P-793H

Защищенный шлюз G.SHDSL.bis с 4 Ethernet-портами

Руководство пользователя

Версия 3.40
1/2007
Вторая редакция

ZyXEL

www.zyxel.ru

О Руководстве пользователя

Целевая аудитория

Это руководство предназначено для пользователей, выполняющих настройку P-793H посредством веб-конфигуратора. Предполагается знание основ TCP/IP и принципов построения сетей.

Другие документы

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

Для настройки P-793H рекомендуется использовать веб-конфигуратор.

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

Отзывы о руководстве пользователя

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

Обозначения, принятые в документации

Предупреждения и примечания

Для предупреждений и примечаний в настоящем руководстве используются следующие обозначения.

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

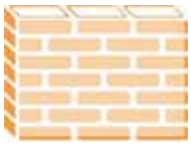
Примечания отмечают другие важные сведения (например, параметры, которые необходимо настроить дополнительно), полезные советы и рекомендации.

Условные обозначения и синтаксис

- Маршрутизатор P-793H может обозначаться в тексте как "P-793H", "устройство", "система" или "изделие".
- Названия изделий, экранов, заголовки полей и выбираемые значения приведены **жирным** шрифтом.
- Названия клавиш набраны заглавными буквами и заключены в квадратные скобки, например, [ENTER] означает нажатие клавиши "Enter" или "Return".
- "Введите" означает, что следует набрать на клавиатуре один или несколько знаков и нажать клавишу [ENTER]. "Выберите" или "Отметьте" означает, что следует выбрать один из предопределенных вариантов.
- Знак ">" обозначает переход между экранами. Например, последовательность **Maintenance > Log > Log Setting** означает, что сначала необходимо щелкнуть в панели навигации на пункте **Maintenance**, затем перейти в подменю **Log** и щелкнуть на вкладке **Log Setting** для перехода на соответствующий экран.
- В зависимости от контекста могут использоваться десятичные или двоичные единицы измерения. В частности, суффикс "к" (кило-) может обозначать 1000 или 1024, суффикс "М" (мега-) – 1000000 или 1048576 и т. д.

Значки, используемые на рисунках

На рисунках в Руководстве пользователя могут встречаться следующие универсальные обозначения. Значок P-793H не является точным изображением вашего устройства.

P-793H 	Компьютер 	Ноутбук 
Сервер 	DSLAM 	Сетевой экран 
Телефон 	Коммутатор 	Маршрутизатор 

Техника безопасности

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

- НЕ устанавливайте устройство вблизи от воды, например, в сыром подвале или рядом с бассейном.
- НЕ подвергайте устройство воздействию влаги, пыли или агрессивных жидкостей.
- НЕ складывайте на устройство никаких предметов.
- НЕ устанавливайте, не эксплуатируйте и не ремонтируйте устройство во время грозы. Грозовые разряды создают риск поражения электрическим током.
- Подключайте к устройству ТОЛЬКО годное к применению вспомогательное оборудование.
- Ремонтировать или разбирать устройство должен ТОЛЬКО квалифицированный специалист.
- Убедитесь, что кабели правильно подключены к клеммам.
- Размещайте соединительные кабели так, чтобы не наступать на них и не задевать их.
- Перед обслуживанием или разборкой в обязательном порядке необходимо отсоединить от устройства все кабели.
- Эксплуатируйте устройство ТОЛЬКО с пригодным для него источником питания или шнуром. Сетевой шнур должен подключаться к сети переменного тока с соответствующим напряжением (110 вольт в Северной Америке и 230 вольт в Европе).
- НЕ ставьте какие-либо предметы на сетевой шнур или блок питания, НЕ размещайте устройство там, где на шнур или блок питания может кто-нибудь наступить.
- НЕ пользуйтесь устройством, если блок питания или шнур поврежден, иначе может произойти поражение электрическим током.
- В случае повреждения необходимо отсоединить шнур или блок питания от устройства и отключить его от электросети.
- НЕ пытайтесь починить шнур или блок питания. Обратитесь к местному поставщику и закажите новый шнур или блок питания.
- Не используйте устройство вне помещений. Убедитесь, что все соединения выполнены внутри помещений. Грозовые разряды создают риск поражения электрическим током.
- НЕ загораживайте вентиляционные проемы устройства. Недостаточная вентиляция может повредить устройство.
- Используйте для телекоммуникационной линии провода калибра 26 AWG (American Wire Gauge, американская система классификации проводов по диаметру) или более толстые.
- Монтируя устройство на стене, следите за тем, чтобы не повредить электропроводку, газо- или водопроводные трубы.

Изделие допускает возможность переработки. Соблюдайте правила утилизации.

Общий обзор

Содержание

Список рисунков

Список таблиц

Часть I
Краткое введение и настройка с помощью мастеров

1

Краткое знакомство с P-793H

В этой главе описаны основные характеристики и функции P-793H.

1.1 Общие сведения

P-793H представляет собой защищенный маршрутизатор G.SHDSL.bis со встроенным четырехпортовым коммутатором.

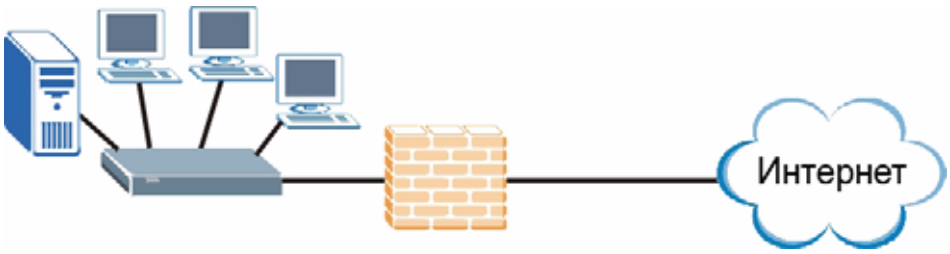
P-793H можно настроить для высокоскоростного доступа в Интернет или высокоскоростного двухточечного соединения с другими совместимыми устройствами P-793H. В обоих случаях P-793H может выступать в качестве маршрутизатора или моста.

Приложение A на стр. 387 содержит развернутый список функций, настраиваемых в P-793H.

1.1.1 Высокоскоростной доступ в Интернет

P-793H будет идеальным решением для высокоскоростного доступа в Интернет. Помимо других преимуществ, стандарт G.SHDSL.bis поддерживает одинаково высокую скорость передачи и приема, что отличает его от ADSL и VDSL.

Рис. 1 Высокоскоростной доступ в Интернет с P-793H

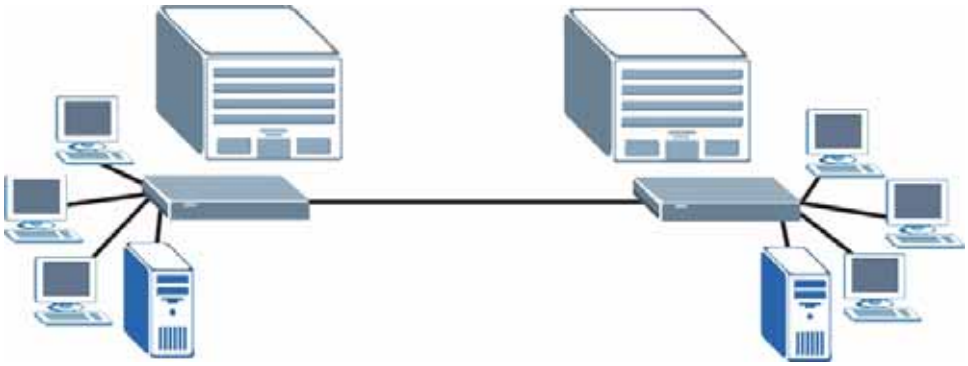


Для доступа в Интернет соедините порт DSL с телефонным портом. После этого подключите ваши компьютеры или серверы к портам LAN, чтобы обеспечить им совместный доступ в Интернет. (Подробные указания по подключению аппаратной части см. в Руководстве по быстрому запуску.) Далее настройте каждое устройство P-793H в режиме маршрутизатора или моста в зависимости от требуемой конфигурации. Работая в качестве маршрутизатора P-793H, обеспечивает такие функции, как межсетевой экран, фильтрация по содержанию сайтов и управление полосой пропускания. Применение P-793H в роли моста сводит к минимуму объем необходимых изменений в настройках существующей сети.

1.1.2 Высокоскоростные соединения по схеме "точка-точка"

С помощью двух устройств P-793H можно построить недорогое высокоскоростное соединение для таких требовательных к полосе пропускания задач, как видеоконференции и дистанционное обучение.

Рис. 2 Соединение по схеме "точка-точка" с помощью P-793H

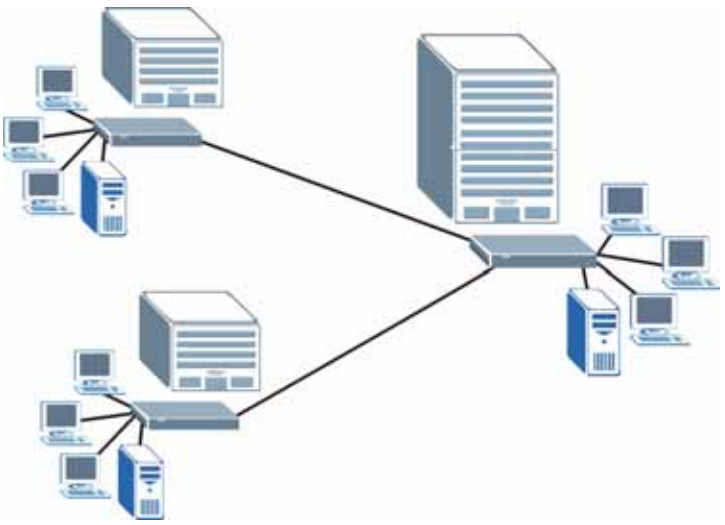


Устройства P-793H позволяют создавать простые и высокоскоростные двухточечные соединения между двумя территориально разнесенными сетями.

1.1.3 Высокоскоростные соединения по схеме "точка – две точки"

С помощью трех устройств P-793H можно соединить две сети с центральным узлом. Например, такая схема может быть использована для соединения двух филиалов со штаб-квартирой. В этом сценарии центральное устройство P-793H работает аналогично поставщику услуг Интернета.

Рис. 3 Соединение по схеме "точка – две точки" с помощью P-793H



Подробное описание соединений по схеме "точка-точка" и "точка – две точки" см. в гл. 4 на стр. 65.

1.2 Способы управления P-793H

Управлять устройством P-793H можно одним из следующих способов.

- Веб-конфигуратор. Это рекомендуемый способ решения повседневных задач управления устройством P-793H. Необходим только поддерживаемый веб-браузер. См. гл. 2 на стр. 43.
- Интерфейс командной строки. Командная строка используется для устранения неполадок инженерами сервисных служб. См. Приложение H на стр. 433.
- SMT. SMT (терминал управления системой) представляет собой текстовый интерфейс на основе меню, позволяющий настраивать устройство. См. гл. 21 на стр. 257.
- FTP. FTP (протокол передачи файлов) используется для обновления микропрограммы, а также резервного копирования и восстановления настроек. См. гл. 15 на стр. 211.
- SNMP. Для контроля и управления устройством можно применять диспетчер SNMP. См. гл. 15 на стр. 211.
- TR-069. Это стандарт, определяющий способы управления устройством P-793H через управляющий сервер. См. гл. 15 на стр. 211.

1.3 Рекомендации по управлению P-793H

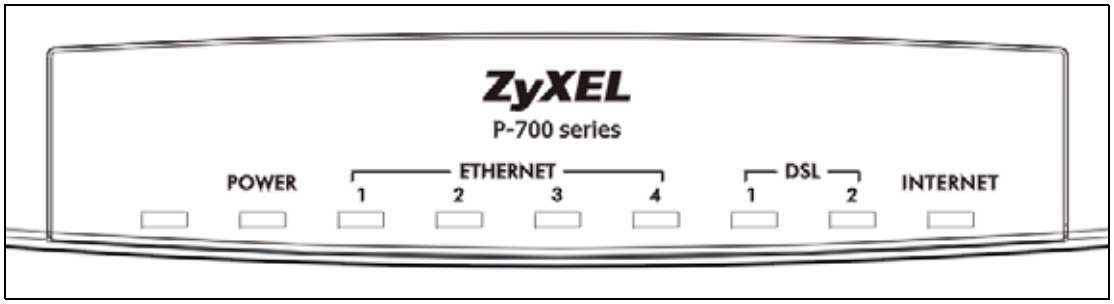
Чтобы максимально защитить P-793H и сделать управление P-793H более эффективным, регулярно выполняйте следующие профилактические операции.

- Меняйте пароль. Используйте пароли, которые сложно подобрать. Составляйте пароль из различных символов, например, цифр и букв.
- Записывайте пароли и храните их в защищенном месте.
- Выполняйте резервное копирование настроек (убедитесь в том, что вам известен способ их восстановления). Восстановление ранее работавших настроек может понадобиться, если устройство начнет работать неустойчиво или откажется функционировать. Если вы забудете пароль, потребуется восстановить заводские настройки P-793H. Наличие ранее сохраненного файла настроек означает, что вам не потребуется перенастраивать P-793H заново. Будет достаточно восстановить последние действовавшие настройки.

1.4 Светодиоды

На следующем рисунке изображено расположение светодиодов.

Рис. 4 Светодиоды



Назначение светодиодов описано в следующей таблице.

Таблица 1 Светодиоды

СВЕТОДИОДЫ	ЦВЕТ	СОСТОЯНИЕ	ОПИСАНИЕ
POWER	Зеленый	Вкл.	Устройство P-793H включено и функционирует исправно.
		Мигание	P-793H перезагружается или проходит диагностику.
	Красный	Вкл.	Для работы P-793H недостаточно питания.
		Выкл.	Система не готова или находится в состоянии сбоя.
LAN 1~4	Зеленый	Вкл.	Порт успешно подключен к Ethernet-сети.
		Мигание	Порт передает/принимает данные.
		Выкл.	Соединение на порту отсутствует.
DSL1/DSL2	Зеленый	Вкл.	DSL-соединение установлено.
		Мигание	P-793H инициализирует DSL-линию.
		Выкл.	DSL-линия разъединена.
Примечание. При доступе в Интернет или организации соединений по схеме "точка-точка" светодиоды DSL1 и DSL2 отображают состояние соединения в целом (работая как один светодиод). Для соединений по схеме "точка – две точки" светодиоды DSL1 и DSL2 отображают, соответственно, состояние соединений 1 и 2.			
INTERNET	Зеленый	Вкл.	Соединение с Интернетом установлено, и устройство P-793H получило IP-адрес. (Если P-793H организует соединение RFC 1483 в режиме моста, этот светодиод не загорается, но он мигает в то время. когда P-793H передает или принимает данные.)
		Мигание	P-793H передает/принимает данные.
	Красный	Вкл.	Устройство P-793H предприняло попытку получить IP-адрес, но возникла ошибка.
		Выкл.	Соединение с Интернетом не установлено.

2

Знакомство с веб-конфигуратором

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

2.1 Обзор веб-конфигуратора

Веб-конфигуратор имеет HTML-интерфейс, поэтому настраивать устройство P-793H 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.

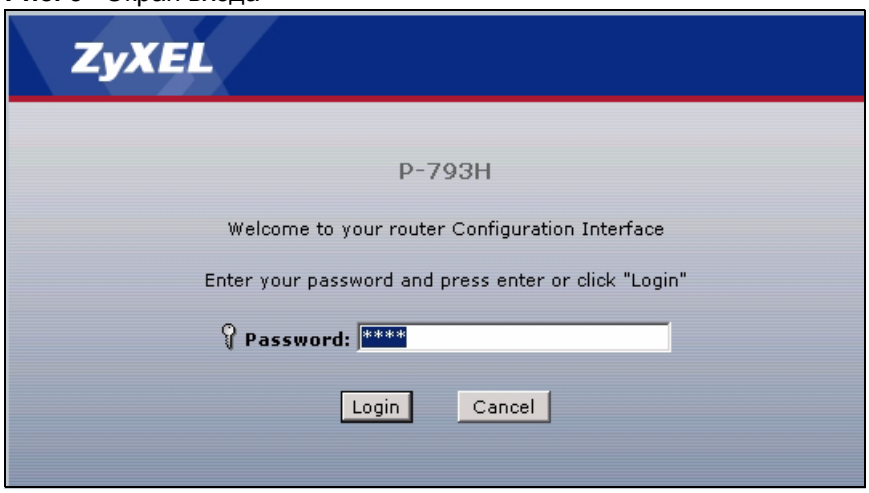
- На компьютере в веб-браузере нужно разрешить всплывающие окна. В операционной системе Windows XP SP с пакетом обновления 2 (SP2) всплывающие окна по умолчанию блокируются.
- Сценарии JavaScript (их выполнение разрешено по умолчанию).
- Разрешения на выполнение Java-кода (включены по умолчанию).

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

2.2 Вызов веб-конфигуратора

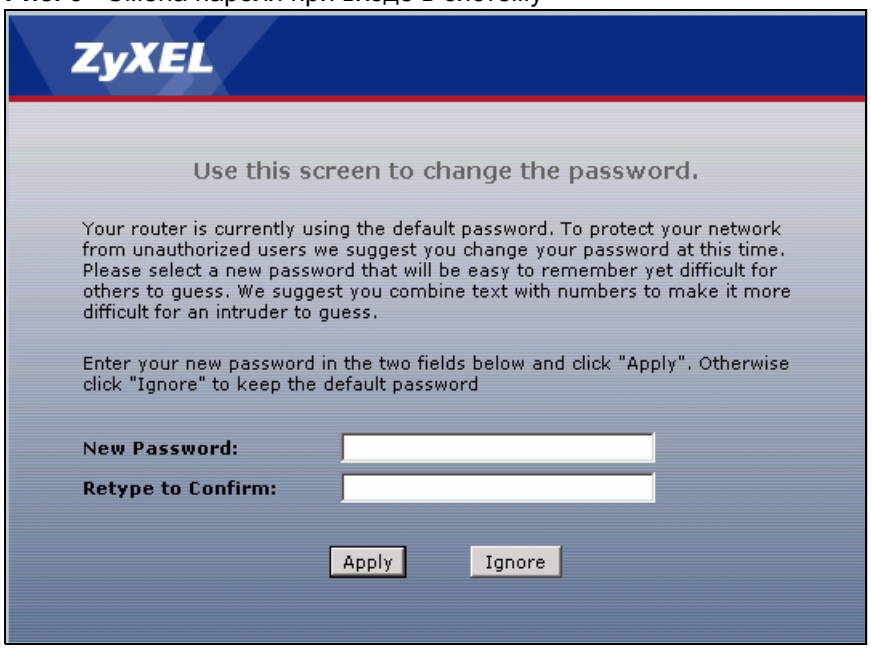
1. Убедитесь, что все аппаратные подключения P-793H выполнены правильно (см. Руководство по быстрому запуску).
2. Подготовьте компьютер/сеть для соединения с P-793H (см. Руководство по быстрому запуску).
3. Откройте веб-браузер.
4. Введите "192.168.1.1" в качестве URL.
5. Появляется экран, изображенный на следующем рисунке. Чтобы воспользоваться мастерами настройки или настроить дополнительные функции, введите пароль администратора по умолчанию: **1234**. Чтобы только просмотреть состояние устройства, введите пароль пользователя по умолчанию: **user**. Чтобы перейти на экран, на котором будет предложено изменить пароль, нажмите кнопку **Login**. Чтобы оставить устройство с паролем по умолчанию, выберите **Cancel**.

Рис. 5 Экран входа



6 Если был введен пароль пользователя, появится экран **Status**. См. разд. 2.4 на стр. 48. Если введен пароль администратора, появится изображенный ниже экран.

Рис. 6 Смена пароля при входе в систему

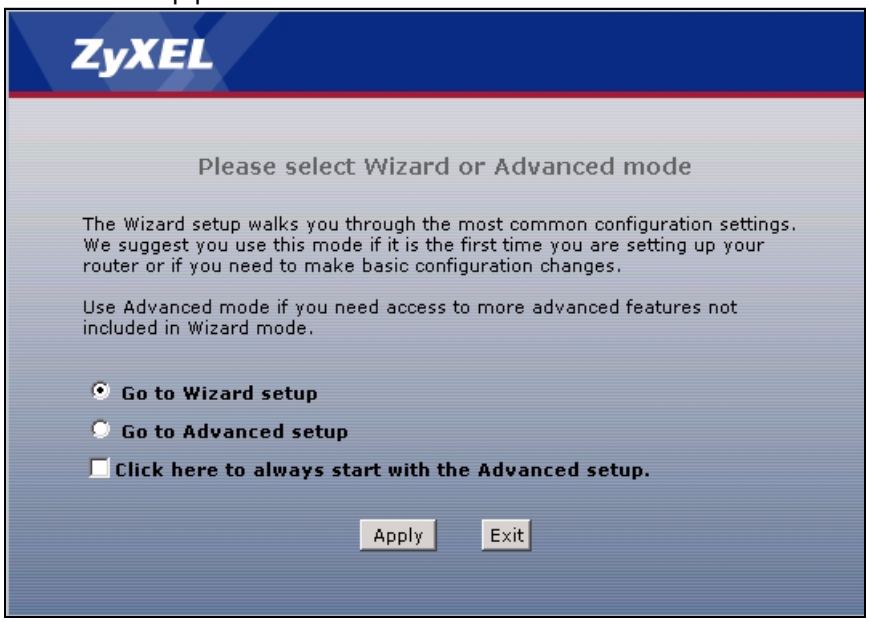


Настоятельно рекомендуется сменить пароль администратора по умолчанию. Введите новый пароль (от 1 до 30 знаков), повторно введите его для подтверждения и нажмите **Apply**. Если вы не хотите менять пароль, нажмите **Ignore**, чтобы перейти к главному меню.

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

7 Чтобы открыть основной экран мастера, выберите **Go to Wizard setup** и нажмите кнопку **Apply**. Для перехода на экран **Status** выберите **Go to Advanced setup** и нажмите кнопку **Apply**. Отметьте флажок **Click here to always start with the Advanced setup**, чтобы отключить этот экран. После этого устройство P-793H всегда будет открывать экран **Status**. См. разд. 2.4 на стр. 48.

Рис. 7 Выбор режима

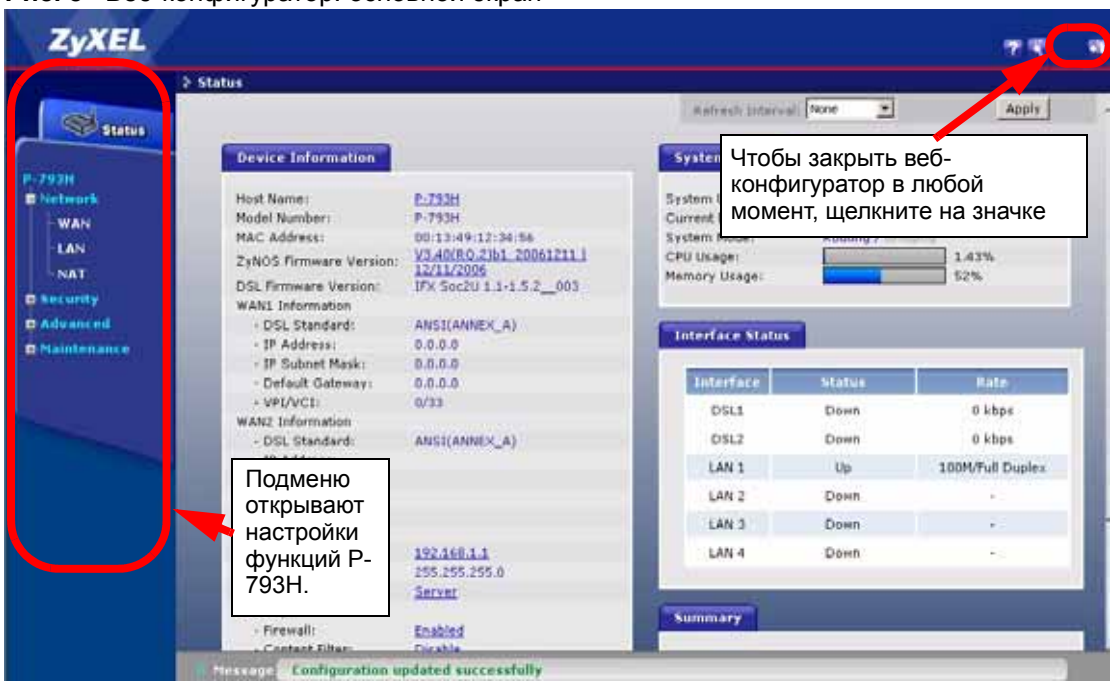


Сеанс управления автоматически прерывается по истечении периода неактивности, заданного в поле **Administrator Inactivity Timer** (по умолчанию – пять минут). В этом случае для возобновления сеанса достаточно повторно войти в управление P-793H.

2.3 Навигация в веб-конфигураторе

Введя пароль администратора, можно перейти к настройке функций P-793H через подменю на навигационной панели. Эти подменю описаны в следующей таблице.

Рис. 8 Веб-конфигуратор: основной экран



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

Таблица 2 Сводка экранов веб-конфигуратора

ССЫЛКА/ ЗНАЧОК	ПОДРАЗДЕЛ	НАЗНАЧЕНИЕ
Мастер	INTERNET SETUP	Эти экраны служат для запуска процесса начальной настройки, включающего общую настройку, установку параметров поставщика услуг Интернета и назначение IP-адреса в сети, DNS-сервера и MAC-адреса.
	BANDWIDTH MANAGEMENT SETUP	Эта группа экранов служит для ограничения полосы пропускания в зависимости от приложений и размера пакетов.
Logout		Этот значок служит для выхода из веб-конфигуратора.
Status		Этот экран позволяет просмотреть общее состояние устройства P-793H, сведения о системе и интерфейсах. На нем также доступны сводные таблицы статистики.
Network		
WAN	Internet Connection	Этот экран служит для настройки параметров поставщика услуг Интернета, присвоения IP-адресов в сети WAN, задания параметров DSL-линий, а также настройки прямых соединений по схемам "точка – точка" и "точка – две точки"
	More Connections	Этот экран служит для настройки и вызова удаленного межсетевого шлюза.
	WAN Backup Setup	Этот экран предназначен для настройки параметров переадресации трафика и резервирования WAN.

Таблица 2 Сводка экранов веб-конфигуратора (продолжение)

ССЫЛКА/ ЗНАЧОК	ПОДРАЗДЕЛ	НАЗНАЧЕНИЕ
LAN	IP	Этот экран служит для настройки параметров TCP/IP локальной сети и других дополнительных параметров.
	DHCP Setup	Этот экран служит для настройки параметров DHCP для локальной сети.
	Client List	Этот экран служит для просмотра текущих параметров DHCP-клиентов и привязки постоянных IP-адресов к определенным MAC-адресам (и именам хостов).
	IP Alias	Этот экран служит для разделения интерфейса LAN на подсети.
NAT	General	Этот экран служит для активации NAT.
	Port Forwarding	Этот экран служит для настройки серверов, находящихся во внутренней сети за P-793H.
	Address Mapping	Этот экран позволяет настроить параметры привязки для трансляции сетевых адресов.
Security		
Firewall	General	Этот экран служит для включения/отключения межсетевого экрана и выбора правил, выполняемых над сетевым трафиком в определенных направлениях.
	Rules	Этот экран содержит сводку правил межсетевого экрана и позволяет редактировать/добавлять правила.
	Anti Probing	Этот экран позволяет изменить настройки защиты от зондирования.
	Threshold	Этот экран служит для настройки порога защиты от DoS-атак.
Content Filter	Keyword	Этот экран служит для блокирования доступа к сайтам по определенным ключевым словам в URL.
	Schedule	Этот экран служит для задания дней и периодов в течение дня, в которые P-793H осуществляет фильтрацию содержания.
	Trusted	Этот экран позволяет в исключительном порядке отменить на P-793H 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		
Static Route	Static Route	Этот экран служит для настройки статических IP-маршрутов.
Bandwidth MGMT	Summary	Этот экран активирует управление полосой пропускания на интерфейсе.
	Rule Setup	Этот экран служит для настройки правила управления полосой пропускания.
	Monitor	По этой ссылке можно просмотреть полосу пропускания, используемую P-793H, и доли распределения полосы пропускания.
Dynamic DNS	Dynamic DNS	Этот экран служит для настройки DNS для динамических адресов.

Таблица 2 Сводка экранов веб-конфигуратора (продолжение)

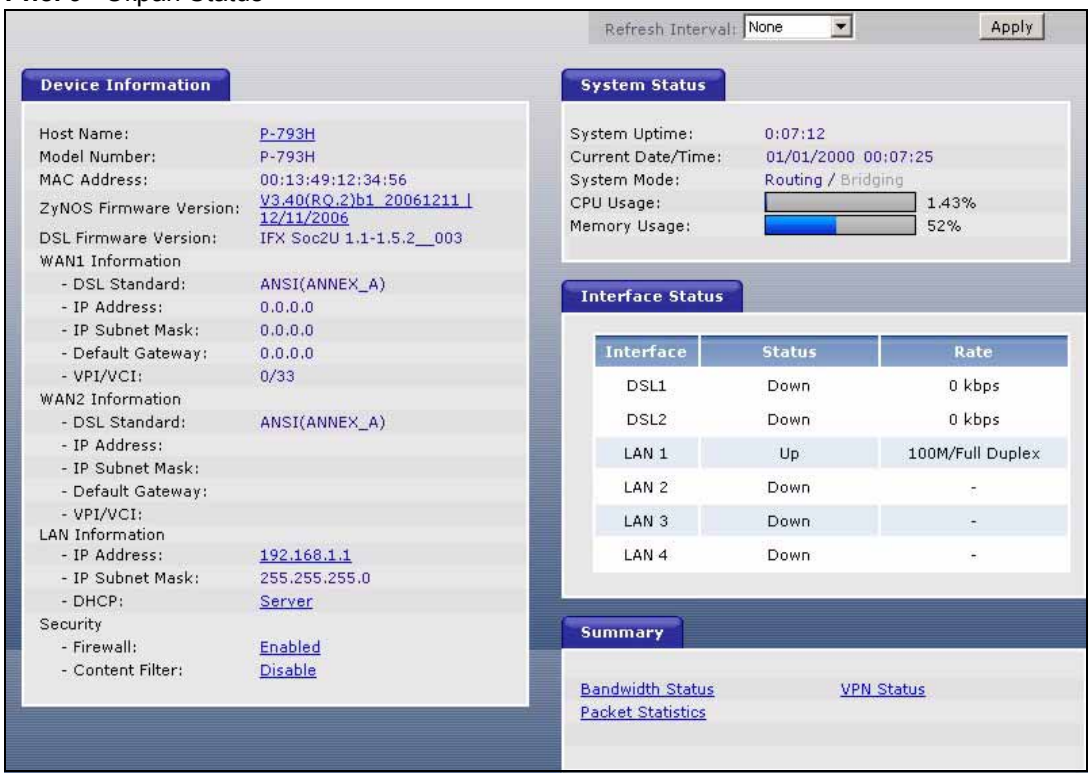
ССЫЛКА/ ЗНАЧОК	ПОДРАЗДЕЛ	НАЗНАЧЕНИЕ
Remote MGMT	WWW	Этот экран позволяет выбрать интерфейсы и пользователей (IP-адреса), которым разрешается управлять устройством P-793H по протоколам HTTPS и HTTP.
	Telnet	Этот экран позволяет выбрать интерфейсы и пользователей (IP-адреса), которым разрешается управлять устройством P-793H по протоколу Telnet.
	FTP	Этот экран позволяет выбрать интерфейсы и пользователей (IP-адреса), которым разрешается управлять устройством P-793H по протоколу FTP.
	SNMP	Этот экран служит для настройки параметров управления P-793H по упрощенному протоколу управления сетью (SNMP).
	DNS	Этот экран позволяет выбрать интерфейсы и пользователей (IP-адреса), которым разрешается направлять DNS-запросы на P-793H.
	ICMP	Этот экран позволяет изменить настройки защиты от зондирования.
UPnP	General	Этот экран позволяет включить или отключить поддержку UPnP в P-793H.
Maintenance		
System	General	Этот экран содержит административную и относящуюся к системе информацию, а также позволяет изменить пароль.
	Time Setting	Это окно служит для настройки даты и времени в P-793H.
Logs	View Log	Этот экран служит для просмотра журналов по выбранным категориям.
	Log Settings	Этот экран служит для настройки ведения журналов в P-793H.
Tools	Firmware	Этот экран служит для загрузки микропрограмм в P-793H.
	Configuration	Этот экран служит для резервного копирования и восстановления файлов настроек или восстановления заводской конфигурации P-793H.
	Restart	Этот экран служит для перезагрузки P-793H без выключения питания.
Diagnostic	General	На этом экране отображаются данные, которые могут помочь вам при диагностике общих проблем, связанных с подключением P-793H.
	DSL Line	На этом экране отображаются данные, которые будут полезны для диагностики DSL-линии.

2.4 Экран состояния (Status)

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

Некоторые поля и ссылки недоступны, если на экране входа был введен пользовательский пароль (см. рис. 5 на стр. 44).

Рис. 9 Экран Status



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

Таблица 3 Экран Status

ПОЛЕ	ОПИСАНИЕ
Refresh Interval	В раскрывающемся списке выберите число секунд, чтобы автоматически обновлять статистику на экране с заданным интервалом, или **None**, чтобы отключить автоматическое обновление.
Apply	Выберите эту кнопку, чтобы обновить статистику на экране.
Device Information	
Host Name	Это имя системы, введенное в поле **System Name** на экране **Maintenance**, **System**, **General**. Оно необходимо в целях идентификации.
Model Number	В этом поле отображается наименование модели P-793H.
MAC Address	В этом поле отображается уникальный MAC или Ethernet-адрес P-793H.
ZyNOS Firmware Version	Это – версия и дата создания микропрограммы ZyNOS. ZyNOS является патентованной разработкой сетевой операционной системы ZyXEL.
DSL Firmware Version	В этом поле отображается версия и дата создания используемой микропрограммы P-793H. Эта информация может потребоваться техническим специалистам для диагностики неисправностей.
WAN1/WAN2 Information	Если настроено соединение по схеме "точка – две точки", информация о сети WAN будет выводиться для обоих соединений: DSL 1 и DSL 2.
DSL Standard	В этом поле отображается стандарт DSL, используемый устройством P-793H.
IP Address	В этом поле указан IP-адрес порта WAN.
IP Subnet Mask	В этом поле отображается маска подсети порта WAN.
Default Gateway (Основной шлюз)	В этом поле отображается IP-адрес шлюза по умолчанию, если он применим.

Таблица 3 Экран Status (продолжение)

ПОЛЕ	ОПИСАНИЕ
VPI/VCI	В этом поле отображаются идентификаторы виртуального пути и виртуального канала, введенные на экране WAN.
LAN Information	
IP Address	В этом поле указан IP-адрес порта LAN.
IP Subnet Mask	В этом поле отображается маска подсети порта LAN.
DHCP	В этом поле отображается роль DHCP для порта WAN: **Server** (сервер), **Relay** (ретрансляция) или **None** (нет).
Security	При входе в веб-конфигуратор с паролем пользователя этот раздел недоступен.
Firewall	В этом поле сообщается, активирован ли межсетевой экран P-793H.
Content Filter	В этом поле сообщается, активирована ли фильтрация содержимого.
System Status	
System Uptime	В этом поле отображается суммарная продолжительность работы P-793H.
Current Date/Time	В этом поле отображаются текущие дата и время по часам P-793H.
System Mode	В этом поле отображается режим работы P-793H: маршрутизатор (router) или мост (bridge).
CPU Usage	Это число характеризует объем хипа, используемый P-793H (в килобайтах). Хип – это оперативная память, которая не используется для системных нужд ZyNOS (сетевой операционной системы ZyXEL) и доступна таким активным процессам, как NAT, VPN и межсетевой экран. В этом поле отображается объем хипа, используемый P-793H (в процентах). Когда объем приближается к максимуму, индикатор меняет цвет с зеленого на красный.
Memory Usage	В этом поле отображается суммарный объем хипа в P-793H (в килобайтах). В этом поле отображается объем хипа, используемый P-793H (в процентах). Когда объем приближается к максимуму, индикатор меняет цвет с зеленого на красный.
Interface Status	
Interface	В этом разделе отображаются интерфейсы P-793H.
Status	В этом поле отображается состояние: **Down** (канал разъединен), **Up** (канал соединен), если используется инкапсуляция Ethernet, и **Down** (канал разъединен), **Up** (канал соединен), **Idle** (соединение (ppp-сеанс) неактивно), **Dial** (начало вызова) и **Drop** (прерывание вызова), если используется инкапсуляция PPPoE.
Rate	Для портов LAN в этом поле отображается скорость порта и используемый режим дуплекса. Порты Ethernet могут быть подключены в полудуплексном (half) или полнодуплексном (full) режиме. Полнодуплексный режим позволяет устройству одновременно передавать и получать информацию, а в полудуплексном режиме информация в каждый момент времени может идти только в одном направлении. Параметры скорости и режима дуплекса для Ethernet-порта должны совпадать с параметрами, используемыми Ethernet-портом на другой стороне соединения. Возможность одновременной передачи по одному порту в обоих направлениях (полный дуплекс) фактически удваивает полосу пропускания. Для порта WAN сообщается скорость передачи по нисходящему и восходящему каналу. Этот параметр отображается для обоих соединений: DSL 1 и DSL 2.
Summary	При входе в веб-конфигуратор с паролем пользователя этот раздел недоступен.
Bandwidth Status	По этой ссылке можно просмотреть полосу пропускания, используемую P-793H, и доли распределения полосы пропускания.
Packet Statistics	Этот экран позволяет просмотреть состояние портов и статистику по пакетам.
VPN Status	Этот экран служит для просмотра текущего состояния туннелей VPN, установленных P-793H.

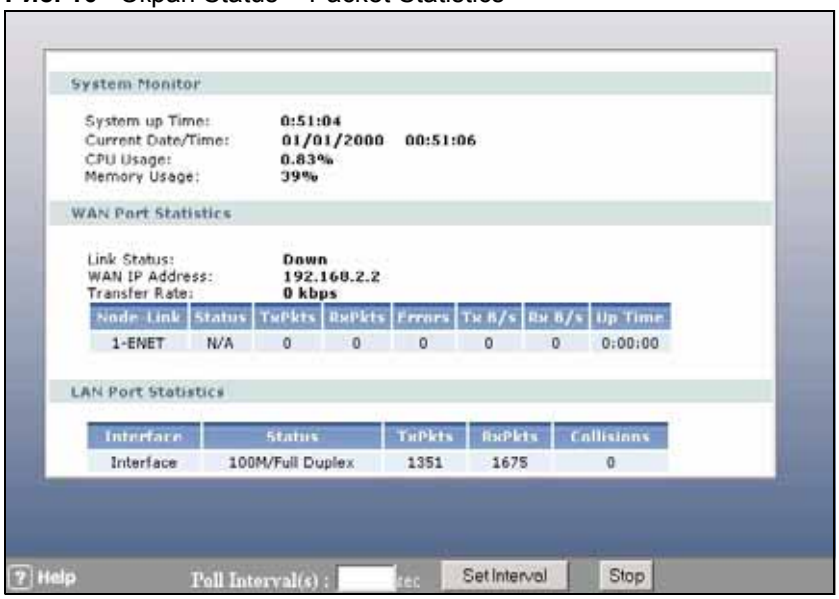
2.4.1 Раздел Status: Bandwidth Status

Этот экран рассмотрен на рис. 97 на стр. 205.

2.4.2 Раздел Status: Packet Statistics

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

Рис. 10 Экран Status > Packet Statistics



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 4 Экран Status > Packet Statistics

ПОЛЕ	ОПИСАНИЕ
System Monitor	
System up Time	В этом поле отображается суммарная продолжительность работы системы.
Current Date/Time	В этом поле отображаются текущие дата и время по часам P-793H.
CPU Usage	В этом поле отображается загрузка ЦП (в процентах).
Memory Usage	В этом поле отображается объем используемой оперативной памяти (в процентах).
WAN Port Statistics	
Link Status	В этом поле отображается состояние соединения с WAN.
WAN IP Address	В этом поле отображается IP-адрес в сети WAN, присвоенный устройству P-793H.
Transfer Rate	В этом поле отображается скорость обмена информацией с P-793H.
Node-Link	В этом поле отображается порядковый номер и тип соединения с удаленным узлом. Возможны следующие типы соединений: PPPoA, ENET, RFC 1483 и PPPoE.

Таблица 4 Экран Status > Packet Statistics (продолжение)

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

2.4.3 Раздел Status: VPN Status

Этот экран рассмотрен на рис. 86 на стр. 185.

2.5 Сброс P-793H

Если вы забыли пароль или не можете получить доступ к веб-конфигуратору, воспользуйтесь кнопкой **RESET** на задней панели P-793H для восстановления заводских настроек. При этом будут потеряны все настройки, выполненные ранее, а в качестве пароля будет восстановлен "1234".

2.5.1 Использование кнопки сброса

1. Убедитесь, что светодиод **POWER** горит (не мигает).
2. Нажмите кнопку **RESET** и удерживайте ее в течение приблизительно десяти секунд или до тех пор, пока светодиод **PWR** не начнет мигать, после чего отпустите кнопку. Когда светодиод **POWER** начинает мигать, это значит, что значения по умолчанию восстановлены, и устройство P-793H перезагружается.

3

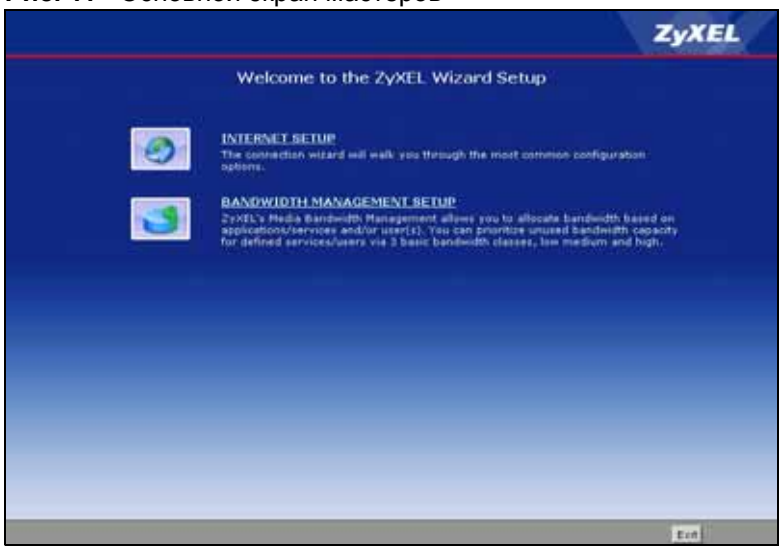
Мастера

Эти экраны служат для настройки доступа в Интернет и базовых параметров управления полосой пропускания.

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

Чтобы перейти к мастерам, выберите **Go to Wizard setup** (см. рис. 7 на стр. 45) или щелкните на значке мастера ( ) в правом верхнем углу веб-конфигуратора. Появится основной экран мастеров.

Рис. 11 Основной экран мастеров



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 5 Основной экран мастеров

ПОЛЕ	ОПИСАНИЕ
INTERNET SETUP	Выберите этот мастер для настройки доступа в Интернет. См. разд. 3.1 на стр. 54.

Таблица 5 Основной экран мастеров

ПОЛЕ	ОПИСАНИЕ
BANDWIDTH MANAGEMENT SETUP	Выберите этот мастер для упрощенной настройки управления полосой пропускания. См. разд. 3.2 на стр. 59.
Exit	Щелкните здесь, чтобы закрыть основной экран мастеров и вернуться на экран **Status** или в основное окно.

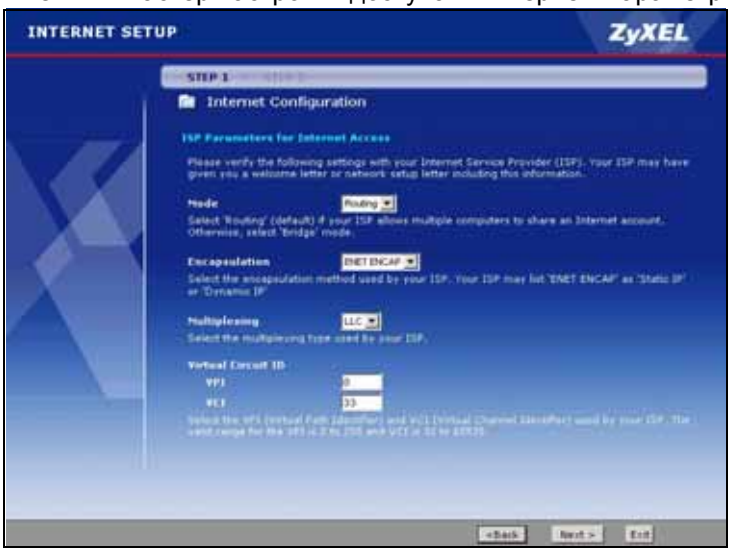
3.1 Мастер настройки доступа в Интернет

Эта группа экранов служит для настройки параметров доступа в Интернет. Для вызова этого мастера выберите **INTERNET SETUP** на основном экране мастеров.

3.1.1 Экран 1

На этом экране можно задать некоторые параметры поставщика услуг Интернета.

Рис. 12 Мастер настройки доступа в Интернет: параметры поставщика услуг Интернета



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 6 Мастер настройки доступа в Интернет: параметры поставщика услуг Интернета

ПОЛЕ	ОПИСАНИЕ
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 **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**.
Multiplexing	Выберите тип инкапсуляции, используемый поставщиком услуг Интернета, из раскрывающегося списка **Multiplex**: VC-based (мультиплексирование на основе виртуальных каналов) или LLC-based (мультиплексирование на основе управления логическим каналом связи).

Таблица 6 Мастер настройки доступа в Интернет: параметры поставщика услуг Интернета

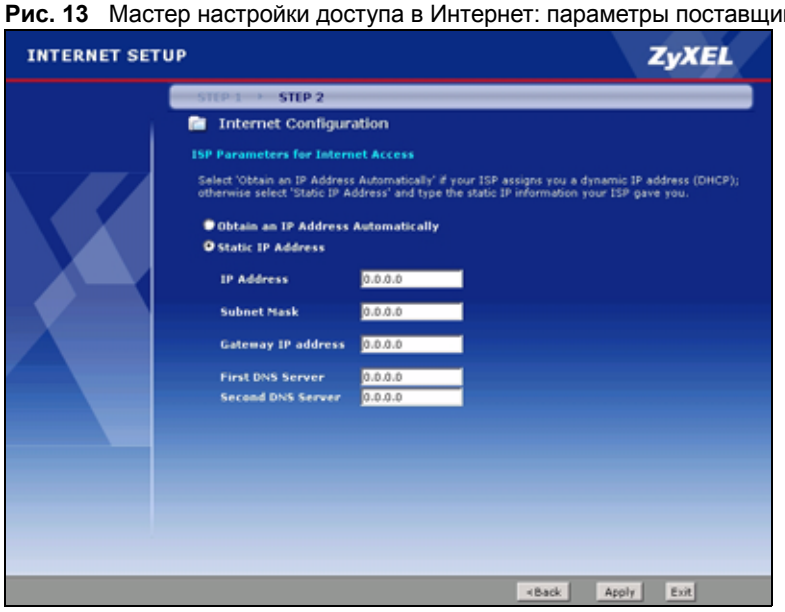
ПОЛЕ	ОПИСАНИЕ
Virtual Circuit ID	Совокупность VPI (идентификатора виртуального пути) и VCI (идентификатора виртуального канала) определяет виртуальную цепь. Подробное описание см. в приложении.
VPI	Введите присвоенный вам VPI. Это поле могло быть настроено заранее.
VCI	Введите присвоенный вам VCI. Это 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 и режима инкапсуляции, выбранных выше.
Exit	Чтобы закрыть экран мастера, не внося изменений, выберите **Exit**.

3.1.2 Экран 2

Эта группа экранов позволяет задать остальные параметры доступа в Интернет, которые будут зависеть от типа инкапсуляции, используемого для соединения с Интернетом (а также режима, выбранного для RFC1483).

Этот экран появляется только для соединений, использующих инкапсуляцию Ethernet.

Рис. 13 Мастер настройки доступа в Интернет: параметры поставщика услуг Интернета (Enternet)



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 7 Мастер настройки доступа в Интернет: параметры поставщика услуг Интернета (Enternet)

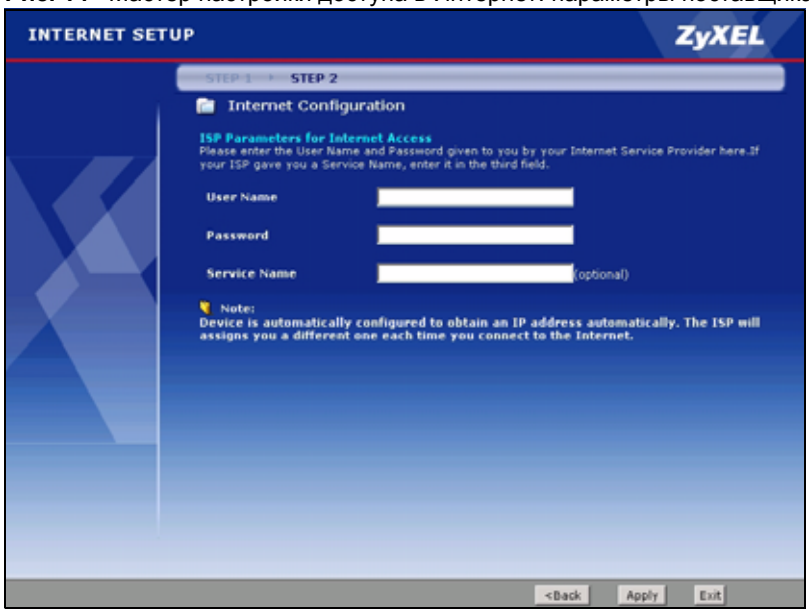
ПОЛЕ	ОПИСАНИЕ
Obtain an IP Address Automatically	Выберите этот вариант, если IP-адрес вам назначается динамически.
Static IP Address	Выберите этот вариант, если вам выделен статический IP-адрес, и введите его ниже.
	Эти поля появляются, если выбран статический адрес (**Static IP Address**).

Таблица 7 Мастер настройки доступа в Интернет: параметры поставщика услуг Интернета (Enternet)

ПОЛЕ	ОПИСАНИЕ
IP Address	Введите статический IP-адрес, предоставленный поставщиком услуг Интернета.
Subnet Mask	Введите маску подсети, предоставленную поставщиком услуг Интернета.
Gateway IP Address	Введите IP-адрес шлюза, предоставленный поставщиком услуг Интернета. Если поставщик услуг Интернета не предоставил соответствующей информации, оставьте значение по умолчанию.
First DNS Server Second DNS Server	Введите IP-адреса одного или двух DNS-серверов, предоставленные поставщиком услуг Интернета. Оставьте значения по умолчанию во втором или обоих полях, если поставщик услуг Интернета не предоставил соответствующей информации.
Back	Для возврата к предыдущему экрану нажмите кнопку **Back**.
Apply	Для завершения ручной настройки нажмите кнопку **Apply**.
Exit	Чтобы закрыть экран мастера, не внося изменений, выберите **Exit**.

Этот экран появляется только для соединений, использующих инкапсуляцию PPPoE.

Рис. 14 Мастер настройки доступа в Интернет: параметры поставщика услуг Интернета (PPPoE)



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 8 Мастер настройки доступа в Интернет: параметры поставщика услуг Интернета (PPPoE)

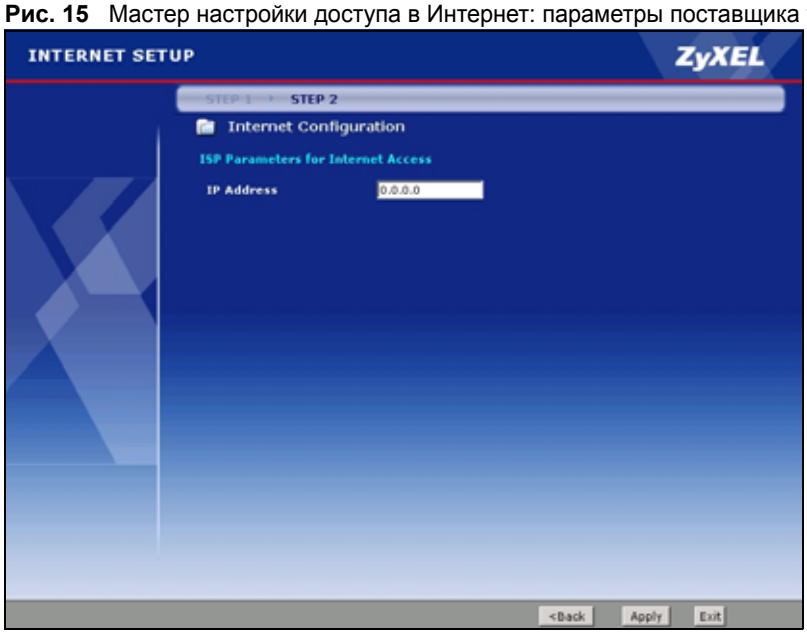
ПОЛЕ	ОПИСАНИЕ
User Name	Введите имя пользователя в точности так, как оно указано поставщиком услуг. Если поставщик присвоил имя пользователя в формате пользователь@домен, где доменом является название службы, следует ввести оба компонента в точном соответствии с указаниями.
Password	Введите пароль, связанный с указанным выше именем пользователя.
Service Name	Введите название службы PPPoE. Если поставщик услуг Интернета не поддерживает сеансов PPPoE, оставьте это поле пустым.
Back	Для возврата к предыдущему экрану нажмите кнопку **Back**.

Таблица 8 Мастер настройки доступа в Интернет: параметры поставщика услуг Интернета (PPPoE)

ПОЛЕ	ОПИСАНИЕ
Apply	Для завершения ручной настройки нажмите кнопку **Apply**.
Exit	Чтобы закрыть экран мастера, не внося изменений, выберите **Exit**.

Этот экран появляется только для соединений, использующих инкапсуляцию RFC1483.

Рис. 15 Мастер настройки доступа в Интернет: параметры поставщика услуг Интернета (RFC1483)



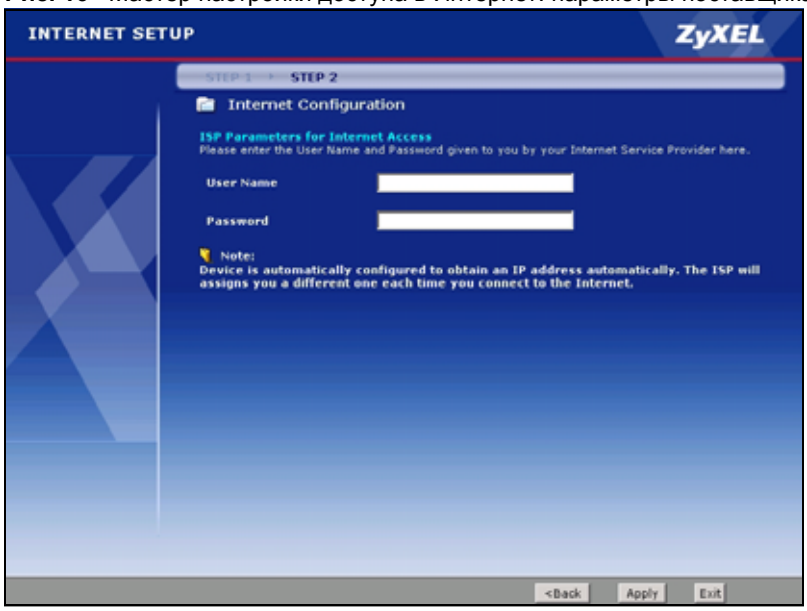
Поля изображенного выше экрана описаны в следующей таблице.

Таблица 9 Мастер настройки доступа в Интернет: параметры поставщика услуг Интернета (RFC1483)

ПОЛЕ	ОПИСАНИЕ
IP Address	Введите статический IP-адрес, предоставленный поставщиком услуг Интернета.
Back	Для возврата к предыдущему экрану нажмите кнопку **Back**.
Apply	Для завершения ручной настройки нажмите кнопку **Apply**.
Exit	Чтобы закрыть экран мастера, не внося изменений, выберите **Exit**.

Этот экран появляется только для соединений, использующих инкапсуляцию PPPoA.

Рис. 16 Мастер настройки доступа в Интернет: параметры поставщика услуг Интернета (PPPoA)



Поля изображенного выше экрана описаны в следующей таблице.

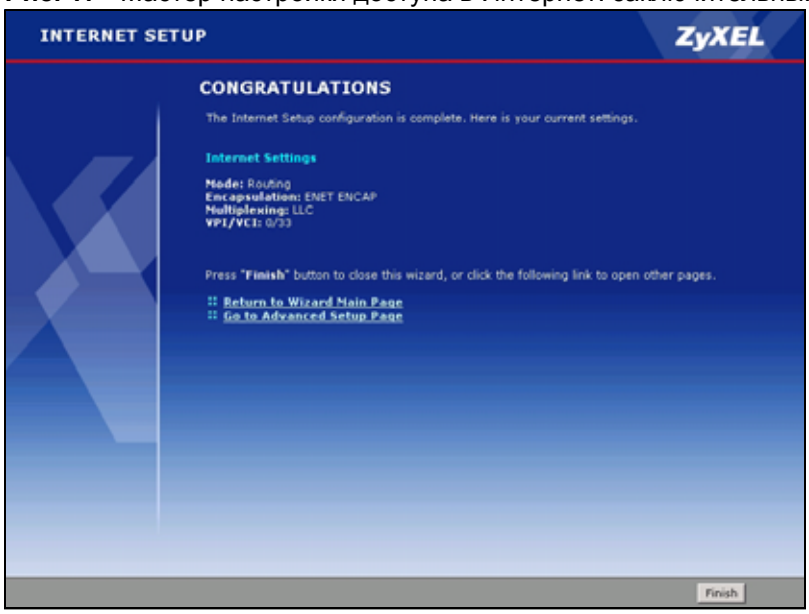
Таблица 10 Мастер настройки доступа в Интернет: параметры поставщика услуг Интернета (PPPoA)

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.
Back	Для возврата к предыдущему экрану нажмите кнопку **Back**.
Apply	Для завершения ручной настройки нажмите кнопку **Apply**.
Exit	Чтобы закрыть экран мастера, не внося изменений, выберите **Exit**.

3.1.3 Экран 3

Следующий экран появляется при завершении работы с мастером **Internet Setup**.

Рис. 17 Мастер настройки доступа в Интернет: заключительный экран



3 Проверьте правильность ваших настроек по сводной таблице (таблица доступна только для чтения). Чтобы закрыть мастера и сохранить настройки, нажмите кнопку **Finish**. Назначение полей этого экрана описано в следующей таблице.

Таблица 11 Мастер настройки доступа в Интернет: сводный экран

ПОЛЕ	ОПИСАНИЕ
Return to Wizard Main Page	Выберите эту ссылку, чтобы вернуться к основной странице мастеров. См. рис. 11 на стр. 53.
Go to Advanced Setup Page	Выберите эту ссылку, чтобы вернуться к основному окну. См. рис. 8 на стр. 46.
Finish	Щелкните здесь, чтобы закрыть основной экран мастеров и вернуться на экран **Status** или в основное окно.

Запустите браузер и откройте сайт www.zyxel.ru. Если вы не можете получить доступ к Интернету, снова откройте веб-конфигуратор и проверьте правильность настроек, указанных вами в мастерах.

Доступ в Интернет – это только начало. Ознакомьтесь с остальными главами этого руководства, чтобы подробнее узнать о всех возможностях P-793H.

3.2 Мастер управления полосой пропускания

Следующие экраны позволяют контролировать суммарную полосу пропускания порта WAN P-793H и упорядочивать распределение полосы пропускания по приоритетам. Это помогает исключить ситуации, когда одна служба или приложение забирает всю полосу пропускания, блокируя работу других служб.

В следующей таблице описаны службы, которые позволяет выбрать мастер.

Таблица 12 Настройка управления полосой пропускания: службы

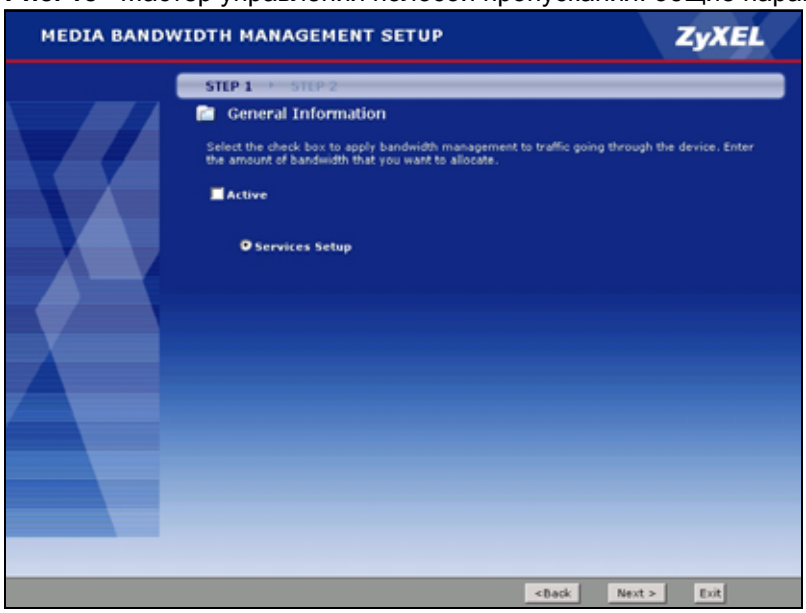
СЛУЖБА	ОПИСАНИЕ
E-Mail	Электронная почта состоит из сообщений, рассылаемых по компьютерной сети определенным группам или людям. По умолчанию для электронной почты часто используются следующие порты: POP3 - порт 110, IMAP - порт 143, SMTP – порт 25, HTTP - порт 80.
FTP	Протокол передачи файлов используется для пересылки файлов, в особенности – больших объемов данных, которые невозможно передать по электронной почте. Для FTP используется порт 21.
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 аудио-, видеопотоков 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 (H.323)	Передача сигналов речевого диапазона по Интернету называется IP-телефонией (VoIP). H.323 – стандартный набор протоколов конференц-связи для передачи аудио-, видеопотоков 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.
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.
TFTP	TFTP (упрощенный протокол пересылки файлов) – протокол передачи файлов в Интернете, подобный FTP, но использующий UDP (протокол пользовательских датаграмм) вместо TCP (протокол управления передачей).
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.

Для доступа к этому мастеру войдите в веб-конфигуратор (см. разд. 2.2 на стр. 43) и нажмите кнопку **BANDWIDTH MANAGEMENT SETUP** на основном экране мастера.

3.2.1 Экран 1

Этот экран активирует управление полосой пропускания для последующего распределения полосы между различными сетевыми службами.

Рис. 18 Мастер управления полосой пропускания: общие параметры



Поля изображенного выше экрана описаны в следующей таблице.

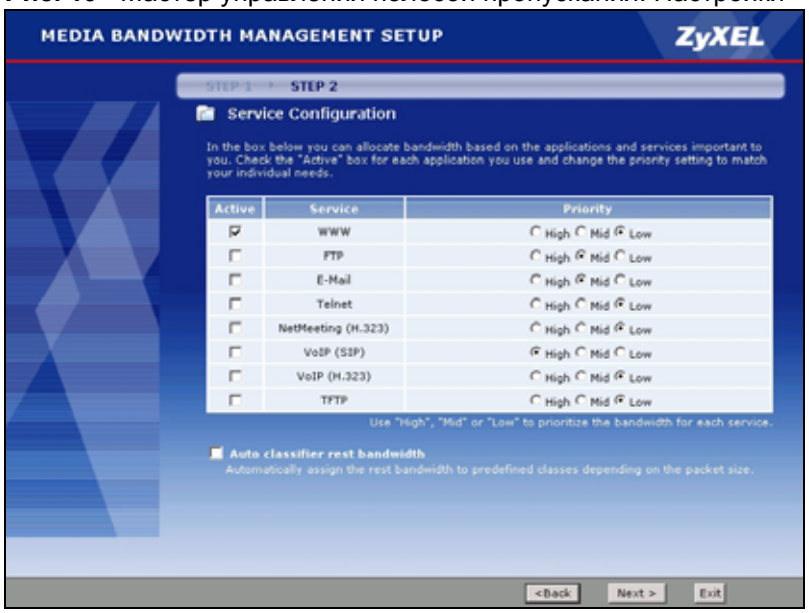
Таблица 13 Мастер управления полосой пропускания: общие параметры

ПОЛЕ	ОПИСАНИЕ
Active	Отметьте флажок **Active**, чтобы разрешить P-793H применять управление полосой пропускания к исходящим пакетам на портах WAN или LAN устройства P-793H. Если этот флажок не выбран, остальные экраны мастера не будут показаны.
Services Setup	Чтобы распределить полосу пропускания между различными сетевыми службами, выберите **Services Setup**.
Back	Нажмите кнопку **Back (Назад)**, чтобы вернуться к предыдущему экрану.
Next	Нажмите кнопку **Next** (Далее) для перехода к следующему экрану.
Exit	Чтобы закрыть экран мастера, не сохраняя изменений, выберите **Exit**.

3.2.2 Экран 2

На втором экране мастера выберите сетевые службы, к которым следует применять управление полосой пропускания, и отметьте приоритеты, назначаемые перечисленным службам.

Рис. 19 Мастер управления полосой пропускания: Настройки



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 14 Мастер управления полосой пропускания: Настройки

ПОЛЕ	ОПИСАНИЕ
Active	Чтобы включить управление полосой пропускания для конкретной службы/ приложения, отметьте флажок **Active**.
Service	В этих полях перечислены названия служб.
Priority	Выберите приоритет, который P-793H будет назначать трафику соответствующих служб: **High**, **Mid** или **Low**. Службы с высоким приоритетом (**High**) получают всю требуемую 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 настраиваемые правила были переопределены на экране **Advanced** > **Bandwidth MGMT** > **Rule Setup**, то переключатель приоритета будет установлен в положение **User Configured** (Настроено пользователем). Эти настройки можно впоследствии отредактировать на экране **Advanced** > **Bandwidth MGMT** > **Rule Setup** .
Auto classifier rest bandwidth	Установите флажок **Auto classifier rest bandwidth**, чтобы автоматически распределять невыделенную или неиспользуемую полосу пропускания между сетевыми службами с учетом типа пакетов.
Back	Для возврата к предыдущему экрану нажмите кнопку **Back**.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-793H.
Exit	Чтобы закрыть экран мастера, не внося изменений, выберите **Exit**.

3.2.3 Экран 3

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

Рис. 20 Мастер управления полосой пропускания: завершение работы

4

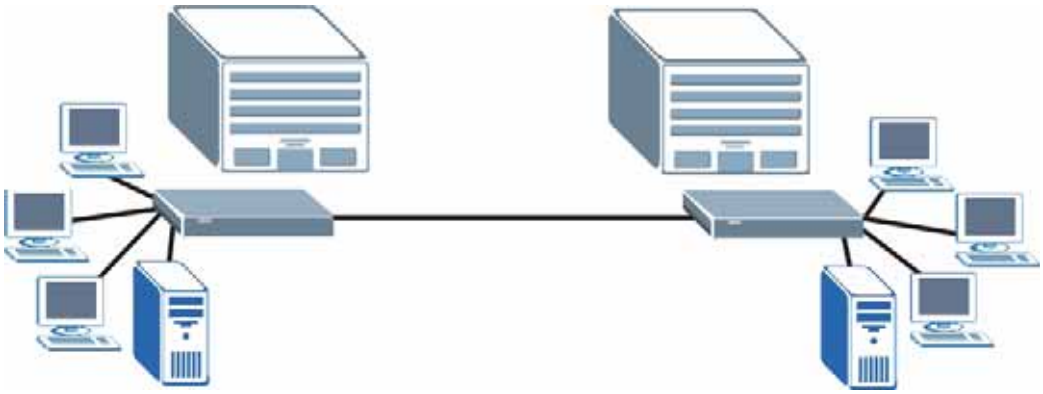
Прямые соединения

В этой главе рассмотрены соединения по схеме "точка-точка" и "точка – две точки".

4.1 Соединения по схеме "точка-точка"

Между двумя устройствами P-793H можно установить соединение по схеме "точка-точка". Это недорогой вариант высокоскоростного канала для таких требовательных к полосе пропускания задач, как видеоконференции и дистанционное обучение. Ниже показан пример такого соединения.

Рис. 21 Пример: обзор соединений по схеме "точка-точка"



В соединении по схеме "точка-точка" DSL-порты обоих устройств P-793H напрямую соединены друг с другом и не используются для подключения к поставщику услуг Интернета.

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

В соединении "точка-точка" оба P-793H должны использовать одинаковые VPI, VCI, режим мультиплексирования и метод инкапсуляции.

При установлении соединения по схеме "точка-точка" одно из устройств P-793H становится сервером (заменяя поставщика услуг Интернета). Сервер управляет некоторыми параметрами DSL-соединения, включая скорости передачи и режим работы DSL. В остальном различия между сервером и клиентом отсутствуют. Любая из сторон может инициировать соединение по схеме "точка-точка".

Соединения по схеме "точка-точка" могут устанавливаться только между устройствами P-793H, поддерживающими такой клиент-серверный режим.

4.2 Настройка соединения по схеме "точка-точка"

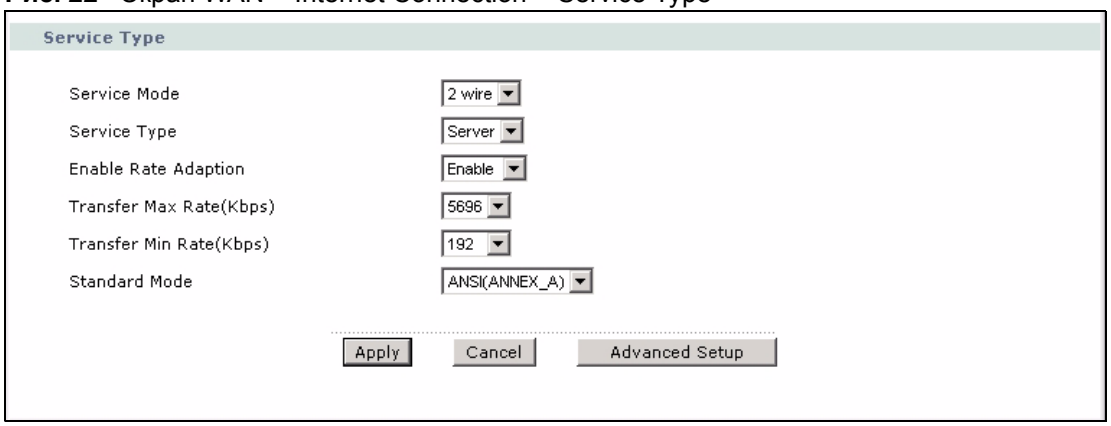
Ниже приведены указания для установления соединения по схеме "точка-точка".

1. Настройка сервера.
2. Настройка клиента.
3. Соединение двух устройств P-793H.

4.2.1 Настройка сервера

1. Войдите в управление устройством P-793H, которое будет выступать в качестве сервера. (См. гл. 2 на стр. 43.)
2. Выберите **Network > WAN > Internet Connection**.
3. В полях **VPI**, **VCI**, **Multiplexing** и **Encapsulation** укажите параметры, которые будут использоваться для прямого соединения. В поле **Encapsulation** выберите режим инкапсуляции: **RFC 1483** или **ENET ENCAP**.
4. Пролистайте экран до раздела **Service Type**. Появится изображенный ниже экран.

Рис. 22 Экран WAN > Internet Connection > Service Type



5 В поле **Service Mode** выберите двух- или четырехпроводную телефонную линию (2-wire или 4-wire).
6 В поле **Service Type** выберите **Server**. Станут доступны остальные поля экрана.
7 Заполните необходимые оставшиеся поля. В частности, можно ограничить максимальную скорость передачи в поле **Transfer Max Rate**.
8 Выберите **Apply**.

4.2.2 Настройка клиента

1 Войдите в управление устройством P-793H, которое будет выступать в качестве клиента. (См. гл. 2 на стр. 43.)
2 Выберите **Network > WAN > Internet Connection**.
3 В полях **VPI**, **VCI**, **Multiplexing** и **Encapsulation** продублируйте значения, заданные на сервере.
4 Пролистайте экран до раздела **Service Type**. См. выше рис. 22 на стр. 66.
5 В поле **Service Mode** выберите тот же тип соединения, который был выбран для сервера.
6 В поле **Service Type** выберите **Client**. Значения остальных полей будут согласованы с сервером.
7 Выберите **Apply**.

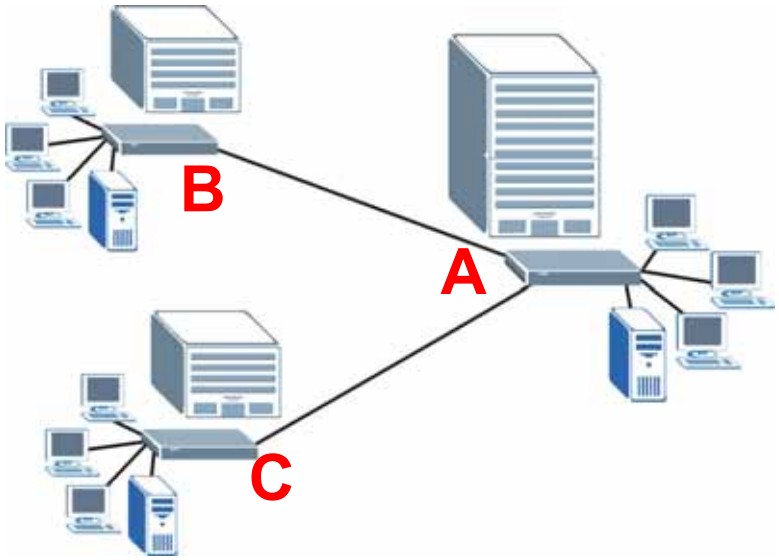
4.2.3 Соединение двух устройств P-793H

Соедините между собой порты **DSL** на обоих устройствах P-793H и дождитесь установления связи между двумя P-793H. Когда соединение установлено, горят светодиоды **DSL1**, **DSL2** и **INTERNET**. Установление соединения может занять полминуты. Если соединение между двумя P-793H не удается установить, необходимо проверить соответствие всех настроек (кроме **Service Type**).

4.3 Соединения по схеме "точка – две точки"

Соединение по схеме "точка – две точки" устанавливается между серверным устройством P-793H и двумя клиентскими P-793H. Такая конфигурация представляет собой безопасный и экономичный способ построения частной IP-сети. Ниже показан пример такого соединения.

Рис. 23 Пример: соединения по схеме "точка – две точки"



В соединении по схеме "точка – две точки" к DSL-порту серверного устройства P-793H (**A**) подключен разветвительный кабель, по которому устанавливаются два DSL-соединения. Для установления соединений можно использовать RFC 1483 в режиме моста или ENET ENCAP в режиме маршрутизатора. Можно задать один набор параметров скорости передачи между сервером P-793H **A** и клиентом P-793H **B** и другой набор для соединения сервера P-793H **A** с клиентом P-793H **C**.

В схеме "точка – две точки" устройство P-793H, имеющее физическое соединение с обоими клиентами, становится сервером. Сервер управляет некоторыми параметрами DSL-соединения, включая скорости передачи и режим работы DSL.

4.4 Настройка соединения по схеме "точка – две точки"

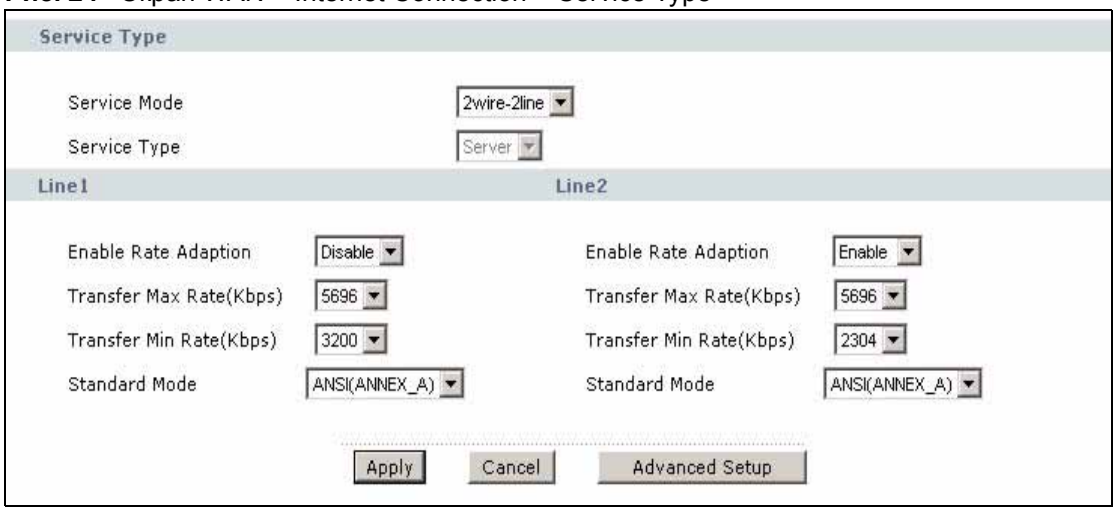
Ниже приведены указания для установления соединения по схеме "точка – две точки".

1. Настройка сервера.
2. Настройка клиентов.
3. Соединение двух устройств P-793H.

4.4.1 Настройка сервера

1. Войдите в управление устройством P-793H, которое будет выступать в качестве сервера. (См. гл. 2 на стр. 43.)
2. Выберите **Network > WAN > Internet Connection**.
3. В полях **VPI**, **VCI**, **Multiplexing** и **Encapsulation** укажите параметры, которые будут использоваться для соединения по схеме "точка – две точки". В поле **Encapsulation** выберите режим инкапсуляции: **RFC 1483** или **ENET ENCAP**. Выберите линию, которая будет использоваться для удаленного устройства по умолчанию (1 или 2).
4. Пролистайте экран до раздела **Service Type**. Появится изображенный ниже экран.

Рис. 24 Экран WAN > Internet Connection > Service Type



5 В поле **Service Mode** выберите конфигурацию телефонной линии **2wire-2line**.

6 В поле **Service Type** автоматически появится значение **Server**.

