода каждого нового IP-адреса.

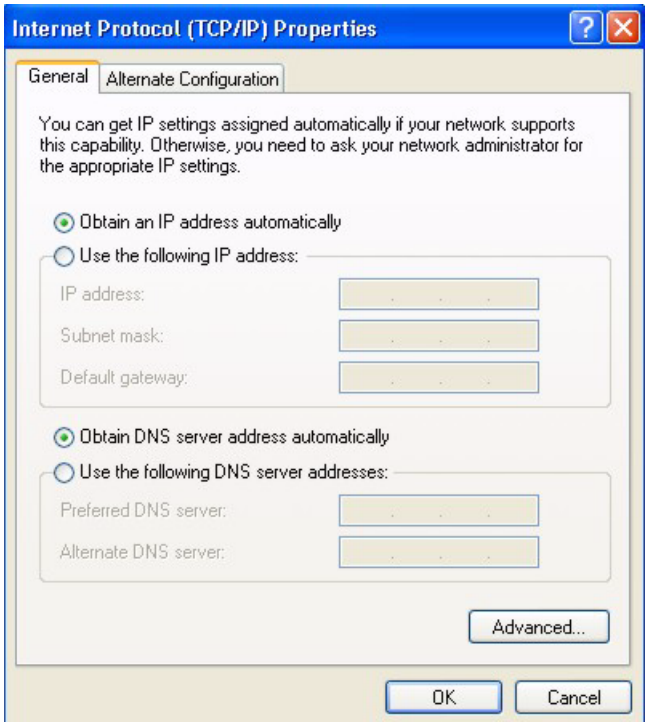
- Настройте дополнительные межсетевые шлюзы по умолчанию на вкладке **IP Settings (Параметры IP)**, щёлкнув кнопку **Add (Добавить)** в разделе **Default gateways (Основные шлюзы)**.
- В окне **TCP/IP Gateway Address (Адрес шлюза TCP/IP)** введите IP-адрес межсетевого шлюза по умолчанию в поле **Gateway (Шлюз)**. Чтобы вручную настроить метрику по умолчанию (количество переходов при передаче), снимите флажок **Automatic metric (Автоматическое назначение метрики)** и введите метрику в поле **Metric (Метрика)**.
- Щелкните кнопку **Add (Добавить)**.
- Повторите три указанных выше действия для добавления каждого межсетевого шлюза по умолчанию.
- Нажмите кнопку **OK** по завершении.

7 В окне **Internet Protocol TCP/IP Properties (Свойства: протокол Интернета TCP/IP)** (вкладка **General (Общие)** в Windows XP):

- Щёлкните переключатель **Obtain DNS server address automatically (Получить адрес DNS-сервера автоматически)**, если адрес сервера неизвестен.
- Если IP-адрес DNS-сервера известен, щёлкните переключатель **Use the following DNS server addresses (Использовать следующие адреса DNS-серверов)** и введите их в полях **Preferred DNS server (Предпочитаемый DNS-сервер)** и **Alternate DNS server (Альтернативный DNS-сервер)**.

  Если DNS-серверы были ранее настроены, щёлкните кнопку **Advanced (Дополнительно)**, затем вкладку **DNS** для их сортировки.

Рис. 208 Windows XP: Internet Protocol (TCP/IP) Properties (Свойства: протокол Интернета TCP/IP)



8 Нажмите кнопку **OK** для закрытия окна **Internet Protocol (TCP/IP) Properties (Свойства: протокол Интернета TCP/IP)**.

9 Нажмите кнопку **OK** для закрытия окна **Local Area Connection Properties (Подключение по локальной сети: свойства)**.

10 Включите P-2602 и перезапустите компьютер (если это будет предложено).

Проверка настроек

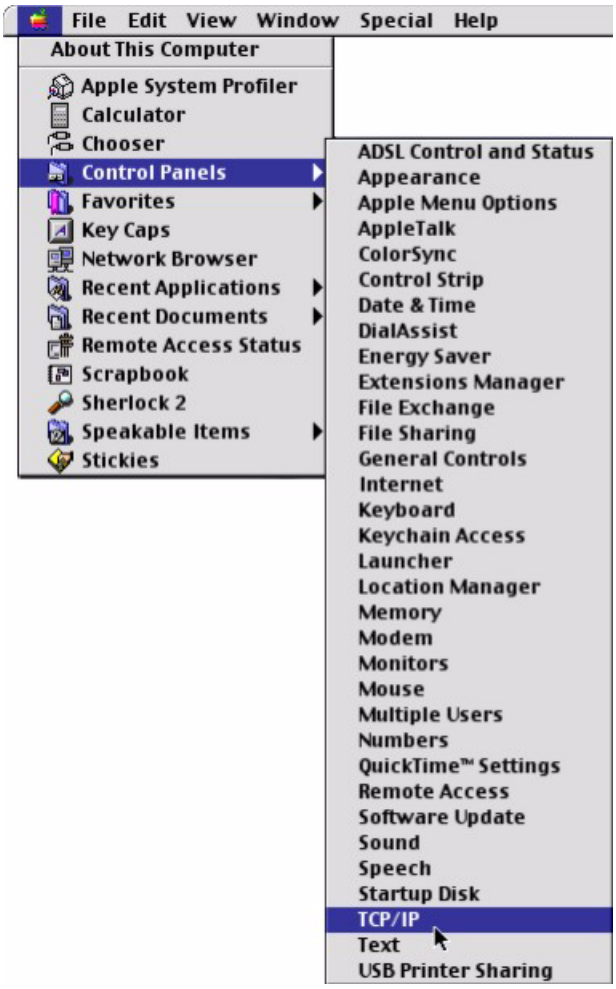
1 Нажмите кнопку **Start (Пуск)**, **All Programs (Все программы)**, **Accessories (Стандартные)**, затем **Command Prompt (Командная строка)**.

2 В окне **Command Prompt (Командная строка)** введите "`ipconfig`" и затем нажмите [ENTER]. Можно также открыть окно **Network Connections (Сетевые подключения)**, щёлкнуть правой кнопкой мыши на сетевом подключении, выбрать пункт **Status (Состояние)**, затем – вкладку **Support (Поддержка)**.

Macintosh OS 8/9

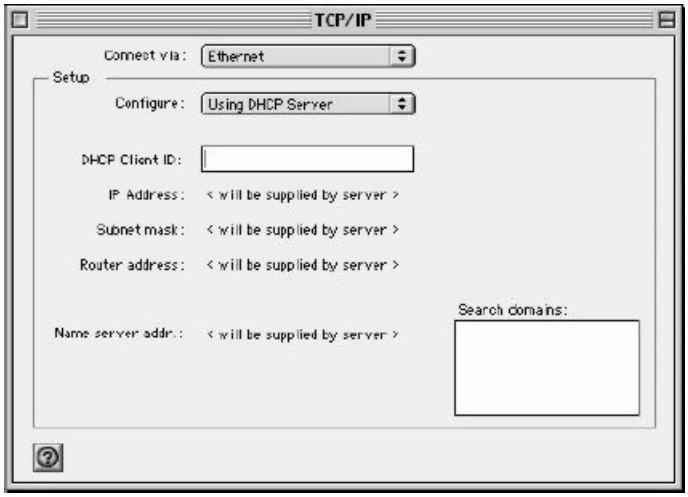
1 Щёлкните меню**Apple**, **Control Panel (Панель управления)** и выберите двойным щелчком пункт **TCP/IP**, чтобы открыть **TCP/IP Control Panel (Панель управления TCP/IP)**.

Рис. 209 Macintosh OS 8/9: меню Apple



2 Выберите **Ethernet built-in (Встроенный Ethernet)** в списке **Connect via (Подключиться через)**.

Рис. 210 Macintosh OS 8/9: TCP/IP



3 Для динамически назначаемых параметров выберите пункт **Using DHCP Server (Использование сервера DHCP)** в списке **Configure:** (Конфигурировать).

4 Для назначения статических параметров выполните следующие действия:

- В списке **Configure (Конфигурировать)** выберите пункт **Manually (Вручную)**.
- Введите свой IP-адрес в поле **IP Address (IP-адрес)**.
- Введите маску подсети в поле **Subnet mask (Маска подсети)**.
- Введите IP-адрес P-2602 в поле **Router address (Адрес маршрутизатора)**.

5 Закройте **TCP/IP Control Panel (Панель управления TCP/IP)**.

6 При появлении приглашения щёлкните **Save (Сохранить)** для сохранения изменений конфигурации.

7 Включите P-2602 и перезапустите компьютер (если это будет предложено).

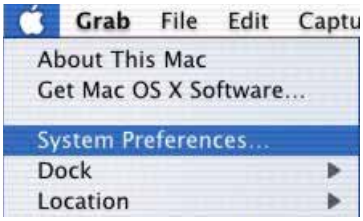
Проверка настроек

Проверьте свойства TCP/IP в окне **TCP/IP Control Panel (Панель управления TCP/IP)**.

Macintosh OS X

1 Щёлкните меню**Apple**, пункт **System Preferences (Параметры системы)** для открытия окна **System Preferences (Параметры системы)**.

Рис. 211 Macintosh OS X: меню Apple

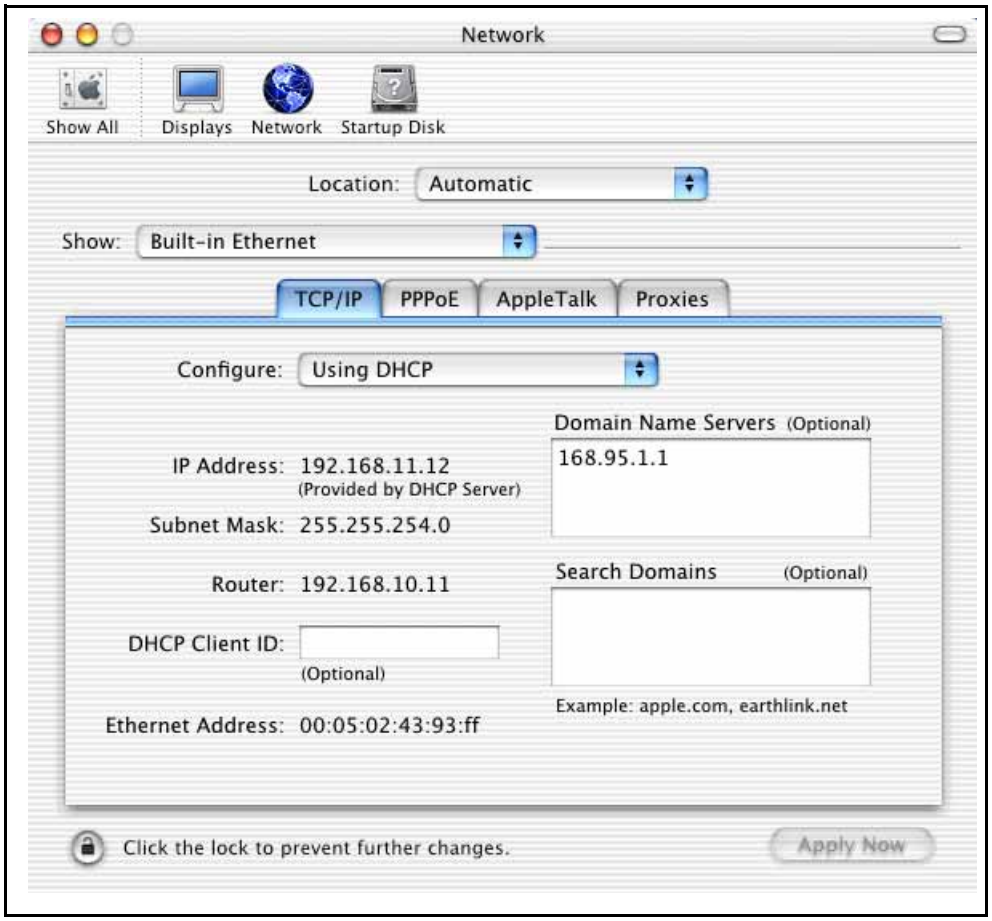


2 Щёлкните **Network (Сеть)** на панели иконок.

- Выберите значение **Automatic (Автоматический)** в списке **Location (Местоположение)**.
- Выберите пункт **Built-in Ethernet (Встроенный Ethernet)** в списке **Show (Показать)**.
- Щёлкните вкладку **TCP/IP**.

3 Для динамического назначения параметров выберите пункт **Using DHCP (Использование DHCP)** в списке **Configure**.

Рис. 212 Macintosh OS X: Network



4 Для назначения статических параметров выполните следующие действия:

- В списке **Configure (Конфигурировать)** выберите пункт **Manually (Вручную)**.
- Введите свой IP-адрес в поле **IP Address (IP-адрес)**.
- Введите маску подсети в поле **Subnet mask (Маска подсети)**.
- Введите IP-адрес P-2602 в поле **Router address (Адрес маршрутизатора)**.

5 Щёлкните кнопку **Apply Now (Применить сейчас)** и закройте окно.

6 Включите P-2602 и перезапустите компьютер (если это будет предложено).

Проверка настроек

Проверьте свойства TCP/IP в окне **Network (Сеть)**.

Приложение D
IP-адреса и деление на подсети

В этом приложении рассмотрены IP-адреса, классы IP-адресов и маски подсетей. Маски подсети можно использовать для деления сети на меньшие по размеру логические подсети.

Общие сведения об IP-адресах

IP-адрес состоит из двух частей: номера сети и идентификатора хоста. Маршрутизаторы ориентируются по номеру сети, чтобы пересылать пакеты в требуемую сеть, а идентификатор хоста идентифицирует конкретное устройство в сети.

IP-адрес состоит из четырёх октетов (восьмибитовых последовательностей), которые записываются в десятичной форме через точку, например, 192.168.1.1. (Октет – это восьмибитовое двоичное число. Таким образом каждый октет имеет возможный диапазон значений от 00000000 до 11111111 в двоичном счислении или от 0 до 255 в десятичном счислении.)

Существует несколько классов IP-адресов. Первый номер сети (192 в вышеупомянутом примере) определяет класс IP-адреса. Номера определены следующим образом:

- Класс “A”: от 0 до 127
- Класс “B”: от 128 до 191
- Класс “C”: от 192 до 223
- Класс “D”: от 224 до 239
- Класс “E”: от 240 до 255

Классы IP-адресов и адреса хостов

Класс IP-адреса определяет число хостов, которое может содержаться в сети.

- В адресе класса “A” первый октет представляет собой номер сети, а оставшиеся три октета образуют номер хоста.
- В адресе класса “B” первые два октета соответствуют номеру сети, а последние два октета - номеру хоста.
- В адресе класса “C” номеру сети соответствуют первые три октета, а идентификатору хоста - последний октет.

В следующей таблице показано распределение номеров сети и идентификаторов хостов для классов A, B и C.

Таб. 133 Классы IP-адресов

IP-АДРЕС	ОКТЕТ 1	ОКТЕТ 2	ОКТЕТ 3	ОКТЕТ 4
Класс “A”	**Номер сети**	Идентификатор хоста	Идентификатор хоста	Идентификатор хоста
Класс “B”	**Номер сети**	**Номер сети**	Идентификатор хоста	Идентификатор хоста
Класс “C”	**Номер сети**	**Номер сети**	**Номер сети**	Идентификатор хоста

IP-адрес, в котором идентификатор хоста состоит целиком из нулей, является IP-адресом сети (пример – 192.168.1.0). IP-адрес, к котором идентификатор хоста состоит целиком из единиц, является широковещательным IP-адресом в соответствующей сети (пример – 192.168.1.255). Поэтому чтобы определить общее количество хостов, разрешенных в сети, необходимо вычесть два из общего числа адресов:

- Адрес класса “C” (1 октет хоста: 8 битов хоста) может иметь $2^8 – 2 = 254$ хоста.
- Адрес класса “B” (2 октета хоста: 16 битов хоста) может иметь $2^{16} – 2 = 65534$ хоста.
- Адрес класса “A” (3 октета хоста: 24 бита хоста) может иметь $2^{24} – 2 =$ приблизительно 16 миллионов хостов.

Классы IP-адресов и идентификаторы сетей

Значение первого октета IP-адреса определяет класс адреса.

- Адреса класса “A” начинаются со старшего бита **0**.
- Адреса класса “B” начинаются с бита **1**, за которым следует бит **0**.
- Адреса класса “C” начинаются с последовательности трех битов: **1 1 0**.
- Адреса класса “D” начинаются с последовательности **1 1 1 0**. Адреса класса “D” используются для многоадресной рассылки, которая служит для отправки информации группам компьютеров.
- Предусмотрен также класс “E”, зарезервированный для использования в будущем.

В следующей таблице приведены допустимые диапазоны адресов для первого октета каждого класса. Этот диапазон определяет число подсетей, которое может иметься в сети.

Таб. 134 Допустимые диапазоны IP-адресов для различных классов

КЛАСС	ДОПУСТИМЫЙ ДИАПАЗОН ЗНАЧЕНИЙ ПЕРВОГО ОКТЕТА (В ДВОИЧНОМ ВИДЕ)	ДОПУСТИМЫЙ ДИАПАЗОН ЗНАЧЕНИЙ ПЕРВОГО ОКТЕТА (В ДЕСЯТИЧНОМ ВИДЕ)
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
Класс “E” (зарезервирован)	От **1111**0000 до **1111**1111	от 240 до 255

Маски подсетей

Маска подсети определяет, какие биты образуют номер сети и какие биты соответствуют идентификатору хоста (с помощью логического “И”).

Маска подсети состоит из 32 двоичных разрядов. Если один из разрядов содержит единицу, соответствующий бит в IP-адресе является частью номера сети. Если разряд содержит ноль, соответствующий бит в IP-адресе является частью идентификатора хоста.

Маски подсетей записываются в десятичном виде через точку, как и IP-адреса. Общепринятые маски подсетей для IP-адресов класса “A”, “B” и “C” выглядят следующим образом.

Таб. 135 Общепринятые маски подсетей

КЛАСС	ОБЩЕПРИНЯТОЕ ЗНАЧЕНИЕ МАСКИ
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Деление на подсети

При делении на подсети назначение классов IP-адресов не учитывается. Например, адрес класса C не обязательно будет состоять из 24-битового номера сети и 8-битового идентификатора хоста. Некоторые биты, отведённые под идентификатор хоста, при делении на подсети могут быть добавлены к битам, обозначающим номер подсети.

Маски подсетей принято задавать в виде непрерывной последовательности единиц, начинающейся со старшего бита, за которой следует непрерывная последовательность нулей; обе последовательности в сумме составляют 32 бита.

Поскольку маска всегда состоит из непрерывной последовательности единиц и непрерывной последовательности нулей, достаточно указывать только число единиц, не записывая значение каждого октета. Для этого обычно после адреса указывается знак “/”, за которым следует число единиц в маске подсети.

Например, обозначение 192.1.1.0 /25 соответствует номеру 192.1.1.0 с маской 255.255.255.128.

В следующей таблице приводятся все допустимые маски подсетей для адресов класса “C”, записанные обоими способами.