7 Заполните необходимые оставшиеся поля. Предположим, что вам необходимо установить параметр **Transfer Max Rate** в максимальное значение для линии **Line1**, но для линии **Line2** выбрать меньшее значение (поскольку клиентское устройство P-793H не может работать на более высоких скоростях).

8 Выберите **Apply**.

9 Перейдите в раздел **Network > WAN > More Connections** и настройте параметры второго удаленного узла.

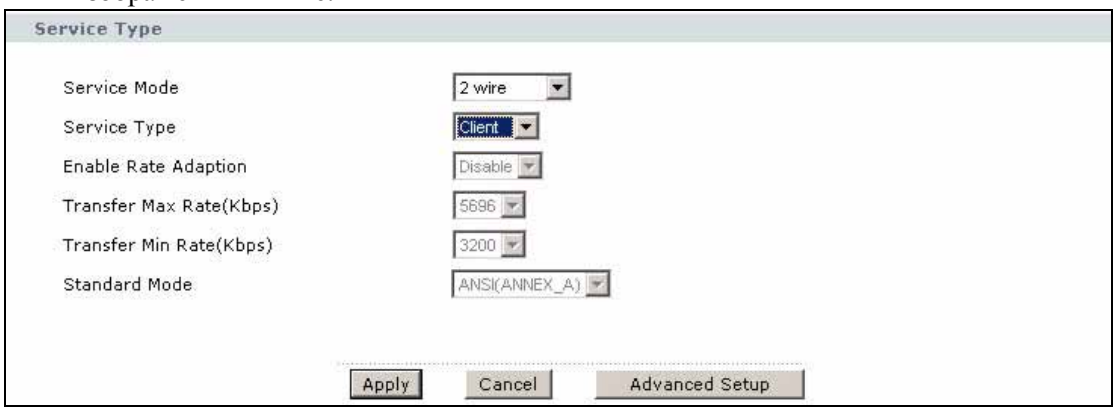
4.4.2 Настройка клиентов

1 Войдите в устройство P-793H, которое будет функционировать в режиме клиента. (См. гл. 2 на стр. 43.)

2 Выберите **Network > WAN > Internet Connection**.

3 В полях **VPI**, **VCI**, **Multiplexing** и **Encapsulation** продублируйте значения, заданные на сервере.

4 Пролистайте экран до раздела **Service Type**. Появится экран, похожий на изображенный ниже.



5 В поле **Service Mode** выберите режим **2 wire**.

6 В поле **Service Type** выберите **Client**. Значения остальных полей будут согласованы с сервером.
7 Нажмите кнопку **Apply**.
8 Повторите шаги с 1 по 7 на втором клиентском устройстве.

4.4.3 Соединение двух устройств P-793H

Соедините между собой порты **DSL** на обоих устройствах P-793H и дождитесь установления связи между двумя P-793H. Убедитесь, что разветвительный кабель подключен к соответствующим выходам DSL. Разъем разветвительного кабеля, помеченный **DSL1**, должен быть подключен к выходу телефонной линии DSL 1, а разъем **DSL2** – к выходу DSL 2.

Когда соединение установлено, горят светодиоды **DSL1**, **DSL2** и **INTERNET**. Установление соединения может занять полминуты. Если соединение между устройствами P-793H не удается установить, необходимо проверить правильность настроек.

Часть II
Настройка сети

5

Настройка WAN

В этой главе описывается настройка параметров глобальной сети.

5.1 Обзор параметров WAN

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

5.1.1 Инкапсуляция

Необходимо использовать тот метод инкапсуляции, которого требует поставщик услуг Интернета.P-793H поддерживает следующие методы.

5.1.1.1 ENET ENCAP

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

5.1.1.2 PPP по Ethernet (PPPoE)

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

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

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

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

Реализация PPPoE непосредственно в P-793H (а не на отдельных компьютерах) снимает необходимость в установке ПО для PPPoE на компьютерах локальной сети, поскольку эту часть задачи выполняет P-793H. Кроме того, благодаря NAT доступ будут иметь все компьютеры в LAN.

5.1.1.3 PPP по ATM (PPPoA)

PPPoA означает протокол "точка-точка" поверх 5-го уровня адаптации ATM (AAL5). PPPoA функционирует так же, как модемное коммутируемое соединение с Интернетом. P-793H инкапсулирует PPP-сеанс по стандарту RFC1483 и передает его через постоянный виртуальный канал (ATM PVC) на оборудование DSLAM (мультиплексор цифровых абонентских каналов) у поставщика услуг. Подробное описание PPPoA см. в RFC 2364. Подробное описание PPP см. в RFC 1661.

5.1.1.4 RFC 1483

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

5.1.2 Мультиплексирование

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

5.1.2.1 Мультиплексирование VC

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

5.1.2.2 Мультиплексирование LLC

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

5.1.3 VPI и VCI

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

5.1.4 Присвоение IP-адресов

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

5.1.4.1 Назначение IP-адресов при использовании инкапсуляции PPPoA или PPPoE

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

5.1.4.2 Назначение IP-адресов при использовании инкапсуляции RFC 1483

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

5.1.4.3 Назначение IP-адресов при использовании инкапсуляции ENET ENCAP

В этом случае вы можете иметь или статический или динамический IP-адрес. Для статического IP-адреса необходимо заполнить поля **IP Address** и **ENET ENCAP Gateway** сведениями, полученными от поставщика услуг Интернета. Однако в случае динамического IP-адреса устройство P-793H будет выступать DHCP-клиентом в сети WAN, и поля **IP Address** и **ENET ENCAP Gateway** будут неприменимы, поскольку P-793H получает соответствующие значения от DHCP-сервера.

5.1.5 Закрепленное соединение (в режиме PPP)

Закрепленное соединение – это коммутируемая линия, где соединение всегда установлено независимо от требований к трафику. Реализация закрепленного соединения в P-793H сводится к тому, что отключается время ожидания, а кроме того, при каждом разрыве сеанса P-793H будет пытаться автоматически восстановить соединение. Закрепленное соединение может оказаться чрезвычайно дорогостоящим по очевидным причинам.

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

5.1.6 NAT

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

5.2 Метрика

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

Метрика устанавливает приоритеты маршрутов, используемых P-793H для связи с Интернетом. Если два маршрута по умолчанию имеют одно и то же значение метрики, P-793H использует следующие предопределенные приоритеты:

- Обычный маршрут: определяется поставщиком услуг Интернета (см. разд. 5.4 на стр. 78)
- Маршрут для переадресации трафика (см. разд. 5.6 на стр. 89)
- Резервный маршрут WAN, также называемый маршрутом резервирования через коммутируемый доступ (см. разд. 5.8 на стр. 90)

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-793H пробует маршрут переадресации трафика. Если маршрут переадресации также оказывается неработоспособен, P-793H использует маршрут резервирования через коммутируемый доступ.

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

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

5.3 Ограничение трафика

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

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

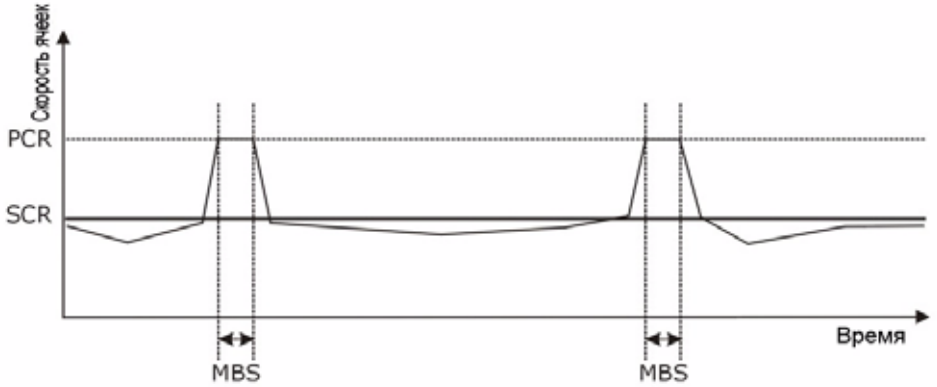
Выдерживаемая скорость ячеек (Sustained Cell Rate, SCR) - средняя скорость ячеек для каждого источника пульсирующего трафика. Она задает максимальную среднюю скорость, с которой ячейки могут пересылаться по виртуальному соединению. SCR не должна превышать PCR.

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 усредненная 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. 25 Пример ограничения трафика



5.3.1 Классы трафика в ATM

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

5.3.1.1 Постоянная скорость (CBR)

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

5.3.1.2 Переменная скорость (VBR)

Класс ATM-трафика с переменной битовой скоростью (Variable Bit Rate, VBR) применяется для соединений с резкими кратковременными пульсациями трафика. Класс трафика с переменной битовой скоростью (Variable Bit Rate, VBR) применяется для соединений с резкими кратковременными пульсациями трафика.

5.3.1.3 Неуказанная битовая скорость (UBR)

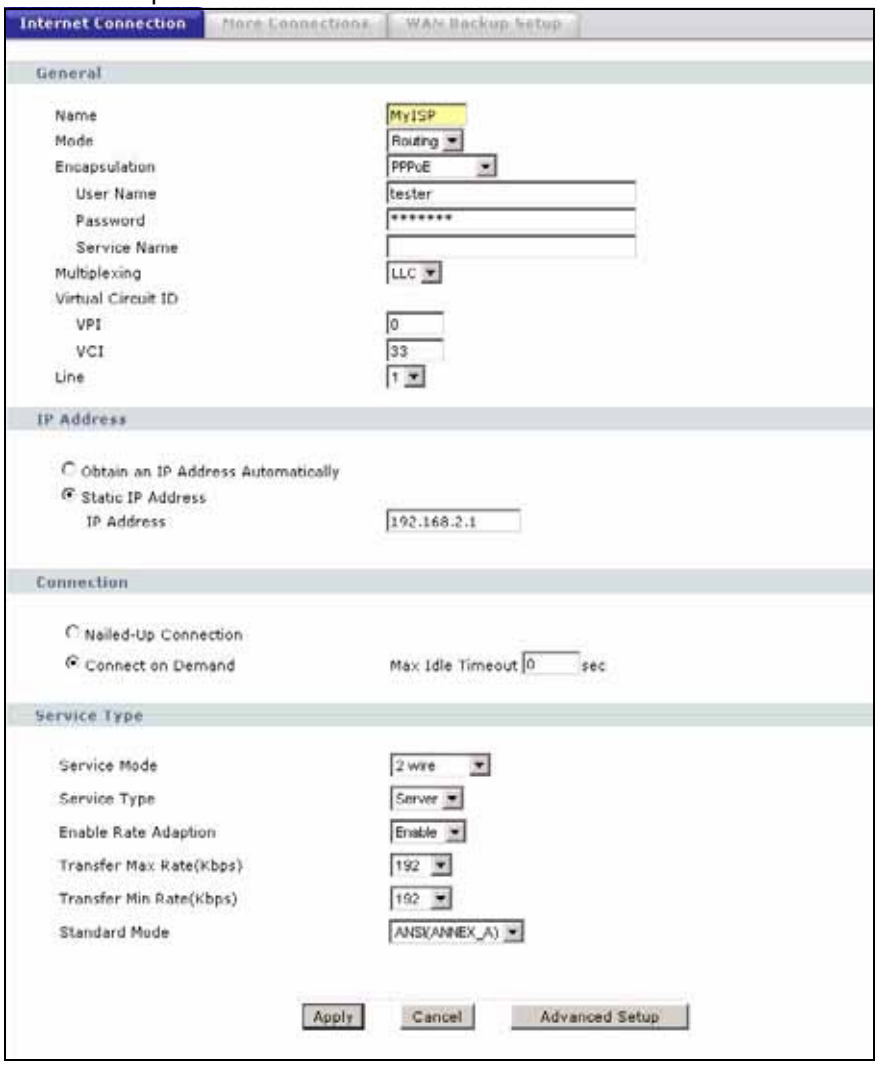
Класс ATM-трафика с неопределенной битовой скоростью (Unspecified Bit Rate, UBR) применяется для пульсирующего трафика. Отличие UBR состоит в том, что он не дает никаких гарантий в отношении полосы пропускания и разрешает доставку трафика только при наличии запаса пропускной способности сети. Пример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

5.4 Настройка подключения к Интернету

Чтобы изменить настройки удаленного узла для P-793H, выберите **Network > WAN > Internet Connection**. Данный экран может быть различным в зависимости от инкапсуляции.

Дополнительные сведения см. в разд. 5.1 на стр. 73.

Рис. 26 Экран WAN > Internet Connection



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 15 Экран WAN > Internet Connection

ПОЛЕ	ОПИСАНИЕ
General	
Name	Введите имя поставщика услуг Интернета, например, "MyISP". Эти сведения используются только для описания.
Mode	Если ваш поставщик услуг Интернета позволяет использовать одну учетную запись с нескольких компьютеров, выберите режим маршрутизации – **Routing** (этот режим действует по умолчанию). В противном случае выберите режим моста - **Bridge**.
Encapsulation	Выберите тип инкапсуляции, используемый поставщиком услуг Интернета, из раскрывающегося списка. Доступные для выбора варианты зависят от режима, выбранного в поле **Mode**. Если в поле **Mode** выбран режим **Bridge**, выберите **PPPoA** или **RFC 1483**. Если в поле **Mode** выбран режим **Routing**, выберите **PPPoA**, **RFC 1483**, **ENET ENCAP** или **PPPoE**. При установке соединения по схеме "точка – точка" или "точка – две точки" выберите один из двух вариантов: **ENET ENCAP** или **RFC 1483**.
User Name	(Только для PPPoA и PPPoE.) Введите имя пользователя в точности так, как оно указано поставщиком услуг. Если поставщик присвоил имя пользователя в формате пользователь@домен, где доменом является название службы, следует ввести оба компонента в точном соответствии с указаниями.
Password	(Только для PPPoA и PPPoE.) Введите пароль, связанный с указанным выше именем пользователя.
Service Name	(Только для инкапсуляции PPPoE.) Введите название службы PPPoE.
Multiplexing	Выберите тип мультиплексирования, используемый поставщиком услуг Интернета, из раскрывающегося списка. Варианты выбора: **VC** или **LLC**.
Virtual Circuit ID	Совокупность VPI (идентификатора виртуального пути) и VCI (идентификатора виртуального канала) определяет виртуальную цепь. Подробное описание см. в приложении.
VPI	Допустимый диапазон значений VPI – от 0 до 255. Введите присвоенный вам VPI.
VCI	Допустимый диапазон значений VCI – от 32 до 65535 (диапазон от 0 до 31 зарезервирован для локального управления трафиком ATM). Введите присвоенный вам VCI.
Line	Выберите DSL-соединение, по которому P-793H будет пересылать исходящий трафик.
IP Address	Эти поля доступны в том случае, если в поле **Mode** выбран режим **Routing**. Статический IP-адрес – это фиксированный адрес, выдаваемый поставщиком услуг Интернета. Динамический IP-адрес не имеет постоянного значения; поставщик услуг Интернета для каждого сеанса работы с Интернетом назначает новый адрес. ‘
Obtain an IP Address Automatically	(Только для PPPoE, PPPoA и ENET ENCAP.) Выберите этот переключатель, если IP-адрес вам присваивается в динамическом режиме.
Static IP Address	(Только для PPPoE, PPPoA и ENET ENCAP.) Выберите этот переключатель, если вам присвоен статический IP-адрес.
IP Address	Введите статический IP-адрес, предоставленный поставщиком услуг Интернета.

Таблица 15 Экран WAN > Internet Connection (продолжение)

ПОЛЕ	ОПИСАНИЕ
Subnet Mask	(Только для ENET ENCAP.) Это поле доступно в том случае, если выбран статический IP-адрес (**Static IP Address**). Введите маску подсети, предоставленную поставщиком услуг Интернета.
Gateway IP Address	(Только для ENET ENCAP.) Это поле доступно в том случае, если выбран статический IP-адрес (**Static IP Address**). Введите IP-адрес шлюза, предоставленный поставщиком услуг Интернета. Для доступа в Интернет адрес должен быть указан верно. Если введен адрес 0.0.0.0, соединение с Интернетом функционировать не будет.
Connection	Этот раздел доступен только в том случае, если в поле **Encapsulation** указано значения **PPPoE** или **PPPoA**.
Nailed-Up Connection	Выберите **Nailed-Up Connection**, чтобы использовать закрепленное соединение, которое активно все время. P-793H будет пытаться автоматически восстановить соединение при разрыве сеанса.
Connect on Demand	Если соединение не требуется поддерживать постоянно, выберите **Connect on Demand** и укажите интервал неактивности в поле **Max Idle Timeout**.
Max Idle Timeout	Если вы выбрали режим **Connect on Demand**, в поле **Max Idle Timeout** укажите интервал неактивности. Значение по умолчанию – 0, при котором сеанс соединения с Интернетом не завершается никогда.
Service Type	
Service Mode	Выберите режим DSL-соединения: **2-wire** (двухпроводной), **4-wire** (четырехпроводной) или **2wire-2line** (двухпроводной двухлинейный). Режим зависит от намеченной конфигурации сети и используемых телефонных линий. В свою очередь, от выбранного режима зависит максимальная скорость соединения. В режиме **2-wire** максимальная скорость составляет 5,69 Мбит/с, а в режиме **4-wire** – 11,38 Мбит/с. В режиме **2wire-2line** максимальная скорость каждой из линий составляет 5,69 Мбит/с. Настройка режима **2wire-2line** более подробно описана в разд. 5.4.1 на стр. 81.
Service Type	Укажите, на какой из сторон DSL-соединения (сервер, клиент) находится P-793H. Выберите **Server**, если устройство P-793H выполняет в соединении "точка – две точки" роль сервера. (См. гл. 4 на стр. 65.) В противном случае выберите **Client**. Если выбран режим **2wire-2line**, это поле недоступно для настройки, поскольку устройство P-793H автоматически установлено в режим **Server**.
Enable Rate Adaption	Это поле активно, если в поле **Service Type** выбрано значение **Server**. Укажите, следует ли включить для P-793H режим согласования скорости соединения с другим устройством.
Transfer Max Rate(Kbps)	Это поле активно, если в поле **Service Type** выбрано значение **Server**. Выберите максимальную скорость отправки и приема информации для P-793H. Фактическая скорость будет лежать в диапазоне между настроенной вами минимальной скоростью и этим значением. Примечание. Если в поле **Service Mode** выбран режим **4-wire**, то фактическая скорость передачи будет вдвое выше указанной. В частности, чтобы задать максимальную скорость 11392 кбит/с, в этом поле необходимо выбрать скорость 5696 кбит/с.

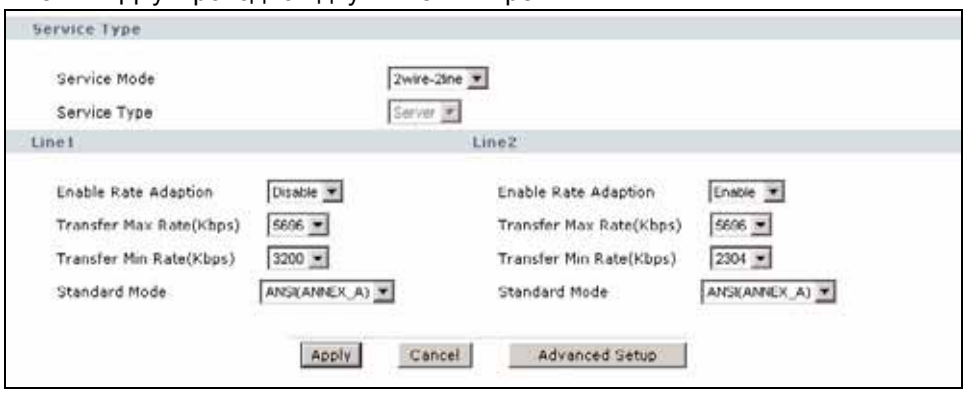
Таблица 15 Экран WAN > Internet Connection (продолжение)

ПОЛЕ	ОПИСАНИЕ
Transfer Min Rate(Kbps)	Это поле активно, если в поле **Service Type** выбрано значение **Server**. Выберите минимальную скорость отправки и приема информации для P-793H. Фактическая скорость будет лежать в диапазоне между этим значением и настроенной вами максимальной скоростью. Примечание. Если в поле **Service Mode** выбран режим **4-wire**, то фактическая скорость передачи будет вдвое выше указанной. В частности, чтобы задать минимальную скорость 384 кбит/с, в этом поле необходимо выбрать скорость 192 кбит/с.
Standard Mode	Это поле активно, если в поле **Service Type** выбрано значение **Server**. Выберите режим DSL-соединения для P-793H. Режим "Annex A" предназначен для соединений, использующих аналоговые телефонные сети общего пользования (ТфОП), а режим "Annex B" – для соединений по цифровым линиям ISDN.
Apply	Чтобы сохранить изменения, выберите **Apply**.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.
Advanced Setup	Нажмите эту кнопку, чтобы перейти на экран **Advanced WAN Setup** для настройки дополнительных параметров глобальной сети.

5.4.1 Двухпроводной двухлинейный режим

Когда выбран режим **2wire-2line**, раздел **Service Mode** экрана **Internet Connection** позволяет настроить два DSL-соединения. Этот режим используется для организации соединения по схеме "точка – две точки". Подробное описание этого режима см. в разд. 5.4.1 на стр. 81.

Рис. 27 Двухпроводной двухлинейный режим



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 16 Двухпроводной двухлинейный режим

ПОЛЕ	ОПИСАНИЕ
Service Type	
Service Mode	Выберите для DSL-соединения режим **2wire-2line**. В этом случае P-793H будет выступать в роли сервера для двух других устройств P-793H.
Service Type	Если выбран режим **2wire-2line**, это поле автоматически меняет значение на **Server**.

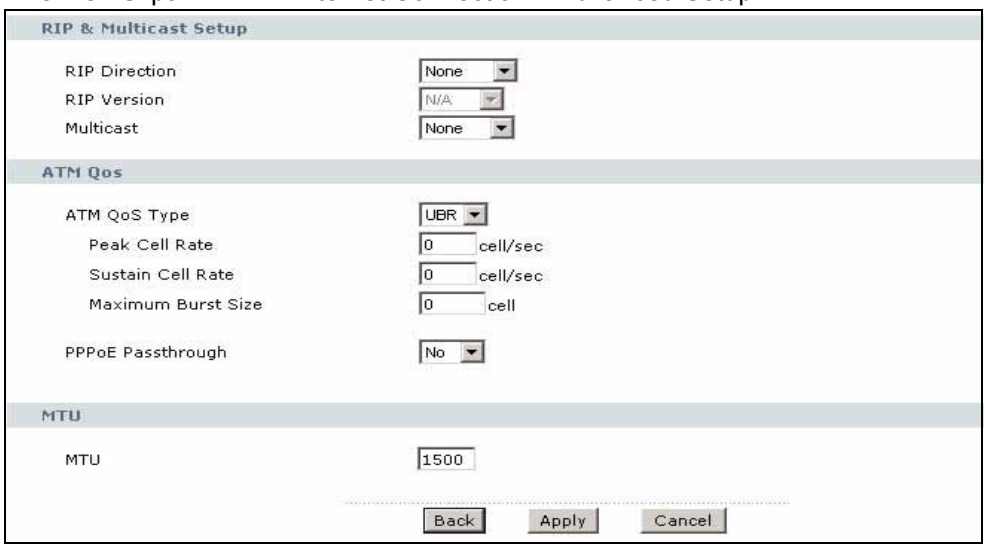
Таблица 16 Двухпроводной двухлинейный режим (продолжение)

ПОЛЕ	ОПИСАНИЕ
Line1 / Line 2	Для двух линий DSL (**Line 1** и **Line 2**) можно настроить разные скорости соединения.
Enable Rate Adaption	Укажите, следует ли включить для P-793H режим согласования скорости соединения с другим устройством.
Transfer Max Rate(Kbps)	Это поле активно, если в поле **Service Type** выбрано значение **Server**. Выберите максимальную скорость отправки и приема информации для P-793H. Фактическая скорость будет лежать в диапазоне между настроенной вами минимальной скоростью и этим значением.
Transfer Min Rate(Kbps)	Это поле активно, если в поле **Service Type** выбрано значение **Server**. Выберите минимальную скорость отправки и приема информации для P-793H. Фактическая скорость будет лежать в диапазоне между этим значением и настроенной вами максимальной скоростью.
Standard Mode	Выберите режим DSL-соединения для P-793H. Режим "Annex A" предназначен для соединений, использующих аналоговые телефонные сети общего пользования (ТфОП), а режим "Annex B" – для соединений по цифровым линиям ISDN.
Apply	Чтобы сохранить изменения, выберите **Apply**.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.
Advanced Setup	Нажмите эту кнопку, чтобы перейти на экран **Advanced WAN Setup** для настройки дополнительных параметров глобальной сети.

5.4.2 Расширенная настройка соединения с Интернетом

Этот экран используется для редактирования расширенных параметров P-793H при определении дополнительных соединений. На экране **Internet Connection** нажмите кнопку **Advanced Setup**. Появится изображенный ниже экран.

Рис. 28 Экран WAN > Internet Connection > Advanced Setup



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 17 Экран WAN > Internet Connection > Advanced Setup

ПОЛЕ	ОПИСАНИЕ
RIP & Multicast Setup	
RIP Direction	RIP (информационный протокол маршрутизации, стандарты RFC 1058 и RFC 1389) позволяет маршрутизатору обмениваться параметрами маршрутизации с другими маршрутизаторами. Поле **RIP Direction** управляет процессом отправки и приема RIP-пакетов. Выберите направление RIP: **Both** (вход-выход), **In Only** (только вход) или **Out Only** (только выход), **None** (нет). Если выбраны значения **Both** или **Out Only**, P-793H будет периодически рассылать таблицу маршрутизации посредством широковещательного сообщения. Если выбраны значения **Both** или **In Only**, устройство будет объединять получаемые параметры RIP; если выбрано значение **None**, устройство не будет рассылать RIP-пакеты и будет игнорировать поступающие RIP-пакеты.
RIP Version	Это поле доступно в том случае, если в поле **RIP Direction** выбран любой параметр, кроме **None**. Поле **RIP Version** управляет форматом и способом широковещательной рассылки RIP-пакетов с P-793H (устройство принимает пакеты обоих форматов). **RIP-1** поддерживается всеми устройствами, а RIP-2 позволяет передавать больше информации. RIP-1 обычно достаточен для большинства сетей, кроме сетей со сложной топологией. Модификации **RIP-2B** и **RIP-2M** передают сведения о маршрутизации в формате RIP-2; различие между ними состоит в том, что в **RIP-2B** используется широковещательная рассылка по подсетям, а в **RIP-2M** – многоадресная рассылка. Многоадресная рассылка может уменьшить загрузку на машинах, не являющихся маршрутизаторами, поскольку они обычно не откликаются по адресу многоадресной рассылки RIP и в этом случае просто не будут получать пакеты RIP. Однако если один маршрутизатор использует многоадресную рассылку, то все маршрутизаторы в вашей сети также должны использовать многоадресную рассылку.
Multicast	IGMP (широковещательный протокол взаимодействия групп в Интернете) – это протокол сетевого уровня, используемый для установления членства в группе многоадресной рассылки. P-793H поддерживает IGMP версии 1 (**IGMP-v1**) и **IGMP-v2**. Чтобы отключить этот протокол, выберите **None**.
QoS для ATM	
ATM QoS Type	Выберите **CBR** (постоянная битовая скорость), 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. Для пульсирующего трафика с совместным использованием полосы пропускания другими приложениями выберите **VBR** (переменная битовая скорость).
Peak Cell Rate	Разделите скорость DSL-линии (бит/с) на 424 (размер ATM-ячейки). Получится пиковая скорость передачи ячеек (PCR). Полученное значение будет соответствовать максимальной скорости посылки ячеек отправителем. Введите значение PCR в этом поле.
Sustain Cell Rate	Средняя скорость передачи ячеек (Sustained Cell Rate, SCR) – средняя скорость передачи ячеек (усреднение выполняется на большом промежутке времени). Введите SCR (значение SCR должно быть меньше PCR). Необходимо помнить, что по умолчанию система использует значение 0 ячеек в секунду.
Maximum Burst Size	Максимальный размер пульсации (Maximum Burst Size, MBS) – это максимальное число ячеек, при посылке которого будет соблюдаться PCR. Введите MBS (меньше 65535).

Таблица 17 Экран WAN > Internet Connection > Advanced Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
PPPoE Passthrough	Это поле действует только для соединений, использующих инкапсуляцию PPPoE. В дополнение к встроенному в устройство ZyXEL PPPoE-клиенту можно включить режим сквозного прохождения PPPoE, чтобы разрешить использование PPPoE-клиентов на хостах в локальной сети для соединения с поставщиком услуг Интернета через устройство ZyXEL. Каждый хост может иметь отдельную учетную запись и глобальный IP-адрес на стороне WAN. Сквозной режим PPPoE – альтернатива NAT для тех применений, где использование NAT невозможно. Отключите сквозной режим PPPoE, чтобы запретить хостам в локальной сети с помощью программных клиентов PPPoE соединяться с поставщиком услуг Интернета.
MTU	Максимальный размер блока передачи. Введите максимальный размер каждого пакета в данных (в байтах), пропускаемого через интерфейс. Более крупные пакеты при поступлении на P-793H делятся на фрагменты меньшего размера. Допустимый диапазон значений – от 512 до 1500. Обычно выбирается значение 1500.
Back	Чтобы вернуться к предыдущему экрану, нажмите кнопку **Back**.
Apply	Чтобы сохранить изменения, выберите **Apply**.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

5.5 Настройка дополнительных соединений

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

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

Рис. 29 Экран WAN > More Connections

Поля изображенного выше экрана описаны в следующей таблице.

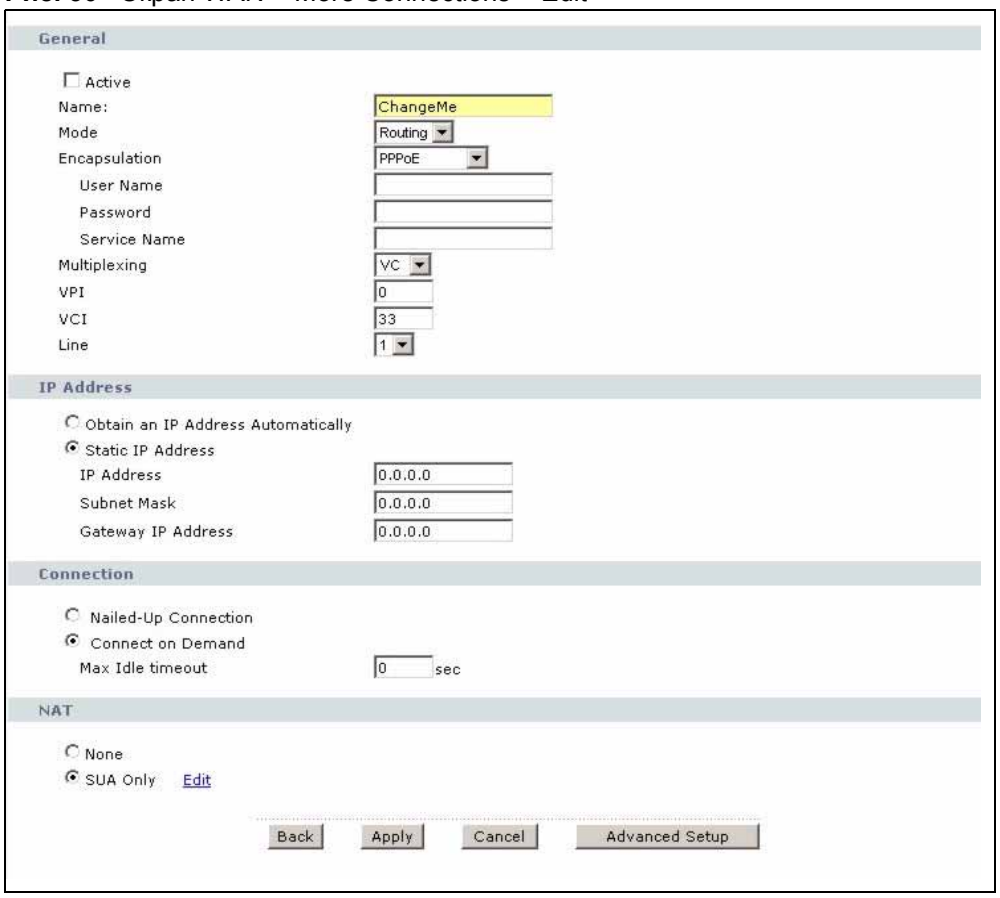
Таблица 18 Экран WAN > More Connections

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

5.5.1 Редактирование дополнительных соединений

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

Рис. 30 Экран WAN > More Connections > Edit



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 19 Экран WAN > More Connections > Edit

ПОЛЕ	ОПИСАНИЕ
General	
Active	Чтобы активировать соединение, отметьте флажок; чтобы сделать соединение неактивным, снимите флажок.
Name	Введите уникальное описательное название (до 13 знаков ASCII), позволяющее идентифицировать данное соединение.
Mode	Если ваш поставщик услуг Интернета позволяет использовать одну учетную запись с нескольких компьютеров, выберите режим маршрутизации – **Routing**. Если выбран режим **Bridge**, то P-793H будет пересылать на этот удаленный узел пакеты, не отправленные посредством маршрутизации, в противном случае такие пакеты удаляются.
Encapsulation	Выберите тип инкапсуляции, используемый поставщиком услуг Интернета, из раскрывающегося списка. Возможны следующие варианты: **PPPoA**, **RFC 1483**, **ENET ENCAP** или **PPPoE**. При настройке соединения по схеме "точка-точка" выберите режим **ENET ENCAP** или **RFC 1483**.
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.

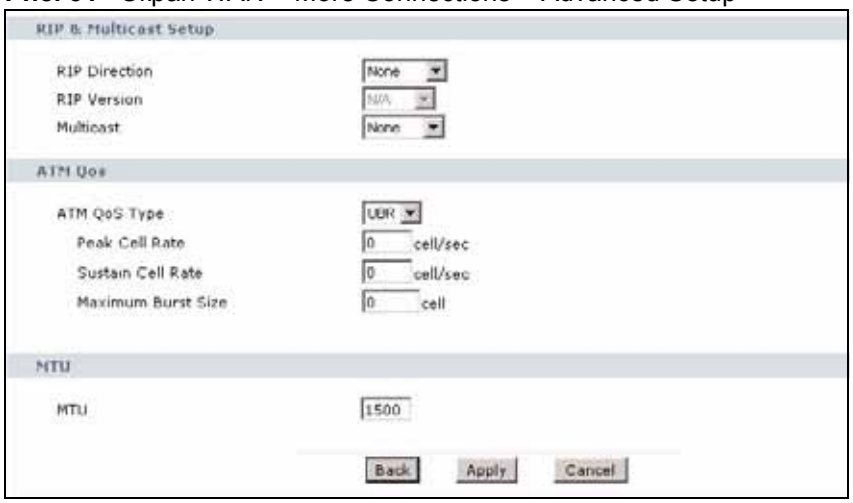
Таблица 19 Экран WAN > More Connections > Edit (продолжение)

ПОЛЕ	ОПИСАНИЕ
Multiplexing	Выберите тип мультиплексирования, используемый поставщиком услуг Интернета, из раскрывающегося списка. Варианты выбора: **VC** или **LLC**. По предварительному согласованию протоколы назначаются соответствующим виртуальным цепям, например, VC1 используется для передачи по протоколу IP. Если вы выбрали режим VC, укажите отдельные номера VPI и VCI для каждого протокола. При мультиплексировании на основе LLC или инкапсуляции PPP одна виртуальная цепь несет в себе несколько протоколов. Идентификационные параметры протокола содержатся в заголовках пакетов. В этом случае для всех протоколов достаточно одного набора номеров VPI и VCI.
VPI	Допустимый диапазон значений VPI – от 0 до 255. Введите присвоенный вам VPI.
VCI	Допустимый диапазон значений VCI – от 32 до 65535 (диапазон от 0 до 31 зарезервирован для локального управления трафиком ATM). Введите присвоенный вам VCI.
Line	Выберите DSL-соединение, по которому P-793H будет передавать исходящий трафик.
IP Address	Эти поля доступны в том случае, если в поле **Mode** выбран режим **Routing**. Статический IP-адрес – это фиксированный адрес, выдаваемый поставщиком услуг Интернета. Динамический IP-адрес не имеет постоянного значения; поставщик услуг Интернета для каждого сеанса работы с Интернетом назначает новый адрес. ‘
Obtain an IP Address Automatically	(Только для PPPoE, PPPoA и ENET ENCAP.) Выберите этот переключатель, если IP-адрес вам присваивается в динамическом режиме.
Static IP Address	(Только для PPPoE, PPPoA и ENET ENCAP.) Выберите этот переключатель, если вам присвоен статический IP-адрес.
IP Address	Введите статический IP-адрес, предоставленный поставщиком услуг Интернета.
Subnet Mask	Введите маску подсети, предоставленную поставщиком услуг Интернета.
Gateway IP Address	Введите IP-адрес шлюза, предоставленный поставщиком услуг Интернета.
Connection	Этот раздел доступен только в том случае, если в поле **Encapsulation** указано значения **PPPoE** или **PPPoA**.
Nailed-Up Connection	Выберите **Nailed-Up Connection**, чтобы использовать закрепленное соединение, которое активно все время. P-793H будет пытаться автоматически восстановить соединение при разрыве сеанса.
Connect on Demand	Если соединение не требуется поддерживать постоянно, выберите **Connect on Demand** и укажите интервал неактивности в поле **Max Idle Timeout**.
Max Idle Timeout	Если вы выбрали режим **Connect on Demand**, в поле **Max Idle Timeout** укажите интервал неактивности. Значение по умолчанию – 0, при котором сеанс соединения с Интернетом не завершается никогда.
NAT	Режим трансляции **SUA Only** доступен только в том случае, если в поле **Mode** выбран режим **Routing** . Выберите **SUA Only**, если NAT требуется использовать всего с одним глобальным IP-адресом. Для редактирования набора привязки серверов нажмите **Edit**, чтобы перейти на экран **Port Forwarding**. В противном случае выберите **None**, чтобы отключить NAT.
Back	Чтобы вернуться к предыдущему экрану, нажмите кнопку **Back**.
Apply	Чтобы сохранить изменения, выберите **Apply**.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.
Advanced Setup	Нажмите эту кнопку, чтобы перейти на экран **More Connections Advanced** для редактирования дополнительных параметров соединения с WAN.

5.5.2 Расширенная настройка дополнительных соединений

Этот экран служит для настройки дополнительных параметров WAN в P-793H. На экране **More Connections Edit** нажмите кнопку **Advanced Setup**. Появится изображенный ниже экран.

Рис. 31 Экран WAN > More Connections > Advanced Setup



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 20 Экран WAN > More Connections > Advanced Setup

ПОЛЕ	ОПИСАНИЕ
RIP & Multicast Setup	
RIP Direction	RIP (информационный протокол маршрутизации, стандарты RFC 1058 и RFC 1389) позволяет маршрутизатору обмениваться параметрами маршрутизации с другими маршрутизаторами. Поле **RIP Direction** управляет процессом отправки и приема RIP-пакетов. Выберите направление RIP: **Both** (вход-выход), **In Only** (только вход) или **Out Only** (только выход), **None** (нет). Если выбраны значения **Both** или **Out Only**, P-793H будет периодически рассылать таблицу маршрутизации посредством широковещательного сообщения. Если выбраны значения **Both** или **In Only**, устройство будет объединять получаемые параметры RIP; если выбрано значение **None**, устройство не будет рассылать RIP-пакеты и будет игнорировать поступающие RIP-пакеты.
RIP Version	Это поле доступно в том случае, если в поле **RIP Direction** выбран любой параметр, кроме **None**. Поле **RIP Version** управляет форматом и способом широковещательной рассылки RIP-пакетов с P-793H (устройство принимает пакеты обоих форматов). **RIP-1** поддерживается всеми устройствами, а RIP-2 позволяет передавать больше информации. RIP-1 обычно достаточен для большинства сетей, кроме сетей со сложной топологией. Модификации **RIP-2B** и **RIP-2M** передают сведения о маршрутизации в формате RIP-2; различие между ними состоит в том, что в **RIP-2B** используется широковещательная рассылка по подсетям, а в **RIP-2M** – многоадресная рассылка. Многоадресная рассылка может уменьшить загрузку на машинах, не являющихся маршрутизаторами, поскольку они обычно не откликаются по адресу многоадресной рассылки RIP и в этом случае просто не будут получать пакеты RIP. Однако если один маршрутизатор использует многоадресную рассылку, то все маршрутизаторы в вашей сети также должны использовать многоадресную рассылку.
Multicast	IGMP (широковещательный протокол взаимодействия групп в Интернете) – это протокол сетевого уровня, используемый для установления членства в группе многоадресной рассылки. P-793H поддерживает IGMP версии 1 (**IGMP-v1**) и **IGMP-v2**. Чтобы отключить этот протокол, выберите **None**.
ATM QoS	

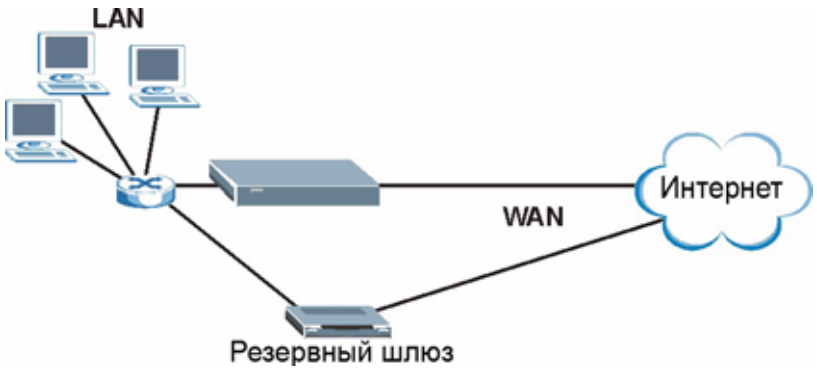
Таблица 20 Экран WAN > More Connections > Advanced Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
ATM QoS Type	Выберите **CBR** (постоянная битовая скорость), 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. Для пульсирующего трафика с совместным использованием полосы пропускания другими приложениями выберите **VBR** (переменная битовая скорость).
Peak Cell Rate	Разделите скорость DSL-линии (бит/с) на 424 (размер ATM-ячейки). Получится пиковая скорость передачи ячеек (PCR). Полученное значение будет соответствовать максимальной скорости посылки ячеек отправителем. Введите значение PCR в этом поле.
Sustain Cell Rate	Средняя скорость передачи ячеек (Sustained Cell Rate, SCR) – средняя скорость передачи ячеек (усреднение выполняется на большом промежутке времени). Введите SCR (значение SCR должно быть меньше PCR). Необходимо помнить, что по умолчанию система использует значение 0 ячеек в секунду.
Maximum Burst Size	Максимальный размер пульсации (Maximum Burst Size, MBS) – это максимальное число ячеек, при посылке которого будет соблюдаться PCR. Введите MBS (меньше 65535).
MTU	Максимальный размер блока передачи. Введите максимальный размер каждого пакета в данных (в байтах), пропускаемого через интерфейс. Более крупные пакеты при поступлении на P-793H делятся на фрагменты меньшего размера. Допустимый диапазон значений – от 512 до 1500. Обычно выбирается значение 1500.
Back	Чтобы вернуться к предыдущему экрану, нажмите кнопку **Back**.
Apply	Чтобы сохранить изменения, выберите **Apply**.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

5.6 Переадресация трафика

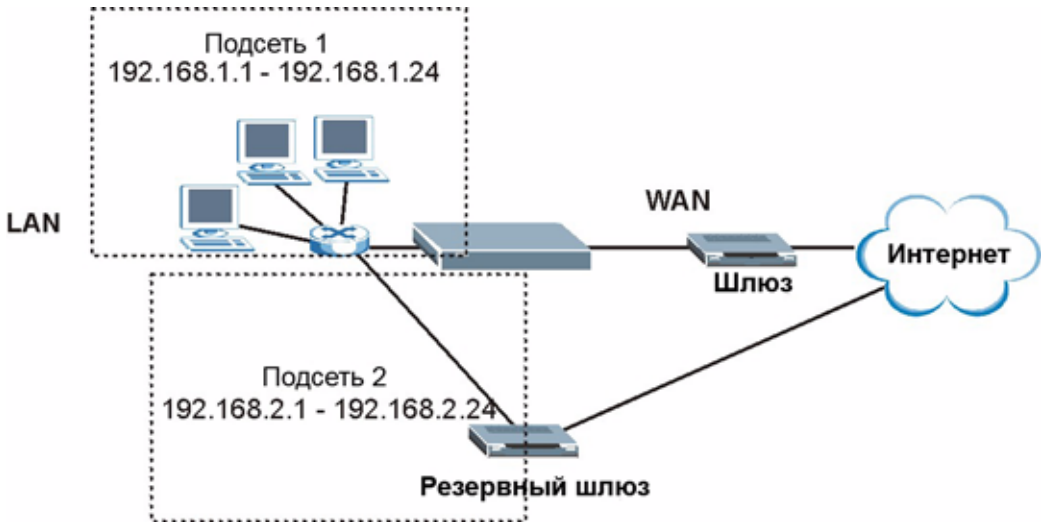
Переадресация трафика направляет трафик к резервному шлюзу, когда P-793H не может подключиться к Интернету. Пример приведен на следующем рисунке.

Рис. 32 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-793H. 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. 33 Настройка LAN для переадресации трафика



5.7 Интерфейс резервирования через коммутируемый доступ

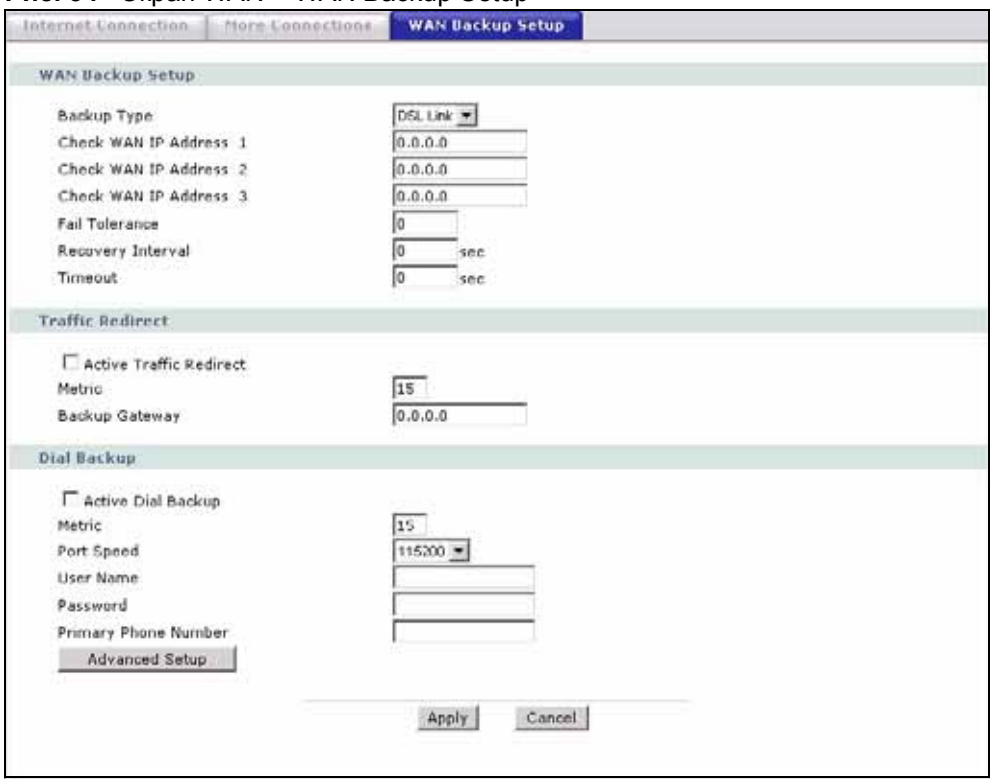
Порт **Dial Backup** может использоваться для резервного доступа через обычное коммутируемое соединение при нарушении связи на порту WAN. Перед использованием вспомогательного порта (**Dial Backup**) для резервирования убедитесь, что переключатель установлен правильно, а порт подключен. Подробные указания см. в Руководстве по быстрому запуску.

5.8 Настройка резервирования WAN

Этот экран служит для настройки переадресации трафика на резервный шлюз или подключения через порт резервирования при невозможности соединения P-793H с Интернетом по обычному каналу. Чтобы перейти на этот экран, выберите **WAN** > **WAN Backup Setup**. Появится изображенный ниже экран.

Резервирование через коммутируемый доступ недоступно, если для P-793H выбран режим (**Service Mode**) **2wire-2line**.

Рис. 34 Экран WAN > WAN Backup Setup



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 21 Экран WAN > WAN Backup Setup

ПОЛЕ	ОПИСАНИЕ
Backup Type	Выберите метод, которым P-793H будет проверять наличие DSL-соединения. Выберите **DSL Link**, чтобы устройство P-793H проверяло наличие физического соединения с DSLAM. Выберите **ICMP**, чтобы периодически отправлять эхозапросы с P-793H на IP-адреса, заданные в полях **Check WAN IP Address**.
Check WAN IP Address 1-3	Это поле задает адреса, с помощью которых P-793H 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-793H 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-793H 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).

Таблица 21 Экран WAN > WAN Backup Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
Recovery Interval	Когда P-793H 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-793H между проверками доступности сети. Увеличьте интервал, если целевой IP-адрес обрабатывает много трафика.
Timeout	Введите число секунд (рекомендуется 3), в течение которого P-793H 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-793H 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-793H не может подключиться к Интернету.
Active Traffic Redirect	Отметьте этот флажок, чтобы устройство P-793H 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-793H. Метрика обозначает "стоимость" передачи пакета. Маршрутизатор определяет оптимальный маршрут передачи, выбирая путь с самой низкой "стоимостью". Для маршрутизации на основе RIP мерой стоимости является число переходов между сетевыми сегментами, минимальное значение – 1 – соответствует напрямую подключенным сетям. Значение метрики должно быть в диапазоне от 1 до 15; значения больше 15 означают, что соединение не функционирует. Чем меньше значение, тем ниже "стоимость".
Backup Gateway	Введите IP-адрес резервного межсетевого шлюза в десятичном виде через точку. P-793H автоматически переадресует трафик на этот IP-адрес, если разрывается соединение P-793H с Интернетом.
Dial Backup	
Active Dial Backup	Отметьте этот флажок, чтобы устройство P-793H использовало резервное соединение через коммутируемый доступ при недоступности обычного соединения с WAN. Примечание. Для работы этой функции необходимо указать как минимум в одном из полей "Check WAN IP Address" проверяемый IP-адрес.
Metric	Это поле задает приоритет маршрута среди других маршрутов, используемых P-793H. Метрика обозначает "стоимость" передачи пакета. Маршрутизатор определяет оптимальный маршрут передачи, выбирая путь с самой низкой "стоимостью". Для маршрутизации на основе RIP мерой стоимости является число переходов между сетевыми сегментами, минимальное значение – 1 – соответствует напрямую подключенным сетям. Значение метрики должно быть в диапазоне от 1 до 15; значения больше 15 означают, что соединение не функционирует. Чем меньше значение, тем ниже "стоимость".
Port Speed	В раскрывающемся списке выберите скорость соединения между DSL-портом и внешним устройством.
User Name	Введите имя пользователя, предоставленное поставщиком услуг Интернета.
Password	Введите пароль, предоставленный поставщиком услуг Интернета.

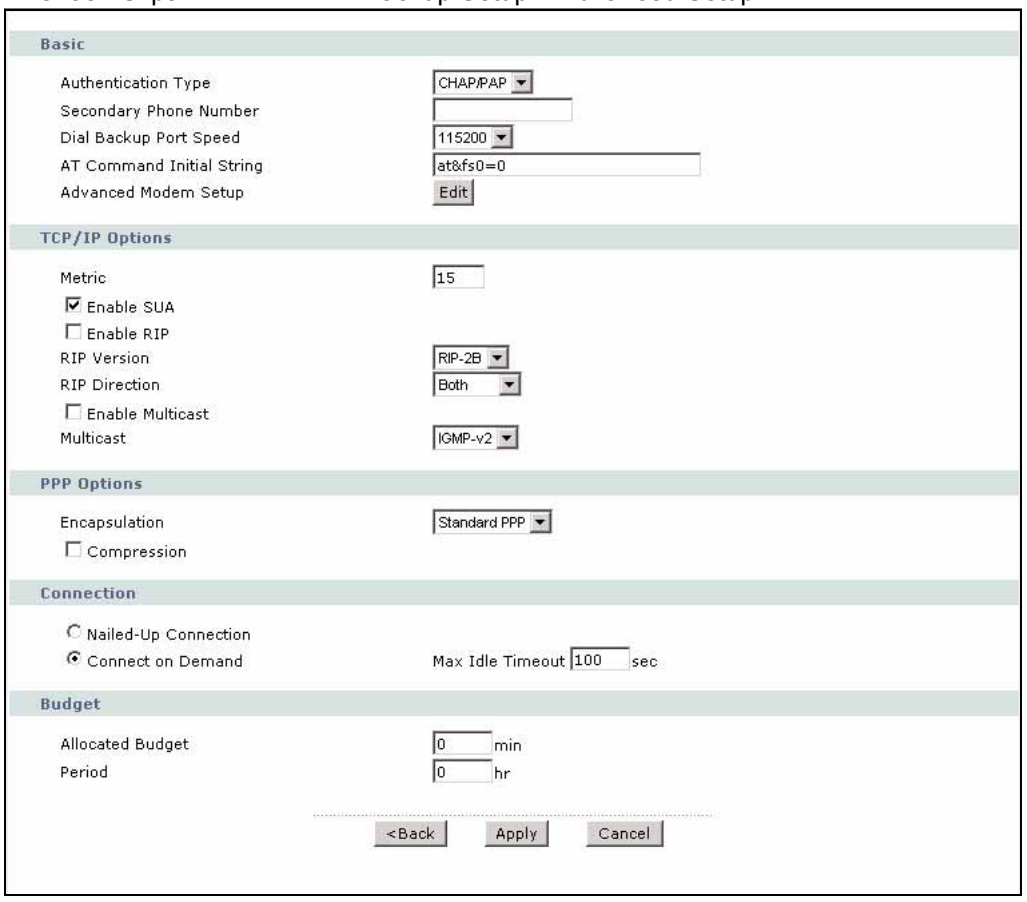
Таблица 21 Экран WAN > WAN Backup Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
Primary Phone Number	Введите первый (основной) телефонный номер поставщика услуг Интернета для данного удаленного узла. В тех случаях, когда основной номер занят или не отвечает, устройство набирает запасной номер (Secondary Phone), если он указан. (См. раздел **Advanced Setup**.) В некоторых телефонных сетях для вызова местных номеров перед ними необходимо набирать решетку (#). В этом случае перед номером нужно указать знак #.
Advanced Setup	Нажмите эту кнопку, чтобы настроить дополнительные параметры резервного соединения.
Apply	Чтобы сохранить изменения, выберите **Apply**.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

5.8.1 Расширенная настройка резервирования

Этот экран служит для изменения расширенных настроек резервирования через коммутируемый доступ в P-793H. Выберите **WAN** > **WAN Backup Setup > Advanced Setup**. Появится изображенный ниже экран.

Рис. 35 Экран WAN > WAN Backup Setup > Advanced Setup



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 22 Экран WAN > WAN Backup Setup > Advanced Setup

ПОЛЕ	ОПИСАНИЕ
Basic	
Authentication Type	В раскрывающемся списке выберите протокол аутентификации для исходящих вызовов. Возможны следующие значения: **CHAP/PAP** - P-793H принимает для данного удаленного узла запросы аутентификации CHAP и PAP. **CHAP** - P-793H принимает только запросы CHAP. **PAP** - P-793H принимает только запросы PAP.
Secondary Phone Number	Введите запасной телефонный номер, сообщенный поставщиком услуг Интернета. В тех случаях, когда основной номер занят или не отвечает, устройство набирает запасной номер (Secondary Phone), если он указан. В некоторых телефонных сетях для вызова местных номеров перед ними необходимо набирать решетку (#). В этом случае перед номером нужно указать знак #.
Dial Backup Port Speed	Выберите скорость соединения между портом резервирования через коммутируемый доступ и внешним устройством. Доступны следующие значения: **9600**, **19200**, **38400**, **57600**, **115200** или **230400** бит/с.
AT Command Initial String	Введите AT-строку инициализации устройства, используемого для доступа в WAN. Описание конкретных AT-команд см. в документации на устройство, подключаемое к порту резервирования.
Advanced Modem Setup	Нажмите кнопку **Edit**, чтобы отредактировать дополнительные настройки модема.
TCP/IP Options	
Metric	Это поле задает приоритет маршрута среди других маршрутов, используемых P-793H. Метрика обозначает "стоимость" передачи пакета. Маршрутизатор определяет оптимальный маршрут передачи, выбирая путь с самой низкой "стоимостью". Для маршрутизации на основе RIP мерой стоимости является число переходов между сетевыми сегментами, минимальное значение – 1 – соответствует напрямую подключенным сетям. Значение метрики должно быть в диапазоне от 1 до 15; значения больше 15 означают, что соединение не функционирует. Чем меньше значение, тем ниже "стоимость".
Enable SUA	Отметьте этот флажок, если требуется использовать NAT, имея один глобальный IP-адрес. Снимите флажок, чтобы отключить NAT.
Enable RIP	Отметьте этот флажок, чтобы включить поддержку протокола RIP для резервного коммутируемого соединения. RIP (информационный протокол маршрутизации, стандарты RFC 1058 и RFC 1389) позволяет маршрутизатору обмениваться параметрами маршрутизации с другими маршрутизаторами. Снимите флажок, чтобы запретить P-793H отправлять пакеты RIP и игнорировать все поступающие пакеты RIP.
RIP Version	Поле **RIP Version** управляет форматом и способом широковещательной рассылки RIP-пакетов с P-793H (устройство принимает пакеты обоих форматов). **RIP-1** поддерживается всеми устройствами, а RIP-2 позволяет передавать больше информации. RIP-1 обычно достаточен для большинства сетей, кроме сетей со сложной топологией. Модификации **RIP-2B** и **RIP-2M** передают сведения о маршрутизации в формате RIP-2; различие между ними состоит в том, что в **RIP-2B** используется широковещательная рассылка по подсетям, а в **RIP-2M** – многоадресная рассылка. Многоадресная рассылка может уменьшить загрузку на машинах, не являющихся маршрутизаторами, поскольку они обычно не откликаются по адресу многоадресной рассылки RIP и в этом случае просто не будут получать пакеты RIP. Однако если один маршрутизатор использует многоадресную рассылку, то все маршрутизаторы в вашей сети также должны использовать многоадресную рассылку.
RIP Direction	Поле **RIP Direction** управляет процессом отправки и приема RIP-пакетов. Выберите направление RIP: **Both** (оба направления) / **In Only** (только вход) / **Out Only** (только выход). Если выбраны значения **Both** или **Out Only**, P-793H будет периодически рассылать таблицу маршрутизации посредством широковещательного сообщения. Если выбрано значение **Both** или **In Only**, устройство будет учитывать информацию, получаемую в пакетах RIP.

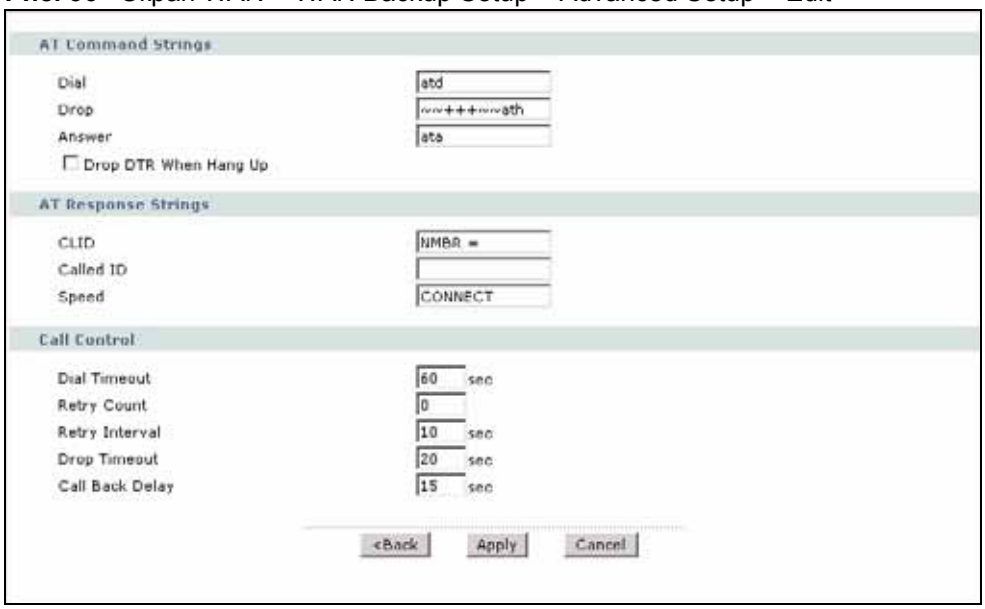
Таблица 22 Экран WAN > WAN Backup Setup > Advanced Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
Enable Multicast	Отметьте этот флажок, чтобы включить поддержку протокола IGMP для резервного коммутируемого соединения. IGMP (широковещательный протокол взаимодействия групп в Интернете) – это протокол сетевого уровня, используемый для установления членства в группе многоадресной рассылки.
Multicast	P-793H поддерживает IGMP версии 1 (**IGMP-v1**) и **IGMP-v2**.
PPP Options	
Encapsulation	Если устройство, через которое осуществляется резервирование, использует протокол инкапсуляции Cisco для PPP-соединений, выберите в раскрывающемся списке **CISCO PPP**, в противном случае выберите **Standard PPP**.
Compression	Отметьте этот флажок, чтобы включить сжатие STAC.
Connection	
Nailed-Up Connection	Выберите **Nailed-Up Connection**, чтобы использовать закрепленное соединение, которое активно все время. P-793H 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.
Budget	
Allocated Budget	Введите максимальную продолжительность каждого вызова (в минутах). Чтобы снять ограничение на продолжительность вызова, введите 0. Поле **Period** позволяет ограничить суммарную продолжительность исходящего вызова с P-793H. Если общее время исходящих вызовов превышает лимит, текущий вызов отбрасывается и все последующие исходящие вызовы блокируются.
Period	Введите количество часов, по истечении которого параметр **Allocated Budget** будет сбрасываться. Например, если в течение каждого часа под исходящие вызовы выделяется 30 минут, установите параметр **Allocated Budget** равным 30, а в этом поле введите 1.
Back	Чтобы вернуться к предыдущему экрану, нажмите кнопку **Back**.
Apply	Чтобы сохранить изменения, выберите **Apply**.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

5.8.2 Расширенные настройки модема для резервирования через коммутируемый доступ

Этот экран служит для изменения расширенных настроек модема для резервирования через коммутируемый доступ в P-793H. Выберите **WAN** > **WAN Backup Setup > Advanced Setup > Edit**. Появится изображенный ниже экран.

Рис. 36 Экран WAN > WAN Backup Setup > Advanced Setup > Edit



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 23 Экран WAN > WAN Backup Setup > Advanced Setup > Edit

ПОЛЕ	ОПИСАНИЕ
AT Command Strings	
Dial	Введите AT-команду для осуществления вызова.
Drop	Введите AT-команду для завершения вызова. Символ "~" кодирует 1-секундную задержку. Например, для модемов с медленным откликом можно использовать строку "~~~+++~~ath".
Answer	Введите AT-команду для ответа на входящий вызов.
Drop DTR When Hang Up	Отметьте этот флажок, чтобы осуществлять сброс сигнала DTR после отправки строки, указанной в поле **Drop**.
AT Response Strings	
CLID	Введите ключевое слово, после которого в AT-строке отклика приводится CLID (идентификация вызывающей линии). Это позволяет P-793H извлекать CLID из AT-строки доступа, полученной от устройства, через которое осуществляется доступ в WAN. Идентификатор CLID применяется для CLID-аутентификации.
Called ID	Введите ключевое слово, которое предшествует набираемому номеру.
Speed	Введите ключевое слово, которое предшествует скорости соединения.
Call Control	
Dial Timeout	Укажите число секунд, в течение которых P-793H будет ожидать установления исходящего соединения перед прекращением операции. P-793H сообщает об истечении времени ожидания и прекращает попытку установления исходящего соединения, если его не удалось установить за указанное время.
Retry Count	Укажите число повторных попыток набора номера, которые P-793H будет предпринимать при обнаружении сигнала "занято" или при отсутствии ответа удаленной стороны, прежде чем номер будет занесен в черный список.

Таблица 23 Экран WAN > WAN Backup Setup > Advanced Setup > Edit (продолжение)

ПОЛЕ	ОПИСАНИЕ
Retry Interval	Укажите продолжительность паузы (в секундах), которую P-793H будет выдерживать между попытками повторного набора номера. Эта пауза действует до занесения номера в черный список.
Drop Timeout	Введите число секунд, по истечении которых P-793H сбросит сигнал DTR, если не будет получено явное подтверждение разъединения.
Call Back Delay	Укажите длительность паузы (в секундах), которую P-793H будет выдерживать между завершением запроса встречного вызова (callback) и началом соответствующего встречного вызова.
Back	Чтобы вернуться к предыдущему экрану, нажмите кнопку **Back**.
Apply	Чтобы сохранить изменения, выберите **Apply**.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

6

Настройка LAN

В этой главе описывается настройка параметров локальной сети.

6.1 Обзор локальной сети

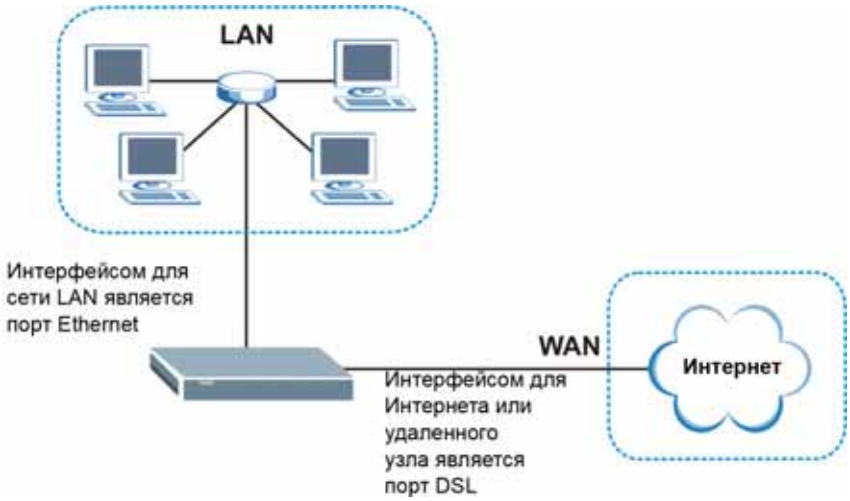
Локальная вычислительная сеть (LAN, ЛВС) - общедоступная система связи, к которой подключено множество компьютеров. Локальная сеть объединяет компьютеры, сосредоточенные на определенной площади, обычно – находящиеся в одном здании или на одном этаже. Экраны LAN помогают настраивать DHCP-сервер для локальной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

Выполнение настроек на экранах **LAN** описано в разд. 6.3 на стр. 103.

6.1.1 Сети LAN, WAN и P-793H

От непосредственного физического подключения зависит, являются ли порты P-793H портами WAN или LAN. Как показано ниже, существуют две раздельных IP-сети: внутренняя (сеть LAN) и внешняя (сеть WAN).

Рис. 37 IP-адреса в сетях LAN и WAN



6.1.2 Настройка DHCP

DHCP (протокол динамической настройки хоста, RFC 2131 и RFC 2132) позволяет клиентам в момент запуска получать настройки TCP/IP с сервера. P-793H позволяет включить или отключить встроенный DHCP-сервер. Когда устройство P-793H настроено в качестве DHCP-сервера, оно сообщает настройки TCP/IP клиентам. Если служба DHCP отключена, необходимо иметь в своей LAN другой DHCP-сервер или настраивать компьютеры вручную.

6.1.2.1 Настройка IP-пула

В P-793H имеется предварительно настроенный диапазон IP-адресов для клиентов DHCP (пул DHCP). См. техническое описание в приложениях. Не назначайте компьютерам в локальной сети статические адреса, принадлежащие пулу DHCP.

6.1.3 Адрес DNS-сервера

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

Поставщик услуг Интернета может распространять адреса серверов DNS двумя способами. Первый способ – адреса DNS-серверов сообщаются абоненту в информационном бюллетене при подключении к услугам. Если ваш поставщик услуг Интернета сообщил вам адреса DNS-серверов, введите их в полях **DNS Server** 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-793H поддерживает расширения IPCP для передачи информации о DNS-серверах посредством функции прокси-сервера для DNS.

Если поля **Primary** и **Secondary DNS Server** на экране **DHCP Setup** не заполнены (в частности, если в них оставлено значение **0.0.0.0**), устройство P-793H будет сообщать DHCP-клиентам, что DNS-сервером является оно само. Когда компьютер в сети LAN отправляет запрос DNS в P-793H, P-793H 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-793H передавать DNS-серверы на компьютеры, которые в свою очередь смогут выполнять запрос DNS-сервера непосредственно без участия P-793H.

6.1.4 Присвоение адресов DNS-серверов

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

Поставщик услуг Интернета может распространять адреса серверов DNS двумя способами.

- Первый способ – адреса DNS-серверов сообщаются абоненту в информационном бюллетене при подключении к услугам. Если ваш поставщик услуг Интернета сообщил вам адреса DNS-серверов, введите их на экране **DHCP Setup**.
- P-793H выступает в роли прокси-сервера для DNS, когда поля **Primary** и **Secondary DNS Server** на экране **DHCP Setup** оставлены со значениями **0.0.0.0**.

6.2 Параметры TCP/IP для локальной сети

P-793H имеет встроенный DHCP-сервер, который назначает IP-адреса и сообщает адреса DNS-серверов системам с функцией DHCP-клиента.

Параметры локальной сети в P-793H предварительно установлены на заводе и имеют следующие значения:

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

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

6.2.1 IP-адрес и маска подсети

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

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

Если поставщик услуг Интернета не сообщил вам номер IP-подсети в явном виде, то наиболее вероятно, что вы используете единственную учетную запись пользователя, и поставщик услуг Интернета назначит вам динамический IP-адрес при установлении соединения. В этом случае рекомендуется выбрать номер сети от 192.168.0.0 до 192.168.255.0. Также потребуется разрешить в P-793H функцию трансляции сетевых адресов (NAT). Комитет по цифровым адресам в Интернете (Internet Assigned Number Authority, IANA) зарезервировал определенные 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-793H 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-793H автоматически вычисляет маску подсети на основе назначаемого пользователем IP-адреса. В отсутствие специальных указаний изменять маску подсети, предлагаемую P-793H, не следует.

6.2.1.1 Частные IP-адреса

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

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

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

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

6.2.2 Настройка RIP

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

- **Both** - P-793H будет периодически распространять таблицу маршрутизации по широковещательному запросу и объединять принимаемые параметры RIP.
- **In Only** - P-793H не будет отправлять RIP-пакеты, но будет обрабатывать все принимаемые RIP-пакеты.
- **Out Only** - P-793H будет отправлять RIP-пакеты, но не будет обрабатывать поступающие RIP-пакеты.
- **None** - P-793H не будет отправлять RIP-пакеты и будет игнорировать все поступающие RIP-пакеты.

Поле **Version** управляет форматом и способом широковещательной рассылки RIP-пакетов со стороны P-793H (устройство принимает пакеты обоих форматов). **RIP-1** поддерживается всеми устройствами, а RIP-2 позволяет передавать больше информации. RIP-1 обычно достаточен для большинства сетей, кроме сетей со сложной топологией.

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

6.2.3 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.

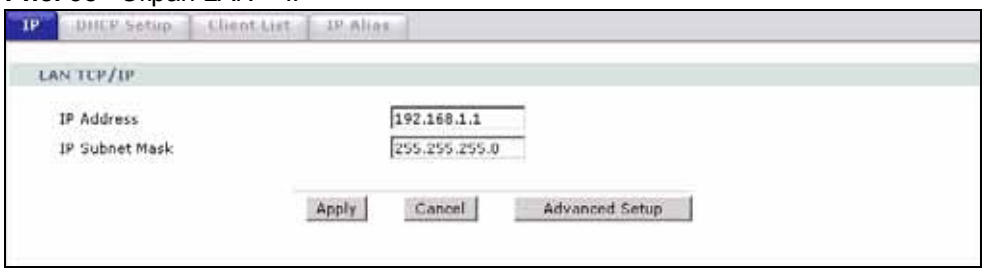
IGMP (межсетевой протокол многоадресной групповой рассылки) представляет собой протокол сетевого уровня для установления членства в группе многоадресной рассылки – он не применяется для пересылки каких-либо пользовательских данных. Версия 2 IGMP (RFC 2236) – развитие версии 1 (RFC 1112), первая версия 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-793H поддерживает версию 1 IGMP (**IGMP-v1**) и версию 2 (**IGMP-v2**). При запуске P-793H опрашивает все непосредственно связанные с ним сети, чтобы собрать информацию о принадлежности к группам. Впоследствии P-793H периодически обновляет эту информацию. Многоадресную рассылку IP на LAN- и/или WAN-интерфейсах P-793H можно разрешить/запретить с помощью веб-конфигуратора (**LAN**; **WAN**). Чтобы отключить многоадресную рассылку на этих интерфейсах, выберите **None**.

6.3 Настройка параметров IP для локальной сети

Этот экран позволяет настроить IP-адрес P-793H со стороны LAN. Выберите **LAN > IP**. Дополнительные сведения см. в разд. 6.1 на стр. 99.

Рис. 38 Экран LAN > IP



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 24 Экран LAN > IP

ПОЛЕ	ОПИСАНИЕ
IP Address	Введите IP-адрес P-793H в виде десятичных чисел через точку, например: 192.168.1.1 (заводская настройка по умолчанию).
IP Subnet Mask	Введите маску подсети, которая используется вашей сетью. Дополнительные сведения см. в разд. 6.2.1 на стр. 101.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-793H.

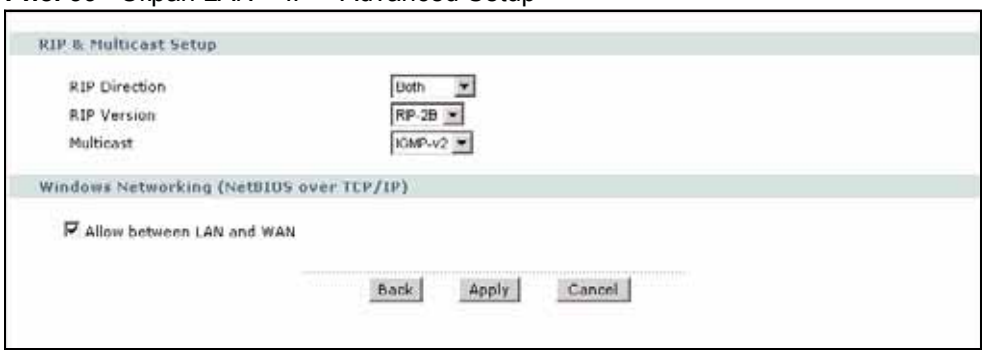
Таблица 24 Экран LAN > IP (продолжение)

ПОЛЕ	ОПИСАНИЕ
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.
Advanced Setup	Нажмите эту кнопку, чтобы перейти на экран **Advanced LAN Setup** для настройки дополнительных параметров локальной сети.

6.3.1 Настройка дополнительных параметров локальной сети

Этот экран используется для редактирования расширенных параметров настройки LAN в P-793H. На экране **LAN IP** нажмите кнопку **Advanced Setup**. Появится изображенный ниже экран.

Рис. 39 Экран LAN > IP > Advanced Setup



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 25 Экран LAN > IP > Advanced Setup

ПОЛЕ	ОПИСАНИЕ
RIP & Multicast Setup	
RIP Direction	RIP (информационный протокол маршрутизации, стандарты RFC 1058 и RFC 1389) позволяет маршрутизатору обмениваться параметрами маршрутизации с другими маршрутизаторами. Поле **RIP Direction** управляет процессом отправки и приема RIP-пакетов. Выберите направление RIP: **Both** (вход-выход), **In Only** (только вход) или **Out Only** (только выход), **None** (нет). Если выбраны значения **Both** или **Out Only**, P-793H будет периодически рассылать таблицу маршрутизации посредством широковещательного сообщения. Если выбраны значения **Both** или **In Only**, устройство будет объединять получаемые параметры RIP; если выбрано значение **None**, устройство не будет рассылать RIP-пакеты и будет игнорировать поступающие RIP-пакеты.
RIP Version	Это поле доступно в том случае, если в поле **RIP Direction** выбран любой параметр, кроме **None**. Поле **RIP Version** управляет форматом и способом широковещательной рассылки RIP-пакетов с P-793H (устройство принимает пакеты обоих форматов). **RIP-1** поддерживается всеми устройствами, а RIP-2 позволяет передавать больше информации. RIP-1 обычно достаточен для большинства сетей, кроме сетей со сложной топологией. Модификации **RIP-2B** и **RIP-2M** передают сведения о маршрутизации в формате RIP-2; различие между ними состоит в том, что в **RIP-2B** используется широковещательная рассылка по подсетям, а в **RIP-2M** – многоадресная рассылка. Многоадресная рассылка может уменьшить загрузку на машинах, не являющихся маршрутизаторами, поскольку они обычно не откликаются по адресу многоадресной рассылки RIP и в этом случае просто не будут получать пакеты RIP. Однако если один маршрутизатор использует многоадресную рассылку, то все маршрутизаторы в вашей сети также должны использовать многоадресную рассылку.
Multicast	IGMP (широковещательный протокол взаимодействия групп в Интернете) – это протокол сетевого уровня, используемый для установления членства в группе многоадресной рассылки. P-793H поддерживает IGMP версии 1 (**IGMP-v1**) и **IGMP-v2**. Чтобы отключить этот протокол, выберите **None**.