Таб. 136 Альтернативный способ записи маски подсети

МАСКА ПОДСЕТИ	ЧИСЛО ЕДИНИЦ В МАСКЕ ПОДСЕТИ	ДВОИЧНОЕ ЗНАЧЕНИЕ ПОСЛЕДНЕГО ОКТЕТА	ДЕСЯТИЧНОЕ ЗНАЧЕНИЕ
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

Первой в таблице приведена общепринятая маска класса “C”. Если маска подсети не указана, то предполагается использование общепринятой маски.

Пример: деление на две подсети

Для примера предположим наличие адреса класса “C” 192.168.1.0 с маской подсети 255.255.255.0.

Таб. 137 Пример деления на две подсети

IP-АДРЕС/МАСКА ПОДСЕТИ	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 в адресе соответствуют номеру сети (класс “C”).

Чтобы разделить сеть 192.168.1.0 на две разные подсети, один из битов IP-адреса, идентифицирующий хост, нужно использовать в качестве бита, составляющего номер сети. Этот “позаимствованный” бит идентификатора хоста может принимать значения “0” и “1”, давая в итоге две подсети: 192.168.1.0 с маской 255.255.255.128 и 192.168.1.128 с маской 255.255.255.128.

Примечание: На следующих схемах выделенная жирным шрифтом часть последнего октета соответствует битам идентификатора хоста, используемым в качестве битов, идентифицирующих номер сети. Количество подсетей, которые можно создать, определяется числом “позаимствованных” битов идентификатора хоста. Оставшееся (после перераспределения) число битов идентификатора хоста определяет количество хостов, которое может находиться в каждой подсети.

Таб. 138 Подсеть 1

IP-АДРЕС/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ДВОИЧНОЕ ЗНАЧЕНИЕ 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	Адрес первого хоста: 192.168.1.1	
Широковещательный адрес: 192.168.1.127	Адрес последнего хоста: 192.168.1.126	

Таб. 139 Подсеть 2

IP-АДРЕС/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ДВОИЧНОЕ ЗНАЧЕНИЕ 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	Адрес первого хоста: 192.168.1.129	
Широковещательный адрес: 192.168.1.255	Адрес последнего хоста: 192.168.1.254	

Идентификаторы хостов, целиком состоящие из нулей, используются как характеристика самой подсети, поэтому в каждой подсети могут находиться не более 2^7 – 2 или 126 хостов.

192.168.1.0 с маской 255.255.255.128 - это адрес самой подсети, а 192.168.1.127 с маской 255.255.255.128 - это целевой адрес широковещательной рассылки для первой подсети. Таким образом, непосредственным хостам в подсети могут назначаться адреса от 192.168.1.1 до 192.168.1.126 включительно. Аналогично, для второй подсети диапазон адресов хостов - от 192.168.1.129 до 192.168.1.254.

Пример: четыре подсети

В рассмотренном выше примере применялась 25-разрядная маска подсети для деления адресного пространства класса “C” на две подсети. Аналогичным образом пространство адресов класса “C” можно поделить и на четыре подсети; для этого необходимо “позаимствовать” из номера хоста два бита, которые вместе имеют следующие возможные значения: 00, 01, 10 и 11). Маска подсети состоит из 26 битов: 11111111.11111111.11111111.**11**000000 или 255.255.255.192. Каждой подсети выделяется по 6 битов под идентификатор хоста, в общей сложности каждая подсеть может иметь до 2^6-2 или 62 хостов (адреса, целиком состоящие из нулей, идентифицируют саму подсеть, а адрес, целиком состоящий из единиц, используется для широковещательной рассылки в подсети).

Таб. 140 Подсеть 1

IP-АДРЕС/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ДВОИЧНОЕ ЗНАЧЕНИЕ 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	Адрес первого хоста: 192.168.1.1	
Широковещательный адрес: 192.168.1.63	Адрес последнего хоста: 192.168.1.62	

Таб. 141 Подсеть 2

IP-АДРЕС/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ДВОИЧНОЕ ЗНАЧЕНИЕ 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	Адрес первого хоста: 192.168.1.65	
Широковещательный адрес: 192.168.1.127	Адрес последнего хоста: 192.168.1.126	

Таб. 142 Подсеть 3

IP-АДРЕС/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ДВОИЧНОЕ ЗНАЧЕНИЕ 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	Адрес первого хоста: 192.168.1.129	
Широковещательный адрес: 192.168.1.191	Адрес последнего хоста: 192.168.1.190	

Таб. 143 Подсеть 4

IP-АДРЕС/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ДВОИЧНОЕ ЗНАЧЕНИЕ 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	Адрес первого хоста: 192.168.1.193	
Широковещательный адрес: 192.168.1.255	Адрес последнего хоста: 192.168.1.254	

Пример для восьми подсетей

Аналогичным образом можно создать восемь подсетей, используя 27-разрядную маску (000, 001, 010, 011, 100, 101, 110 и 111).

В следующей таблице приведены значения последнего октета для адресов каждой подсети, построенной на базе IP-адреса класса “C”.

Таб. 144 Восемь подсетей

ПОДСЕТЬ	АДРЕС ПОДСЕТИ	ПЕРВЫЙ АДРЕС	ПОСЛЕДНИЙ АДРЕС	ШИРОКОВЕЩАТЕЛЬНЫЙ АДРЕС
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

При планировании подсетей класса “C” можно руководствоваться следующей таблицей.

Таб. 145 Планирование подсетей класса “C”

ЧИСЛО “ЗАИМСТВОВАННЫХ” БИТОВ ИДЕНТИФИКАТОРА ХОСТА	SUBNET MASK	ЧИСЛО ПОДСЕТЕЙ	КОЛИЧЕСТВО ХОСТОВ В ОДНОЙ ПОДСЕТИ
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

Выделение подсетей в сетях классов “A” и “B”

Для адресов класса “A” и “B” маска подсети таким же образом определяет число битов, составляющих номер сети и идентификатор хоста.

В адресе класса “B” для выделения подсетей доступны два октета идентификатора хоста, а в адресе класса “A” – три октета (таб. 133 на стр. 382).

При планировании подсетей класса “B” можно руководствоваться следующей таблицей.

Таб. 146 Планирование подсетей класса “B”

ЧИСЛО “ЗАИМСТВОВАННЫХ” БИТОВ ИДЕНТИФИКАТОРА ХОСТА	SUBNET MASK	ЧИСЛО ПОДСЕТЕЙ	КОЛИЧЕСТВО ХОСТОВ В ОДНОЙ ПОДСЕТИ
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Приложение E
Беспроводные локальные сети

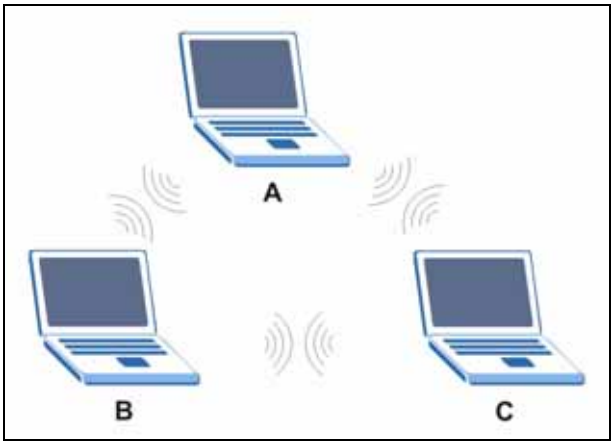
Топологии беспроводных сетей

В этом разделе рассматривается топология ad-hoc и инфраструктурная топология беспроводных сетей.

Конфигурация беспроводной сети ad-hoc

Простейшая конфигурация WLAN – независимая сеть ad-hoc (называемая также прямой или самоорганизующейся сетью), соединяющая несколько компьютеров с беспроводными станциями (A, B, C). Два или несколько беспроводных адаптеров всегда находятся в пределах общего диапазона и могут устанавливать независимую сеть, которая обычно называется специализированной сетью или “независимым базовым набором услуг” (IBSS). На следующей диаграмме показан пример использования беспроводных адаптеров ноутбуками при формировании специализированной беспроводной LAN.

Рис. 213 Обмен данными между равноправными узлами в специализированной сети

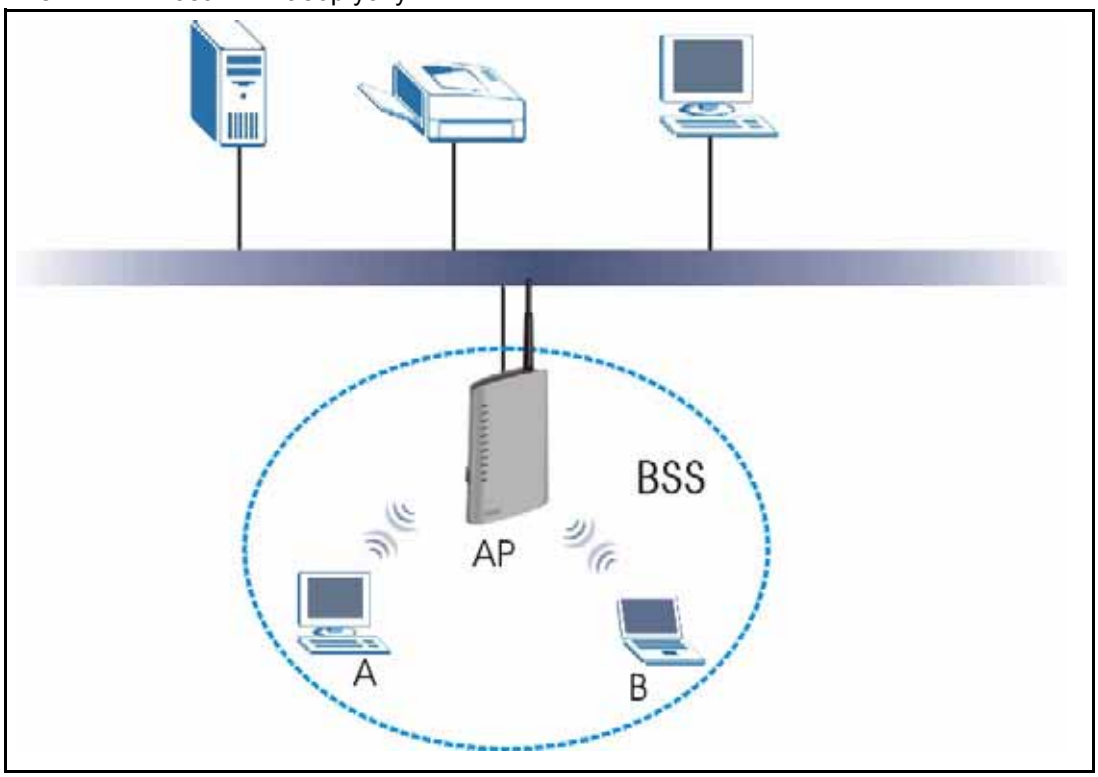


BSS

Набор базовых услуг (BSS) существует, когда весь обмен данными между беспроводными станциями или между беспроводной станцией и клиентом проводной сети проходит через одну точку доступа (AP).

Трафик внутри BSS является трафиком между беспроводными станциями BSS. При включении внутреннего BSS беспроводные станции A и B могут получать доступ к проводной сети и передавать данные друг другу. При выключении внутреннего BSS беспроводные станции A и B могут по-прежнему получать доступ к проводной сети, но не могут обмениваться информацией друг с другом.

Рис. 214 Базовый набор услуг



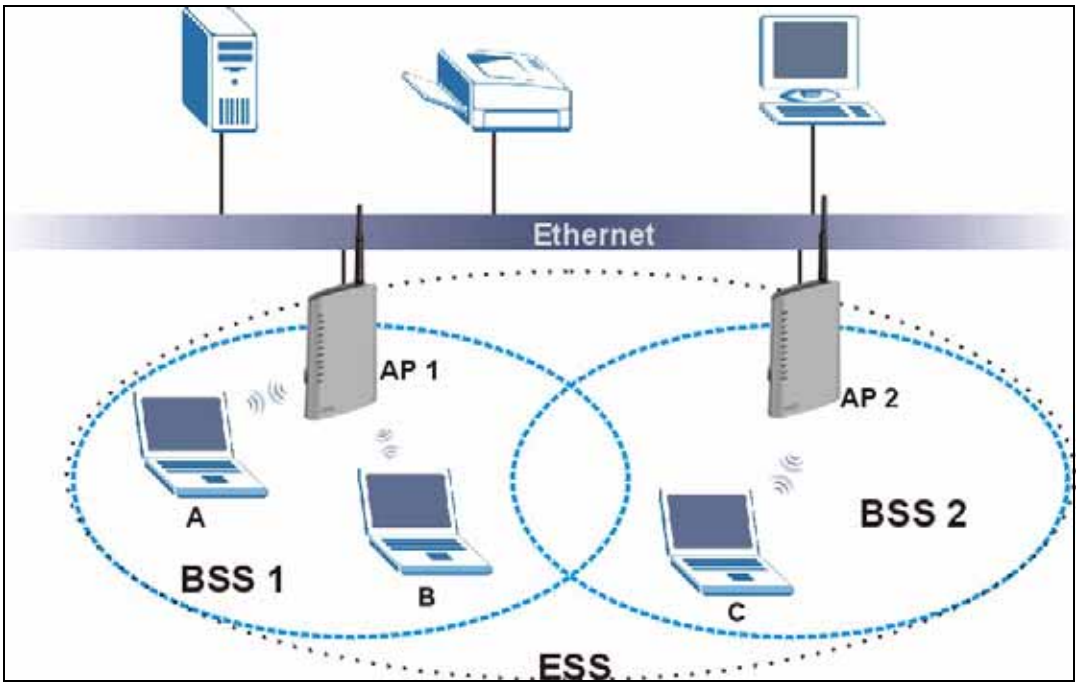
ESS

Расширенный набор услуг (ESS) состоит из серии перекрывающихся BSS, каждый из которых содержит точку доступа, где каждая точка доступа соединена с остальными проводной сетью. Эта проводная сеть между AP называется распределительной системой (DS).

Этот тип топологии беспроводных сетей называется инфраструктурной топологией. Точки доступа не только обеспечивают обмен данными с проводной сетью, но и являются промежуточными звеньями в беспроводной сети при передаче данных ближайшему окружению.

ESSID (ESS IDentification - Идентификация ESS) обеспечивает уникальную идентификацию каждого ESS. Все точки доступа и связанные с ними беспроводные станции в пределах одного и того же ESS должны иметь одну и ту же ESSID для обеспечения коммуникации.

Рис. 215 Инфраструктурная WLAN



Канал

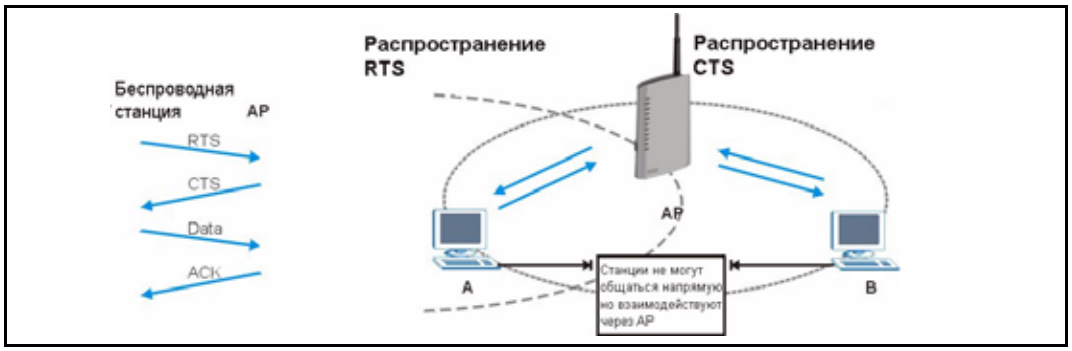
Каналы – это радиочастоты, используемые беспроводными устройствами IEEE 802.11a/b/g. Состав доступных каналов зависит от вашего географического местонахождения. В вашем регионе может быть разрешен некий набор каналов, из которого по соображениям защиты от взаимных помех следует выбрать канал, не используемый ни одной из соседних AP (точек доступа). Взаимные помехи также случаются при наложении радиосигналов от разных от точек доступа; в результате помех производительность сети ухудшается.

Соседние каналы частично перекрываются по частоте, и во избежание помех, вызванных наложением частот, частота вашей точки доступа должна как минимум на пять каналов отличаться от частоты, используемой соседней AP. Например, если в вашем регионе разрешено 11 каналов, а соседняя точка доступа использует канал 1, вам необходимо выбрать канал с номером от 6 до 11.

RTS/CTS

Скрытый узел имеет место, когда две станции находятся в зоне покрытия одной и той же точки доступа, но их собственные зоны покрытия не пересекаются. На следующем рисунке показан скрытый узел. Обе станции (STA) находятся в зоне покрытия точки доступа (AP) или беспроводного межсетевого шлюза, но за пределами своих зон покрытия, в результате чего они не могут “слышать“ друг друга, т.е. не знают, используется ли в данный момент канал. Поэтому они считаются скрытыми по отношению друг к другу.

Рис. 216 RTS/CTS



Когда станция A отправляет данные на AP, она может не знать, что станция B уже использует данный канал. Если эти две станции направляют данные в один и тот же момент времени, могут происходить столкновения, когда оба набора данных достигают AP в одно и то же время, результатом чего становится потеря сообщений обеих станций.

Протокол квитирования **RTS/CTS** предназначен для предотвращения коллизий, вызванных наличием скрытых узлов. **RTS/CTS** регламентирует максимальный размер передаваемого кадра данных, после которого инициируется согласование RTS (запрос на передачу)/CTS (готовность к отправке).

Когда размер кадра превышает заданный порог **RTS/CTS** (от 0 до 2432 байт), станция, отправляющая кадр такого размера, должна предварительно послать сообщение RTS (запрос на передачу) на точку доступа, запрашивая таким образом разрешение. Точка доступа присылает ответное сообщение CTS (готовность к отправке) всем другим станциям в своей зоне покрытия, чтобы они временно приостановили передачу своих данных. Она также резервирует диапазон времени для запрошенной передачи и согласует его с запрашивающей станцией.

Станции могут пересылать кадры меньшего размера, чем порог **RTS/CTS**, напрямую на точку доступа без выполнения согласования RTS/CTS.

RTS/CTS следует настраивать только если в вашей сети могут существовать скрытые узлы, а “стоимость” пересылки крупных кадров превышает накладные расходы, связанные с согласованием RTS/RTS.

Если порог **RTS/CTS** выше порога фрагментации (**Fragmentation Threshold** – см. далее), то согласование RTS/CTS не будет никогда производиться – кадры будут фрагментироваться до того, как их размер достигнет порога **RTS/CTS**.

Примечание: Включение порога RTS вызывает избыточную нагрузку на сеть, которая вместо решения проблемы производительности сети может отрицательно сказаться на пропускной способности.

Порог фрагментации

Порог фрагментации – это максимальный размер фрагмента данных (от 256 до 2432 байт), который может быть передан точкой доступа по беспроводной сети без разбиения на меньшие по размеру кадры.

Большие значения **порога фрагментации** рекомендуются для сетей, не подверженных воздействию помех. Меньший порог рекомендуется применять для сетей с высокой загрузкой или помехами.

Если величина порога фрагментации (**Fragmentation Threshold**) меньше заданного порога **RTS/CTS** (см. выше), то согласование RTS/CTS никогда не будет производиться, поскольку кадры будут фрагментироваться еще до того, как их размер достигнет порога **RTS/CTS**.

Тип преамбулы

Преамбула используется для расчета времени передачи в беспроводной сети. Существует 2 режима преамбулы: **Long (Длинная)** и **Short (Короткая)**

Обработка короткой преамбулы занимает меньше времени, объем служебных сигналов минимизируется, поэтому она должна использоваться в хорошей беспроводной сети, когда все беспроводные станции поддерживают ее.

Выберите **Long**, если сеть “шумная” или нет уверенности в том, какой режим преамбулы поддерживается беспроводными станциями, поскольку все беспроводные адаптеры, совместимые с IEEE 802.11b, должны поддерживать длинную преамбулу. Однако не все беспроводные адаптеры поддерживают короткую преамбулу. Используйте длинную преамбулу, если нет уверенности в том, какой режим преамбулы поддерживается беспроводными адаптерами, чтобы убедиться в интерпретируемости данных, передающихся между точкой доступа и беспроводными станциями, и обеспечить более надежную связь в “шумных” сетях.

Выберите **Dynamic**, чтобы точка доступа автоматически использовала короткую преамбулу, если она поддерживается всеми беспроводными станциями, а в остальных случаях применяла длинную преамбулу.

Примечание: Точка доступа и беспроводные станции ДОЛЖНЫ использовать один и тот же режим преамбулы для установки связи.

Беспроводная сеть стандарта IEEE 802.11g

Стандарт IEEE 802.11g сохраняет полную совместимость со стандартом IEEE 802.11b. Это означает, что адаптер 802.11b может непосредственно взаимодействовать с устройством 802.11g (и наоборот) на скорости 11 Мбит/с или ниже в зависимости от диапазона. Стандарт 802.11g имеет несколько промежуточных скоростей между максимальной и минимальной скоростью передачи данных. Стандарт 802.11g предусматривает следующие скорости передачи данных и типы модуляции:

Таб. 147 IEEE 802.11g

СКОРОСТЬ ПЕРЕДАЧИ ДАННЫХ (МБИТ/С)	МОДУЛЯЦИЯ
1	DBPSK (дифференциальная двухпозиционная фазовая манипуляция)
2	DQPSK (дифференциальная квадратурная фазовая манипуляция)
5.5 / 11	CCK (манипуляция дополнительного кода)
6/9/12/18/24/36/48/54	OFDM (мультиплексирование с ортогональным частотным разделением сигналов)

IEEE 802.1x

В июне 2001 года был создан стандарт IEEE 802.1x, расширяющий возможности IEEE 802.11, что позволило использовать расширенную аутентификацию, а также дополнительные возможности контроля и учёта. Он поддерживается Windows XP и рядом сетевых устройств. Преимущества IEEE 802.1x:

- Идентификация пользователя, обеспечивающая возможность роуминга.
- Поддержка RADIUS (Служба дистанционной аутентификации пользователей по коммутируемым линиям, RFC 2138, 2139) для централизованного управления профилем пользователя и учётными записями на сервере RADIUS.
- Поддержка EAP (расширяемого протокола аутентификации, RFC 2486), обеспечивающая применение дополнительных методов аутентификации без изменения точек доступа или беспроводных станций.

RADIUS

RADIUS – это клиент-серверный протокол для аутентификации, авторизации и учета. Клиентом является точка доступа, а сервером – RADIUS-сервер. Помимо прочего, RADIUS-сервер выполняет следующие задачи:

- Аутентификация

  Определяет идентичность пользователей.

- Авторизация

  Определяет набор сетевых служб, доступных прошедшим аутентификацию пользователям после их подключения к сети.

- Учёт

  Отслеживает активность клиента в сети.

Пользователь RADIUS – простой обмен сообщениями, в которых точка доступа функционирует как ретранслятор сообщений между беспроводной станцией и сервером сети RADIUS.

Типы сообщений RADIUS

Следующие типы сообщений RADIUS пересылаются между точкой доступа и сервером RADIUS для аутентификации пользователя:

- Access-Request (Доступ - запрос)

  Отправляется точкой доступа, запрашивающей аутентификацию.

- Access-Reject (Доступ – запрет)

  Отправляется сервером RADIUS, запрещающим доступ

- Access-Accept (Доступ—принятие)

  Отправляется сервером RADIUS для разрешения доступа

- Access- Challenge (Доступ – Вызов)

  Отправляется сервером RADIUS для получения дополнительной информации для разрешения доступа. Точка доступа посылает надлежащий ответ от пользователя и затем – еще одно сообщение Access-Request (Доступ – запрос).

Следующие типы сообщений RADIUS пересылаются между точкой доступа и сервером RADIUS для учета пользователя:

- Accounting-Request (Учет-запрос)

  Отправляется точкой доступа, запрашивающей учет.

- Accounting- Response (Учет-ответ)

  Отправляется сервером RADIUS для указания на то, что он запустил или прекратил учет.

Чтобы гарантировать безопасность сети, точка доступа и сервер RADIUS применяют совместно используемый секретный ключ – пароль, известный обеим сторонам. Этот ключ не пересылается по сети. В дополнение к совместно используемому ключу обмениваемая информация о пароле также зашифрована, чтобы защитить сеть от несанкционированного доступа.

Типы аутентификации

В этом приложении даётся объяснение нескольких распространенных типов аутентификации: **EAP-MD5**, **EAP-TLS**, **EAP-TTLS**, **PEAP** и **LEAP**.

Тип используемой аутентификации зависит от сервера RADIUS или точки доступа. Обращайтесь к своему администратору сети для получения дополнительной информации.

EAP-MD5 (алгоритм 5 представления сообщения в краткой форме)

Аутентификация MD5 – простейший однонаправленный метод аутентификации. Сервер аутентификации отправляет запрос на беспроводную станцию. Беспроводная станция “доказывает”, что знает пароль, шифруя пароль вместе с вызовом, и отправляет информацию обратно. Пароль в виде простого текста не отправляется.

Однако аутентификация MD5 имеет слабые стороны. Поскольку сервер аутентификации нуждается в получении паролей в виде простого текста, пароли необходимо сохранять. Поэтому к файлу с паролем может получить доступ не только сервер аутентификации. Кроме того, можно имитировать сервер аутентификации, поскольку метод аутентификации MD5 не выполняет взаимную аутентификацию. Наконец, метод аутентификации MD5 не поддерживает шифрование данных с использованием динамического ключа сессии. Необходимо настраивать ключи шифрования WEP для шифрования данных.

EAP-TLS (защита транспортного уровня)

При использовании EAP-TLS серверу и беспроводным станциям для взаимной аутентификации требуются цифровые сертификаты. Сервер предоставляет сертификат клиенту. После проверки идентичности сервера клиент отправляет серверу другой сертификат. Обмен сертификатами выполняется открыто перед созданием защищённого канала. Из-за этого идентичность пользователя может пострадать от пассивных атак. Цифровой сертификат – это электронная карта идентификации, подтверждающая идентичность отправителя. Однако для применения EAP-TLS необходим Центр сертификации (CA) для обработки сертификатов, что приводит к повышению издержек управления.

EAP-TTLS (туннелированная служба транспортного уровня)

EAP-TTLS – расширение аутентификации EAP-TLS, в котором используются сертификаты только для аутентификации на стороне сервера при установке защищённого соединения. Затем выполняется аутентификация клиента посредством отправки имени пользователя и пароля через защищённое соединение, что позволяет защитить идентичность клиента. Для аутентификации пользователя EAP-TTLS поддерживает методы EAP и обычные методы аутентификации, такие как PAP, CHAP, MS-CHAP и MS-CHAP v2.

PEAP (защищенный EAP)

Как и в EAP-TTLS, аутентификация сертификата на стороне сервера используется для установки защищённого соединения, затем используются методы передачи простого имени пользователя и пароля через защищённое соединение для аутентификации клиентов, что позволяет скрыть идентичность клиента. Однако для аутентификации клиента PEAP поддерживаются только методы EAP, такие как EAP-MD5, EAP-MSCHAPv2 и EAP-GTC (универсальная карта-метка EAP). EAP-GTC применяется только Cisco.

LEAP

LEAP (легковесный расширяемый протокол аутентификации) – это реализация IEEE 802.1x, разработанная компанией Cisco.

Динамический обмен ключами WEP

Точка доступа применяет уникальный ключ, генерируемый сервером RADIUS. Действие этого ключа прекращается при истечении периода неактивности беспроводного соединения, разрыве сеанса или истечении времени аутентификации. При каждой повторной аутентификации генерируется новый ключ WEP.

Если эта функция включена, настраивать ключ для шифрования по умолчанию на экране Wireless не требуется. Ключи можно по-прежнему настраивать и хранить на этом экране, но они не будут использоваться, пока включен режим динамического обмена ключами WEP.

Примечание: EAP-MD5 не может применяться с динамическим обменом ключами

Для повышения безопасности в методах аутентификации, построенных на сертификатах (EAP-TLS, EAP-TTLS and PEAP), для шифрования используются динамические ключи. Такие методы часто применяются в корпоративной среде, но для общего пользования более практичным будет простое сочетание имени пользователя и пароля. В следующей таблице приведено сравнение разных типов аутентификации.

Таб. 148 Сравнение типов аутентификации EAP

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Взаимная аутентификация	Нет	Да	Да	Да	Да
Сертификат – клиент	Нет	Да	Опционально	Опционально	Нет
Сертификат – сервер	Нет	Да	Да	Да	Нет
Динамический обмен ключами	Нет	Да	Да	Да	Да
Целостность мандатов	Нет	Строгая	Строгая	Строгая	Умеренная
Сложность внедрения	Легкая	Трудная	Умеренная	Умеренная	Умеренная
Защита идентичности клиента	Нет	Нет	Да	Да	Нет

WPA

Аутентификация пользователя

В WPA применяется IEEE 802.1x и расширяемый протокол аутентификации (EAP) для аутентификации беспроводных станций с использованием внешней БД RADIUS.

Шифрование

WPA позволяет улучшить шифрование данных посредством использования протокола целостности временного ключа (TKIP), проверки целостности сообщения (MIC) и IEEE 802.1x.

В протоколе TKIP используются 128-битные ключи, генерируемые динамически и распределяемые сервером аутентификации. Он включает функцию смешивания ключей по пакетам, проверку целостности сообщения (MIC) под названием Michael, расширяемый вектор инициализации (IV) с правилами упорядочения и механизм повторного назначения ключа.

TKIP регулярно изменяет и меняет ключи шифрования, чтобы один и тот же ключ шифрования никогда не использовался дважды.

Сервер RADIUS распределяет ключ Pairwise Master Key (PMK) (“парный мастер-ключ”) в точку доступа, которая затем устанавливает иерархию ключей и систему управления с использованием парного ключа для динамического генерирования уникальных ключей шифрования данных для шифрования каждого пакета данных, которые передаются по беспроводной сети между AP и беспроводным клиентами. Все это происходит автоматически в фоновом режиме.

Алгоритм AES (усовершенствованный стандарт шифрования) также использует секретный ключ. В данной реализации AES к каждому 128-битному блоку данных применяется 128-битный ключ.

Проверка целостности сообщения (MIC) разработана для предотвращения перехвата пакетов данных, изменения и их повторной отправки злоумышленником. MIC обеспечивает выполнение строгой математической функции, благодаря которой получатель и отправитель вычисляют и сравнивают MIC. Если они не совпадают, делается вывод, что данные сфальсифицированы, и пакет отбрасывается.

Благодаря созданию уникальных ключей для шифрования данных для каждого пакета данных и созданию механизма проверки целостности (MIC) TKIP затрудняет дешифровку данных в сети Wi-Fi по сравнению с WEP, усложняя злоумышленнику задачу проникновения в сеть.

Механизмы шифрования, используемые для WPA и WPA-PSK, одинаковы. Единственное различие между ними состоит в том, что в WPA-PSK используется простой общий пароль вместо мандатов конкретных пользователей. Подход, состоящий в использовании общего пароля, делает WPA-PSK восприимчивым к атакам и разгадыванию пароля методом “грубой силы”, но все же является лучшим выбором по сравнению с WEP, поскольку в нем используется более легкий в использовании, согласованный, отдельный буквенно-цифровой пароль.

Сводка параметров безопасности

Обращайтесь к этой таблице для получения информации о том, какие параметры безопасности нужно дополнительно настроить для каждого метода аутентификации/ типа протокола управления ключом. Фильтры MAC-адреса не зависят от того, как настроены эти параметры безопасности.

Таб. 149 Реляционная матрица безопасности беспроводного соединения

МЕТОД АУТЕНТИФИКАЦИИ/ ПРОТОКОЛ УПРАВЛЕНИЯ КЛЮЧАМИ	МЕТОД ШИФРОВАНИЯ	ВВОД КЛЮЧА ВРУЧНУЮ	ПРОТОКОЛ IEEE 802.1X
Открытый	Отсутствует	Нет	Нет

Таб. 149 Реляционная матрица безопасности беспроводного соединения (продолжение)

МЕТОД АУТЕНТИФИКАЦИИ/ ПРОТОКОЛ УПРАВЛЕНИЯ КЛЮЧАМИ	МЕТОД ШИФРОВАНИЯ	ВВОД КЛЮЧА ВРУЧНУЮ	ПРОТОКОЛ IEEE 802.1X
Открытый	WEP	Нет	Включен с динамическим ключом WEP
		Да	Включен без динамического ключа WEP
		Да	Отключен
Совместное использование	WEP	Нет	Включен с динамическим ключом WEP
		Да	Включен без динамического ключа WEP
		Да	Отключен
WPA	WEP	Нет	Да
WPA	TKIP	Нет	Да
WPA-PSK	WEP	Да	Да
WPA-PSK	TKIP	Да	Да

Приложение F
Сетевые службы

В следующей таблице перечислены часто используемые сетевые службы и соответствующие им типы протоколов и номера портов.

- **Наименование**: Это краткое название службы. Можно использовать это название или указать другое.
- **Протокол**: Это тип протокола IP, используемого данной службой. Если в этом поле указано **TCP/UDP**, то для данной службы на одном номере порта используются одновременно TCP и UDP. Если в качестве протокола указан **ПОЛЬЗОВАТЕЛЬСКИЙ**, то в графе **Порт(ы)** указан номер протокола IP, а не номер порта.
- **Порт(ы)**: Значение зависит от содержимого поля **Протокол**.
    - Если в графе **Протокол** указан **TCP**, **UDP** или **TCP/UDP**, здесь приводится номер порта IP.
    - Если в графе **Протокол** указан **ПОЛЬЗОВАТЕЛЬСКИЙ**, здесь приводится номер протокола IP.
- **Описание**: Ниже приведено краткое описание применений каждой службы и ситуаций, в которых она используется.

Таб. 150 Примеры служб

НАЗВАНИЕ	ПРОТОКОЛ	ПОРТ(Ы)	ОПИСАНИЕ
AH (IPSEC_TUNNEL)	ПОЛЬЗОВАТЕЛЬСКИЙ	51	Эта служба используется протоколом туннелирования IPSEC AH (Authentication Header – заголовок аутентификации).
AIM	TCP	5190	Служба мгновенного обмена сообщениями America Online.
AUTH	TCP	113	Протокол аутентификации, используемый некоторыми серверами.
BGP	TCP	179	Протокол для граничных маршрутизаторов.
BOOTP_CLIENT	UDP	68	DHCP-клиент.
BOOTP_SERVER	UDP	67	DHCP-сервер.
CU-SEEME	TCP/UDP TCP/UDP	7648 24032	Популярное решение для видеоконференций, разработанное White Pines Software.
DNS	TCP/UDP	53	Сервер доменных имен. Служба, которая ставит в соответствие буквенным адресам (например, www.zyxel.com) IP-адреса.

Таб. 150 Примеры служб (продолжение)

НАЗВАНИЕ	ПРОТОКОЛ	ПОРТ(Ы)	ОПИСАНИЕ
ESP (IPSEC_TUNNEL)	ПОЛЬЗОВАТЕЛЬСКИЙ	50	Эта служба используется протоколом IPSEC ESP (Encapsulation Security Protocol – протокол защищенного сокрытия содержания).
FINGER	TCP	79	Finger – команда, позволяющая проверять состояние пользователя в системах UNIX или Интернете.
FTP	TCP TCP	20 21	Протокол передачи файлов используется для пересылки файлов, в особенности – больших объемов данных, которые невозможно передать по электронной почте.
H.323	TCP	1720	Этот протокол используется программой NetMeeting.
HTTP	TCP	80	Протокол передачи гипертекста – клиент-серверный протокол для “Всемирной паутины”.
HTTPS	TCP	443	HTTPS - защищенный сеанс HTTP, часто используемый в электронной коммерции.
ICMP	ПОЛЬЗОВАТЕЛЬСКИЙ	1	Межсетевой протокол контрольных сообщений часто используется в диагностических целях.
ICQ	UDP	4000	Это популярная программа для общения в Интернете.
IGMP (MULTICAST)	ПОЛЬЗОВАТЕЛЬСКИЙ	2	Протокол Internet Group Multicast Protocol используется при отправке пакетов отдельной группе хостов.
IKE	UDP	500	Для распространения ключей и управления ключами используется алгоритм IKE (Internet Key Exchange – обмен ключами в Интернете).
IMAP4	TCP	143	Протокол доступа к сообщениям в Интернете используется для электронной почты.
IMAP4S	TCP	993	Это более защищенная версия IMAP4, работающая по SSL.
IRC	TCP/UDP	6667	Это популярная служба для общения (чата) в Интернете.
MSN Messenger	TCP	1863	Служба мгновенного обмена сообщениями Microsoft Network использует этот протокол.
NetBIOS	TCP/UDP TCP/UDP TCP/UDP TCP/UDP	137 138 139 445	Сетевая базовая система ввода-вывода используется для обмена данными между компьютерами в локальной сети.
NEW-ICQ	TCP	5190	Программа для общения в Интернете.
NEWS	TCP	144	Протокол для групп новостей.

Таб. 150 Примеры служб (продолжение)

НАЗВАНИЕ	ПРОТОКОЛ	ПОРТ(Ы)	ОПИСАНИЕ
NFS	UDP	2049	Сетевая файловая система (NFS) – распределенная клиент-серверная файловая система , которая обеспечивает прозрачный совместный доступ к файлам в сетевых средах.
NNTP	TCP	119	Сетевой протокол передачи новостей – механизм доставки сообщений для групп новостей USENET.
PING	ПОЛЬЗОВАТЕЛЬСКИЙ	1	Пакетный межсетевой объединитель (Packet INternet Groper) – это протокол отправки эхозапросов ICMP для проверки доступности удаленного хоста.
POP3	TCP	110	Почтовый протокол версии 3 позволяет клиентскому компьютеру получать электронную почту с сервера POP3 по временному соединению (посредством TCP/IP или другого протокола).
POP3S	TCP	995	Это более защищенная версия POP3, работающая по SSL.
PPTP	TCP	1723	Двухточечный протокол туннелирования обеспечивает защищенную передачу данных по сетям общего пользования. Эта служба соответствует управляющему каналу.
PPTP_TUNNEL (GRE)	ПОЛЬЗОВАТЕЛЬСКИЙ	47	Двухточечный протокол туннелирования обеспечивает защищенную передачу данных по сетям общего пользования. Эта служба соответствует каналу данных.
RCMD	TCP	512	Служба удаленного выполнения команд.
REAL_AUDIO	TCP	7070	Протокол поточной передачи аудиоданных, обеспечивающий передачу звука в реальном времени по WWW.
REXEC	TCP	514	Демон удаленного выполнения команд.
RLOGIN	TCP	513	Служба удаленного входа в систему.
ROADRUNNER	TCP/UDP	1026	Это поставщик услуг Интернета, предлагающий услуги преимущественно в секторе кабельных модемов.
RTELNET	TCP	107	Удаленный Telnet.
RTSP	TCP/UDP	554	Протокол поточного вещания в реальном времени (RTSP) – это служба дистанционного управления мультимедиа-вещанием в Интернете.
SFTP	TCP	115	Простой протокол пересылки файлов – старый механизм передачи файлов между компьютерами.
SMTP	TCP	25	Простой протокол передачи почты – стандарт обмена почтовыми сообщениями в Интернете. SMTP позволяет передавать сообщения от одного почтового сервера к другому.