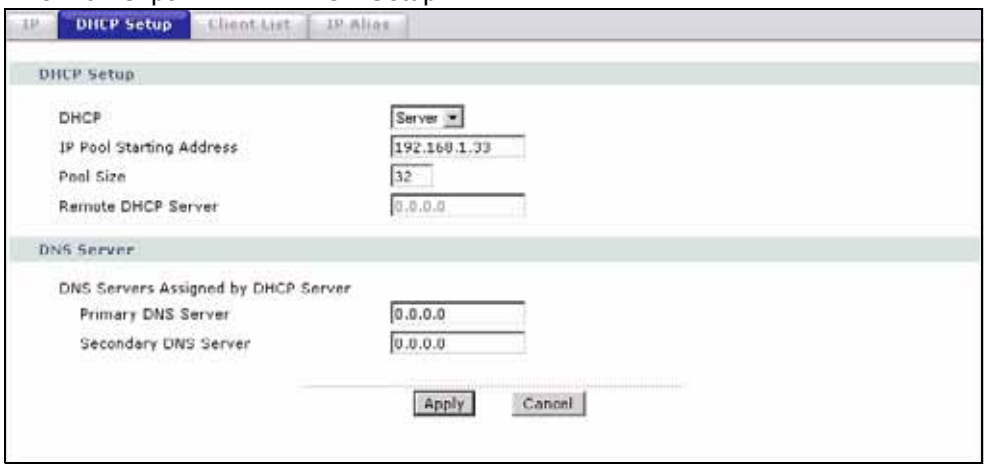
Таблица 25 Экран LAN > IP > Advanced Setup (продолжение)

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

6.4 Настройка DHCP

Этот экран служит для настройки параметров DNS-сервера, которые P-793H сообщает DHCP-клиентам в локальной сети.

Рис. 40 Экран LAN > DHCP Setup



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 26 Экран LAN > DHCP Setup

ПОЛЕ	ОПИСАНИЕ
DHCP Setup	
DHCP	Выберите тип DHCP-службы, который P-793H будет предоставлять в локальной сети. Возможны следующие варианты: **None** – P-793H не предоставляет службу DHCP в локальной сети. В сети уже имеется DHCP-сервер. **Relay** – P-793H пересылает DHCP-запросы на DHCP-сервер. DHCP-сервер может находиться в другой сети. **Server** – P-793H присваивает сетевым клиентам IP-адреса и предоставляет им маску подсети, адрес шлюза и параметры DNS-серверов. P-793H выступает в качестве DHCP-сервера в сети.

Таблица 26 Экран LAN > DHCP Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
IP Pool Starting Address	Это поле доступно в том случае, если P-793H выступает в качестве сервера (**Server**). Введите начальный адрес непрерывного пула IP-адресов.
Pool Size	Это поле доступно в том случае, если P-793H выступает в качестве сервера (**Server**). Введите размер DHCP-пула (количество IP-адресов).
Remote DHCP Server	Это поле доступно в том случае, если P-793H работает в режиме ретрансляции (**Relay**). Введите IP-адрес DHCP-сервера, которому устройство P-793H должно ретранслировать запросы.
DNS Server	
DNS Servers Assigned by DHCP Server	P-793H передает IP-адрес сервера DNS (системы доменных имен) клиентам DHCP.
Primary DNS Server Secondary DNS Server	Это поле доступно в том случае, если параметр **DHCP** установлен в значение **Relay**. Введите IP-адреса DNS-серверов. Адреса DNS-серверов передаются клиентским компьютерам вместе с присвоенными им IP-адресами и маской подсети. Если в этих полях оставлено значение 0.0.0.0, P-793H выступает в качестве прокси-сервера для DNS, передавая запрос на DNS-сервер, адрес которого получен в IPCP и возвращая отклик компьютеру.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-793H.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

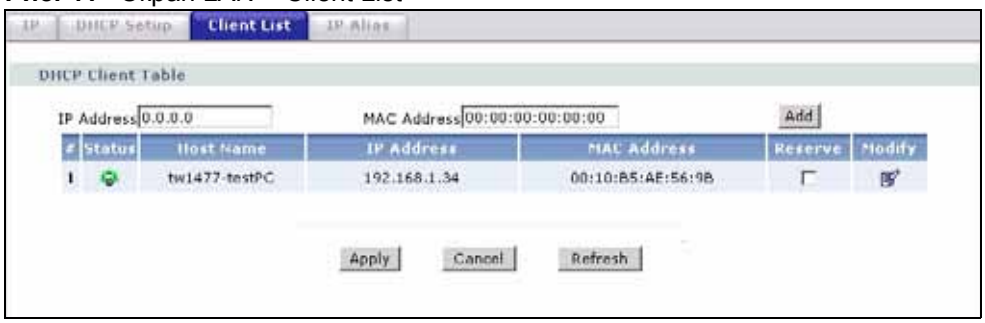
6.5 Список клиентов в локальной сети

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

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

Этот экран служит для изменения статических настроек DHCP в P-793H. Выберите **Network > LAN > Client List**. Появится изображенный ниже экран.

Рис. 41 Экран LAN > Client List



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 27 Экран LAN > Client List

ПОЛЕ	ОПИСАНИЕ
IP Address	Введите IP-адрес, который требуется присвоить компьютеру в локальной сети с указанным ниже MAC-адресом. IP-адрес DHCP-клиента должен находиться в диапазоне IP-адресов, указанном в поле **DHCP Setup**.
MAC Address	Введите MAC-адрес компьютера в локальной сети.
Add	Нажмите **Add**, чтобы добавить статическую запись DHCP.
#	В данном поле отображается порядковый номер (строка) в статической таблице IP-адресов.
Status	В данном поле отображается состояние соединения клиента с P-793H.
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 жестко запрограммированный заводской адрес. Порядок присвоения таких адресов является промышленным стандартом и позволяет исключить появление двух адаптеров с одинаковым адресом.
Reserve	Отметьте флажками записи, которым P-793H всегда будет присваивать выбранные IP-адреса в соответствии с указанными MAC-адресами (и именами хостов). В таблице можно выбрать до 32 записей.
Modify	Щелкните на значке редактирования, чтобы сделать поле IP-адреса доступным для редактирования и изменить адрес.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-793H.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.
Refresh	Чтобы повторно загрузить таблицу DHCP, нажмите кнопку **Refresh**.

6.6 Совмещение IP-адресов в локальной сети

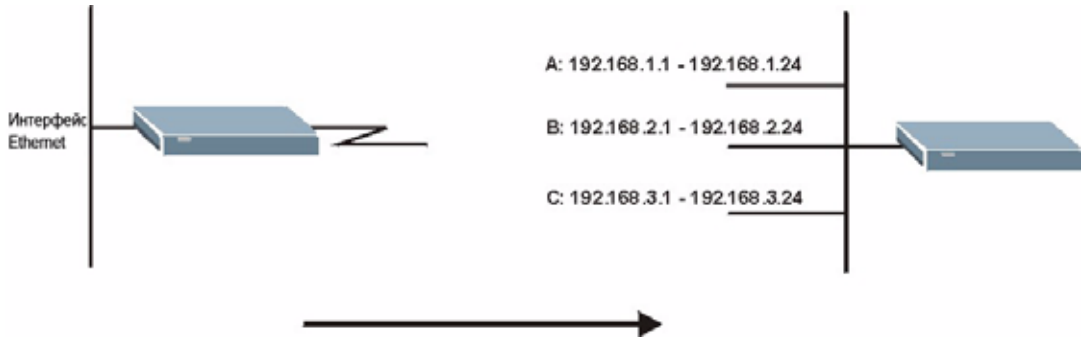
Функция совмещения IP-адресов (IP aliasing) позволяет разделить физическую сеть на различные логические сети, использующие один и тот же интерфейс Ethernet. P-793H поддерживает до трех логических интерфейсов LAN на одном физическом интерфейсе Ethernet, при этом P-793H будет выступать в качестве межсетевого 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.

Следите за тем, чтобы подсети логических сетей не перекрывались.

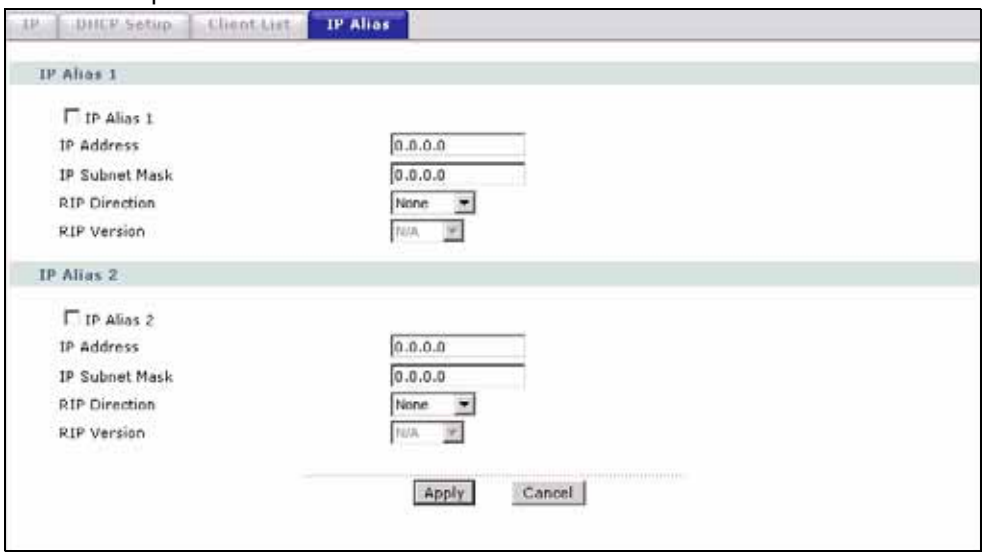
На следующем рисунке показана сеть LAN, разделенная на подсети A, B, и C.

Рис. 42 Физическая сеть и отдельные логические сети



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

Рис. 43 Экран LAN > IP Alias



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 28 Экран LAN > IP Alias

ПОЛЕ	ОПИСАНИЕ
IP Alias 1, 2	Отметьте флажок, чтобы настроить другую сеть LAN для P-793H.
IP Address	Введите IP-адрес вашего P-793H в десятичном виде через точку. Вместо этого можно щелкнуть правой кнопкой мыши, чтобы скопировать и/или вставить IP-адрес.
IP Subnet Mask	P-793H автоматически вычисляет маску подсети на основе назначаемого пользователем IP-адреса. Если вам не требуется деление на подсети, используйте маску подсети, рассчитанную P-793H.
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-793H будет периодически рассылать таблицу маршрутизации посредством широковещательного сообщения. Если выбраны значения **Both** или **In Only**, устройство будет объединять получаемые параметры RIP; если выбрано значение **None**, устройство не будет рассылать RIP-пакеты и будет игнорировать поступающие RIP-пакеты.

Таблица 28 Экран LAN > IP Alias (продолжение)

ПОЛЕ	ОПИСАНИЕ
RIP Version	Это поле доступно в том случае, если в поле **RIP Direction** выбран любой параметр, кроме **None**. Поле **RIP Version** управляет форматом и способом широковещательной рассылки RIP-пакетов с P-793H (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.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-793H.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

7

Экраны настройки NAT

В этой главе поясняется способ настройки NAT в P-793H.

7.1 Краткий обзор NAT

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

7.1.1 Определения, относящиеся к NAT

Термины "внешний" и "внутренний" определяют положение хоста относительно P-793H, например, компьютеры абонентов - это внутренние хосты, а веб-серверы в Интернете являются внешними хостами.

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

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

Таблица 29 Определения, относящиеся к NAT

ТЕРМИН	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.

7.1.2 Назначение NAT

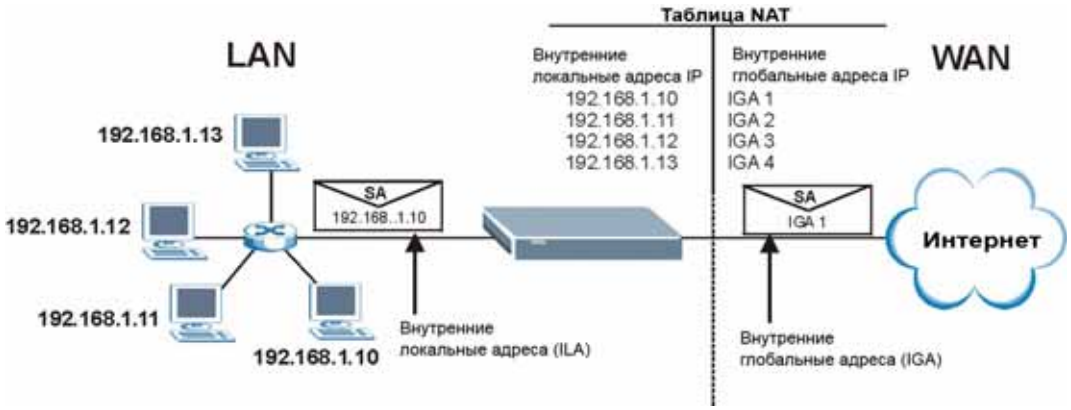
В самой простой форме NAT заменяет исходный IP-адрес в пакете, полученном от абонента (внутреннего локального адреса), на другой адрес (внутренний глобальный адрес) перед отправлением пакета на сторону WAN. Когда ответ возвращается, NAT преобразовывает адрес получателя (внутренний глобальный адрес) обратно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

Глобальные IP-адреса для внутренних хостов могут назначаться ISP статически или динамически. Кроме того, можно определять серверы (например, веб-сервер и telnet-сервер) в локальной сети и делать их доступными для внешнего мира. Если серверы не определены (для схем трансляции "многие к одному" и "многие ко многим с перегрузкой" – см. таб. 30 на стр. 114), NAT обеспечивает дополнительную защиту, играя роль сетевого экрана. Если серверы не определены, P-793H отфильтровывает все поступающие запросы, таким образом препятствуя проникновению в сеть злоумышленников. Для получения дополнительной информации о преобразовании IP-адреса обращайтесь к *RFC 1631*, *Преобразователь IP- адресов сети (NAT)*.

7.1.3 Принцип работы NAT

Каждый пакет имеет два адреса – адрес источника и адрес получателя. Для исходящих пакетов ILA (Внутренний локальный адрес) – исходный адрес в LAN, а IGA (Внутренний глобальный адрес) – исходный адрес в WAN. Для поступающих пакетов ILA - адрес места назначения в LAN, а IGA - в WAN. NAT привязывает частные (локальные) IP-адреса к глобальным уникальным, требуемым для обмена данными с хостами в других сетях. В каждом пакете заменяется исходный IP-адрес (а в режимах "многие к одному" и "многие ко многим с перегрузкой" – также и номер исходного порта TCP/UDP), после чего пакет пересылается в Интернет. P-793H отслеживает оригинальные адреса и номера портов, чтобы в поступающих ответных пакетах восстанавливались исходные значения. Это проиллюстрировано на следующем рисунке.

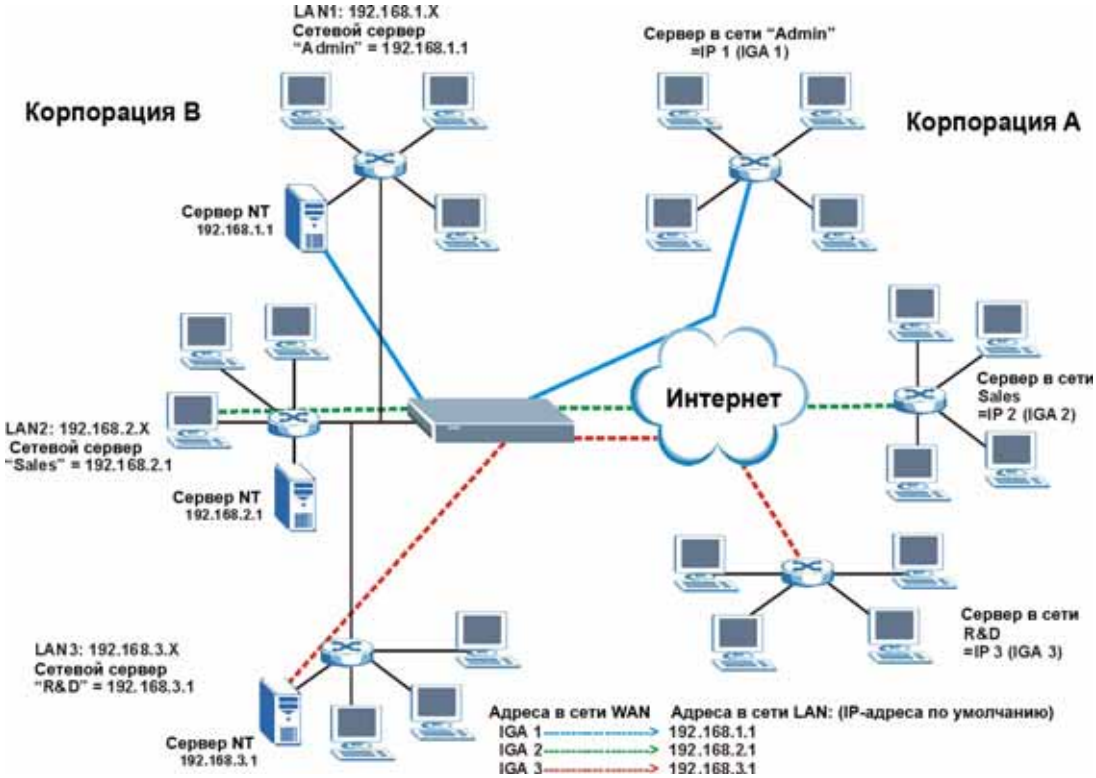
Рис. 44 Принцип работы NAT



7.1.4 Применение NAT

На следующем рисунке иллюстрируется возможное применение NAT, в котором три внутренние сети LAN (логические LAN, использующие совмещение IP-адресов) за P-793H могут обмениваться данными с тремя раздельными сетями WAN. Дополнительные примеры приводятся в конце этой главы.

Рис. 45 Применение NAT с IP-псевдонимом



7.1.5 Типы привязки NAT

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

- **Один - один**: в режиме "один к одному" P-793H привязывает один локальный IP-адрес к одному глобальному IP-адресу.
- **Многие к одному**: в режиме "многие к одному" P-793H 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-793H привязывает несколько локальных IP-адресов к общим глобальным IP-адресам.
- **Многие ко многим без перегрузки**: в режиме "многие ко многим без перегрузки" P-793H 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.

Таблица 30 Типы привязки NAT

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

7.2 Сравнение SUA и NAT

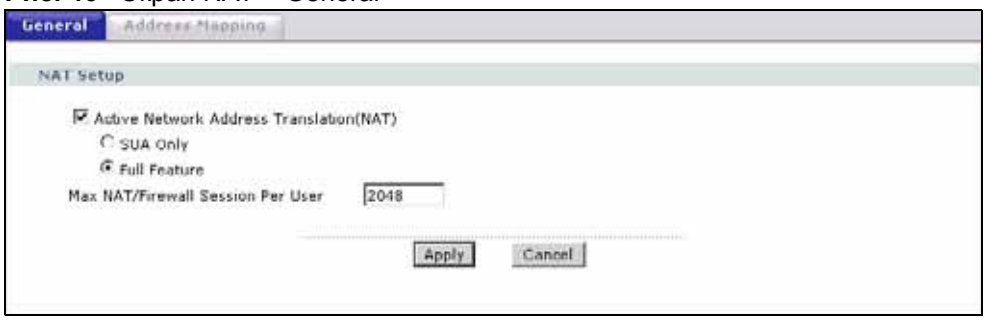
SUA (Single User Account – одна учетная запись) представляет собой подмножество NAT, реализуемое операционной системой ZyNOS и включающее два типа привязки: **"многие к одному"** и **"сервер"**. P-793H также поддерживает полноценный режим NAT (Full Feature), в котором несколько глобальных IP-адресов привязываются к нескольким IP-адресам клиентов или серверов в частных сетях LAN с помощью одного из способов, перечисленных в таб. 30 на стр. 114.

- Если для P-793H выделен только один глобальный IP-адрес в сети WAN, выберите **SUA Only**.
- Если для P-793H выделено несколько глобальных IP-адресов в сети WAN, выберите **Full Feature**.

7.3 Общая настройка NAT

Чтобы разрешить пересылку трафика из WAN через P-793H, в дополнение к настройке SUA/NAT необходимо создать правило для сетевого экрана. Выберите **Network** > NAT, чтобы открыть следующий экран.

Рис. 46 Экран NAT > General



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 31 Общие настройки NAT

ПОЛЕ	ОПИСАНИЕ
Active Network Address Translation (NAT)	Установите этот флажок, чтобы активировать NAT.
SUA Only	Выберите этот переключатель, если для P-793H выделен только один глобальный IP-адрес в сети WAN.
Full Feature	Выберите этот переключатель, если для P-793H выделено несколько глобальных IP-адресов в сети WAN.
Max NAT/ Firewall Session Per User	Для компьютеров, работающих в одноранговых (P2P) сетях, например, в файлообменных сетях, необходимо устанавливать сеансы через NAT. В отсутствие ограничения на число сеансов NAT, открываемых одним клиентом, все сеансы NAT могут оказаться исчерпаны. В этом случае невозможно установить новые сеансы NAT, и пользователи не могут выходить в Интернет. Для каждого сеанса NAT устанавливается соответствующий сеанс сетевого экрана. Это поле позволяет ограничить число сеансов NAT/сетевого экрана, открываемых клиентскими компьютерами посредством P-793H. 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-793H.
Cancel	Чтобы возвратить настройки на этом экране в их прежнее состояние, нажмите **Cancel**.

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

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

7.4.1 IP-адрес сервера по умолчанию

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

Если IP-адрес сервера по умолчанию (**Default Server**) не указан, P-793H будет отбрасывать все пакеты для портов, не указанных на этом экране или в настройке дистанционного управления.

7.4.2 Переадресация портов: сетевые службы и номера портов

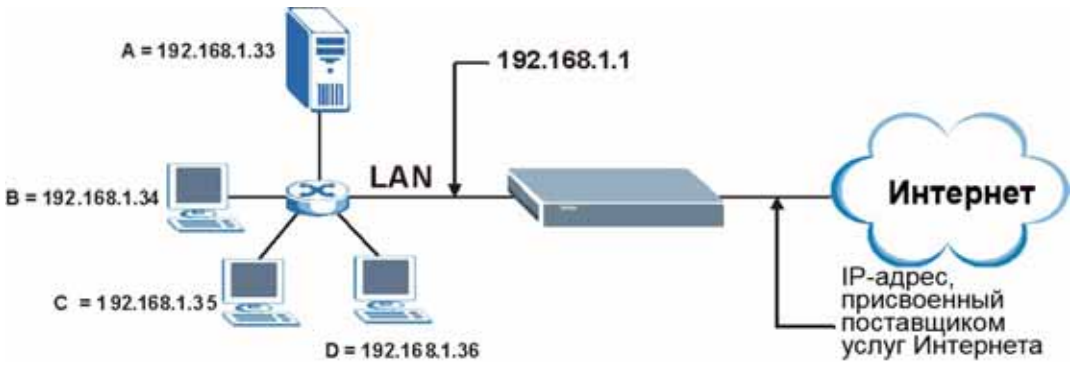
Экран Port Forwarding служит для переадресации входящих обращений к сетевым службам на серверы в локальной сети.

Приложение G на стр. 429 содержит список распространенных номеров портов. Дополнительные сведения о номерах портов см. в документе RFC 1700.

7.4.3 Настройка серверов с переадресацией портов (пример)

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

Рис. 47 Пример нескольких серверов, закрытых функцией NAT



7.5 Настройка переадресации портов

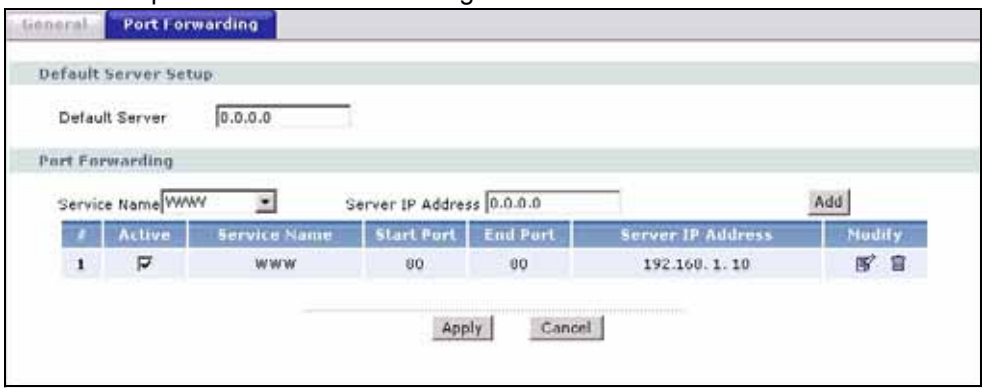
Экран **Port Forwarding** доступен, если на экране **NAT > General** выбран параметр **SUA Only**, а также при редактировании набора привязки сервера в режиме **Full Feature** NAT.

Если IP-адрес сервера по умолчанию (**Default Server**) не указан, P-793H 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 Приложение G на стр. 429.

Рис. 48 Экран NAT > Port Forwarding



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 32 Экран NAT > Port Forwarding

ПОЛЕ	ОПИСАНИЕ
Default Server Setup	
Default Server	В дополнение к серверам для заданных типов сетевых служб NAT поддерживает сервер по умолчанию. Сервер по умолчанию получает пакеты для портов, не указанных на этом экране. Если IP-адрес сервера по умолчанию (**Default Server**) не указан, P-793H будет отбрасывать все пакеты для портов, не указанных на этом экране или в настройке дистанционного управления.
Port Forwarding	
Service Name	Выберите тип сетевой службы для данного правила. Чтобы перейти на экран **Rule Setup** для задания собственных типов служб, выберите **User define**.
Server IP Address	Введите IP-адрес сервера для указанной сетевой службы.
Add	Нажмите эту кнопку, чтобы добавить правило в расположенную ниже таблицу.
#	В этом поле отображается порядковый номер правила (только для чтения).

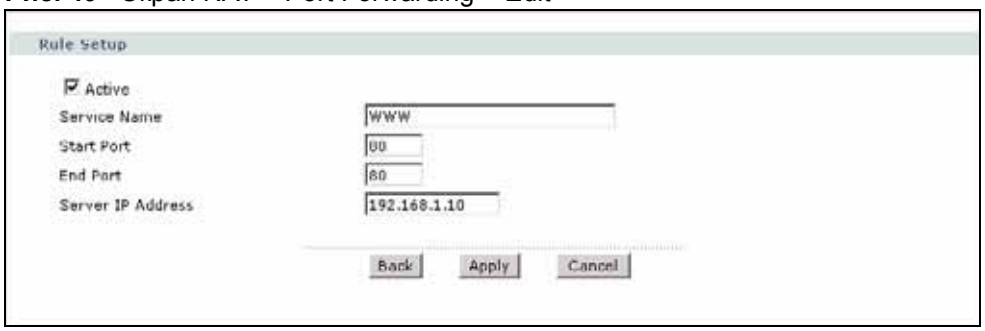
Таблица 32 Экран NAT > Port Forwarding (продолжение)

ПОЛЕ	ОПИСАНИЕ
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-793H.
Cancel	Нажмите **Cancel**, чтобы вернуться к прежнему состоянию настроек.

7.5.1 Редактирование правил переадресации портов

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

Рис. 49 Экран NAT > Port Forwarding > Edit



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 33 Экран NAT > Port Forwarding > Edit

ПОЛЕ	ОПИСАНИЕ
Active	Отметьте этот флажок, чтобы активировать правило.
Service Name	Введите название для идентификации данного правила переадресации портов.
Start Port	Введите номер порта. Если переадресация требуется только для одного порта, введите его номер повторно в поле **End Port**. Чтобы включить переадресацию для диапазона портов, введите в данном поле номер первого порта, а в поле **End Port** – номер последнего порта.
End Port	Введите номер порта. Если переадресация требуется только для одного порта, в поле **Start Port** и в этом поле укажите один и тот же номер порта. Чтобы включить переадресацию для нескольких портов, введите номер последнего порта в диапазоне. Началом диапазона будет порт, введенный выше в поле **Start Port**.
Server IP Address	Здесь вводится внутренний IP-адрес сервера.

Таблица 33 Экран NAT > Port Forwarding > Edit (продолжение)

ПОЛЕ	ОПИСАНИЕ
Back	Чтобы вернуться к предыдущему экрану, нажмите кнопку **Back**.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-793H.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

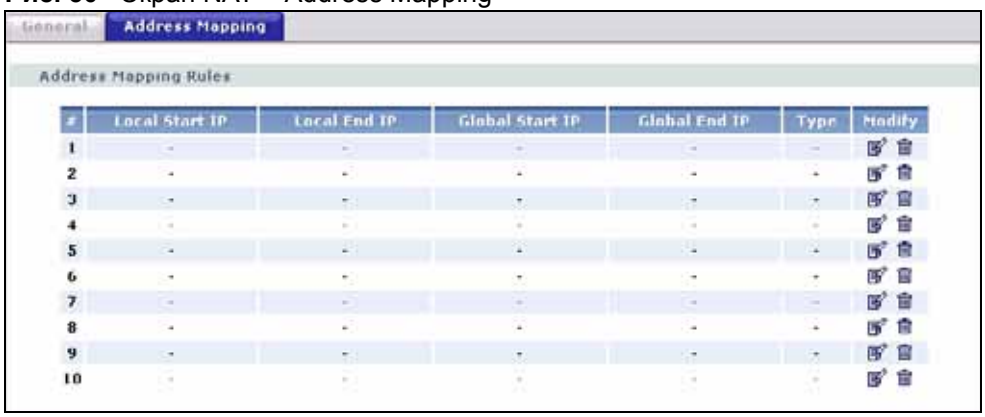
7.6 Привязка адресов

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

Порядок следования правил имеет важное значение, поскольку P-793H применяет правила в том порядке, в котором они определены. Когда правило соответствует текущему пакету, P-793H выполняет соответствующее действие, и остальные правила игнорируются. Если перед сконфигурированным правилом есть пустые правила, это созданное правило передвинется вверх на конкретное числое пустых правил. Например, если в текущем наборе правила 1 - 6 уже конфигурированы, а теперь ведется настройка правила номер 9. На экране с резюме набора новое правило будет правилом 7, а не 9. Если удалить правило 4, то правила 5 - 7 передвинутся вверх на 1 правило, поэтому старые правила 5, 6 и 7 станут новыми правилами 4, 5 и 6.

Этот экран позволяет изменить привязку адресов в P-793H. Чтобы открыть следующий экран, выберите **Network > NAT > Address Mapping**.

Рис. 50 Экран NAT > Address Mapping



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 34 Экран NAT > Address Mapping

ПОЛЕ	ОПИСАНИЕ
#	В этом поле указан порядковый номер правила.
Local Start IP	Это начальный внутренний локальный адрес (ILA). Локальные IP-адреса недоступны (**N/A**) в режиме привязки **Server**.

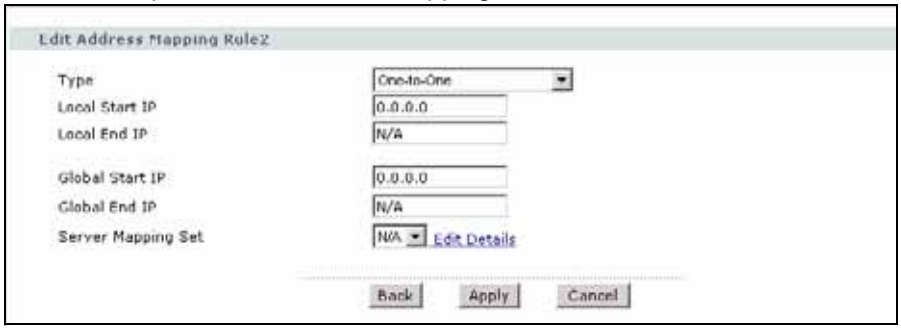
Таблица 34 Экран NAT > Address Mapping (продолжение)

ПОЛЕ	ОПИСАНИЕ
Local End IP	Это конечный внутренний локальный IP-адрес (ILA). Если правило предназначено для всех локальных IP-адресов, в графе **Local Start IP** будет указан адрес 0.0.0.0, а в графе **Local End IP** – адрес 255.255.255.255. Это поле недоступно (**N/A**) для типов привязки **One-to-One** и **Server**.
Global Start IP	Это начальный внутренний глобальный IP-адрес (IGA). Если поставщик услуг Интернета предоставляет динамический IP-адрес, введите 0.0.0.0. Это возможно только при типах привязки **Many-to-One** и **Server**.
Global End IP	Это - конечный внутренний глобальный IP-адрес (IGA). Это поле недоступно (**N/A**) для типов привязки **One-to-one**, **Many-to-One** и **Server**.
Type	**1-1**: режим "один к одному" привязывает один локальный IP-адрес к одному глобальному IP-адресу. Примечание: номера портов не изменяются для типа привязки NAT One-to-one (Один – один). **M-1**: режим "многие к одному" привязывает несколько локальных IP-адресов к одному глобальному IP-адресу. Этот режим эквивалентен однопользовательскому режиму SUA (фактически представляющему собой PAT – трансляцию адресов портов), который использовался в прежних маршрутизаторах ZyXEL. **M-M Ov** (с перегрузкой): режим "многие ко многим с перегрузкой" привязывает несколько локальных IP-адресов к совместно используемым глобальным IP-адресам. **MM No** (без перегрузки): Режим "многие ко многим без перегрузки" привязывает каждый локальный IP-адрес к уникальным глобальным IP-адресам. **Server (Сервер)**: Этот тип позволяет указывать внутренние серверы различных служб в NAT, которые должны быть доступными для внешнего мира.
Modify	Чтобы перейти на экран для редактирования правила привязки адресов, щелкните на значке редактирования. Для удаления существующего правила привязки адресов щелкните на значке удаления. При удалении одного правила все последующие правила смещаются вверх.

7.6.1 Редактирование правила привязки адресов

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

Рис. 51 Экран NAT > Address Mapping > Edit



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 35 Экран NAT > Address Mapping > Edit

ПОЛЕ	ОПИСАНИЕ
Type	Выберите тип привязки порта из числа следующих вариантов. **One-to-One**: в режиме "один к одному" привязывает один локальный IP-адрес к одному глобальному IP-адресу. Примечание: номера портов не изменяются для типа привязки NAT One-to-one (один – один). **Many-to-One**: режим "многие к одному" привязывает несколько локальных IP-адресов к одному глобальному IP-адресу. Этот режим эквивалентен однопользовательскому режиму SUA (фактически представляющему собой PAT – трансляцию адресов портов), который использовался в прежних маршрутизаторах ZyXEL. **Many-to-Many Overload**: режим "многие ко многим с перегрузкой" привязывает несколько локальных IP-адресов к совместно используемым глобальным IP-адресам. **Many-to-Many No Overload**: режим "многие ко многим без перегрузки" привязывает каждый локальный IP-адрес к уникальным глобальным IP-адресам. **Server**: Этот режим позволяет указывать внутренние серверы различных служб в NAT, которые должны быть доступными для внешнего мира.
Local Start IP	Это начальный локальный IP-адрес (ILA). Локальные IP-адреса недоступны (**N/A**) в режиме привязки **Server**.
Local End IP	Это конечный локальный IP-адрес (ILA). Если правило предназначено для всех локальных IP-адресов, введите 0.0.0.0 в поле **Local Start IP** и 255.255.255.255 в поле **Local End IP**. Это поле недоступно (**N/A**) для типов привязки **One-to-One** и **Server**.
Global Start IP	Это начальный глобальный IP-адрес (IGA). Если поставщик услуг Интернета предоставляет динамический IP-адрес, введите 0.0.0.0.
Global End IP	Это конечный глобальный IP-адрес (IGA). Это поле недоступно (**N/A**) для типов привязки **One-to-One**, **Many-to-One** и **Server**.
Server Mapping Set	Этот параметр доступен только в том случае, если поле **Type** имеет значение **Server**. Чтобы выбрать новый набор привязки сервера, в раскрывающемся меню укажите его порядковый номер.
Edit Details	Выберите эту ссылку, чтобы перейти на экран **Port Forwarding** (разд. 7.5 на стр. 117) для редактирования набора привязки сервера, выбранного в поле **Server Mapping Set**.
Back	Чтобы вернуться к предыдущему экрану, нажмите кнопку **Back**.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-793H.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

Часть III
Безопасность и дополнительные настройки

8

Межсетевые экраны

В этой главе даны основные сведения о межсетевых экранах и кратко рассмотрен межсетевой экран в P-793H.

8.1 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 надежной сети от ненадежной. 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. 9.6 на стр. 144.

Просмотр правил межсетевого экрана описан в разд. 9.7 на стр. 145.

Настройка правил межсетевого экрана описана в разд. 9.7.1 на стр. 147.

Настройка собственных типов сетевых служб описана в разд. 9.7.2 на стр. 149.

Настройка пороговых значений для межсетевых экранов описана в разд. 9.10.3 на стр. 157.

8.2 Типы межсетевых экранов

Существует три основных типа межсетевых экранов:

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

8.2.1 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.

8.2.2 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.

8.2.3 Динамические межсетевые экраны

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. 8.5 на стр. 131.

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

8.3 Краткий обзор межсетевого экрана ZyXEL

Межсетевой экран в составе P-793H представляет собой динамический межсетевой экран, который может быть активирован для защиты от атак, провоцирующих отказ в обслуживании (DoS). Назначение P-793H состоит в том, чтобы частная локальная сеть (LAN) была надежно подключена к Интернету. P-793H может использоваться для предотвращения хищения, разрушения и модификации данных, а также операций по регистрации, которые могут иметь важное значение для безопасности сети. P-793H также имеет средства фильтрации пакетов.

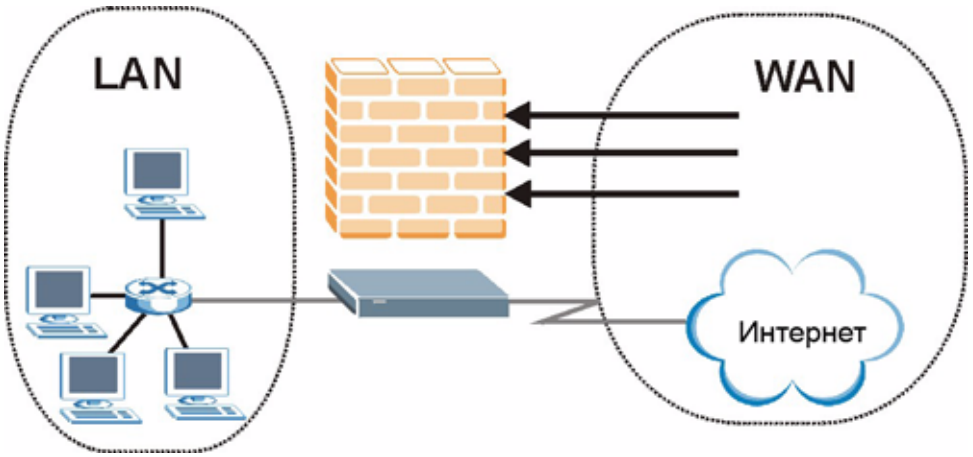
P-793H размещается между локальной сетью и Интернетом. Благодаря этому он функционирует как безопасный интернет-центр для всех данных, пересылаемых между Интернетом и LAN.

P-793H 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.

8.3.1 Атаки, вызывающие отказ в обслуживании

Рис. 52 P-793H Применение межсетевого экрана



8.4 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-793H предусмотрено обнаружение и нейтрализация всех известных видов DoS-атак.

8.4.1 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.

Приложение G на стр. 429 содержит описание распространенных номеров портов IP.

8.4.2 Типы DoS-атак

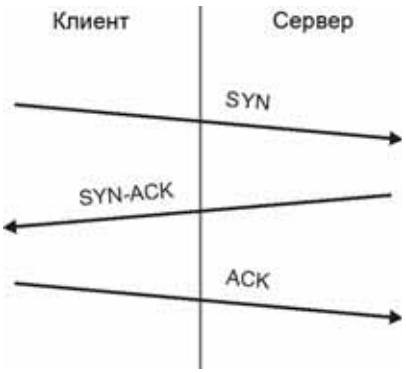
Существует четыре типа DoS-атак:

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.

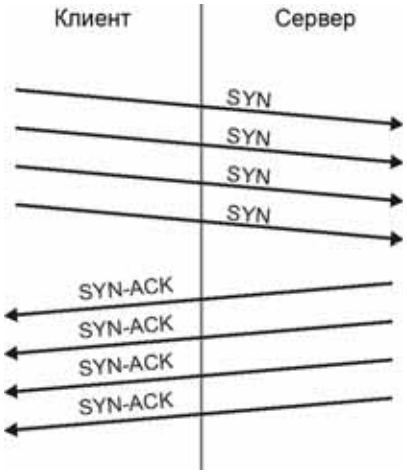
Рис. 53 Три этапа установления сеанса



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.

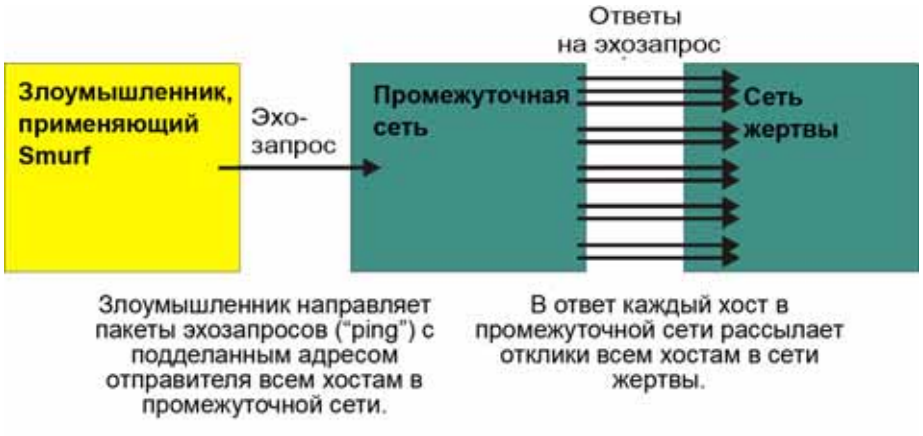
Рис. 54 SYN Flood



- 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. 55 Атака Smurf



8.4.2.1 Уязвимость ICMP

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

Таблица 36 Команды ICMP, вызывающие предупреждения

5	REDIRECT
13	TIMESTAMP_REQUEST
14	TIMESTAMP_REPLY
17	ADDRESS_MASK_REQUEST
18	ADDRESS_MASK_REPLY

8.4.2.2 Недопустимые команды (NetBIOS и SMTP)

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

Таблица 37 Допустимые команды NetBIOS

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

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

Таблица 38 Допустимые команды SMTP

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

8.4.2.3 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.

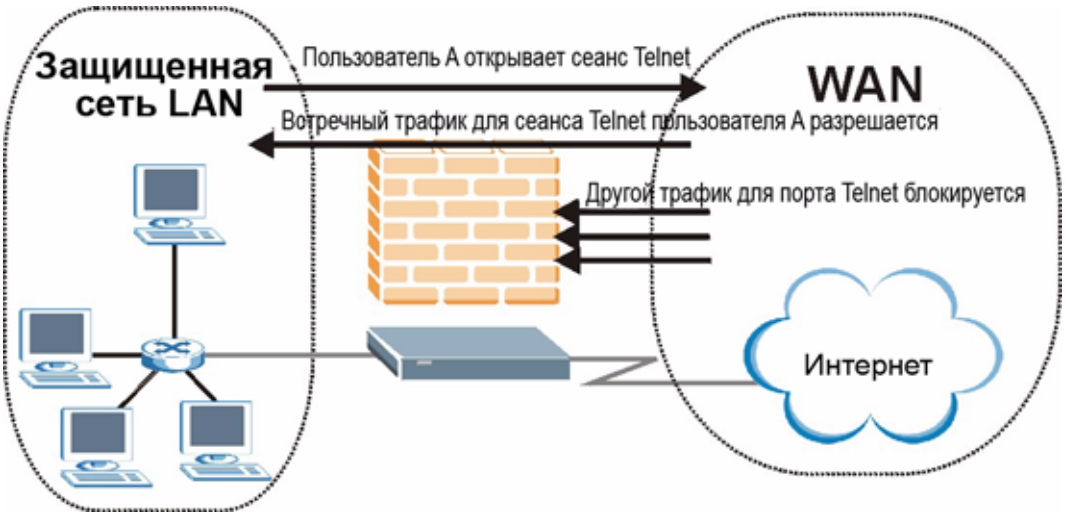
Часто для DoS-атак также используется прием, известный как **подмена IP-адреса**. Целью подмены может быть проникновение в системы, сокрытие истинного местонахождения хакера или увеличение эффекта DoS-атаки. Подмена IP-адреса используется для несанкционированного доступа на компьютеры, при этом маршрутизатор 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-793H блокирует все попытки подмены IP-адреса.

8.5 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-793H защищает частные LAN от хакеров и вандалов в Интернете. По умолчанию механизм динамического анализа пакетов в P-793H 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. 56 Динамический анализ пакетов



На приведенном выше рисунке показано действие правил межсетевого экрана P-793H 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.

8.5.1 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.

8.5.2 Динамический анализ пакетов и P-793H

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 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.

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-793H (как в случае с "виртуальными соединениями", создаваемыми для UDP и ICMP).

8.5.3 Безопасность TCP

P-793H 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-793H 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).

8.5.4 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-793H 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.

8.5.5 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-793H 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.

8.6 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.

8.6.1 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.

8.7 Сравнение фильтрации пакетов и межсетевого экрана

Ниже проведено краткое сравнение функций фильтрации пакетов и межсетевого экрана, реализованных в P-793H.

8.7.1 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.

8.7.1.1 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).

8.7.2 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.

8.7.2.1 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).

9

Настройка межсетевого экрана

В этой главе описывается активация и настройка межсетевого экрана в P-793H.

9.1 Методы доступа

Веб-конфигуратор является наиболее универсальным инструментом настройки межсетевого экрана, имеющимся в устройстве P-793H. 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.

9.2 Общие сведения о политиках межсетевого экрана

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

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

По умолчанию функция динамического анализа пакетов в P-793H разрешает прохождение пакетов в следующих направлениях:

- Из LAN в LAN/маршрутизатор (LAN to LAN/Router).
  Это позволяет компьютерам в составе LAN управлять P-793H и обмениваться данными с сетями или подсетями, связанными с интерфейсом LAN.
- Для трафика из LAN в WAN.

По умолчанию функция динамического анализа пакетов в P-793H 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-793H как шлюз для связи с другими компьютерами в WAN и/или для управления P-793H.
  Можно также определить дополнительные наборы правил или модифицировать существующие, но при этом необходимо соблюдать крайнюю осторожность.

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-793H по умолчанию.

9.3 Логика правил

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

9.3.1 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.

9.3.2 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.

9.3.3 Основные поля для настройки правил

9.3.3.1 Action

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

"Drop" означает, что межсетевой экран попросту отбрасывает пакет. "Reject" означает, что межсетевой экран отбрасывает пакет, возвращая отправителю ICMP-сообщение о недоступности адресата.

9.3.3.2 Service

Выберите сетевую службу из списка **Service**. Если требуемая служба в списке отсутствует, необходимо сначала ее определить. Подробнее о предопределенных типах служб см. Приложение G на стр. 429 .

9.3.3.3 Source Address

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

9.3.3.4 Destination Address

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

9.4 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" относятся к пакетам, входящим с соответствующего интерфейса (LAN или WAN). "LAN to LAN/Router" обозначает политики для пакетов, следующих из LAN на P-793H (т.е. политики управления P-793H 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 правила "WAN to WAN/ Router" применяются к порту WAN.

9.4.1 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 служат для защиты локальной сети от несанкционированного доступа из WAN.

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.

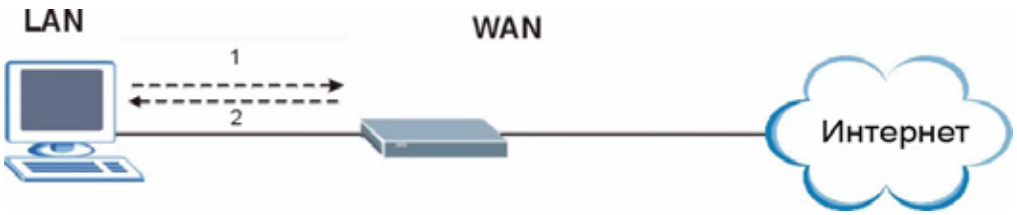
9.4.2 Предупреждения

Предупреждения – это сообщения о событиях (например, об атаках), требующих немедленного внимания. На экране **Edit Rule** (см. рис. 62 на стр. 147) 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. Подробное описание см. в главе, посвященной ведению журналов.

9.5 Треугольный маршрут

Когда активирован межсетевой экран, P-793H выступает в качестве защищенного шлюза между локальной сетью и Интернетом. В идеальной топологии сети весь входящий и исходящий сетевой трафик проходит через P-793H, и ваша локальная сеть защищена от атак.

Рис. 57 Идеальная топология сети с межсетевым экраном



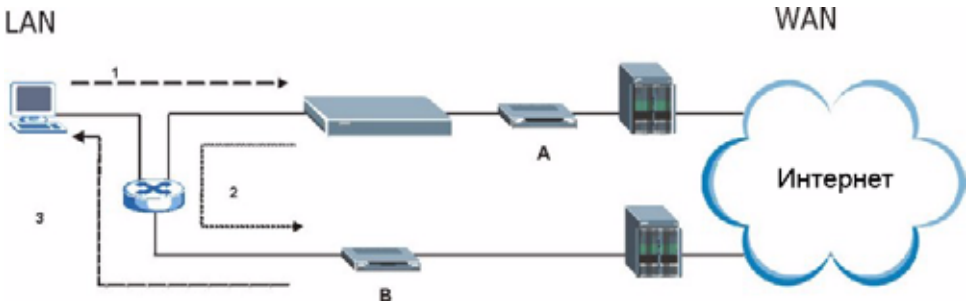
9.5.1 Проблема треугольного маршрута

У вас может иметься несколько альтернативных маршрутов к одному или нескольким поставщикам услуг Интернета. Если альтернативный шлюз находится в сети LAN (и его IP-адрес лежит в одной подсети с адресом P-793H в сети LAN), возникает проблема "треугольного маршрута" (также называемого асимметричным маршрутом), природу которой иллюстрирует следующая ситуация.

1. Компьютер в сети LAN устанавливает соединение, посылая пакет SYN на принимающий сервер в сети WAN.
2. P-793H пересылает пакет SYN через шлюз **A** в локальной сети LAN по направлению к WAN.
3. Ответ из WAN поступает напрямую на компьютер в LAN, минуя P-793H.

В результате P-793H сбрасывает соединение как неподтвержденное.

Рис. 58 Проблема треугольного маршрута



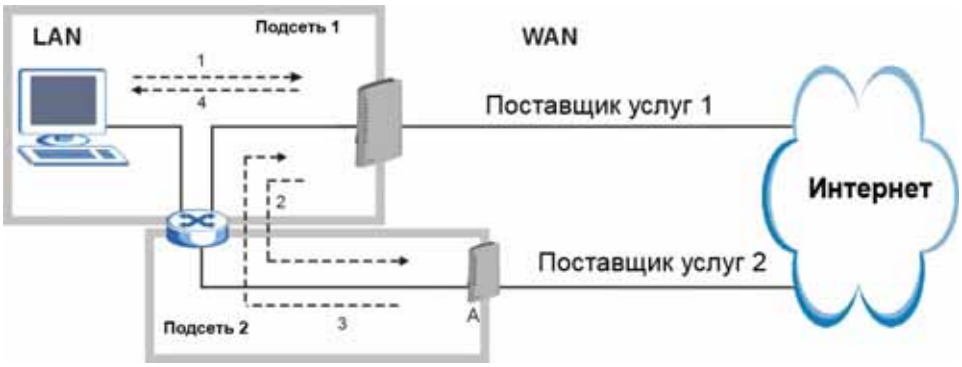
9.5.2 Решение проблемы треугольного маршрута

Можно разрешить P-793H устанавливать сеансы с треугольными маршрутами. Однако это позволяет пропускать трафик из WAN непосредственно к компьютерам в LAN, минуя P-793H и межсетевой экран в его составе.

Другой способ решения проблемы треугольного маршрута состоит в совмещении IP-адресов. Совмещение IP-адресов (IP aliasing) позволяет разделить физическую сеть на логические секции через один и тот же интерфейс Ethernet. P-793H поддерживает до трех логических интерфейсов LAN, при этом P-793H выступает шлюзом для каждой логической сети. Разнеся вашу локальную сеть и шлюз **A** по различным подсетям, вы заставите весь возвращающийся сетевой трафик проходить через P-793H 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-793H пересылает пакет на шлюз A, находящийся в подсети 2.
3. Отклик из сети WAN поступает на P-793H.
4. P-793H в свою очередь пересылает его компьютеру в локальной сети, находящемуся в подсети 1.

Рис. 59 Совмещение IP-адресов

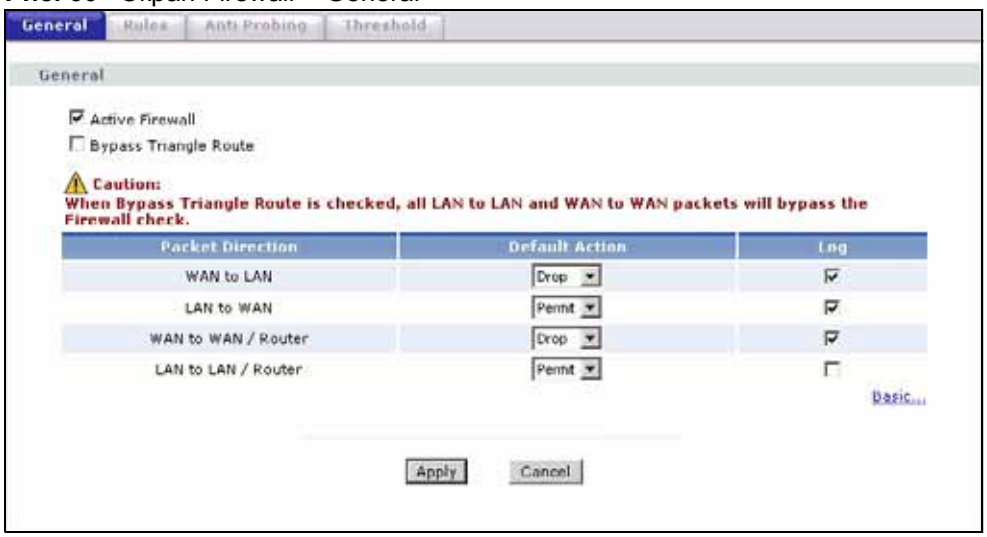


9.6 Общая политика межсетевого экрана

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

Для дополнительной информации см. разд. 8.1 на стр. 125.

Рис. 60 Экран Firewall > General



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 39 Экран Firewall > General

ПОЛЕ	ОПИСАНИЕ
Active Firewall	Установите этот флажок, чтобы активировать межсетевой экран. Когда межсетевой экран активирован, P-793H 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-793H 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.

Таблица 39 Экран Firewall > General (продолжение)

ПОЛЕ	ОПИСАНИЕ
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-793H или к самому устройству P-793H.
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-793H.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

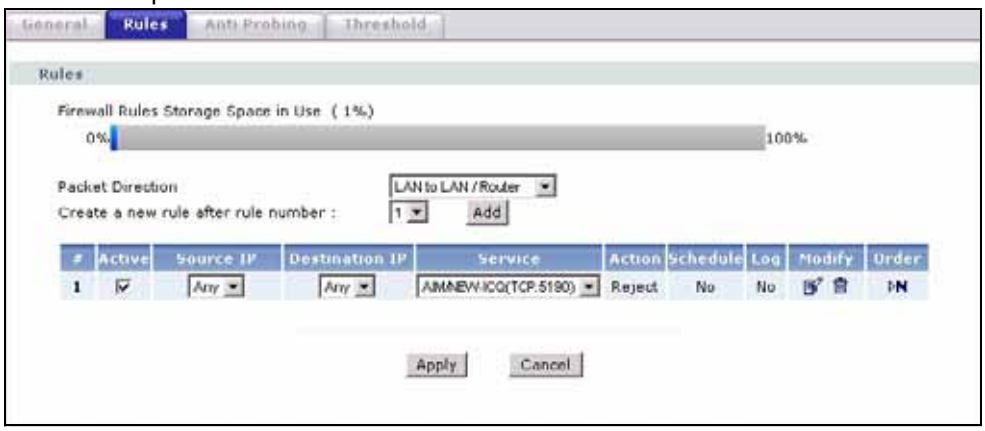
9.7 Сводка правил межсетевого экрана

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

Для дополнительной информации см. разд. 8.1 на стр. 125.

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

Рис. 61 Экран Firewall > Rules



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 40 Экран Firewall > Rules

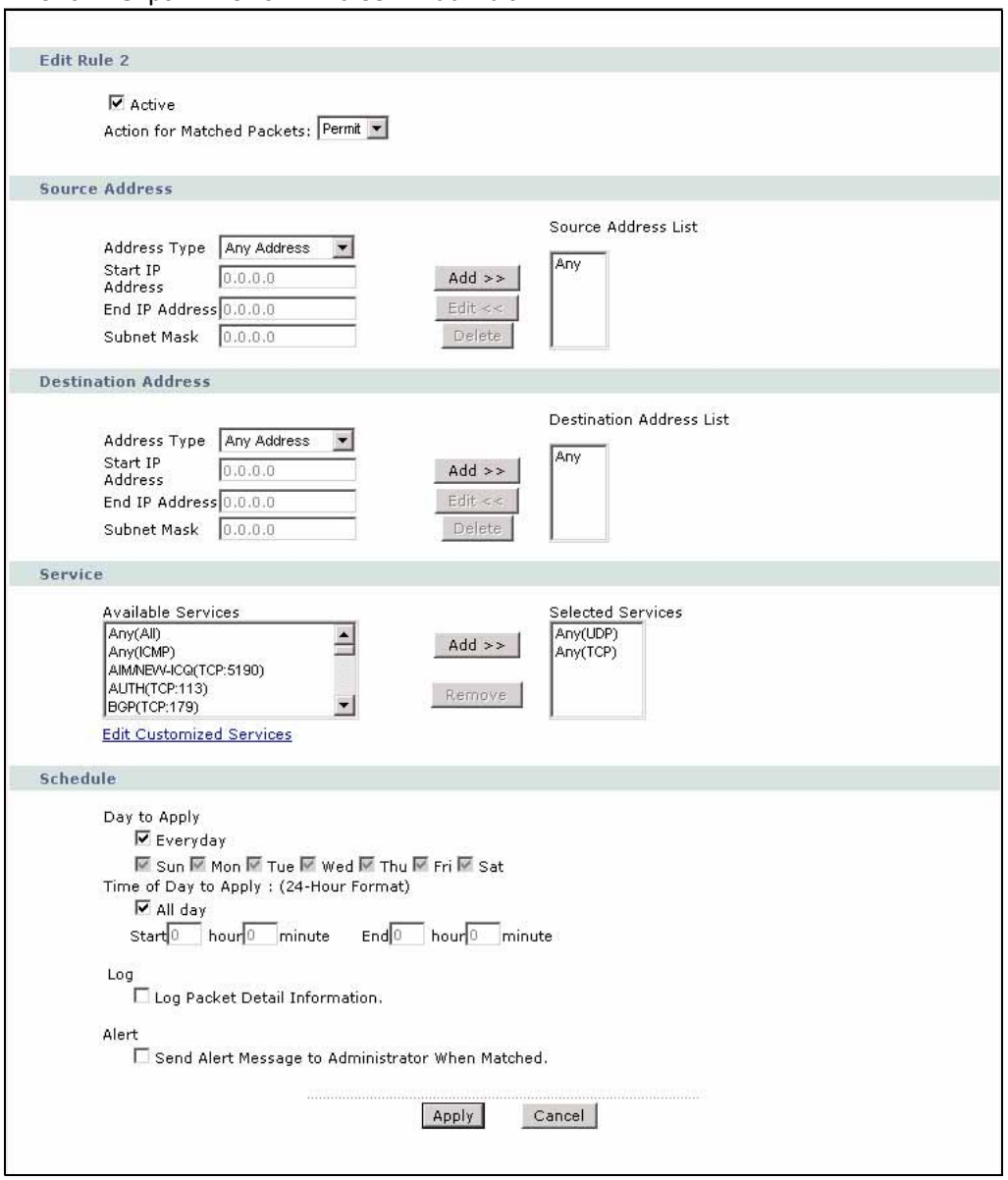
ПОЛЕ	ОПИСАНИЕ
Firewall Rules Storage Space in Use	Этот неизменяемый индикатор сообщает, сколько из объема памяти P-793H, отведенного под правила межсетевого экрана, используется в настоящий момент. Когда используется не более 80% объема, индикатор имеет зеленый цвет. При превышении 80% объема индикатор становится красным.
Packet Direction	Этот раскрывающийся список позволяет выбрать направление прохождения пакетов для настройки правил межсетевого 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 действиями межсетевого экрана по умолчанию, указанными 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 Приложение G на стр. 429.
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**. Чтобы изменить порядок следования правил, в поле **Move the rule to** введите новый номер правила и нажмите кнопку **Move**. Порядок следования правил имеет большое значение, поскольку правила применяются по очереди.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-793H.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

9.7.1 Настройка правил межсетевого экрана

Для дополнительной информации см. разд. 8.1 на стр. 125.

Этот экран служит для создания и редактирования правил межсетевого экрана.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. 62 Экран Firewall > Rules > Add/Edit



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 41 Экран Firewall > Rules > Add/Edit

ПОЛЕ	ОПИСАНИЕ
Edit Rule #	
Active	Выберите этот параметр, чтобы включить данное правило межсетевого экрана.

Таблица 41 Экран Firewall > Rules > Add/Edit (продолжение)

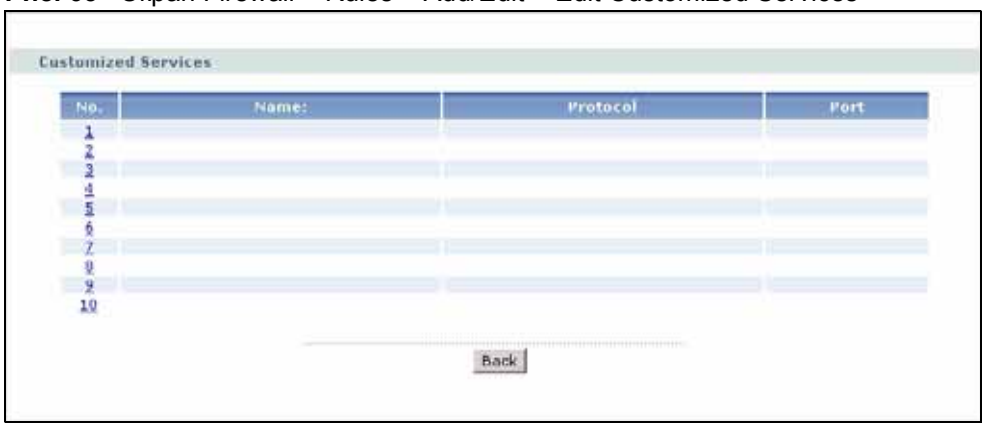
ПОЛЕ	ОПИСАНИЕ
Action for Matched Packet	В раскрывающемся списке выберите действие, выполняемое межсетевым экраном над пакетами, которым соответствует правило. Выберите **Drop**, чтобы отбрасывать пакеты, не возвращая отправителю пакет сброса TCP или ICMP-сообщение о недоступности адресата. Выберите **Reject**, 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.
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	Это поле доступно в том случае, если в поле **Address Type** выбран любой параметр, кроме **Any Address**. Введите в этом поле один IP-адрес или начальный IP-адрес диапазона.
End IP Address	Это поле доступно в том случае, если в поле **Address Type** выбран параметр **Range Address**. Введите в этом поле конечный IP-адрес диапазона.
Subnet Mask	Это поле доступно в том случае, если в поле **Address Type** выбран параметр **Subnet Address**. 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	Приложение G на стр. 429 содержит более подробное описание предусмотренных сетевых служб. 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 Services	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-793H, перейдите на страницу **Log Settings** и выберите категорию журналов **Access Control**.
Alert	
Send Alert Message to Administrator When Matched	Отметьте этот флажок, чтобы устройство P-793H генерировало предупреждение для пакетов, соответствующих правилу.
Apply	Нажмите кнопку **Apply** для сохранения настроек и выхода из данного экрана.
Cancel	Чтобы закрыть экран, не сохраняя изменений, выберите **Cancel**.

9.7.2 Настройка собственных портов для сетевых служб

P-793H позволяет задать собственные типы служб и номера портов, не предусмотренные в заводской конфигурации. Подробный перечень номеров портов и сетевых служб см. на сайте IANA (Комитета по цифровым адресам в Интернете). Дополнительные сведения об этих типах пакетов см. в Приложение G на стр. 429. Чтобы задать собственный номер порта для сетевой службы, во время редактирования правила межсетевого экрана пройдите по ссылке **Edit Customized Services**. Откроется следующий экран.

Для дополнительной информации см. разд. 8.1 на стр. 125.

Рис. 63 Экран Firewall > Rules > Add/Edit > Edit Customized Services



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 42 Экран Firewall > Rules > Add/Edit > Edit Customized Services

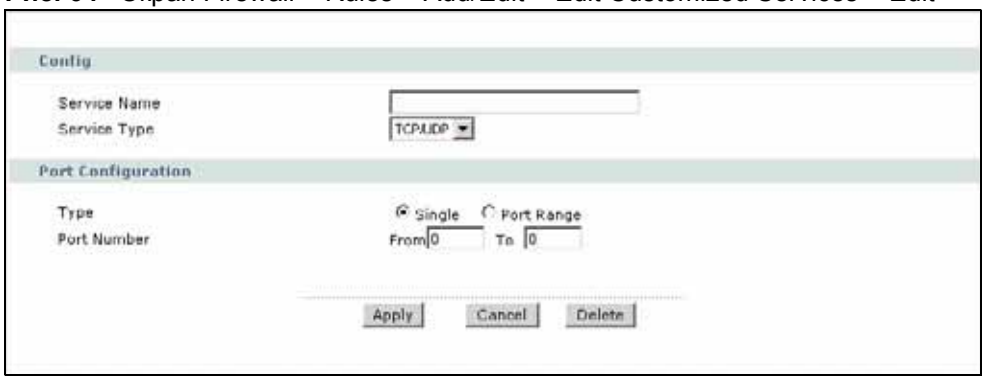
ПОЛЕ	ОПИСАНИЕ
No.	В этом поле отображается порядковый номер настроенной вами сетевой службы. Щелкните на номере службы, чтобы перейти на экран **Firewall Customized Services Config** для настройки или редактирования собственных сетевых служб. Дополнительные сведения см. в разд. 9.7.3 на стр. 149.
Name	В этом поле отображается наименование настроенной вами сетевой службы.
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**.

9.7.3 Задание собственной сетевой службы

Этот экран служит для задания нового собственного номера порта или редактирования существующего. На экране **Firewall Customized Services** щелкните на порядковом номере правила. Откроется следующий экран.

Для дополнительной информации см. разд. 8.1 на стр. 125.

Рис. 64 Экран Firewall > Rules > Add/Edit > Edit Customized Services > Edit



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 43 Экран Firewall > Rules > Add/Edit > Edit Customized Services > Edit

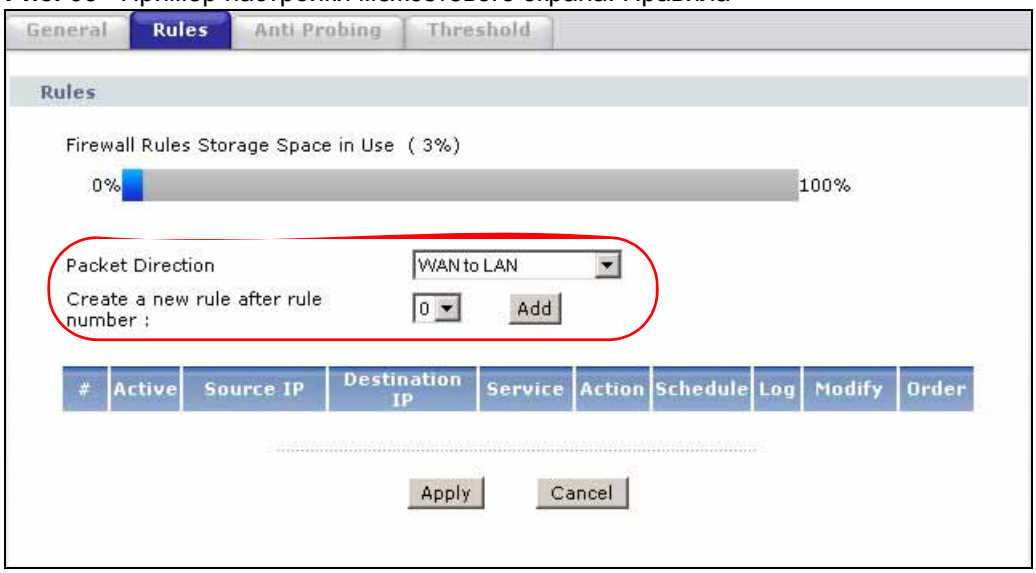
ПОЛЕ	ОПИСАНИЕ
Config	
Service Name	Укажите уникальное название для данного порта.
Service Type	Выберите IP-порт (**TCP**, **UDP** или **TCP/UDP**), который соответствует настроенному порту, выбранному в раскрывающемся списке.
Port Configuration	
Type	Выберите **Single**, чтобы указать только один порт, или **Port 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.
Cancel	Для возврата к предыдущему экрану нажмите кнопку **Cancel**.
Delete	Чтобы удалить существующее правило и возвратиться на предыдущий экран, выберите **Delete**.

9.8 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. 65 Пример настройки межсетевого экрана: Правила



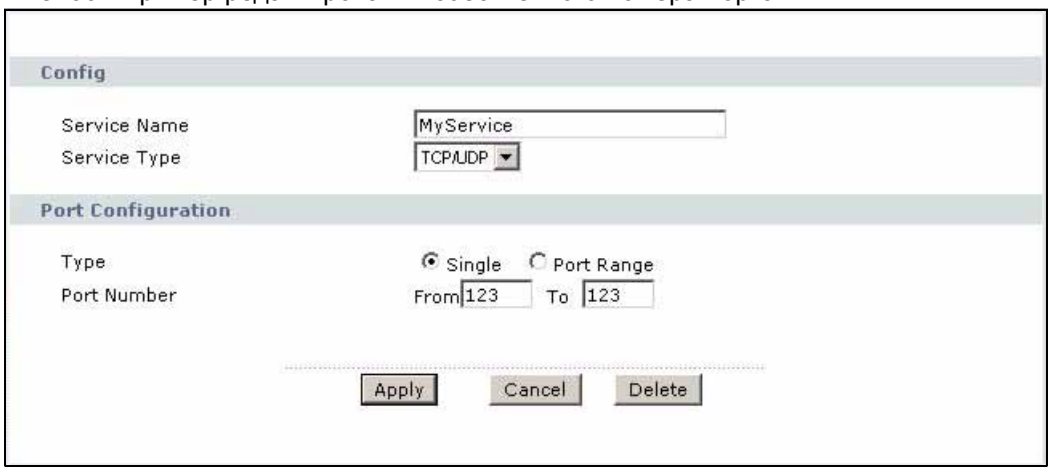
3 На экране **Rules** выберите порядковый номер правила, за которым должно следовать вновь добавляемое правило. Например, если выбран номер 6, новое правило получит номер 7, а прежнее правило №7 (если оно существует) станет правилом №8.

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**.

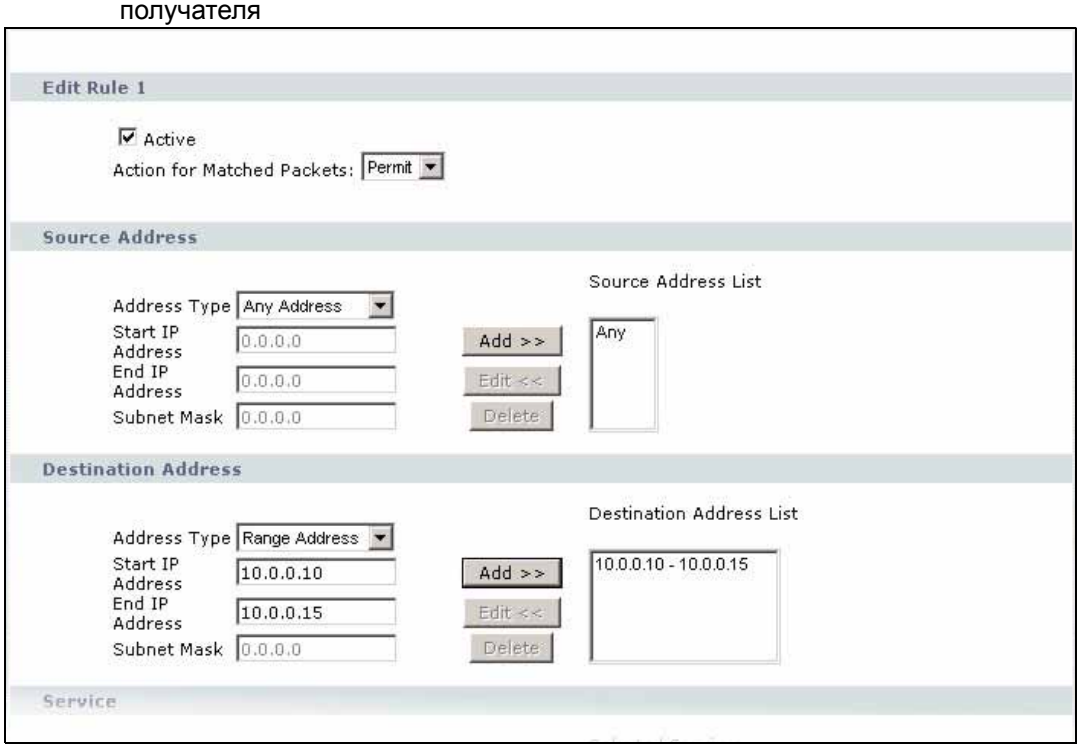
Рис. 66 Пример редактирования собственного номера порта



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

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

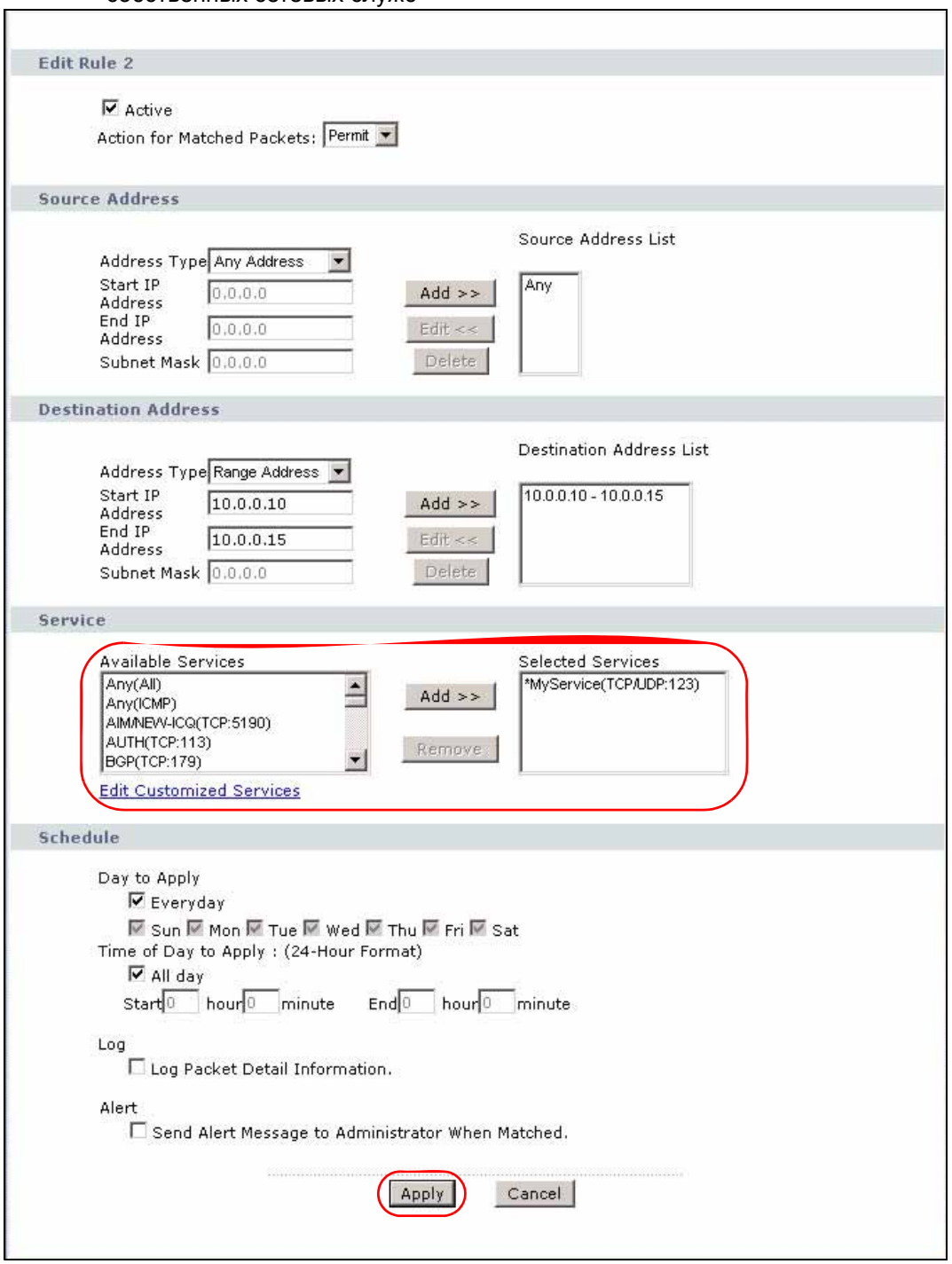
Рис. 67 Пример настройки межсетевого экрана: Редактирование правил: адрес получателя



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

В списках **Services** и **Rules** перед названиями сетевых служб, заданных пользователями, стоит знак "*".