Таб. 150 Примеры служб (продолжение)

НАЗВАНИЕ	ПРОТОКОЛ	ПОРТ(Ы)	ОПИСАНИЕ
SMTPS	TCP	465	Это более защищенная версия SMTP, работающая по SSL.
SNMP	TCP/UDP	161	Упрощённый протокол управления сетью.
SNMP-TRAPS	TCP/UDP	162	Прерывания, используемые SNMP (RFC:1215).
SQL-NET	TCP	1521	Язык структурированных запросов (SQL) – интерфейс для доступа к данным в различных СУБД, включая СУБД на мейнфреймах, системах среднего уровня, UNIX-системах и сетевых серверах.
SSDP	UDP	1900	Простой протокол обнаружения сетевых служб поддерживает универсальную систему “включай и работай” (UPnP).
SSH	TCP/UDP	22	Программа для защищенного удаленного входа в системную оболочку.
STRM WORKS	UDP	1558	Протокол Stream Works.
SYSLOG	UDP	514	SYSLOG позволяет оставлять сообщения в файле журнала на UNIX-сервере.
TACACS	UDP	49	Протокол хоста регистрации (Terminal Access Controller Access Control System – система управления доступом для контроля доступа к оконечным узлам).
TELNET	TCP	23	Telnet – протокол регистрации в системе и эмуляции терминала, распространенный в Интернете и в среде UNIX. Он предназначен для работы по сетям TCP/IP. Его основное назначение – обеспечить дистанционный доступ пользователей к хостам.
TFTP	UDP	69	TFTP (упрощенный протокол пересылки файлов) – протокол передачи файлов в Интернете, подобный FTP, но использующий UDP (протокол пользовательских датаграмм) вместо TCP (протокол управления передачей).
VDOLIVE	TCP UDP	7000 ПОЛЬ-ЗОВА-ТЕЛЬ-СКИЙ	Решение для проведения видеоконференций. Номер порта UDP задается в приложении.

Приложение G
Команды для управления межсетевым экраном

Группа команд Sys Firewall

Ниже описаны команды для управления межсетевым экраном. Подробное описание структуры команд см. в приложении об интерпретаторе команд. Перед каждой из этих команд необходимо набирать `sys firewall`. Например, чтобы включить межсетевой экран, следует ввести `sys firewall active yes`.

Таб. 151 Группа команд Sys Firewall

Команда		Описание
`acl`		
	`disp`	Выводит содержание всех ACL, либо содержание конкретного ACL с указанным номером набора и номером правила.
`active`	`<yes|no>`	Активирует или деактивирует межсетевой экран, включая или отключая его.
`cnt`		
	`disp`	Выводит типы журналов межсетевого экрана и число отметок в журналах.
	`clear`	Сбрасывает счетчики в журналах межсетевого экрана.
`pktdump`		Выводит последние 64 байта пакетов, запрещенных межсетевым экраном.
`dynamicrule`	`display`	Выводит список динамических правил межсетевого экрана.
`tcprst`		
	`rst`	Включает или отключает отправку уведомления о разрыве TCP-сеанса.
	`rst113`	Включает или отключает отправку уведомления о разрыве TCP-сеанса для порта 113.
	`display`	Выводит настройки уведомлений о разрыве TCP-сеанса.
`icmp`		Это правило не используется.
`dos`		
	`smtp`	Включает или отключает защиту от DoS-атак на SMTP-порт.
	`display`	Выводит текущую настройку защиты от DoS-атак на SMTP-порт.
	`ignore`	Разрешает/запрещает межсетевому экрану игнорировать DoS-атаки в LAN/WAN.
`ignore`		

Таб. 151 Группа команд Sys Firewall

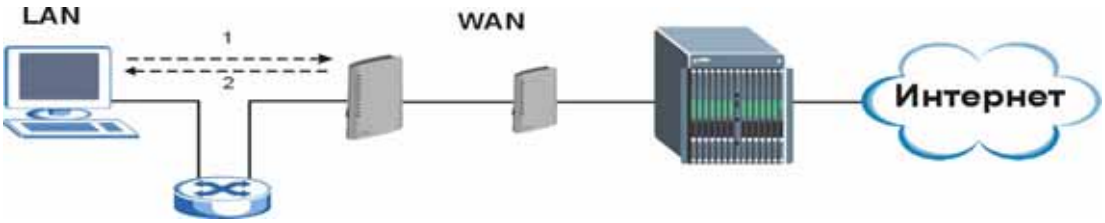
Команда		Описание
	`dos`	Разрешает/запрещает межсетевому экрану игнорировать DoS-атаки в LAN/WAN.
	`triangle`	Разрешает/запрещает межсетевому экрану игнорировать пакеты, проходящие по треугольному маршруту в LAN/WAN.

Приложение H
Треугольный маршрут

Анализ идеальной топологии

Когда активирован межсетевой экран, P-2602 выступает в качестве шлюза между локальной сетью и Интернетом. В идеальной топологии сети весь входящий и исходящий сетевой трафик проходит через P-2602, и ваша локальная сеть защищена от атак.

Рис. 217 Идеальная топология



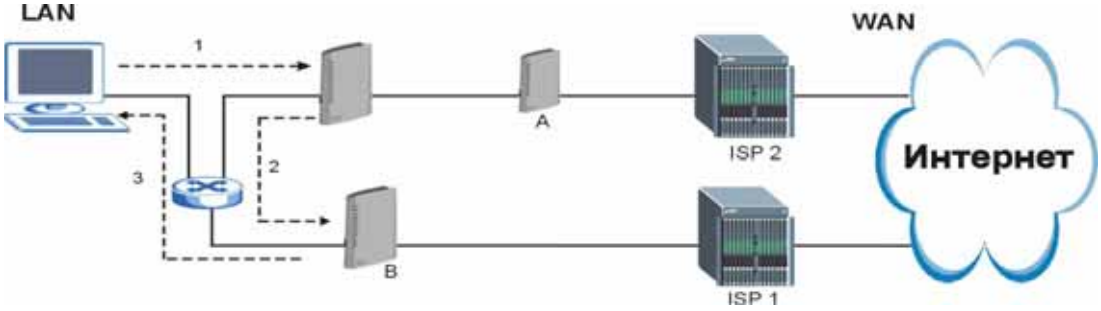
Проблема треугольного маршрута

Маршрут – это путь отправки или приема пакетов данных между двумя Ethernet-устройствами. Некоторые компании имеют несколько альтернативных маршрутов к одному или нескольким поставщикам услуг Интернета. Если локальная сеть (LAN) и поставщик(и) услуг Интернета (ISP) находятся в одной и той же подсети, может возникнуть проблема “треугольного маршрута”, природу которой иллюстрирует следующая ситуация.

1. Компьютер в сети LAN устанавливает соединение, посылая пакет SYN на принимающий сервер в сети WAN.
2. P-2602 маршрутизирует пакет SYN через шлюз **B** в локальной сети LAN по направлению к WAN.
3. Ответ из WAN поступает напрямую на компьютер в LAN, минуя P-2602.

В результате P-2602 сбрасывает соединение как неподтвержденное.

Рис. 218 Проблема треугольного маршрута



Решения проблемы треугольного маршрута

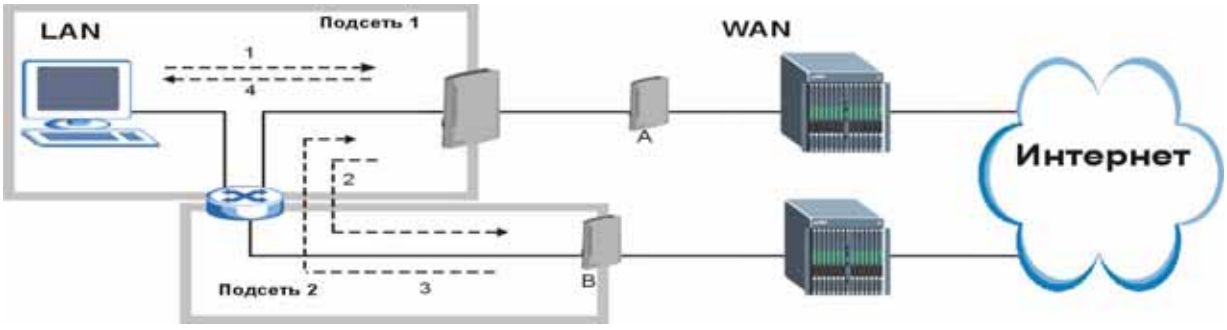
Ниже рассмотрены два возможных решения проблемы треугольного маршрута.

Совмещение IP-адресов

Совмещение IP-адресов (IP aliasing) позволяет разделить физическую сеть на логические секции через один и тот же интерфейс Ethernet. P-2602 поддерживает до трех логических интерфейсов LAN, при этом P-2602 выступает шлюзом для каждой логической сети. Разнеся вашу локальную сеть и шлюз **B** по различным подсетям, вы заставите весь возвращающийся сетевой трафик проходить через P-2602 в локальную сеть. Этот сценарий можно проиллюстрировать следующим образом.

1. Компьютер в сети LAN устанавливает соединение, посылая пакет SYN на принимающий сервер в сети WAN.
2. P-2602 маршрутизирует пакет на шлюз B, находящийся в подсети 2.
3. Ответ из WAN проходит через P-2602 к компьютеру, находящемуся в подсети 1 локальной сети.

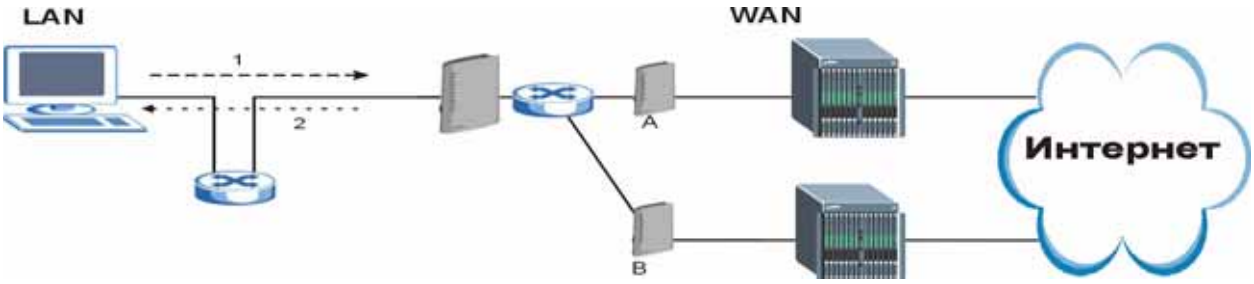
Рис. 219 Совмещение IP-адресов



Шлюзы на стороне WAN

Второе решение проблемы треугольного маршрута – разместить все сетевые шлюзы на стороне WAN, как показано на следующем рисунке. При этом весь поступающий сетевой трафик проходит через P-2602 в вашу локальную сеть. Благодаря этому обеспечивается защита локальной сети.

Рис. 220 Шлюзы на стороне WAN



Приложение I
Формат журналов

В этом приложении приведены расшифровки сообщений в журналах.

Таб. 152 Журналы обслуживания системы

СООБЩЕНИЕ	ОПИСАНИЕ
`Time calibration is successful`	Маршрутизатор скорректировал время по показаниям сервера точного времени.
`Time calibration failed`	Маршрутизатор не может получить информацию с сервера точного времени.
`WAN interface gets IP: %s`	Интерфейс WAN получил новый IP-адрес от серверов DHCP, PPPoE, PPTP или сервера коммутируемого доступа.
`DHCP client IP expired`	Истек срок действия IP-адреса DHCP-клиента.
`DHCP server assigns %s`	DHCP-сервер присвоил IP-адрес клиенту.
`Successful WEB login`	Пользователь вошел в интерфейс веб-конфигуратора маршрутизатора.
`WEB login failed`	Пользователю не удалось войти в интерфейс веб-конфигуратора маршрутизатора.
`Successful TELNET login`	Пользователь вошел в маршрутизатор через telnet.
`TELNET login failed`	Пользователю не удалось войти в маршрутизатор через telnet.
`Successful FTP login`	Пользователь вошел в маршрутизатор через tftp.
`FTP login failed`	Пользователю не удалось войти в маршрутизатор через tftp.
`NAT Session Table is Full!`	Превышено максимальное число записей в таблице сеансов NAT, таблица переполнена.
`Starting Connectivity Monitor`	Идет запуск сетевого монитора.
`Time initialized by Daytime Server`	Маршрутизатор получил дату и время с сервера Daytime.
`Time initialized by Time server`	Маршрутизатор получил дату и время с сервера точного времени.
`Time initialized by NTP server`	Маршрутизатор получил дату и время с сервера NTP.
`Connect to Daytime server fail`	Маршрутизатор не смог подключиться к серверу Daytime.
`Connect to Time server fail`	Маршрутизатор не смог подключиться к серверу точного времени.
`Connect to NTP server fail`	Маршрутизатор не смог подключиться к серверу NTP.
`Too large ICMP packet has been dropped`	Маршрутизатор удалил ICMP-пакет недопустимо большого размера.

Таб. 152 Журналы обслуживания системы (продолжение)

СООБЩЕНИЕ	ОПИСАНИЕ
`Configuration Change: PC = 0x%x, Task ID = 0x%x`	Маршрутизатор сохраняет изменения в настройках.
`Successful SSH login`	Пользователь вошел в маршрутизатор через встроенный SSH-сервер.
`SSH login failed`	Пользователю не удалось войти в маршрутизатор через встроенный SSH-сервер.
`Successful HTTPS login`	Пользователь вошел в веб-конфигуратор маршрутизатора по протоколу HTTPS.
`HTTPS login failed`	Пользователю не удалось войти в веб-конфигуратор маршрутизатора по протоколу HTTPS.

Таб. 153 Системные журналы ошибок

СООБЩЕНИЕ	ОПИСАНИЕ
`%s exceeds the max. number of session per host!`	При очередной попытке создания сеанса NAT было превышено ограничение на емкость таблицы сеансов NAT для конкретного хоста.
`setNetBIOSFilter: calloc error`	Маршрутизатор не смог выделить память для параметров настройки фильтра NetBIOS.
`readNetBIOSFilter: calloc error`	Маршрутизатор не смог выделить память для параметров настройки фильтра NetBIOS.
`WAN connection is down.`	Соединение с WAN отсутствует. Вы не можете получить доступ к сети через этот интерфейс.

Таб. 154 Журналы контроля доступа

СООБЩЕНИЕ	ОПИСАНИЕ
`Firewall default policy: [ TCP | UDP | IGMP | ESP | GRE | OSPF ] <Направление движения пакетов>`	Обращение по TCP/UDP/IGMP/ESP/GRE/OSPF совпало с условиями политики по умолчанию и было заблокировано/пропущено в соответствии с политикой по умолчанию.
`Firewall rule [NOT] match:[ TCP | UDP | IGMP | ESP | GRE | OSPF ] <Направление движения пакетов>, <правило:%d>`	Обращение по TCP/UDP/IGMP/ESP/GRE/OSPF совпало (или не совпало) с настроенным правилом межсетевого экрана (с указанным номером) и было заблокировано/пропущено в соответствии с правилом.
`Triangle route packet forwarded: [ TCP | UDP | IGMP | ESP | GRE | OSPF ]`	Межсетевой экран пропустил сеанс по треугольному маршруту.

Таб. 154 Журналы контроля доступа (продолжение)

СООБЩЕНИЕ	ОПИСАНИЕ
`Packet without a NAT table entry blocked: [ TCP | UDP | IGMP | ESP | GRE | OSPF ]`	Маршрутизатор заблокировал пакет, для которого отсутствует соответствующая запись в таблице NAT.
`Router sent blocked web site message: TCP`	Маршрутизатор отправил сообщение, уведомляющее пользователя о том, что в маршрутизаторе заблокирирован доступ к запрошенному пользователем веб-сайту.

Таб. 155 Журналы пакетов сброса TCP

СООБЩЕНИЕ	ОПИСАНИЕ
`Under SYN flood attack, sent TCP RST`	Маршрутизатор отправил пакет сброса TCP, поскольку хост подвергался атаке “SYN Flood” (число частично открытых сеансов TCP указывается для хоста адресата.)
`Exceed TCP MAX incomplete, sent TCP RST`	Маршрутизатор отправил пакет сброса TCP, поскольку число частично открытых сеансов TCP превысило заданный пользователем порог (число частично открытых сеансов TCP указывается для хоста адресата.) Примечание: См. параметр **TCP Maximum Incomplete** на экране **Firewall Attack Alerts**.
`Peer TCP state out of order, sent TCP RST`	Маршрутизатор отправил пакет сброса TCP, обнаружив нарушение порядка состояний TCP-соединения. Примечание: при проверке состояния TCP-соединений межсетевой экран руководствуется схемой на рис. 6 в документе RFC793.
`Firewall session time out, sent TCP RST`	Маршрутизатор отправил пакет сброса TCP по истечении длительности динамического сеанса межсетевого экрана. По умолчанию принята следующая продолжительность сеансов (в секундах): неактивность ICMP: 60, неактивность UDP – 60, неактивность TCP-соединения (трехэтапное согласование) – 30, время ожидания TCP FIN – 60, неактивность (установленного) TCP-соединения – 3600
`Exceed MAX incomplete, sent TCP RST`	Маршрутизатор отправил пакет сброса TCP, поскольку число частично открытых сеансов (TCP и UDP) превысило заданный пользователем порог (учитывается суммарное число частично открытых сеансов TCP и UDP через межсетевой экран.) Примечание: Если для числа частично открытых сеансов выполняется условие (TCP + UDP) > “Maximum Incomplete High”, маршрутизатор отправляет пакеты TCP RST для TCP-сеансов и удаляет TOS (динамические сеансы межсетевого экрана), пока число частично открытых сеансов не станет < “Maximum Incomplete Low”.
`Access block, sent TCP RST`	Маршрутизатор отправляет пакет TCP RST и оставляет эту запись в журнале, если вы включили механизм сброса TCP-соединений в межсетевом экране (через команду интерфейса КС: “sys firewall tcprst”).

Таб. 156 Журналы фильтрации пакетов

СООБЩЕНИЕ	ОПИСАНИЕ
`[ TCP | UDP | ICMP | IGMP | Generic ] packet filter matched (set: %d, rule: %d)`	Попытка доступа совпала с настроенным правилом фильтра (набор и номер правила указаны в скобках) и была заблокирована или разрешена согласно правилу.

Расшифровку типов и кодов см. в таб. 165 на стр. 420.

Таб. 157 Журналы ICMP

СООБЩЕНИЕ	ОПИСАНИЕ
`Firewall default policy: ICMP <направление движения пакетов>, <тип:%d>, <код:%d>`	Обращение по ICMP совпало с условиями политики по умолчанию и было заблокировано/пропущено в соответствии с политикой по умолчанию.
`Firewall rule [NOT] match: ICMP <направление движения пакетов>, <правило:%d>, <тип:%d>, <код:%d>`	Обращение по ICMP совпало (или не совпало) с настроенным правилом межсетевого экрана (с указанным номером) и было заблокировано/ пропущено в соответствии с правилом.
`Triangle route packet forwarded: ICMP`	Межсетевой экран пропустил сеанс по треугольному маршруту.
`Packet without a NAT table entry blocked: ICMP`	Маршрутизатор заблокировал пакет, для которого отсутствует соответствующая запись в таблице NAT.
`Unsupported/out-of-order ICMP: ICMP`	Межсетевой экран не поддерживает данный вид пакетов ICMP или нарушен порядок следования пакетов ICMP.
`Router reply ICMP packet: ICMP`	Маршрутизатор отослал ответный ICMP-пакет отправителю.

Таб. 158 Журналы вызовов (CDR)

СООБЩЕНИЕ	ОПИСАНИЕ
`board %d line %d channel %d, call %d, %s C01 Outgoing Call dev=%x ch=%x %s`	Маршрутизатор получил требования для подготовки вызова. “call” – учетный (порядковый) номер вызова. “dev” – тип устройства (3 – коммутируемый доступ, 6 – PPPoE, 10 – PPTP). “channel” или “ch” – идентификатор канала вызова. Например, запись “board 0 line 0 channel 0, call 3, C01 Outgoing Call dev=6 ch=0” означает, что маршрутизатор три раза вызывал сервер PPPoE.
`board %d line %d channel %d, call %d, %s C02 OutCall Connected %d %s`	Установлено соединение при вызове посредством PPPoE, PPTP или коммутируемого доступа.
`board %d line %d channel %d, call %d, %s C02 Call Terminated`	Вызов PPPoE, PPTP или коммутируемого доступа разъединен.

Таб. 159 PPP Logs

СООБЩЕНИЕ	ОПИСАНИЕ
`ppp:LCP Starting`	Начат этап PPP-соединения с использованием протокола управления соединением (LCP).
`ppp:LCP Opening`	Открывается этап PPP-соединения с использованием протокола управления соединением (LCP).
`ppp:CHAP Opening`	Открывается этап PPP-соединения с использованием протокола аутентификации с предварительным согласованием вызова (CHAP).
`ppp:IPCP Starting`	Начат этап PPP-соединения с использованием протокола управления протоколом IP (IPCP).
`ppp:IPCP Opening`	Открывается этап PPP-соединения с использованием протокола управления протоколом IP (IPCP).
`ppp:LCP Closing`	Закрывается этап PPP-соединения с использованием протокола управления соединением (LCP).
`ppp:IPCP Closing`	Закрывается этап PPP-соединения с использованием протокола управления протоколом IP (IPCP).

Таб. 160 Журналы UPnP

СООБЩЕНИЕ	ОПИСАНИЕ
`UPnP pass through Firewall`	Пакетам UPnP разрешено проходить через межсетевой экран.

Таб. 161 Журналы фильтрации содержания

СООБЩЕНИЕ	ОПИСАНИЕ
`%s: block keyword`	Содержание запрошенной веб-страницы совпало с ключевым словом, заданным пользователем.
`%s`	Система переслала веб-содержание.

Расшифровку типов и кодов см. в таб. 165 на стр. 420.

Таб. 162 Журналы атак

СООБЩЕНИЕ	ОПИСАНИЕ
`attack [ TCP | UDP | IGMP | ESP | GRE | OSPF ]`	Межсетевой экран обнаружил атаку по протоколу TCP/UDP/IGMP/ESP/GRE/OSPF.
`attack ICMP (type:%d, code:%d)`	Межсетевой экран обнаружил атаку по протоколу ICMP.
`land [ TCP | UDP | IGMP | ESP | GRE | OSPF ]`	Межсетевой экран обнаружил LAND-атаку по протоколу TCP/UDP/IGMP/ESP/GRE/OSPF.

Таб. 162 Журналы атак (продолжение)

СООБЩЕНИЕ	ОПИСАНИЕ
land ICMP (type:%d, code:%d)	Межсетевой экран обнаружил LAND-атаку по протоколу ICMP.
ip spoofing - WAN [TCP | UDP | IGMP | ESP | GRE | OSPF]	Межсетевой экран обнаружил атаку с подменой IP-адреса на порту WAN.
ip spoofing - WAN ICMP (type:%d, code:%d)	Межсетевой экран обнаружил атаку по протоколу ICMP с подменой IP-адреса на порту WAN.
icmp echo : ICMP (type:%d, code:%d)	Межсетевой экран обнаружил атаку посредством эхозапроса ICMP.
syn flood TCP	Межсетевой экран обнаружил атаку типа “SYN Flood” по протоколу TCP.
ports scan TCP	Межсетевой экран обнаружил атаку со сканированием портов посредством протокола TCP.
teardrop TCP	Межсетевой экран обнаружил атаку типа “Teardrop” по протоколу TCP.
teardrop UDP	Межсетевой экран обнаружил атаку типа “Teardrop” по протоколу UDP.
teardrop ICMP (type:%d, code:%d)	Межсетевой экран обнаружил атаку типа “Teardrop” по протоколу ICMP.
illegal command TCP	Межсетевой экран обнаружил атаку с применением недопустимой команды TCP.
NetBIOS TCP	Межсетевой экран обнаружил атаку по протоколу NetBIOS посредством TCP.
ip spoofing - no routing entry [TCP | UDP | IGMP | ESP | GRE | OSPF]	Межсетевой экран классифицировал пакет с отсутствующим маршрутом к отправителю как попытку атаки с подменой IP-адреса.
ip spoofing - no routing entry ICMP (type:%d, code:%d)	Межсетевой экран классифицировал ICMP-пакет с отсутствующим маршрутом к отправителю как попытку атаки с подменой IP-адреса.
vulnerability ICMP (type:%d, code:%d)	Межсетевой экран обнаружил атаку, эксплуатирующую уязвимость ICMP.
traceroute ICMP (type:%d, code:%d)	Межсетевой экран обнаружил атаку с использованием ICMP-запроса для трассировки маршрута.

Таб. 163 Журналы 802.1X

СООБЩЕНИЕ	ОПИСАНИЕ
Local User Database accepts user.	Пользователь прошел аутентификацию по локальной базе данных.
Local User Database reports user credential error.	Пользователь не прошел аутентификацию по локальной базе данных, указав неверный пароль.
Local User Database does not find user`s credential.	Пользователь не прошел аутентификацию по локальной базе данных, так как указанное имя пользователя в локальной базе данных отсутствует.

Таб. 163 Журналы 802.1X (продолжение)

СООБЩЕНИЕ	ОПИСАНИЕ
RADIUS accepts user.	Пользователь прошел аутентификацию на RADUIS-сервере.
RADIUS rejects user. Pls check RADIUS Server.	Пользователь не прошел аутентификацию на RADUIS-сервере. Проверьте данные на RADIUS-сервере.
Local User Database does not support authentication method.	Локальная база данных поддерживает только метод аутентификации EAP-MD5. Пользователь пытался использовать другой метод и не прошел аутентификацию.
User logout because of session timeout expired.	Маршрутизатор отключил пользователя по истечении времени неактивности сеанса.
User logout because of user deassociation.	Маршрутизатор отключил пользователя, завершившего сеанс.
User logout because of no authentication response from user.	Маршрутизатор отключил пользователя, от которого не последовало отклика при аутентификации.
User logout because of idle timeout expired.	Маршрутизатор отключил пользователя по истечении периода неактивности.
User logout because of user request.	Пользователь вышел из системы.
Local User Database does not support authentication method.	Пользователь попытался применить метод аутентификации, не поддерживаемый локальной базой данных (поддерживается только метод EAP-MD5).
No response from RADIUS. Pls check RADIUS Server.	Отклик от RADIUS-сервера не поступил. Проверьте настройки RADIUS-сервера.
Use Local User Database to authenticate user.	В качестве сервера аутентификации используется локальная база данных пользователей.
Use RADIUS to authenticate user.	В качестве сервера аутентификации используется RADIUS-сервер.
No Server to authenticate user.	Аутентификацию пользователя провести невозможно, так как отсутствует сервер аутентификации.
Local User Database does not find user`s credential.	Пользователь не прошел аутентификацию по локальной базе данных, так как указанное имя пользователя в локальной базе данных отсутствует.

Таб. 164 Замечания по заданию ACL

НАПРАВЛЕНИЕ ДВИЖЕНИЯ ПАКЕТОВ	НАПРАВЛЕНИЕ	ОПИСАНИЕ
(L to W)	Из LAN в WAN	ACL задается для пакетов, пересылаемых из LAN в WAN.
(W to L)	Из WAN в LAN	ACL задается для пакетов, пересылаемых из WAN в LAN.

Таб. 164 Замечания по заданию ACL (продолжение)

НАПРАВЛЕНИЕ ДВИЖЕНИЯ ПАКЕТОВ	НАПРАВЛЕНИЕ	ОПИСАНИЕ
(L to L/P-2602)	Из LAN в LAN/P-2602	ACL задается для пакетов, пересылаемых из LAN в LAN или на P-2602.
(W to W/P-2602)	Из WAN в WAN/P-2602	ACL задается для пакетов, пересылаемых из WAN в WAN или на P-2602.

Таб. 165 Пояснения к кодам ICMP

ТИП	КОД	ОПИСАНИЕ
0		Отклик на эхозапрос
	0	Сообщение с откликом на эхозапрос
3		Адресат недоступен
	0	Сеть недоступна
	1	Хост недоступен
	2	Протокол недоступен
	3	Порт недоступен
	4	Пакет, для которого требовалась фрагментация, был отброшен из-за наличия флажка DF (“не фрагментировать”)
	5	Маршрутизация к источнику невозможна
4		Источник должен снизить трафик
	0	Шлюз может удалять IP-датаграммы при отсутствии достаточного буфера для накопления датаграмм перед отправкой в следующую сеть по маршруту к сети адресата.
5		Redirect
	0	Переадресация датаграмм для сети
	1	Переадресация датаграмм для хоста
	2	Переадресация датаграмм для типа службы и сети
	3	Переадресация датаграмм для типа службы и хоста
8		Эхозапрос
	0	Сообщение эхозапроса
11		Превышено допустимое время
	0	На маршруте превышено время жизни пакета (TTL)
	1	Превышено время сборки фрагментов
12		Ошибка в параметре
	0	Ошибка отмечена указателем
13		Timestamp
	0	Сообщение запроса метки времени
14		Отклик метки времени

Таб. 165 Пояснения к кодам ICMP (продолжение)

ТИП	КОД	ОПИСАНИЕ
	0	Сообщение с откликом метки времени
15		Информационный запрос
	0	Сообщение с информационным запросом
16		Информационный отклик
	0	Сообщение с информационным откликом

Таб. 166 Журналы SYSLOG

СООБЩЕНИЕ	ОПИСАНИЕ
<Объект*8 + значимость>Мес дд чч:мм:сс имя_хоста src="<IP_источника:порт_источника>" dst="<IP_адресата:порт_адресата>" msg="<сообщение>" note="<примечание>" devID="<три последних разряда MAC-адреса>" cat="<категория>	Это сообщение отсылается системой (в качестве имени системы, если не было настроено другое имя, указывается “RAS”), когда маршрутизатор оставляет запись в системном журнале. Тип журнального объекта задается на странице MAIN MENU->LOGS->Log Settings. В качестве уровня значимости используется класс значимости SYSLOG. Расшифровка сообщений и примечаний приведена в таблицах журнальных сообщений далее в этом приложении. Поле “devID” содержит последние три символа MAC-адреса на порту LAN маршрутизатора. Поле “cat” соответствует категории в журналах маршрутизатора.

Таб. 167 Журналы SIP

СООБЩЕНИЕ	ОПИСАНИЕ
SIP Registration Success by SIP: (телефонный номер SIP)	Указанная учетная запись SIP успешно зарегистрирована на сервере регистрации SIP.
SIP Registration Fail by SIP: (телефонный номер SIP)	Указанную учетную запись SIP не удалось зарегистрировать на сервере регистрации SIP.
SIP UnRegistration Success by SIP: (телефонный номер SIP)	Указанная учетная запись SIP удалена с сервера регистрации SIP.
SIP UnRegistration Success by SIP: (телефонный номер SIP)	Указанную учетную запись SIP не удалось удалить с сервера регистрации SIP.

Таб. 168 Журналы RTP

СООБЩЕНИЕ	ОПИСАНИЕ
`Error, RTP init fail`	Сбой инициализации сеанса RTP.
`Error, Call fail: RTP connect fail`	VoIP-вызов не может быть выполнен, так как невозможно установить RTP-сеанс.
`Error, RTP connection cannot close`	Не удалось завершить сеанс RTP.

Таб. 169 Журналы FSM: Вызывающая сторона

СООБЩЕНИЕ	ОПИСАНИЕ
`VoIP Call Start Ph[номер телефонного порта] <- номер исходящего вызова`	На телефоне, подключенном к телефонному порту, был набран указанный номер VoIP.
`VoIP Call Established Ph[телефонный порт] -> номер исходящего вызова`	На телефоне, подключенном к телефонному порту, было установлено соединение с указанным номером VoIP.
`VoIP Call End Phone[телефонный порт]`	Вызов VoIP, осуществлявшийся с указанного телефонного порта, завершен.

Таб. 170 Журналы FSM: Вызываемая сторона

СООБЩЕНИЕ	ОПИСАНИЕ
`VoIP Call Start from SIP[Номер порта SIP]`	На P-2602 поступил телефонный вызов с указанного номера SIP.
`VoIP Call Established Ph[телефонный порт] <- номер исходящего вызова`	Установлено входящее соединение VoIP между P-2602 и указанным телефонным номером SIP.
`VoIP Call End Phone[телефонный порт]`	Вызов VoIP, поступивший на P-2602, завершен.

Таб. 171 Журналы вызовов ТфОП

СООБЩЕНИЕ	ОПИСАНИЕ
`PSTN Call Start`	Начат вызов по ТфОП.
`PSTN Call End`	Вызов по ТфОП завершен.
`PSTN Call Established`	Установлено соединение по ТфОП.

В следующей таблице приведены типы полезной нагрузки ISAKMP по стандарту RFC 2408 , отображаемые в журнале. Подробное описание каждого типа см. в RFC 2408.

Таб. 172 Типы полезной нагрузки ISAKMP по стандарту RFC-2408

СОДЕРЖАНИЕ ЖУРНАЛА	ТИП ПОЛЕЗНОЙ НАГРУЗКИ
SA	Ассоциация безопасности
PROP	Предложение
TRANS	Преобразование
KE	Обмен ключами
ID	Идентификация
CER	Сертификат
CER_REQ	Запрос сертификата
HASH	Хеш
SIG	Подпись
NONCE	Псевдослучайное число
NOTFY	Уведомление
DEL	Удаление
VID	Код поставщика оборудования

Команды для управления журналом

В описании интерфейса командной строки (прилож. J на стр. 427) поясняется вызов и использование команд.

Настройка содержания журнала P-2602

1. Команда `sys logs load` загружает буфер настроек журнала, позволяющий задать типы журналов, которые будет вести устройство P-2602.
2. Список категорий журналов можно просмотреть с помощью команды `sys logs category`.

Рис. 221 Пример просмотра списка категорий журналов

```
Copyright (c) 1994 - 2004 ZyXEL Communications Corp.
ras> ?
Действительными командами являются следующие:
sys             exit            ether           wan
wlan            ip              bridge          lan
radius          8021x           dsp             voiceradius          8021x
ras>
```

3 Чтобы просмотреть список параметров, доступных для конкретной категории, наберите команду `sys logs category`, следом указав тип категории.

Рис. 222 Пример просмотра параметров ведения журнала

```
ras> sys logs category access
Использование: [0:none/1:log/2:alert/3:both]
ras>
```

4 Чтобы задать типы журнальных сообщений, наберите команду `sys logs category`, следом указав тип категории и параметр.

0 отключает ведение журналов для данной категории, 1 указывает регистрировать только журнальные сообщения для данной категории, 2 – регистрировать только предупреждения для данной категории, 3 – регистрировать для данной категории и журнальные сообщения, и предупреждения. Для некоторых категорий определенные параметры могут быть недоступны.

5 Команда `sys logs save` сохраняет настройки в P-2602 (для ведения журналов необходимо выполнить эту команду).

Просмотр журналов

- Команда `sys logs display` служит для просмотра всех сообщений в журнале P-2602.
- Команда `sys logs category` служит для просмотра настроек журналов или для просмотра всех категорий журналов.
- Команда `sys logs display [log category]` служит для просмотра отдельной категории журналов P-2602.
- Команда `sys logs clear` служит для удаления всех журналов P-2602.

Пример команд для работы с журналами

В этом примере выполняется настройка P-2602 для ведения журналов доступа и предупреждений, после чего вызывается просмотр результатов.

Рис. 223 Пример команд для работы с журналами

```
ras> sys logs load
ras> sys logs category access 3
ras> sys logs save
ras> sys logs display access
#  .time                source                  destination            notes

    message
  7|01/01/2000 09:40:13 |192.168.1.1:3         |192.168.1.33:1        |ACCESS FO
RWARD
    Router reply ICMP packet: ICMP(type:3, code:1)
  8|01/01/2000 09:40:07 |192.168.1.1:3         |192.168.1.33:1        |ACCESS FO
RWARD
    Router reply ICMP packet: ICMP(type:3, code:1)
  9|01/01/2000 09:40:04 |192.168.1.1:3         |192.168.1.33:1        |ACCESS FO
RWARD
    Router reply ICMP packet: ICMP(type:3, code:1)
 10|01/01/2000 09:40:04 |192.168.1.33:1199     |207.69.188.186:110    |ACCESS FO
RWARD
    Firewall default policy: TCP (L to W)
 11|01/01/2000 09:40:04 |192.168.1.1:53        |192.168.1.33:1200     |ACCESS FO
RWARD
    none: UDP
```

Приложение J
Интерпретатор команд

Ниже приведено описание интерпретатора команд. Для работы с интерпретатором войдите в P-2602 по Telnet и введите пароль. Подробную информацию о командах см. на прилагающемся компакт-диске или на zyxel.com.

Примечание: Использование недокументированных команд или некорректное выполнение настроек может нарушить работоспособность устройства или вывести его из строя.

Синтаксис команд

- Ключевые слова команд выделены шрифтом `courier new`.
- Введите ключевые слова команд именно так, как показано ниже, не сокращая.
- Обязательные поля команды заключены в угловые скобки <>.
- Необязательные поля команды заключены в квадратные скобки `[]`.
- Знак " | " означает "или".