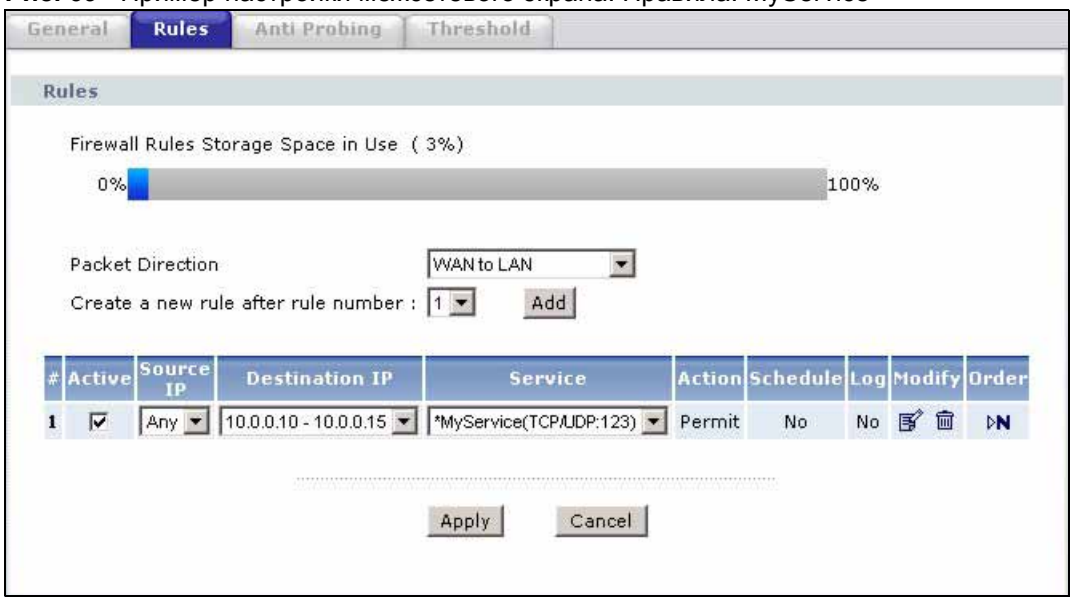
Рис. 68 Пример настройки межсетевого экрана: Редактирование правил: выбор собственных сетевых служб



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. 69 Пример настройки межсетевого экрана: Правила: MyService



9.9 Защита от зондирования

Если внешний пользователь попытается прозондировать неподдерживаемый порт P-793H, автоматически будет возвращен пакет с откликом ICMP (протокол управляющих сообщений в Интернете). Это позволяет внешнему пользователю узнать о том, что P-793H существует. P-793H поддерживает защиту от зондирования, которая не допускает пересылки откликов на пакеты ICMP. Это препятствует обнаружению P-793H посторонними при зондировании неподдерживаемых портов.

ICMP (межсетевой протокол контрольных сообщений) представляет собой протокол управления сообщениями и предоставления отчетов об ошибках при взаимодействии между сервером хоста и Интернетом. В ICMP используются датаграммы межсетевого протокола (IP), но сообщения обрабатываются программным обеспечением TCP/IP и отображаются в понятном виде для пользователя приложения.

Подробное описание см. в разд. 8.1 на стр. 125.

Чтобы вызвать показанный ниже экран, выберите **Security > Firewall > Anti Probing**.

Рис. 70 Экран Firewall > Anti Probing

Поля изображенного выше экрана описаны в следующей таблице.

Таблица 44 Экран Firewall > Anti Probing

ПОЛЕ	ОПИСАНИЕ
Respond to PING on	Если выбрано значение **Disable**, P-793H не будет реагировать на входящие эхозапросы. 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-793H хакерами путем зондирования неиспользуемых портов. В этом случае P-793H не будет отвечать на запросы неиспользуемых портов, что позволит скрыть неиспользуемые порты и P-793H. По умолчанию этот параметр не выбран, и P-793H 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-793H, прежде чем они будут обрабатываться механизмом противодействия зондированию. Поэтому если межсетевой экран заблокирует пакет с попыткой зондирования, то действие, предпринимаемое P-793H, 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**, чтобы сохранить изменения в P-793H.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

9.10 Пороговые значения для защиты от DoS

Для защиты от DoS-атак в P-793H 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. 9.10.3 на стр. 157.

9.10.1 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.

9.10.2 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. 53 на стр. 128). Для UDP частично открытыми сеансами считаются те, в которых межсетевой экран не обнаружил встречного трафика.

P-793H 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-793H начинает удалять частично открытые сеансы, освобождая ресурсы для новых запросов на соединение. P-793H 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-793H начинает удалять частично открытые сеансы, освобождая ресурсы для новых запросов на соединение. P-793H 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.

9.10.2.1 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-793H начинает удалять частично открытые сеансы, руководствуясь одним из следующих методов.

- Если величина **Blocking Time** равна 0 (значение по умолчанию), P-793H 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-793H блокирует все новые запросы на подключение к данному хосту, оставляя серверу время для обработки существующих соединений. P-793H продолжает блокировать все вновь поступающие запросы на подключение, пока не истечет задержка **Blocking Time**.

9.10.3 Настройка пороговых значений для межсетевого экрана

При превышении порога **TCP Maximum Incomplete** P-793H также направляет предупреждения. Глобальные значения порога и времени блокировки применяются ко всем TCP-соединениям.

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

Рис. 71 Экран Firewall > Threshold

Поля изображенного выше экрана описаны в следующей таблице.

Таблица 45 Экран Firewall > Threshold

ПОЛЕ	ОПИСАНИЕ
Denial of Service Thresholds	
One Minute Low	Введите частоту накопления частично открытых сеансов, при которой межсетевой экран прекращает удалять частично открытые сеансы. P-793H продолжает удалять частично открытые сеансы, пока это необходимо, т.е. пока частота накопления частично открытых сеансов не опустится ниже этого порога. Пример см. в описании параметра **One Minute High**.
One Minute High	Введите частоту накопления частично открытых сеансов, при которой межсетевой экран начинает удалять частично открытые сеансы. Когда частота накопления частично открытых сеансов превышает этот порог, P-793H начинает удалять частично открытые сеансы, освобождая ресурсы для новых запросов на соединение. Например, если параметр **One Minute Low** равен 80, а параметр **One Minute High** равен 100, P-793H начинает удалять частично открытые сеансы, когда за последнюю минуту обнаруживается более 100 попыток установления сеанса, и прекращает удалять частично открытые сеансы, если за последнюю минуту число обнаруженных попыток установления сеанса не превышает 80.
Maximum Incomplete Low	Введите число существующих частично открытых сеансов, при котором межсетевой экран прекращает удалять частично открытые сеансы. P-793H продолжает удалять частично открытые сеансы, пока это необходимо, т.е. пока число существующих частично открытых сеансов не опустится ниже данного порога. Пример см. в описании параметра **Maximum Incomplete High**.

Таблица 45 Экран Firewall > Threshold (продолжение)

ПОЛЕ	ОПИСАНИЕ
Maximum Incomplete High	Введите число существующих частично открытых сеансов, при котором межсетевой экран начинает удалять частично открытые сеансы. Когда число существующих частично открытых сеансов превышает этот порог, P-793H 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**. Например, если параметр **Maximum Incomplete Low** равен 80, а параметр **Maximum Incomplete High** равен 100, то P-793H 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	Введите 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.
Action taken when 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-793H 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-793H.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

10

Фильтрация содержания

В этой главе описывается настройка фильтрации содержания.

10.1 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-793H будет применять фильтрацию содержания. Также можно указать доверенные IP-адреса в локальной сети, для которых P-793H не будет применять фильтрацию содержания.

10.2 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-793H 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-793H блокировать сайты, в URL которых содержатся определенные ключевые слова, выберите **Security > Content Filter**. Появится изображенный ниже экран.

Рис. 72 Экран Content Filter > Keyword

Поля изображенного выше экрана описаны в следующей таблице.

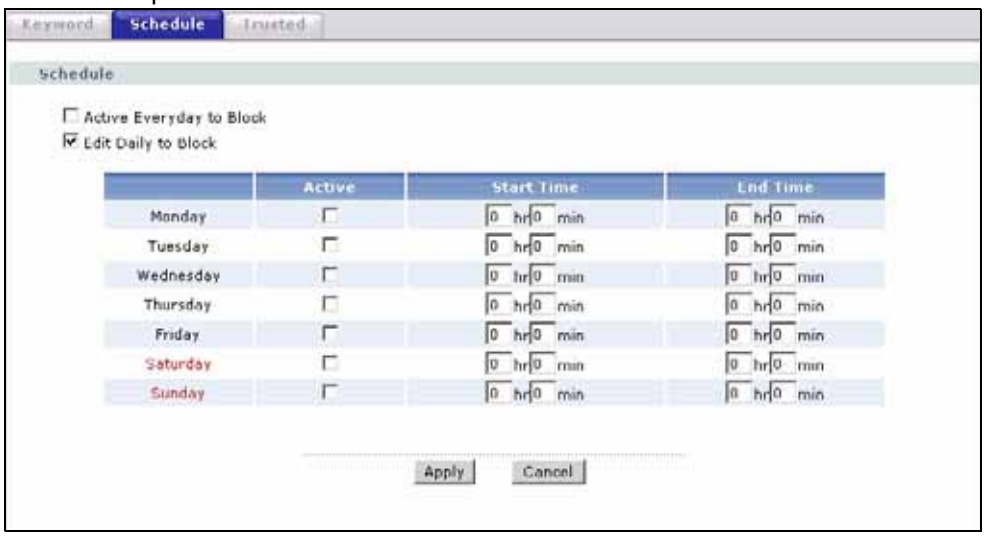
Таблица 46 Экран Content Filter > Keyword

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-793H 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-793H.
Cancel	Чтобы вернуться к прежним настройкам, нажмите **Cancel**.

10.3 Настройка графика

Этот экран служит для задания дней и периодов в течение дня, в которые P-793H осуществляет фильтрацию содержания. Выберите **Security > Content Filter** > **Schedule**. Появится изображенный ниже экран.

Рис. 73 Экран Content Filter > Schedule



Поля изображенного выше экрана описаны в следующей таблице.

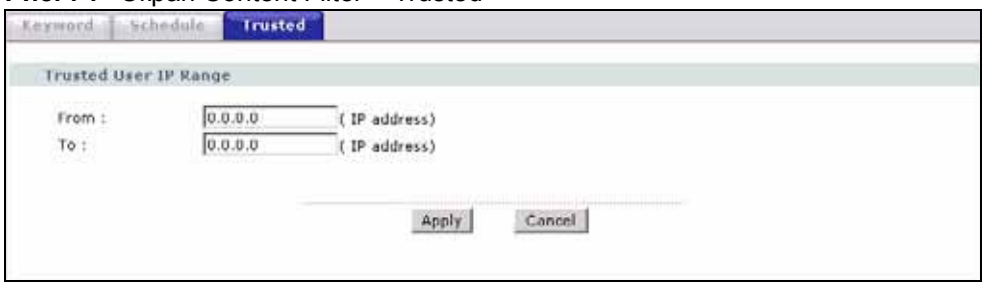
Таблица 47 Экран Content Filter > Schedule

ПОЛЕ	ОПИСАНИЕ
Schedule	Выберите **Active Everyday to Block**, 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**.

10.4 Настройка адресов доверенных компьютеров

Этот экран позволяет в исключительном порядке отменить на P-793H фильтрацию содержания для определенных пользователей в локальной сети. Выберите **Security > Content Filter** > **Trusted**. Появится изображенный ниже экран.

Рис. 74 Экран Content Filter > Trusted



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 48 Экран Content Filter > Trusted

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-793H.
Cancel	Чтобы вернуться к прежним настройкам, нажмите **Cancel**.

11

Сети VPN на базе IPSec

В этой главе описаны настройка и управление VPN на базе IPSec в P-793H.

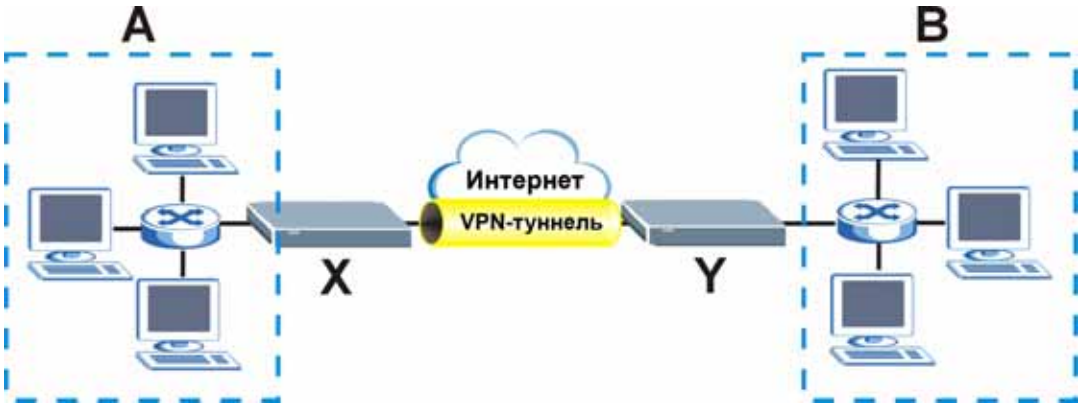
11.1 Обзор VPN/IPSec

VPN (виртуальная частная сеть) реализует защищенный обмен данными между двумя физическими объектами, не требуя затрат на организацию между ними выделенной линии. Защита VPN реализуется в комплексе: туннелирование, шифрование, аутентификация, управление доступом и аудит. Сети VPN используются для пересылки трафика через Интернет или любую незащищенную сеть, использующую протокол TCP/IP для обмена данными.

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.

На следующем рисунке изображен пример VPN-туннеля.

Рис. 75 VPN: пример

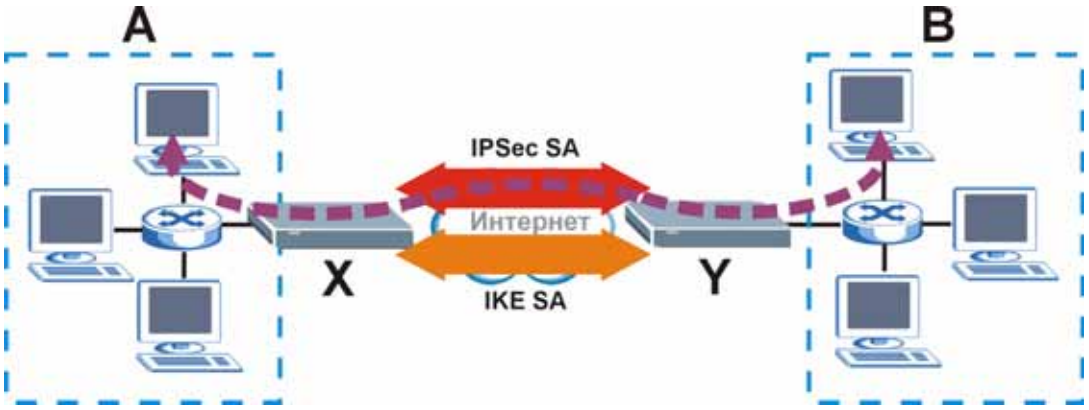


VPN-туннель соединяет P-793H (**X**) с удаленным маршрутизатором IPSec (**Y**). Эти маршрутизаторы соединяют локальную сеть (**A**) с удаленной сетью (**B**).

VPN-туннель обычно устанавливается в две фазы. Каждая фаза формирует ассоциацию безопасности (SA) – соглашение, указывающее параметры безопасности, используемые P-793H и удаленным маршрутизатором IPSec. На первой фазе устанавливается SA для обмена ключами через Интернет (IKE) между P-793H и удаленным маршрутизатором

IPSec. На второй фазе сформированная IKE SA используется для защищенного согласования IPSec SA, посредством которой P-793H и удаленный маршрутизатор IPSec могут обмениваться данными с компьютерами в локальной и удаленной сети. На следующем рисунке приведен пример.

Рис. 76 VPN: IKE SA и IPSec SA



В этом примере компьютер, находящийся в сети **A**, обменивается данными с компьютером в сети **B**. В пределах сетей **A** и **B** данные пересылаются обычным образом. На участке между маршрутизаторами **X** и **Y** данные защищены туннелированием, шифрованием и аутентификацией IPSec SA. IPSec SA устанавливается в защищенном сеансе, который маршрутизаторы **X** и **Y** заранее устанавливают посредством IKE SA.

В остальной части этого раздела IKE SA и IPSec SA будут рассмотрены более подробно.

11.1.1 Обзор IKE SA

IKE SA обеспечивает защищенное соединение между P-793H и удаленным маршрутизатором IPSec.

Установление IKE SA осуществляется в несколько этапов. Режим согласования определяет необходимое число этапов. Существует два режима согласования: основной и агрессивный. Основной режим надежнее защищен, а агрессивный отличается большим быстродействием.

Оба маршрутизатора должны использовать один и тот же режим согласования.

Более подробно эти режимы рассмотрены в разд. 11.1.2.1 на стр. 167. Примеры в этом разделе используют основной режим.

11.1.1.1 IP-адреса P-793H и удаленного маршрутизатора IPSec.

Для установления IKE SA в P-793H необходимо указать IP-адреса P-793H и удаленного маршрутизатора IPSec.

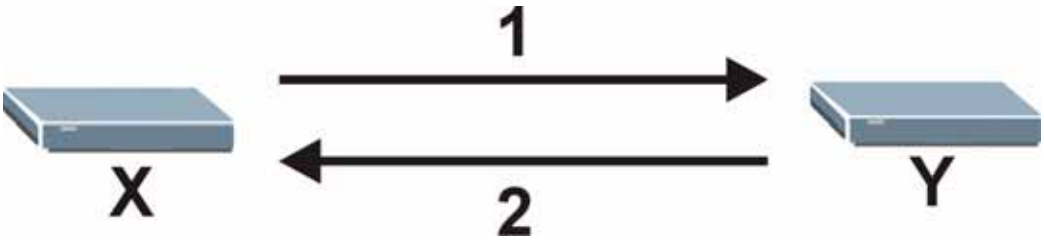
Для идентификации P-793H, как правило, вводится статический IP-адрес или доменное имя, но в некоторых случаях P-793H может предлагать альтернативные варианты, например, использование IP-адреса порта или интерфейса.

Для удаленного маршрутизатора IPSec обычно также можно указать статический IP-адрес или доменное имя. Если IP-адрес удаленного маршрутизатора IPSec неизвестен (например, для сотрудников, работающих удаленно), сформировать IKE SA по-прежнему возможно, но инициировать установление IKE SA сможет только удаленный маршрутизатор.

11.1.1.2 Предложение IKE SA

Предложение IKE SA указывает алгоритмы шифрования и идентификации, а также группу ключей Диффи-Хелмана (DH), используемые P-793H и удаленным маршрутизатором IPSec в IKE SA. В основном режиме это осуществляется на этапах 1 и 2, как показано ниже.

Рис. 77 IKE SA: основной режим согласования, этапы 1 - 2: Предложение IKE SA



P-793H направляет одно или несколько предложений удаленному маршрутизатору IPSec. (Некоторые устройства допускают настройку только одного предложения.) Каждое предложение содержит алгоритм шифрования, алгоритм аутентификации и группу ключей DH, которые P-793H предлагает использовать в IKE SA. Удаленный маршрутизатор IPSec выбирает приемлемое предложение и возвращает принятое предложение P-793H. Если удаленный маршрутизатор IPSec отвергает все предложения (например, при неверной настройке VPN-туннеля), установление IKE SA между P-793H и удаленным маршрутизатором будет невозможно.

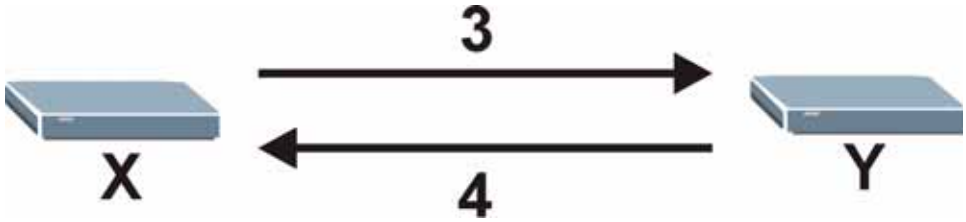
Оба маршрутизатора должны использовать один и тот же алгоритм шифрования, алгоритм аутентификации и группу ключей Диффи-Хелмана.

Конкретные алгоритмы шифрования, алгоритмы аутентификации и группы ключей рассмотрены в описаниях полей. Более подробно роль групп ключей DH описана в разд. 11.1.1.3 на стр. 165.

11.1.1.3 Обмен ключами Диффи-Хелмана (DH)

P-793H и удаленный маршрутизатор IPSec с помощью обмена ключами Диффи-Хелмана согласовывают общий секретный ключ, на основе которого формируются ключи шифрования для IKE SA и IPSec SA. В основном режиме обмен ключами DH осуществляется на этапах 3 и 4, как показано ниже.

Рис. 78 IKE SA: основной режим согласования, этапы 3 - 4: Обмен ключами DH



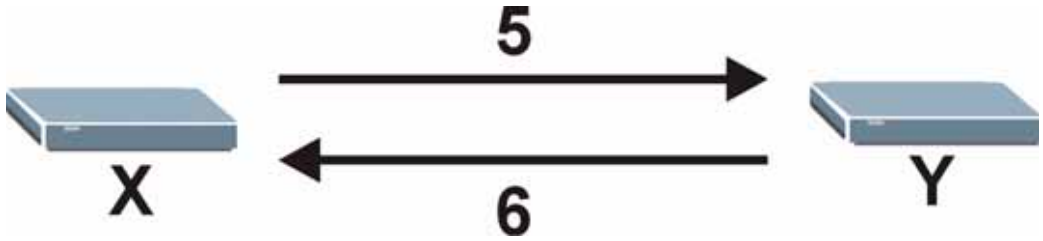
Обмен ключами DH построен на группах ключей DH. Группа представляет собой битовую последовательность фиксированной длины. Более длинные ключи отличаются большей защищенностью, но увеличивают затраты времени на шифрование и расшифровку информации. Например, ключи DH2 (1024 бита) надежнее защищены по сравнению с ключами DH1 (768 битов), но шифрование и расшифровка с использованием DH2 осуществляются медленнее.

11.1.1.4 Аутентификация

Прежде чем P-793H и удаленный маршрутизатор IPSec установят IKE SA, устройства должны проверить подлинность друг друга. Для этой процедуры используются предварительно согласованные ключи и идентификационные данные маршрутизаторов.

В основном режиме взаимная аутентификация P-793H и удаленного маршрутизатора IPSec осуществляется на этапах 5 и 6, как показано ниже. Эти идентификационные данные шифруются с использованием алгоритма и ключа шифрования, выбранных P-793H и удаленным маршрутизатором IPSec на предыдущих этапах.

Рис. 79 IKE SA: основной режим согласования, этапы 5 - 6: аутентификация



В процессе аутентификации P-793H и удаленный маршрутизатор IPSec используют предварительно согласованный ключ, но сам ключ не передается и не участвует в обмене.

P-793H и удаленный маршрутизатор IPSec должны использовать один и тот же предварительно согласованный ключ.

Идентификатор маршрутизатора состоит из полей типа и содержания. Типом идентификатора может быть произвольный IP-адрес, доменное имя или адрес электронной почты, а содержанием – конкретный IP-адрес, доменное имя или адрес электронной почты. Содержание идентификатора используется только в целях идентификации. Не обязательно указывать существующий IP-адрес, доменное имя или адрес электронной почты.

P-793H и удаленный маршрутизатор IPSec имеют собственные идентификаторы, поэтому каждое устройство должно хранить два набора данных: для самого себя и для второго маршрутизатора. Тип и содержание локального идентификатора в IKE SA относятся к самому маршрутизатору, а тип и содержание удаленного идентификатора – к маршрутизатору на противоположной стороне соединения.

Тип и содержание локального и удаленного идентификаторов P-793H должны совпадать, соответственно, с типом и содержанием удаленного и локального идентификаторов на удаленном коммутаторе IPSec.

В следующем примере P-793H и удаленный маршрутизатор IPSec успешно проводят взаимную аутентификацию.

Таблица 49 Пример VPN: совпадение типа и содержания идентификаторов

P-793H	УДАЛЕННЫЙ МАРШРУТИЗАТОР IPSEC
Тип локального идентификатора: E-mail	Тип локального идентификатора: IP
Содержание локального идентификатора: tomasz@yourcompany.com	Содержание локального идентификатора: 1.1.1.2
Тип удаленного идентификатора: IP	Тип удаленного идентификатора: E-mail
Содержание удаленного идентификатора: 1.1.1.2	Содержание удаленного идентификатора: tomasz@yourcompany.com

В следующем примере аутентификация не проходит, и установить IKE SA невозможно.

Таблица 50 Пример VPN: несовпадение типа и содержания идентификаторов

P-793H	УДАЛЕННЫЙ МАРШРУТИЗАТОР IPSEC
Тип локального идентификатора: E-mail	Тип локального идентификатора: IP
Содержание локального идентификатора: tom@yourcompany.com	Содержание локального идентификатора: **1.1.1.2**
Тип удаленного идентификатора: IP	Тип удаленного идентификатора: E-mail
Содержание удаленного идентификатора: **1.1.1.15**	Содержание удаленного идентификатора: tom@yourcompany.com

Можно настроить P-793H так, чтобы идентификационные данные удаленного маршрутизатора IPSec игнорировались. В этом случае обычно устанавливается тип удаленного маршрутизатора **Any**. Необходимо помнить, что этот способ не является столь же защищенным, как другие типы идентификации удаленной стороны.

11.1.2 Дополнительные сведения об IKE SA

В этой главе подробно рассматриваются ассоциации безопасности IKE SA.

11.1.2.1 Режим согласования

Существует два режима согласования: основной и агрессивный. Основной режим надежнее защищен, а агрессивный отличается большим быстродействием.

В основном режиме установление IKE SA осуществляется в шесть этапов.

Этапы 1-2: P-793H направляет предложения удаленному маршрутизатору IPSec. Удаленный маршрутизатор IPSec выбирает приемлемое предложение и возвращает его P-793H.

Этапы 3-4: Руководствуясь принятой группой ключей Диффи-Хелмана, P-793H и удаленный маршрутизатор осуществляют обмен ключами DH, согласовывая общий секретный ключ.

Этапы 5-6: В заключение P-793H и удаленный маршрутизатор IPSec формируют ключ шифрования на основе общего секретного ключа, шифруют свои идентификационные данные и обмениваются ими для аутентификации.

Отличие агрессивного режима состоит в том, что установление IKE SA осуществляется всего в три этапа.

Этап 1: P-793H направляет предложения удаленному маршрутизатору IPSec. Устройство также запускает обмен ключами Диффи-Хелмана и посылает свои идентификационные данные (в незашифрованном виде) удаленному маршрутизатору IPSec для аутентификации.

Этап 2: Удаленный маршрутизатор IPSec выбирает приемлемое предложение и возвращает его P-793H. На этом же этапе маршрутизатор завершает обмен ключами DH, проводит аутентификацию P-793H и возвращает свои идентификационные данные в незашифрованном виде P-793H для аутентификации.

Этап 3: P-793H проводит аутентификацию удаленного маршрутизатора IPSec и подтверждает установление IKE SA.

Агрессивный режим не обеспечивает того уровня безопасности, который достигается в основном режиме, поскольку идентификационные данные P-793H и удаленного маршрутизатора IPSec пересылаются в незашифрованном виде. Обычно этот режим используется в тех условиях, где инициатор неизвестен отвечающей стороне, и обе стороны реализуют аутентификацию посредством предварительно согласованных ключей (например, при подключении дистанционно работающих сотрудников).

11.1.2.2 VPN, NAT и прослеживание NAT

В следующем примере между маршрутизаторами **X** и **Y** имеется третий маршрутизатор (**A**).

Рис. 80 Пример VPN/NAT

Если маршрутизатор **A** реализует режим NAT, он может изменять IP-адреса источника или адресата, номера портов источника или адресата, либо одновременно IP-адреса и номера портов. Если маршрутизаторы **X** и **Y** попытаются установить VPN-туннель, аутентификацию выполнить не удастся, поскольку для нее необходимы первоначальные IP-адреса и номера портов.

Многие маршрутизаторы с поддержкой NAT (в данном примере – **A**) имеют функцию сквозного прохождения IPSec (pass-through), благодаря которой маршрутизатор **A** может распознавать пакеты VPN и пересылать их соответствующим образом. Если маршрутизатор **A** имеет поддержку этой функции, маршрутизаторы **X** и **Y** смогут установить туннель VPN при условии, что активен протокол ESP. (Более подробно об активных протоколах см. в разд. 11.1.3.2 на стр. 170.)

Если маршрутизатор A не имеет функции сквозного прохождения IPSec или активным протоколом является AH, эту проблему можно решить, включив прослеживание NAT (NAT Traversal). В режиме прослеживания NAT маршрутизаторы **X** и **Y** добавляют в пакеты IKE SA и IPSec SA специальный заголовок. Если маршрутизатору **A** можно указать пересылать такие пакеты без изменений, то маршрутизаторы **X** и **Y** смогут установить VPN-туннель.

Для настройки прослеживания NAT необходимо выполнить следующие операции.

- Включить прослеживание NAT на P-793H и удаленном маршрутизаторе IPSec.
- Маршрутизатор, на котором осуществляется NAT, настроить на пересылку пакетов со специальным заголовком без изменений. Специальный заголовок может отличаться тем, что в нем указан UDP-порт 500 или 4500, в зависимости от набора стандартов, поддерживаемых P-793H и удаленным маршрутизатором IPSec.

На P-793H и удаленном маршрутизаторе IPSec необходимо включить прослеживание NAT, настроив маршрутизатор NAT на пересылку пакетов, имеющих специальный заголовок, без изменений.

11.1.3 Обзор IPSec SA

IKE SA, согласованная P-793H и удаленным маршрутизатором IPSec, может использоваться для защищенного согласования IPSec SA, посредством которой данные будут пересылаться между компьютерами в сетях.

IPSec SA остается соединенной даже после того, как положенная в ее основу IKE SA становится недоступна.

В этом разделе рассматриваются ключевые компоненты IPSec SA.

11.1.3.1 Локальная сеть и удаленная сеть

В терминологии IPSec SA локальной сетью, или локальной политикой, называются одна или несколько сетей, подключенных к P-793H. Аналогично, удаленной сетью, или удаленной политикой, называются одна или несколько сетей, подключенных к удаленному маршрутизатору IPSec.

11.1.3.2 Активный протокол

Активный протокол определяет формат каждого пакета. Он указывает, какие части пакета должны защищаться протоколами шифрования и аутентификации. В IPSec VPN предусмотрено два активных протокола: AH (заголовок аутентификации, RFC 2402) и ESP (защищенное сокрытие содержания, RFC 2406).

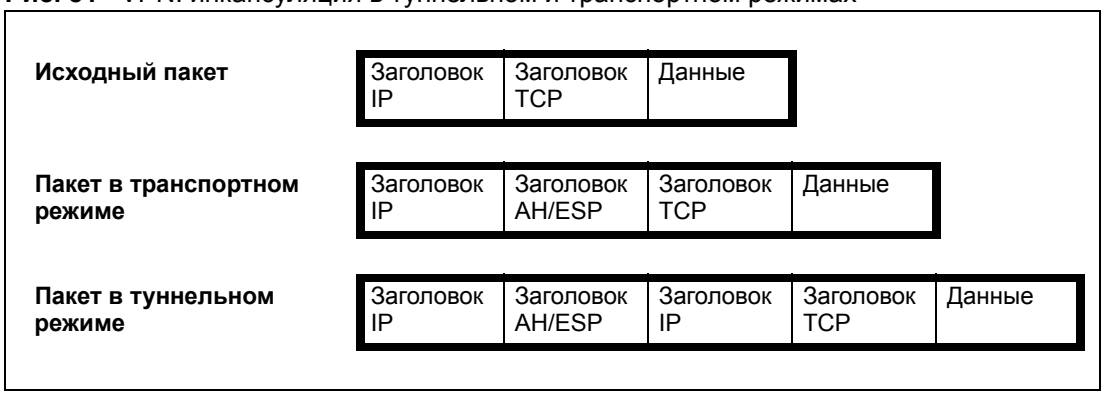
P-793H и удаленный маршрутизатор IPSec должны использовать один и тот же активный протокол. Рекомендуется применять ESP.

Протокол ESP предпочтителен, поскольку AH не поддерживает шифрования, а также поскольку ESP более совместим с NAT. Протокол AH целесообразно применять только в том случае, если удаленный маршрутизатор IPSec не поддерживает ESP.

11.1.3.3 Инкапсуляция

Инкапсуляция пакетов может осуществляться двумя способами. Эти способы проиллюстрированы ниже.

Рис. 81 VPN: инкапсуляция в туннельном и транспортном режимах



В туннельном режиме P-793H инкапсулирует пакет IP полностью, в результате чего пакет содержит два заголовка IP, а также заголовок активного протокола.

- Внешний заголовок: внешний заголовок IP содержит IP-адреса P-793H и удаленного шлюза VPN.
- Заголовок AH/ESP: заголовок активного протокола инкапсулирует исходный пакет.
- Внутренний заголовок: внутренний заголовок IP содержит IP-адреса компьютеров, расположенных за P-793H, и удаленного маршрутизатора VPN.

В транспортном режиме заголовок IP представляет собой первоначальный заголовок IP, а тип инкапсуляции зависит от активного протокола. Если активен протокол AH, P-793H при инкапсуляции пакета включает часть заголовка IP. Если активен протокол ESP, P-793H не включает исходный заголовок IP при инкапсуляции пакета, и в этом случае гарантировать подлинность IP-адреса источника нельзя.

P-793H и удаленный маршрутизатор IPSec должны использовать один и тот же тип инкапсуляции.

Обычно следует использовать туннельный режим в силу его большей защищенности. Транспортный режим следует использовать только в том случае, когда для обмена данными между P-793H и удаленным маршрутизатором IPSec используются IPSec SA (например, при дистанционном управлении), но не для обмена данными между компьютерами в локальной и удаленной сетях.

11.1.3.4 Предложение IPSec SA и защита от разглашения ключей

Предложение IPSec SA аналогично предложению IKE SA (см. разд. 11.1.1.2 на стр. 165), за исключением того, что P-793H выполняет обмен ключами DH заново всякий раз, когда устанавливается IPSec SA. Эта особенность представляет собой защиту от разглашения использованных ключей (Perfect Forward Secrecy – PFS)

Если включен режим PFS, P-793H и удаленный маршрутизатор IPSec будут выполнять обмен ключами DH при каждом создании IPSec SA, меняя общий секретный ключ, на основе которого формируются ключи шифрования. В результате утечка одного из ключей шифрования не создаст угрозы для других ключей, поскольку они созданы из разных общих секретных ключей.

Если режим PFS не используется, P-793H и удаленный маршрутизатор IPSec будут генерировать ключи шифрования из одного и того же общего секретного ключа, созданного при установлении IKE SA. При очередном установлении или переустановлении IKE SA P-793H и удаленный маршрутизатор по-прежнему могут сменить общий секретный ключ.

Обмен ключами Диффи-Хелмана занимает значительное время, поэтому если установление IPSec SA создает ощутимую задержку, а VPN-туннель сам по себе надежно защищен (например, путем использования криптостойких алгоритмов шифрования), PFS можно отключить.

11.1.4 Дополнительные сведения об IPSec SA

В этой главе подробно рассматриваются ассоциации безопасности IPSec SA.

11.1.4.1 Ручное задание ключей для IPSec SA

Можно сформировать IPSec SA, задав ключи вручную, если требуется быстрое установление VPN-туннеля (например, при диагностике ошибок). IPSec SA, созданная таким способом, защищена слабее, и прибегать к нему рекомендуется только в качестве временного решения.

При формировании IPSec SA с ручным заданием ключей P-793H и удаленный маршрутизатор IPSec не устанавливают IKE SA, создавая непосредственно IPSec SA. В результате процедура установления IPSec SA по вручную заданным ключам сочетает в себе некоторые свойства IKE SA и свойства IPSec SA. Ассоциации IPSec SA с заданными вручную ключами отличаются в ряде аспектов от других типов SA.

11.1.4.1.1 Предложение IPSec SA при ручном способе задания ключей

При ручном задании ключей для IPSec SA можно указать только один алгоритм шифрования и один алгоритм аутентификации. Создать несколько предложений невозможно. Поскольку обмен ключами DH не производится, необходимо предоставить ключ шифрования и аутентификации для P-793H и удаленного маршрутизатора IPSec.

P-793H и удаленный маршрутизатор IPSec должны использовать одни и те же ключи шифрования и аутентификации.

11.1.4.1.2 Аутентификация и индекс параметров безопасности (SPI)

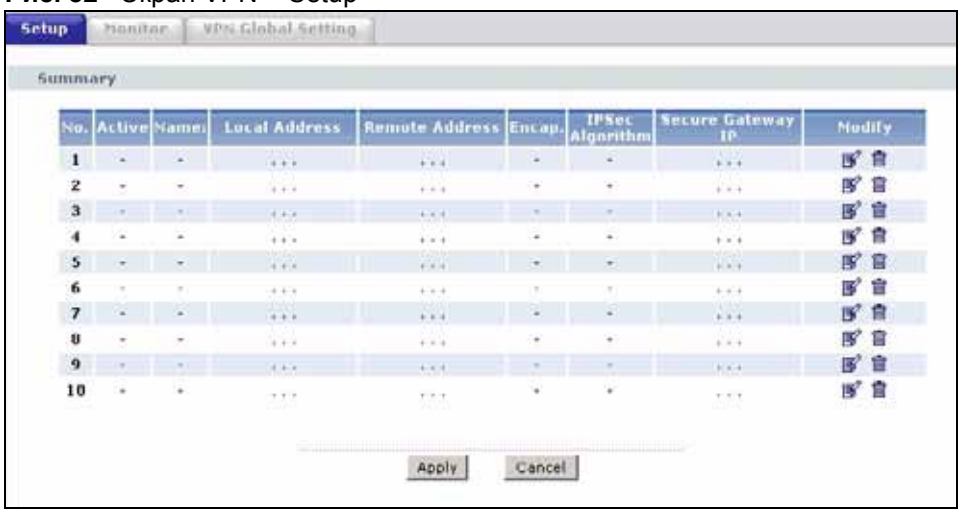
При установлении IPSec SA с ручным заданием ключей P-793H и удаленный маршрутизатор IPSec используют SPI для аутентификации вместо предварительно согласованных ключей, типов и содержания идентификаторов. SPI представляет собой произвольное число, идентифицирующее IPSec SA.

SPI, используемые P-793H и удаленным маршрутизатором IPSec, должны совпадать.

11.2 Экран VPN Setup

Чтобы перейти на экран **VPN Setup**, выберите **Security** и **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. 82 Экран VPN > Setup



Поля изображенного выше экрана описаны в следующей таблице.

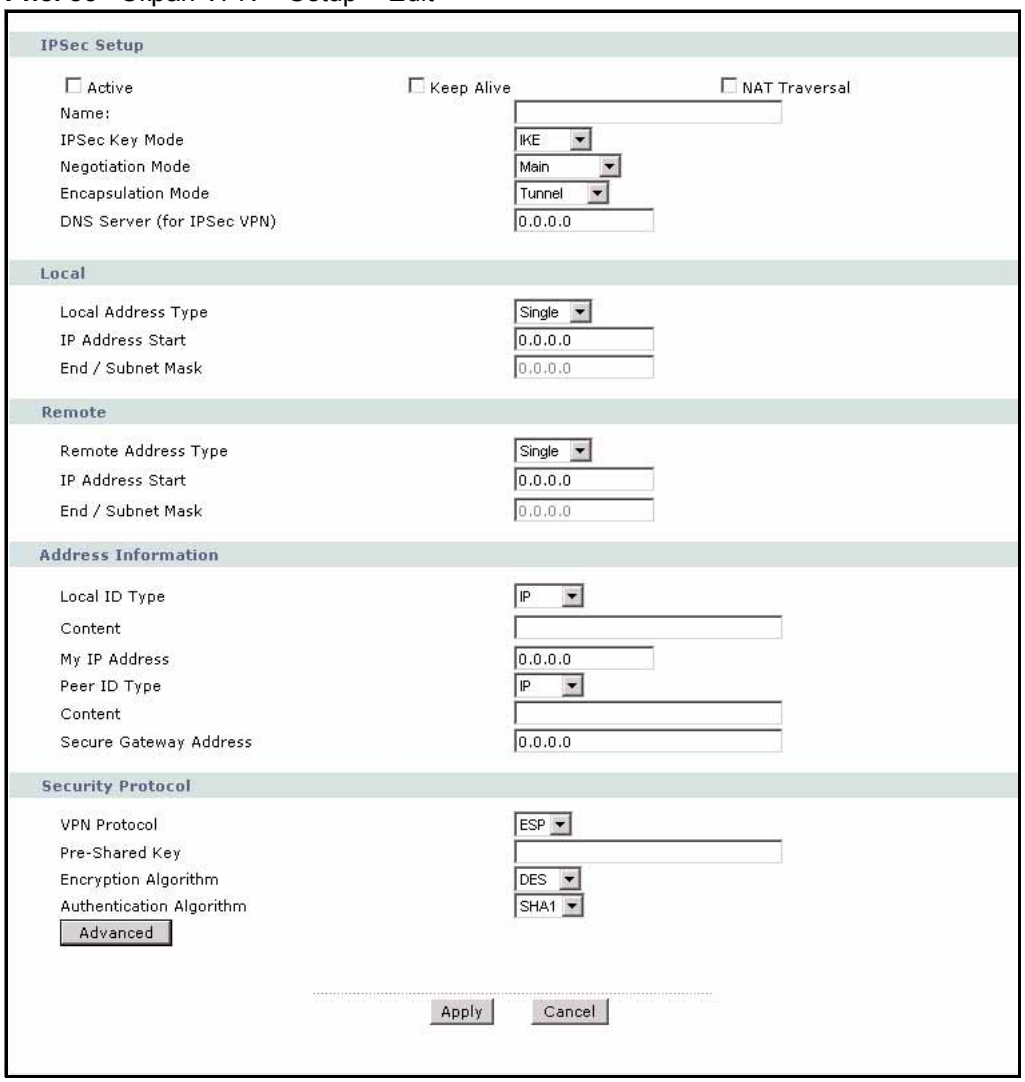
Таблица 51 Экран VPN > Setup

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-793H. 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** (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-793H 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 кнопку **Apply**, чтобы сохранить изменения в P-793H.
Cancel	Чтобы вернуться к прежним настройкам, нажмите **Cancel**.

11.3 Редактирование политик VPN

Дополнительные сведения см. в разд. 11.1 на стр. 163. Этот экран предназначен для редактирования политик VPN. На экране Экран VPN Setup щелкните значок **Edit**.

Рис. 83 Экран VPN > Setup > Edit



Поля изображеенного выше экрана описаны в следующей таблице.

Таблица 52 Экран VPN > Setup > Edit

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-793H автоматически запустило SA повторно после истечения срока действия, даже если трафика нет. Чтобы использовать эту возможность, на удаленном IPSec-маршрутизаторе должна быть включена функция поддержки активности.

Таблица 52 Экран VPN > Setup > Edit (продолжение)

ПОЛЕ	ОПИСАНИЕ
NAT Traversal	Прослеживание NAT позволяет настроить соединение VPN, когда между P-793H 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-793H.
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 защищенный 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-793H будет назначать этот дополнительный DNS-сервер DHCP-клиентам P-793H, 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 удаленным IP-адресам удаленного IPSec-маршрутизатора. Две активных SA могут иметь одинаковый локальный или удаленный IP-адрес, но не оба сразу. Можно настроить несколько SA между одинаковыми локальными и удаленными 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-793H. Если в поле **Local Address Type** выбрано **Range**, введите начальный (статический) IP-адрес диапазона адресов компьютеров в вашей сети LAN за устройством P-793H. Если в поле **Local Address Type** выбрано **Subnet**, введите (статический) IP-адрес в вашей сети LAN за устройством P-793H.
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-793H. Если в поле **Local Address Type** выбрано **Subnet**, введите маску подсети, которая соответствует вашей сети LAN за устройством P-793H.

Таблица 52 Экран VPN > Setup > Edit (продолжение)

ПОЛЕ	ОПИСАНИЕ
Remote	Удаленные IP-адреса должны быть статическими и соответствовать настроенным локальным IP-адресам удаленного 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 удаленных IP-адресов. Две активных SA могут иметь одинаковый локальный или удаленный IP-адрес, но не оба сразу. Можно настроить несколько SA между одинаковыми локальными и удаленными 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-адрес 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-793H по его IP-адресу. Выберите **DNS** для идентификации P-793H по доменному имени. Выберите **E-mail** для идентификации P-793H по адресу электронной почты.
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-793H 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-793H. 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.

Таблица 52 Экран VPN > Setup > Edit (продолжение)

ПОЛЕ	ОПИСАНИЕ
My IP Address	Введите IP-адрес вашего устройства P-793H 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-793H использует текущий IP-адрес (статический или динамический), присвоенный P-793H в сети WAN (static or dynamic). При обрыве соединения с WAN P-793H 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. главу, посвященную параметрам WAN.
Peer ID Type	Выберите **IP** для идентификации удаленного 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 удаленного 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-793H 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-793H различало VPN-соединения от разных IPSec-маршрутизаторов с динамическими IP-адресами в сети WAN.
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 удаленный 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).

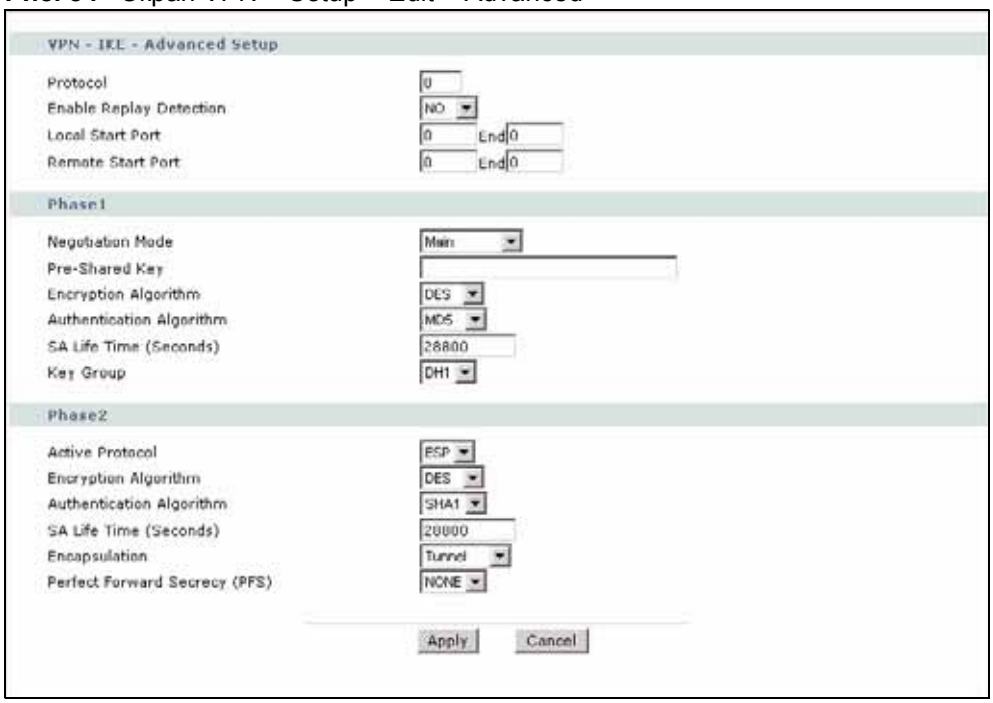
Таблица 52 Экран VPN > Setup > Edit (продолжение)

ПОЛЕ	ОПИСАНИЕ
Pre-Shared Key (Предварительно согласованный ключ)	Введите ваш предварительно согласованный ключ в этом поле. Предварительно согласованный ключ 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 предварительно согласованный ключ. 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.
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 надежным, 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**.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-793H.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

11.4 Настройка расширенных параметров IKE

Дополнительные сведения см. в разд. 11.1 на стр. 163. Этот экран служит для настройки расширенных параметров туннеля VPN. Чтобы перейти на этот экран, на экране Редактирование политик VPN выберите **Advanced**.

Рис. 84 Экран VPN > Setup > Edit > Advanced



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 53 Экран VPN > Setup > Edit > Advanced

ПОЛЕ	ОПИСАНИЕ
VPN - IKE - Advanced Setup	
Protocol	Введите номер протокола IP, для которого разрешено использовать VPN-туннель. 0 разрешает пропускать через VPN-туннель трафик всех протоколов IP. Список ряда распространенных протоколов IP см. в Приложение G на стр. 429.
Enable Replay Detection	Выберите YES, чтобы включить защиту от атак воспроизведения. Поскольку обслуживание VPN-соединений является ресурсоемким, система уязвима к DoS-атакам. Получатель IPSec может выявлять и запрещать поступление старых или повторяющихся пакетов для защиты от атак воспроизведения.
Local Start Port End	Введите номер порта или диапазон номеров портов в локальной сети, трафик которых разрешено пересылать через VPN-туннель. Чтобы разрешить пересылать через VPN-туннель трафик для всех портов локальной сети, введите 0 в обоих полях. Приложение G на стр. 429 содержит перечень распространенных номеров портов.
Remote Start Port End	Введите номер порта или диапазон номеров портов в удаленной сети, трафик которых разрешено пересылать через VPN-туннель. Чтобы разрешить пересылать через VPN-туннель трафик для всех портов удаленной сети, введите 0 в обоих полях. Приложение G на стр. 429 содержит перечень распространенных номеров портов.
Phase 1	
Negotiation Mode	Выберите режим согласования IKE SA. Основной режим (**Main**) защищен надежнее, чем агрессивный режим (**Aggressive**). P-793H и удаленный маршрутизатор IPSec должны использовать один и тот же протокол согласования.

Таблица 53 Экран VPN > Setup > Edit > Advanced (продолжение)

ПОЛЕ	ОПИСАНИЕ
Pre-Shared Key	Введите предварительно согласованный ключ для IKE SA. P-793H и удаленный маршрутизатор IPSec должны использовать один и тот же предварительно согласованный ключ. При несовпадении ключей P-793H получит пакет "PYLD_MALFORMED" (повреждение полезной нагрузки). Введите 8 – 31 символа ASCII (регистр, в котором набраны символы, учитывается) или 16 – 62 шестнадцатеричных символа ("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.
Encryption Algorithm	Выберите один из следующих алгоритмов шифрования для IKE SA. Алгоритмы перечислены в порядке возрастания криптостойкости. Стандарт шифрования данных (**DES**) – широко используемый, но слабо защищенный метод шифрования данных с помощью секретного ключа. В стандарте DES к каждому 64-битному блоку данных применяется 56-битный ключ. Тройной DES (**3DES**) представляет собой разновидность DES, в которой используются три прохода с тремя отдельными ключами. Криптостойкость DES при этом фактически утраивается. Усовершенствованный стандарт шифрования (**AES**) - более новый алгоритм, также использующий секретный ключ. В AES к каждому 128-битному блоку данных применяется 128-битный ключ. Чтобы настроить VPN-туннель без шифрования, выберите значение **NULL**.
Authentication Algorithm	Выберите один из следующих алгоритмов аутентификации для IKE SA. Алгоритмы перечислены в порядке возрастания криптостойкости. В алгоритме **MD5** (Message Digest 5) для аутентификации пакетов используется 128-битная свертка. В алгоритме SHA1 (**Secure Hash Algorithm**) для аутентификации пакетов используется 160-битная свертка.
SA Life Time (Seconds)	Укажите в этом поле период времени, по истечении которого P-793H будет автоматически повторять согласование IKE SA. Допустимый диапазон – от 60 до 3 000 000 секунд (почти 35 дней). Малые значения позволяют укрепить безопасность, вынуждая оба межсетевых шлюза VPN регулярно обновлять ключи шифрования и аутентификации. Однако при каждом согласовании IKE SA пользователи, пытающиеся установить IPSec SA, могут ощутить задержку (на существующие IPSec SA эта процедура не влияет).
Key Group	Для IKE SA необходимо выбрать группу ключей DH. Чем длиннее группа ключей, тем сильнее шифрование, но тем выше вычислительная нагрузка. **DH1** – группа Диффи-Хелмана 1, случайное число 768 битов. **DH2** – группа Диффи-Хелмана 2, случайное число 1024 бита (1 Кбит).
Phase 2	
Active Protocol	Выберите активный протокол, используемый для IPSec SA. Рекомендуется выбирать протокол ESP, за исключением тех случаев, когда удаленный маршрутизатор использует только протокол AH.

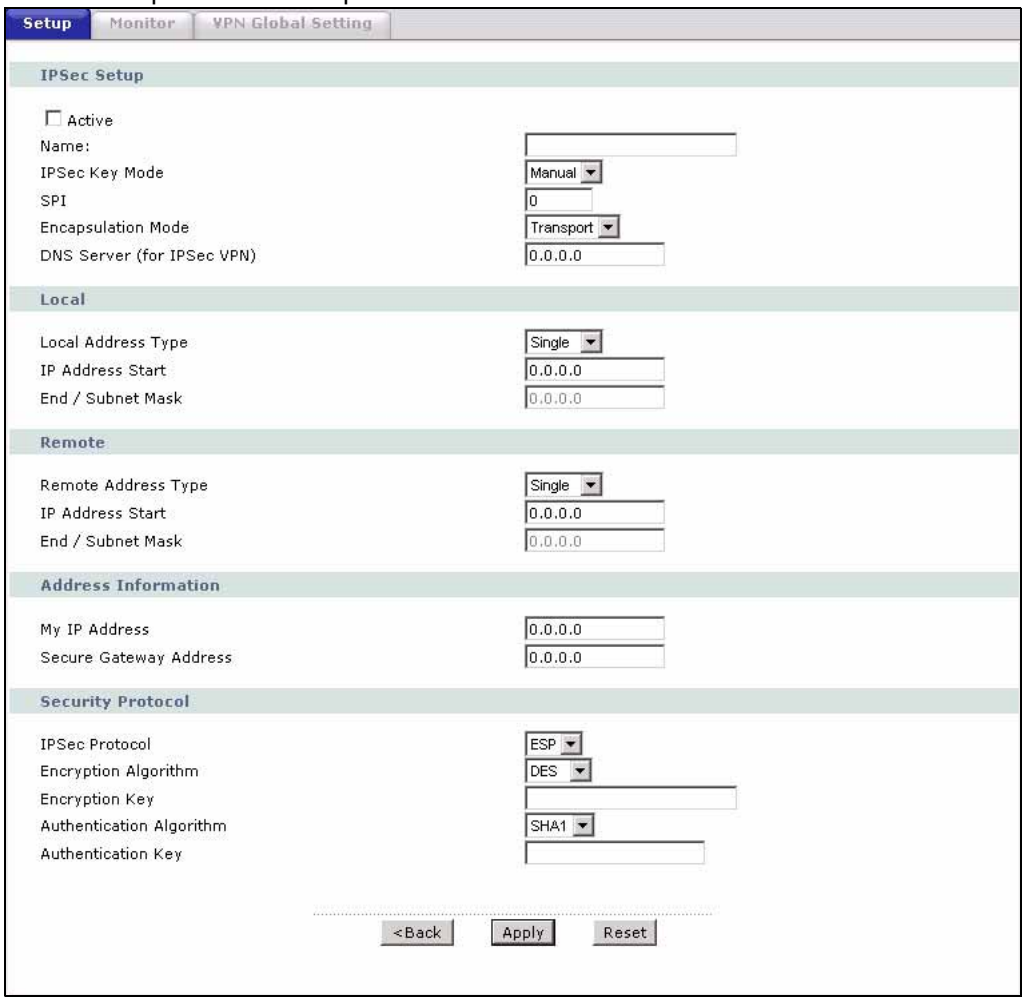
Таблица 53 Экран VPN > Setup > Edit > Advanced (продолжение)

ПОЛЕ	ОПИСАНИЕ
Encryption Algorithm	Выберите один из следующих алгоритмов шифрования для IPSec SA. Алгоритмы перечислены в порядке возрастания криптостойкости. Стандарт шифрования данных (**DES**) – широко используемый, но слабо защищенный метод шифрования данных с помощью секретного ключа. В стандарте DES к каждому 64-битному блоку данных применяется 56-битный ключ. Тройной DES (**3DES**) представляет собой разновидность DES, в которой используются три прохода с тремя отдельными ключами. Криптостойкость DES при этом фактически утраивается. Усовершенствованный стандарт шифрования (**AES**) – более новый алгоритм, также использующий секретный ключ. В AES к каждому 128-битному блоку данных применяется 128-битный ключ. Чтобы настроить VPN-туннель без шифрования, выберите значение **NULL**.
Authentication Algorithm	Выберите один из следующих алгоритмов аутентификации для IPSec SA. Алгоритмы перечислены в порядке возрастания криптостойкости. В алгоритме **MD5** (Message Digest 5) для аутентификации пакетов используется 128-битная свертка. В алгоритме SHA1 (**Secure Hash Algorithm**) для аутентификации пакетов используется 160-битная свертка.
SA Life Time (Seconds)	Укажите в этом поле период времени, по истечении которого P-793H будет автоматически повторять согласование IPSec SA. Допустимый диапазон – от 60 до 3 000 000 секунд (почти 35 дней). Малые значения позволяют укрепить безопасность, вынуждая оба межсетевых шлюза VPN регулярно обновлять ключи шифрования и аутентификации. Однако каждый раз при повторном согласовании IPSec SA все пользователи, получающие доступ к удаленным ресурсам, временно отключаются.
Encapsulation	Выберите тип инкапсуляции. Выберите **Tunnel**. Значение **Transport** следует выбирать только в том случае, если удаленный маршрутизатор не поддерживает других типов инкапсуляции, кроме туннеля. P-793H и удаленный маршрутизатор IPSec должны использовать один и тот же тип инкапсуляции.
Perfect Forward Secrecy (PFS)	Укажите, следует ли включить защиту от разглашения использованных ключей (PFS) и, если да, то какую группу ключей следует использовать для обмена ключами DH. Чем длиннее группа ключей, тем сильнее шифрование, но тем выше вычислительная нагрузка. **NONE** отключает PFS. Это ускоряет процесс настройки ценой меньшей защищенности. **DH1** активирует PFS с использованием группы Диффи-Хелмана 1, случайного числа длиной 768 битов. **DH2** активирует PFS с использованием группы Диффи-Хелмана 2, случайного числа длиной 1024 бита.
Apply	Выберите **Apply,** чтобы сохранить изменения в P-793H и возвратиться на экран **VPN-IKE**.
Cancel	Нажмите кнопку **Cancel** для возвращения к предыдущему экрану без сохранения изменений.

11.5 Ввод ключа вручную

Настройка на экране **VPN Manual Key** выполняется только в том случае, если на экране **VPN IKE** в поле **IPSec Key Mode** выбрано значение **Manual**. Экран **VPN Manual Key** показан ниже.

Рис. 85 Экран VPN > Setup > Edit > Manual



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 54 Экран VPN > Setup > Edit > Manual

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-793H.
IPSec Key Mode	В раскрывающемся списке выберите **IKE** или **Manual**. Режим **Manual** 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.
Encapsulation Mode	В раскрывающемся списке выберите режим: **Tunnel** или **Transport**.

Таблица 54 Экран VPN > Setup > Edit > Manual (продолжение)

ПОЛЕ	ОПИСАНИЕ
DNS Server (for IPSec VPN)	Если для данной VPN-сети существует частный DNS-сервер, введите его IP-адрес в этом поле. P-793H будет назначать этот дополнительный DNS-сервер DHCP-клиентам P-793H, 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 удаленным IP-адресам удаленного IPSec-маршрутизатора. У двух активных SA не может быть одинаковых локальных и удаленных IP-адресов. Две активных SA могут иметь одинаковый локальный или удаленный IP-адрес, но не оба сразу. Можно настроить несколько SA между одинаковыми локальными и удаленными 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-793H. Если в поле **Local Address Type** выбрано **Range**, введите начальный (статический) IP-адрес диапазона адресов компьютеров в вашей сети LAN за устройством P-793H. Если в поле **Local Address Type** выбрано **Subnet**, введите (статический) IP-адрес в вашей сети LAN за устройством P-793H.
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-793H. Если в поле **Local Address Type** выбрано **Subnet**, введите маску подсети, которая соответствует вашей сети LAN за устройством P-793H.
Remote	Удаленные IP-адреса должны быть статическими и соответствовать настроенным локальным IP-адресам удаленного маршрутизатора IPSec. У двух активных SA не может быть одинаковых локальных и удаленных IP-адресов. Две активных SA могут иметь одинаковый локальный или удаленный IP-адрес, но не оба сразу. Можно настроить несколько SA между одинаковыми локальными и удаленными 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-адрес 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.

Таблица 54 Экран VPN > Setup > Edit > Manual (продолжение)

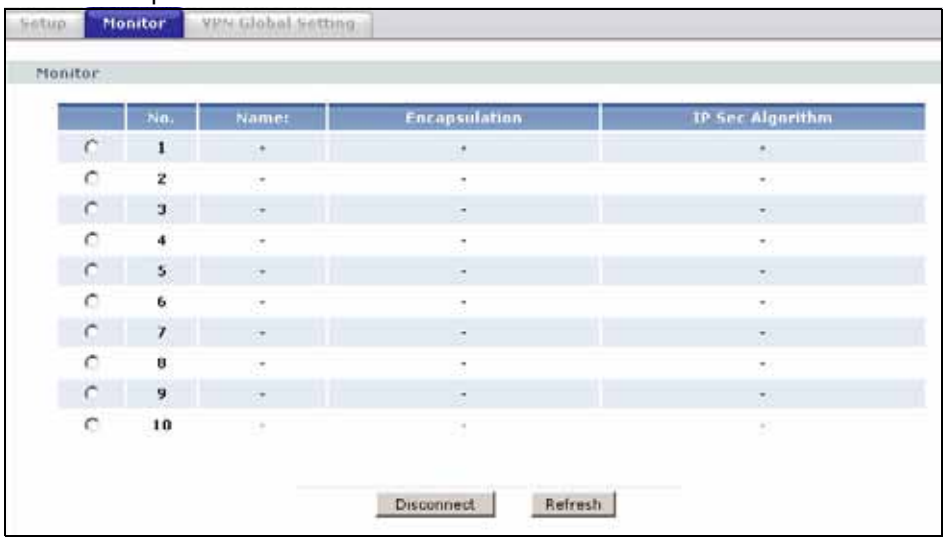
ПОЛЕ	ОПИСАНИЕ
Address Information	
My IP Address	Введите IP-адрес вашего устройства P-793H в сети WAN. Туннель VPN необходимо построить заново в случае изменения этого IP-адреса. Если в этом поле введен адрес **0.0.0.0**, действует следующий алгоритм: для настройки VPN-туннеля P-793H использует текущий IP-адрес (статический или динамический), присвоенный P-793H в сети WAN (static or dynamic). При обрыве соединения с WAN P-793H 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. главу, посвященную параметрам WAN.
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.
Encryption Key	В алгоритме шифрования **DES** используется 8-битный ключ. В алгоритме шифрования **3DES** используется 24-битный ключ. Можно использовать 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 надежным, 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. Введите последовательность длиной 16 символов для аутентификации **MD5** или 20 символов для аутентификации **SHA1**. Можно использовать любые символы, включая пробелы, но конечные пробелы отсекаются.
Back	Чтобы вернуться к предыдущему экрану, нажмите кнопку **Back**.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-793H.
Reset	Нажмите кнопку **Reset**, чтобы заново начать настройку на данном экране.

11.6 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.

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. Можно указать P-793H всегда выполнять повторное согласование IPSec SA при истечении срока действия SA, даже если трафик в данный момент отсутствует.

Рис. 86 Экран VPN > Monitor



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 55 Экран VPN > Monitor

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.

11.7 Настройка глобальных параметров

Этот экран служит для изменения глобальных настроек P-793H. Выберите **VPN** и потом **VPN Global Setting**. Появится изображенный ниже экран.

Рис. 87 Экран VPN > VPN Global Setting

Поля изображенного выше экрана описаны в следующей таблице.

Таблица 56 Экран VPN > VPN 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-793H.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

11.8 Примеры настройки VPN/IPSec для дистанционных сотрудников

В следующих примерах рассматривается установление нескольких VPN-соединений между дистанционными сотрудниками и одним устройством P-793H в штаб-квартире. Дистанционные сотрудники используют IPSec-маршрутизаторы с динамическими IP-адресами в сети WAN. Устройству P-793H в штаб-квартире присвоен статический глобальный IP-адрес.

11.8.1 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-793H в штаб-квартире (на рисунке – "HQ"). IP-адресам IPSec-маршрутизаторов дистанционных сотрудников в сети WAN не присвоены доменные имена. Все дистанционные сотрудники должны иметь одинаковые параметры IPSec, но локальные IP-адреса (или диапазоны адресов) не должны перекрываться.

Рис. 88 Пример совместного использованием одного правила VPN несколькими дистанционными сотрудниками

Таблица 57 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)

11.8.2 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. 11.1.2.1 на стр. 167) P-793H может различать правила VPN по типам и содержанию идентификаторов. Дистанционные сотрудники могут использовать отдельные правила VPN для одновременного доступа к P-793H в штаб-квартире. Они могут использовать различные параметры IPSec. Локальные IP-адреса (или диапазоны адресов) в правилах, настроенных на P-793H 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-793H, расположенным в штаб-квартире. P-793H 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-793H в штаб-квартире может также инициировать VPN-соединения с дистанционными сотрудниками, находя их по доменным именам.

Рис. 89 Пример использования уникальных правил VPN различными дистанционными сотрудниками

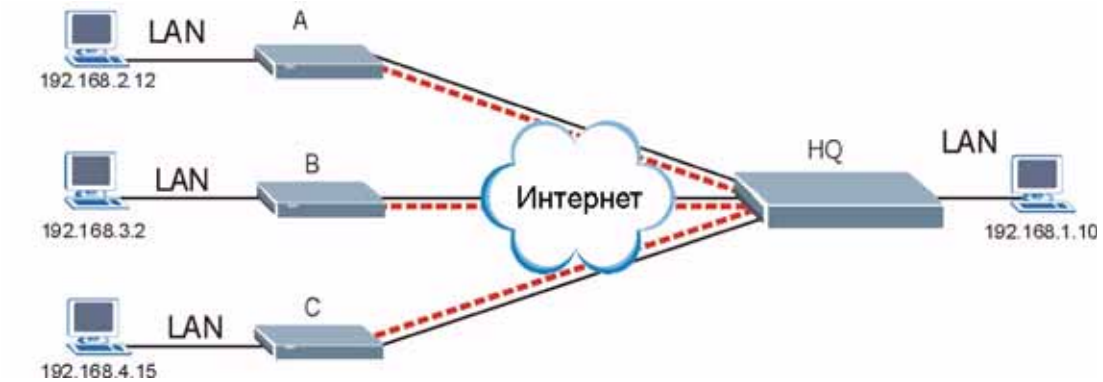


Таблица 58 Пример использования уникальных правил VPN различными дистанционными сотрудниками

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-793H в штаб-квартире:
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-793H 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

Таблица 58 Пример использования уникальных правил VPN различными дистанционными сотрудниками (продолжение)

ДИСТАНЦИОННЫЕ СОТРУДНИКИ	ШТАБ-КВАРТИРА
Сотрудник C (telecommuterc.dydns.org)	Правило 3 для P-793H 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

11.9 VPN и удаленное управление

Если VPN-туннель использует Telnet, FTP или WWW, то для доступа к соответствующей службе необходимо настроить удаленное управление (**Remote Management**).

12

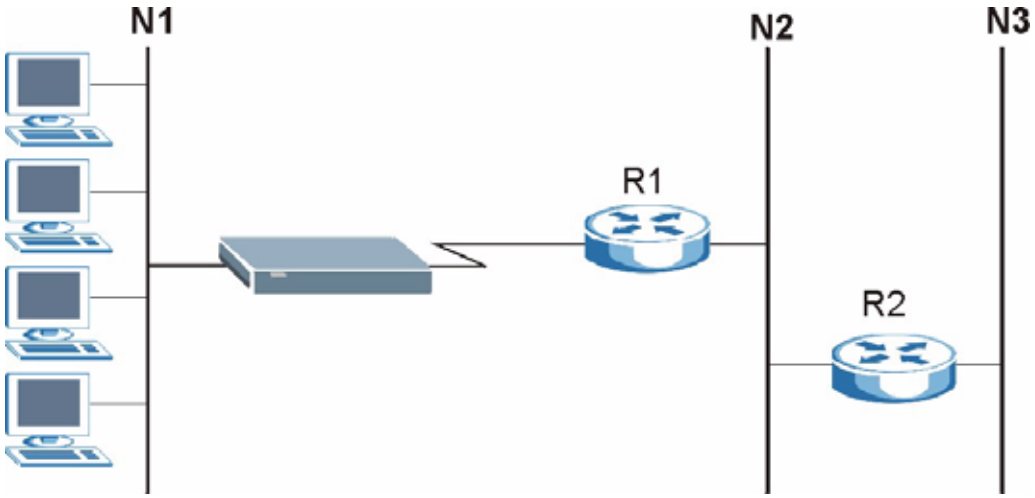
Статическая маршрутизация

В этой главе описывается настройка статических маршрутов для P-793H.

12.1 Статическая маршрутизация

Каждый удаленный узел определяет только ту сеть, к которой непосредственно подключен маршрутизатор, и P-793H не имеет информации о сетях, расположенных за ее пределами. Например, на следующем рисунке P-793H получает сведения о сети N2 через удаленный маршрутизатор R1. Однако P-793H не имеет возможности отправить пакет в сеть N3, поскольку ему неизвестно о существовании маршрута через удаленный маршрутизатор R1 (и далее через R2). Статические маршруты позволяют сообщать P-793H о сетях, находящихся за пределами удаленных узлов.

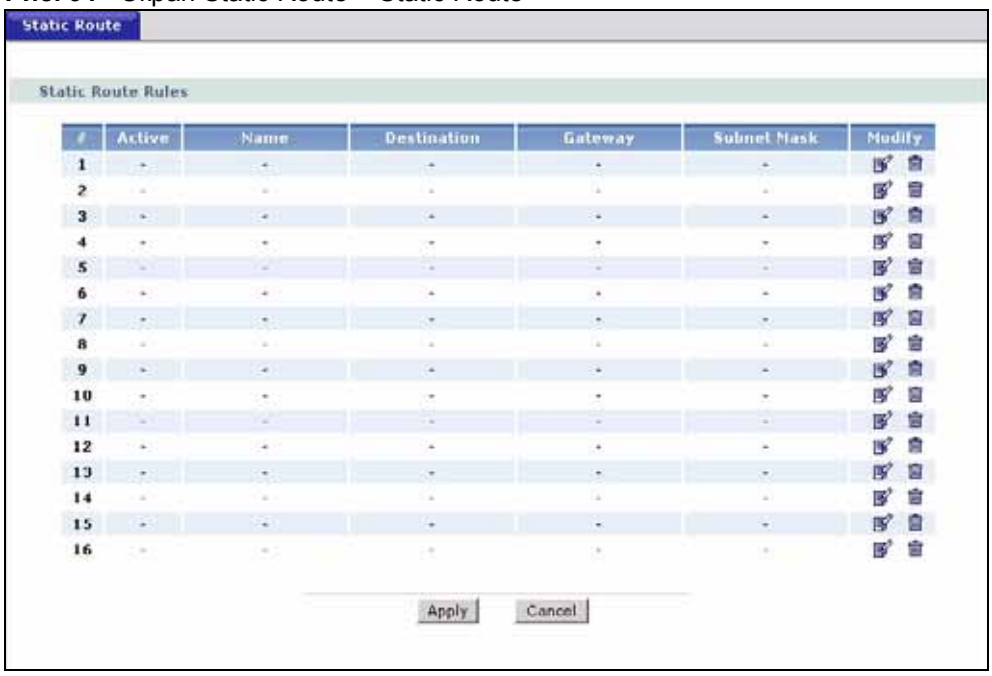
Рис. 90 Пример топологии статической маршрутизации



12.2 Настройка статических маршрутов

Этот экран служит для просмотра статических маршрутов в P-793H. Чтобы перейти на экран **Static Route**, выберите **Advanced > Static Route**.

Рис. 91 Экран Static Route > Static Route



Поля изображенного выше экрана описаны в следующей таблице.

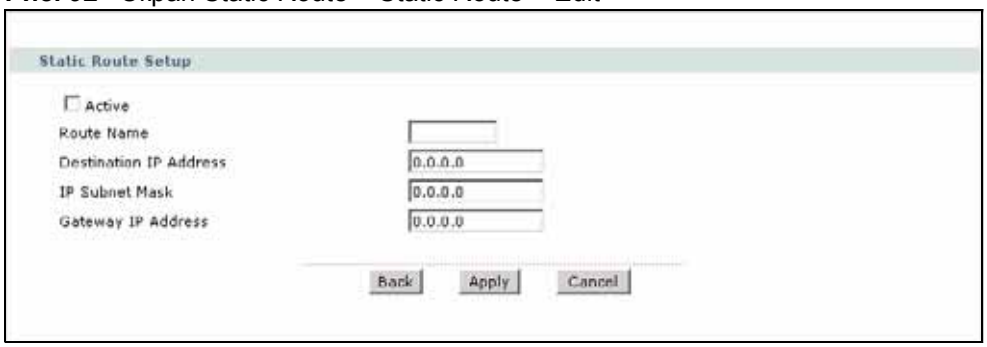
Таблица 59 Экран Static Route > Static Route

ПОЛЕ	ОПИСАНИЕ
#	В этом поле отображается номер статического маршрута.
Active	Это поле показывает, активен ли данный статический маршрут: **Yes (Да)** или **No (Нет)**.
Name	В этом поле выводится описание или идентификация данного машрута.
Destination	Этот параметр указывает IP-адрес конечной точки маршрута. Маршрутизация всегда подразумевает диапазон сетевых адресов.
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.
Subnet Mask	В этом поле отображается маска подсети статического маршрута.
Modify	Чтобы перейти на экран задания статических маршрутов для P-793H, щелкните на значке редактирования. Щелкните на значке удаления, чтобы удалить статический маршрут из P-793H. Появится окно с просьбой подтвердить удаление маршрута.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-793H.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

12.2.1 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. 92 Экран Static Route > Static Route > Edit



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 60 Экран Static Route > Static Route > Edit

ПОЛЕ	ОПИСАНИЕ
Active	Это поле позволяет активировать/деактивировать данный статический маршрут.
Route Name	Введите имя статического IP-маршрута. Для удаления данного статического маршрута оставьте это поле пустым.
Destination IP Address	Этот параметр указывает IP-адрес конечной точки маршрута. Маршрутизация всегда подразумевает диапазон сетевых адресов. Если требуется указать маршрут до отдельного хоста, в поле "IP Subnet Mask" введите маску подсети 255.255.255.255 – при этом диапазон сетевых адресов будет ограничен до адреса хоста.
IP Subnet Mask	Введите маску подсети IP.
Gateway IP Address	Введите IP-адрес интернет-центра. Шлюз – это маршрутизатор или коммутатор, расположенный в одном сегменте с LAN- или WAN-портом устройства. Шлюз пересылает пакеты к месту назначения.
Back	Для возврата к предыдущему экрану без сохранения настроек нажмите кнопку **Back**.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-793H.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

13

Управление полосой пропускания

В этой главе описывается настройка управления полосой пропускания, редактирование правил и просмотр журналов управления полосой пропускания в P-793H.

13.1 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-793H применяет правила управления полосой пропускания к трафику, проходящему через интерфейс. P-793H 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-793H, в результате чего на трафик также будут распространяться правила управления полосой пропускания.

Сумма выделяемых долей полосы пропускания для любого интерфейса должна быть меньше или равна скорости интерфейса, настроенной на экране Bandwidth Management Summary.

13.2 Управление полосой пропускания с учетом приложений

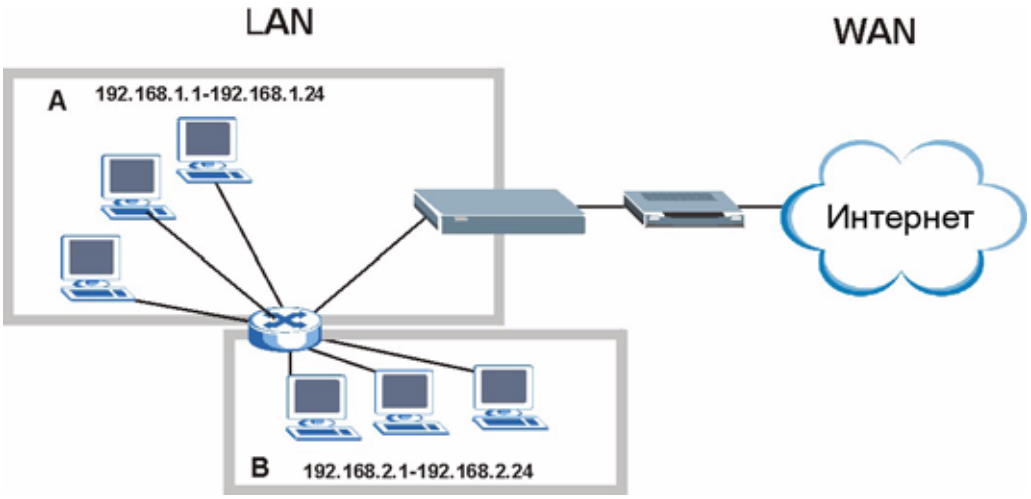
Можно настроить классы полосы пропускания для различных приложений (например, VoIP, WWW, FTP, электронная почта и потоковое видео).

13.3 Управление полосой пропускания с учетом подсетей

Можно определить классы полосы пропускания в зависимости от подсетей.

Пример подсетей LAN приведен на следующем рисунке. Для подсети **A** можно настроить один класс полосы пропускания, а для подсети **B** – другой.

Рис. 93 Управление полосой пропускания с учетом подсетей



13.4 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 определенных приложений от отдельных подсетей LAN.

Таблица 61 Пример управления полосой пропускания с учетом приложений и подсетей

ТИП ТРАФИКА	ОТ ПОДСЕТИ A	ОТ ПОДСЕТИ B
VoIP	64 кбит/с	64 кбит/с
Веб	64 кбит/с	64 кбит/с
FTP	64 кбит/с	64 кбит/с
E-mail	64 кбит/с	64 кбит/с
Видеофайлы	64 кбит/с	64 кбит/с

13.5 Планировщик

Планировщик распределяет полосу пропускания интерфейса по классам полосы пропускания. В P-793H реализованы планировщики двух типов: на основе равнодоступности и на основе приоритета.

13.5.1 Планировщик на основе приоритета

С планировщиком на основе приоритета P-793H 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).

13.5.2 Планировщик на основе равнодоступности

С планировщиком на основе равнодоступности P-793H одинаково делит полосу пропускания среди классов полосы пропускания и не позволяет одному классу полосы пропускания использовать всю полосу пропускания интерфейса.