  Например,

  sys filter netbios config <type> <on|off>

  означает, что необходимо указать тип фильтра netbios и то, нужно ли его включить или выключить.

Использование команд

Список действительных команд можно найти, введя `help` или `?` в командной строке. Всегда вводите команду полностью. По завершении работы с командами введите "`exit`" для выхода.

Приложение K
Встроенный генератор SPTGEN

Обзор встроенного генератора SPTGEN

Встроенный SPTGEN (генератор таблицы системных параметров) – это текстовый файл настроек, который облегчает одновременную настройку нескольких P-2602. Встроенный SPTGEN позволяет настраивать, сохранять и загружать параметры сразу из нескольких меню, используя всего один текстовый файл, благодаря чему снимается необходимость прохождения нескольких экранов настройки на кажом P-2602.

Формат текстового файла настроек

Все текстовые файлы встроенного SPTGEN отвечают следующему формату:

```
<идентификационный номер поля = имя поля = допустимые значения
параметров = входное значение>,
```

где <входное значение> – это вводимое вами значение, отвечающее условиям поля <допустимые значения параметров>.

На следующем рисунке приведен пример текстового файла для встроеного SPTGEN.

Рис. 224 Формат текстового файла настроек: описание столбцов

```
/ Menu 1 – Общая настройка
 10000000 = Configured                <0(No)| 1(Yes)>       = 1
 10000001 = System Name               <Str>                 = Your Device
 10000002 = Location                  <Str>                 =
 10000003 = Contact Person's Name     <Str>                 =
 10000004 = Route IP                  <0(No)| 1(Yes)>       = 1
 10000005 = Route IPX                <0(No)| 1(Yes)>       = 0
 10000006 = Bridge                   <0(No)| 1(Yes)>       = 0
```

Примечание: НЕ изменяйте и не удаляйте содержимое никаких полей, кроме поля “входное значение”.

В этом приложении рассмотрен встроенный генертор SPTGEN. Все меню приведены в качестве примера для иллюстрации применения SPTGEN. Фактический вид меню в конкретном продукте может отличаться.

Редактирование файлов встроенного SPTGEN – моменты, которые необходимо учесть

Перед каждым вводимым параметром должен следовать знак “=” и один пробел.

Некоторые параметры зависят от других. Например, если в меню 1 вы отключили поле **Configured** (см. рис. 224 на стр. 429), то в этом меню необходимо отключить все поля.

Если в столбце **входное значение** вы ввели неверный пароль, P-2602 не сохранит настройки, а в командной строке появится **идентификационный номер поля**. рис. 225 на стр. 430 иллюстрирует пример ошибки, которую P-2602 выдает, если в столбце **входное значение** поля с **идентификационным номером** 1000000 введено значение, отличное от “0” или “1” (см. рис. 224 на стр. 429).

Рис. 225 Неверный ввод параметра: пример командной строки

```
field value is not legal error:-1
ROM-t is not saved, error Line ID:10000000
reboot to get the original configuration
Bootbase Version: V2.02 | 2/22/2001 13:33:11
RAM: Size = 8192 Kbytes
FLASH: Intel 8M *2
```

Если *все* введенные параметры действительны, P-2602 выдаст следуюее сообщение:

Рис. 226 Верный ввод параметра: 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
RAM: Size = 8192 Kbytes
FLASH: Intel 8M *2
```

Пример приема файла встроенного SPTGEN по FTP

1. Запустите FTP-клиента.
2. Введите “`bin`”. Команда “`bin`” устанавливает двоичный режим передачи.
3. С помощью команды “get” примите файл “`rom-t`”. Команда `get` копирует файлы с P-2602 на компьютер. Имя “`rom-t`” соответствует файлу настроек P-2602.
4. Отредактируйте файл “`rom-t`” в текстовом редакторе (не используйте для этого офисные текстовые процессоры). Для редактирования необходимо закрыть экран FTP.

Рис. 227 Пример приема файла, встроенного SPTGEN по FTP

```
c:\ftp 192.168.1.1
220 PPP FTP version 1.0 ready at Sat Jan 1 03:22:12 2000
User (192.168.1.1:(none)):
331 Enter PASS command
Password:
230 Logged in
ftp>bin
200 Type I OK
ftp> get rom-t
ftp>bye
c:\edit rom-t
(отредактируйте файл "rom-t" в текстовом редакторе и сохраните его)
```

Примечание: При сохранении на компьютере файл "rom-t" можно переименовать, но при загрузке в P-2602 он снова должен быть назван "rom-t".

Пример отправки файла встроенного SPTGEN по FTP

1. Запустите FTP-клиента.
2. Введите "bin". Команда "bin" устанавливает двоичный режим передачи.
3. Загрузите файл настроек P-2602 "rom-t" с компьютера в P-2602 с помощью команды "put".
4. Закройте FTP-клиента.

Рис. 228 Пример отправки файла, встроенного SPTGEN по FTP