13.6 Максимизация использования полосы пропускания

Параметр максимизации использования полосы пропускания (см. рис. 94 на стр. 200) позволяет P-793H 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-793H сначала проверяется, получает ли каждый класс полосы пропускания необходимую долю полосы. Далее P-793H 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-793H выделяет дополнительную полосу пропускания только этому классу.

Когда расширить полосу требуется нескольким классам, P-793H 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-793H равномерно распределяет доступную полосу пропускания между классами с одинаковым уровнем приоритета.

13.6.1 Резервирование полосы пропускания для трафика, не отнесенного к классам

Чтобы разрешить P-793H выделять полосу пропускания трафику, не указанному в фильтре полосы пропускания, выполните следующие три операции.

1. Оставьте некоторую часть полосы пропускания интерфейса, не внося ее в бюджет.
2. Не включайте для интерфейса параметр **Maximize Bandwidth Usage**.
3. Не включайте заимствование полосы пропускания на дочерних классах, имеющих корневой класс в качестве родительского (см. разд. 13.8 на стр. 201).

13.6.2 Пример максимизации использования полосы пропускания

Рассмотрим пример настройки P-793H 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.

Таблица 62 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-793H делит неиспользуемые 2048 кбит/с между классами, требующими большей полосы пропускания. Если администрация только использует 1024 кбит/с из выделенных 2048 кбит/с, P-793H также делит оставшиеся 1024 кбит/с среди классов, которым требуется большая полоса пропускания. Таким образом, P-793H делит 3072 кбит/с невыделенной и неиспользованной полосы пропускания между классами, которым требуется увеличенная полоса пропускания.

13.6.2.1 Распределение неиспользованной и невыделенной полосы пропускания на основе приоритетов

В следующей таблице указаны приоритеты классов полосы пропускания и доля полосы пропускания, выделяемая каждому классу.

Таблица 63 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-793H 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.

13.6.2.2 Распределение неиспользованной и невыделенной полосы пропускания на основе равнодоступности

В следующей таблице представлен бюджет полосы пропускания для каждого класса.

Таблица 64 Распределение неиспользованной и невыделенной полосы пропускания на основе равнодоступности

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-793H 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.

13.6.3 Перерасход полосы пропускания

Скорость интерфейса в управлении полосой пропускания можно установить выше его фактической скорости. В этом случае более приоритетный трафик использует всю выделенную ему полосу пропускания вплоть до физической полосы пропускания интерфейса. В результате передача трафика с меньшим приоритетом может быть приостановлена. Пример представлен ниже.

Таблица 65 Пример перерасхода полосы пропускания

КЛАССЫ И РАСПРЕДЕЛЯЕМЫЕ ДОЛИ ПОЛОСЫ ПРОПУСКАНИЯ		ПРИОРИТЕТЫ
Фактическая полоса пропускания интерфейса: 1000 кбит/с		
Корневой класс: 1500 кбит/с (совпадает с настройкой в поле Speed)	Трафик VoIP (Service = SIP): 500 кбит/с	Высокая
	Трафик NetMeeting (Service = H.323): 500 кбит/с	Высокая
	Трафик FTP (Service = FTP): 500 кбит/с	Средняя

При одновременном использовании VoIP и NetMeeting устройство выделяет каждому из приложений полосу до 500 кбит/с и только затем отдает остаток протоколу FTP. В результате канал доступен для протокола FTP только в те периоды времени, когда VoIP и NetMeeting не используют всю выделенную им полосу пропускания.

Предположим, что пользователь также пытается работать с WWW. В этом случае VoIP, NetMeeting и FTP, имея более высокий приоритет, получают полосу пропускания в первую очередь. Использование WWW возможно только в то время, когда VoIP, NetMeeting и FTP в совокупности используют менее 1000 кбит/с (физически доступной полосы пропускания).

13.6.4 Приоритеты для управления полосой пропускания

В следующей таблице описаны приоритеты, которые можно применять к трафику, отправляемому P-793H через интерфейс.

Таблица 66 Приоритеты для управления полосой пропускания

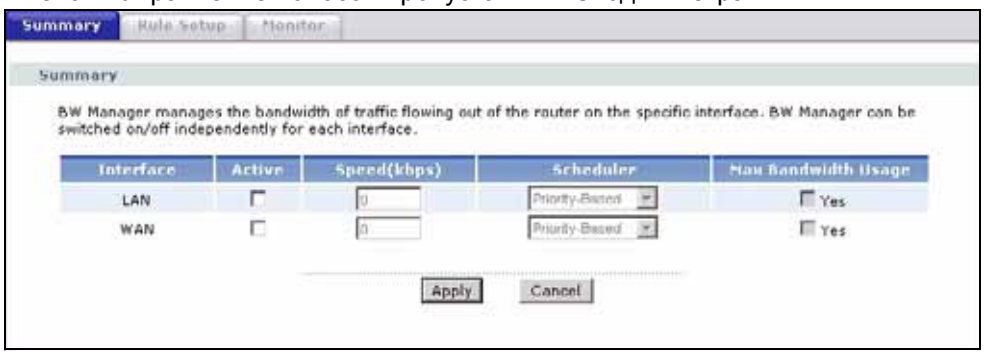
УРОВНИ ПРИОРИТЕТА: ТРАФИК С БОЛЕЕ ВЫСОКИМ ПРИОРИТЕТОМ ПРОХОДИТ БЫСТРЕЕ, В ТО ВРЕМЯ КАК ТРАФИК С МЕНЬШИМ ПРИОРИТЕТОМ ОТБРАСЫВАЕТСЯ, ЕСЛИ СЕТЬ ПЕРЕПОЛНЕНА.	
Высокий (high)	Обычно применяется для голосового или видеотрафика, особенно чувствительного к неустойчивой синхронизации (т. е. к изменчивости задержек).
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.

13.7 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. 94 Управление полосой пропускания > Сводный экран



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 67 Управление полосой пропускания > Сводный экран

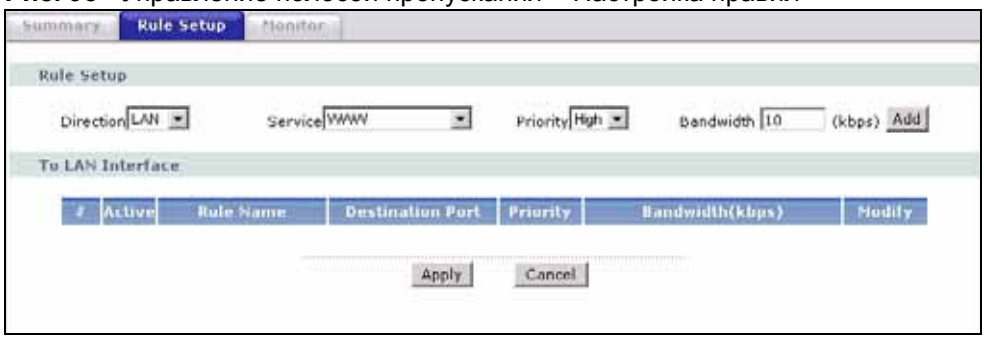
ПОЛЕ	ОПИСАНИЕ
Interface	В этих нередактируемых полях отображаются физические интерфейсы. Чтобы включить для интерфейса управление полосой пропускания, отметьте флажок. Управление полосой пропускания применяется ко всему трафику, выходящему через интерфейс, независимо от источника трафика. Переадресация трафика или совмещение IP-адресов могут вызывать прохождение трафика из LAN в LAN через P-793H, 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-793H примет в качестве полосы пропускания значение, заданное в этом поле. P-793H не будет использовать дополнительную полосу пропускания для соединений через этот интерфейс, даже если исходящая полоса пропускания у этого интерфейса выше.
Scheduler	В раскрывающемся меню выберите тип планировщика для трафика: **Priority-Based** (на основе 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-793H 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-793H.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

13.8 Настройка правил управления полосой пропускания

Дополнительные сведения см. в разд. 13.1 на стр. 195. 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. 95 Управление полосой пропускания > Настройка правил



Поля изображенного выше экрана описаны в следующей таблице.

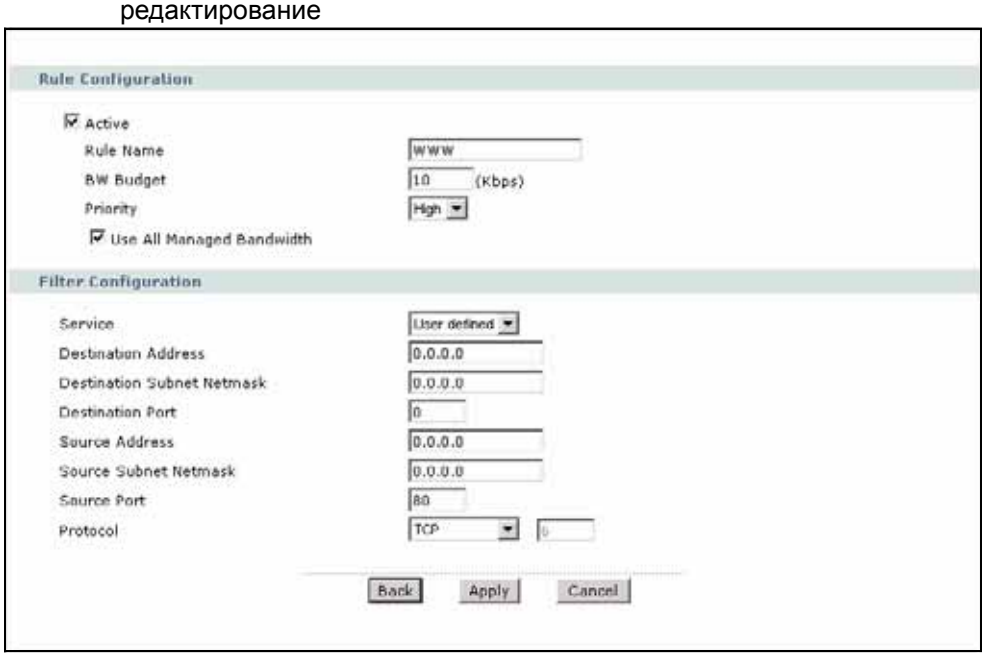
Таблица 68 Управление полосой пропускания > Настройка правил

ПОЛЕ	ОПИСАНИЕ
Rule Setup	
Direction	Выберите направление трафика, к которому применяется управление полосой пропускания.
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	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.
Add	Нажмите эту кнопку, чтобы добавить правило в расположенную ниже таблицу.
To Interface	
#	В этом поле отображается номер правила управления полосой пропускания.
Active	В этом поле отображается состояние правила. Отметьте этот флажок, чтобы активировать данное правило в P-793H. Активация правила означает, что весь трафик, соответствующий данному правилу, будет иметь приоритет над остальным трафиком. Активация правила управления полосой пропускания также позволяет задать максимальную долю полосы пропускания, которая может использоваться трафиком, подпадающим под правило.
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 редактирования правила, щелкните на значке **Edit**. Для удаления существующего правила щелкните на значке **Remove**.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-793H.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

13.8.1 Rule Configuration

Дополнительные сведения см. в разд. 13.1 на стр. 195. Этот экран служит для настройки правила управления полосой пропускания. Правила управления полосой пропускания служат для распределения определенных долей полосы пропускания (бюджетов) между различными приложениями и/или подсетями. Чтобы открыть этот экран, щелкните на значке редактирования (Edit) или выберите **User define** в поле **Service**.

Рис. 96 Управление полосой пропускания > Настройка правила > Добавление/редактирование



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 69 Управление полосой пропускания > Настройка правила > Добавление/редактирование

ПОЛЕ	ОПИСАНИЕ
Rule Configuration	
Active	Отметьте этот флажок, чтобы активировать данное правило в P-793H. Активация правила означает, что весь трафик, соответствующий данному правилу, будет иметь приоритет над остальным трафиком. Активация правила управления полосой пропускания также позволяет задать максимальную долю полосы пропускания, которая может использоваться трафиком, подпадающим под правило.
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).

Таблица 69 Управление полосой пропускания > Настройка правила > Добавление/редактирование (продолжение)

ПОЛЕ	ОПИСАНИЕ
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	
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 аудио-, видеопотоков 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**, которые заполняются только если указывается соответствующий IP-адрес источника или получателя).
Адрес получателя	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 приложениях.
Destination Port	Укажите номер порта на стороне получателя. *Приложение G на стр. 429* содержит перечень часто используемых номеров портов и сетевых служб. 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 приложениях. Пустое поле означает любой номер порта.
Source Port	Укажите номер порта на стороне источника. *Приложение G на стр. 429* содержит перечень часто используемых номеров портов и сетевых служб.

Таблица 69 Управление полосой пропускания > Настройка правила > Добавление/редактирование (продолжение)

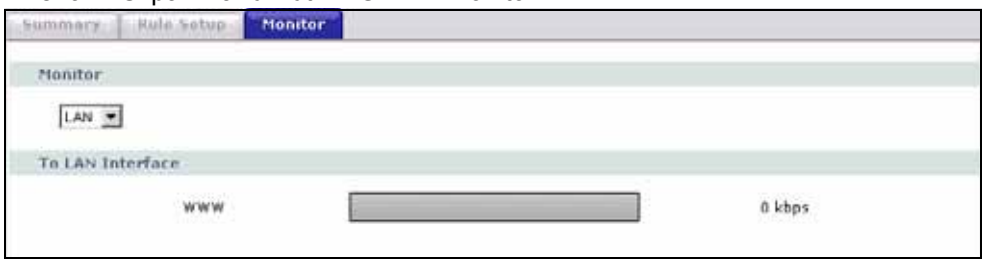
ПОЛЕ	ОПИСАНИЕ
Protocol	Выберите протокол (**TCP** или **UDP**) или выберите **User defined** и укажите номер протокола (тип службы). ID 0 означает любой номер протокола.
Back	Для возврата к предыдущему экрану нажмите кнопку **Back**.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-793H.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

13.9 Монитор полосы пропускания

Дополнительные сведения см. в разд. 13.1 на стр. 195. По этой ссылке можно просмотреть полосу пропускания, используемую P-793H, и объемы выделения полосы пропускания. Нажмите кнопку **Advanced > Bandwidth MGMT > Monitor**. Появится изображенный ниже экран.

Чтобы просмотреть полосу пропускания, используемую интерфейсом и его правила, выберите интерфейс из раскрывающегося списка.

Рис. 97 Экран Bandwidth MGMT > Monitor



14

Настройка DNS для динамических адресов

В этой главе поясняется способ настройки DNS для динамических адресов в P-793H.

14.1 Обзор поддержки DNS для динамических адресов

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

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

14.1.1 Шаблон DYNDNS

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

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

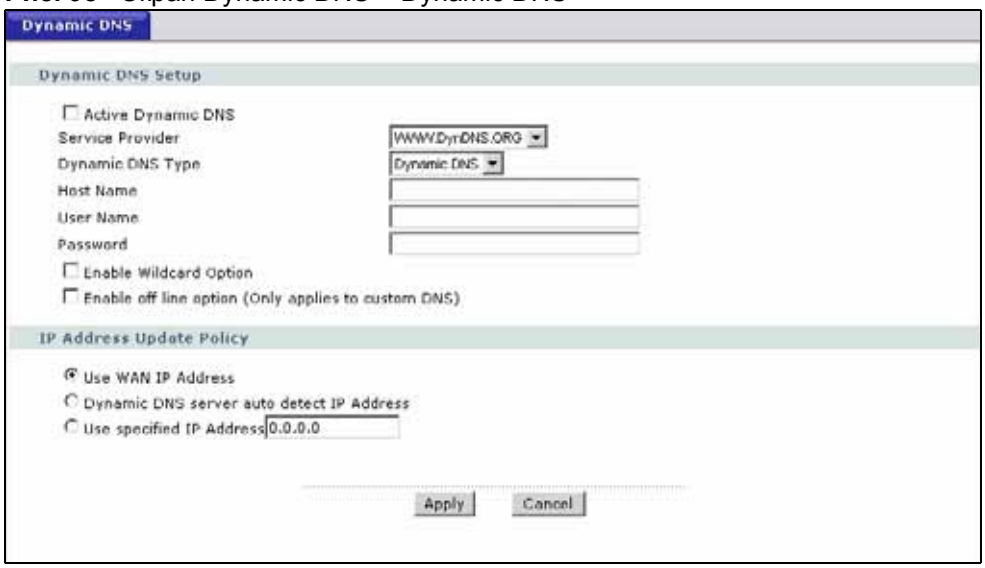
Указания по настройке см. в разд. 14.2 на стр. 207.

14.2 Настройка динамической DNS

Этот экран позволяет изменить параметры DDNS в P-793H. Выберите **Advanced > Dynamic DNS**. Появится изображенный ниже экран.

Дополнительные сведения см. в разд. 14.1 на стр. 207.

Рис. 98 Экран Dynamic DNS > Dynamic DNS



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 70 Экран Dynamic DNS > Dynamic DNS

ПОЛЕ	ОПИСАНИЕ
Dynamic DNS Setup	
Active Dynamic DNS	Установите этот флажок, чтобы использовать динамическую DNS.
Service Provider	Это название поставщика услуг динамической DNS.
Dynamic DNS Type	Выберите тип услуги, зарегистрированной у поставщика услуг DDNS.
Host Name	Введите доменное имя, присвоенное вашему P-793H поставщиком услуг DDNS. В каждом поле можно указать до двух имен хостов, отделенных запятыми.
User Name	Введите имя пользователя.
Password	Введите присвоенный вам пароль.
Enable Wildcard Option	Чтобы активировать шаблон DynDNS, отметьте флажок.
Enable off line option	Это поле доступно только в том случае, если в поле **DDNS Type** выбрано значение **Custom DNS**. Узнайте у поставщика услуг динамической DNS о возможности переадресации трафика на указанный вами URL в то время, когда вы не подключены к сети.
IP Address Update Policy	
Use WAN IP Address	Выберите этот параметр, чтобы использовать для обновления IP-адресов указанных имен хостов IP-адрес со стороны WAN.

Таблица 70 Экран Dynamic DNS > Dynamic DNS (продолжение)

ПОЛЕ	ОПИСАНИЕ
Dynamic DNS server auto detect IP Address	Этот параметр следует выбирать только в том случае, если между P-793H 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-793H 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-793H.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

15

Настройка удаленного управления

В этой главе содержится информация о настройке удаленного управления.

15.1 Обзор удаленного управления

Удаленное управление позволяет определять, какие службы/протоколы могут получать доступ к определенному интерфейсу P-793H (если это возможно) и с каких компьютеров.

При настройке удаленного управления с целью управления из WAN необходимо настроить правило межсетевого экрана, разрешающее доступ.

Устройством P-793H можно управлять удаленно через:

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

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-793H 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

15.1.1 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-793H 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.

15.1.2 Удаленное управление и NAT

При включенной системе NAT:

- Если настройка выполняется через WAN, укажите IP-адрес P-793H на стороне WAN.
- Если настройка выполняется через LAN, укажите IP-адрес P-793H на стороне LAN.

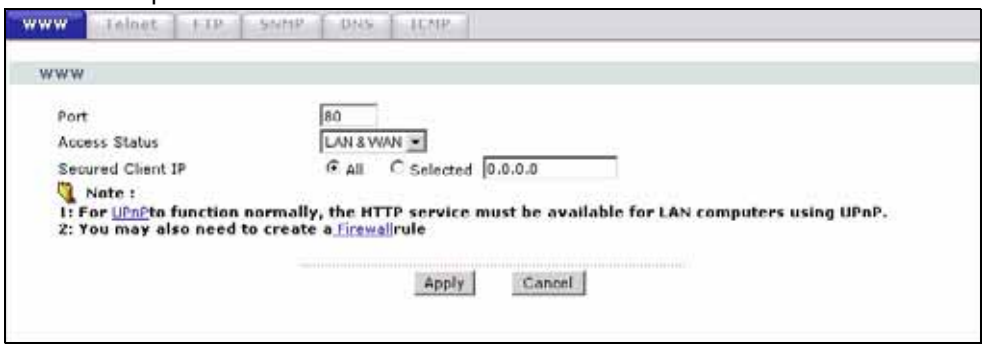
15.1.3 Системный таймер неактивности

Для управления системой установлен интервал неактивности. P-793H автоматически отменяет регистрацию пользователя, если сеанс управления остается бездействующим дольше этого периода времени ожидания. Сеанс управления не прерывается при выполнении опроса на экране статистики. По умолчанию он равен пяти минутам. Настройка этого интервала и запрет разъединения по неактивности описаны в разд. 17.1.2 на стр. 237.

15.2 WWW

Этот параметр позволяет настроить параметры веб-интерфейса для удаленного управления P-793H. Чтобы перейти на экран **WWW**, выберите **Advanced > Remote MGMT**.

Рис. 99 Экран Remote MGMT > WWW



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 71 Экран Remote MGMT > WWW

ПОЛЕ	ОПИСАНИЕ
Port	При необходимости можно изменить номер порта сервера для службы, однако следует использовать тот же самый номер порта для применения данной службы в целях удаленного управления.
Access Status	Выберите интерфейсы, через которые компьютер может получать доступ к P-793H с использованием данной службы.
Secured Client IP	Защищенный клиент – это "доверенный" компьютер, которому разрешается обмениваться данными с P-793H, используя эту службу. Выберите **All**, чтобы разрешить любому компьютеру получать доступ к P-793H посредством этой службы. Выберите **Selected**, чтобы доступ к P-793H посредством данной службы был разрешен только компьютеру с указанным IP- адресом.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-793H.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

15.3 Telnet

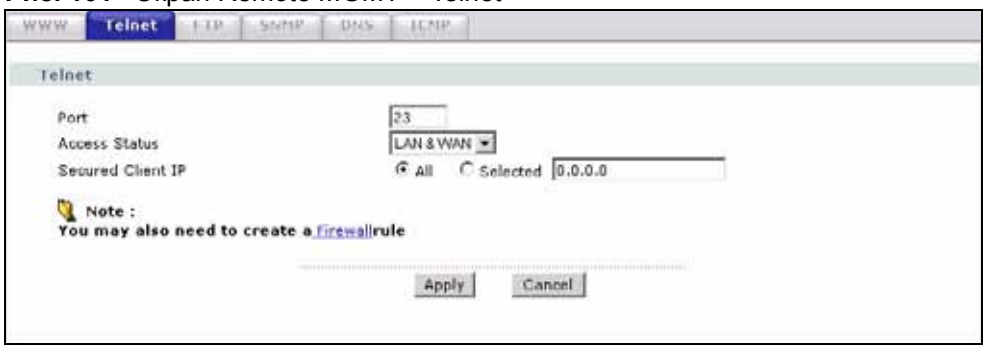
P-793H можно настроить для удаленного доступа по Telnet, как показано ниже. Администратор использует Telnet с компьютера в удаленной сети для получения доступа к P-793H.

Рис. 100 Настройка Telnet в сети TCP/IP

15.4 Настройка Telnet

Дополнительные сведения см. в разд. 15.1 на стр. 211. Этот экран служит для настройки доступа по Telnet к P-793H. Чтобы перейти на показанный ниже экран, выберите **Advanced > Remote MGMT** > вкладка **Telnet** .

Рис. 101 Экран Remote MGMT > Telnet



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 72 Экран Remote MGMT > Telnet

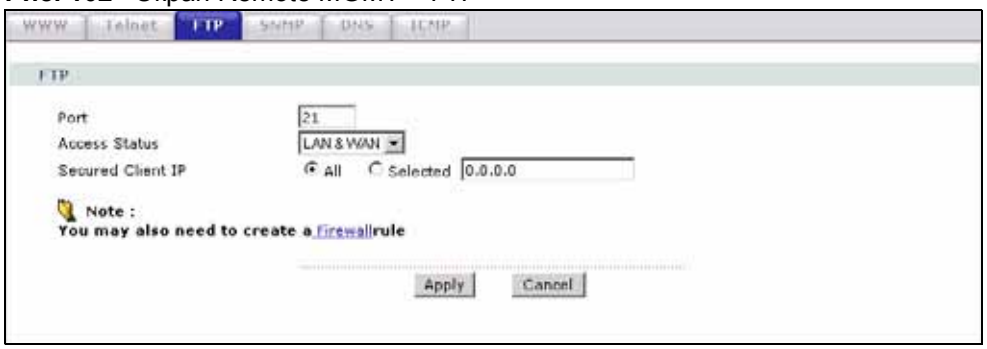
ПОЛЕ	ОПИСАНИЕ
Port	При необходимости можно изменить номер порта сервера для службы, однако следует использовать тот же самый номер порта для применения данной службы в целях удаленного управления.
Access Status	Выберите интерфейсы, через которые компьютер может получать доступ к P-793H с использованием данной службы.
Secured Client IP	Защищенный клиент – это "доверенный" компьютер, которому разрешается обмениваться данными с P-793H, используя эту службу. Выберите **All**, чтобы разрешить любому компьютеру получать доступ к P-793H посредством этой службы. Выберите **Selected**, чтобы доступ к P-793H 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**.

15.5 Настройка FTP

По протоколу FTP можно загружать в P-793H файлы микропрограмм и настроек. Подробности см. в главе о работе с файлом настроек. Для использования этой возможности ваш компьютер должен иметь FTP-клиента.

Дополнительные сведения см. в разд. 15.1 на стр. 211. Этот экран служит для управления доступом к P-793H по FTP. Чтобы изменить параметры FTP для P-793H, выберите **Advanced > Remote MGMT** > закладка **FTP**. Появится изображенный ниже экран.

Рис. 102 Экран Remote MGMT > FTP



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 73 Экран Remote MGMT > FTP

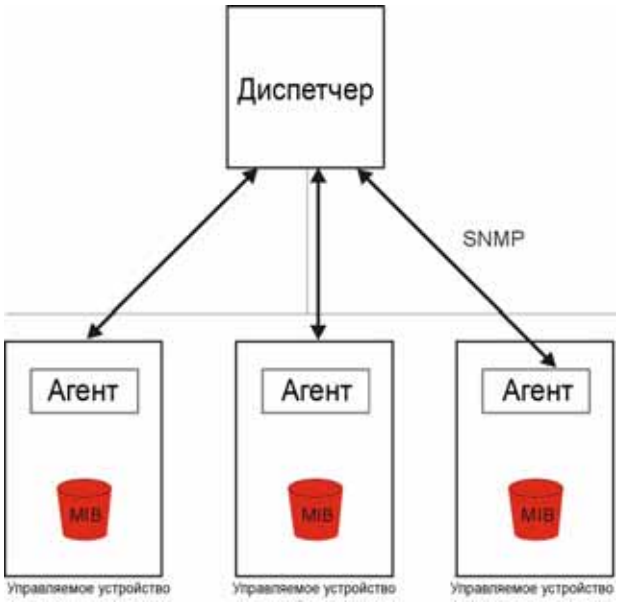
ПОЛЕ	ОПИСАНИЕ
Port	При необходимости можно изменить номер порта сервера для службы, однако следует использовать тот же самый номер порта для применения данной службы в целях удаленного управления.
Access Status	Выберите интерфейсы, через которые компьютер может получать доступ к P-793H с использованием данной службы.
Secured Client IP	Защищенный клиент – это "доверенный" компьютер, которому разрешается обмениваться данными с P-793H, используя эту службу. Выберите **All**, чтобы разрешить любому компьютеру получать доступ к P-793H посредством этой службы. Выберите **Selected**, чтобы доступ к P-793H 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**.

15.6 SNMP

Протокол SNMP (Simple Network Management Protocol - упрощенный протокол управления сетью) используется для обмена управляющей информацией между сетевыми устройствами. SNMP входит в семейство протоколов TCP/IP. P-793H поддерживает функциональные возможности агента SNMP, что позволяет управляющей станции выполнять управление и мониторинг P-793H через сеть. P-793H поддерживает первую (SNMPv1) и вторую (SNMPv2) версии протокола SNMP. На следующем рисунке показана схема управления на основе SNMP.

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

Рис. 103 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-793H). Агент преобразует локальные параметры управления, используемые в управляемом устройстве, в формат, совместимый с SNMP. Менеджер – это консоль, через которую администратор сети управляет устройствами. Диспетчер выполняет ПО для управления и мониторинга управляемых устройств.

Управляемые устройства содержат объекты-переменные или управляемые объекты, характеризующие все виды сведений, которые можно получить об устройстве. Примерами таких переменных являются: число полученных пакетов, состояние портов узла и т. д. Информационная база управления (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 определенных событиях.

15.6.1 Поддерживаемые базы MIB

P-793H 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.

15.6.2 Прерывания SNMP

P-793H направляет прерывания диспетчеру SNMP при наступлении одного из следующих событий:

Таблица 74 Прерывания SNMPv1

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).
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 превышенном коде, если система перезагружается из-за неустранимых ошибок.

Таблица 75 Прерывания SNMPv2

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

15.6.3 Настройка SNMP

Дополнительные сведения см. в разд. 15.1 на стр. 211. Этот экран позволяет изменить настройки SNMP в P-793H. Выберите **Advanced > Remote MGMT** > **SNMP**. Появится изображенный ниже экран.

Рис. 104 Экран Remote MGMT > SNMP

Поля изображенного выше экрана описаны в следующей таблице.

Таблица 76 Экран Remote MGMT > SNMP

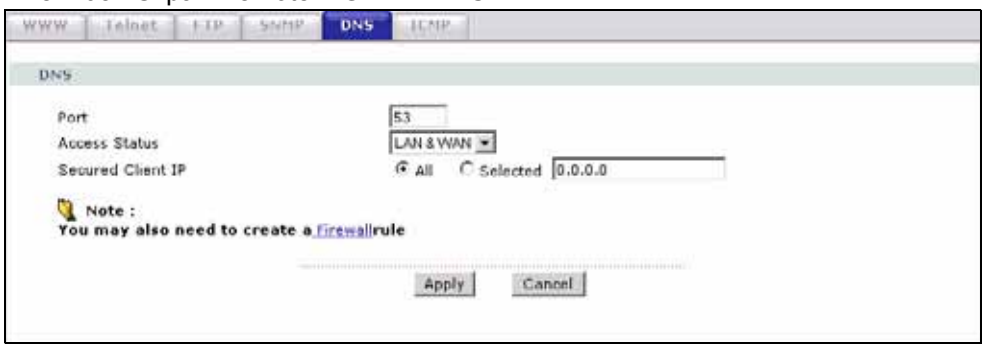
ПОЛЕ	ОПИСАНИЕ
SNMP	
Port	При необходимости можно изменить номер порта сервера для службы, однако следует использовать тот же самый номер порта для применения данной службы в целях удаленного управления.
Access Status	Выберите интерфейсы, через которые компьютер может получать доступ к P-793H с использованием данной службы.
Secured Client IP	Защищенный клиент – это "доверенный" компьютер, которому разрешается обмениваться данными с P-793H, используя эту службу. Выберите **All**, чтобы разрешить любому компьютеру получать доступ к P-793H посредством этой службы. Выберите **Selected**, чтобы доступ к P-793H 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.
Trap Community	Введите сообщество для прерываний, которое будет выступать в качестве пароля при отправке прерываний диспетчеру SNMP. Значение по умолчанию – "общедоступно", все запросы разрешены.
Trap Destination	Введите IP-адрес станции, которой следует направлять прерывания SNMP.
Apply	Нажмите кнопку **Apply** для сохранения настроек и выхода из данного экрана.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

15.7 Настройка DNS

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

Дополнительные сведения см. в разд. 15.1 на стр. 211. Выберите **Advanced > Remote MGMT** > **DNS**. Появится изображенный ниже экран. Этот экран позволяет задать IP-адреса, от которых P-793H будет принимать DNS-запросы, и указать интерфейс, через который P-793H будет рассылать параметры DNS на эти адреса.

Рис. 105 Экран Remote MGMT > DNS



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 77 Экран Remote MGMT > DNS

ПОЛЕ	ОПИСАНИЕ
Port	При необходимости можно изменить номер порта сервера для службы, однако следует использовать тот же самый номер порта для применения данной службы в целях удаленного управления.
Access Status	Выберите интерфейсы, через которые компьютер может отправлять запросы DNS на P-793H.
Secured Client IP	Защищенный клиент – это "доверенный" компьютер, которому разрешается отправлять запросы DNS на P-793H. Выберите переключатель **All**, чтобы разрешить любому компьютеру отправлять запросы DNS на P-793H. Выберите переключатель **Selected**, чтобы разрешить только компьютеру с указанным IP-адресом отправлять запросы DNS на P-793H.
Apply	Нажмите кнопку **Apply** для сохранения настроек и выхода из данного экрана.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

15.8 Настройка ICMP

Этот экран определяет режим обработки других видов запросов в P-793H. Выберите **Advanced > Remote MGMT** > **ICMP**. Появится изображенный ниже экран.

Если внешний пользователь попытается прозондировать неподдерживаемый порт P-793H, автоматически будет возвращен пакет с откликом ICMP (протокол управляющих сообщений в Интернете). Это позволяет внешнему пользователю узнать о том, что P-793H существует. P-793H предусматривает защиту от зондирования, отключающую отправку пакета с откликом ICMP. Это препятствует обнаружению P-793H посторонними при зондировании неподдерживаемых портов.

Рис. 106 Экран Remote MGMT > ICMP

Поля изображенного выше экрана описаны в следующей таблице.

Таблица 78 Экран Remote MGMT > ICMP

ПОЛЕ	ОПИСАНИЕ
ICMP	Internet Control Message Protocol (межсетевой протокол управляющих сообщений) является протоколом управления сообщениями и предоставления отчетов об ошибках при взаимодействии между сервером хоста и шлюзом. В ICMP используются датаграммы 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-793H не будет реагировать на входящие запросы. Выберите **LAN**, чтобы разрешить ответ на поступающие через локальную сеть эхозапросы. Выберите **WAN** , чтобы разрешить ответ на эхозапросы из WAN. В противном случае выберите **LAN & WAN** для передачи ответов на поступающие эхозапросы LAN и WAN.
Do not respond to requests for unauthorized services	Выберите этот параметр, чтобы предотвратить обнаружение P-793H хакерами путем зондирования неиспользуемых портов. В этом случае P-793H не будет отвечать на запросы неиспользуемых портов, что позволит скрыть неиспользуемые порты и P-793H. По умолчанию этот параметр не выбран, и P-793H 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-793H, прежде чем они будут обрабатываться механизмом противодействия зондированию. Таким образом, если механизм межсетевого экрана блокирует пакет зондирования, P-793H принимает решение, руководствуясь политикой брандмауэра, которая по умолчанию указывает отправить пакет сброса TCP в ответ на заблокированный пакет TCP. Для изменения этой политики можно использовать команду "`sys firewall tcprst rst [on|off]`". Когда механизм брандмауэра блокирует пакет UDP, пакет удаляется без отправки пакета с откликом.
Apply	Нажмите кнопку **Apply** для сохранения настроек и выхода из данного экрана.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

15.9 TR-069

TR-069 – это стандарт, определяющий способы управления устройством P-793H через управляющий сервер, например, через ZyXEL Vantage CNM Access. TR-069 основан на обмене сообщениями RPC (удаленного вызова процедур) между управляющим сервером и клиентским устройством (которым может являться P-793H). Обмен сообщениями RPC осуществляется в формате XML (расширяемого языка разметки) по транспортному протоколу HTTP.

С помощью CNM Access администратор может дистанционно настраивать и перенастраивать P-793H, обновлять микропрограмму, а также осуществлять контроль и диагностику P-793H. Для этого достаточно разрешить управление устройством с CNM Access и указать IP-адрес или доменное имя CNM Access, а также имя пользователя и пароль.

Для настройки управления P-793H посредством CNM Access выполните описанные ниже операции. Структура команд и вызов CLI (интерфейса командной строки) в P-793H описаны в приложении "Интерпретатор команд".

В этом примере CNM Access имеет IP-адрес **a.b.c.d**. Вы должны изменить это значение, указав фактический IP-адрес или доменное имя управляющего сервера. Подробное описание команд см. в **таб. 79 на стр. 221**.

Рис. 107 Активация TR-069

```
ras> wan tr069 load
ras> wan tr069 acsUrl a.b.c.d
Auto-Configuration Server URL: http://a.b.c.d
ras> wan tr069 periodicEnable 1
ras> wan tr069 informInterval 2400
TR069 Informinterval 2400
ras> wan tr069 active 1
ras> wan tr069 save
```

Описание команд TR-069 приведено в следующей таблице.

Таблица 79 Команды TR-069

КОРЕНЬ	КОМАНДА ИЛИ ПОДКАТАЛОГ	КОМАНДА	ОПИСАНИЕ
wan	tr069		Все команды, связанные с TR-069, начинаются с текста `wan tr069`.
		load	Начинает настройку TR-069 в P-793H.
		active [0:нет/1:да]	Включает или отключает TR-069
		acsUrl <URL>	Задает IP-адрес или доменное имя CNM Access.
		username [до 15 знаков]	Имя пользователя для аутентификации устройства при подключении к CNM Access. Это имя пользователя задается на сервере и должно быть предоставлено администратором CNM Access.
		password [до 15 знаков]	Пароль для аутентификации устройства при подключении к CNM Access. Этот пароль задается на сервере и должен быть предоставлен администратором CNM Access.

Таблица 79 Команды TR-069

КОРЕНЬ	КОМАНДА ИЛИ ПОДКАТАЛОГ	КОМАНДА	ОПИСАНИЕ
		`periodicEnable [0:выкл./1:вкл.]`	Указывает, должно ли устройство периодически отправлять информацию серверу CNM Access. Рекомендуется установить это значение равным `1`, разрешив устройству P-793H отправлять информацию на CNM Access.
		`informInterval [сек.]`	Продолжительность интервала (в секундах), в течение которого устройство ДОЛЖНО осуществить попытку соединения с CNM Access для отправки сведений и проверки обновлений конфигурации. Введите значение в диапазоне от 30 до 2147483647 секунд.
		`save`	Сохраняет параметры TR-069 в P-793H.

16

Универсальная технология "включи и работай" (UPnP)

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

16.1 Обзор технологии UPnP

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

Указания по настройке см. в разд. 16.2.1 на стр. 224.

16.1.1 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.

16.1.2 Прослеживание NAT

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

- динамическую привязку портов,
- получение данных об общедоступных IP-адресах,
- назначение сроков действия привязок.

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

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

16.1.3 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-793H 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.

16.2 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.

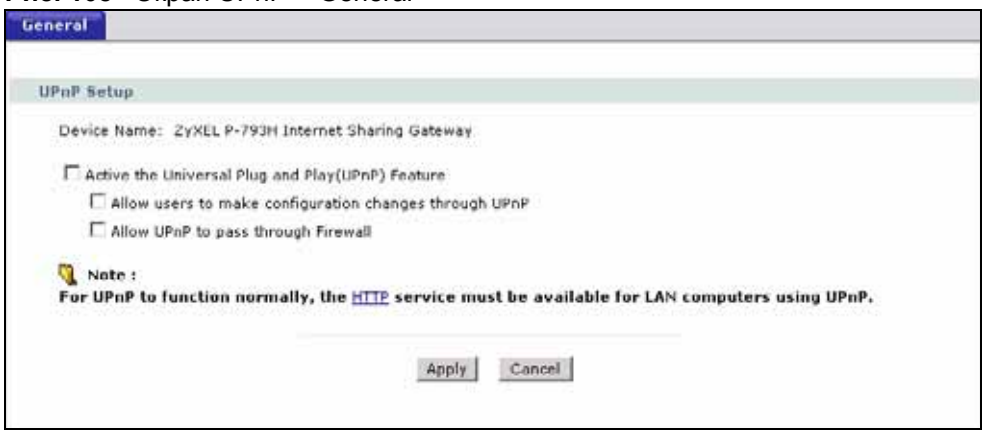
В следующих разделах рассмотрены примеры установки и использования UPnP.

16.2.1 Настройка UPnP

Этот экран служит для настройки UPnP в P-793H. Чтобы перейти на показанный ниже экран, выберите **Advanced > UPnP**.

Дополнительные сведения см. в разд. 16.1 на стр. 223.

Рис. 108 Экран UPnP > General



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 80 Экран UPnP > General

ПОЛЕ	ОПИСАНИЕ
Active the Universal Plug and Play (UPnP) Feature	Отметьте этот флажок, чтобы активировать UPnP. Помните, что любой пользователь сможет посредством приложения UPnP перейти на экран регистрации веб-конфигуратора, не вводя IP-адрес P-793H (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-793H так, чтобы они могли взаимодействовать через P-793H; 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 приложениям, поддерживающим UPnP, автоматически проходить через межсетевой экран P-793H. Будучи менее защищенным, этот вариант снимает необходимость в настройке правил межсетевого экрана для соответствующих приложений.
Apply	Нажмите кнопку **Apply**, чтобы сохранить настройки в P-793H.
Cancel	Чтобы вернуться к прежним настройкам, нажмите **Cancel**.

16.3 Пример установки UPnP в Windows

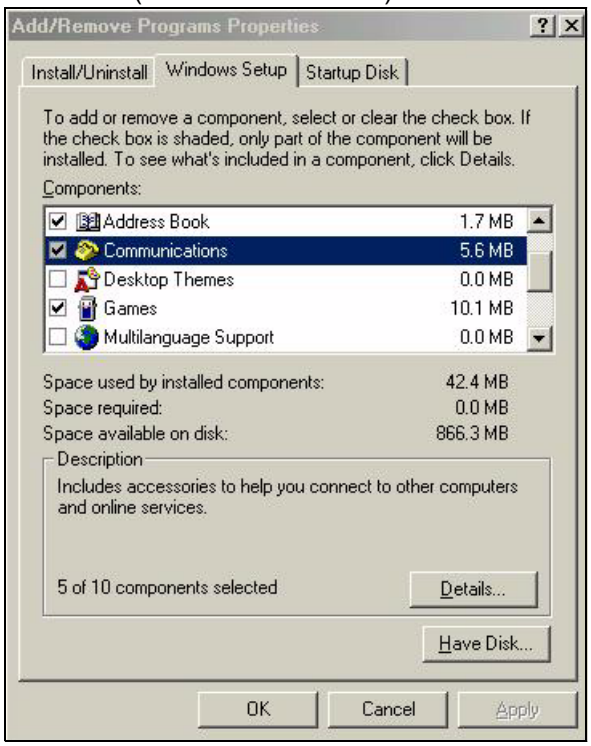
В этом разделе описана установка системы UPnP в Windows Me и Windows XP.

Установка UPnP в Windows Me

Для установки UPnP в Windows Me выполните указанные ниже действия.

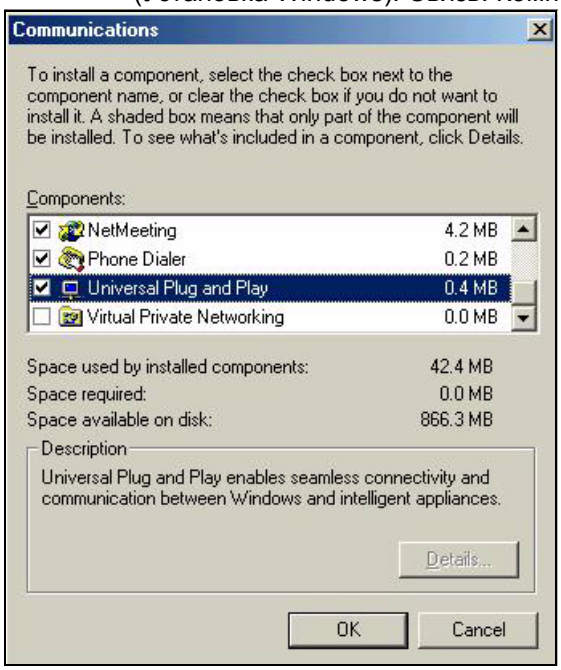
1. Нажмите кнопку **Start (Пуск)** и выберите **Control Panel (Панель управления)**. Выполните двойной щелчок на значке **Add/Remove Programs (Установка и удаление программ)**.
2. Щелкните вкладку **Windows Setup (Установка Windows)** и выберите строку **Communication (Связь)** в поле выбора **Components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

Рис. 109 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. 110 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)**.

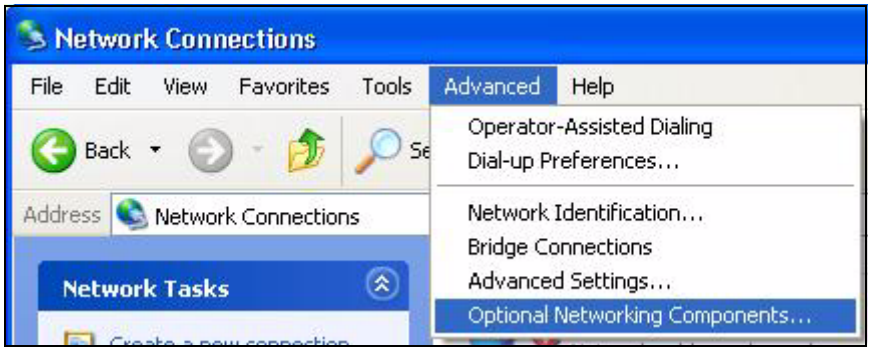
5 Перезапустите компьютер, когда это будет предложено.

Установка UPnP в Windows XP

Для установки UPnP в Windows XP выполните указанные ниже действия.

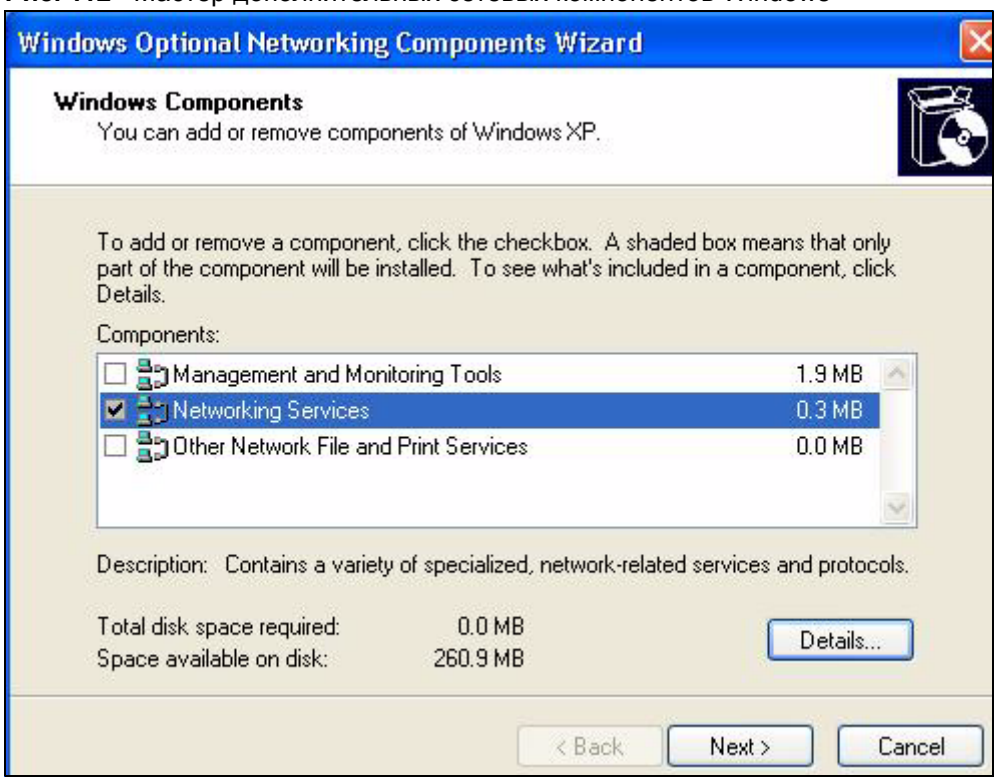
1 Нажмите кнопку **Start (Пуск)** и выберите **Control Panel (Панель управления)**.
2 Дважды щелкните на значке **Network Connections (Сетевые подключения)**.
3 В окне **Network Connections (Сетевые подключения)** щелкните кнопку **Advanced (Дополнительно)** в главном меню и выберите пункт **Optional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

Рис. 111 Сетевые подключения



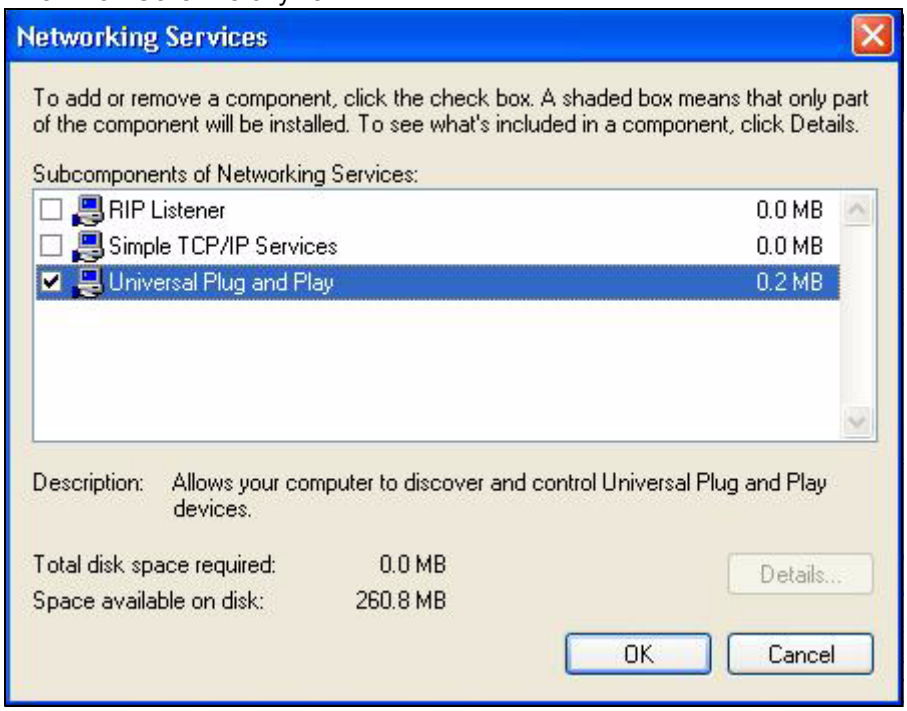
4 Появится окно **Windows Optional Networking Components Wizard (Мастер дополнительных сетевых компонентов Windows)**. Выберите **Networking Service (Сетевые службы)** в окне выбора **Components (Компоненты)** и щелкните кнопку **Details (Состав)**.

Рис. 112 Мастер дополнительных сетевых компонентов Windows



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

Рис. 113 Сетевые службы



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

16.4 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-793H.

Убедитесь в том, что компьютер подключен к порту LAN на P-793H. Включите компьютер и P-793H.

Автоматическое обнаружение сетевого устройства с поддержкой UPnP

1 Нажмите кнопку **Start (Пуск)** и выберите **Control Panel (Панель управления)**. Дважды щелкните на значке **Network Connections (Сетевые подключения)**. Значок отображается под Internet Gateway (шлюзом).

2 Щелкните правой кнопкой мыши по этому значку и выберите **Properties (Свойства)**.

Рис. 114 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. 115 Свойства подключения к Интернету

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

Рис. 116 Свойства подключения к Интернету: Дополнительные параметры

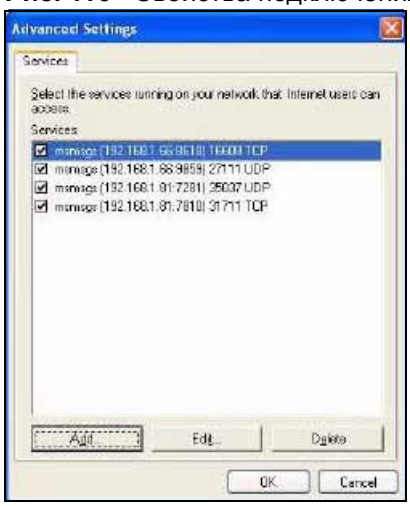
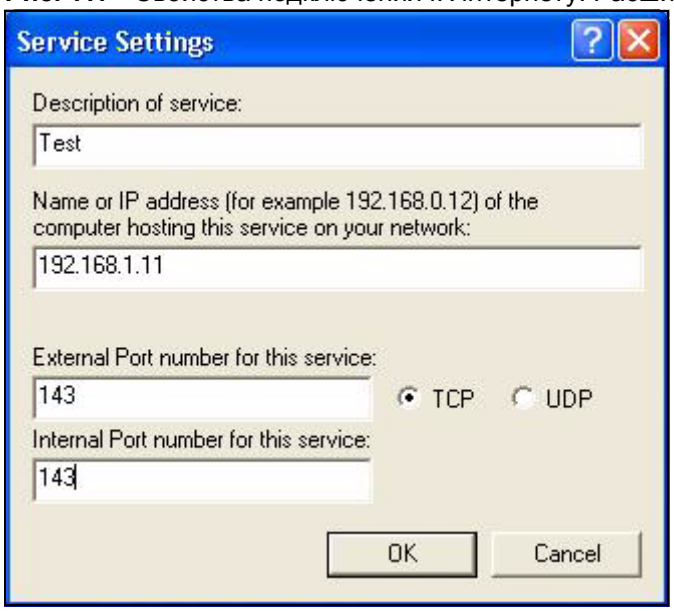


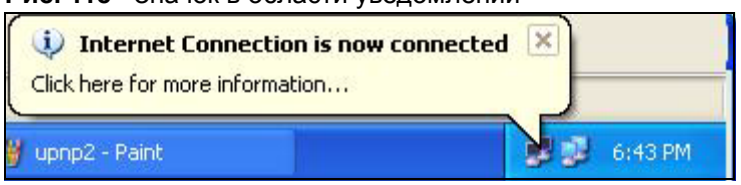
Рис. 117 Свойства подключения к Интернету: Расширенные параметры: Add



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. 118 Значок в области уведомлений



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

Рис. 119 Состояние подключения к Интернету

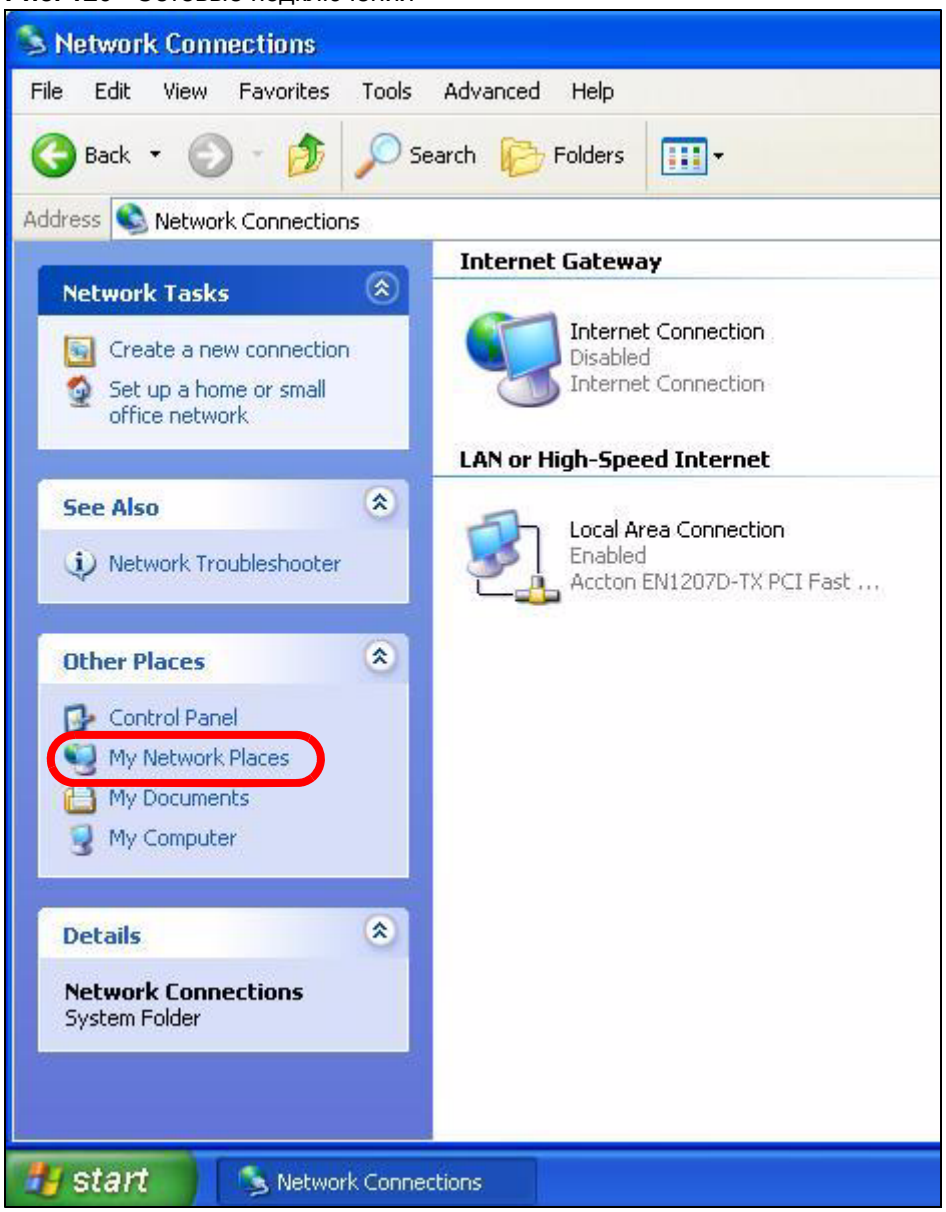
Упрощенный доступ к веб-конфигуратору

Благодаря системе UPnP можно получать доступ к веб-конфигуратору в P-793H без выяснения IP-адреса P-793H. Это полезно, если неизвестен IP-адрес P-793H.

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**.

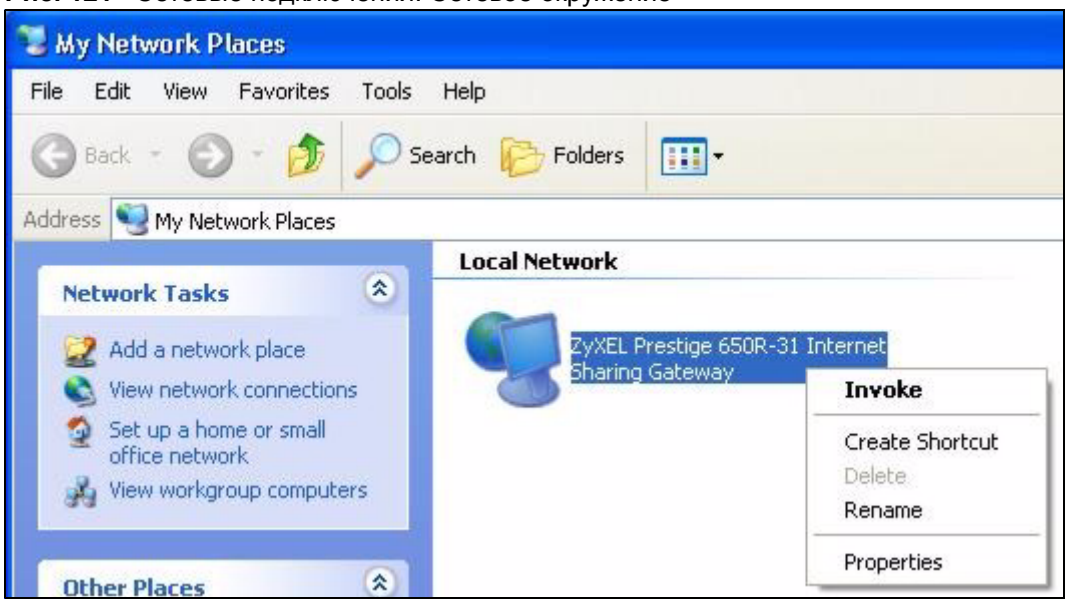
Рис. 120 Сетевые подключения



4 Под заголовком **Local Network** отображается значок с описанием каждого устройства с поддержкой UPnP.

5 Щелкните правой кнопкой мыши по значку P-793H и выберите **Invoke** (Вызвать). Отображается экран регистрации веб-конфигуратора.

Рис. 121 Сетевые подключения: Сетевое окружение



6 Щелкните правой кнопкой мыши по значку P-793H и выберите **Properties** (Свойства). Отображается окно свойств с основной информацией о P-793H.

Рис. 122 Сетевые подключения: Сетевое окружение: свойства: пример

Часть IV
Техническое обслуживание

17

Экран System

В этой главе описывается настройка имени системы, имени домена, пароля, а также времени и даты в P-793H.

17.1 Общая настройка

17.1.1 Разделы General Setup и System Name

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

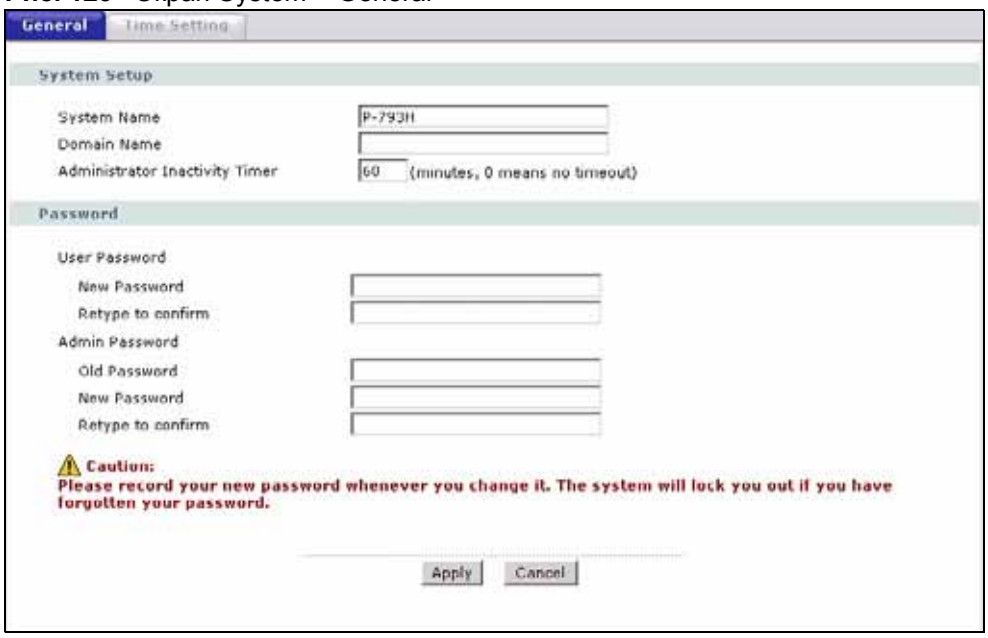
- В Windows 95/98 выберите **Start**(Пуск) , **Settings** (Настройки), **Control Panel** (Панель управления), **Network** (Сеть). Щелкните вкладку Identification (Идентификация), обратите внимание на текст в поле **Computer name** (Имя компьютера) и введите его в поле **System Name**.
- В Windows 2000 нажмите **Start** (Пуск), **Settings** (Настройки), **Control Panel** (Панель управления) и дважды щелкните **System** (Система). Щелкните вкладку **Network Identification** (Идентификация сети), а затем – кнопку **Properties** (Свойства). Обратите внимание на текст в поле **Computer name** (Имя компьютера) и введите его в поле **System Name**.
- В Windows XP нажмите кнопку **Start** (Пуск), **My Computer** (Мой компьютер), **View system information** (Просмотр сведений о системе), а затем щелкните вкладку **Computer Name** (Имя компьютера). Обратите внимание на текст в поле **Full computer name** (Полное имя компьютера) и введите его в поле **System Name** на P-793H.

17.1.2 Общая настройка

В поле **Domain Name** указывается информация, распространяемая DHCP-клиентам в локальной сети. Если оставить это поле пустым, используется имя домена, полученное DHCP от ISP. В то время как имя хоста (System Name – Имя системы) следует вводить на каждом отдельном компьютере, доменное имя назначается из P-793H через DHCP.

Этот экран служит для настройки имени системы P-793H и имени домена, установки таймера неактивности и задания паролей. Чтобы перейти на экран **General**, выберите **Maintenance > System**.

Рис. 123 Экран System > General



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 81 Экран System > General

ПОЛЕ	ОПИСАНИЕ
Общая настройка системы	
System Name	Выберите описательное название, позволяющее идентифицировать оборудование. Рекомендуется ввести в этом поле то же значение, что и в поле "Computer name" ("Имя компьютера"). Допустимая длина – до 30 алфавитно-цифровых знаков. Пробелы не допускаются. Вместо них можно использовать тире "-" и символы подчеркивания "_".
Domain Name	Введите здесь имя домена (если оно известно). Если оставить это поле пустым, ISP может назначить имя домена через DHCP. Имя домена, введенное пользователем, получает приоритет над назначенным ISP именем домена.
Administrator Inactivity Timer	Укажите число минут неактивности сеанса управления (через веб-конфигуратор или интерфейс командной строки), по истечении которого сеанс разрывается. Значение по умолчанию - 5 минут. После истечения сеанса потребуется повторно войти в веб-конфигуратор и ввести пароль. Большая длительность периода неактивности является фактором риска для безопасности системы. Значение "0" означает, что сеанс никогда не разрывается, независимо от периода неактивности (использовать данное значение не рекомендуется).
Password	
User Password	Войдя в систему с паролем пользователя, вы можете только просматривать текущее состояние P-793H. Пароль пользователя по умолчанию – **user**.
New Password	Введите новый системный пароль (до 30 символов). Обратите внимание, что при вводе пароля вместо вводимых символов на экране отображаются звездочки "*". После смены пароля для обращения к P-793H нужно использовать новый пароль.
Retype to Confirm	Снова введите новый пароль для подтверждения.
Admin Password	В дополнение к настройке через мастер пользователь может настраивать специальные функции P-793H, войдя в систему с именем пользователя и паролем администратора.

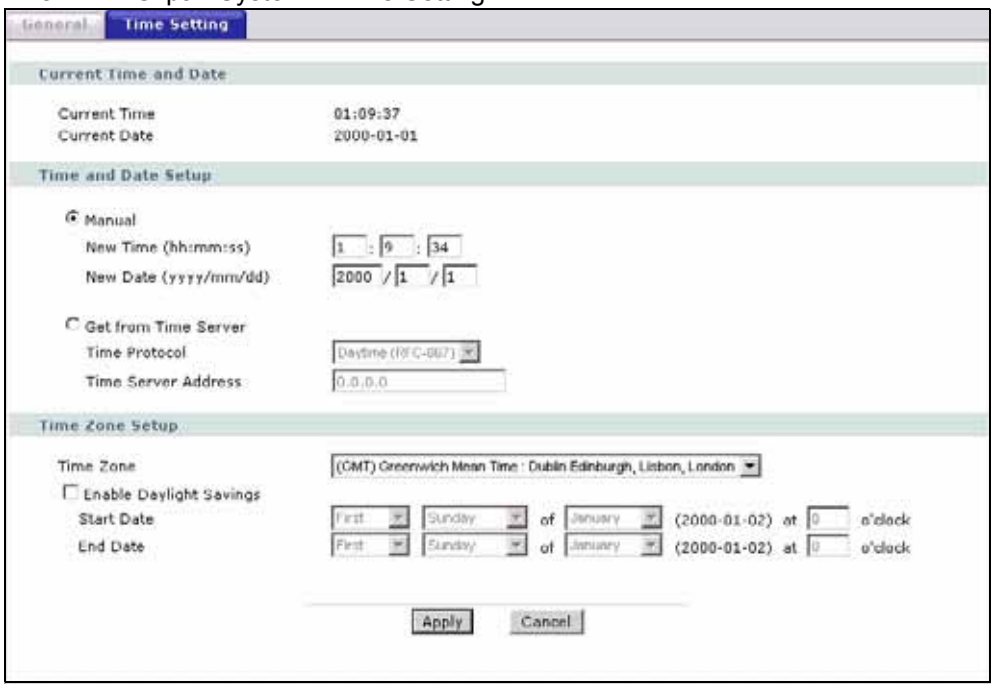
Таблица 81 Экран System > General (продолжение)

ПОЛЕ	ОПИСАНИЕ
Old Password	Для настройки специальных функций введите в этом поле пароль администратора по умолчанию (**1234**) или существующий пароль, используемый для доступа к системе.
New Password	Введите новый системный пароль (до 30 символов). Обратите внимание, что при вводе пароля вместо вводимых символов на экране отображаются звездочки "*". После смены пароля для обращения к P-793H нужно использовать новый пароль.
Retype to Confirm	Снова введите новый пароль для подтверждения.
Apply	Нажмите кнопку **Apply**, чтобы сохранить изменения в P-793H.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

17.2 Установка часов

Для изменения даты и времени в P-793H выберите **Maintenance > System > Time Setting**. Появится изображенный ниже экран. Используйте это окно для настройки времени в P-793H с учетом вашего часового пояса.

Рис. 124 Экран System > Time Setting



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 82 Экран System > Time Setting

ПОЛЕ	ОПИСАНИЕ
Current Time and Date	
Current Time	В этом поле отображается текущее время по часам P-793H. При каждом обновлении этой страницы в браузере P-793H синхронизирует часы с сервером точного времени.

Таблица 82 Экран System > Time Setting (продолжение)

ПОЛЕ	ОПИСАНИЕ
Current Date	В этом поле отображается текущая дата по часам P-793H. При каждом обновлении этой страницы в браузере P-793H 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-793H получало показания даты и времени с указанного ниже сервера точного времени, выберите этот параметр.
Time Protocol	Выберите протокол службы точного времени, по которому P-793H будет обращаться к серверу при включении питания. Не все серверы точного времени поддерживают полный набор протоколов; обратитесь к оператору/администратору сети или подберите работающий протокол методом проб и ошибок. Основные различия между ними заключаются в формате сообщаемого времени. Формат **Daytime (RFC 867)**: день/месяц/год/часовой пояс, в котором находится сервер. Формат **Time (RFC868)**: целое число длиной 4 байта, означающее количество секунд, прошедшее с 0:0:0 01.01.1970 (1970/1/1 в 0:0:0). Формат **NTP (RFC 1305)** похож на Time (RFC 868).
Time Server Address	Введите IP-адрес или URL (до 20 знаков расширенного набора ASCII) сервера точного времени. Если вы не уверены в том, какие значения требуется ввести, обратитесь к провайдеру или администратору сети.
Time Zone Setup	
Time Zone	Выберите часовой пояс для данной местности. Это поле задает разницу во времени между местной временной зоной и гринвичским временем (GMT).
Enable Daylight Saving	Летнее время – это период между поздней весной и началом осени, когда во многих странах стрелки переводятся вперед на 1 час по отношению к обычному местному времени, чтобы продлить светлое время в конце дня. Выберите этот параметр, если в вашем часовом поясе действует переход на зимнее/летнее время.
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.

Таблица 82 Экран System > Time Setting (продолжение)

ПОЛЕ	ОПИСАНИЕ
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-793H.
Cancel	Если нужно начать настройку заново, нажмите кнопку **Cancel**.

18

Журналы

В данной главе описывается настройка общих параметров ведения журналов и просмотр журналов P-793H. Пояснения по сообщениям, оставляемым в журналах, приведены в приложении.

18.1 Обзор средств ведения журналов

Веб-конфигуратор позволяет указать, какие категории событий и/или предупреждений должны отмечаться в журнале P-793H, и затем просмотреть журналы P-793H или переслать их администратору (по электронной почте) или на SYSLOG-сервер.

18.1.1 Журналы и предупреждения

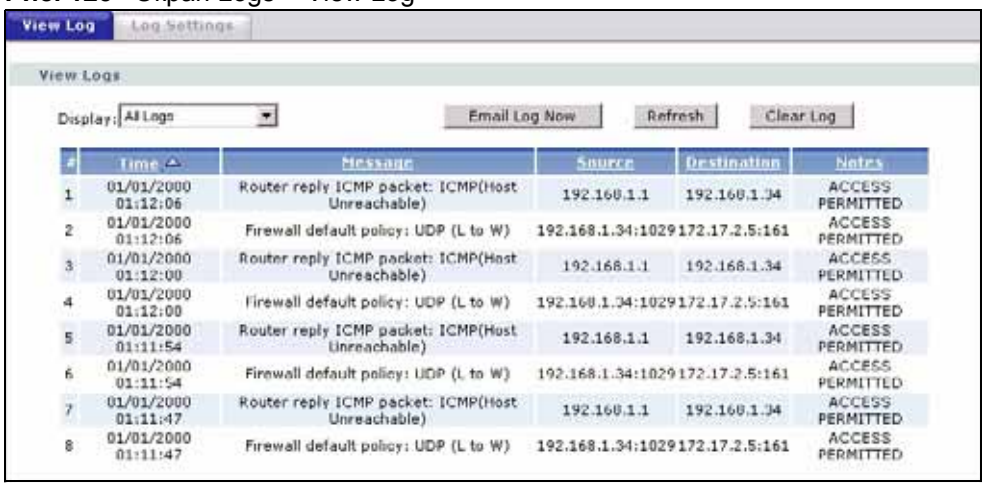
Предупреждение – это журнальное сообщение, требующее более серьезного внимания. К предупреждениям относятся системные ошибки, атаки и попытки доступа к заблокированным веб-сайтам. Некоторые категории, такие как **системные ошибки**, состоят одновременно из простых журнальных сообщений и предупреждений.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

18.2 Просмотр журналов

Чтобы перейти на экран **View Log**, выберите **Maintenance > Logs**. Экран **View Log** служит для просмотра журналов в категориях, выбранных на экране **Log Settings** (см. разд. 18.3 на стр. 244).

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. 125 Экран Logs > View Log



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 83 Экран Logs > View Log

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

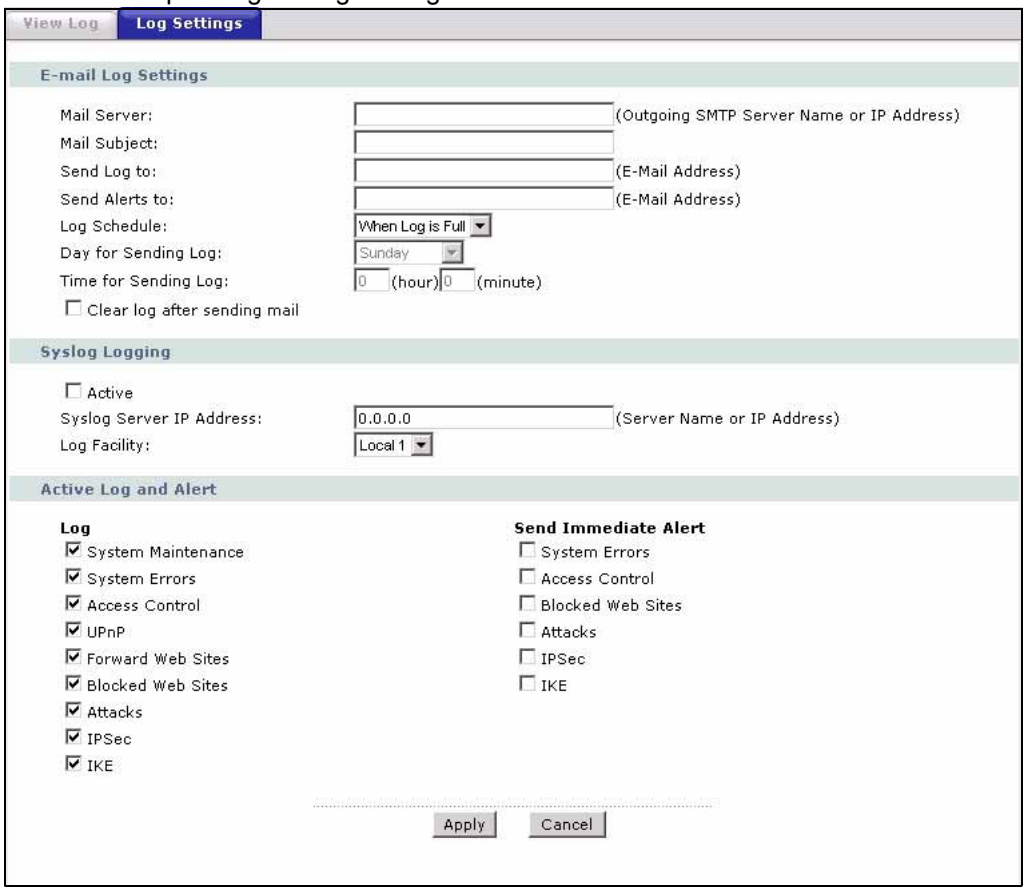
18.3 Настройка параметров ведения журналов

Дополнительные сведения см. в разд. 18.1 на стр. 243. Экран **Log Settings** служит для настройки содержания журналов P-793H, графика отправки сообщений в журналы P-793H и состава журнальных сообщений и экстренных предупреждений, регистрируемых P-793H. Дополнительные сведения см. в разд. 18.1 на стр. 243.

Чтобы изменить параметры ведения журналов P-793H, 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. 126 Экран Logs > Log Settings



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 84 Экран Logs > Log Settings

ПОЛЕ	ОПИСАНИЕ
E-mail Log Settings	
Mail Server	Введите имя сервера или IP-адрес почтового сервера для адресов электронной почты, указанных ниже. Если это поле оставить пустым, журналы и сообщения с предупреждениями не будут отправляться по электронной почте.
Mail Subject	Введите тему, которая будет указываться в заголовке журнальных сообщений, отправляемых P-793H по электронной почте. Это поле имеется не у всех моделей P-793H.
Send Log To	P-793H отправляет журналы по адресу электронной почты, указанному в данном поле. Если это поле оставить пустым, P-793H не будет отправлять журналы по электронной почте.

Таблица 84 Экран Logs > Log Settings

ПОЛЕ	ОПИСАНИЕ
Send Alerts To	Оповещения - это уведомления, отправляемые в режиме реального времени, как только происходит событие, такое как атака DoS, ошибка системы или попытка доступа к запрещенному веб-узлу. Введите адрес электронной почты, по которому должны отправляться сообщения с предупреждениями. Оповещения содержат ошибки системы, атаки и попытки доступа к заблокированным веб-сайтам. Если это поле оставить пустым, сообщения с предупреждениями не будут отправляться по электронной почте.
Log Schedule	Это раскрывающееся меню используется для настройки периодичности отправки журнальных сообщений по электронной почте: **Daily (ежедневно)** **Weekly (еженедельно)** **Hourly (ежечасно)** **When Log is Full (когда журнал полон)** **None (Нет).** При выборе **Weekly** или **Daily** укажите время суток, когда должны отправляться сообщения по электронной почте. При выборе варианта **Weekly** укажите также день недели, когда должно отправляться сообщение. При выборе **When Log is Full** предупреждение отправляется, когда заполнен журнал. При выборе варианта **None** журнальные сообщения не отправляются.
Day for Sending Log	В раскрывающемся списке выберите день недели для отправки журналов.
Time for Sending Log	Введите время дня в 24-часовом формате (например, 23:00 соответствует 11:00 вечера) для отправки журналов.
Clear log after sending mail	Установите этот флажок, чтобы удалять все журналы после того, как P-793H отправит их по электронной почте.
Syslog Logging	P-793H отправляет журнальное сообщение на внешний сервер системного журнала (SYSLOG).
Active	Щелкните на флажке **Active** для включения регистрации системных журналов.
Syslog Server IP Address	Введите имя или IP-адрес сервера SYSLOG, который будет принимать журнальные сообщения указанной категории.
Log Facility	Выберите местоположение из раскрывающегося списка. Распределение по журнальным объектам ("log facility") позволяет записывать сообщения на сервере в различные файлы. Обращайтесь к руководству сервера системных журналов для получения дополнительной информации.
Active Log and Alert	
Log	Выберите категории журналов, которые необходимо записать.
Send Immediate Alert	Выберите категории журналов, предупреждения по которым должны немедленно отправляться P-793H по электронной почте.
Apply	Нажмите кнопку **Apply** для сохранения настроек и выхода из данного экрана.
Cancel	Чтобы вернуться к прежним настройкам, нажмите **Cancel**.

19

Системные инструменты

В этой главе описывается загрузка новой микропрограммы, управление настройками и перезагрузка P-793H.

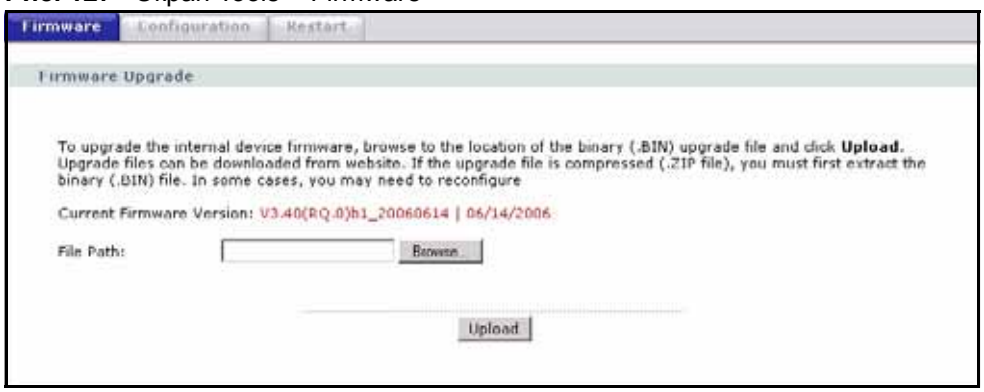
19.1 Обновление микропрограммы

Найдите файл с микропрограммой на сайте www.zyxel.com. Обычно имя файла соответствует номеру модели с расширением ".bin" – например, "P-793H.bin". В процессе загрузки, длящейся до двух минут, используется HTTP (Протокол передачи гипертекста). После успешной загрузки система перезапускается.

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

Чтобы перейти на экран **Firmware**, выберите **Maintenance > Tools**. Для загрузки микропрограммы в P-793H следуйте указаниям на этом экране.

Рис. 127 Экран Tools > Firmware



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 85 Экран Tools > Firmware

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

Таблица 85 Экран Tools > Firmware (продолжение)

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

НЕ выключайте P-793H, пока идет загрузка микропрограммы!

После того, как появится экран **Firmware Upload in Progress**, подождите две минуты, прежде чем снова обращаться к P-793H.

Рис. 128 Выполнение загрузки микропрограммы

По окончании загрузки микропрограммы P-793H автоматически перезапускается, что приводит к временному отключению от сети. В некоторых операционных системах на рабочем столе может находиться следующий значок.

Рис. 129 Сеть временно недоступна

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

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

Рис. 130 Сообщение об ошибке

19.2 Экран Configuration

Этот экран служит для резервного копирования или восстановления настроек P-793H. На нем также можно осуществить сброс P-793H к заводским настройкам по умолчанию. Для перехода на этот экран выберите **Maintenance > Tools > Configuration**.

Рис. 131 Экран Tools > Configuration

Поля изображенного выше экрана описаны в следующей таблице.

Таблица 86 Экран Tools > Configuration

ПОЛЕ	ОПИСАНИЕ
Backup Configuration	
Резервное копирование	Нажмите эту кнопку, чтобы сохранить текущие настройки P-793H на вашем компьютере. После того, как устройство будет настроено и начнет работать в штатном режиме, рекомендуется перед любым изменением настроек делать резервную копию файла настроек. Резервный файл будет полезен в том случае, если потребуется вернуться к предыдущим настройкам.
Restore Configuration	
File Path	Введите местоположение файла для загрузки в устройство или нажмите **Browse...**, чтобы найти файл на диске.
Browse	Нажмите эту кнопку, чтобы найти файл, который требуется загрузить.

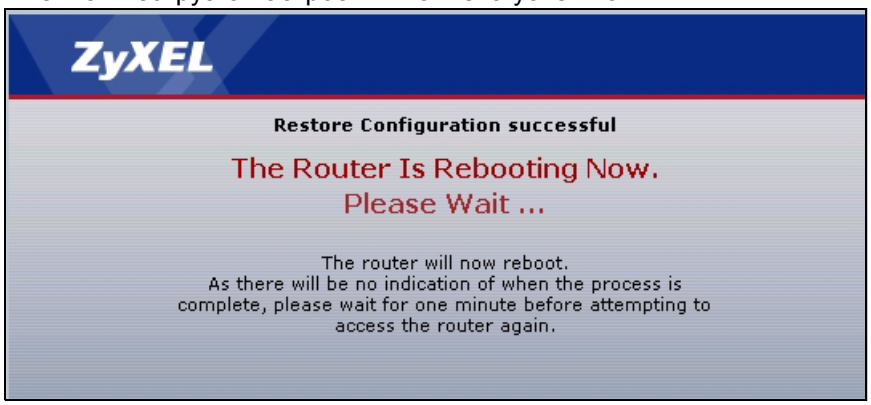
Таблица 86 Экран Tools > Configuration (продолжение)

ПОЛЕ	ОПИСАНИЕ
Upload	Нажмите эту кнопку для восстановления настроек из выбранного файла. Дополнительные сведения приведены ниже. Примечание. Не выключайте устройство во время загрузки в него файла настроек.
Reset to Factory Default Settings	
Reset	Нажмите эту кнопку, чтобы сбросить все пользовательские настройки и восстановить в P-793H заводские настройки по умолчанию. Предупреждающий экран в этом случае не появится. Подробное описание процедуры сброса P-793H см. в разд. 2.5 на стр. 52.

Не выключайте устройство во время загрузки в него файла настроек!

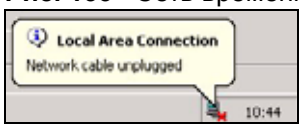
Завершив восстановление настроек из выбранного файла, P-793H выдаст следующий экран.

Рис. 132 Загрузка настроек выполнена успешно



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

Рис. 133 Сеть временно недоступна



Если прежний IP-адрес P-793H отличается от указанного в файле настроек. необходимо проверить, находится ли IP-адрес компьютера в одной подсети с P-793H. Указания по настройки IP-адреса компьютера см. в Руководстве по быстрому запуску.

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

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

Рис. 134 Ошибка при загрузке настроек

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

19.3 Перезагрузка

Функция перезагрузки системы позволяет перезагрузить P-793H, не выключая питание.

Выберите **Maintenance > Tools** > **Restart**. Чтобы перезагрузить P-793H, выберите **Restart**. Эта операция не влияет на настройки P-793H.

Рис. 135 Экран Tools > Restart

20

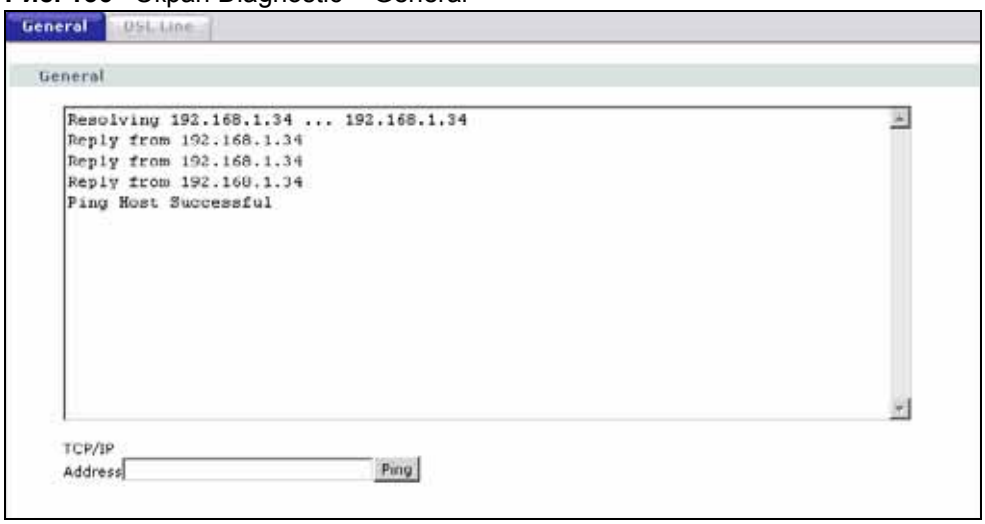
Diagnostic

На этих экранах (доступных только для чтения) отображаются данные, которые могут помочь вам при диагностике проблем с P-793H.

20.1 Общая диагностика

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

Рис. 136 Экран Diagnostic > General



Поля изображенного выше экрана описаны в следующей таблице.

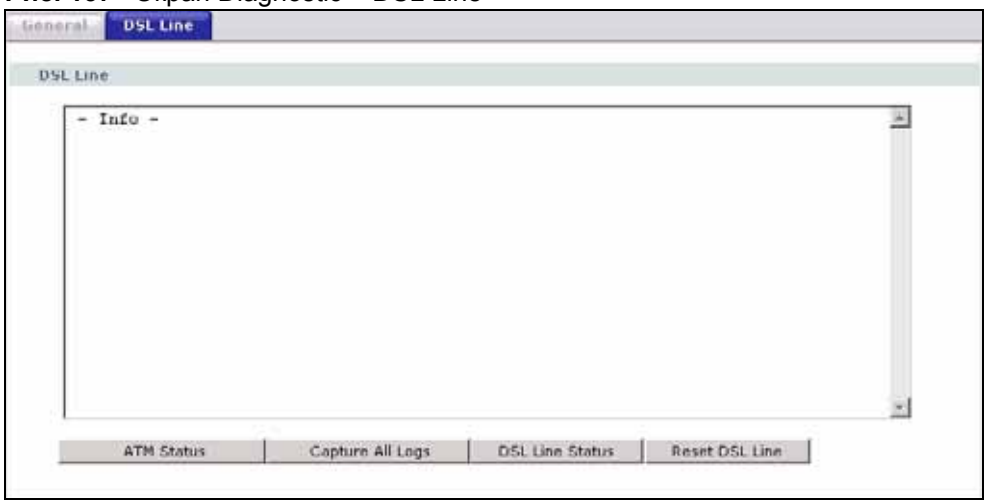
Таблица 87 Экран Diagnostic > General

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

20.2 Экран DSL Line Diagnostic

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

Рис. 137 Экран Diagnostic > DSL Line



Поля изображенного выше экрана описаны в следующей таблице.

Таблица 88 Экран Diagnostic > DSL Line

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

Часть V
Использование SMT и устранение неполадок

21

Введение в SMT

Терминал управления системой (SMT) представляет собой текстовую консоль с системой меню для управления устройством P-793H. В этой главе описан вызов SMT и приведена краткая сводка имеющихся меню.

21.1 Вызов SMT

SMT доступен по протоколу SMT. Выполните следующие операции:

1. В Windows нажмите кнопку **Start** (Пуск) > **Run** (Выполнить).
2. Введите "telnet w.x.y.z", и нажмите **OK**.
   Вместо w.x.y.z укажите IP-адрес устройства P-793H; адрес по умолчанию – 192.168.1.1.
   P-793H предложит ввести пароль.

Рис. 138 Экран входа

```
Password: xxxx
```

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

Изменить пароль можно в меню 23.1.

Рис. 139 Главное меню SMT

```
                Copyright (c) 1994 - 2006 ZyXEL Communications Corp.

                              P-793H Main Menu

    Getting Started                       Advanced Management
      1. General Setup                      21. Filter and Firewall Setup
      2. WAN Setup                          22. SNMP Configuration
      3. LAN Setup                          23. System Password
      4. Internet Access Setup              24. System Maintenance
                                            25. IP Routing Policy Setup
    Advanced Applications                   26. Schedule Setup
      11. Remote Node Setup
      12. Static Routing Setup
      15. NAT Setup                         99. Exit

                            Enter Menu Selection Number:
```

В системе предусмотрен таймер неактивности, по умолчанию настроенный на 10 минут. При отсутствии действий пользователя в течение этого времени P-793H автоматически разрывает сеанс. В этом случае потребуется повторно войти в управление P-793H. Длительность периода неактивности можно настроить в веб-конфигураторе или посредством командной строки (меню 24.8).

21.2 Структура меню SMT

Каждый пункт меню кратко описан в следующей таблице.

Таблица 89 Краткий обзор главного меню

МЕНЮ	НАЗНАЧЕНИЕ
1 General Setup	Это меню позволяет настроить режим работы устройства, службу DNS для динамических адресов и настроить параметры администрирования.
2 WAN Setup	Это меню служит для настройки параметров DSL-соединения, переадресации трафика и резервирования через коммутируемый доступ.
3 LAN Setup	Этот раздел меню служит для применения фильтров LAN, настройки параметров DHCP и TCP/IP для сети LAN, а также для разрешения или блокирования обмена данными на 2-м уровне между отдельными парами портов.
4 Internet Access Setup	Это меню служит для настройки подключения к Интернету.

Таблица 89 Краткий обзор главного меню

МЕНЮ	НАЗНАЧЕНИЕ
11 Remote Node Setup	Это меню используется для детальной настройки параметров удаленного узла (которым может являться ваш поставщик услуг Интернета), а также для применения фильтров.
12 Static Routing Setup	Это меню служит для настройки статических маршрутов IP и статических маршрутов моста (на уровне MAC).
15 NAT Setup	Этот экран позволяет настроить параметры трансляции сетевых адресов (NAT) в P-793H.
21 Filter and Firewall Setup	Это меню используется для настройки фильтров и для активации или деактивации межсетевого экрана.
22 SNMP Configuration	Это меню служит для настройки SNMP.
23 System Password	Это меню служит для изменения пароля.
24 System Maintenance	Это меню служит для комплексной диагностики и обслуживания системы, от контроля состояния до загрузки микропрограммы. Из него также доступен интерфейс командной строки (КС).
25 IP Routing Policy Setup	Это меню служит для настройки маршрутов в соответствии с политиками.
26 Schedule Setup	Это меню служит для настройки наборов расписаний.
99 Exit	Это меню служит для выхода из SMT.

Содержание отдельных меню SMT описано в следующей таблице.

Таблица 90 Общая структура меню SMT

МЕНЮ	ПОДМЕНЮ		
1 General Setup (общая настройка)	1.1 Configure Dynamic DNS (настройка DNS для динамических адресов)		
2 WAN Setup (настройка WAN)	2.1 Traffic Redirect Setup (настройка переадресации трафика)		
	2.2 Dial Backup Setup (настройка резервирования через коммутируемый доступ)	2.2.1 Advanced Dial Backup Setup (расширенная настройка резервирования)	
3 LAN Setup (настройка локальной сети)	3.1 LAN Port Filter Setup (настройка фильтрации портов LAN)		
	3.2 TCP/IP and DHCP Setup (настройка TCP/IP и DHCP)	3.2.1 IP Alias Setup (настройка совмещения IP-адресов)	
	3.6 Port Based VLAN Setup (настройка VLAN на основе портов)		
4 Internet Access Setup (настройка доступа в Интернет)			

Таблица 90 Общая структура меню SMT (продолжение)

МЕНЮ	ПОДМЕНЮ		
11 Remote Node Setup (настройка удаленного узла)	11.1 Remote Node Profile (профиль удаленного узла)	11.1.3 Remote Node Network Layer Options (параметры сетевого уровня для удаленного узла)	
		11.1.5 Remote Node Filter (фильтр удаленного узла)	
		11.1.6 Remote Node ATM Layer Options (параметры уровня ATM для удаленного узла)	
12 Static Route Setup (настройка статических маршрутов)	12.1 IP Static Route Setup (настройка статических маршрутов IP)	12.1.1 Edit IP Static Route (редактирование статических маршрутов IP)	
	12.3 Bridge Static Route Setup (настройка статических маршрутов в режиме моста)	12.3.1 Edit Bridge Static Route (редактирование статических маршрутов моста)	
15 NAT Setup (настройка NAT)	15.1 Address Mapping Sets (наборы привязки адресов)	15.1.x Address Mapping Rules (правила привязки адресов)	15.1.x.x Address Mapping Rule (правило привязки адресов)
	15.2 NAT Server Sets (наборы серверов для NAT)	15.2.x NAT Server Setup (настройка сервера, находящегося за NAT)	
21 Filter and Firewall Setup (настройка фильтров и межсетевого экрана)	21.1 Filter Set Configuration (настройка набора фильтров)	21.1.x Filter Rules Summary (сводка правил фильтра)	21.1.x.x Generic Filter Rule (универсальное правило фильтра)
			21.1.x.x TCP/IP Filter Rule (правило фильтра TCP/IP)
	21.2 Firewall Setup (настройка межсетевого экрана)		
22 SNMP Configuration (настройка SNMP)			
23 System Password (системный пароль)			

Таблица 90 Общая структура меню SMT (продолжение)

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

21.3 Использование интерфейса SMT

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

Таблица 91 Команды главного меню

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

22

Общая настройка

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

22.1 Задание общих настроек

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

Рис. 140 Меню 1: Общая настройка

```
                    Menu 1 - General Setup

          System Name= P-793H
          Location=
          Contact Person's Name=
          Domain Name=
          Edit Dynamic DNS= No

          Route IP= Yes
          Bridge= No
```

Поля изображенного выше меню описаны в следующей таблице.

Таблица 92 Меню 1: Экран General Setup

ПОЛЕ	ОПИСАНИЕ
System Name	Выберите описательное название, позволяющее идентифицировать оборудование. Рекомендуется ввести "Computer name" ("Имя компьютера") в данном поле. Допустимая длина – до 30 алфавитно-цифровых знаков. Пробелы не допускаются. Вместо них можно использовать тире "–" и символы подчеркивания "_".
Location	Введите описание места размещения P-793H. В этом поле можно ввести до 31 символов или оставить его пустым.
Contact Person's Name	Укажите ФИО лица, которому могут быть направлены вопросы, касающиеся P-793H. В этом поле можно ввести до 30 символов или оставить его пустым.

Таблица 92 Меню 1: Экран General Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
Domain Name	Введите здесь имя домена (если оно известно). Если оставить это поле пустым, ISP может назначить имя домена через DHCP. Можно перейти к меню 24.8 и ввести "sys domain name" ("имя домена системы"), чтобы увидеть текущее имя домена, используемое интернет–центром. Имя домена, введенное пользователем, получает приоритет над назначенным ISP именем домена. Если нужно очистить это поле, просто нажмите пробел, а затем [ENTER].
Edit Dynamic DNS	Нажмите пробел и [ENTER], чтобы выбрать значение **Yes** или **No** (по умолчанию). Выберите **Yes** для настройки раздела **Menu 1.1: Configure Dynamic DNS**, описанного ниже.
Route IP	Выберите **Yes**, чтобы включить в P-793H IP-маршрутизацию. Этот параметр начинает действовать для данного удаленного узла только после того, как на удаленном узле также будет выбрана IP-маршрутизация. См. Настройка удаленного узла в разд. 26.3 на стр. 285. На этом экране необходимо включить **Route IP**, **Bridge** или оба режима. Если режимы **Route IP** и **Bridge** отключены, устройство не будет пересылать трафик между портами LAN и удаленным узлом.
Bridge	Если для параметра **Route IP** выбрано значение **Yes**, выберите в этом поле **Yes**, чтобы разрешить режим моста в P-793H для протоколов, не поддерживаемых IP-маршрутизацией (например, SNA). Если для параметра **Route IP** выбрано значение **No**, выберите **Yes**, чтобы установить мост через P-793H для всех протоколов. Во всех случаях этот параметр становится действителен только после того, как на соответствующем удаленном узле также будет активирован мост. См. Настройка удаленного узла в разд. 26.3 на стр. 285. На этом экране необходимо включить **Route IP**, **Bridge** или оба режима. Если режимы **Route IP** и **Bridge** отключены, устройство не будет пересылать трафик между портами LAN и удаленным узлом.
После завершения работы с данным меню нажмите клавишу [ENTER] в приглашении "Press ENTER to Confirm…" для сохранения конфигурации или клавишу [ESC] для отмены операции в любой момент.	

22.1.1 Настройка динамической DNS

Чтобы настроить DNS для динамических адресов, установите P-793H в режим маршрутизатора в меню 1 или на экране **MAINTENANCE Device Mode**, перейдите в раздел **Menu 1 - General Setup**, затем нажмите пробел, чтобы выбрать **Yes** в поле **Edit Dynamic DNS**. Нажмите [ENTER], чтобы вызвать раздел **Menu 1.1 - Configure Dynamic DNS** (показанный ниже).

Рис. 141 Меню 1.1: Настройка DNS для динамических адресов

```
                    Menu 1.1 - Configure Dynamic DNS

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

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

Таблица 93 Меню 1.1: Настройка DNS для динамических адресов

ПОЛЕ	ОПИСАНИЕ
Service Provider	Это название поставщика услуг динамической DNS.
Active	Нажмите пробел, чтобы выбрать значение **Yes**, а затем нажмите [ENTER], чтобы активировать DNS для динамических адресов.
DDNSType	Если вы используете службу DNS для динамических адресов, нажмите пробел и [ENTER], чтобы выбрать **DynamicDNS**. Выберите **StaticDNS**, если используется DNS для статических адресов. Выберите **CustomDNS**, если используется специализированная служба DNS.
Host 1-3	Введите в этих полях имена хостов (не более трех).
Username	Введите свое имя пользователя.
Password	Введите присвоенный вам пароль.
Enable Wildcard Option	P-793H поддерживает шаблоны DYNDNS. Нажмите пробел и [ENTER] для выбора значения **Yes** или **No**. Это поле не учитывается (**N/A**), если в качестве поставщика услуг используется клиент DDNS.
Enable Off Line Option	Это поле доступно только в том случае, когда в поле **DDNS Type** выбрано значение **CustomDNS**. Нажмите пробел и [ENTER] для выбора значения **Yes**. Когда выбрано значение **Yes (Да)**, трафик http://www.dyndns.org/ перенаправляется на адрес, указанный ранее (обращайтесь по адресу www.dyndns.org для получения дополнительных сведений).
IP Address Update Policy:	Можно выбрать значение **Yes** в любом из полей: **DDNS Server Auto Detect IP Address** (рекомендуемое) или **Use Specified IP Address**, но не в обоих полях. Если поля **DDNS Server Auto Detect IP Address** и **Use Specified IP Address** оба имеют значение **No**, сервер DDNS будет автоматически обновлять IP-адреса для имен хостов P-793H, руководствуясь своим IP-адресом в сети WAN. DDNS не работает с частным IP-адресом. Если значения обоих полей – **No**, то для работы с DDNS устройство P-793H должно иметь глобальный IP-адрес в сети WAN.

Таблица 93 Меню 1.1: Настройка DNS для динамических адресов

ПОЛЕ	ОПИСАНИЕ
DDNS Server Auto Detect IP Address	Этот параметр следует выбирать только в том случае, если между P-793H и сервером DDNS присутствуют один или несколько маршрутизаторов с поддержкой **NAT**. Нажмите пробел, чтобы выбрать **Yes**, затем нажмите [ENTER], чтобы сервер DDNS автоматически определил и запомнил IP-адрес маршрутизатора NAT, которому присвоен глобальный IP- адрес. Примечание. DDNS-сервер может неверно определить IP-адрес, если между P-793H и DDNS-сервером присутствует прокси-сервер HTTP.
Use Specified IP Address	Нажмите пробел для выбора значения **Yes**, а затем нажмите [ENTER] для обновления IP-адреса имени (имен) хоста, чтобы установить значение IP-адреса, указанное ниже. Значение **Yes** следует выбирать только в том случае, если P-793H использует статический глобальный IP-адрес или находится за другим устройством, использующим такой адрес.
Use IP Address	Если в поле **Use Specified IP Address** было выбрано значение **Yes**, введите статический глобальный IP-адрес.
После завершения работы с данным меню нажмите клавишу [ENTER] в приглашении "Press ENTER to Confirm…" для сохранения конфигурации или клавишу [ESC] для отмены операции в любой момент.	

23

Настройка WAN

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

23.1 Настройка WAN

В главном меню введите 2 для открытия меню 2.

Рис. 142 Меню 2: Настройка WAN

```
                        Menu 2 - WAN Setup

        Service Mode= 2wire
        Service Type= Server
          Rate Adaption= Disable                Rate Adaption= N/A
         Transfer Max Rate(Kbps)= 5696        Transfer Max Rate(Kbps)= N/A
          Transfer Min Rate(Kbps)= 192         Transfer Min Rate(Kbps)= N/A
          Standard Mode= ETSI(ANNEX_B)          Standard Mode= N/A
        Wan Backup Setup:
          Check Mechanism = ICMP
          Check WAN IP Address1 = 0.0.0.0
          Check WAN IP Address2 = 0.0.0.0
          Check WAN IP Address3 = 0.0.0.0
            KeepAlive Fail Tolerance = 31
            Recovery Interval(sec) = 3
            ICMP Timeout(sec) = 9677
          Traffic Redirect = No
          Dial Backup = No
```

Поля изображенного выше экрана описаны в следующей таблице.

Таблица 94 Меню 2: Настройка WAN

ПОЛЕ	ОПИСАНИЕ
Service Mode	Нажмите пробел, чтобы указать режим DSL (2- или 4-проводной), используемый P-793H. Выбираемый режим зависит от параметров имеющейся телефонной линии и влияет на максимальную скорость соединения. В двухпроводном режиме максимальная скорость передачи данных составляет 5,69 Мбит/с, а в 4-проводном режиме – 11,38 Мбит/с. Подробное описание режима **2wire-2line** см. в разд. 23.1.1 на стр. 269.
Service Type	Нажмите пробел, чтобы указать, на какой из сторон DSL-соединения (клиентской или серверной) находится P-793H. Выберите **Server**, если данное устройство P-793H является сервером в соединении по схеме "точка-точка". (См. Гл. 4 на стр. 65.) В противном случае выберите **Client**.

Таблица 94 Меню 2: Настройка WAN (продолжение)

ПОЛЕ	ОПИСАНИЕ
Rate Adaption	Это поле доступно для настройки, если в поле **Service Type** указано значение **Server**. Нажмите пробел, чтобы разрешить устройству P-793H согласовывать скорость соединения с другим устройством.
Transfer Max Rate(Kbps)	Это поле активно, если в поле **Service Type** выбрано значение **Server**. Нажмите пробел, чтобы указать максимальную скорость отправки и приема данных для P-793H. Если активирован режим **Rate Adaption**, P-793H будет подстраиваться под скорость удаленного устройства и может превысить указанную скорость.
Transfer Min Rate(Kbps)	Это поле активно, если в поле **Service Type** выбрано значение **Server**. Нажмите пробел, чтобы указать минимальную скорость отправки и приема данных для P-793H. Если активирован режим **Rate Adaption**, P-793H будет подстраиваться под скорость удаленного устройства и может передавать информацию на меньшей скорости.
Standard Mode	Это поле активно, если в поле **Service Type** выбрано значение **Server**. Нажмите пробел, чтобы выбрать режим, используемый P-793H для организации DSL-соединения.
Wan Backup Setup	
Check Mechanism	Выберите метод, которым P-793H будет проверять наличие DSL-соединения. Выберите **DSL Link**, чтобы устройство P-793H проверяло наличие физического соединения с DSLAM. Выберите **ICMP**, чтобы периодически отправлять эхозапросы с P-793H на IP-адреса, заданные в полях **Check WAN IP Address**.
Check WAN IP Address1 Check WAN IP Address2 Check WAN IP Address3	Это поле задает адреса, с помощью которых P-793H будет проверять доступность WAN. Введите IP-адреса от одного до трех близкорасположенных надежных хостов (например, адрес DNS-сервера поставщика услуг). Примечание. Если вы активируете перенаправление трафика или резервирование через коммутируемый доступ, здесь необходимо указать по крайней мере один IP-адрес. При использовании резервирования WAN P-793H периодически отправляет эхозапросы на указанные здесь адреса и при неполучении ответа переключается на резервное соединение с WAN (если оно настроено).
KeepAlive Fail Tolerance	Укажите число раз (рекомендуемое значение – 2), которое P-793H может отправить эхозапросы на указанные в поле **Check WAN IP Address** IP-адреса без получения отклика, прежде чем переключится на резервное соединение с WAN (или на другой вид резервного соединения с WAN).
Recovery Interval(sec)	Когда P-793H 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-793H между проверками доступности сети. Увеличьте интервал, если целевой IP-адрес обрабатывает много трафика.
ICMP Timeout(sec)	Введите число секунд (рекомендуется 3), в течение которых P-793H 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-793H 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	Выберите **Yes**, нажав пробел, затем нажмите [ENTER], чтобы активировать перенаправление трафика и отредактировать ее параметры.
Dial Backup	Выберите **Yes**, нажав пробел, затем нажмите [ENTER], чтобы активировать интерфейс резервирования через коммутируемый доступ и отредактировать его параметры.
После завершения работы с данным меню нажмите клавишу [ENTER] в приглашении "Press ENTER to Confirm…" для сохранения конфигурации или клавишу [ESC] для отмены операции в любой момент.	

23.1.1 Двухпроводной двухлинейный режим

Чтобы перейти на показанный ниже экран, в основном меню выберите 2 для входа в меню 2, затем выберите **2wire-2line** в поле **Service Mode**.

Рис. 143 Меню 2: двухпроводной двухлинейный режим

```
                Menu 2 - WAN Setup

          Service Mode= 2wire-2line
          Service Type= N/A
            Rate Adaption= Disable           Rate Adaption= Enable
            Transfer Max Rate(Kbps)= 4480    Transfer Max Rate(Kbps)= 5696
            Transfer Min Rate(Kbps)= 4480    Transfer Min Rate(Kbps)= 3200
            Standard Mode= ANSI(ANNEX_A)     Standard Mode= ANSI(ANNEX_A)
          Wan Backup Setup:
            Check Mechanism = DSL Link
            Check WAN IP Address1 = 0.0.0.0
            Check WAN IP Address2 = 0.0.0.0
            Check WAN IP Address3 = 0.0.0.0
            KeepAlive Fail Tolerance = 0
            Recovery Interval(sec) = 0
            ICMP Timeout(sec) = 0
            Traffic Redirect = No
            Dial Backup = No
```

Поля изображенного выше экрана описаны в следующей таблице.

Таблица 95 Меню 2: двухпроводной двухлинейный режим

ПОЛЕ	ОПИСАНИЕ
Service Mode	Нажмите пробел, чтобы выбрать режим "2wire-2line", используемый для организации соединения по схеме "точка – две точки". Гл. 4 на стр. 65 содержит более подробное описание этого режима. В двухпроводном двухлинейном режиме скорость передачи данных по каждому из DSL-соединений составляет 5,69 Мбит/с.
Service Type	Работая в двухпроводном двухлинейном режиме, P-793H автоматически принимает на себя функцию сервера.
Rate Adaption	Левое поле относится к соединению DSL 1, а правое – к соединению DSL 2. Нажмите пробел, чтобы разрешить устройству P-793H согласовывать скорость соединения с другим устройством.
Transfer Max Rate(Kbps)	Левое поле относится к соединению DSL 1, а правое – к соединению DSL 2. Нажмите пробел, чтобы указать максимальную скорость отправки и приема данных для P-793H. Если активирован режим **Rate Adaption**, P-793H будет подстраиваться под скорость удаленного устройства и может превысить указанную скорость.
Transfer Min Rate(Kbps)	Левое поле относится к соединению DSL 1, а правое – к соединению DSL 2. Нажмите пробел, чтобы указать минимальную скорость отправки и приема данных для P-793H. Если активирован режим **Rate Adaption**, P-793H будет подстраиваться под скорость удаленного устройства и может передавать информацию на меньшей скорости.
Standard Mode	Левое поле относится к соединению DSL 1, а правое – к соединению DSL 2. Нажмите пробел, чтобы выбрать режим, используемый P-793H для организации DSL-соединения.
Wan Backup Setup	

Таблица 95 Меню 2: двухпроводной двухлинейный режим (продолжение)

ПОЛЕ	ОПИСАНИЕ
Check Mechanism	Выберите метод, которым P-793H будет проверять наличие DSL-соединения. Выберите **DSL Link**, чтобы устройство P-793H проверяло наличие физического соединения с DSLAM. Выберите **ICMP**, чтобы периодически отправлять эхозапросы с P-793H на IP-адреса, заданные в полях **Check WAN IP Address**.
Check WAN IP Address1 Check WAN IP Address2 Check WAN IP Address3	Это поле задает адреса, с помощью которых P-793H будет проверять доступность WAN. Введите IP-адреса от одного до трех близкорасположенных надежных хостов (например, адрес DNS-сервера поставщика услуг). Примечание. Если вы активируете перенаправление трафика или резервирование через коммутируемый доступ, здесь необходимо указать по крайней мере один IP-адрес. При использовании резервирования WAN P-793H периодически отправляет эхозапросы на указанные здесь адреса и при неполучении ответа переключается на резервное соединение с WAN (если оно настроено).
KeepAlive Fail Tolerance	Укажите число раз (рекомендуемое значение – 2), которое P-793H может отправить эхозапросы на указанные в поле **Check WAN IP Address** IP-адреса без получения отклика, прежде чем переключится на резервное соединение с WAN (или на другой вид резервного соединения с WAN).
Recovery Interval(sec)	Когда P-793H 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-793H между проверками доступности сети. Увеличьте интервал, если целевой IP-адрес обрабатывает много трафика.
ICMP Timeout(sec)	Введите число секунд (рекомендуется 3), в течение которых P-793H 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-793H 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	Эта функция в двухпроводном двухлинейном режиме отключена.
Dial Backup	Эта функция в двухпроводном двухлинейном режиме отключена.
После завершения работы с данным меню нажмите клавишу [ENTER] в приглашении "Press ENTER to Confirm…" для сохранения конфигурации или клавишу [ESC] для отмены операции в любой момент.	

23.2 Настройка перенаправления трафика

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

Рис. 144 Меню 2.1: Настройка перенаправления трафика

```
                Menu 2.1 - Traffic Redirect Setup

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

Поля изображенного выше меню описаны в следующей таблице.

Таблица 96 Меню 2.1: Настройка перенаправления трафика

ПОЛЕ	ОПИСАНИЕ
Active	Это поле включает (**Yes**) или отключает (**No**) функцию перенаправления трафика.
Configuration	
Backup Gateway IP Address	Введите IP-адрес резервного межсетевого шлюза в десятичном виде через точку. P-793H автоматически переадресует трафик на этот IP-адрес, если разрывается соединение P-793H с Интернетом.
Metric	Это поле задает приоритет маршрута среди других маршрутов, используемых P-793H. Метрика обозначает "стоимость" передачи пакета. Маршрутизатор определяет оптимальный маршрут передачи, выбирая путь с самой низкой "стоимостью". Для маршрутизации на основе RIP мерой стоимости является число переходов между сетевыми сегментами, минимальное значение – 1 – соответствует напрямую подключенным сетям. Значение метрики должно быть в диапазоне от 1 до 15; значения больше 15 означают, что соединение не функционирует. Чем меньше значение, тем ниже "стоимость".
После завершения работы с данным меню нажмите клавишу [ENTER] в приглашении "Press ENTER to Confirm…" для сохранения конфигурации или клавишу [ESC] для отмены операции в любой момент.	

23.3 Интерфейс резервирования через коммутируемый доступ

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

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

23.4 Настройка резервирования через коммутируемый доступ в меню 2

В главном меню введите 2 для открытия меню 2.

Рис. 145 Меню 2.2: Настройка резервирования через коммутируемый доступ

```
                    2.2 - Dial Backup Setup

                  Dial-Backup:
                    Active= No
                    Port Speed= 115200

                  AT Command String:
                    Init= at&fs0=0

                    Edit Advanced Setup= No
```

Поля изображенного выше меню описаны в следующей таблице.

Таблица 97 Меню 2.2: Настройка резервирования через коммутируемый доступ

ПОЛЕ	ОПИСАНИЕ
Dial-Backup:	
Active	Это поле включает (**Yes**) или отключает (**No**) функцию резервирования через коммутируемый доступ.
Port Speed	Нажмите пробел и [ENTER], чтобы выбрать скорость соединения между портом резервирования через коммутируемый доступ и внешним устройством. Доступны следующие скорости: **9600**, **19200**, **38400**, **57600**, **115200** или **230400** бит/с.
AT Command String:	
Init	Введите AT-строку инициализации устройства, используемого для доступа в WAN. Описание конкретных AT-команд см. в документации на устройство, подключаемое к порту резервирования.
Edit Advanced Setup	Чтобы отредактировать расширенные параметры порта резервирования через коммутируемый доступ, подведите курсор к этому полю, нажмите пробел, чтобы выбрать **Yes**, затем нажмите [ENTER] для входа в раздел **Menu 2.1 - Advanced Setup**.
После завершения работы с данным меню нажмите клавишу [ENTER] в приглашении "Press ENTER to Confirm…" для сохранения конфигурации или клавишу [ESC] для отмены операции в любой момент.	

23.5 Расширенная настройка резервирования через коммутируемый доступ

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

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

Рис. 146 Меню 2.2.1: Расширенная настройка резервирования через коммутируемый доступ

```
                  Menu 2.2.1 - Advanced Dial Backup Setup

AT Command Strings:                    Call Control:
  Dial= atd                              Dial Timeout(sec)= 60
  Drop= ~~+++~~ath                       Retry Count= 0
  Answer= ata                            Retry Interval(sec)= N/A
                                         Drop Timeout(sec)= 20
Drop DTR When Hang Up= No                Call Back Delay(sec)= 15

AT Response Strings:
  CLID= NMBR =
  Called Id=
  Speed= CONNECT
```

Поля изображенного выше меню описаны в следующей таблице.

Таблица 98 Меню 2.2.1: Расширенная настройка резервирования через коммутируемый доступ

ПОЛЕ	ОПИСАНИЕ
AT Command Strings:	
Dial	Введите AT-команду для осуществления вызова.
Drop	Введите AT-команду для завершения вызова. Символ "~" кодирует 1-секундную задержку. Например, для модемов с медленным откликом можно использовать строку "~~~+++~~ath".
Answer	Введите AT-команду для ответа на входящий вызов.
Drop DTR When Hang Up	Нажмите пробел, чтобы выбрать значение **Yes** (да) или **No** (нет). Когда выбрано значение **Yes** (действующее по умолчанию), после отправки строки "AT Command String: Drop" осуществляется сброс сигнала DTR.
AT Response Strings:	
CLID (идентификация вызывающей линии)	Введите ключевое слово, после которого в AT-строке отклика приводится CLID (идентификация вызывающей линии). Это позволяет P-793H извлекать CLID из AT-строки доступа, полученной от устройства, через которое осуществляется доступ в WAN. Идентификатор CLID применяется для CLID-аутентификации.
Called Id	Введите ключевое слово, которое предшествует набираемому номеру.
Speed	Введите ключевое слово, которое предшествует скорости соединения.
Call Control	
Dial Timeout (sec)	Укажите число секунд, в течение которых P-793H будет ожидать установления исходящего соединения перед прекращением операции. P-793H сообщает об истечении времени ожидания и прекращает попытку установления исходящего соединения, если его не удалось установить за указанное время.
Retry Count	Укажите число повторных попыток набора номера, которые P-793H будет предпринимать при обнаружении сигнала "занято" или при отсутствии ответа удаленной стороны, прежде чем номер будет занесен в черный список.

Таблица 98 Меню 2.2.1: Расширенная настройка резервирования через коммутируемый доступ (продолжение)

ПОЛЕ	ОПИСАНИЕ
Retry Interval (sec)	Укажите продолжительность паузы (в секундах), которую P-793H будет выдерживать между попытками повторного набора номера. Эта пауза действует до занесения номера в черный список.
Drop Timeout (sec)	Введите число секунд, по истечении которых P-793H сбросит сигнал DTR, если не будет получено явное подтверждение разъединения.
Call Back Delay (sec)	Укажите длительность паузы (в секундах), которую P-793H будет выдерживать между завершением запроса встречного вызова (callback) и началом соответствующего встречного вызова.

24

Настройка LAN

Этот раздел меню служит для применения фильтров LAN, настройки параметров DHCP и TCP/IP для сети LAN, а также активации и деактивации VLAN для каждого порта LAN.

24.1 Вход в меню LAN

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

Рис. 147 Меню 3: Настройка LAN

```
                        Menu 3 - LAN Setup

                1. LAN Port Filter Setup
                2. TCP/IP and DHCP Setup



                6. Port Based VLAN Setup
```

24.2 Меню LAN Port Filter Setup

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

Рис. 148 Меню 3.1: Настройка фильтров для порта LAN

```
                  Menu 3.1 - LAN Port Filter Setup

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

24.3 Меню TCP/IP and DHCP Setup

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

Рис. 149 Меню 3.2: Настройка TCP/IP и DHCP для Ethernet

```
                Menu 3.2 - TCP/IP and DHCP Setup

DHCP Setup
  DHCP= Server
  Client IP Pool Starting Address= 192.168.1.33
  Size of Client IP Pool= 32
  Primary DNS Server= 0.0.0.0
  Secondary DNS Server= 0.0.0.0
  Remote DHCP Server= N/A
TCP/IP Setup (Íàñòðîéêà TCP/IP):
  IP Address= 192.168.1.1
  IP Subnet Mask= 255.255.255.0
  RIP Direction= Both
    Version= RIP-2B
  Multicast= IGMP-v2
  IP Policies=
  Edit IP Alias= No
```

Для настройки этих полей руководствуйтесь следующей таблицей.

Таблица 99 Меню 3.2: Настройка TCP/IP и DHCP для Ethernet

ПОЛЕ	ОПИСАНИЕ
DHCP Setup	
DHCP	Это поле позволяет включить/выключить DHCP-сервер. Если выбрано значение **Server**, P-793H будет работать в режиме DHCP-сервера. Потребуется настроить остальные поля в этом разделе, за исключением **Remote DHCP Server**. При выборе значения **Relay** P-793H действует как заменитель DHCP-сервера и выполняет обмен запросами и откликами между удаленным сервером и клиентами. В этом случае необходимо указать удаленный DHCP-сервер (**Remote DHCP Server**). При выборе значения **None** сервер будет выключен.
Client IP Pool Starting Address:	В этом поле указывается первый адрес в непрерывном пуле IP-адресов.
Size of Client IP Pool	В этом поле указывается размер или общая численность пула IP-адресов.

Таблица 99 Меню 3.2: Настройка TCP/IP и DHCP для Ethernet (продолжение)

ПОЛЕ	ОПИСАНИЕ
Primary DNS Server Secondary DNS Server	P-793H сообщает IP-адреса DNS-серверов в указанном порядке DHCP-клиентам. Выберите **From ISP**, если поставщик услуг Интернета динамически назначает параметры DNS-сервера (а также IP-адрес P-793H в сети WAN). В поле **IP Address (IP-адрес)** внизу отображается IP-адрес DNS-сервера (только для чтения), назначаемый оператором. Выберите **User-Defined**, если вам известен IP-адрес DNS-сервера. Введите IP-адрес DNS-сервера в поле **IP Address** внизу. Если выбрано значение **User-Defined (Определяется пользователем)**, но значение IP-адреса остается равным 0.0.0.0, **User-Defined (Определяется пользователем)** заменяется значением **None (Нет)** после сохранения изменений. Если во втором случае выбрана опция **User-Defined (Определяется пользователем)** и введен тот же IP-адрес, вторая опция **User-Defined (Определяется пользователем)** приобретает значение **None (Нет)** после сохранения изменений. Выберите **DNS Relay**, чтобы использовать P-793H в режиме прокси-сервера для DNS. IP-адрес P-793H в сети LAN отображается в расположенном ниже поле **IP Address** (это поле недоступно для редактирования). P-793H сообщает DHCP-клиентам в локальной сети, что само устройство P-793H является DNS-сервером. Когда компьютер в локальной сети отправляет запрос DNS на P-793H, P-793H переадресует запрос DNS-серверу, настроенному для P-793H в меню 1, и возвращает отклик компьютеру. Режим **DNS Relay** можно выбрать только для одного из трех серверов; режим **DNS Relay**, выбранный для второго или третьего сервера, изменяется на **None** после сохранения изменений. Выберите **None**, если DNS-серверы настраивать не требуется. Если настройка DNS-сервера не выполняется, для получения доступа к машине необходимо знать ее IP-адрес.
Remote DHCP Server	Если в поле **DHCP** выбран режим **Relay**, введите здесь IP-адрес фактического удаленного DHCP-сервера.
TCP/IP Setup:	
IP Address	Введите IP-адрес P-793H в сети LAN в десятичном виде через точку.
IP Subnet Mask	P-793H автоматически вычисляет маску подсети на основе назначаемого пользователем IP-адреса. Если вам не требуется деление на подсети, используйте маску подсети, рассчитанную P-793H.
RIP Direction	Нажмите пробел, а затем [ENTER] для выбора направления RIP. Возможны следующие значения: **Both (Оба)**, **In Only (Только внутри)**, **Out Only (Только снаружи)** или **None (Нет)**.
Version	Нажмите пробел и [ENTER] для выбора версии RIP. Возможны следующие значения: **RIP-1**, **RIP-2B** или **RIP-2M**.
Multicast	IGMP (Широковещательный протокол взаимодействия групп в Интернете) – протокол уровня сессии, используемый для установки членства в группе многоадресной рассылки. P-793H поддерживает протокол IGMP версии 1 (**IGMP-v1**) и версии 2 (**IGMP-v2**). Нажмите пробел и [ENTER] для включения многоадресной IP-рассылки или выберите **None** (по умолчанию) для ее отключения.
IP Policies	Для данного удаленного узла могут применяться до четырех политик маршрутизации. Политики должны быть предварительно настроены в меню 25. Подробное описание политик маршрутизации см. в Гл. 36 на стр. 367.
Edit IP Alias	P-793H поддерживает до трех логических интерфейсов LAN на одном физическом интерфейсе Ethernet, при этом P-793H будет выступать в качестве межсетевого шлюза для каждой сети LAN. Чтобы войти в меню 3.2.1, выберите **Yes**, нажав пробел, а затем нажмите [ENTER].
После завершения работы с данным меню нажмите клавишу [ENTER] в приглашении [Press ENTER to Confirm…] для сохранения конфигурации или клавишу [ESC] для отмены операции в любой момент.	

24.4 Совмещение IP-адресов в локальной сети

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

Рис. 150 Меню 3.2.1: Настройка совмещения IP-адресов

```
                Menu 3.2.1 - IP Alias Setup

            IP Alias 1= No
              IP Address= N/A
              IP Subnet Mask= N/A
              RIP Direction= N/A
              Version= N/A
              Incoming protocol filters= N/A
              Outgoing protocol filters= N/A
            IP Alias 2= No
              IP Address= N/A
              IP Subnet Mask= N/A
              RIP Direction= N/A
              Version= N/A
              Incoming protocol filters= N/A
              Outgoing protocol filters= N/A
```

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

Таблица 100 Меню 3.2.1: Настройка совмещения IP-адресов

ПОЛЕ	ОПИСАНИЕ
IP Alias 1, 2	Выберите **Yes**, чтобы настроить сеть LAN для P-793H.
IP Address	Введите IP-адрес вашего P-793H в десятичном виде через точку.
IP Subnet Mask	P-793H автоматически вычисляет маску подсети на основе назначаемого пользователем IP-адреса. Если вам не требуется деление на подсети, используйте маску подсети, рассчитанную P-793H.
RIP Direction	Нажмите пробел и [ENTER] для выбора направления RIP. Возможны следующие значения: **Both** (оба), **In Only** (только вход), **Out Only** (только выход) или **None** (нет).
Version	Нажмите пробел и [ENTER] для выбора версии RIP. Возможны следующие значения: **RIP-1**, **RIP-2B** или **RIP-2M**.
Incoming protocol filters	Укажите наборы фильтров, применяемые ко входящему трафику между данным узлом и P-793H.
Outgoing protocol filters	Укажите наборы фильтров, применяемые к исходящему трафику между данным узлом и P-793H.
После завершения работы с данным меню нажмите клавишу [ENTER] в приглашении [Press ENTER to Confirm…] для сохранения конфигурации или клавишу [ESC] для отмены операции в любой момент.	

24.4.1 Настройка VLAN на основе портов

Меню 3.6 разрешает или запрещает устройству P-793H пересылать трафик 2-го уровня (уровня MAC-адресов) между отдельными портами LAN. Например, если к портам LAN 1 и 2 подключены сети двух разных отделов, можно запретить P-793H распространять широковещательный трафик из одной сети в другую. В этом случае необходимо отключить соединение между двумя портами. После этого отделы смогут взаимодействовать только на уровне IP-адресов, но не MAC-адресов.

В главном меню наберите цифру 3**,** чтобы войти в меню **Menu 3 - LAN Setup**, затем выберите подменю 6.

Рис. 151 Меню 3.6: Настройка VLAN на основе портов

```
                Menu 3.6 - Port Based VLAN Setup

                  1    2    3    4
            1     -    Yes  Yes  Yes
            2          -    Yes  Yes
            3               -    Yes
            4                    -
```

Нажмите пробел, чтобы выбрать **Yes** (Да) или **No** (Нет) для разрешения или блокирования трафика 2-го уровня между отдельными парами портов.

25

Настройка доступа к Интернету

Это меню служит для настройки подключения к Интернету. Чтобы настроить доступ к Интернету в P-793H, используйте информацию, полученную от поставщика услуг Интернета, а также указания, приведенные в этой главе. Обращайтесь к своему оператору, чтобы определить, какой тип инкапсуляции следует использовать.

25.1 Настройка доступа к Интернету

Введите 4 в главном меню.

Рис. 152 Меню 4: Настройка доступа к Интернету

```
                Menu 4 - Internet Access Setup

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

Поля изображенного выше меню описаны в следующей таблице.

Таблица 101 Меню 4: Настройка доступа к Интернету

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

Таблица 101 Меню 4: Настройка доступа к Интернету (продолжение)

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

Таблица 101 Меню 4: Настройка доступа к Интернету (продолжение)

ПОЛЕ	ОПИСАНИЕ
Network Address Translation	Трансляция сетевых адресов (NAT) обеспечивает преобразование IP-адреса, используемого в пределах одной сети (например, частного IP-адреса, используемого в локальной сети) в другой IP-адрес, известный в пределах другой сети (например, открытый IP-адрес, используемый в Интернете). Выберите **None (Нет)**, чтобы отключить NAT. Выберите **SUA Only (Только SUA)**, если существует 1 общедоступный IP-адрес. SUA (Учетная запись одного пользователя) является подмножеством NAT, поддерживающим 2 типа привязки: **Many-to-One (Множество – один)** и **Server (Сервер)**. Выберите **Full Feature (Полный набор возможностей)**, если существует несколько общедоступных IP-адресов. Типы привязки **Full Feature (Полный набор возможностей)** включают: **One-to-One (Один – один)**, **Many-to-One (Множество – один)** (SUA/PAT), **Many-to-Many Overload (Перегрузка множество – множество)**, **Many- One-to-One (Множество – один – один)** и **Server (Сервер)**. При выборе опции **Full Feature** необходимо настроить как минимум один набор привязки адресов. Подробное описание функции трансляции сетевых адресов см. в Гл. 7 на стр. 111.
Address Mapping Set	Это поле доступно в том случае, если в поле **Network Address Translation** выбрано значение **Full Feature**. Введите номер набора привязки адресов, который требуется использовать для данного соединения с Интернетом.
После завершения работы с данным меню нажмите клавишу [ENTER] в приглашении "Press ENTER to Confirm…" для сохранения конфигурации или клавишу [ESC] для отмены операции в любой момент.	

26

Настройка удаленного узла

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

26.1 Введение в настройку удаленного узла

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

26.2 Настройка удаленного узла

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

Рис. 153 Меню 11: Настройка удаленного узла

```
                    Menu 11 - Remote Node Setup

                1. MyISP (ISP, SUA)
                2. _________
                3. _________
                4. _________
                5. _________
                6. _________
                7. _________
                8. ChangeMe (BACKUP_ISP, SUA)

        Enter Node # to Edit:
```

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

26.3 Профиль удаленного узла

Настройка удаленных узлов 1 – 7 описана ниже.

Рис. 154 Меню 11.1: Профиль удаленного узла (узлы 1 – 7)

```
                    Menu 11.1 - Remote Node Profile

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

Encapsulation= PPPoE                    Edit IP/Bridge= No
Multiplexing= LLC-based                 Edit ATM Options= No
Service Name=                           Edit Advance Options= No
Incoming:                               Telco Option:
  Rem Login=                              Allocated Budget(min)= 0
  Rem Password= ********                  Period(hr)= 0
Outgoing:                                 Schedule Sets=
  My Login=                               Nailed-Up Connection= No
  My Password= ********                 Session Options:
  Authen= CHAP/PAP                        Edit Filter Sets= No
Line=1                                    Idle Timeout(sec)= 0
```

Поля изображенного выше экрана описаны в следующей таблице.

Таблица 102 Меню 11.1: Профиль удаленного узла (узлы 1 – 7)

ПОЛЕ	ОПИСАНИЕ
Rem Node Name	Введите название поставщика услуг Интернета.
Active	Укажите, используется ли данное соединение с Интернетом.
Encapsulation	Выберите тип инкапсуляции, используемый поставщиком услуг Интернета.
Multiplexing	Выберите тип мультиплексирования, используемый поставщиком услуг Интернета, из раскрывающегося списка. Варианты выбора: **VC** или **LLC**.
Service Name	(Только для инкапсуляции PPPoE). Введите название службы, предоставленное поставщиком услуг Интернета. Если поставщик услуг Интернета не предоставил соответствующей информации, оставьте это поле пустым.
Incoming	Этот раздел доступен только для инкапсуляции PPPoA/PPPoE.
Rem Login	Введите имя пользователя, которое будет использоваться дистанционным узлом при вызове вашего устройства P-793H. Для аутентификации узла будут использоваться указанное имя пользователя и пароль из поля **Rem Password**.
Rem Password	Введите пароль, который будет использоваться дистанционным узлом при вызове вашего устройства P-793H.
Outgoing	Этот раздел доступен только для инкапсуляции PPPoA/PPPoE.
My Login	Введите имя пользователя, предоставленное поставщиком услуг Интернета.
My Password	Введите пароль, предоставленный поставщиком услуг Интернета.
Retype to Confirm	Введите пароль повторно.
Authen	Это поле доступно в том случае, если в поле **Encapsulation** выбран режим инкапсуляции **PPPoE**. Выберите тип аутентификации, используемый поставщиком услуг Интернета. Чтобы разрешить P-793H использовать оба варианта аутентификации, выберите **CHAP/PAP**.
Line	Выберите DSL-соединение, по которому устройство ZyXEL будет пересылать исходящий трафик.

Таблица 102 Меню 11.1: Профиль удаленного узла (узлы 1 – 7) (продолжение)

ПОЛЕ	ОПИСАНИЕ
Route	Нажмите пробел и [ENTER], чтобы выбрать параметр **IP**, разрешающий IP-маршрутизацию через данный удаленный узел. Этот параметр становится действителен только после того, как в устройстве P-793H также будет активирована IP-маршрутизация. См. Общая настройка в разд. 22.1 на стр. 263. На этом экране необходимо включить **Route IP**, **Bridge** или оба режима. Если режимы **Route IP** и **Bridge** отключены, устройство не будет пересылать трафик между портами LAN и удаленным узлом.
Bridge	Если для параметра **Route** выбрано значение **IP**, выберите в этом поле **Yes**, чтобы установить мост с этим удаленным узлом для протоколов, не поддерживаемых IP-маршрутизацией (например, SNA). Если для параметра **Route** выбрано значение **None**, выберите в этом поле **Yes**, чтобы установить мост с этим удаленным узлом для всех протоколов. Во всех случаях этот параметр становится действителен только после того, как в устройстве P-793H также будет активирован мост. См. Общая настройка в разд. 22.1 на стр. 263. На этом экране необходимо включить **Route IP**, **Bridge** или оба режима. Если режимы **Route IP** и **Bridge** отключены, устройство не будет пересылать трафик между портами LAN и удаленным узлом.
Edit IP/Bridge	Это поле доступно в том случае, если параметр **Route** установлен в значение **IP**. Для задания IP-адреса в сети WAN и дополнительных параметров порта WAN нажмите пробел, чтобы выбрать **Yes**, затем нажмите [ENTER]. Появится меню 11.3.
Edit ATM Options	Это поле доступно в том случае, если параметр **Route** установлен в значение **IP**. Для редактирования параметров виртуального канала и ATM QoS нажмите пробел, чтобы выбрать **Yes**, затем нажмите [ENTER]. Появится меню 11.6.
Edit Advance Options	Это поле отображается при редактировании удаленного узла 1 и доступно только для соединений PPPoE. Для задания дополнительных параметров подключения к Интернету нажмите пробел, чтобы выбрать **Yes**, затем нажмите [ENTER]. Появится меню 11.8.
Telco Option	Этот раздел доступен только для инкапсуляции PPPoA / PPPoE.
Allocated Budget(min)	Введите максимальную продолжительность каждого вызова (в минутах). Чтобы снять ограничение на продолжительность вызова, введите 0. Поле **Period** позволяет ограничить суммарную продолжительность исходящего вызова с P-793H. Если общее время исходящих вызовов превышает лимит, текущий вызов отбрасывается и все последующие исходящие вызовы блокируются.
Period(hr)	Введите количество часов, по истечении которого параметр **Allocated Budget** будет сбрасываться. Например, если в течение каждого часа под исходящие вызовы выделяется 30 минут, установите параметр **Allocated Budget** равным 30, а в этом поле введите 1.
Schedule Sets	Введите наборы расписаний, действующие для данного соединения.
Nailed-Up Connection	Выберите этот флажок, чтобы автоматически соединять P-793H с поставщиком услуг Интернета при включении питания и никогда не разрывать соединение. Не рекомендуется использовать этот режим, если у поставщика услуг Интернета действует повременная оплата.
Session Options	
Edit Filter Sets	Для задания дополнительных наборов входных и выходных фильтров на порту WAN нажмите пробел, чтобы выбрать **Yes**, затем нажмите [ENTER]. Появится меню 11.5.
Idle Timeout (sec)	Введите число секунд, по истечении которых P-793H отключается от поставщика услуг Интернета, если за это время трафик отсутствовал. Допустимые интервалы – от 10 до 9999 секунд.

Ниже описана настройка удаленного узла 8 – 7 для резервирования соединения по коммутируемой линии.

Рис. 155 Меню 11.1: Профиль удаленного узла (узел 8)

```
                Menu 11.1 - Remote Node Profile (Backup ISP)

    Rem Node Name= ?                        Edit PPP Options= No
    Active= Yes                             Rem IP Addr= ?
                                            Edit IP= No
    Outgoing:                               Edit Script Options= No
      My Login=
      My Password= ********                 Telco Option:
      Authen= CHAP/PAP                        Allocated Budget(min)= 0
      Pri Phone #= ?                            Period(hr)= 0
      Sec Phone #=                          Nailed-Up Connection= No

                                            Session Options:
                                              Edit Filter Sets= No
                                              Idle Timeout(sec)= 100
```

Поля изображенного выше экрана описаны в следующей таблице.

Таблица 103 Меню 11.1: Профиль удаленного узла (узел 8)

ПОЛЕ	ОПИСАНИЕ
Rem Node Name	Введите название поставщика услуг Интернета.
Active	Укажите, используется ли данное соединение с Интернетом.
Outgoing	Этот раздел доступен только для инкапсуляции PPPoA / PPPoE.
My Login	Введите имя пользователя, предоставленное поставщиком услуг Интернета.
My Password	Введите пароль, предоставленный поставщиком услуг Интернета.
Retype to Confirm	Введите пароль повторно.
Authen	Это поле доступно в том случае, если в поле **Encapsulation** выбран режим инкапсуляции **PPPoE**. Выберите тип аутентификации, используемый поставщиком услуг Интернета. Чтобы разрешить P-793H использовать оба варианта аутентификации, выберите **CHAP/PAP**.
Pri Phone # Sec Phone #	Введите один или два телефонных номера удаленного узла. В тех случаях, когда основной номер (Primary Phone) занят или не отвечает, P-793H набирает запасной номер (Secondary Phone), если он указан. В некоторых телефонных сетях для вызова местных номеров перед ними необходимо набирать решетку (#). В этом случае перед номером нужно указать знак #.
Edit PPP Options	Для редактирования параметров PPP резервного поставщика услуг Интернета нажмите пробел, чтобы выбрать **Yes**, затем нажмите [ENTER]. Появится меню 11.2.
Rem IP Addr	В этом поле отображается тип маршрутизации, используемый устройством P-793H.
Edit IP/Bridge	Это поле доступно в том случае, если параметр **Route** установлен в значение **IP**. Для задания IP-адреса в сети WAN и дополнительных параметров порта WAN нажмите пробел, чтобы выбрать **Yes**, затем нажмите [ENTER]. Появится меню 11.3.
Edit ATM Options	Это поле доступно в том случае, если параметр **Route** установлен в значение **IP**. Для редактирования параметров виртуального канала и ATM QoS нажмите пробел, чтобы выбрать **Yes**, затем нажмите [ENTER]. Появится меню 11.1.6.
Edit Advance Options	Это поле отображается при редактировании удаленного узла 1 и доступно только для соединений PPPoE. Для задания дополнительных параметров подключения к Интернету нажмите пробел, чтобы выбрать **Yes**, затем нажмите [ENTER]. Появится меню 11.1.8.

Таблица 103 Меню 11.1: Профиль удаленного узла (узел 8) (продолжение)

ПОЛЕ	ОПИСАНИЕ
Telco Option	Этот раздел доступен только для инкапсуляции PPPoA / PPPoE.
Allocated Budget(min)	Введите максимальную продолжительность каждого вызова (в минутах). Чтобы снять ограничение на продолжительность вызова, введите 0. Поле **Period** позволяет ограничить суммарную продолжительность исходящего вызова с P-793H. Если общее время исходящих вызовов превышает лимит, текущий вызов отбрасывается и все последующие исходящие вызовы блокируются.
Period(hr)	Введите количество часов, по истечении которых параметр **Allocated Budget** будет сбрасываться. Например, если в течение каждого часа под исходящие вызовы выделяется 30 минут, установите параметр **Allocated Budget** равным 30, а в этом поле введите 1.
Schedule Sets	Введите наборы расписаний, действующие для данного соединения.
Nailed-Up Connection	Выберите этот флажок, чтобы автоматически соединять P-793H с поставщиком услуг Интернета при включении питания и никогда не разрывать соединение. Не рекомендуется использовать этот режим, если у поставщика услуг Интернета действует повременная оплата.
Session Options	
Edit Filter Sets	Для задания дополнительных наборов входных и выходных фильтров на порту WAN нажмите пробел, чтобы выбрать **Yes**, затем нажмите [ENTER]. Появится меню 11.1.4.
Idle Timeout (sec)	Введите число секунд, по истечении которых P-793H отключается от поставщика услуг Интернета, если за это время трафик отсутствовал. Допустимые интервалы – от 10 до 9999 секунд.

26.4 Параметры сетевого уровня для удаленного узла

Подведите курсор к полю **Edit IP/Bridge** в меню 11.1, затем нажмите пробел, чтобы выбрать **Yes**. Нажмите клавишу [ENTER] для открытия раздела **Menu 11.3 - Remote Node Network Layer Options**.

Рис. 156 Меню 11.3: Параметры сетевого уровня удаленного узла

```
                Menu 11.3 - Remote Node Network Layer Options

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

Поля изображенного выше меню описаны в следующей таблице.

Таблица 104 Меню 11.3: Параметры сетевого уровня для удаленного узла

ПОЛЕ	ОПИСАНИЕ
IP Address Assignment	Если поставщик услуг Интернета не присвоил вам фиксированный (статический) IP-адрес, выберите **Dynamic**. Если поставщик услуг Интернета выделил вам фиксированный (статический) IP-адрес, выберите **Static**. Следующие три поля недоступны, если был выбран динамический адрес (**Dynamic**).
	Эти поля появляются, если в меню 11 для параметра **Encapsulation** выбрано значение **Ethernet**.
IP Address	Введите фиксированный (статический) IP-адрес, предоставленный поставщиком услуг Интернета.
IP Subnet Mask	Введите маску подсети, предоставленную поставщиком услуг Интернета.
Gateway IP Addr	Введите IP-адрес шлюза, предоставленный поставщиком услуг Интернета.
	Эти поля появляются, если в меню 11 для параметра **Encapsulation** выбрано значение **PPPoE**.
Rem IP Addr	Введите IP-адрес удаленного компьютера, с которым соединяется P-793H.
Rem Subnet Mask	Введите маску подсети удаленного компьютера, с которым соединяется P-793H.
My WAN Addr	Введите фиксированный (статический) IP-адрес, предоставленный поставщиком услуг Интернета.
NAT	Если использовать переадресацию портов, триггерные порты или NAT не предполагается, выберите **None**. Если вы планируете использовать некоторые из этих функций, но для P-793H выделен только один глобальный IP-адрес в сети WAN, выберите **SUA Only**. Если вы планируете использовать некоторые из этих функций, и для P-793H выделено несколько глобальных IP-адресов в сети WAN, выберите **Full Feature**.
Address Mapping Set	Это поле доступно в том случае, если параметр **NAT** установлен в значение **Full Feature**. Укажите набор привязки адресов, который должен использоваться для этого удаленного узла.
Metric	Это поле задает приоритет маршрута среди других маршрутов, используемых P-793H. Метрика обозначает "стоимость" передачи пакета. Маршрутизатор определяет оптимальный маршрут передачи, выбирая путь с самой низкой "стоимостью". Для маршрутизации на основе RIP мерой стоимости является число переходов между сетевыми сегментами, минимальное значение – 1 – соответствует напрямую подключенным сетям. Значение метрики должно быть в диапазоне от 1 до 15; значения больше 15 означают, что соединение не функционирует. Чем меньше значение, тем ниже "стоимость".
Private (Частный)	Это поле используется протоколом RIP и указывает, будет ли P-793H включать данный маршрут к конкретному удаленному узлу в широковещательную рассылку RIP. Если выбрано **Yes**, маршрут не включается в широковещательную рассылку RIP. Если выбрано **No**, маршрут к данному удаленному узлу сообщается другим хостам в широковещательных рассылках RIP. Обычно для этого поля будет приемлемым значение по умолчанию.

Таблица 104 Меню 11.3: Параметры сетевого уровня для удаленного узла

ПОЛЕ	ОПИСАНИЕ
RIP Direction	Это поле определяет состав сведений о маршрутизации, принимаемых и отправляемых P-793H по данному соединению. **None** - P-793H не отправляет и не принимает сведения о маршрутизации по данному соединению. **Both** - P-793H отправляет и принимает сведения о маршрутизации по данному соединению. **In Only** - P-793H использует данное соединение только для приема сведений о маршрутизации. **Out Only** - P-793H использует данное соединение только для отправки сведений о маршрутизации.
Version	Выберите версию протокола RIP, используемую P-793H при отправке или приеме сведений о подсети. **RIP-1** - P-793H для обмена сведениями о маршрутизации использует RIPv1. **RIP-2B** - P-793H для обмена сведениями о маршрутизации использует широковещательные сообщения RIPv2. **RIP-2M** - P-793H для обмена сведениями о маршрутизации использует многоадресные сообщения RIPv2.
Multicast	Для использования **RIP-2M** включать многоадресную рассылку не требуется. (См. описание параметра **RIP Version**.) Выберите версию протокола IGMP, используемую P-793H для реализации многоадресной рассылки на данном порту. При многоадресной рассылке пакеты отправляются только определенной группе компьютеров, что отличает этот способ от одноадресной (отправка пакетов на один компьютер) и широковещательной (отправка пакетов всем компьютерам) рассылок. **None** – P-793H не поддерживает многоадресную рассылку. **IGMP-v1** – P-793H поддерживает IGMP версии 1. **IGMP-v2** – P-793H поддерживает IGMP версии 2. Многоадресная рассылка может улучшить общую производительность сети ценой большей вычислительной нагрузки и повышенного объема трафика. Кроме того, используемая версия IGMP должна поддерживаться всеми компьютерами в сети.
IP Policies	Для данного удаленного узла могут применяться до четырех политик маршрутизации. Политики должны быть предварительно настроены в меню 25. Подробное описание политик маршрутизации см. в гл. 36 на стр. 367.
Bridge Options	
Ethernet Addr Timeout(min)	Это поле доступно в том случае, если в SMT (Меню 11.1: Профиль удаленного узла (узлы 1 – 7)) параметр **Bridge** установлен в значение **Yes**. Введите интервал времени (в минутах), в течение которого P-793H будет сохранять информацию об Ethernet-адресах в собственных внутренних таблицах после разъединения линии. Наличие этой информации поможет избежать необходимости повторного составления таблиц в P-793H после восстановления соединения.
После завершения работы с данным меню нажмите клавишу [ENTER] в сообщении "Press ENTER to Confirm…", чтобы сохранить настройки и вернуться в меню 11.1, либо нажмите клавишу [ESC] для отмены операции в любой момент.	

26.5 Фильтр удаленного узла

В меню 11.1 переместите курсор в поле **Edit Filter Sets** и нажмите пробел, чтобы установить значение **Yes**. Нажмите [ENTER] для входа в раздел **Menu 11.1.5 - Remote Node Filter** (фильтр удаленных узлов).

Это меню позволяет задать набор(ы) фильтров, применяемых к входящему и исходящему трафику между данным удаленным узлом и P-793H для предотвращения исходящих вызовов при поступлении определенных типов пакетов. Можно указать до 4 наборов фильтров, отделенных запятыми, например, 1, 5, 9, 12, в каждом поле фильтра. Обратите внимание на то, что в этом поле применяются пробелы. гл. 30 на стр. 317 содержит подробное описание настройки фильтров. Для выполнения инкапсуляции PPPoE или PPTP существует дополнительная опция указания наборов фильтров для вызовов удаленных узлов.

Рис. 157 Меню 11.5: Фильтр удаленного узла.

```
                Menu 11.5 - Remote Node Filter

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

Поля изображенного выше экрана описаны в следующей таблице.

Таблица 105 Меню 11.5: Фильтр удаленного узла.

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

Таблица 105 Меню 11.5: Фильтр удаленного узла. (продолжение)

ПОЛЕ	ОПИСАНИЕ
Protocol filters	Введите наборы фильтров (не более четырех). Чтобы ввести несколько наборов, перечислите их через запятую (,).
Device filters	Введите наборы фильтров (не более четырех). Чтобы ввести несколько наборов, перечислите их через запятую (,).

26.6 Параметры уровня ATM для удаленного узла

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

Рис. 158 Меню 11.6: Параметры уровня ATM для удаленного узла

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

VC Options for IP:                  VC Options for Bridge:
  VPI #= 0                            VPI #= 0
  VCI #= 38                           VCI #= 38
  ATM QoS Type= UBR                   ATM QoS Type= UBR
  Peak Cell Rate (PCR)= 0             Peak Cell Rate (PCR)= 0
  Sustain Cell Rate (SCR)= 0          Sustain Cell Rate (SCR)= 0
  Maximum Burst Size (MBS)= 0         Maximum Burst Size (MBS)= 0
```

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

                    VPI #= 0
                    VCI #= 38
                    ATM QoS Type= UBR
                    Peak Cell Rate (PCR)= 0
                    Sustain Cell Rate (SCR)= 0
                    Maximum Burst Size (MBS)= 0
```

Поля изображенного выше меню описаны в следующей таблице.

Таблица 106 Меню 11.6: Параметры уровня ATM для удаленного узла

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

Таблица 106 Меню 11.6: Параметры уровня ATM для удаленного узла (продолжение)

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

26.7 Специальные параметры настройки

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

Рис. 159 Меню 11.8: Специальные параметры настройки

```
                    Menu 11.8 - Advance Setup Options

                PPPoE pass-through= No
```

Поля изображенного выше меню описаны в следующей таблице.

Таблица 107 Меню 11.8: Специальные параметры настройки

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

27

Настройка статического маршрута

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

27.1 Настройка статического IP-маршрута

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

Рис. 160 Меню 12.1: Настройка статического IP-маршрута

```
                Menu 12.1 - IP Static Route Setup

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

Введите номер статического маршрута, который необходимо настроить.

Рис. 161 Меню 12.1.1: Редактирование статического IP-маршрута

```
                Menu 12.1.1 - Edit IP Static Route

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

Поля изображенного выше экрана описаны в следующей таблице.

Таблица 108 Меню 12.1.1: Редактирование статического маршрута IP

ПОЛЕ	ОПИСАНИЕ
Route #	Это – порядковый номер статического маршрута, выбранного в меню 12.
Route Name	Введите описательное имя для данного маршрута. Оно служит только для идентификации.
Active	Это поле позволяет активировать/деактивировать данный статический маршрут.
Destination IP Address	Этот параметр указывает IP-адрес конечной точки маршрута. Маршрутизация всегда подразумевает диапазон сетевых адресов. Если требуется указать маршрут до отдельного хоста, в поле "IP Subnet Mask" введите маску подсети 255.255.255.255 – при этом диапазон сетевых адресов будет ограничен до адреса хоста.
IP Subnet Mask	Введите маску подсети для места назначения данного маршрута.
Gateway IP Address	Введите IP-адрес интернет-центра. Шлюз – это непосредственно соседствующая с P-793H система, которая направляет пакет к месту назначения. В сети LAN шлюз должен быть маршрутизатором, находящимся в одном сегменте с P-793H; в WAN шлюз должен иметь IP-адрес одного из удаленных узлов.
Metric	Введите число от 1 до 15, определяющее приоритет данного маршрута в наборе маршрутов P-793H (см. разд. 5.2 на стр. 76). Чем меньше число, тем выше приоритет маршрута.
Private (Частный)	Этот параметр определяет, будет ли P-793H включать данный маршрут к удаленному узлу в свою широковещательную рассылку RIP. При установке значения **Yes (Да)** этот маршрут является частным и не включается в широковещательную рассылку RIP. При выборе значения **No (Нет)** маршрут к данному удаленному узлу распространяется на другие хосты через широковещательную рассылку RIP.
После завершения работы с данным меню нажмите клавишу [ENTER] в сообщении "Press ENTER to Confirm or ESC to Cancel", чтобы сохранить настройки, либо клавишу [ESC] для отмены.	

27.2 Настройка статического маршрута в режиме моста

Находясь в меню 12,3, введите 3. Для настройки статических маршрутов в меню 12.3 выберите один из маршрутов, перечисленных ниже.

Рис. 162 Меню 12.3: Настройка статического маршрута в режиме моста

```
                Menu 12.3 - Bridge Static Route Setup

              1. _________
              2. _________
              3. _________
              4. _________
```

Введите номер статического маршрута, который необходимо настроить.