```
c:\ftp 192.168.1.1
220 PPP FTP version 1.0 ready at Sat Jan 1 03:22:12 2000
User (192.168.1.1:(none)):
331 Enter PASS command
Password:
230 Logged in
ftp>bin
200 Type I OK
ftp> put rom-t
ftp>bye
```

Примеры экранов встроенного SPTGEN

В этом разделе рассмотрены экраны встроенного SPTGEN для P-2602.

Таб. 173 Сокращения, используемые в таблице с примерами экранов встроенного SPTGEN

СОКРАЩЕНИЕ	ЗНАЧЕНИЕ
FIN	Идентификационный номер поля
FN	Имя поля
PVA	Допустимые значения параметров
INPUT	Пример вводимых данных
*	Применяется к P-2602.

Ниже перечислены меню встроенного SPTGEN.

Таб. 174 Общая настройка Меню 1

/ Menu 1 – Общая настройка			
FIN	FN	PVA	INPUT
10000000 =	Настраивается	<0(Нет) | 1(Да)>	= 0
10000001 =	Имя системы	<Стр>	= ваше устройство
10000002 =	Местонахождение	<Стр>	=
10000003 =	ФИО контактного лица	<Стр>	=
10000004 =	Маршрутизатор IP	<0(Нет) | 1(Да)>	= 1
10000006 =	Мост	<0(Нет) | 1(Да)>	= 0

Таб. 175 Меню 3

/ Menu 3.1 – Общая настройка Ethernet			
FIN	FN	PVA	INPUT
30100001 =	Входные фильтры протоколов, набор 1		= 2
30100002 =	Входные фильтры протоколов, набор 2		= 256
30100003 =	Входные фильтры протоколов, набор 3		= 256
30100004 =	Входные фильтры протоколов, набор 4		= 256
30100005 =	Входные фильтры устройств, набор 1		= 256
30100006 =	Входные фильтры устройств, набор 2		= 256
30100007 =	Входные фильтры устройств, набор 3		= 256
30100008 =	Входные фильтры устройств, набор 4		= 256
30100009 =	Выходные фильтры протоколов, набор 1		= 256
30100010 =	Выходные фильтры протоколов, набор 2		= 256
30100011 =	Выходные фильтры протоколов, набор 3		= 256
30100012 =	Выходные фильтры протоколов, набор 4		= 256
30100013 =	Выходные фильтры устройств, набор 1		= 256

Таб. 175 Меню 3

30100014 =	Выходные фильтры устройств, набор 2		= 256
30100015 =	Выходные фильтры устройств, набор 3		= 256
30100016 =	Выходные фильтры устройств, набор 4		= 256
/ Меню 3.2 – настройка TCP/IP и DHCP для Ethernet			
FIN	FN	PVA	INPUT
30200001 =	DHCP	<0(Нет) | 1(Сервер) | 2(Ретранс-лятор)>	= 0
30200002 =	Начальный адрес пула клиентских IP-адресов		= 192.168.1.33
30200003 =	Размер пула клиентских адресов		= 32
30200004 =	Первичный DNS-сервер		= 0.0.0.0
30200005 =	Вторичный DNS-сервер		= 0.0.0.0
30200006 =	Удаленный DHCP-сервер		= 0.0.0.0
30200008 =	IP-адрес		= 172.21.2.200
30200009 =	Маска подсети IP		= 16
30200010 =	Направление RIP	<0(Нет) | 1(Вход-выход) | 2(Только вход) | 3(Только выход)>	= 0
30200011 =	Версия	<0(Rip-1) | 1(Rip-2B) |2(Rip-2M)>	= 0
30200012 =	Многоадресная рассылка	<0(IGMP-v2) | 1(IGMP-v1) | 2(Нет)>	= 2
30200013 =	Набор политик IP 1 (1~12)		= 256
30200014 =	Набор политик IP 2 (1~12)		= 256
30200015 =	Набор политик IP 3 (1~12)		= 256
30200016 =	Набор политик IP 4 (1~12)		= 256
/ Меню 3.2.1 – Настройка совмещения IP-адресов			
FIN	FN	PVA	INPUT
30201001 =	Совмещение IP-адреса 1	<0(Нет) | 1(Да)>	= 0
30201002 =	IP-адрес		= 0.0.0.0
30201003 =	Маска подсети IP		= 0
30201004 =	Направление RIP	<0(Нет) | 1(Вход-выход) | 2(Только вход) | 3(Только выход)>	= 0

Таб. 175 Меню 3

30201005 =	Версия	<0(Rip-1) | 1(Rip-2B) |2(Rip-2M)>	= 0
30201006 =	Совмещенный IP-адрес 1: входные фильтры протоколов, набор 1		= 256
30201007 =	Совмещенный IP-адрес 1: входные фильтры протоколов, набор 2		= 256
30201008 =	Совмещенный IP-адрес 1: входные фильтры протоколов, набор 3		= 256
30201009 =	Совмещенный IP-адрес 1: входные фильтры протоколов, набор 4		= 256
30201010 =	Совмещенный IP-адрес 1: выходные фильтры протоколов, набор 1		= 256
30201011 =	Совмещенный IP-адрес 1: выходные фильтры протоколов, набор 2		= 256
30201012 =	Совмещенный IP-адрес 1: выходные фильтры протоколов, набор 3		= 256
30201013 =	Совмещенный IP-адрес 1: выходные фильтры протоколов, набор 4		= 256
30201014 =	Совмещенный IP-адрес 2 <0(Нет) | 1(Да)>		= 0
30201015 =	IP-адрес		= 0.0.0.0
30201016 =	Маска подсети IP		= 0
30201017 =	Направление RIP	<0(Нет) | 1(Вход-выход) | 2(Только вход) | 3(Только выход)>	= 0
30201018 =	Версия	<0(Rip-1) | 1(Rip-2B) |2(Rip-2M)>	= 0
30201019 =	Совмещенный IP-адрес 2: входные фильтры протоколов, набор 1		= 256
30201020 =	Совмещенный IP-адрес 2: входные фильтры протоколов, набор 2		= 256
30201021 =	Совмещенный IP-адрес 2: входные фильтры протоколов, набор 3		= 256
30201022 =	Совмещенный IP-адрес 2: входные фильтры протоколов, набор 4		= 256
30201023 =	Совмещенный IP-адрес 2: выходные фильтры протоколов, набор 1		= 256
30201024 =	Совмещенный IP-адрес 2: выходные фильтры протоколов, набор 2		= 256
30201025 =	Совмещенный IP-адрес 2: выходные фильтры протоколов, набор 3		= 256
30201026 =	Совмещенный IP-адрес 2: выходные фильтры протоколов, набор 4		= 256

Таб. 175 Меню 3

*/ Меню 3.5 – настройка беспроводной сети			
FIN	FN	PVA	INPUT
30500001 =	ESSID		Беспроводное соединение
30500002 =	Скрыть ESSID	<0(Нет) | 1(Да)>	= 0
30500003 =	Идентификатор канала	<1|2|3|4|5|6|7|8|9|10|11|12|13>	= 1
30500004 =	Порог RTS	<0 ~ 2432>	= 2432
30500005 =	Порог фрагментации	<256 ~ 2432>	= 2432
30500006 =	WEP	<0(выкл.) | 1(64-бит WEP) | 2(128-бит WEP)>	= 0
30500007 =	Ключ по умолчанию	<1|2|3|4>	= 0
30500008 =	WEP-ключ 1		=
30500009 =	WEP-ключ 2		=
30500010 =	WEP-ключ 3		=
30500011 =	WEP-ключ 4		=
30500012 =	Активация WLAN	<0(Выкл.) | 1(Вкл.)>	= 0
*/ МЕНЮ 3.5.1 – ФИЛЬТР MAC-АДРЕСОВ WLAN			
FIN	FN	PVA	INPUT
30501001 =	Активация фильтра MAC-адресов	<0(Нет) | 1(Да)>	= 0
30501002 =	Действие фильтра	<0(Разрешение) | 1(Запрет)>	= 0
30501003 =	Адрес 1		= 00:00:00:00:00:00
30501004 =	Адрес 2		= 00:00:00:00:00:00
30501005 =	Адрес 3		= 00:00:00:00:00:00
Продолжение	…		…
30501034 =	Адрес 32		= 00:00:00:00:00:00

Таб. 176 Меню 4 – настройка доступа к Интернету

/ Меню 4 – настройка доступа к Интернету			
FIN	FN	PVA	INPUT
40000000 =	Настраивается	<0(Нет) | 1(Да)>	= 1
40000001 =	Поставщик услуг Интернета	<0(Нет) | 1(Да)>	= 1
40000002 =	Активация	<0(Нет) | 1(Да)>	= 1
40000003 =	Наименование поставщика услуг		= ВвестиНазвание
40000004 =	Инкапсуляция	<2(PPPOE) | 3(RFC 1483)| 4(PPPoA)| 5(ENET ENCAP)>	= 2
40000005 =	Мультиплексирование	<1(LLC) | 2(VC)	= 1
40000006 =	Номер VPI		= 0
40000007 =	Номер VCI		= 35
40000008 =	Наименование службы	<Стр>	= any (любое)
40000009 =	Имя пользователя	<Стр>	= test@pqa
40000010 =	Пароль	<Стр>	= 1234
40000011 =	Учетная запись одного пользователя (SUA)	<0(Нет) | 1(Да)>	= 1
40000012 =	Назначение IP-адресов	<0(Статическое)|1(Динамическое)>	= 1
40000013 =	IP-адрес		= 0.0.0.0
40000014 =	IP-адрес удаленной стороны		= 0.0.0.0
40000015 =	Маска подсети удаленной стороны		= 0
40000016 =	Входные фильтры протоколов поставщика услуг Интернета, набор 1		= 6
40000017 =	Входные фильтры протоколов поставщика услуг Интернета, набор 2		= 256
40000018 =	Входные фильтры протоколов поставщика услуг Интернета, набор 3		= 256
40000019 =	Входные фильтры протоколов поставщика услуг Интернета, набор 4		= 256
40000020 =	Выходные фильтры протоколов поставщика услуг Интернета, набор 1		= 256
40000021 =	Выходные фильтры протоколов поставщика услуг Интернета, набор 2		= 256

Таб. 176 Меню 4 – настройка доступа к Интернету (продолжение)

40000022 =	Выходные фильтры протоколов поставщика услуг Интернета, набор 3		= 256
40000023 =	Выходные фильтры протоколов поставщика услуг Интернета, набор 4		= 256
40000024 =	Период неактивности PPPoE-соединения с поставщиком услуг		= 0
40000025 =	Маршрутизатор IP	<0(Нет) | 1(Да)>	= 1
40000026 =	Мост	<0(Нет) | 1(Да)>	= 0
40000027 =	Тип QoS для ATM	<0(CBR) | (1 (UBR)>	= 1
40000028 =	Пиковая скорость передачи ячеек (PCR)		= 0
40000029 =	Выдерживаемая скорость передачи ячеек (SCR)		= 0
40000030 =	Максимальный размер пульсации (MBS)		= 0
40000031=	Направление RIP	<0(Нет) | 1(Вход-выход) | 2(Только вход) | 3(Только выход)>	= 0
40000032=	RIP Version	<0(Rip-1) | 1(Rip-2B) |2(Rip-2M)>	= 0
40000033=	Закрепленное соединение	<0(Нет) | 1(Да)>	= 0

Таб. 177 Меню 12

/ Меню 12 – настройка статического IP-маршрута			
FIN	FN	PVA	INPUT
120101001 =	Набор статических маршрутов 1, наименование	<Стр>	=
120101002 =	Набор статических маршрутов 1, активация	<0(Нет) | 1(Да)>	= 0
120101003 =	Набор статических маршрутов 1, IP-адрес места назначения		= 0.0.0.0
120101004 =	Набор статических маршрутов 1, маска подсети места назначения		= 0
120101005 =	Набор статических маршрутов 1, шлюз		= 0.0.0.0
120101006 =	Набор статических маршрутов 1, метрика		= 0
120101007 =	Набор статических маршрутов 1, флажок “частный”	<0(Нет) | 1(Да)>	= 0

Таб. 177 Меню 12 (продолжение)

/ Меню 12.1.2 – настройка статического IP-маршрута			
FIN	FN	PVA	INPUT
120102001 =	Набор статических маршрутов 2, наименование		=
120102002 =	Набор статических маршрутов 2, активация	<0(Нет) | 1(Да)>	= 0
120102003 =	Набор статических маршрутов 2, IP-адрес места назначения		= 0.0.0.0
120102004 =	Набор статических маршрутов 2, маска подсети места назначения		= 0
120102005 =	Набор статических маршрутов 2, шлюз		= 0.0.0.0
120102006 =	Набор статических маршрутов 2, метрика		= 0
120102007 =	Набор статических маршрутов 2, флажок “частный”	<0(Нет) | 1(Да)>	= 0
/ Меню 12.1.3 – настройка статического IP-маршрута			
FIN	FN	PVA	INPUT
120103001 =	Набор статических маршрутов 3, наименование	<Стр>	=
120103002 =	Набор статических маршрутов 3, активация	<0(Нет) | 1(Да)>	= 0
120103003 =	Набор статических маршрутов 3, IP-адрес места назначения		= 0.0.0.0
120103004 =	Набор статических маршрутов 3, маска подсети места назначения		= 0
120103005 =	Набор статических маршрутов 3, шлюз		= 0.0.0.0
120103006 =	Набор статических маршрутов 3, метрика		= 0
120103007 =	Набор статических маршрутов 3, флажок “частный”	<0(Нет) | 1(Да)>	= 0
/ Меню 12.1.4 – настройка статического IP-маршрута			
FIN	FN	PVA	INPUT
120104001 =	Набор статических маршрутов 4, наименование	<Стр>	=
120104002 =	Набор статических маршрутов 4, активация	<0(Нет) | 1(Да)>	= 0
120104003 =	Набор статических маршрутов 4, IP-адрес места назначения		= 0.0.0.0
120104004 =	Набор статических маршрутов 4, маска подсети места назначения		= 0
120104005 =	Набор статических маршрутов 4, шлюз		= 0.0.0.0
120104006 =	Набор статических маршрутов 4, метрика		= 0
120104007 =	Набор статических маршрутов 4, флажок “частный”	<0(Нет) | 1(Да)>	= 0

Таб. 177 Меню 12 (продолжение)

/ Меню 12.1.5 – настройка статического IP-маршрута			
FIN	FN	PVA	INPUT
120105001 =	Набор статических маршрутов 5, наименование	<Стр>	=
120105002 =	Набор статических маршрутов 5, активация	<0(Нет) | 1(Да)>	= 0
120105003 =	Набор статических маршрутов 5, IP-адрес места назначения		= 0.0.0.0
120105004 =	Набор статических маршрутов 5, маска подсети места назначения		= 0
120105005 =	Набор статических маршрутов 5, шлюз		= 0.0.0.0
120105006 =	Набор статических маршрутов 5, метрика		= 0
120105007 =	Набор статических маршрутов 5, флажок “частный”	<0(Нет) | 1(Да)>	= 0
/ Меню 12.1.6 – настройка статического IP-маршрута			
FIN	FN	PVA	INPUT
120106001 =	Набор статических маршрутов 6, наименование	<Стр>	=
120106002 =	Набор статических маршрутов 6, активация	<0(Нет) | 1(Да)>	= 0
120106003 =	Набор статических маршрутов 6, IP-адрес места назначения		= 0.0.0.0
120106004 =	Набор статических маршрутов 6, маска подсети места назначения		= 0
120106005 =	Набор статических маршрутов 6, шлюз		= 0.0.0.0
120106006 =	Набор статических маршрутов 6, метрика		= 0
120106007 =	Набор статических маршрутов 6, флажок “частный”	<0(Нет) | 1(Да)>	= 0
/ Меню 12.1.7 – настройка статического IP-маршрута			
FIN	FN	PVA	INPUT
120107001 =	Набор статических маршрутов 7, наименование	<Стр>	=
120107002 =	Набор статических маршрутов 7, активация	<0(Нет) | 1(Да)>	= 0
120107003 =	Набор статических маршрутов 7, IP-адрес места назначения		= 0.0.0.0
120107004 =	Набор статических маршрутов 7, маска подсети места назначения		= 0
120107005 =	Набор статических маршрутов 7, шлюз		= 0.0.0.0
120107006 =	Набор статических маршрутов 7, метрика		= 0
120107007 =	Набор статических маршрутов 7, флажок “частный”	<0(Нет) | 1(Да)>	= 0

Таб. 177 Меню 12 (продолжение)

/ Меню 12.1.8 – настройка статического IP-маршрута			
FIN	FN	PVA	INPUT
120108001 =	Набор статических маршрутов 8, наименование	<Стр>	=
120108002 =	Набор статических маршрутов 8, активация	<0(Нет) | 1(Да)>	= 0
120108003 =	Набор статических маршрутов 8, IP-адрес места назначения		= 0.0.0.0
120108004 =	Набор статических маршрутов 8, маска подсети места назначения		= 0
120108005 =	Набор статических маршрутов 8, шлюз		= 0.0.0.0
120108006 =	Набор статических маршрутов 8, метрика		= 0
120108007 =	Набор статических маршрутов 8, флажок “частный”	<0(Нет) | 1(Да)>	= 0
*/ Меню 12.1.9 – настройка статического IP-маршрута			
FIN	FN	PVA	INPUT
120109001 =	Набор статических маршрутов 9, наименование	<Стр>	=
120109002 =	Набор статических маршрутов 9, активация	<0(Нет) | 1(Да)>	= 0
120109003 =	Набор статических маршрутов 9, IP-адрес места назначения		= 0.0.0.0
120109004 =	Набор статических маршрутов 9, маска подсети места назначения		= 0
120109005 =	Набор статических маршрутов 9, шлюз		= 0.0.0.0
120109006 =	Набор статических маршрутов 9, метрика		= 0
120109007 =	Набор статических маршрутов 9, флажок “частный”	<0(Нет) | 1(Да)>	= 0
*/ Меню 12.1.10 – настройка статического IP-маршрута			
FIN	FN	PVA	INPUT
120110001 =	Набор статических маршрутов 10, наименование		=
120110002 =	Набор статических маршрутов 10, активация	<0(Нет) | 1(Да)>	= 0
120110003 =	Набор статических маршрутов 10, IP-адрес места назначения		= 0.0.0.0
120110004 =	Набор статических маршрутов 10, маска подсети места назначения		= 0
120110005 =	Набор статических маршрутов 10, шлюз		= 0.0.0.0
120110006 =	Набор статических маршрутов 10, метрика		= 0
120110007 =	Набор статических маршрутов 10, флажок “частный”	<0(Нет) | 1(Да)>	= 0

Таб. 177 Меню 12 (продолжение)

*/ Меню 12.1.11 – настройка статического IP-маршрута			
FIN	FN	PVA	INPUT
120111001 =	Набор статических маршрутов 11, наименование	<Стр>	=
120111002 =	Набор статических маршрутов 11, активация	<0(Нет) | 1(Да)>	= 0
120111003 =	Набор статических маршрутов 11, IP-адрес места назначения		= 0.0.0.0
120111004 =	Набор статических маршрутов 11, маска подсети места назначения		= 0
120111005 =	Набор статических маршрутов 11, шлюз		= 0.0.0.0
120111006 =	Набор статических маршрутов 11, метрика		= 0
120111007 =	Набор статических маршрутов 11, флажок “частный”	<0(Нет) | 1(Да)>	= 0
*/ Меню 12.1.12 – настройка статического IP-маршрута			
FIN	FN	PVA	INPUT
120112001 =	Набор статических маршрутов 12, наименование	<Стр>	=
120112002 =	Набор статических маршрутов 12, активация	<0(Нет) | 1(Да)>	= 0
120112003 =	Набор статических маршрутов 12, IP-адрес места назначения		= 0.0.0.0
120112004 =	Набор статических маршрутов 12, маска подсети места назначения		= 0
120112005 =	Набор статических маршрутов 12, шлюз		= 0.0.0.0
120112006 =	Набор статических маршрутов 12, метрика		= 0
120112007 =	Набор статических маршрутов 12, флажок “частный”	<0(Нет) | 1(Да)>	= 0
*/ Меню 12.1.13 – настройка статического IP-маршрута			
FIN	FN	PVA	INPUT
120113001 =	Набор статических маршрутов 13, наименование	<Стр>	=
120113002 =	Набор статических маршрутов 13, активация	<0(Нет) | 1(Да)>	= 0
120113003 =	Набор статических маршрутов 13, IP-адрес места назначения		= 0.0.0.0
120113004 =	Набор статических маршрутов 13, маска подсети места назначения		= 0
120113005 =	Набор статических маршрутов 13, шлюз		= 0.0.0.0
120113006 =	Набор статических маршрутов 13, метрика		= 0
120113007 =	Набор статических маршрутов 13, флажок “частный”	<0(Нет) | 1(Да)>	= 0

Таб. 177 Меню 12 (продолжение)

*/ Меню 12.1.14 – настройка статического IP-маршрута			
FIN	FN	PVA	INPUT
120114001 =	Набор статических маршрутов 14, наименование	<Стр>	=
120114002 =	Набор статических маршрутов 14, активация	<0(Нет) | 1(Да)>	= 0
120114003 =	Набор статических маршрутов 14, IP-адрес места назначения		= 0.0.0.0
120114004 =	Набор статических маршрутов 14, маска подсети места назначения		= 0
120114005 =	Набор статических маршрутов 14, шлюз		= 0.0.0.0
120114006 =	Набор статических маршрутов 14, метрика		= 0
120114007 =	Набор статических маршрутов 14, флажок “частный”	<0(Нет) | 1(Да)>	= 0
*/ Меню 12.1.15 – настройка статического IP-маршрута			
FIN	FN	PVA	INPUT
120115001 =	Набор статических маршрутов 15, наименование	<Стр>	=
120115002 =	Набор статических маршрутов 15, активация	<0(Нет) | 1(Да)>	= 0
120115003 =	Набор статических маршрутов 15, IP-адрес места назначения		= 0.0.0.0
120115004 =	Набор статических маршрутов 15, маска подсети места назначения		= 0
120115005 =	Набор статических маршрутов 15, шлюз		= 0.0.0.0
120115006 =	Набор статических маршрутов 15, метрика		= 0
120115007 =	Набор статических маршрутов 15, флажок “частный”	<0(Нет) | 1(Да)>	= 0
*/ Меню 12.1.16 – настройка статического IP-маршрута			
FIN	FN	PVA	INPUT
120116001 =	Набор статических маршрутов 16, наименование	<Стр>	=
120116002 =	Набор статических маршрутов 16, активация	<0(Нет) | 1(Да)>	= 0
120116003 =	Набор статических маршрутов 16, IP-адрес места назначения		= 0.0.0.0
120116004 =	Набор статических маршрутов 16, маска подсети места назначения		= 0
120116005 =	Набор статических маршрутов 16, шлюз		= 0.0.0.0
120116006 =	Набор статических маршрутов 16, метрика		= 0
120116007 =	Набор статических маршрутов 16, флажок “частный”	<0(Нет) | 1(Да)>	= 0

Таб. 178 Меню 15 – настройка сервера для режима SUA

/ Меню 15 – настройка сервера для режима SUA			
FIN	FN	PVA	INPUT
150000001 =	IP-адрес сервера SUA для порта по умолчанию		= 0.0.0.0
150000002 =	Активация SUA-сервера 2	<0(Нет) | 1(Да)>	= 0
150000003 =	Протокол SUA-сервера 2	<0(Все)|6(TCP)|17 (UDP)>	= 0
150000004 =	Начальный номер порта SUA-сервера 2		= 0
150000005 =	Конечный номер порта SUA-сервера 2		= 0
150000006 =	Локальный IP-адрес SUA-сервера 2		= 0.0.0.0
150000007 =	Активация SUA-сервера 3	<0(Нет) | 1(Да)>	= 0
150000008 =	Протокол SUA-сервера 3	<0(Все)|6(TCP)|17 (UDP)>	= 0
150000009 =	Начальный номер порта SUA-сервера 3		= 0
150000010 =	Конечный номер порта SUA-сервера 3		= 0
150000011 =	Локальный IP-адрес SUA-сервера 3		= 0.0.0.0
150000012 =	Активация SUA-сервера 4	<0(Нет) | 1(Да)>	= 0
150000013 =	Протокол SUA-сервера 4	<0(Все)|6(TCP)|17 (UDP)>	= 0
150000014 =	Начальный номер порта SUA-сервера 4		= 0
150000015 =	Конечный номер порта SUA-сервера 4		= 0
150000016 =	Локальный IP-адрес SUA-сервера 4		= 0.0.0.0
150000017 =	Активация SUA-сервера 5	<0(Нет) | 1(Да)>	= 0
150000018 =	Протокол SUA-сервера 5	<0(Все)|6(TCP)|17 (UDP)>	= 0
150000019 =	Начальный номер порта SUA-сервера 5		= 0
150000020 =	Конечный номер порта SUA-сервера 5		= 0
150000021 =	Локальный IP-адрес SUA-сервера 5		= 0.0.0.0
150000022 =	Активация SUA-сервера 6	<0(Нет) | 1(Да)> = 0	= 0
150000023 =	Протокол SUA-сервера 6	<0(Все)|6(TCP)|17 (UDP)>	= 0
150000024 =	Начальный номер порта SUA-сервера 6		= 0
150000025 =	Конечный номер порта SUA-сервера 6		= 0
150000026 =	Локальный IP-адрес SUA-сервера 6		= 0.0.0.0
150000027 =	Активация SUA-сервера 7	<0(Нет) | 1(Да)>	= 0
150000028 =	Протокол SUA-сервера 7	<0(Все)|6(TCP)|17 (UDP)>	= 0.0.0.0
150000029 =	Начальный номер порта SUA-сервера 7		= 0
150000030 =	Конечный номер порта SUA-сервера 7		= 0

Таб. 178 Меню 15 – настройка сервера для режима SUA (продолжение)

150000031 =	Локальный IP-адрес SUA-сервера 7		= 0.0.0.0
150000032 =	Активация SUA-сервера 8	<0(Нет) | 1(Да)>	= 0
150000033 =	Протокол SUA-сервера 8	<0(Все)|6(TCP)|17 (UDP)>	= 0
150000034 =	Начальный номер порта SUA-сервера 8		= 0
150000035 =	Конечный номер порта SUA-сервера 8		= 0
150000036 =	Локальный IP-адрес SUA-сервера 8		= 0.0.0.0
150000037 =	Активация SUA-сервера 9	<0(Нет) | 1(Да)>	= 0
150000038 =	Протокол SUA-сервера 9	<0(Все)|6(TCP)|17 (UDP)>	= 0
150000039 =	Начальный номер порта SUA-сервера 9		= 0
150000040 =	Конечный номер порта SUA-сервера 9		= 0
150000041 =	Локальный IP-адрес SUA-сервера 9		= 0.0.0.0
150000042 =	Активация SUA-сервера 10	<0(Нет) | 1(Да)>	= 0
150000043 =	Протокол SUA-сервера 10	<0(Все)|6(TCP)|17 (UDP)>	= 0
150000044 =	Начальный номер порта SUA-сервера 10		= 0
150000045 =	Конечный номер порта SUA-сервера 10		= 0
150000046 =	Локальный IP-адрес SUA-сервера 10		= 0.0.0.0
150000047 =	Активация SUA-сервера 11	<0(Нет) | 1(Да)>	= 0
150000048 =	Протокол SUA-сервера 11	<0(Все)|6(TCP)|17 (UDP)>	= 0
150000049 =	Начальный номер порта SUA-сервера 11		= 0
150000050 =	Конечный номер порта SUA-сервера 11		= 0
150000051 =	Локальный IP-адрес SUA-сервера 11		= 0.0.0.0
150000052 =	Активация SUA-сервера 12	<0(Нет) | 1(Да)>	= 0
150000053 =	Протокол SUA-сервера 12	<0(Все)|6(TCP)|17 (UDP)>	= 0
150000054 =	Начальный номер порта SUA-сервера 12		= 0
150000055 =	Конечный номер порта SUA-сервера 12		= 0
150000056 =	Локальный IP-адрес SUA-сервера 12		= 0.0.0.0

Таб. 179 Меню 21.1 – набор фильтров 1

/ Меню 21 – набор фильтров 1			
FIN	FN	PVA	INPUT
210100001 =	Набор фильтров 1, наименование	<Стр>	=
/ Меню 21.1.1.1 – набор фильтров 1, правило 1			
FIN	FN	PVA	INPUT
210101001 =	Набор фильтров 1, правило 1, тип	<2(TCP/IP)>	= 2

Таб. 179 Меню 21.1 – набор фильтров 1 (продолжение)

210101002 =	Набор фильтров 1, правило 1, активация	<0(Нет) | 1(Да)>	= 1
210101003 =	Набор фильтров 1, правило 1, протокол		= 6
210101004 =	Набор фильтров 1, правило 1, IP-адрес получателя		= 0.0.0.0
210101005 =	Набор фильтров 1, правило 1, маска подсети получателя		= 0
210101006 =	Набор фильтров 1, правило 1, порт получателя		= 137
210101007 =	Набор фильтров 1, правило 1, условие сравнения порта получателя	<0(нет)|1(равно)| 2(не равно)| 3(меньше)| 4(больше)>	= 1
210101008 =	Набор фильтров 1, правило 1, IP-адрес источника		= 0.0.0.0
210101009 =	Набор фильтров 1, правило 1, маска подсети источника		= 0
210101010 =	Набор фильтров 1, правило 1, порт источника		= 0
210101011 =	Набор фильтров 1, правило 1, условие сравнения порта источника	<0(нет)|1(равно)| 2(не равно)| 3(меньше)| 4(больше)>	= 0
210101013 =	Набор фильтров 1, правило 1, действие при совпадении	<1(следующее правило)|2(пересылка)|3(запрет)>	= 3
210101014 =	Набор фильтров 1, правило 1, действие при несовпадении	<1(следующее правило)|2(пере-сылка)|3(запрет)>	= 1
/ Меню 21.1.1.2 – набор фильтров 1, правило 2			
FIN	FN	PVA	INPUT
210102001 =	Набор фильтров 1, правило 2, тип	<2(TCP/IP)>	= 2
210102002 =	Набор фильтров 1, правило 2, активация	<0(Нет) | 1(Да)>	= 1
210102003 =	Набор фильтров 1, правило 2, протокол		= 6
210102004 =	Набор фильтров 1, правило 2, IP-адрес получателя		= 0.0.0.0
210102005 =	Набор фильтров 1, правило 2, маска подсети получателя		= 0
210102006 =	Набор фильтров 1, правило 2, порт получателя		= 138
210102007 =	Набор фильтров 1, правило 2, условие сравнения порта получателя	<0(нет)|1(равно)| 2(не равно)| 3(меньше)| 4(больше)>	= 1
210102008 =	Набор фильтров 1, правило 2, IP-адрес источника		= 0.0.0.0
210102009 =	Набор фильтров 1, правило 2, маска подсети источника		= 0

Таб. 179 Меню 21.1 – набор фильтров 1 (продолжение)

210102010 =	Набор фильтров 1, правило 2, порт источника		= 0
210102011 =	Набор фильтров 1, правило 2, условие сравнения порта источника	<0(нет)|1(равно)| 2(не равно)| 3(меньше)| 4(больше)>	= 0
210102013 =	Набор фильтров 1, правило 2, действие при совпадении	<1(следующее правило)|2(пересылка)|3(запрет)>	= 3
210102014 =	Набор фильтров 1, правило 2, действие при несовпадении	<1(следующее правило)|2(пересылка)|3(запрет)>	= 1
/ Меню 21.1.1.3 – набор фильтров 1, правило 3			
FIN	FN	PVA	INPUT
210103001 =	Набор фильтров 1, правило 3, тип	<2(TCP/IP)>	= 2
210103002 =	Набор фильтров 1, правило 3, активация	<0(Нет) | 1(Да)>	= 1
210103003 =	Набор фильтров 1, правило 3, протокол		= 6
210103004 =	Набор фильтров 1, правило 3, IP-адрес получателя		= 0.0.0.0
210103005 =	Набор фильтров 1, правило 3, маска подсети получателя		= 0
210103006 =	Набор фильтров 1, правило 3, порт получателя		= 139
210103007 =	Набор фильтров 1, правило 3, условие сравнения порта получателя	<0(нет)|1(равно)| 2(не равно)| 3(меньше)| 4(больше)>	= 1
210103008 =	Набор фильтров 1, правило 3, IP-адрес источника		= 0.0.0.0
210103009 =	Набор фильтров 1, правило 3, маска подсети источника		= 0
210103010 =	Набор фильтров 1, правило 3, порт источника		= 0
210103011 =	Набор фильтров 1, правило 3, условие сравнения порта источника	<0(нет)|1(равно)| 2(не равно)| 3(меньше)| 4(больше)>	= 0
210103013 =	Набор фильтров 1, правило 3, действие при совпадении	<1(следующее правило)|2(пересылка)|3(запрет)	= 3
210103014 =	Набор фильтров 1, правило 3, действие при несовпадении	<1(следующее правило)|2(пересылка)|3(запрет)	= 1
/ Меню 21.1.1.4 – набор фильтров 1, правило 4			
FIN	FN	PVA	INPUT
210104001 =	Набор фильтров 1, правило 4, тип	<2(TCP/IP)>	= 2
210104002 =	Набор фильтров 1, правило 4, активация	<0(Нет) | 1(Да)>	= 1

Таб. 179 Меню 21.1 – набор фильтров 1 (продолжение)

210104003 =	Набор фильтров 1, правило 4, протокол		= 17
210104004 =	Набор фильтров 1, правило 4, IP-адрес получателя		= 0.0.0.0
210104005 =	Набор фильтров 1, правило 4, маска подсети получателя		= 0
210104006 =	Набор фильтров 1, правило 4, порт получателя		= 137
210104007 =	Набор фильтров 1, правило 4, условие сравнения порта получателя	<0(нет)|1(равно)| 2(не равно)| 3(меньше)| 4(больше)>	= 1
210104008 =	Набор фильтров 1, правило 4, IP-адрес источника		= 0.0.0.0
210104009 =	Набор фильтров 1, правило 4, маска подсети источника		= 0
210104010 =	Набор фильтров 1, правило 4, порт источника		= 0
210104011 =	Набор фильтров 1, правило 4, условие сравнения порта источника	<0(нет)|1(равно)| 2(не равно)| 3(меньше)| 4(больше)>	= 0
210104013 =	Набор фильтров 1, правило 4, действие при совпадении	<1(следующее правило)|2(пере-сылка)|3(запрет)	= 3
210104014 =	Набор фильтров 1, правило 4, действие при несовпадении	<1(следующее правило)|2(пере-сылка)|3(запрет)	= 1
/ Меню 21.1.1.5 – набор фильтров 1, правило 5			
FIN	FN	PVA	INPUT
210105001 =	Набор фильтров 1, правило 5, тип	<2(TCP/IP)>	= 2
210105002 =	Набор фильтров 1, правило 5, активация	<0(Нет) | 1(Да)>	= 1
210105003 =	Набор фильтров 1, правило 5, протокол		= 17
210105004 =	Набор фильтров 1, правило 5, IP-адрес получателя		= 0.0.0.0
210105005 =	Набор фильтров 1, правило 5, маска подсети получателя		= 0
210105006 =	Набор фильтров 1, правило 5, порт получателя		= 138
210105007 =	Набор фильтров 1, правило 5, условие сравнения порта получателя	<0(нет)|1(равно)| 2(не равно)| 3(меньше)| 4(больше)>	= 1
210105008 =	Набор фильтров 1, правило 5, IP-адрес источника		= 0.0.0.0
210105009 =	Набор фильтров 1, правило 5, маска подсети источника		= 0

Таб. 179 Меню 21.1 – набор фильтров 1 (продолжение)

210105010 =	Набор фильтров 1, правило 5, порт источника		= 0
210105011 =	Набор фильтров 1, правило 5, условие сравнения порта источника	<0(нет)|1(равно)| 2(не равно)| 3(меньше)| 4(больше)>	= 0
210105013 =	Набор фильтров 1, правило 5, действие при совпадении	<1(следующее правило)|2(пере-сылка)|3(запрет)>	= 3
210105014 =	Набор фильтров 1, правило 5, действие при несовпадении	<1(следующее правило)|2(пере-сылка)|3(запрет)>	= 1
/ Меню 21.1.1.6 – набор фильтров 1, правило 6			
FIN	FN	PVA	INPUT
210106001 =	Набор фильтров 1, правило 6, тип	<2(TCP/IP)>	= 2
210106002 =	Набор фильтров 1, правило 6, активация	<0(Нет) | 1(Да)>	= 1
210106003 =	Набор фильтров 1, правило 6, протокол		= 17
210106004 =	Набор фильтров 1, правило 6, IP-адрес получателя		= 0.0.0.0
210106005 =	Набор фильтров 1, правило 6, маска подсети получателя		= 0
210106006 =	Набор фильтров 1, правило 6, порт получателя		= 139
210106007 =	Набор фильтров 1, правило 6, условие сравнения порта получателя	<0(нет)|1(равно)| 2(не равно)| 3(меньше)| 4(больше)>	= 1
210106008 =	Набор фильтров 1, правило 6, IP-адрес источника		= 0.0.0.0
210106009 =	Набор фильтров 1, правило 6, маска подсети источника		= 0
210106010 =	Набор фильтров 1, правило 6, порт источника		= 0
210106011 =	Набор фильтров 1, правило 6, условие сравнения порта источника	<0(нет)|1(равно)| 2(не равно)| 3(меньше)| 4(больше)>	= 0
210106013 =	Набор фильтров 1, правило 6, действие при совпадении	<1(следующее правило)|2(пере-сылка)|3(запрет)>	= 3
210106014 =	Набор фильтров 1, правило 6, действие при несовпадении	<1(следующее правило)|2(пере-сылка)|3(запрет)>	= 2

Таб. 180 Меню 21.1 – набор фильтров 2,

/ Меню 21.1 – набор фильтров 2,			
FIN	FN	PVA	INPUT
210200001 =	Набор фильтров 2, наименование	<Стр>	= NetBIOS_WAN
/ Меню 21.1.2.1 – набор фильтров 2, правило 1			
FIN	FN	PVA	INPUT
210201001 =	Набор фильтров 2, правило 1, тип	<0(нет)|2(TCP/IP)>	= 2
210201002 =	Набор фильтров 2, правило 1, активация	<0(Нет) | 1(Да)>	= 1
210201003 =	Набор фильтров 2, правило 1, протокол		= 6
210201004 =	Набор фильтров 2, правило 1, IP-адрес получателя		= 0.0.0.0
210201005 =	Набор фильтров 2, правило 1, маска подсети получателя		= 0
210201006 =	Набор фильтров 2, правило 1, порт получателя		= 137
210201007 =	Набор фильтров 2, правило 1, условие сравнения порта получателя	<0(нет)|1(равно)|2 (не равно)| 3(меньше)| 4(больше)>	= 1
210201008 =	Набор фильтров 2, правило 1, IP-адрес источника		= 0.0.0.0
210201009 =	Набор фильтров 2, правило 1, маска подсети источника		= 0
210201010 =	Набор фильтров 2, правило 1, порт источника		= 0
210201011 =	Набор фильтров 2, правило 1, условие сравнения порта источника	<0(нет)|1(равно)|2 (не равно)| 3(меньше)| 4(больше)>	= 0
210201013 =	Набор фильтров 2, правило 1, действие при совпадении	<1(следующее правило)|2(пере-сылка)|3(запрет)>	= 3
210201014 =	Набор фильтров 2, правило 1, действие при несовпадении	<1(следующее правило)|2(пере-сылка)|3(запрет)>	= 1
/ Меню 21.1.2.2 – набор фильтров 2, правило 2			
FIN	FN	PVA	INPUT
210202001 =	Набор фильтров 2, правило 2, тип	<0(нет)|2(TCP/IP)>	= 2
210202002 =	Набор фильтров 2, правило 2, активация	<0(Нет) | 1(Да)>	= 1
210202003 =	Набор фильтров 2, правило 2, протокол		= 6

Таб. 180 Меню 21.1 – набор фильтров 2, (продолжение)

210202004 =	Набор фильтров 2, правило 2, IP-адрес получателя		= 0.0.0.0
210202005 =	Набор фильтров 2, правило 2, маска подсети получателя		= 0
210202006 =	Набор фильтров 2, правило 2, порт получателя		= 138
210202007 =	Набор фильтров 2, правило 2, условие сравнения порта получателя	<0(нет)|1(равно)|2 (не равно)| 3(меньше)| 4(больше)>	= 1
210202008 =	Набор фильтров 2, правило 2, IP-адрес источника		= 0.0.0.0
210202009 =	Набор фильтров 2, правило 2, маска подсети источника		= 0
210202010 =	Набор фильтров 2, правило 2, порт источника		= 0
210202011 =	Набор фильтров 2, правило 2, условие сравнения порта источника	<0(нет)|1(равно)|2 (не равно)| 3(меньше)| 4(больше)>	= 0
210202013 =	Набор фильтров 2, правило 2, действие при совпадении	<1(следующее правило)|2(пере-сылка)|3(запрет)>	= 3
210202014 =	Набор фильтров 2, правило 2, действие при несовпадении	<1(следующее правило)|2(пере-сылка)|3(запрет)>	= 1
/ Меню 21.1.2.3 – набор фильтров 2, правило 3			
FIN	FN	PVA	INPUT
210203001 =	Набор фильтров 2, правило 3, тип	<0(нет)|2(TCP/IP)>	= 2
210203002 =	Набор фильтров 2, правило 3, активация	<0(Нет) | 1(Да)>	= 1
210203003 =	Набор фильтров 2, правило 3, протокол		= 6
210203004 =	Набор фильтров 2, правило 3, IP-адрес получателя		= 0.0.0.0
210203005 =	Набор фильтров 2, правило 3, маска подсети получателя		= 0
210203006 =	Набор фильтров 2, правило 3, порт получателя		= 139
210203007 =	Набор фильтров 2, правило 3, условие сравнения порта получателя	<0(нет)|1(равно)|2 (не равно)| 3(меньше)| 4(больше)>	= 1
210203008 =	Набор фильтров 2, правило 3, IP-адрес источника		= 0.0.0.0
210203009 =	Набор фильтров 2, правило 3, маска подсети источника		= 0

Таб. 180 Меню 21.1 – набор фильтров 2, (продолжение)

210203010 =	Набор фильтров 2, правило 3, порт источника		= 0
210203011 =	Набор фильтров 2, правило 3, условие сравнения порта источника	<0(нет)|1(равно)|2(не равно)|3(меньше)|4(больше)>	= 0
210203013 =	Набор фильтров 2, правило 3, действие при совпадении	<1(следующее правило)|2(пересылка)|3(запрет)>	= 3
210203014 =	Набор фильтров 2, правило 3, действие при несовпадении	<1(следующее правило)|2(пересылка)|3(запрет)>	= 1
/ Меню 21.1.2.4 – набор фильтров 2, правило 4			
FIN	FN	PVA	INPUT
210204001 =	Набор фильтров 2, правило 4, тип	<0(нет)|2(TCP/IP)>	= 2
210204002 =	Набор фильтров 2, правило 4, активация		<0(Нет) | 1(Да)> = 1
210204003 =	Набор фильтров 2, правило 4, протокол		= 17
210204004 =	Набор фильтров 2, правило 4, IP-адрес получателя		= 0.0.0.0
210204005 =	Набор фильтров 2, правило 4, маска подсети получателя		= 0
210204006 =	Набор фильтров 2, правило 4, порт получателя		= 137
210204007 =	Набор фильтров 2, правило 4, условие сравнения порта получателя	<0(нет)|1(равно)|2(не равно)|3(меньше)|4(больше)>	= 1
210204008 =	Набор фильтров 2, правило 4, IP-адрес источника		= 0.0.0.0
210204009 =	Набор фильтров 2, правило 4, маска подсети источника		= 0
210204010 =	Набор фильтров 2, правило 4, порт источника		= 0
210204011 =	Набор фильтров 2, правило 4, условие сравнения порта источника	<0(нет)|1(равно)|2(не равно)|3(меньше)|4(больше)>	= 0
210204013 =	Набор фильтров 2, правило 4, действие при совпадении	<1(следующее правило)|2(пересылка)|3(запрет)>	= 3
210204014 =	Набор фильтров 2, правило 4, действие при несовпадении	<1(следующее правило)|2(пересылка)|3(запрет)>	= 1
/ Меню 21.1.2.5 – набор фильтров 2, правило 5			
FIN	FN	PVA	INPUT

Таб. 180 Меню 21.1 – набор фильтров 2, (продолжение)

210205001 =	Набор фильтров 2, правило 5, тип	<0(нет)|2(TCP/IP)>	= 2
210205002 =	Набор фильтров 2, правило 5, активация	<0(Нет) | 1(Да)>	= 1
210205003 =	Набор фильтров 2, правило 5, протокол		= 17
210205004 =	Набор фильтров 2, правило 5, IP-адрес получателя		= 0.0.0.0
210205005 =	Набор фильтров 2, правило 5, маска подсети получателя		= 0
210205006 =	Набор фильтров 2, правило 5, порт получателя		= 138
210205007 =	Набор фильтров 2, правило 5, условие сравнения порта получателя	<0(нет)|1(равно)|2 (не равно)| 3(меньше)| 4(больше)>	= 1
210205008 =	Набор фильтров 2, правило 5, IP-адрес источника		= 0.0.0.0
210205009 =	Набор фильтров 2, правило 5, маска подсети источника		= 0
210205010 =	Набор фильтров 2, правило 5, порт источника		= 0
210205011 =	Набор фильтров 2, правило 5, условие сравнения порта источника	<0(нет)|1(равно)|2 (не равно)| 3(меньше)| 4(больше)>	= 0
210205013 =	Набор фильтров 2, правило 5, действие при совпадении	<1(следующее правило)|2(пересыл-ка)|3(запрет)>	= 3
210205014 =	Набор фильтров 2, правило 5, действие при несовпадении	<1(следующее правило)|2(пересыл-ка)|3(запрет)>	= 1
/ Меню 21.1.2.6 – набор фильтров 2, правило 6			
FIN	FN	PVA	INPUT
210206001 =	Набор фильтров 2, правило 6, тип	<0(нет)|2(TCP/IP)>	= 2
210206002 =	Набор фильтров 2, правило 6, активация	<0(Нет) | 1(Да)>	= 1
210206003 =	Набор фильтров 2, правило 6, протокол		= 17
210206004 =	Набор фильтров 2, правило 6, IP-адрес получателя		= 0.0.0.0
210206005 =	Набор фильтров 2, правило 6, маска подсети получателя		= 0
210206006 =	Набор фильтров 2, правило 6, порт получателя		= 139

Таб. 180 Меню 21.1 – набор фильтров 2, (продолжение)

210206007 =	Набор фильтров 2, правило 6, условие сравнения порта получателя	<0(нет)|1(равно)|2 (не равно)| 3(меньше)| 4(больше)>	= 1
210206008 =	Набор фильтров 2, правило 6, IP-адрес источника		= 0.0.0.0
210206009 =	Набор фильтров 2, правило 6, маска подсети источника		= 0
210206010 =	Набор фильтров 2, правило 6, порт источника		= 0
210206011 =	Набор фильтров 2, правило 6, условие сравнения порта источника	<0(нет)|1(равно)|2 (не равно)| 3(меньше)| 4(больше)>	= 0
210206013 =	Набор фильтров 2, правило 6, действие при совпадении	<1(следующее правило)|2(пересыл-ка)|3(запрет)>	= 3
210206014 =	Набор фильтров 2, правило 6, действие при несовпадении	<1(следующее правило)|2(пересыл-ка)|3(запрет)>	= 2
241100005 =	Доступ к FTP-серверу	<0(все)|1(нет)|2 (LAN)|3(WAN)>	= 0
241100006 =	IP-адрес защищенного клиента FTP-сервера		= 0.0.0.0
241100007 =	Порт веб-сервера		= 80
241100008 =	Доступ к веб-серверу	<0(все)|1(нет)|2 (LAN)|3(WAN)>	= 0
241100009 =	IP-адрес защищенного клиента веб-сервера		= 0.0.0.0

Таб. 181 Menu 23 – системные меню

*/ Меню 23.1 – пароль для системы			
FIN	FN	PVA	INPUT
230000000 =	Пароль системы		= 1234
*/ Меню 23.2 – безопасность системы: RADIUS-сервер			
FIN	FN	PVA	INPUT
230200001 =	Сервер аутентификации настроен	<0(Нет) | 1(Да)>	= 1
230200002 =	Сервер аутентификации активен	<0(Нет) | 1(Да)>	= 1
230200003 =	IP-адрес сервера аутентификации		= 192.168.1.32
230200004 =	Порт сервера аутентификации		= 1822

Таб. 181 Menu 23 – системные меню (продолжение)

230200005 =	Общий секретный ключ сервера аутентификации		= 111111111111111 111111111111111
230200006 =	Сервер учета настроен	<0(Нет) | 1(Да)>	= 1
230200007 =	Сервер учета активен	<0(Нет) | 1(Да)>	= 1
230200008 =	IP-адрес сервера учета		= 192.168.1.44
230200009 =	Порт сервера учета		= 1823
230200010 =	Общий секретный ключ сервера учета		= 1234
*/ Меню 23,4 – безопасность системы: IEEE 802.1x			
FIN	FN	PVA	INPUT
230400001 =	Управление беспроводным портом	<0(Требуется аутентификация) |1(Доступ запрещен) |2(Аутентификация не требуется)>	= 2
230400002 =	Таймер повторной аутентификации (в секундах)		= 555
230400003 =	Время ожидания (в секундах)		= 999
230400004 =	Базы данных для аутентификации	<0(Только локальная БД пользователей) |1(Только RADIUS) |2(Локальная БД,RADIUS) |3(RADIUS,локальная БД)>	= 1
230400005 =	Протокол управления ключами	<0(8021x) |1(WPA) |2(WPAPSK)>	= 0
230400006 =	Динамический обмен ключами WEP	<0(Выкл.) |1(64-бит WEP) |2(128-бит WEP)>	= 0
230400007 =	PSK =		=
230400008 =	Смешанный режим WPA	<0(Выкл.) | 1(Вкл.)>	= 0
230400009 =	Конфиденциальность данных для пакетов широковещательной/ многоадресной рассылки	<0(TKIP) |1(WEP)>	= 0
230400010 =	Таймер обновления ключа широковещательной / многоадресной рассылки WPA		= 0

Таб. 182 Меню 24.11 – управление удаленным доступом

/ Меню 24.11 – управление удаленным доступом			
FIN	FN	PVA	INPUT
241100001 =	Порт TELNET-сервера		= 23
241100002 =	Доступ к TELNET-серверу	<0(все)|1(нет)|2(LAN)|3(WAN)>	= 0
241100003 =	IP-адрес защищенного клиента TELNET-сервера		= 0.0.0.0
241100004 =	Порт TELNET-сервера		= 21
241100005 =	Доступ к FTP-серверу	<0(все)|1(нет)|2(LAN)|3(WAN)>	= 0
241100006 =	IP-адрес защищенного клиента FTP-сервера		= 0.0.0.0
241100007 =	Порт веб-сервера		= 80
241100008 =	Доступ к веб-серверу	<0(все)|1(нет)|2(LAN)|3(WAN)>	= 0
241100009 =	IP-адрес защищенного клиента веб-сервера		= 0.0.0.0

Примеры команд

Ниже приведены примеры экранов встроенного SPTGEN, связанных с интерпретатором команд P-2602.

Таб. 183 Примеры команд

FIN	FN	PVA	INPUT
/Команда КС (для Annex A): wan adsl opencmd			
FIN	FN	PVA	INPUT
990000001 =	Модуляция ADSL	<0(glite)|1(t1.413)|2(gdmt)|3(мультирежимная)>	= 3
/Команда КС (для Annex B): wan adsl opencmd			
FIN	FN	PVA	INPUT
990000001 =	Модуляция ADSL	<0(etsi)|1(норм.)|2(gdmt)|3(мультирежимная)>	= 3

Указатель

Numerics

А

Б

В

Г

Д

Е

Ж

З

И

К

M

H

O

П

Р

С

Т

У

Ф

Х

Ц

Ч

Ш

Э

A

B

C

D

E

F

G

H

I

L

N

O

P

Q

R

S

T

U

V

W

Z