Рис. 163 Меню 12.3.1: Редактирование статического маршрута моста

```
                 Menu 12.3.1 - Edit Bridge Static Route

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

Поля изображенного выше экрана описаны в следующей таблице.

Таблица 109 Меню 12.3.1: Редактирование статического маршрута моста

ПОЛЕ	ОПИСАНИЕ
Route #	Это – порядковый номер статического маршрута, выбранного в меню 12.
Route Name	Введите описательное имя для данного маршрута. Оно служит только для идентификации.
Active	Это поле позволяет активировать/деактивировать данный статический маршрут.
Ether Address	Этот параметр указывает MAC-адрес конечной точки маршрута.
IP Address	Введите IP-адрес интернет-центра. Шлюз – это непосредственно соседствующая с P-793H система, которая направляет пакет к месту назначения. В сети LAN шлюз должен быть маршрутизатором, находящимся в одном сегменте с P-793H; в WAN шлюз должен иметь IP-адрес одного из удаленных узлов.
Gateway Node	Нажмите пробел и [ENTER], чтобы выбрать номер удаленного узла, являющегося шлюзом для данного статического маршрута.
После завершения работы с данным меню нажмите клавишу [ENTER] в сообщении "Press ENTER to Confirm or ESC to Cancel", чтобы сохранить настройки, либо клавишу [ESC] для отмены.	

28

Настройка NAT

Этот экран позволяет настроить параметры трансляции сетевых адресов (NAT) в P-793H.

28.1 Использование NAT

Чтобы разрешить пересылку трафика из WAN через P-793H, в дополнение к настройке SUA/NAT необходимо создать правило для сетевого экрана.

28.1.1 Сравнение SUA и других режимов NAT

SUA (Учетная запись отдельного пользователя) является подмножеством ZyNOS NAT и поддерживает два типа привязки - **Many-to-One ("Множество-один")** и **Server (Сервер)**. Подробное описание настройки NAT для SUA см. в разд. 28.2.1 на стр. 301. P-793H также поддерживает полноценный режим NAT (**Full Feature**), в котором несколько глобальных IP-адресов привязываются к нескольким IP-адресам клиентов или серверов в частных сетях LAN одним из нескольких способов.

Если для P-793H выделен только один глобальный IP-адрес в сети WAN, выберите **SUA Only**.

Если для P-793H выделено несколько глобальных IP-адресов в сети WAN, выберите **Full Feature**.

28.1.2 Применение NAT

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

Рис. 164 Меню 4: Применение NAT для доступа к Интернету

```
                Menu 4 - Internet Access Setup

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

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

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

Рис. 165 Меню 11.3: Применение NAT к удаленному узлу

```
          Menu 11.3 - Remote Node Network Layer Options

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

Поля изображенного выше меню описаны в следующей таблице.

Таблица 110 Применение NAT в меню 4 и 11.3.

ПОЛЕ	ОПИСАНИЕ	ЗНАЧЕНИЯ
Network Address Translation	Если выбрано это значение, SMT будет использовать указанный набор привязки адресов (меню 15.1 – подробности см. в разд. 28.2.1 на стр. 301). Можно настроить любой из перечисленных типов привязки (гл. 7 на стр. 111). Выберите **Full Feature**, если для P-793H выделено несколько глобальных IP-адресов в сети WAN. При выборе опции **Full Feature** необходимо настроить как минимум один набор привязки адресов.	Full Feature
	Это значение параметра отключает NAT.	Нет
	Если выбран этот параметр, SMT использует набор привязки адресов 255 (меню 15.1 – см. разд. 28.2.1 на стр. 301). Если для P-793H выделен только один глобальный IP-адрес в сети WAN, выберите **SUA Only**.	SUA Only

28.2 Настройка NAT

Меню и подменю наборов привязки адресов используются для создания таблицы привязки, по которой присваиваются глобальные адреса компьютерам в LAN и DMZ. **Набор 255** используется для SUA. Если в меню 4 или меню 11.3 выбран режим **Full Feature**, SMT будет использовать указанный набор привязки адресов. При выборе **SUA Only** SMT использует предварительно заданный набор **255** (только для чтения).

Набор серверов – это список серверов в локальной сети, которым поставлены в соответствие внешние порты. Для использования этого набора правило сервера должно устанавливаться внутри набора привязки адресов NAT. Подробнее об этих меню см. в описании переадресации портов в разд. 7.4 на стр. 115. Для настройки NAT введите 15 в главном меню для отображения следующего экрана.

Рис. 166 Меню 15: Настройка NAT

```
                        Menu 15 - NAT Setup

                1. Address Mapping Sets
                2. NAT Server Sets
```

28.2.1 Наборы привязки адресов

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

Рис. 167 Меню 15.1: Наборы привязки адресов

```
                    Menu 15.1 - Address Mapping Sets

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

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

28.2.1.1 Определяемые пользователем наборы привязки адресов

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

Рис. 168 Меню 15.1.1: Правила привязки адресов

```
          Menu 15.1.1 - Address Mapping Rules

  Set Name= ACL Default Set

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

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

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

Таблица 111 Меню 15.1.1: правила привязки адресов

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

Порядок следования правил имеет важное значение, поскольку P-793H применяет правила в том порядке, в котором они определены. Когда правило соответствует текущему пакету, P-793H выполняет соответствующее действие, и остальные правила игнорируются. Если перед настроенным правилом есть пустые правила, это созданное правило передвинется вверх на определенное число пустых правил. Например, если правила 1 – 6 уже заданы в текущем наборе и выполняется настройка правила номер 9, на экране с обзором набора новое правило получает номер 7, а не 9.

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

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

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

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

Рис. 169 Меню 15.1.1.1: Правило привязки адресов

```
                    Menu 15.1.1.1 Address Mapping Rule

                    Type= Server

                    Local IP:
                      Start= N/A
                      End  = N/A

                    Global IP:
                      Start= 0.0.0.0
                      End  = N/A

                    Server Mapping Set= 2
```

Поля изображенного выше меню описаны в следующей таблице.

Таблица 112 Меню 15.1.1.1: Правило привязки адресов

ПОЛЕ	ОПИСАНИЕ
Type	Нажмите пробел и [ENTER], чтобы выбрать один из пяти типов. В этой графе перечисляются типы привязок, описанные ранее (гл. 7 на стр. 111). **Server** позволяет указать несколько серверов различных типов, расположенных на данном компьютере за различными типами NAT. Пример см. в разд. 28.4.3 на стр. 308 .
Local IP	Доступность отдельных полей зависит от содержимого поля **Type**.
Start	Введите начальный локальный IP-адрес (ILA).
End	Введите конечный локальный IP-адрес (ILA). Если данное правило применяется для всех локальных IP, в этом случае установите значение 0.0.0.0 для начального IP-адреса и 255.255.255.255 – для конечного. Это поле **N/A** (недоступно) для типов One-to-One и Server.
Global IP	Доступность отдельных полей зависит от содержимого поля **Type**.
Start	Введите начальный глобальный IP-адрес (IGA). При наличии динамического IP-адреса введите 0.0.0.0 в качестве **Global Start IP (Глобального начального IP-адреса)**. Обратите внимание на то, что для **Global IP Start (Глобального начального адреса)** можно установить значение 0.0.0.0 только в том случае, если выбраны типы **Many-to-One (Множество – один)** или **Server (Сервер)**.
End	Введите конечный глобальный IP-адрес (IGA). Это поле **N/A** (недоступно) для привязок **One-to-One**, **Many-to-One** и **Server**.
Server Mapping Set	Это поле доступно только в том случае, если в поле **Type** выбран режим **Server**. Выберите набор привязок сервера, используемый для данного правила.
Завершив настройку правила в этом меню, нажмите клавишу [ENTER] в сообщении "Press ENTER to Confirm or ESC to Cancel", чтобы сохранить настройки, либо клавишу [ESC] для отмены.	

28.3 Настройка сервера, находящегося за NAT

Если IP-адрес сервера по умолчанию (**Default Server**) не указан, P-793H будет отбрасывать все пакеты для портов, не указанных на этом экране или в настройке дистанционного управления.

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

1. Введите 15 в главном меню для перехода к **Menu 15 - NAT Setup**.
2. Введите 2, чтобы войти в меню 15.2 (для настройки правил привязки адресов на порту WAN устройства P-793H, снабженного одним портом WAN).

Рис. 170 Меню 15.2: Наборы серверов NAT

```
                Menu 15.2 - NAT Server Sets

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

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

Рис. 171 Меню 15.2: Настройка NAT в режиме сервера

```
                    Menu 15.2 - NAT Server Setup


 Rule   Start Port No.   End Port No.   IP Address
-------------------------------------------------------
   1.    Default          Default        0.0.0.0
   2.      80               80           192.168.1.10
   3.      0                0            0.0.0.0
   4.      0                0            0.0.0.0
   5.      0                0            0.0.0.0
   6.      0                0            0.0.0.0
   7.      0                0            0.0.0.0
   8.      0                0            0.0.0.0
   9.      0                0            0.0.0.0
  10.      0                0            0.0.0.0
  11.      0                0            0.0.0.0
  12.      0                0            0.0.0.0
```

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

Таблица 113 Меню 15.2: Настройка NAT в режиме сервера

ПОЛЕ	ОПИСАНИЕ
Rule	Это поле содержит порядковый номер и не связано с каким-либо правилом. Однако сам порядок также имеет значение. P-793H последовательно проверяет каждое активное правило и применяет только первое найденное правило, для которого выполняются условия.
Start Port	В этом поле отображается начало диапазона номеров портов, переадресуемых данным правилом.
End Port	В этом поле отображается конец диапазона номеров портов, переадресуемых данным правилом. Если указан только один номер порта, значение этого поля будет совпадать со значением поля **Start Port**.
IP Address	В этом поле отображается IP-адрес DHCP-сервера, на который переадресуются пакеты для указанных портов.

28.4 Общие примеры NAT

Ниже приведены некоторые примеры конфигурации NAT.

28.4.1 Пример 1: только доступ к Интернету

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

Рис. 172 NAT: пример 1

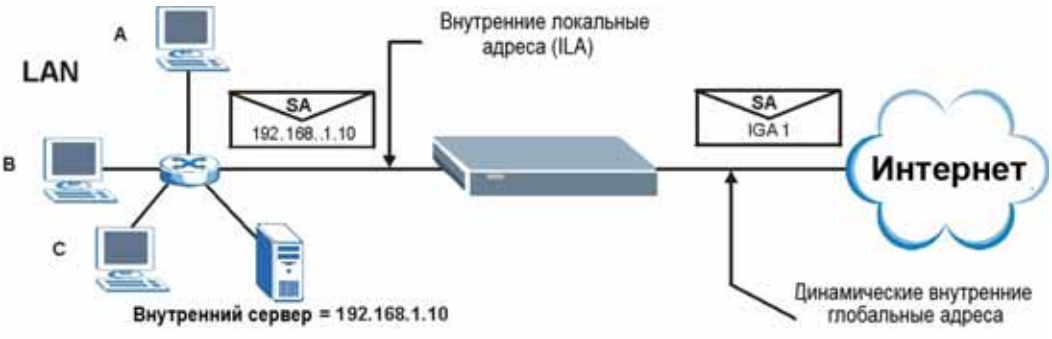
Рис. 173 Меню 4: Пример применения NAT для доступа в Интернет

```
                Menu 4 - Internet Access Setup

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

В показанном выше меню 4 выберите параметр **SUA Only** из поля **Network Address Translation**. При этом активируется режим привязки "многие к одному", описанный в разд. 28.4 на стр. 306. Недоступный для редактирования параметр **SUA Only** в поле **Network Address Translation** меню 4 и 11.3 изначально настроен на этот случай.

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

Рис. 174 NAT: пример 2



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

Рис. 175 Меню 15.2: указание внутреннего сервера

```
                Menu 15.2 - NAT Server Setup


 Rule   Start Port No.   End Port No.   IP Address
-------------------------------------------------
   1.    Default          Default        192.168.1.10
   2.      21               25           192.168.1.33
   3.      0                0            0.0.0.0
   4.      0                0            0.0.0.0
   5.      0                0            0.0.0.0
   6.      0                0            0.0.0.0
   7.      0                0            0.0.0.0
   8.      0                0            0.0.0.0
   9.      0                0            0.0.0.0
  10.      0                0            0.0.0.0
  11.      0                0            0.0.0.0
  12.      0                0            0.0.0.0
```

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

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

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

Можно привести следующий пример:

Рис. 176 NAT: пример 3

1. В этом случае следует настроить набор привязки адресов 1 в разделе **Menu 15.1 - Address Mapping Sets**. Для этого в поле **Network Address Translation** (меню 4 или меню 11.3) необходимо выбрать режим **Full Feature**, как показано на рис. 177 на стр. 310.
2. Затем введите 15 в главном меню.
3. Введите 1 для настройки наборов привязки адресов.
4. Введите 1, чтобы начать настройку этого нового набора. Введите имя набора, выберите значение **Edit Action** (Редактировать действие) и затем введите 1 в поле **Select Rule** (Выбрать правило). Нажмите [ENTER] для подтверждения.
5. В поле **Type** выберите **One-to-One** (непосредственная привязка для пакетов, пересылаемых в обоих направлениях) и в качестве локального начального IP-адреса (**Start IP**) введите 192.168.1.10 (IP-адрес FTP-сервера 1), а в качестве глобального начального IP-адреса (**Start IP**) введите 10.132.50.1. Этот адрес будет первым IGA. (См. рис. 178 на стр. 310.)
6. Повторите предыдущее действие для выполнения правил 2 – 4, как указано выше.
7. После выполнения этих настроек меню 15.1.1 должно принять вид, показанный на рис. 179 на стр. 311.

Рис. 177 Пример 3: меню 11.3

```
                Menu 11.3 - Remote Node Network Layer Options

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

Следующий рисунок иллюстрирует настройку первого правила.

Рис. 178 Пример 3: меню 15.1.1.1

```
                  Menu 15.1.1.1 Address Mapping Rule

                  Type= One-to-One

                  Local IP:
                    Start= 192.168.1.10
                    End  = N/A

                  Global IP:
                    Start= 10.132.50.1
                    End  = N/A

                  Server Mapping Set= N/A
```

Рис. 179 Пример 3: заключительное меню 15.1.1

```
          Menu 15.1.1 - Address Mapping Rules

 Set Name= Example3

Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
---  ---------------  ---------------  ---------------  ---------------  --
 1.  192.168.1.10                      10.132.50.1                        1-1
 2.  192.168.1.11                      10.132.50.2                        1-1
 3.  0.0.0.0          255.255.255.255  10.32.50.3                         M-1
 4.                                   10.132.50.3                       Serve+
 5.
 6.
 7.
 8.
 9.
10.

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

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

1. Введите 15 в главном меню.
2. Введите 2, чтобы перейти в меню 15.2.
3. (Для P-793H с несколькими портами WAN в меню 15.2 введите 1 или 2.) Настройте меню, как показано на рис. 180 на стр. 311.

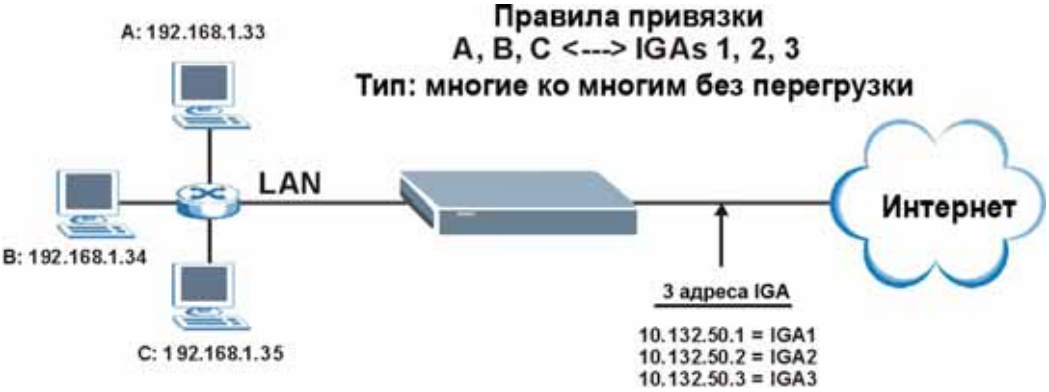
Рис. 180 Пример 3: меню 15.2

```
                    Menu 15.2 - NAT Server Setup


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

28.4.4 Пример 4: программы, несовместимые с NAT

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

Рис. 181 NAT: пример 4



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

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

Рис. 182 Пример 4: меню 15.1.1.1: Правило привязки адресов

```
Menu 15.1.1.1 Address Mapping Rule

Type= Many-to-Many No Overload

Local IP:
  Start= 192.168.1.10
  End  = 192.168.1.12

Global IP:
  Start= 10.132.50.1
  End  = 10.132.50.3

Server Mapping Set= N/A
```

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

Рис. 183 Пример 4: меню 15.1.1: Правила привязки адресов

```
          Menu 15.1.1 - Address Mapping Rules

 Set Name= Example4

Idx  Local Start IP   Local End IP    Global Start IP  Global End IP   Type
---  ---------------  --------------- ---------------  --------------- --
 1. 192.168.1.10      192.168.1.12    10.132.50.1      10.132.50.3     M-M N+
 2.
 3.
 4.
 5.
 6.
 7.
 8.
 9.
10.

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

29

Меню Firewall Setup

Это меню используется для активации или деактивации межсетевого экрана.

29.1 Работа с меню SMT в P-793H

В главном меню введите 21 для перехода в меню **Menu 21 - Filter and Firewall Setup**. Появится показанный ниже экран.

Рис. 184 Меню 21: Настройка фильтра и межсетевого экрана

```
                Menu 21 - Filter and Firewall Setup

              1. Filter Setup
              2. Firewall Setup
```

29.1.1 Активация межсетевого экрана

Введите опцию 2 в этом меню для отображения следующего экрана. Нажмите пробел, затем [ENTER], чтобы выбрать значение **Yes** в поле **Active** для активирования межсетевого экрана. Межсетевой экран защищает от атак, вызывающих отказ в обслуживании (DoS). Для настройки правил межсетевого экрана необходимо использовать веб-конфигуратор. Настройка названий наборов правил (**LAN-to-WAN Set Name** и **WAN-to-LAN Set Name**) может осуществляться через веб-конфигуратор или в меню 15 SMT.

Рис. 185 Меню 21.2: Настройка межсетевого экрана

```
                        Menu 21.2 - Firewall Setup

     The firewall protects against Denial of Service (DoS) attacks when
     it is active. The default Policy sets

         1. allow all sessions originating from the LAN to the WAN and
         2. deny all sessions originating from the WAN to the LAN

     You may define additional Policy rules or modify existing ones but
     please exercise extreme caution in doing so

         Active: Yes

         LAN-to-WAN Set Name: ACL Default Set
         WAN-to-LAN Set Name: ACL Default Set

     Please configure the Firewall function through Web Configurator
```

Для настройки правил межсетевого экрана рекомендуется использовать веб-конфигуратор.

30

Настройка фильтра

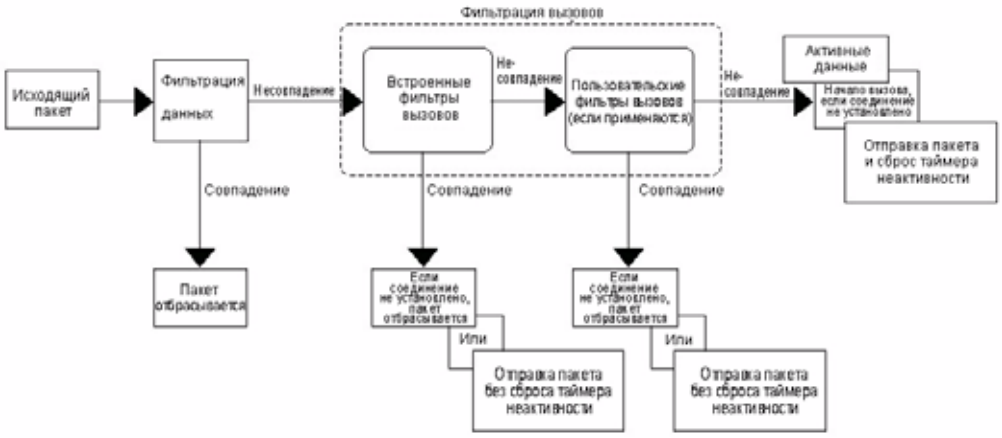
В этой главе дается описание того, как создавать и применять фильтры.

30.1 Основы применения фильтров

P-793H использует фильтры для принятия решений о прохождении или запрете пакета, а также об осуществлении исходящего вызова. Существует два типа применения фильтров: фильтрация данных и фильтрация вызовов. Фильтры данных подразделяются на фильтры устройств и протоколов, описание которых дается ниже.

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

Рис. 186 Процесс фильтрации исходящих пакетов



К исходящим пакетам P-793H применяет только фильтры данных. Пакеты обрабатываются в зависимости от того, найдено ли соответствие. В следующих разделах описана настройка наборов фильтров.

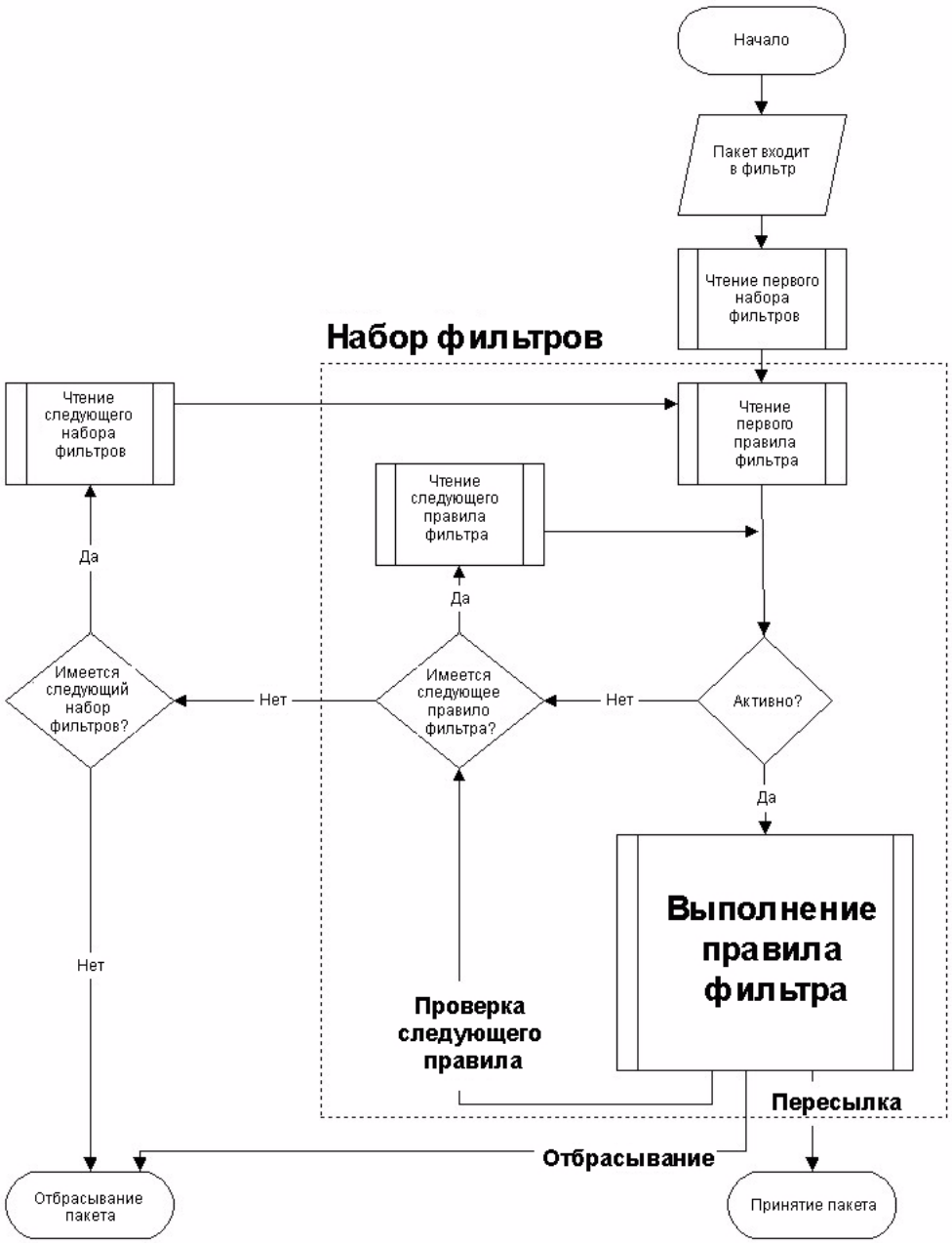
30.1.1 Структура фильтров устройства P-793H

Набор фильтров состоит из одного или нескольких правил фильтров. Обычно группы объединяют соответствующие правила, например, все правила для NetBIOS, в набор с общим именем. P-793H позволяет настроить до двенадцати наборов фильтров, содержащих 6 правил в каждом наборе, что всего составляет 72 правила фильтров в системе. В одном наборе нельзя смешивать правила фильтров устройств и правила фильтров протоколов. Можно применить до четырех наборов фильтров для конкретного порта с целью блокирования нескольких типов пакетов. При том, что каждый набор фильтров содержит до шести правил, можно иметь максимум 24 правила, задействованных для одного порта.

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

На следующем рисунке проиллюстрирован логический поток при выполнении правила фильтра. Смотрите также рис. 192 на стр. 325, где изображен логический поток при выполнении IP-фильтра.

Рис. 187 Процесс выполнения правил фильтра



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

30.2 Настройка набора фильтров

P-793H осуществляет фильтрацию пакетов протокола NetBIOS поверх TCP/IP по умолчанию. Для настройки другого набора фильтров выполните указанные ниже действия.

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

Рис. 188 Меню 21: Настройка фильтра и межсетевого экрана

```
                    Menu 21 - Filter and Firewall Setup

                  1. Filter Setup
                  2. Firewall Setup
```

2. Введите 1 для отображения следующего меню.

Рис. 189 Меню 21.1: Настройка набора фильтров

```
                  Menu 21.1 - Filter Set Configuration

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

                  Enter Filter Set Number to Configure= 0

                  Edit Comments= N/A
```

3. Выберите набор фильтров, которые необходимо настроить (1-12), и нажмите [ENTER].
4. Введите описательное имя или комментарий в поле **Edit Comments** и нажмите [ENTER].
5. Нажмите [ENTER] в сообщении [Press ENTER to confirm] для открытия **Menu 21.1.1 - Filter Rules Summary**.

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

Рис. 190 Меню 21.1.1: Сводка правил фильтра

```
                    Menu 21.1.1 - Filter Rules Summary

# A Type                      Filter Rules                            M m n
- - ---- ------------------------------------------------------------ -
1 N
2 N
3 N
4 N
5 N
6 N
```

Поля изображенного выше экрана описаны в следующей таблице.

Таблица 114 Аббревиатуры, используемые в меню сводки правил фильтров

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

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

Таблица 115 Используемые аббревиатуры правил

СОКРАЩЕНИЯ	ОПИСАНИЕ
IP	
Pr	Протокол
SA	Адрес источника
SP	Номер порта источника
DA	Адрес получателя

Таблица 115 Используемые аббревиатуры правил

СОКРАЩЕНИЯ	ОПИСАНИЕ
DP	Номер порта получателя
GEN	
Off	Смещение
Len	Длина

Настройка правил фильтров описана в следующем разделе.

30.2.1 Настройка правила фильтра

Чтобы настроить правило фильтра, введите его номер в разделе **Menu 21.1.1 - Filter Rules Summary** и нажмите [ENTER]. Откроется меню 21.1.1.1 для редактирования правила.

Для ускорения фильтрации все правила в наборе фильтров должны относиться к одному и тому же классу, т.е. быть фильтрами протоколов или универсальными фильтрами. Класс набора фильтров определяется по первому правилу, создаваемому пользователем. При применении наборов фильтров к порту отдельные поля меню предоставляются для наборов фильтров протоколов и устройств. При попытке указать набор фильтров протокола в поле фильтров устройства или наоборот P-793H отображает предупреждение и не позволяет выполнить сохранение.

30.2.2 Настройка правила фильтра TCP/IP

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

Для настройки правил TCP/IP выберите **TCP/IP Filter Rule** в поле **Filter Type** и нажмите [ENTER], чтобы открыть раздел **Menu 21.1.1.1 - TCP/IP Filter Rule**, показанный ниже.

Рис. 191 Меню 21.1.1.1: Правила фильтров TCP/IP

```
                Menu 21.1.1.1 - TCP/IP Filter Rule

            Filter #: 1,1
            Filter Type= TCP/IP Filter Rule
            Active= No
            IP Protocol= 0     IP Source Route= No
            Destination: IP Addr=
                         IP Mask=
                         Port #=
                         Port # Comp= None
                 Source: IP Addr=
                         IP Mask=
                         Port #=
                         Port # Comp= None
            TCP Estab= N/A
            More= No           Log= None
            Action Matched= Check Next Rule
            Action Not Matched= Check Next Rule
```

Настройка правила фильтра TCP/IP описана в следующей таблице.

Таблица 116 Меню 21.1.1.1: Правила фильтров TCP/IP

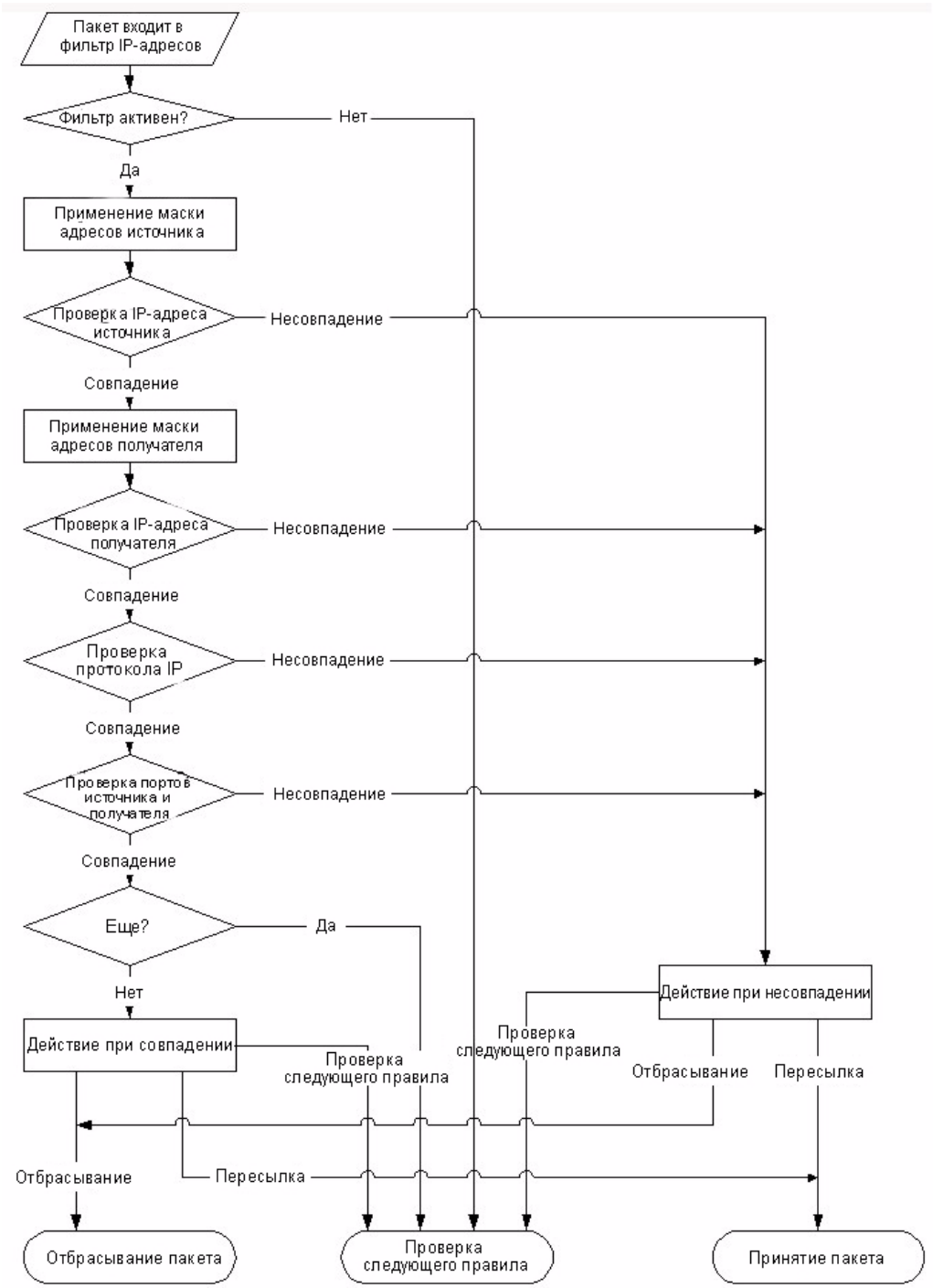
ПОЛЕ	ОПИСАНИЕ
Active	Нажмите пробел, затем [ENTER], чтобы выбрать **Yes** и активировать правило фильтра, или **No** для деактивации правила.
IP Protocol	Укажите протокол верхнего уровня, например, TCP – 6, UDP – 17, ICMP – 1. Введите значение от 0 до 255. Значение 0 соответствует ЛЮБОМУ протоколу.
IP Source Route	Нажмите пробел и [ENTER], чтобы выбрать значение **Yes** для применения правила к пакетам с опцией исходного маршрута IP. В противном случае пакеты не должны иметь опцию исходного маршрута. Большинство пакетов IP не содержат исходный маршрут.
Destination	
IP Addr	Введите IP-адрес места поолучателя пакета, который необходимо фильтровать. Поле игнорируется, если его значение – 0.0.0.0.
IP Mask	Введите маску IP, применяемую к полю **Destination: IP Addr**.
Port #	Введите порт получателя пакетов, подлежащих фильтрации. Диапазон данного поля – 0 - 65535. Это поле игнорируется, если его значение 0.
Port # Comp	Нажмите [SPACE BAR], затем [ENTER] для выбора сравнения с целью применения к порту места назначения в пакете и значения, заданного в поле **Destination: Port #**. Возможны следующие значения: **None** (нет), **Equal** (равно), **Not Equal** (не равно), **Less** (меньше) и **Greater** (больше).
Source	
IP Addr	Введите IP-адрес источника пакета, который необходимо фильтровать. Поле игнорируется, если его значение – 0.0.0.0.
IP Mask	Введите маску IP для применения к **Source (Источнику): IP Addr**.
Port #	Введите порт источника пакетов, которые необходимо фильтровать. Диапазон данного поля – 0 - 65535. Это поле игнорируется, если его значение 0.
Port # Comp	Нажмите пробел, затем [ENTER] для выбора сравнения, применяемого к порту источника в пакете, и значения, заданного в поле **Source: Port #**. Возможны следующие значения: **None** (нет), **Equal** (равно), **Not Equal** (не равно), **Less** (меньше) и **Greater** (больше).
TCP Estab	Это поле действует только в том случае, когда значение поля IP Protocol (Протокол IP) –6, TCP. Нажмите пробел и [ENTER], чтобы выбрать значение **Yes** и применять правило к пакетам, устанавливающим соединение TCP (SYN=1 и ACK=0); если значение – **No**, правило игнорируется.
More	Нажмите пробел и [ENTER] для выбора значения **Yes** или **No**. Если значение – **Yes (Да)**, соответствующий пакет передается следующему правилу фильтров перед выполнением действия; если **No (Нет)**, пакет отбрасывается в соответствии с полями действия. Если значение поля **More** – **Yes (Да)**, в таком случае **Action Matched** и **Action Not Matched** будут **N/A**.
Log	Нажмите пробел, затем [ENTER] для выбора опции регистрации из следующих вариантов: **None (Нет)** – Пакеты не регистрируются. **Action Matched** - Регистрируются только пакеты, соответствующие параметрам правила. **Action Not Matched** - Регистрируются только пакеты, не соответствующие параметрам правила. **Both (Оба)** – Регистрируются все пакеты.

Таблица 116 Меню 21.1.1.1: Правила фильтров TCP/IP (продолжение)

ПОЛЕ	ОПИСАНИЕ
Action Matched	Нажмите пробел и [ENTER], чтобы выбрать действие для пакетов, соответствующих условиям. Возможны следующие значения: **Check Next Rule** (проверить следующее правило), **Forward** (переслать) и **Drop** (отбросить).
Action Not Matched	Нажмите пробел и [ENTER] для выбора действия для пакета, не соответствующего условиям правила. Возможны следующие значения: **Check Next Rule** (проверить следующее правило), **Forward** (переслать) и **Drop** (отбросить).
По завершении настроек в меню **Menu 21.1.1.1 - TCP/IP Filter Rule** нажмите [ENTER] в сообщении "Press ENTER to Confirm", чтобы сохранить настройки, или [ESC] для отмены. Эти данные теперь должны отображаться в **Menu 21.1.1 - Filter Rules Summary (Меню 21.1.1 – Сводка правил фильтра)**.	

На следующем рисунке проиллюстрирован логический поток фильтра IP.

Рис. 192 Выполнение фильтра IP



30.2.3 Настройка универсального правила фильтра

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

При обработке универсальных правил P-793H рассматривает пакет как поток байтов, а не как структурированный пакет IP или IPX. Следует указать часть пакета, подлежащую проверке с использованием полей **Offset** (от 0) и **Length**, выраженных в байтах. P-793H применяет к блоку данных маску (с использованием побитового "И"), после чего сравнивает результат со значением для определения соответствия. Поля **Mask** и **Value** указываются в виде шестнадцатеричных чисел. Обратите внимание на то, что для представления байта требуется две шестнадцатеричных цифры, поэтому если длина – 4, для ввода значения в каждом поле требуется 8 цифр, например, FFFFFFFF.

Для настройки универсального правила выберите **Generic Filter Rule** в поле **Filter Type** в меню 21.1.1.1 и нажмите [ENTER], чтобы открыть универсальное правило фильтра, как показано ниже.

Рис. 193 Меню 21.1.1.1: Универсальное правило фильтра

```
                Menu 21.1.1.1 - Generic Filter Rule

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

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

Таблица 117 Меню 21.1.1.1: Универсальное правило фильтра

ПОЛЕ	ОПИСАНИЕ
Filter #	В этом поле указываются координаты правила. Например, 2,3 означает второй набор фильтров и третье правило этого набора.
Filter Type	Нажмите пробел и [ENTER] для выбора типа правила. Параметры, отображаемые под каждым типом, различны. Правила фильтров TCP/IP используются для фильтрации пакетов IP, тогда как универсальные правила фильтров допускают фильтрацию пакетов, не относящихся к IP. Возможны следующие значения: **Generic Filter Rule** (универсальное правило фильтра) и **TCP/IP Filter Rule** (правило фильтра TCP/IP).
Active	Выберите **Yes (Да)** для включения правила фильтров или **No (Нет)** для его выключения.
Offset	Введите начальный байт блока данных в пакете, который необходимо сравнить. Диапазон этого поля – от 0 до 255.
Length	Введите сумму байтов блока данных в пакете, который необходимо сравнить. Диапазон этого поля – от 0 до 8.
Mask	Введите маску(в шестнадцатеричном формате) для применения к блоку данных перед сравнением.
Value	Введите значение (в шестнадцатеричном формате) для сравнения с блоком данных.
More	Если значение – **Yes (Да)**, соответствующий пакет передается следующему правилу фильтров перед выполнением действия; в противном случае пакет отбрасывается в соответствии с полями действия. Если в поле **More** указано значение **Yes**, то поля Action Matched и Action Not Matched будут содержать значение **No**.

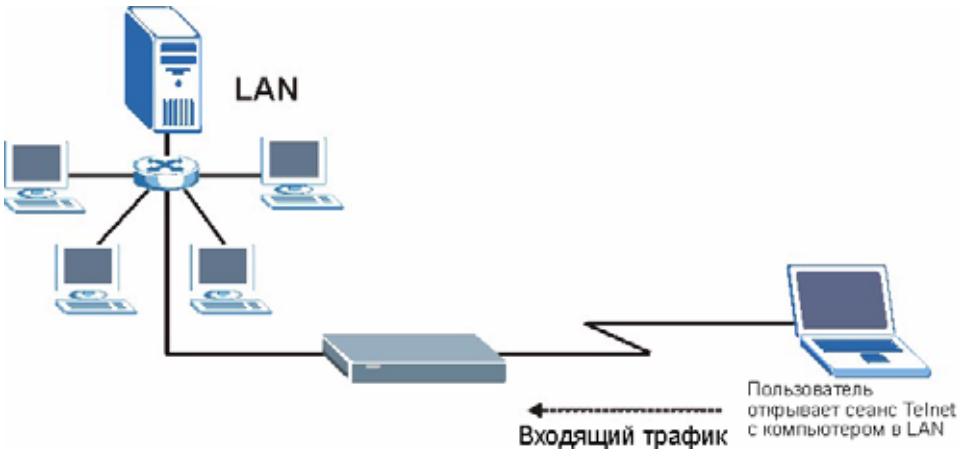
Таблица 117 Меню 21.1.1.1: Универсальное правило фильтра (продолжение)

ПОЛЕ	ОПИСАНИЕ
Log	Выберите опцию регистрации из числа следующих вариантов: **None** – пакеты не регистрируются. **Action Matched** - регистрируются только пакеты, соответствующие параметрам правила. **Action Not Matched** - регистрируются только пакеты, не соответствующие параметрам правила. **Both** – Регистрируются все пакеты.
Action Matched	Выберите действие для пакета, соответствующему правилу. Возможны следующие значения: **Check Next Rule** (проверить следующее правило), **Forward** (переслать) и **Drop** (отбросить).
Action Not Matched	Выберите действие для пакетов, не соответствующих правилу. Возможны следующие значения: **Check Next Rule** (проверить следующее правило), **Forward** (переслать) и **Drop** (отбросить).
Заполнив поля в разделе **Menu 21.1.1.1 - Generic Filter Rule**, нажмите [ENTER] на сообщении "Press ENTER to Confirm", чтобы сохранить настройки, или [ESC] для отмены. Эти данные теперь должны отображаться в **Menu 21.1.1 - Filter Rules Summary (Меню 21.1.1 – Сводка правил фильтра)**.	

30.3 Пример фильтра

Рассмотрим пример блокирования доступа внешних пользователей к устройству P-793H через Telnet. Другие примеры фильтров можно найти на компакт-диске в комплекте с устройством.

Рис. 194 Пример фильтра для Telnet



1. Перейдите в раздел **Menu 21 - Filter and Firewall Setup**, введя 21 в главном меню.
2. Введите 1 для входа в меню 21.1 - Filter Set Configuration (настройка набора фильтров).
3. Выберите номер набора фильтров, который необходимо настроить (например, 3), и нажмите [ENTER].
4. Введите описательное имя или комментарий в поле **Edit Comments** и нажмите [ENTER].
5. Чтобы открыть раздел **Menu 21.1.3 - Filter Rules Summary**, в сообщении [Press ENTER to confirm] нажмите [ENTER].
6. Введите 1 для настройки первого правила фильтров (единственное правило фильтров в данном наборе). Внесите записи в это меню, как показано на следующем рисунке.

Рис. 195 Пример фильтра: меню 21.1.3.1

```
                    Menu 21.1.3.1 - TCP/IP Filter Rule

                Filter #: 3,1
                Filter Type= TCP/IP Filter Rule
                Active= Yes
                IP Protocol= 6      IP Source Route= No
                Destination: IP Addr=
                             IP Mask=
                             Port #= 23
                             Port # Comp= Equal
                     Source: IP Addr=
                             IP Mask=
                             Port #=
                             Port # Comp= None
                TCP Estab= No
                More= No            Log= None
                Action Matched= Drop
                Action Not Matched= Forward
```

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

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

Рис. 196 Пример сводки правил фильтров: меню 21.1.3

```
                    Menu 21.1.3 - Filter Rules Summary

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

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

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

После создания набора фильтров необходимо применить его.

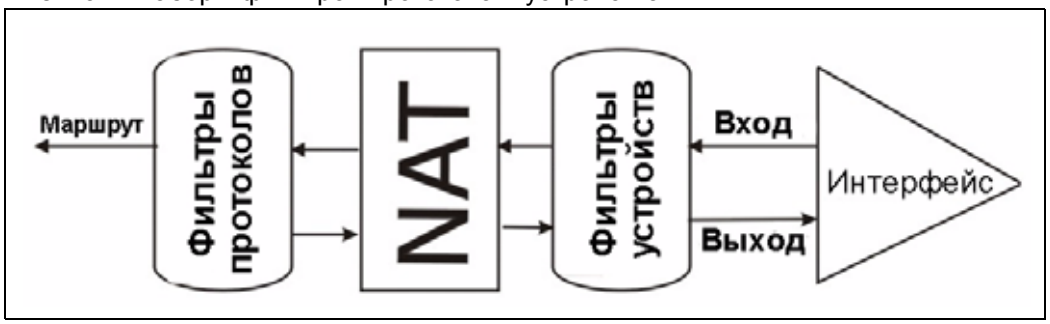
1. Введите 11 в главном меню для перехода к меню 11.
2. Введите 1 или 2 для входа в раздел **Menu 11.x - Remote Node Profile**.

3 Перейдите в поле **Edit Filter Sets,** нажмите пробел для выбора значения **Yes**, а затем – [ENTER].
4 Откроется меню 11.1.4. Активируйте набор фильтров (в данном примере – набор 3), как показано на рис. 157 на стр. 292.
5 Указав номера наборов и покинув меню 11.1.4, нажмите [ENTER] для подтверждения.

30.4 Типы фильтров и NAT

Существует два класса правил фильтров: универсальные правила устройства (**Generic Filter**) и правила фильтра протоколов (**TCP/IP**). Правила универсального фильтра действуют по отношению к необработанным данным, пересылаемым в/из LAN и WAN. Правила фильтра протокола воздействуют на пакеты IP. Более подробно правила универсального фильтра и фильтра TCP/IP рассматриваются в следующем разделе. При включении NAT (трансляции сетевых адресов) внутренний адрес IP и номер порта заменяются на основе последовательных соединений, что делает возможным выяснение точного адреса и порта в сети. Поэтом, P-793H применяет фильтры протоколов к "известному" IP-адресу и номеру порта перед прохождением NAT для исходящих пакетов и после NAT – для входящих пакетов. С другой стороны, универсальные фильтры или фильтры устройств применяются к необработанным пакетам, появляющимся в сети. Фильтры на P-793H применяются в момент приема и отправки пакетов, т.е. на интерфейсе. Интерфейсом может служить порт Ethernet или любой другой аппаратный порт. Это проиллюстрировано на следующей диаграмме.

Рис. 197 Наборы фильтров протокола и устройства



30.5 Сравнение межсетевого экрана и фильтров

Гл. 9 на стр. 139 подробно рассматривает настройку межсетевого экрана. Также проводится сравнение фильтрации, NAT и межсетевого экрана.

30.6 Применение фильтра

В этом разделе показано, где применять фильтр(ы) после его (их) создания. В устройстве P-793H предусмотрены стандартные фильтры для предотвращения исходящих вызовов в результате трафика NetBIOS, а также блокирования входящих соединений по Telnet, FTP и HTTP.

Если межсетевой экран не активирован, рекомендуется применять фильтры.

30.6.1 Применение фильтров LAN

Наборы фильтров трафика LAN могут быть полезны для блокировки определенных пакетов, сокращения объема трафика и предотвращения возникновения брешей в системе безопасности. Перейдите в меню 3.1 (показано ниже) и введите номер(а) набора(ов) фильтров, которые необходимо применить соответствующим образом. Можно выбрать до четырех наборов фильтров (из 12), введя их номера через запятую, например, 3, 4, 6, 11. Наборы входных фильтров фильтруют входящий в P-793H трафик, а наборы выходных фильтров – трафик, исходящий из P-793H.

Рис. 198 Фильтрация трафика LAN

```
                Menu 3.1 - LAN Port Filter Setup

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

30.6.2 Применение фильтров удаленного узла

Перейдите в показанное ниже меню 11.5 (необходимо учесть, что наборы фильтров вызовов предусмотрены только для инкапсуляции PPPoA или PPPoE) и введите соответствующие номера наборов фильтров. Можно последовательно ввести до четырех наборов фильтров, вводя их номера, разделенные запятыми. В устройстве P-793H предусмотрены стандартные фильтры для предотвращения исходящих вызовов в результате трафика NetBIOS, а также блокирования входящих соединений по Telnet, FTP и HTTP.

Рис. 199 Фильтрация трафика удаленного узла

```
                Menu 11.5 - Remote Node Filter

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

31

Меню SNMP Configuration

Это меню служит для настройки SNMP. Дополнительные сведения о протоколе SNMP см. в разд. 15.6 на стр. 215.

31.1 Настройка SNMP

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

Рис. 200 Меню 22: Настройка SNMP

```
                Menu 22 - SNMP Configuration

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

В следующей таблице описаны параметры конфигурации SNMP.

Таблица 118 Меню 22: Настройка SNMP

ПОЛЕ	ОПИСАНИЕ
Get Community	Введите сообщество для запроса Get, которое будет выступать в качестве пароля для всех входящих запросов Get и GetNext от диспетчерской станции.
Set Community	Введите сообщество для запроса Set, которое будет выступать в качестве пароля для всех входящих запросов Set от диспетчерской станции.
Trusted Host	Если указан доверенный хост, P-793H будет отвечать на SNMP-сообщения, исходящие только с этого адреса. Пустое (по умолчанию) поле означает, что P-793H будет отвечать на все сообщения SNMP, получаемые им, независимо от источника.
Trap	
Community	Введите сообщество для прерываний, которое будет выступать в качестве пароля при отправке прерываний диспетчеру SNMP.
Destination	Введите IP-адрес станции, которой следует направлять прерывания SNMP.
Заполнив поля в этом меню, нажмите [ENTER] в приглашении "Press [ENTER] to confirm or [ESC] to cancel", чтобы сохранить настройки, или [ESC] для отмены и возврата на предыдущий экран.	

32

Системный пароль

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

Рис. 201 Меню 23: Системный пароль

```
                    Menu 23 - System Password

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

Поля изображенного выше экрана описаны в следующей таблице.

Таблица 119 Меню 23: Системный пароль

ПОЛЕ	ОПИСАНИЕ
Old Password	Введите текущий пароль администратора для P-793H.
New Password	Введите новый пароль администратора для P-793H.
Retype to confirm	Повторно введите новый пароль администратора.

33

Информация о системе и диагностика

В этой главе рассматриваются меню SMT с 24.1 по 24.4.

33.1 Обзор средств наблюдения за состоянием системы

В этой главе описываются диагностические средства, которые могут использоваться для обслуживания P-793H. Эти инструменты сообщают текущее состояние системы и портов, обеспечивают ведение журналов и трассировку.

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

Рис. 202 Меню 24: Обслуживание системы

```
                Menu 24 - System Maintenance

              1.  System Status
              2.  System Information and Console Port Speed
              3.  Log and Trace
              4.  Diagnostic
              5.  Backup Configuration
              6.  Restore Configuration
              7.  Upload Firmware
              8.  Command Interpreter Mode
              9.  Call Control
              10. Time and Date Setting
              11. Remote Management
```

33.2 Меню System Status

Первый пункт – System Status (состояние системы) – содержит сведения о версии микропрограммы и состоянии портов, а также статистику по портам, как показано на следующем рисунке. Экран System Status можно использовать для наблюдения за состоянием P-793H. В частности, этот экран предоставляет информацию о версии микропрограммы и числе отправленных и полученных пакетов.

Для входа в раздел System Status:

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

Рис. 203 Меню 24.1: Состояние системы

```
                  Menu 24.1 - System Maintenance - Status          06:28:45
                                                          Sat. Jan. 01, 2000

Node-Lnk Status      TxPkts      RxPkts     Errors  Tx B/s  Rx B/s     Up Time
 1-ENET  N/A              0           0          0       0       0     0:00:00
 2       N/A              0           0          0       0       0     0:00:00
 3       N/A              0           0          0       0       0     0:00:00
 4       N/A              0           0          0       0       0     0:00:00
 5       N/A              0           0          0       0       0     0:00:00
 6       N/A              0           0          0       0       0     0:00:00
 7       N/A              0           0          0       0       0     0:00:00
 8       N/A              0           0          0       0       0     0:00:00

My WAN IP (from ISP): 0.0.0.0

    Ethernet:                                      WAN:
      Status: 100M/Full Duplex Tx Pkts: 4210       Line Status: Down
      Collisions: 0            Rx Pkts: 4466       Transfer Rate:     0 kbps
    CPU Load =    1.27%
                                 Press Command:
                       COMMANDS: 1-Reset Counters  ESC-Exit
```

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

Таблица 120 Меню 24.1: Состояние системы

ПОЛЕ	ОПИСАНИЕ
Node-Lnk	В этом поле отображается порядковый номер и тип соединения с удаленным узлом (тип инкапсуляции).
Status	В этом поле отображается состояние: **Down** (канал разъединен), **Up** (канал соединен), если используется инкапсуляция Ethernet, и **Down** (канал разъединен), **Up** (канал соединен), **Idle** (соединение (ppp-сеанс) неактивно), **Dial** (начало вызова) и **Drop** (прерывание вызова), если используется инкапсуляция PPPoE. Отсутствие соединения на порту обозначается **N/A**.
TxPkts	В этом поле отображается количество пакетов, отправленных P-793H на удаленный узел.
RxPkts	В этом поле отображается количество пакетов, принятых P-793H с удаленного узла.
Errors	В этом поле отображается количество пакетов, полученных через данное соединение.
Tx B/s	В этом поле отображается скорость передачи данных в байтах в секунду через данный порт.

Таблица 120 Меню 24.1: Состояние системы (продолжение)

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

33.3 Информация о системе и скорость консольного порта

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

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

Рис. 204 Меню 24.2: Информация о системе и скорость консольного порта

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

                  1. System Information
                  2. Console Port Speed
```

33.3.1 Информация о системе

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

Рис. 205 Меню 24.2.1: Обслуживание системы – информация

```
                Menu 24.2.1 - System Maintenance - Information

                   Name: P-793H
                   Routing: IP
                   ZyNOS F/W Version (Версия ZyNOS F/W):
V3.40(RQ.0)b1_20060614 | 06/14/2006
                   SHDSL Chipset Vendor: IFX Soc2U 1.1-1.5.2__001
                   Standard: ANSI(ANNEX_A)

                   LAN
                     Ethernet Address: 00:13:49:65:43:21
                     IP Address: 192.168.1.1
                     IP Mask: 255.255.255.0
                     DHCP: Server
```

Поля изображенного выше экрана описаны в следующей таблице.

Таблица 121 Меню 24.2.1: Обслуживание системы – информация

ПОЛЕ	ОПИСАНИЕ
Name	В этом поле отображается имя системы P-793H и имя домена, назначенное в меню 1. Пример: System Name= xxx; Domain Name= baboo.mickey.com Name= xxx.baboo.mickey.com
Routing	Указывает на используемый протокол маршрутизации.
ZyNOS F/W Version	Отображает версию сетевой операционной системы ZyXEL.
SHDSL Chipset Vendor	Отображает тип чипсета SHDSL в устройстве P-793H.
Standard	Отображает протокол, используемый P-793H и DSLAM (мультиплексором цифровых абонентских каналов).
LAN	
Ethernet Address	Отображает MAC-адрес устройства P-793H.
IP Address	В этом поле отображается IP-адрес P-793H в десятичном виде через точку.
IP Mask	В этом поле отображается маска IP-подсети P-793H.
DHCP	В этом поле отображается режим DHCP, используемый P-793H.
Просмотрев настройки, нажмите [ESC] или [ENTER] для выхода.	

33.3.2 Настройка скорости консольного порта

Экран **Menu 24.2.2 – System Maintenance - Change Console Port Speed** позволяет изменить скорость консольного порта. Консольный порт P-793H поддерживает следующие скорости передачи: 9600 (по умолчанию), 19200, 38400, 57600 и 115200 бит/с. Чтобы выбрать требуемую скорость, в меню 24.2.2 нажмите пробел и [ENTER].

Рис. 206 Меню 24.2.2: Обслуживание системы - изменение скорости консольного порта

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

Console Port Speed: 9600
```

33.4 Регистрация и трассировка

Устройство P-793H реализует две функции ведения журналов. Первая – журналы ошибок и записи трассировки (отслеживания), сохраняемые локально. Вторая – регистрация сообщений на UNIX SYSLOG-сервере.

33.4.1 Просмотр журнала ошибок

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

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

После того, как P-793H выведет журнал полностью, устройство предложит очистить журнал.

Рис. 207 Меню 24.3: Обслуживание системы – журналы и трассировка

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

   1. View Error Log
   2. UNIX Syslog
```

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

Рис. 208 Примеры ошибок и информационных сообщений

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

33.4.2 Ведение журнала на SYSLOG-сервере

По протоколу SYSLOG P-793H передает на сервер SYSLOG записи CDR (детализацию вызовов) и системные сообщения. Параметры SYSLOG и учета настраиваются на экране **Menu 24.3.2 - System Maintenance - Syslog Logging**, показанном ниже.

Рис. 209 Меню 24.3.2: Обслуживание системы – UNIX SYSLOG

```
                Menu 24.3.2 - System Maintenance - UNIX Syslog

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

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

Таблица 122 Меню 24.3.2: Обслуживание системы - UNIX Syslog

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

Таблица 122 Меню 24.3.2: Обслуживание системы - UNIX Syslog (продолжение)

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

P-793H направляет в SYSLOG пять различных типов сообщений. Ниже показаны некоторые примеры сообщений (не все из них относятся строго к P-793H) и описан их формат:

1 CDR

Формат сообщения CDR
SdcmdSyslogSend(SYSLOG_CDR, SYSLOG_INFO, строка); строка = board xx line xx channel xx, call xx, str board = идентификатор платы line = идентификатор платы в сети WAN channel = идентификатор канала в сети WAN call = код вызова, который начинается с 1 и увеличивается на 1 для каждого нового вызова str = C01 - исходящий вызов, dev xx, ch xx (dev:номер устройства, ch:номер канала) L02 - соединение туннеля (L2TP) C02 - соединение исходящего вызова xxxx (скорость соединения) xxxxx (номер вызова удаленной стороны) L02 - завершение вызова C02 - завершение вызова Jul 19 11:19:27 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C01 Outgoing Call dev=2 ch=0 40002 Jul 19 11:19:32 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C02 OutCall Connected 64000 40002 Jul 19 11:20:06 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C02 Call Terminated

2 Триггерный пакет

Формат сообщения о триггерном пакете
SdcmdSyslogSend(SYSLOG_PKTTRI, SYSLOG_NOTICE, строка); строка = Packet trigger: Protocol=xx Data=xxxxxxxxxx…..x Protocol: номер протокола (1:IP 2:IPX 3:IPXHC 4:BPDU 5:ATALK 6:IPNG) Data: 48 шестнадцатеричных символов, отправляемых на сервер. Jul 19 11:28:39 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1, Data=4500003c100100001f010004c0a86614ca849a7b08004a5c020001006162636465666768696a6b6c6d6e6f7071727374 Jul 19 11:28:56 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1, Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e00000000600220008cd40000020405b4 Jul 19 11:29:06 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1, Data=450000282401400001f06ac12c0a86614ca849a7b0427001700195b451d143013500400007 7600000

3 Журнал фильтра

Формат сообщения в журнале фильтра
SdcmdSyslogSend(SYSLOG_FILLOG, SYSLOG_NOTICE, строка); строка = IP[Src=xx.xx.xx.xx Dst=xx.xx.xx.xx prot spo=xxxx dpo=xxxx] S04>R01mD IP[…] расшифровывает заголовок пакета, а S04>R01mD означает набор фильтров 4 (S), правило 1 (R), совпадение (m) и отбрасывание (D). Src: адрес источника Dst: адрес получателя prot: протокол ("TCP","UDP","ICMP") spo: исходный порт dpo: порт на удаленной стороне. Mar 03 10:39:43 202.132.155.97 ZyXEL: GEN[ffffffffffnordff0080] }S05>R01mF Mar 03 10:41:29 202.132.155.97 ZyXEL: GEN[00a0c5f502fnord010080] }S05>R01mF Mar 03 10:41:34 202.132.155.97 ZyXEL: IP[Src=192.168.2.33 Dst=202.132.155.93 ICMP]}S04>R01mF Mar 03 11:59:20 202.132.155.97 ZyXEL: GEN[00a0c5f502fnord010080] }S05>R01mF Mar 03 12:00:52 202.132.155.97 ZyXEL: GEN[ffffffffffff0080] }S05>R01mF Mar 03 12:00:57 202.132.155.97 ZyXEL: GEN[00a0c5f502010080] }S05>R01mF Mar 03 12:01:06 202.132.155.97 ZyXEL: IP[Src=192.168.2.33 Dst=202.132.155.93 TCP spo=01170 dpo=00021]}S04>R01mF

4 Журнал PPP

PPP Log Message Format (Формат сообщения о журнале PPP)
SdcmdSyslogSend(SYSLOG_PPPLOG, SYSLOG_NOTICE, String) (SdcmdSyslogSend(SYSLOG_PPPLOG, SYSLOG_NOTICE, строка)); строка = ppp:prot Starting (запуск) / ppp:prot Opening (открытие) / ppp:prot Closing (закрытие) / ppp:prot Shutdown (завершение) prot = LCP / ATCP / BACP / BCP / CBCP / CCP / CHAP/ PAP / IPCP / IPXCP Jul 19 11:42:44 192.168.102.2 ZyXEL: ppp:LCP Closing Jul 19 11:42:49 192.168.102.2 ZyXEL: ppp:IPCP Closing Jul 19 11:42:54 192.168.102.2 ZyXEL: ppp:CCP Closing

5 Журнал межсетевого экрана

Формат сообщений в журнале межсетевого экрана
SdcmdSyslogSend(SYSLOG_FIREWALL, SYSLOG_NOTICE, buf); buf = IP[Src=xx.xx.xx.xx : spo=xxxx Dst=xx.xx.xx.xx : dpo=xxxx | prot | rule | action] Src: адрес источника spo: порт источника (поле будет пустым, если в отношении исходного порта информация отсутствует) Dst: адрес получателя dpo: порт получателя (поле будет пустым, если в отношении порта получателя информация отсутствует) prot: протокол ("TCP","UDP","ICMP", "IGMP", "GRE", "ESP") rule: правило в формате <a,b> (a - номер набора, b - номер правила). Action: действие: нет (N), запрет (B), пересылка (F) 08-01-200011:48:41Local1.Notice192.168.10.10RAS: FW 172.21.1.80 :137 ->172.21.1.80 :137 |UDP|default permit:<2,0>|B 08-01-200011:48:41Local1.Notice192.168.10.10RAS: FW 192.168.77.88 :520 ->192.168.77.88 :520 |UDP|default permit:<2,0>|B 08-01-200011:48:39Local1.Notice192.168.10.10RAS: FW 172.21.1.50 ->172.21.1.50 |IGMP<2>|default permit:<2,0>|B 08-01-200011:48:39Local1.Notice192.168.10.10RAS: FW 172.21.1.25 ->172.21.1.25 |IGMP<2>|default permit:<2,0>|B

33.5 Диагностика

Средства диагностики позволяют тестировать различные компоненты P-793H для проверки их работоспособности. Меню 24.4 позволяет выбрать один из нескольких диагностических тестов для контроля состояния системы, как показано ниже. Доступные поля будут зависеть от модели устройства.

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

1. В главном меню введите 24, чтобы перейти в меню **Menu 24 - System Maintenance**.
2. В этом меню выберите пункт 4. Diagnostic. Откроется раздел **Menu 24.4 - System Maintenance - Diagnostic**.

Рис. 210 Меню 24.4: Обслуживание системы - диагностика

```
                Menu 24.4 - System Maintenance - Diagnostic

xDSL                                    System
  1.  Reset xDSL                          21. Reboot System
                                          22. Command Mode




TCP/IP
  12. Ping Host




                        Enter Menu Selection Number:

                  Host IP Address= N/A
```

Поля изображенного выше экрана описаны в следующей таблице.

Таблица 123 Меню 24.4: Обслуживание системы – диагностика

ПОЛЕ	ОПИСАНИЕ
Reset xDSL	Введите 1, чтобы сбросить DSL-соединение на порту WAN.
Ping Host	Введите 12 для выполнения эхозапроса любой машины (с IP-адресом) в сети LAN или WAN. Введите IP-адрес в поле **Адрес IP-хоста** внизу.
Reboot System	Введите 11, чтобы перезагрузить P-793H.
Command Mode	Введите 22 для перехода в интерпретатор командной строки (КС) для углубленной диагностики. Войти в интерпретатор команд можно также через меню 24.8.
Host IP Address	Если в поле **Enter Menu Selection Number** был выбран пункт 1, укажите в этом поле IP-адрес компьютера для отправки эхозапроса.
Введите номер пункта или нажмите [ESC] для отмены.	

34

Работа с файлами микропрограмм и настроек

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

34.1 Введение

Для изменения файла настроек и обновления микропрограммы P-793H следуйте указаниям в этой главе. Завершив настройку P-793H, можно сохранить на компьютере резервную копию файла настроек. Это позволяет впоследствии, если настройки P-793H будут ошибочно изменены, восстановить сохраненные значения из резервной копии файла настроек. Можно также загрузить файл с заводскими настройками, если требуется возвратить P-793H к заводским настройкам. Все функции и возможности P-793H реализуются микропрограммой. Обновления микропрограмм для улучшения работы P-793H можно загрузить с веб-сайта компании www.zyxel.ru.

34.2 Принятая схема именования файлов

Файл настроек (часто называемый romfile или rom-0) содержит заводские настройки по умолчанию в меню, такие как пароль, настройка DHCP, настройка TCP/IP и т.д. Поставляется ZyXEL с расширением в имени файла "rom". После настройки параметров устройства P-793H их можно сохранить на своем компьютере, присвоив имя файла по своему усмотрению.

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

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

Это примерный фрагмент FTP-сеанса для передачи файла "firmware.bin" с компьютера в P-793H.

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

Это примерный фрагмент 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-793H принимает только файлы с именами "rom-0" и "ras". Для использования в дальнейшем сохраните неизмененные копии обоих файлов.

Общее описание файлов дано в следующей таблице. Внутренним именем файла называется имя файла в P-793H, а внешним именем файла называется имя файла вне P-793H, например, на диске компьютера, в локальной сети или на FTP-сервере, где оно может быть другим (не изменяется только расширение файла). Загрузив новую микропрограмму, проверьте версию микропрограммы в поле **ZyNOS F/W Version** на экране **Menu 24.2.1 - System Maintenance - Information**. Команда AT – та команда, которая вводится пользователем после нажатия "y" при появлении приглашения в меню SMT для перехода в режим отладки.

Таблица 124 Принятая схема именования файлов

ТИП ФАЙЛА	ВНУТРЕННЕЕ ИМЯ	ВНЕШНЕЕ ИМЯ	ОПИСАНИЕ
Файл настроек	Rom-0	Это имя файла настроек в P-793H. При загрузке файла rom-0 замещается вся файловая система в ПЗУ устройства, включая настройки P-793H, системные данные (в т.ч. пароль по умолчанию), журнал ошибок и журнал трассировки.	*.rom
Микропрограмма	Ras	Это имя файла микропрограммы ZyNOS в P-793H.	*.bin

34.3 Резервное копирование настроек

В меню 24.5, 24.6, 24.7.1 и 24.7.2 устройство P-793H объясняет различные способы резервного копирования, восстановления и загрузки файлов, в зависимости от того, осуществляется ли управление через консольный порт или по Telnet.

Пункт 5 в разделе **Menu 24 - System Maintenance** выполняет резервное копирование текущих настроек P-793H на компьютер. Настоятельно рекомендуется выполнить резервное копирование после того, как устройство P-793H будет приведено в рабочее состояние. Использование протокола FTP – предпочтительный метод резервного копирования текущих настроек на свой компьютер, поскольку он работает быстрее. Выполнять резервное копирование и восстановление в меню 24 можно также через консольный порт. Для этого годится любая программа связи через последовательные порты, однако для передачи и приема файлов необходимо использовать строго протокол Xmodem, а сами файлы не следует переименовывать.

Имейте в виду, что термин "загрузка" предполагает два направления: с P-793H на компьютер, либо с компьютера в P-793H.

34.3.1 Резервное копирование настроек

Следуйте указаниям, приведенным на показанном ниже экране.

Рис. 211 Меню 24.5: Резервное копирование настроек

```
                    Меню 24.5 - резервное копирование настроек

  Для передачи файла настроек на ваш компьютер выполните следующие
  действия:

    1. Запустите FTP-клиент на своем компьютере.
    2. Введите "open" ("открыть") и IP-адрес системы. Затем введите "root" и
       пароль, необходимый для доступа к SMT.
    3. Найдите файл 'rom-0'.
    4. Введите 'get rom-0', чтобы скопировать текущие настройки системы
       на свой компьютер.

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

34.3.2 Выполнение команды FTP из командной строки

1. Запустите FTP-клиент на своем компьютере.
2. Наберите "open", пробел, и укажите IP-адрес P-793H.
3. Когда будет запрошено имя пользователя, нажмите [ENTER].
4. Введите пароль (по умолчанию – "1234").
5. Введите "bin", чтобы установить режим передачи двоичных файлов.
6. Для передачи файлов с P-793H на компьютер используйте команду "get". Например, "get rom-0 config.rom" передает файл настроек с P-793H на компьютер, сохраняя его под именем "config.rom". Подробнее о принятой схеме именования файлов см. выше в данной главе.
7. Введите "quit" для выхода из приглашения FTP.

34.3.3 Пример выполнения команд FTP из командной строки

Рис. 212 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
```

34.3.4 Клиенты FTP на основе графического интерфейса пользователя

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

Таблица 125 Общие команды для клиентов FTP на основе GUI.

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

34.3.5 Управление файлами через WAN

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

1. Активирован сетевой экран (отключите сетевой экран в меню 21.2 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 P-793H немедленно прерывает сеанс Telnet.
5. Выполняется консольная сессия SMT.

34.3.6 Резервное копирование настроек посредством TFTP

P-793H 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-793H и зарегистрируйтесь. Поскольку TFTP не имеет системы проверки безопасности,

P-793H записывает IP-адрес клиента telnet и принимает запросы TFTP только с этого адреса.

2. Находясь в SMT, перейдите в интерпретатор команд (CI), набрав 8 в разделе **Menu 24 – System Maintenance**.
3. Введите команду "sys stdio 0" для отключения времени ожидания SMT, чтобы пересылка TFTP не прерывалась. Введите команду "sys stdio 5" для восстановления пятиминутного времени ожидания SMT (по умолчанию), когда завершится передача файлов.
4. Запустите клиент TFTP на своем компьютере и подключитесь к P-793H. Установите бинарный режим передачи перед тем, как начинать пересылку данных.
5. Используйте клиент TFTP (смотрите пример ниже) для передачи файлов между P-793H и компьютером. Имя файла настроек – "rom-0" (rom-нуль, а не заглавная буква "O").

Обратите внимание на то, что соединение telnet должно быть активным, и SMT должен находиться в режиме CI перед и во время передачи по TFTP. Для дополнительной информации о командах TFTP (смотрите следующий пример) обращайтесь к документации о программе-клиенте TFTP. При работе в системе UNIX используйте команду "get" для передачи файлов с P-793H на компьютер и команду "binary" для установки режима передачи двоичных файлов.

34.3.7 Пример команды TFTP

Ниже дан пример команды TFTP:

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

где "i" указывает на передачу в режиме двоичных файлов (используйте этот режим для передачи нетекстовых файлов), "host" – IP-адрес P-793H, "get" передает исходный файл в P-793H (rom-0, имя файла настроек в P-793H) в целевой файл на компьютере и переименовывает его в config.rom.

34.3.8 Клиенты TFTP на основе графического интерфейса пользователя

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

Таблица 126 Общие команды для клиентов TFTP на основе GUI

КОМАНДА	ОПИСАНИЕ
Host	Введите IP-адрес P-793H. 192.168.1.1 – заводской IP-адрес P-793H.
Send/Fetch	"Send" ("Отправить") используется для загрузки файла в P-793H, а "Fetch" ("Получить") – для резервного копирования файла на компьютер.
Local File	Введите путь и имя файла микропрограммы (расширение *.bin) или файл настроек (расширение *.rom) в своем компьютере.
Remote File	Это имя файла настроек в P-793H. Имя файла микропрограммы - "ras", а для файла настроек – "rom-0".
Binary	Передача файла в бинарном режиме.
Abort	Остановка передачи файла.

Настройки, запрещающие доступ по TFTP или FTP через WAN, описаны в разд. 34.3.5 на стр. 348.

34.3.9 Резервное копирование через консольный порт

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

1 Откройте меню 24.5 и введите "y" на следующем экране.

Рис. 213 Обслуживание системы: резервное копирование настроек

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

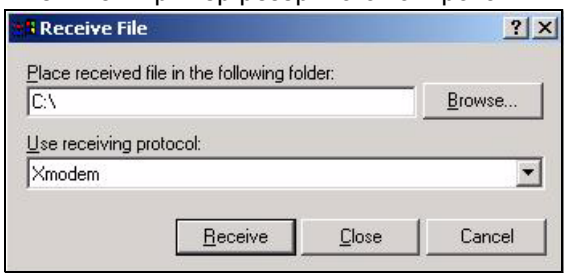
2 Следующий экран означает, что прием файла по протоколу Xmodem начался.

Рис. 214 Обслуживание системы: экран начала приема файла по Xmodem

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

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

Рис. 215 Пример резервного копирования настроек



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

Выберите протокол **Xmodem**.

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

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

Рис. 216 Экран подтверждения выполнения резервного копирования

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

34.4 Восстановление настроек

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

FTP – предпочтительный метод восстановления текущих настроек P-793H с компьютера, поскольку FTP работает быстрее. Имейте в виду, что необходимо подождать, пока система не перезапустится автоматически после того, как завершится передача файла.

Не прерывайте процесс передачи файлов, иначе P-793H может НЕОБРАТИМО ВЫЙТИ ИЗ СТРОЯ. После завершения восстановления настроек P-793H автоматически перезагрузится.

34.4.1 Восстановление с использованием FTP

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

Рис. 217 Меню 24.6: Восстановление настроек

```
                    Меню 24.6 - восстановление настроек

Для передачи файла микропрограммы или настроек выполните следующие
действия:

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

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

1. Запустите FTP-клиент на своем компьютере.
2. Наберите "open", пробел, и укажите IP-адрес P-793H.
3. Нажмите [ENTER], когда потребуется имя пользователя.
4. Введите пароль (по умолчанию – "1234").

5 Введите "bin", чтобы установить режим передачи двоичных файлов.
6 На компьютере найдите файл "rom" для передачи в P-793H.
7 Используйте " put" для передачи файлов с компьютера на P-793H, например, команда "put config.rom-0" вызывает передачу файла настроек "config.rom", находящегося на компьютере, в P-793H. Подробнее о принятой схеме именования файлов см. выше в данной главе.
8 Введите "quit" для выхода из приглашения FTP. P-793H автоматически перезагружается после успешного выполнения процесса восстановления.

34.4.2 Пример восстановления с использованием сеанса FTP

Рис. 218 Пример восстановления с использованием сеанса FTP

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

Подробнее о настройках, запрещающих доступ по TFTP и FTP из сети WAN, см. в разд. 34.3.5 на стр. 348.

34.4.3 Восстановление через консольный порт

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

1 Откройте меню 24.6 и введите "y" на следующем экране.

Рис. 219 Обслуживание системы: восстановление настроек

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

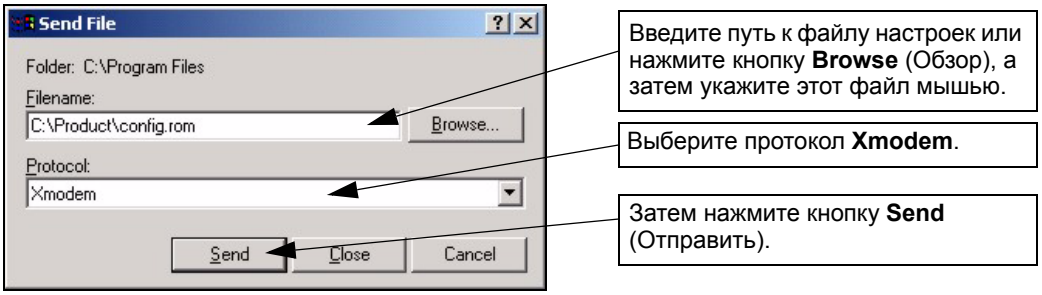
2 Следующий экран означает, что прием файла по протоколу Xmodem начался.

Рис. 220 Обслуживание системы: экран начала приема файла по Xmodem

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

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

Рис. 221 Пример восстановления настроек



4 После успешного восстановления настроек появится следующий экран. Нажмите любую клавишу, чтобы перезагрузить P-793H и возвратиться в меню SMT.

Рис. 222 Экран подтверждения восстановления настроек

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

34.5 Загрузка микропрограммы и файлов настроек в устройство

В этом разделе описано, как загружать в устройство микропрограмму и файлы настроек. Для загрузки файлов настроек в устройство можно руководствоваться разд. 34.4 на стр. 351 или указаниями на экране **Menu 24.7.2 - System Maintenance - Upload System Configuration File** (при доступе через консольный порт).

Не прерывайте процесс передачи файлов, иначе P-793H может НЕОБРАТИМО ВЫЙТИ ИЗ СТРОЯ.

34.5.1 Загрузка файла микропрограммы в устройство

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

Если доступ к P-793H осуществляется по протоколу Telnet, вы увидите следующие экраны, описывающие порядок загрузки микропрограмм и файлов настроек по FTP.

Рис. 223 Меню 24.7.1: Обслуживание системы – загрузка микропрограммы

```
 Меню 24.7.1 - обслуживание системы - загрузка микропрограммы в систему

Для загрузки микропрограммы в систему выполните следующие действия:

  1. Запустите FTP-клиент на вашей рабочей станции.
  2. Наберите "open" и укажите IP-адрес вашей системы.  Затем введите
     "root" и пароль, необходимый для доступа к SMT.
  3. Введите "put файл_микропрограммы ras", где "файл_микропрограммы"
     - имя файла с обновлением микропрограммы на рабочей станции, а "ras"
     - имя файла на удаленной системе.
  4. После успешного обновления микропрограммы система автоматически
     перезагрузится.

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

34.5.2 Загрузка файла настроек в устройство

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

Рис. 224 Меню 24.7.2: Обслуживание системы – загрузка файла настроек

```
    Меню 24.7.2 - обслуживание системы - загрузка файла настроек в систему

Чтобы загрузить файл настроек, выполните следующие действия:

  1. Запустите FTP-клиент на вашей рабочей станции.
  2. Наберите "open" и укажите IP-адрес вашей системы. Затем введите
     "root"и пароль, необходимый для доступа к SMT.
  3. Введите "put файл_настроек rom-0", где "файл_настроек" - имя файла
     настроек на рабочей станции. В системе файл будет переименован
     в "rom-0".
  4. После завершения загрузки файла настроек система автоматически
     перезагрузится.

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

Для загрузки микропрограммы и файла настроек следуйте приведенным ниже примерам.

34.5.3 Пример команды загрузки файла по FTP из приглашения DOS

1. Запустите FTP-клиент на своем компьютере.
2. Наберите "open", пробел, и укажите IP-адрес P-793H.
3. Когда будет запрошено имя пользователя, нажмите [ENTER].

4 Введите пароль (по умолчанию – "1234").
5 Введите "bin", чтобы установить режим передачи двоичных файлов.
6 Для передачи файлов с компьютера в P-793H используйте команду "put". Например, "put firmware.bin ras" передает микропрограмму с компьютера (firmware.bin) в P-793H и переименовывает ее в "ras". Подобным образом команда "put config.rom rom-0" передает файл настроек с компьютера (config.rom) в P-793H, переименовывая его в "rom-0". Аналогичным образом "get rom-0 config.rom" обеспечивает передачу файла настроек с P-793H 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.

34.5.4 Пример сессии FTP для загрузки файла микропрограммы

Рис. 225 Пример сессии FTP для загрузки файла микропрограммы

```
331 Enter PASS command
Password:
230 Logged in
ftp>bin
200 Type I OK
ftp> put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 1103936 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

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

Настройки, запрещающие доступ по TFTP или FTP через WAN, описаны в разд. 34.3.5 на стр. 348.

34.5.5 Загрузка файла по протоколу TFTP

P-793H также поддерживает загрузку файлов микропрограмм через локальную сеть с использованием TFTP (упрощенного протокола передачи файлов). Хотя TFTP тоже должен работать через WAN, это не рекомендуется.

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

1 Используйте telnet со своего компьютера для подключения к устройству P-793H и зарегистрируйтесь. Поскольку TFTP не имеет системы проверки безопасности, P-793H записывает IP-адрес клиента telnet и принимает запросы TFTP только с этого адреса.
2 Находясь в SMT, перейдите в интерпретатор команд (CI), набрав 8 в разделе **Menu 24 – System Maintenance**.
3 Введите команду "sys stdio 0" для отключения времени ожидания, чтобы пересылка TFTP не прерывалась. Введите команду "command sys stdio 5" для

восстановления пятиминутного времени ожидания консоли (по умолчанию), когда завершится передача файлов.

4. Запустите клиент TFTP на своем компьютере и подключитесь к P-793H. Установите бинарный режим передачи перед тем, как начинать пересылку данных.
5. Используйте клиент TFTP (смотрите пример ниже) для передачи файлов между P-793H и компьютером. Имя файла микропрограммы – "ras".

Обратите внимание, что до и во время передачи по TFTP Telnet-соединение должно быть активным, а устройство P-793H должно находиться в режиме командной строки. Для дополнительной информации о командах TFTP (смотрите следующий пример) обращайтесь к документации о программе-клиенте TFTP. При работе в системе UNIX используйте команду "get" для передачи от P-793H к компьютеру, "put" – в обратном направлении и "binary" для установки режима бинарной передачи.

34.5.6 Пример команды загрузки по TFTP

Ниже дан пример команды TFTP:

```
tftp [-i] host put firmware.bin ras
```

где "i" указывает на передачу в режиме двоичных файлов (используйте этот режим для передачи нетекстовых файлов), "host" – IP-адрес P-793H, "put" передает исходный файл с компьютера (firmware.bin - имя файла микропрограммы на компьютере) в целевой файл на P-793H и переименовывает его в ras.

Команды, имеющиеся в клиентах TFTP на основе GUI, перечислены выше в данной главе.

34.5.7 Загрузка файлов в устройство через консольный порт

FTP и TFTP – рекомендуемые протоколы для загрузки микропрограмм в P-793H. Однако в случае недоступности устройства по сети загрузить файлы в P-793H можно только по прямому соединению через консольный порт. В обычных случаях прибегать к загрузке через консольный порт не рекомендуется, поскольку FTP и TFTP отличаются намного большей скоростью. Для загрузки файлов годится любая программа связи через последовательные порты, однако для передачи и приема необходимо использовать строго протокол Xmodem.

34.5.8 Загрузка файлов микропрограммы через консольный порт

1. Находясь в разделе меню "Menu 24.7 – System Maintenance – Upload Firmware", введите 1, чтобы перейти на экран "Menu 24.7.1 - System Maintenance - Upload System Firmware", и следуйте указаниям на экране.

Рис. 226 Меню 24.7.1 При доступе через консольный порт

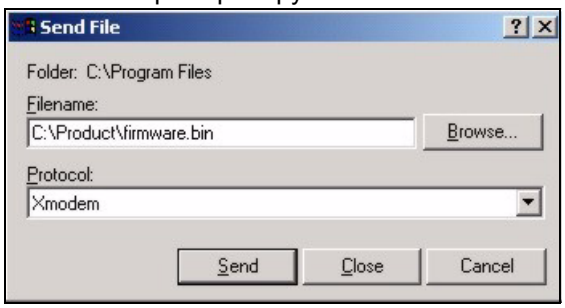
```
Меню 24.7.1 - обслуживание системы - загрузка микропрограммы в систему

Для загрузки новой микропрограммы в систему:
1. Введите "y" в следующем приглашении, чтобы войти в отладочный режим.
2. После появления сообщения "Enter Debug Mode" введите "atur".
3. Дождитесь сообщения о готовности к загрузке по Xmodem ("Starting XMODEM upload"),
   после чего начните загрузку по Xmodem в вашем терминале.
4. Если загрузка микропрограммы успешно завершена, введите "atgo", чтобы
   перезагрузить маршрутизатор.

Внимание: загрузка приведет к удалению текущей микропрограммы.

     Продолжить? (Y - да, N - нет)
```

2 После появления сообщения "Starting Xmodem upload" запустите протокол Xmodem на компьютере. Для программы HyperTerminal следуйте указаниям, приведенным выше. Для других коммуникационных программ порядок действий будет аналогичным.

34.5.9 Пример загрузки файла микропрограммы по протоколу Xmodem с помощью программы HyperTerminal

Нажмите **Transfer** (Передача), затем **Send File** (Отправить файл). Появится следующий экран.

Рис. 227 Пример загрузки Xmodem



По завершении загрузки микропрограммы P-793H автоматически перезагрузится.

34.5.10 Загрузка файлов настроек через консольный порт

1 В разделе "Menu 24.7 – System Maintenance – Upload Firmware" выберите 2, чтобы перейти на экран "Menu 24.7.2 - System Maintenance - Upload System Configuration File". Следуйте указаниям, приведенным на показанном ниже экране.

Рис. 228 Меню 24.7.2 При доступе через консольный порт

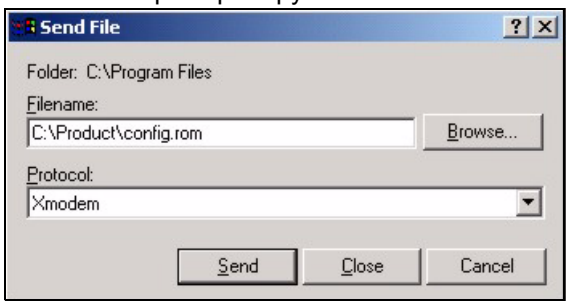
```
Меню 24.7.2 - обслуживание системы - загрузка файла настроек в систему

Для загрузки файла настроек в систему:
1. Введите "y" в следующем приглашении, чтобы войти в отладочный режим.
2. После появления сообщения "Enter Debug Mode" введите "atlc".
3. Дождитесь сообщения о готовности к загрузке по Xmodem ("Starting
   XMODEM upload"), после чего начните загрузку по Xmodem в вашем
   терминале.
4. Если загрузка успешно завершена, введите "atgo", чтобы перезагрузить
   систему.

Внимание:
1. Загрузка приведет к удалению текущего файла настроек.
2. После перезапуска скорость консольного порта (см. меню 24.2.2) может
   измениться. В этом случае потребуется перенастроить скорость в
   программе терминала. Пароль также может измениться (см. меню 23).
3. В случае загрузки файла настроек по умолчанию скорость консольного
   порта сменится на 9600 бит/с, а пароль - на "1234".

          Продолжить? (Y - да, N - нет)
```

2. После появления сообщения "Starting Xmodem upload" запустите протокол Xmodem на компьютере. Для программы HyperTerminal следуйте указаниям, приведенным выше. Для других коммуникационных программ порядок действий будет аналогичным.
3. Введите "atgo", чтобы перезагрузить P-793H.

34.5.11 Пример загрузки файла настроек по протоколу Xmodem с помощью программы HyperTerminal

Нажмите **Transfer** (Передача), затем **Send File** (Отправить файл). Появится следующий экран.

Рис. 229 Пример загрузки по Xmodem



По завершении загрузки настроек необходимо перезагрузить P-793H, набрав команду "atgo".

35

Разделы меню с 24.8 по 24.11

В этой главе рассматриваются меню SMT 24.8 – 24.11.

35.1 Режим интерпретатора команд

Интерпретатор командной строки (КС) является частью микропрограммы маршрутизатора. CI обеспечивает почти те же функциональные возможности, что и SMT, а также некоторые функции настройки низкого уровня и диагностики. Введите CI из SMT, выбрав меню 24.8. Командная строка доступна по Telnet и на консольном порту. При этом некоторые команды доступны только через консольный порт. Подробную информацию о командах см. на прилагающемся компакт-диске или на www.zyxel.ru. В меню **Menu 24 - System Maintenance** введите 8.

Использование недокументированных команд или некорректное выполнение настроек может нарушить работоспособность устройства или вывести его из строя.

Рис. 230 Режим команд в меню 24

```
                Menu 24 - System Maintenance

                1.  System Status
                2.  System Information and Console Port Speed
                3.  Log and Trace
                4.  Diagnostic
                5.  Backup Configuration
                6.  Restore Configuration
                7.  Upload Firmware
                8.  Command Interpreter Mode
                9.  Call Control
                10. Time and Date Setting
                11. Remote Management
```

35.1.1 Синтаксис команд

Ключевые слова команд приводятся шрифтом `Courier New`.

Введите ключевые слова команд именно так, как показано ниже, не сокращая.

Обязательные поля команды заключены в угловые скобки <>.

Необязательные поля команды заключены в квадратные скобки [].

Знак "|" означает "или".

Например,

```
sys filter netbios config <type> <on|off>
```

означает, что необходимо указать тип фильтра netbios и то, нужно ли его включить или выключить.

35.1.2 Использование команд

Чтобы получить список команд, в приглашении командной строки введите help или ?. Всегда вводите команду полностью. Введите "exit" для возвращения в главное меню SMT после завершения действий.

Рис. 231 Допустимые команды

```
Copyright (c) 1994 - 2006 ZyXEL Communications Corp.
P-793H> ?
Valid commands are:
sys             exit            device          ether
wan             poe             xdsl            aux
config          ip              ipsec           ppp
bridge          hdap            bm              lan
P-793H>
```

35.2 Поддержка управления вызовами

В P-793H предусмотрена функция управления вызовами для реализации бюджетных ограничений. Необходимо учесть, что это меню применяется только в том случае, когда в поле **Encapsulation** в меню 4 или 11.1 выбран режим **PPPoE** или **PPPoA**.

Функция управления бюджетом позволяет лимитировать суммарную продолжительность исходящих вызовов на P-793H за определенный период времени. Если общее время исходящих вызовов превышает лимит, текущий вызов отбрасывается и все последующие исходящие вызовы блокируются.

История вызовов содержит сведения о предыдущих входящих и исходящих вызовах.

Для доступа к меню управления вызовом выберите пункт 9 в меню 24, чтобы перейти в раздел **Menu 24.9 — System Maintenance — Call Control**, показанный ниже.

Рис. 232 Меню 24.9: Обслуживание системы – управление вызовами

```
                Menu 24.9 - System Maintenance - Call Control

                  1. Budget Management
```

35.2.1 Управление бюджетом

В меню 24.9.1 показаны статистические данные об управлении бюджетом для исходящих вызовов. Введите 1 в разделе **Menu 24.9 - System Maintenance - Call Control** для открытия показанного ниже меню. Доступные поля будут зависеть от модели устройства.

Рис. 233 Меню 24.9.1 – Управление бюджетом

```
                    Menu 24.9.1 - Budget Management

  Remote Node   Connection Time/Total Budget   Elapsed Time/Total Period

1.MyISP                   No Budget                   No Budget
2.--------                    ---                         ---
3.--------                    ---                         ---
4.--------                    ---                         ---
5.--------                    ---                         ---
6.--------                    ---                         ---
7.--------                    ---                         ---
8.--------                    ---                         ---
```

Общий бюджет – лимит времени в аккумулированном периоде для вызовов, исходящих по направлению к удаленному узлу. Когда этот лимит достигнут, вызов отбрасывается и дальнейшие исходящие вызовы на этот удаленный узел блокируются. После завершения каждого периода общий бюджет сбрасывается. Значение по умолчанию для общего бюджета – 0 минут, период – 0 часов, что означает отсутствие управления бюджетом. Можно сбросить аккумулированное время соединения в этом меню, введя индекс удаленного узла. Введите 0 для обновления этого экрана. Бюджет и период сброса можно настроить в меню 11.1 для удаленного узла.

Таблица 127 Меню 24.9.1 – Управление бюджетом

ПОЛЕ	ОПИСАНИЕ	ПРИМЕР
Remote Node	Введите порядковый номер удаленного узла, который необходимо сбросить (в данном случае только один).	1
Connection Time/ Total Budget	Это – общее истекшее время соединения (в пределах выделенного бюджета, установленного в меню 11.1).	5/10 означает, что израсходовано 5 минут из выделенных 10 минут.
Elapsed Time/Total Period	Этот период – цикл времени в часах, в соответствии с которым сбрасывается выделенный бюджет (см. меню 11.1). Время работы – это время, использованное в пределах данного периода.	0.5/1 означает, что израсходовано 30 минут из выделенного 1 часа.
Введите "0" для обновления экрана или нажмите [ESC] для возвращения к предыдущему экрану.		

35.3 Установка даты и времени

В устройстве P-793H имеются часы реального времени, хранящие текущее время и дату. Имеется также программный механизм установки времени вручную или получения текущего времени и даты с внешнего сервера при включении P-793H. Меню 24.10 позволяет обновить текущую дату и время в P-793H. После этого в журналах ошибок и сетевого экрана P-793H будет отображаться текущее время.

Выберите меню 24 в главном меню для открытия меню **Menu 24 - System Maintenance**, как показано ниже.

Рис. 234 Меню 24: Обслуживание системы

```
                    Menu 24 - System Maintenance

                  1.  System Status
                  2.  System Information and Console Port Speed
                  3.  Log and Trace
                  4.  Diagnostic
                  5.  Backup Configuration
                  6.  Restore Configuration
                  7.  Upload Firmware
                  8.  Command Interpreter Mode
                  9.  Call Control
                  10. Time and Date Setting
                  11. Remote Management
```

Чтобы изменить настройки даты и времени в P-793H, перейдите в раздел **Menu 24.10 - System Maintenance - Time and Date Setting**, показанный на следующем рисунке.

Рис. 235 Меню 24.10: Управление системой – настройка времени и даты

```
        Menu 24.10 - System Maintenance - Time and Date Setting

     Time Protocol= None
     Time Server Address= N/A

     Current Time:                        06 : 43 : 17
     New Time (hh:mm:ss):                 06 : 43 : 00

     Current Date:                        2000 - 01 - 01
     New Date (yyyy-mm-dd):               2000 - 01 - 01

     Time Zone= (GMT+0100) Brussels, Copenhagen, Madrid, Paris

     Daylight Saving= No
Start Date (mm-nth-week-hr):          Jan. - 1st  - Sun.(02)  - 00
End Date (mm-nth-week-hr):            Jan. - 1st  - Sun.(02)  - 00
```

Поля изображенного выше экрана описаны в следующей таблице.

Таблица 128 Меню 24.10: Управление системой – настройка времени и даты

ПОЛЕ	ОПИСАНИЕ
Time Protocol	Укажите протокол, используемый сервером точного времени. Не все серверы точного времени поддерживают полный набор протоколов; обратитесь к оператору/администратору сети или подберите работающий протокол методом проб и ошибок. В основном они отличаются форматом. Формат **Daytime (RFC 867)**: день/месяц/год/часовой пояс, в котором находится сервер. Формат **Time (RFC-868)**: целое число длиной 4 байта, означающее количество секунд, прошедшее с 0:0:0 01.01.1970 (1970/1/1 в 0:0:0). По умолчанию используется протокол **NTP (RFC-1305)**, являющийся аналогом протокола **Time (RFC-868)**. Выберите **None**, чтобы вручную задать новое время и дату.
Time Server Address	Введите IP-адрес или имя домена сервера времени. Если вы не уверены в том, какие значения требуется ввести, обратитесь к провайдеру или администратору сети. Значение по умолчанию – tick.stdtime.gov.tw
Current Time	В этом поле отображается обновленное время только после повторного входа в это меню.
New Time (hh:mm:ss)	Введите новое время в формате "часы : минуты : секунды". Это поле доступно в том случае, если в поле **Time Protocol** выбрано значение **None**.
Current Date	В этом поле отображается обновленная дата только после повторного входа в это меню.
New Date (yyyy-mm-dd)	Введите новую дату в формате "год – месяц – день". Это поле доступно в том случае, если в поле **Time Protocol** выбрано значение **None**.
Time Zone	Нажмите пробел и [ENTER] для установки разницы во времени между данной временной зоной и гринвичским временем (GMT).
Daylight Saving	Летнее время – это период между поздней весной и началом осени, когда во многих странах стрелки переводятся вперед на 1 час по отношению к обычному местному времени, чтобы продлить светлое время в конце дня. Если нужно использовать переход на летнее время, выберите **Yes (Да)**.
Start Date (mm-nth-week-hr):	Укажите месяц и день перехода на летнее время, если в поле **Enable Daylight Saving** (Разрешить переход на летнее время) выбрано значение **Yes**. В поле **hr** используется 24-часовой формат. Примеры: На большей части территории США летнее время начинается в первое воскресенье апреля. Для каждого часового пояса летнее время в США начинает действовать с 2:00 по местному времени. В США необходимо выбрать **Apr.**, **1st**, **Sun.** и ввести 02 в поле **hr**. В Европейском союзе и в России летнее время начинается в последнее воскресенье марта. Во всех часовых поясах на территории Евросоюза летнее время начинается одновременно (в 1:00 по Гринвичу или UTC). В странах Евросоюза необходимо выбрать **Mar.**, **Last**, **Sun.** Время, вводимое в поле **hr**, зависит от вашего часового пояса. Например, для Германии, где время на один час опережает гринвичское (GMT+1), следует ввести 2.

Таблица 128 Меню 24.10: Управление системой – настройка времени и даты

ПОЛЕ	ОПИСАНИЕ
End Date (mm-nth-week-hr)	Укажите месяц и день перехода на зимнее время, если в поле **Enable Daylight Saving** (Разрешить переход на летнее время) выбрано значение **Yes**. В поле **hr** используется 24-часовой формат. Примеры: 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. В США необходимо выбрать **Oct.**, **Last**, **Sun.** и ввести 02 в поле **hr**. В Европейском союзе и в России летнее время заканчивается в последнее воскресенье октября. Во всех часовых поясах на территории Евросоюза летнее время заканчивается одновременно (в 1:00 по Гринвичу или UTC). В странах Евросоюза необходимо выбрать **Oct.**, **Last**, **Sun.** Время, вводимое в поле **hr**, зависит от вашего часового пояса. Например, для Германии, где время на один час опережает гринвичское (GMT+1), следует ввести 2.
После завершения работы с данным меню нажмите клавишу [ENTER] в сообщении "Press ENTER to Confirm or ESC to Cancel" для сохранения настроек или клавишу [ESC] для отмены.	

35.4 Удаленное управление

Для отключения удаленного доступа через одну из служб выберите **Disable** в соответствующем поле **Server Access**. Введите 11 в меню 24, чтобы открыть раздел **Menu 24.11 – Remote Management Control**.

Рис. 236 Menu 24.11 – Настройка удаленного управления

```
                Menu 24.11 - Remote Management Control

TELNET Server:
  Server Port = 23                  Server Access = ALL
  Secured Client IP = 0.0.0.0

FTP Server:
  Server Port = 21                  Server Access = ALL
  Secured Client IP = 0.0.0.0

Web Server:
  Server Port = 80                  Server Access = ALL
  Secured Client IP = 0.0.0.0
```

Поля изображенного выше экрана описаны в следующей таблице.

Таблица 129 Меню 24.11 – Настройка удаленного управления

ПОЛЕ	ОПИСАНИЕ
TELNET Server FTP Server Web Server	Каждое из этих нередактируемых полей обозначает тип сетевой службы, используемой для дистанционного управления P-793H.
Server Port	В данном поле показан номер порта для службы или протокола. При необходимости можно изменить номер порта, но для доступа к P-793H можно использовать только этот номер порта.

Таблица 129 Меню 24.11 – Настройка удаленного управления (продолжение)

ПОЛЕ	ОПИСАНИЕ
Server Access	Если требуется указать интерфейс доступа, нажмите пробел и [ENTER], чтобы выбрать один из следующих вариантов: **LAN only (Только LAN)**, **WAN only (ТолькоWAN)**, **ALL (ВСЕ)** или **Disable (Отключить)**.
Secured Client IP	Значение по умолчанию 0.0.0.0 позволяет любому клиенту использовать эту службу или протокол для дистанционного управления P-793H. Введите IP-адрес для ограничения доступа к клиенту с соответствующим IP-адресом.
После завершения работы с данным меню нажмите клавишу [ENTER] в сообщении "Press ENTER to Confirm or ESC to Cancel" для сохранения настроек или клавишу [ESC] для отмены.	

35.4.1 Ограничения удаленного управления

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

1. Фильтр в меню 3.1 (LAN) или в меню 11.5 (WAN) применяется для блокировки служб Telnet, FTP или веб-служб.
2. Данная служба отключена в меню 24.11.
3. IP-адрес в поле **Secured Client IP (Надежный IP-адрес клиента)** (меню 24.11) не соответствует IP-адресу клиента. При таком несоответствии P-793H немедленно прерывает сеанс.
4. Выполняется консольная сессия SMT.
5. Уже выполняется другой сеанс удаленного управления с равным или более высоким приоритетом. В каждый момент времени может выполняться только один сеанс удаленного управления.
6. Правило межсетевого экрана блокирует удаленное управление.

36

Настройка политик маршрутизации IP

Это меню служит для просмотра и настройки политик маршрутизации.

36.1 Назначение политик маршрутизации

Обычно решения о маршрутизации принимаются только по адресу получателя, и P-793H выбирает для отправки пакета кратчайший путь. Политика маршрутизации IP (IPPR) реализует алгоритм, заменяющий стандартный механизм маршрутизации и позволяющий изменить правила пересылки пакетов в зависимости от политики, настраиваемой администратором. Политики применяются ко входящим пакетам на каждом интерфейсе до обычной маршрутизации.

36.2 Преимущества

- Маршрутизация на основе источников – администраторы сетей могут использовать маршрутизацию на основе политик для пересылки трафика от различных пользователей по разным соединениям.
- Ограничение полосы пропускания – применение политик маршрутизации в корпоративной среде позволяет классифицировать трафик по приоритетам, распределяя полосу пропускания требуемым образом.
- Экономия – IPPR позволяет организациям направлять ценный интерактивный трафик через дорогостоящие широкополосные каналы, а для пакетных передач использовать более дешевые маршруты.
- Распределение нагрузки – администраторы сетей могут использовать IPPR для распределения трафика по нескольким путям.
- NAT – P-793H по умолчанию применяет NAT к трафику, проходящему через интерфейс **ge1**. Защищенный механизм трансляции адресов (SNAT), реализуемый политиками маршрутизации, позволяет администраторам задавать определенный IP-адрес источника для трафика, принимаемого через определенные интерфейсы.

36.3 Политики маршрутизации

Отдельные политики маршрутизации являются частью общей схемы IPPR. Политика определяет критерии сравнения и действия, выполняемые над пакетами, которые отвечают этим критериям. Действие выполняется только при удовлетворении всем критериям. Критериями могут являться: имя пользователя, исходный адрес и входной интерфейс, адрес получателя, расписание, протокол IP (ICMP, UDP, TCP и т. п.) и номер порта.

Могут выполняться следующие действия:

- Пересылка пакета через другой шлюз, выходной интерфейс, туннель VPN или группу каналов.
- Ограничение доступной полосы пропускания и упорядочение трафика по приоритетам.

Структура и реализация IPPR во многом повторяет существующее средство фильтрации пакетов в составе RAS.

36.4 Настройка политик маршрутизации IP

Это меню служит для просмотра сводки политик маршрутизации. Чтобы открыть это меню, в основном меню введите 25.

Рис. 237 Меню 25: Настройка политик маршрутизации IP

```
                    Menu 25 - IP Routing Policy Setup

Policy                                  Policy
Set #         Name                      Set #         Name
------  -----------------               ------  -----------------
  1      _________________                 7      _________________
  2      _________________                 8      _________________
  3      _________________                 9      _________________
  4      _________________                10      _________________
  5      _________________                11      _________________
  6      _________________                12      _________________



               Enter Policy Set Number to Configure= 0

               Edit Name= N/A
```

1. Выберите набор фильтров, которые необходимо настроить (1-12), и нажмите [ENTER].
2. Введите описательное название или комментарий в поле **Edit Name** и нажмите [ENTER].
3. В сообщении [Press ENTER to confirm] нажмите [ENTER], чтобы войти в раздел **Menu 25.1 - IP Routing Policy Setup**.

36.5 Настройка политик маршрутизации IP

Этот раздел меню служит для поиска политик маршрутизации. Для входа в это меню укажите номер и название политики маршрутизации из меню 25.

Рис. 238 Меню 25.1: Настройка политик маршрутизации IP

```
                    Menu 25.1 - IP Routing Policy Setup

# A                          Criteria/Action
- - ------------------------------------------------------------------------
1 N SA=1.1.1.1-1.1.1.1 DA=2.2.2.2-2.2.2.5
     SP=20-25 DP=20-25 P=6 T=NM PR=0      |GW=192.168.1.1 T=MT PR=0
2 N ____________________________________________________________________________
    ____________________________________________________________________________
3 N ____________________________________________________________________________
    ____________________________________________________________________________
4 N ____________________________________________________________________________
    ____________________________________________________________________________
5 N ____________________________________________________________________________
    ____________________________________________________________________________
6 N ____________________________________________________________________________
    ____________________________________________________________________________

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

Поля изображенного выше экрана описаны в следующей таблице.

Таблица 130 Меню 25.1: Настройка политик маршрутизации IP

ПОЛЕ	ОПИСАНИЕ
#	В этом поле отображается номер правила.
Criteria/Action	См. таб. 131 на стр. 369.
Enter Policy Rule Number (1-6) to Configure:	Введите номер редактируемого правила.

Таблица 131 Меню 25: Настройка политик маршрутизации IP, сокращения

СОКРАЩЕНИЕ	ЗНАЧЕНИЕ
SA	IP-адрес источника
SP	Порт источника
DA	IP-адрес получателя
DP	Порт получателя
P	Номер IP-протокола 4-го уровня (TCP=6, UDP=17…)
T	Тип обслуживания (ToS) во входящем пакете
PR	Приоритет входящего пакета
Действия: GW	IP-адрес шлюза
T	Тип службы для исходящего трафика
P	Приоритет исходящего трафика
Уровень обслуживания: NM	Обычный
MD	Минимальная задержка
MT	Максимальная пропускная способность

Таблица 131 Меню 25: Настройка политик маршрутизации IP, сокращения

СОКРАЩЕНИЕ	ЗНАЧЕНИЕ
MR	Максимальная надежность
MC	Минимальная стоимость

36.6 Меню IP Routing Policy

Это меню служит для настройки маршрутов в соответствии с политиками. Для входа в это меню, находясь в меню 25, выберите **Edit** и введите соответствующий номер правила.

Рис. 239 Меню 25.1.1: Меню IP Routing Policy

```
                    Menu 25.1.1 - IP Routing Policy

          Policy Set Name= ex1
          Active= No
          Criteria:
            IP Protocol    = 0
            Type of Service= Don't Care           Packet length= 0
            Precedence     = Don't Care             Len Comp= N/A
            Source:
              addr start= 0.0.0.0                 end= N/A
              port start= N/A                     end= N/A
            Destination:
              addr start= 0.0.0.0                 end= N/A
              port start= N/A                     end= N/A
          Action= Matched
            Gateway addr   = 0.0.0.0              Log= No
            Type of Service= No Change
            Precedence     = No Change
```

Поля изображенного выше экрана описаны в следующей таблице.

Таблица 132 Меню 25.1.1: Политика маршрутизации IP

ПОЛЕ	ОПИСАНИЕ
Policy Set Name	В этом поле указывается описательное название политики маршрутизации, выбранной в меню **Menu 25.1 - IP Routing Policy Summary**.
Active	Чтобы активировать политику, выберите **Yes**, нажав пробел и [ENTER].
Criteria	
IP Protocol	Введите номер протокола уровня 4 IP. Например, UDP=17, TCP=6, ICMP=1, любой протокол=0.
Type of Service	Укажите приоритет входящего трафика: **Don't Care** (не имеет значения), **Normal** (нормальный), **Min Delay** (минимальная задержка), **Max Thruput** (максимальная скорость передачи) и **Max Reliable** (максимальная надежность).
Precedence	Приоритет входящего пакета. Нажмите пробел и [ENTER], чтобы выбрать приоритет из списка: от **0** до **7** или **Don't Care** (не имеет значения).
Packet Length	Введите длину входящих пакетов (в байтах). Операторы в следующем поле (**Len Comp**) применяются к пакетам этой длины.

Таблица 132 Меню 25.1.1: Политика маршрутизации IP (продолжение)

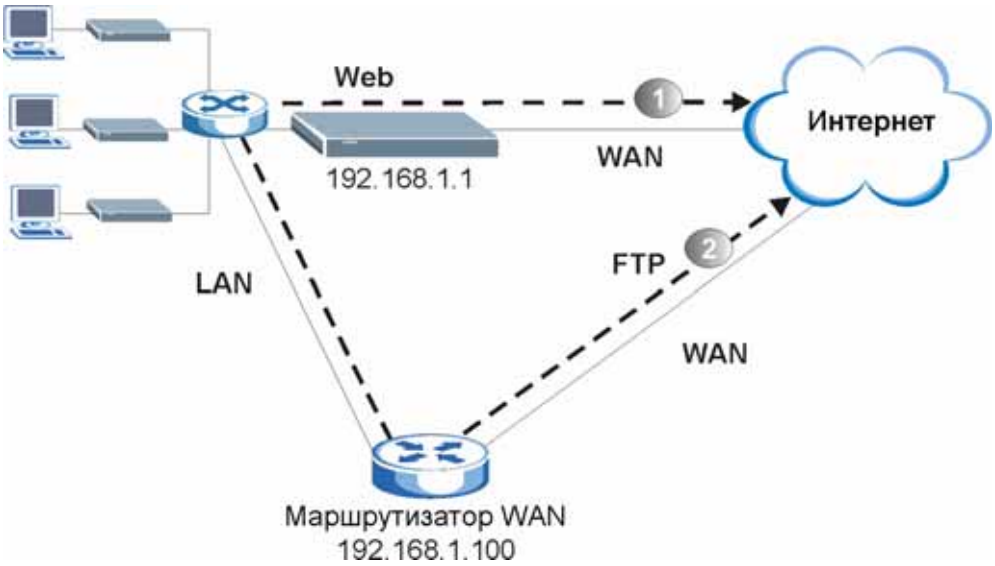
ПОЛЕ	ОПИСАНИЕ
Len Comp	Нажмите пробел и ENTER, чтобы выбрать критерий сравнения длины:**Equal** (равно), **Not Equal** (не равно), **Less** (меньше), **Greater** (больше), **Less or Equal** (меньше или равно) или **Greater or Equal** (больше или равно).
Source	
addr start / end	Начало и конец диапазона IP-адресов источника.
port start / end	Начало и конец диапазона номеров портов источника (только для протоколов TCP/UDP).
Destination	
addr start / end	Начало и конец диапазона IP-адресов адресата.
port start / end	Начало и конец диапазона номеров портов адресата (только для протоколов TCP/UDP).
Action	Указывает, должно ли описанное действие выполняться при соответствии или несоответствии критериям.
Gateway addr	Введите IP-адрес шлюза, на который устройство P-793H пересылает пакет. Шлюз должен непосредственно соседствовать с P-793H, находясь в одной подсети с P-793H, если он относится к сети LAN, или иметь IP-адрес удаленного узла, если он относится к сети WAN. Чтобы указать шлюз по умолчанию, введите 0.0.0.0.
Type of Service	Укажите новое значение TOS для исходящего пакета, выбрав **No Change** (без изменения), **Normal** (нормальный), **Min Delay** (минимальная задержка), **Max Thruput** (максимальная скорость передачи), **Max Reliable** (максимальная надежность) или **Min Cost** (минимальная стоимость).
Precedence	Укажите новый приоритет исходящего пакета, выбрав одно из значений: от **0** до **7** или **Don't Care** (не имеет значения).
Log	Чтобы оставлять в системном журнале отметку при выполнении политики, выберите **Yes**, нажав пробел и [ENTER].

36.7 Пример IP-маршрутизации с использованием политик

Если одна сеть имеет соединения с Интернетом и удаленным узлом, можно использовать две разные политики: для маршрутизации пакетов WWW в Интернет и для маршрутизации пакетов FTP в удаленную сеть. Этот пример проиллюстрирован на следующем рисунке.

Маршрут 1 является маршрутом IP по умолчанию, а маршрут 2 представляет собой отдельно настроенный маршрут IP.

Рис. 240 Пример IP-маршрутизации с использованием политик



Чтобы принудительно перенаправлять пакеты WWW от клиентов с IP-адресами из диапазона 192.168.1.33 – 192.168.1.64 в Интернет через порт WAN на устройстве ZyWALL, выполните следующие операции.

1 Создайте правило в меню **Menu 25.1 - IP Routing Policy Setup**, как показано ниже.

Рис. 241 Политика маршрутизации IP. Пример 1.

```
                Menu 25.1.1 - IP Routing Policy

Policy Set Name= example1
Active= Yes
Criteria:
  IP Protocol    = 6
  Type of Service= Don't Care          Packet length= 10
  Precedence     = Don't Care            Len Comp= Equal
  Source:
    addr start= 192.168.1.33           end= 192.168.1.64
    port start= 0                      end= N/A
  Destination:
    addr start= 0.0.0.0                end= N/A
    port start= 80                     end= 80
Action= Matched
  Gateway addr   = 192.168.1.1         Log= No
  Type of Service= Max Thruput
  Precedence     = 0
```

2 Чтобы применить политику к пакетам, получаемым через порт LAN, в меню 25.1.1 выберите **Yes** в поле **LAN**.

3 Проверьте, успешно ли добавлено правило, в разделе **Menu 25 - IP Routing Policy Summary**.

4 В меню 25.1 создайте новое правило, разрешающее пересылать пакеты от любого хоста (IP-адрес 0.0.0.0 обозначает любой хост) по протоколу TCP для порта FTP через другой шлюз (192.168.1.100).

Рис. 242 Политика маршрутизации IP. Пример 2.

```
                    Menu 25.1.1 - IP Routing Policy

        Policy Set Name= example2
        Active= No
        Criteria:
          IP Protocol    = 6
          Type of Service= Don't Care           Packet length= 10
          Precedence     = Don't Care             Len Comp= Equal
          Source:
            addr start= 0.0.0.0                 end= N/A
            port start= 0                       end= N/A
          Destination:
            addr start= 0.0.0.0                 end= N/A
            port start= 20                      end= 21
        Action= Matched
          Gateway addr   = 0.0.0.0              Log= No
          Type of Service= No Change
          Precedence     = No Change
```

5 Проверьте, успешно ли добавлено правило, в разделе **Menu 25 - IP Routing Policy Summary**.

37

Настройка расписания

Это меню служит для просмотра и настройки наборов расписаний в P-793H.

37.1 Краткие сведения о наборах расписаний

Расписания вызовов (применяемые только для инкапсуляции PPPoA или PPPoE) используются P-793H для управления соединением с удаленным узлом и задают время и продолжительность вызова удаленного узла. Эта функция аналогична программированию записи телепрограмм в видеомагнитофонах и системах цифрового телевидения.

37.2 Настройка расписания

Это меню действует только для соединений с Интернетом, использующих инкапсуляцию PPPoE. Это меню служит для просмотра наборов расписаний в P-793H. Чтобы открыть это меню, в основном меню введите 26.

Рис. 243 Меню 26: Настройка расписания

```
                        Menu 26 - Schedule Setup

Schedule                                Schedule
Set #          Name                     Set #          Name
------  -----------------               ------  -----------------
  1      ________________                  7      ________________
  2      ________________                  8      ________________
  3      ________________                  9      ________________
  4      ________________                 10      ________________
  5      ________________                 11      ________________
  6      ________________                 12      ________________


                Enter Schedule Set Number to Configure= 0

                Edit Name= N/A
```

Поля изображенного выше экрана описаны в следующей таблице.

Таблица 133 Меню 26: Настройка расписания

ПОЛЕ	ОПИСАНИЕ
1-12	В этом поле отображается начало названия каждого набора расписаний. Наборы с более низкими номерами обладают приоритетом над наборами с более высокими номерами, что позволяет избежать конфликтов между расписаниями. Например, если к удаленному узлу применяются наборы 1, 2, 3 и 4, набор 1 имеет приоритет над наборами 2, 3 и 4.
Enter Schedule Set Number to Configure	Для настройки набора расписаний введите в этом поле номер статического маршрута, в поле **Edit Name** введите имя расписания, затем нажмите [ENTER]. Появится меню 26.1. Чтобы удалить набор расписаний, введите в этом поле номер статического маршрута, в поле **Edit Name** оставьте пустое имя и нажмите [ENTER].
Edit Name	Введите имя настраиваемого расписания или оставьте поле пустым, чтобы удалить указанный набор расписаний.

37.3 Настройка набора расписаний

Это меню действует только для соединений с Интернетом, использующих инкапсуляцию PPPoE. Это меню служит для настройки наборов расписаний в P-793H. Чтобы открыть это меню, введите номер набора расписаний в поле **Enter Schedule Set Number to Configure**, введите имя набора расписаний в поле **Edit Name** и нажмите [ENTER] в меню 26.

Рис. 244 Меню 26.1: Настройка набора расписаний

```
                    Menu 26.1 Schedule Set Setup

        Active= Yes
        Start Date(yyyy-mm-dd)= 2000 - 01 - 01
        How Often= Once
        Once:
          Date(yyyy-mm-dd)= 2000 - 01 - 01
        Weekdays:
          Sunday= N/A
          Monday= N/A
          Tuesday= N/A
          Wednesday= N/A
          Thursday= N/A
          Friday= N/A
          Saturday= N/A
        Start Time(hh:mm)= 00 : 00
        Duration(hh:mm)= 00 : 00
        Action= Forced On
```

Поля изображенного выше экрана описаны в следующей таблице.

Таблица 134 Меню 26.1: Настройка набора расписаний

ПОЛЕ	ОПИСАНИЕ
Active	Нажмите клавишу [SPACE BAR] ([ПРОБЕЛ]) для выбора значения **Yes (Да)** или **No (Нет)**. Выберите **Yes** и нажмите [ENTER] для активации набора расписаний.
Start Date	Должен ли набор расписаний повторяться еженедельно или использоваться только один раз? Нажмите пробел, затем - [ENTER], чтобы выбрать **Once** (однократно) или **Weekly** (еженедельно). Эти опции взаимоисключающие. Если выбрано значение **Once (Один раз)** , все настройки рабочего дня недоступны (**N/A**). При выборе значения **Once (Один раз)** правило расписания удаляется автоматически после истечения времени расписания.
How Often	Введите дату начала, когда набор должен вступить в силу, в формате год – месяц – дата. Действительными датами являются все даты от текущей до 5 февраля 2036 г.
Once	
Date	Если в поле **How Often** выбрано значение **Once**, введите дату, когда набор должен активироваться, в формате год-месяц-день.
Weekdays	При выборе значения **Weekly** в поле **How Often**, укажите дни, в которые набор должен активироваться (и повторяться), перейдя к соответствующим дням и нажав пробел для выбора значения **Yes**, затем нажмите [ENTER].
Start Time	Введите время начала, когда набор расписаний должен вступать в силу, в формате час – минута.
Duration	Введите максимальную длину времени данного соединения в формате час – минута.
Action	**Forced On (Принудительное)** означает, что соединение устанавливается независимо от того, есть ли вызов с запросом на линии, и будет поддерживаться в течение того периода времени, который указан в поле **Duration (Продолжительность)**. **Forced Down (Принудительное отключение)** означает, что соединение блокируется независимо от того, есть ли вызов с запросом на линии. **Enable Dial-On-Demand (Включить набор по требованию)** означает, что это расписание допускает вызов по требованию на линии. **Disable Dial-On-Demand (Выключить набор по требованию)** означает, что это расписание не допускает вызов по требованию на линии.

38

Поиск и устранение неполадок

В этой главе приведены рекомендации по решению возможных проблем. Проблемы сгруппированы в несколько категорий.

38.1 Питание, подключение оборудования, светодиоды

? P-793H не включается. Не горит ни один светодиод.

1. Убедитесь, что питание P-793H включено.
2. Убедитесь, что используются шнур и источник питания из комплекта поставки P-793H.
3. Убедитесь, что блок питания или шнур соединены с P-793H и включены в соответствующую розетку. Убедитесь, что источник питания включен.
4. Выключите P-793H и включите устройство снова.
5. Если проблему не удается устранить, обратитесь к поставщику.

? Показания одного из светодиодов не соответствуют обычному состоянию.

1. Убедитесь, что вы верно понимаете показания светодиодов в нормальном режиме. См. разд. 1.4 на стр. 41.
2. Проверьте правильность подключения оборудования. См. Руководство по быстрому запуску.
3. Осмотрите кабели на предмет повреждений. Для замены поврежденных кабелей обратитесь к поставщику.
4. Выключите P-793H и включите устройство снова.
5. Если проблему не удается устранить, обратитесь к поставщику.

38.2 Доступ к P-793H и вход в систему

Утерян IP-адрес P-793H.

1. По умолчанию устройству присвоен IP-адрес **192.168.1.1**.
2. Подключитесь к P-793H через консольный порт.
3. Если вы изменили IP-адрес устройства и забыли его, узнать IP-адрес P-793H можно, сверившись с IP-адресом шлюза по умолчанию на вашем компьютере. В большинстве компьютеров с ОС Windows это можно сделать, выбрав **Start (Пуск) > Run** (Выполнить), введя **cmd** и набрав **ipconfig**. Полученный IP-адрес шлюза по умолчанию (**Default Gateway**) может совпадать с IP-адресом P-793H (это зависит от конфигурации сети). Попробуйте ввести этот IP-адрес в браузере.
4. Если обратиться к устройству таким путем не получилось, может потребоваться возврат к заводским настройкам. См. разд. 38.5 на стр. 384.

Утерян пароль.

1. Пароль по умолчанию – **1234**.
2. Если обратиться к устройству таким путем не получилось, может потребоваться возврат к заводским настройкам. См. разд. 38.5 на стр. 384.

Не удается войти в веб-конфигуратор или обратиться к экрану **Login**.

1. Убедитесь, что IP-адрес введен верно.
   - По умолчанию устройству присвоен IP-адрес 192.168.1.1.
   - Если вы изменили IP-адрес устройства (см. разд. 6.3 на стр. 103), используйте новый IP-адрес.
   - Если вы изменили IP-адрес устройства и впоследствии забыли его, обратитесь к указаниям, приведенным в подразделе Утерян IP-адрес P-793H..
2. Проверьте подключения оборудования и убедитесь, что показания светодиодов соответствуют норме. См. Руководство по быстрому запуску и разд. 38.1 на стр. 379.
3. Убедитесь, что ваш браузер не блокирует всплывающие окна (pop-up) и в нем включена поддержка JavaScript и Java. См. Приложение D на стр. 409.
4. Убедитесь, что компьютер находится в одной подсети с P-793H. (Если вам известно, что между компьютером и P-793H имеются маршрутизаторы, пропустите этот шаг.)
   - Если в сети присутствует DHCP-сервер, убедитесь, что ваш компьютер использует динамический адрес IP. См. Приложение C на стр. 393. По умолчанию в P-793H включен режим DHCP-сервера.

5 Сбросьте устройство к заводским настройкам и попробуйте обратиться к P-793H, используя IP-адрес по умолчанию. См. разд. 38.5 на стр. 384.
6 Если проблему устранить не удалось, обратитесь к системному администратору или поставщику, либо прибегните к углубленной диагностике.

Углубленный способ диагностики

- Попробуйте обратиться к P-793H через другую сетевую службу, например, Telnet. Если вам удалось войти в P-793H, проверьте настройки дистанционного управления устройством, правила межсетевого экрана и фильтры SMT, чтобы установить причину, по которой веб-интерфейс P-793H оказался недоступен. См. разд. 21.1 на стр. 257.

Экран **Login** доступен, но войти в управление P-793H не удается.

1 Убедитесь, что вы правильно вводите пароль. Пароль по умолчанию – **1234**. Пароль воспринимается с учетом регистра, поэтому при вводе индикатор клавиши [Caps Lock] не должен гореть.
2 Веб-конфигуратор нельзя использовать, если одновременно активен сеанс управления P-793H через SMT, Telnet или консольный порт. Завершите другой сеанс управления P-793H или попросите пользователя, работающего в этом сеансе, выйти из системы.
3 Выключите P-793H и включите его снова.
4 Если обратиться к устройству таким путем не получилось, может потребоваться возврат к заводским настройкам. См. разд. 38.5 на стр. 384.

SMT недоступен/не удается войти в P-793H по Telnet.

См. указания по устранению неполадок под заголовком Не удается войти в веб-конфигуратор или обратиться к экрану Login.. Не обращайте внимание на указания, касающиеся браузера.

Не удается загрузить или принять по FTP файл настроек или обновить микропрограмму.

См. указания по устранению неполадок под заголовком Не удается войти в веб-конфигуратор или обратиться к экрану Login.. Не обращайте внимание на указания, касающиеся браузера.

Не удается обратиться к P-793H посредством TR-069/CNM Access.

1. Убедитесь, что в P-793H включено управление по TR-069 и правильно настроен IP-адрес сервера управления. См. разд. 15.9 на стр. 220.
2. Убедитесь, что настроены правила межсетевого экрана и переадресация портов NAT для прохождения трафика от сервера управления к P-793H. См. документацию на сервер управления.

Невозможно подключиться к P-793H через консольный порт.

Убедитесь, что вы используете консольный кабель из комплекта поставки, а переключатель **CON/AUX** на P-793H установлен в положение **CON**. См. Руководство по быстрому запуску.

38.3 Доступ к Интернету

Не удается выйти в Интернет.

1. Проверьте подключения оборудования и убедитесь, что показания светодиодов соответствуют норме. См. Руководство по быстрому запуску и разд. 1.4 на стр. 41.
2. Убедитесь, что вы правильно ввели в мастере параметры учетной записи поставщика услуг Интернета. Пароль воспринимается с учетом регистра, поэтому индикатор клавиши [Caps Lock] не должен гореть.
3. Если проблему не удается устранить, обратитесь к поставщику услуг Интернета.

Доступ в Интернет прекратился. Ранее Интернет был доступен через P-793H, но сейчас соединение не функционирует.

1. Проверьте подключения оборудования и убедитесь, что показания светодиодов соответствуют норме. См. Руководство по быстрому запуску и разд. 1.4 на стр. 41.
2. Выключите P-793H и включите устройство снова.
3. Если проблему не удается устранить, обратитесь к поставщику услуг Интернета.

Низкая скорость или перебои в работе Интернет-соединения.

1. Сеть может быть перегружена трафиком. Проверьте светодиоды и обратитесь к разд. 1.4 на стр. 41. Если устройство P-793H перегружено отправляемой или принимаемой информацией, закройте программы, использующие Интернет, в первую очередь – приложения для файлообменных сетей (P2P).

1 Сеть может быть перегружена трафиком. Попробуйте закрыть программы, использующие Интернет, начав с приложений для файлообменных сетей.
2 Выключите и снова включите P-793H и ваш компьютер.
3 Если проблему устранить не удалось, обратитесь к системному администратору или поставщику, либо прибегните к углубленной диагностике.

Углубленный способ диагностики

- Проверьте настройки управления полосой пропускания. Если управление полосой пропускания не активно, возможно, потребуется его активировать. Если управление полосой пропускания активно, попробуйте изменить параметры распределения полосы пропускания. См. гл. 13 на стр. 195.

Невозможно обратиться к веб-сайту (по определенным дням недели).

Проверьте настройки фильтрации содержания и убедитесь, что вы не заблокировали себе доступ к каким-либо сайтам. См. гл. 10 на стр. 159.

Не работает резервирование через коммутируемый доступ или переадресация трафика.

1 Если для резервирования через коммутируемый доступ вы используете порт **CON/AUX**, проверьте, установлен ли переключатель **CON/AUX** на P-793H в положение **AUX**. См. Руководство по быстрому запуску.
2 В конфигурации "точка – две точки" резервирование WAN недоступно.

38.4 Специальные функции

Не удается настроить VPN-туннель на другое устройство.

1 Убедитесь, что все настройки VPN заданы верно. В первую очередь проверьте настройки аутентификации. См. гл. 11 на стр. 163.
2 В конфигурации "точка – две точки" VPN-туннель можно установить только с удаленным узлом 1.

38.5 Сброс P-793H к заводским настройкам

При сбросе настроек P-793H все изменения в настройках будут потеряны. P-793H восстановит настройки по умолчанию, а также исходный пароль: **1234**. Может потребоваться повторное выполнение всех настроек.

При нажатии кнопки **RESET** все изменения в настройках будут потеряны!

Чтобы сбросить настройки P-793H:

1. Убедитесь, что светодиод **POWER** горит и не мигает.
2. Нажмите и держите нажатой кнопку **RESET** в течение 10 секунд. Отпустите кнопку **RESET**, когда светодиод **POWER** начнет мигать. Это означает, что настройки по умолчанию восстановлены.

Если устройство P-793H автоматически начало перезагружаться, дождитесь окончания перезагрузки P-793H и войдите в веб-конфигуратор с паролем "1234".

Если автоматической перезагрузки P-793H не произошло, отключите и снова включите питание P-793H. После этого выполните приведенные выше указания.

Часть VI
Приложения и предметный указатель

A

Технические характеристики

Таблица 135 Устройство

IP-адрес по умолчанию	192.168.1.1
Маска подсети по умолчанию	255.255.255.0 (24 бита)
Пароль по умолчанию	пользователь: "user" администратор: "1234"
Пул адресов DHCP	192.168.1.33 – 192.168.1.64
Габариты (Ш x Г x В)	180 x 128 x 36 мм
Электропитание	12 В перем. тока, 1 А
Встроенный коммутатор	Четыре Ethernet-порта RJ-45 с автоматическим согласованием MDI/MDI-X 10/100 Мбит/с
Порт G.SHDSL	Интерфейсный разъем RJ-11 Скорость передачи данных: 192 кбит/с - 5696 кбит/с, 384-11392 кбит/с (4-проводной режим) Кодирование: фазоамплитудная модуляция с решетчатым кодированием (TC-PAM) Импеданс линии: 135 Вт Проводное подключение: одна пара (2 провода), две пары (4 провода) или две однопарные линии (2 провода в паре)
Рабочая температура	0° C ~ 40° C
Температура хранения	-20° ~ 60° C
Рабочая влажность	20% ~ 90% относительной влажности
Влажность при хранении	10% ~ 90% относительной влажности
Расстояние между центрами отверстий на задней стороне корпуса	108 мм
Размер шурупов для настенного крепления	M4

Таблица 136 Микропрограмма

Поддержка режима маршрутизатора/моста	Поддерживается маршрутизация IP (RFC 791). TCP, UDP, ICMP, IGMP v1 и v2, ARP, RIP v1, RIP v2 Прозрачный режим моста (IEEE 802.1d) Поддержка PPP BCP (RFC 3185)
G.SHDSL	Фазоамплитудная модуляция с решетчатым кодированием (TC-PAM) Настройка в режиме клиента или сервера Автоматическое согласование / ручная подстройка скорости Подключение по 2- и 4-проводной линии - Скорость передачи данных: От 192 кбит/с до 5696 кбит/с (2-проводной режим) - Скорость передачи данных: От 384 кбит/с до 11392 кбит/с (4-проводной режим)
Поддержка ATM	Многопротокольная передача поверх AAL5 (RFC1483) PPP поверх ATM (RFC 2364) PPP поверх Ethernet (RFC2516) Поддержка ATM AAL5 Поддержка восьми PVC ATM Forum UNI3.0/4.0 PVC Режимы ограничения трафика: UBR, CBR и VBR
Совместный доступ в Интернет	NAT (включая режим "многие ко многим") / SUA, 2048 сеансов NAT Стандартный NAT с ограничением по номерам портов Серверный режим NAT (перенаправление портов) NAT для нескольких хостов Динамическая DNS (www.dyndns.org) DHCP-сервер/клиент/агент ретрансляции
Security (Безопасность)	Аутентификация пользователя (PAP, CHAP) при использовании PPP (RFC 1334, RFC 1994) Microsoft CHAP Межсетевой экран с динамическим анализом пакетов Фильтрация содержания Предотвращение DoS-атак Управление доступом для сетевых служб Предупреждение об атаках и ведение журналов в реальном времени
Управление сетью	Веб-конфигуратор Интерфейс командной строки Поддержка доступа через Telnet по паролю Поддержка SNMP MIB I / MIB II Обновление микропрограммы и резервное копирование настроек по TFTP и FTP
VPN	Поддержка IPSec VPN 10 туннелей VPN IKE / ручное задание ключей Программное шифрование DES/3DES/AES Аутентификация MD5/ SHA1 Полные доменные имена (FQDN) Сквозной режим NETBIOS для IPSec Поддержание активности соединений IPSec VPN Прослеживание NAT IPSec
Диагностические средства (для следующих подсистем)	Флэш-память Цепи и микросхемы SDSL ОЗУ Порт LAN
Прочее	Прокси-сервер для DNS Системный журнал (UNIX SYSLOG)

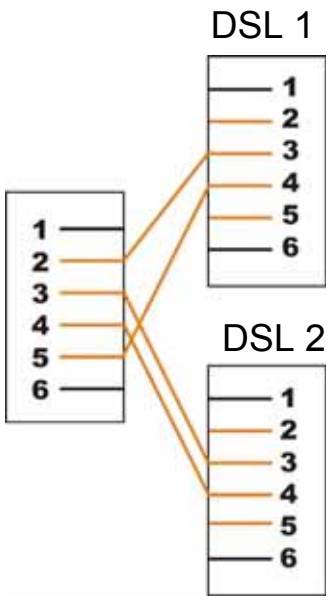
Таблица 137 Функциональные возможности микропрограммы

ФУНКЦИЯ	ОПИСАНИЕ
Firmware Upgrade	После выхода новой микропрограммы ее можно загрузить с сайта ZyXEL и передать в P-793H с помощью веб-конфигуратора или клиента FTP/TFTP. Примечание. Используйте только микропрограмму, предназначенную для вашей модели устройства!
Резервное копирование и восстановление настроек	Создав резервную копию конфигурации P-793H, вы сможете в дальнейшем загрузить ее в P-793H, если потребуется вернуться к прежним настройкам.
Трансляция сетевых адресов (NAT)	Каждому компьютеру в сети должен быть присвоен собственный уникальный IP-адрес. NAT позволяет преобразовывать присвоенный вам внешний IP-адрес (диапазон адресов) в несколько частных IP-адресов, используемых компьютерами в вашей сети.
Перенаправление портов	Если в сети имеется сервер (например, почтовый или веб-сервер), с помощью этой функции можно обеспечить доступ к нему из Интернета.
DHCP (динамический протокол настройки хоста)	С помощью этой функции P-793H может назначать компьютерам в сети IP-адреса, адрес шлюза по умолчанию и адреса DNS-серверов.
Поддержка динамической DNS	Динамическая служба DNS (система доменных имен) позволяет использовать фиксированный URL-адрес, например www.zyxel.com, с динамическим IP-адресом. Для получения такой услуги необходимо зарегистрироваться у провайдера динамической DNS.
IP Multicast	Многоадресная рассылка используется для доставки трафика определенной группе хостов. P-793H поддерживает протокол IGMP (Internet Group Management Protocol - межсетевой протокол управления группами) версии 1 и 2 для присоединения к группам многоадресной рассылки (см. RFC 2236).
IP Alias	Совмещение IP-адресов (IP aliasing) позволяет разделить физическую сеть на различные логические сети через один и тот же интерфейс Ethernet. P-793H в этом случае выступает в качестве шлюза для каждой подсети.
Время и дата	Текущее время и дату можно получать от внешнего сервера при включении P-793H. Кроме того, время можно установить вручную. Полученные дата и время в последующем используются в журналах.
Регистрация и отслеживание	Средства отслеживания пакетов и ведения журналов можно использовать для устранения неполадок. Журнальные сообщения с P-793H можно передавать на внешний SYSLOG-сервер.
PPPoE	PPPoE имитирует модемное коммутируемое соединение с Интернетом.
Инкапсуляция PPTP	Двухточечный протокол туннелирования (PPTP) обеспечивает защищенную передачу данных в рамках виртуальной частной сети (VPN). P-793H поддерживает одновременно не более одного PPTP-соединения.
Универсальная технология Plug and Play (UPnP)	Устройство с поддержкой UPnP может динамически присоединяться к сети, получать IP-адрес, сообщать свои возможности другим устройствам в сети.
Firewall	Для защищенного доступа в Интернет на устройстве ZyXEL можно настроить межсетевой экран. По умолчанию при активном межсетевом экране весь входящий трафик из Интернета в вашу сеть блокируется, если он не был запрошен из вашей сети. Таким образом, попытки проникнуть в вашу сеть извне пресекаются, при этом вы имеете безопасный доступ к Интернету и можете, в частности, загружать из сети файлы.

Таблица 137 Функциональные возможности микропрограммы

ФУНКЦИЯ	ОПИСАНИЕ
Content Filter	P-793H блокирует или разрешает доступ к указанным вами сайтам, а также может блокировать доступ к сайтам, в URL которых содержатся определенные ключевые слова. Можно определить периоды времени и дни недели, в которые будет активна фильтрация содержания. Отдельные компьютеры в вашей сети можно включить или исключить из механизма фильтрации содержания.
Управление полосой пропускания	Можно эффективно управлять трафиком в вашей сети, резервируя полосу пропускания и предоставляя приоритет определенным типам трафика и/или определенным компьютерам.
Удаленное управление	Функция удаленного управления позволяет указать, с каких компьютеров в сети (WAN или LAN) и с использованием каких служб (например, HTTP, FTP) может осуществляться доступ к P-793H.

Рис. 245 Конфигурация разветвительного кабеля



B

Инструкция по монтажу на стене

Для установки P-793H на стене выполните следующие действия.

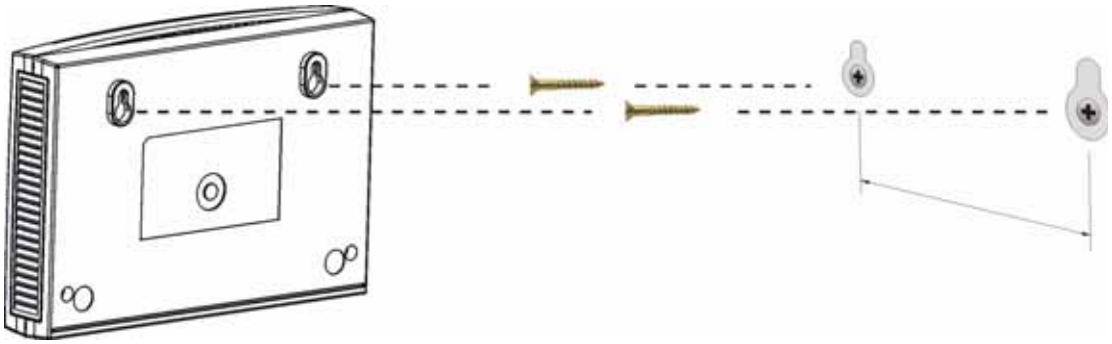
Уточните размер крепежных шурупов и расстояние между ними, обратившись к приложению с характеристиками продукта.

1. Подберите достаточно высокое место на стене, свободное от посторонних предметов. Используйте только прочные стены.
2. Просверлите два отверстия под шурупы. Убедитесь, что расстояние между центрами отверстий совпадает с указанным в приложении о характеристиках продукта.

При сверлении отверстий будьте осторожны, чтобы не повредить трубы и кабели, которые могут быть проложены в стене.

3. Не завинчивайте шурупы в стену до конца. Оставьте небольшой зазор (примерно 0,5 см) между головками шурупов и стеной.
4. Убедитесь, что шурупы прочно закреплены в стене – они должны выдерживать массу P-793H с соединительными кабелями.
5. Совместите отверстия с задней стороны корпуса P-793H с шурупами в стене. Повесьте P-793H на шурупы.

Рис. 246 Пример монтажа на стене



C

Настройка IP-адреса компьютера

Все компьютеры должны быть оборудованы адаптером Ethernet 10 или 100 Мбит/с, и на компьютерах должен быть установлен протокол TCP/IP.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 и более новые версии этих операционных систем, а также все версии UNIX/LINUX включают программные компоненты, необходимые для установки и использования протокола TCP/IP на компьютере. При работе с Windows 3.1 требуется приобретение пакета приложений TCP/IP сторонних производителей.

TCP/IP должен быть уже установлен на компьютерах под управлением Windows NT/2000/XP, Macintosh OS 7 и более поздних версий этих операционных систем.

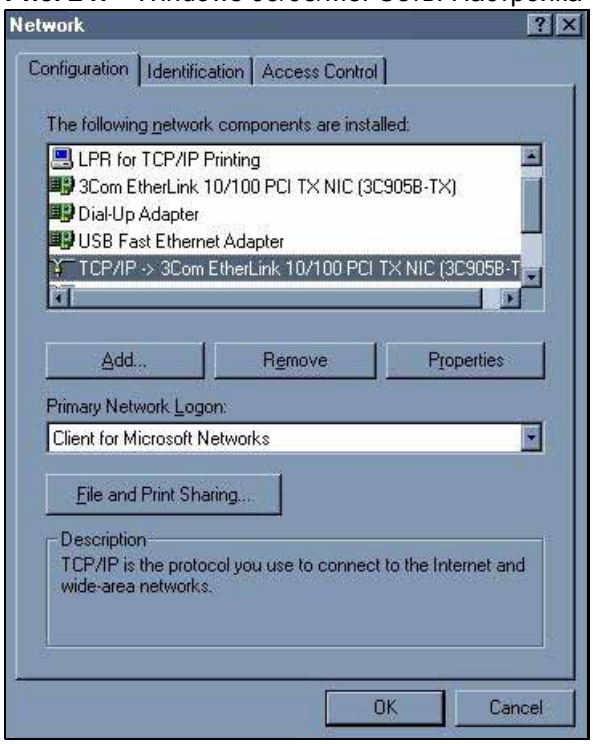
После установки необходимых компонентов TCP/IP настройте параметры TCP/IP для обмена данными через сеть.

Если вместо динамического назначения параметры IP присваиваются в ручном режиме, убедитесь в том, что компьютеры имеют IP-адреса, относящиеся к той же подсети, в которой находится LAN-порт P-793H.

Windows 95/98/Me

Нажмите кнопку **Start (Пуск)**, выберите **Settings (Настройки)**, **Control Panel (Панель управления)** и выберите двойным щелчком значок **Network (Сеть)** для открытия окна **Network (Сеть)**.

Рис. 247 Windows 95/98/Me: Сеть: Настройка



Установка компонентов

На вкладке **Configuration (Конфигурация)** окна **Network (Сеть)** отображается список установленных компонентов. Необходимы сетевой адаптер, протокол TCP/IP и клиент для сетей Microsoft.

Если необходим адаптер, выполните следующие действия.

1. В окне **Network (Сеть)** нажмите кнопку **Add (Добавить)**.
2. Выберите **Adapter (Адаптер)** и нажмите кнопку **Add (Добавить)**.
3. Выберите производителя и модель сетевого адаптера, затем нажмите кнопку **OK**.

Если необходимо установить протокол TCP/IP, выполните следующие действия.

1. В окне **Network (Сеть)** нажмите кнопку **Add (Добавить)**.
2. Выберите **Protocol (Протокол)** и нажмите кнопку **Add (Добавить)**.
3. Выберите **Microsoft** в списке **производителей**.
4. Выберите **TCP/IP** в списке сетевых протоколов и нажмите кнопку **OK**.

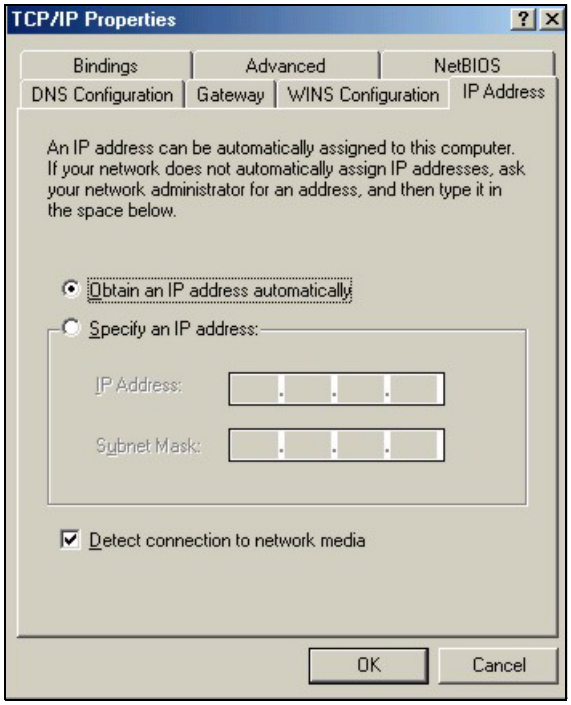
Если необходим клиент для сетей Microsoft, выполните следующие действия.

1. Нажмите кнопку **Add (Добавить)**.
2. Выберите **Client (Клиент)** и нажмите кнопку **Add (Добавить)**.
3. Выберите **Microsoft** в списке производителей.
4. Выберите **Client for Microsoft Networks (Клиент для сетей Microsoft)** в списке сетевых клиентов и нажмите кнопку **OK**.
5. Перезапустите компьютер, чтобы изменения вступили в силу.

Настройка

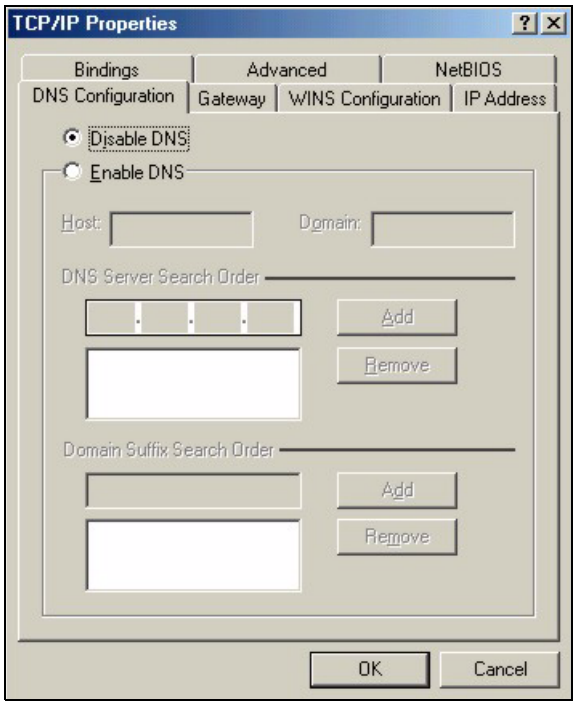
1. На вкладке **Configuration (Конфигурация)** окна **Network (Сеть)** выберите запись TCP/IP своего сетевого адаптера и нажмите кнопку **Properties (Свойства)**.
2. Выберите вкладку **IP Address (IP-адрес)**.
   - Если IP-адрес динамический, установите переключатель **Obtain an IP address automatically (Получить IP-адрес автоматически)**.
   - Если имеется статический IP-адрес, выберите переключатель **Specify an IP address (Указать IP-адрес)** и введите информацию в поля **IP Address (IP-адрес)** и **Subnet Mask (Маска подсети)**.

Рис. 248 Windows 95/98/Me: Свойства TCP/IP: IP-адрес



3. Выберите вкладку **DNS Configuration (Конфигурация DNS)**.
   - Если информация о DNS неизвестна, установите переключатель **Disable DNS (Отключить DNS)**.
   - Если информация о DNS известна, установите переключатель **Enable DNS (Включить DNS)** и введите информацию в полях внизу (необязательно заполнять их все).

Рис. 249 Windows 95/98/Me: Свойства TCP/IP: Конфигурация DNS



4 Выберите вкладку **Gateway (Шлюз)**.
   - Если IP-адрес межсетевого шлюза неизвестен, удалите ранее установленные межсетевые шлюзы.
   - Если IP-адрес шлюза известен, введите его в поле **New gateway (Новый шлюз)** и нажмите кнопку **Add (Добавить)**.
5 Нажмите кнопку **OK** для сохранения изменений и закройте окно **TCP/IP Properties (Свойства TCP/IP)**.
6 Нажмите кнопку **OK** для закрытия окна **Network (Сеть)**. При появлении запроса вставьте компакт-диск Windows.
7 Включите P-793H и перезапустите компьютер, когда это будет предложено.

Проверка настроек

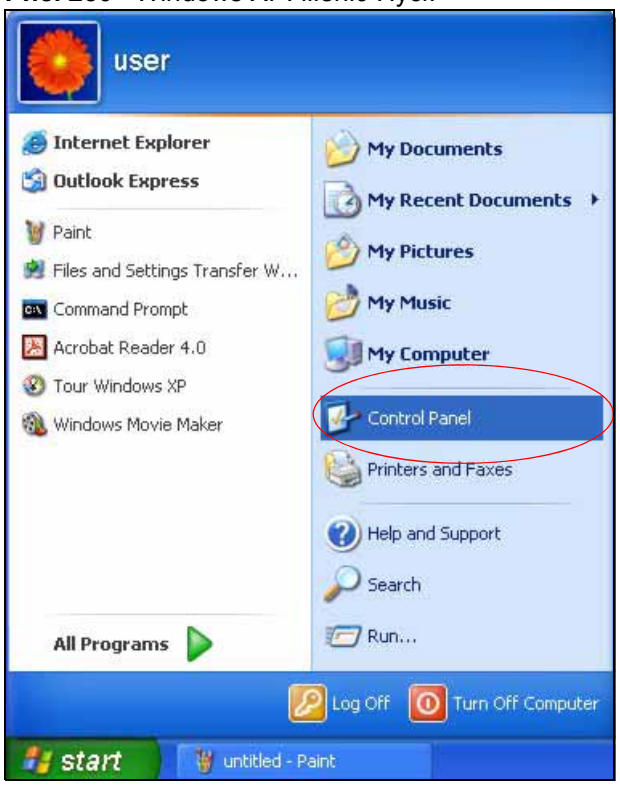
1 Нажмите кнопку **Start (Пуск)**, выберите **Run (Выполнить)**.
2 В окне **Run (Выполнить)** введите "winipcfg" и нажмите кнопку **OK** для открытия окна **IP Configuration (Конфигурация IP)**.
3 Выберите свой сетевой адаптер. Вы должны увидеть IP-адрес, маску подсети и основной шлюз своего компьютера.

Windows 2000/NT/XP

В следующем примере рисунки приведены для Windows XP со стандартной темой интерфейса.

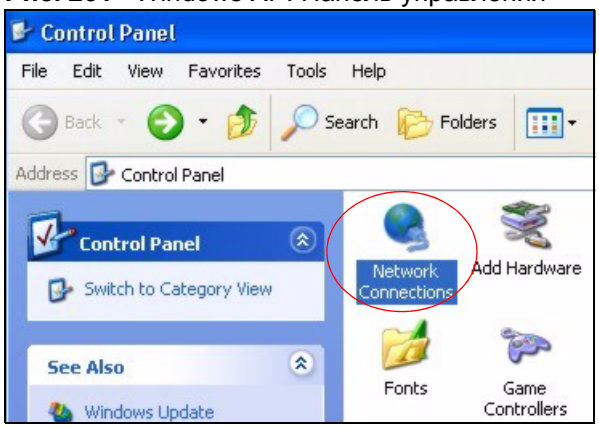
1 Нажмите кнопку **Пуск** (**Start** в англоязычных версиях Windows), **Настройка**, **Панель управления**.

Рис. 250 Windows XP: меню Пуск



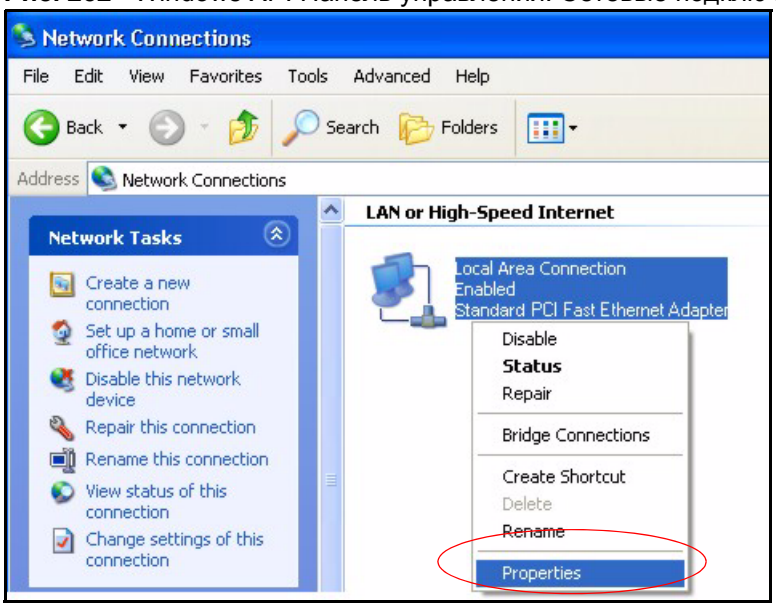
2 В **Панели управления** дважды щелкните на пункт **Сетевые подключения** (в Windows 2000/NT – **Сеть и коммутируемые подключения**).

Рис. 251 Windows XP: Панель управления



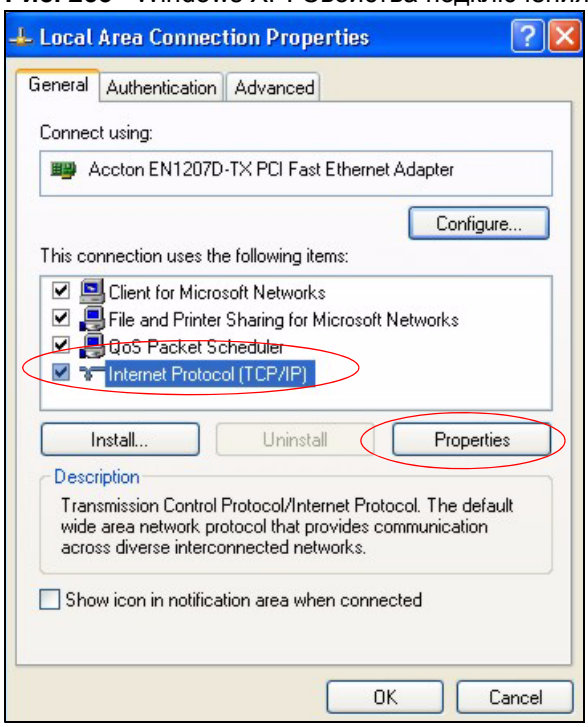
3 Щелкните правой кнопкой мыши **Local Area Connection (Подключение по локальной сети)**, затем выберите **Properties (Свойства)**.

Рис. 252 Windows XP: Панель управления: Сетевые подключения: Свойства



4 Выберите **Internet Protocol (TCP/IP) (Протокол Интернета (TCP/IP))** (на вкладке **General (Общие)**в Win XP) и щелкните **Properties (Свойства)**.

Рис. 253 Windows XP: Свойства подключения по локальной сети

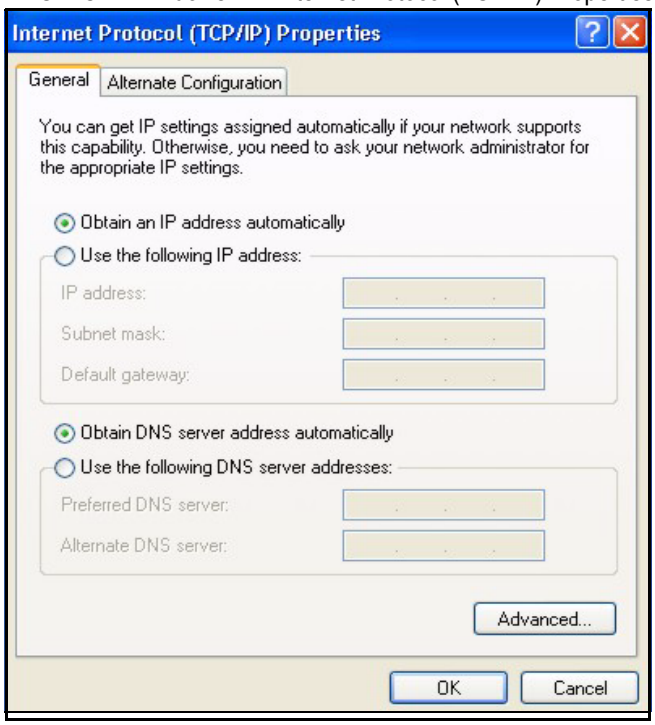


5 Откроется окно **Internet Protocol TCP/IP Properties (Свойства протокола Интернета (TCP/IP))** (вкладка **General (Общие)** в Windows XP).

- Если имеется динамический IP-адрес, установите переключатель **Obtain an IP address automatically (Получить IP-адрес автоматически)**.

- Если имеется статический IP-адрес, установите переключатель **Use the following IP Address (Использовать следующий IP-адрес)** и заполните поля **IP address (IP-адрес)**, **Subnet mask (Маска подсети)** и **Default gateway (Основной шлюз)**.
- Нажмите кнопку **Advanced (Дополнительно)**.

Рис. 254 Windows XP: Internet Protocol (TCP/IP) Properties (Свойства протокола Интернета (TCP/IP))



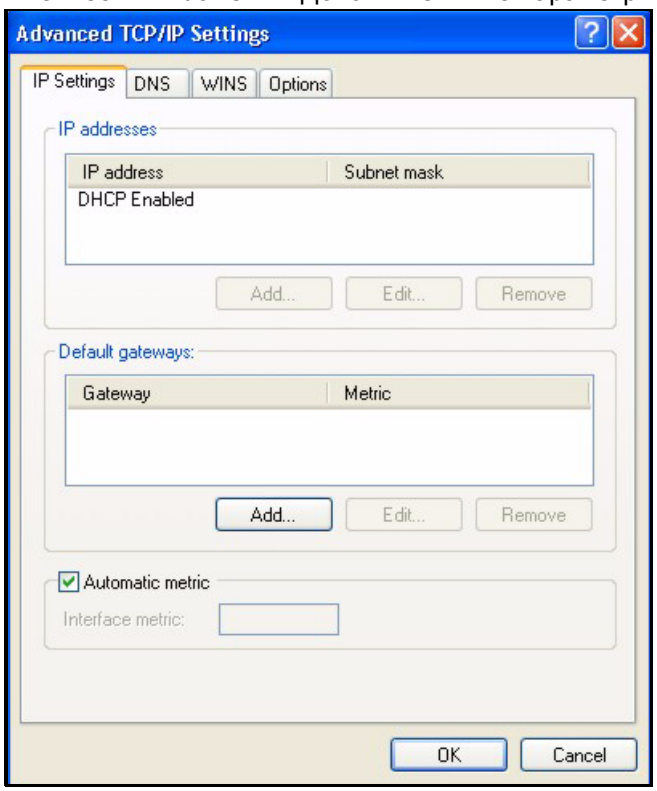
6 Если IP-адрес шлюза неизвестен, удалите все ранее установленные шлюзы на вкладке **Параметры IP** и нажмите кнопку **OK**.

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), нажмите кнопку **Add (Добавить)**.
- В окне **TCP/IP Address (Адрес TCP/IP)** введите IP-адрес в поле **IP address (IP-адрес)** и маску подсети в поле **Subnet mask (Маска подсети)**, затем нажмите кнопку **Add (Добавить)**.
- Выполните два вышеописанных действия для ввода каждого нового IP-адреса.
- Настройте дополнительные основные шлюзы по умолчанию на вкладке **IP Settings (Параметры IP)**, щелкнув кнопку **Add (Добавить)** в разделе **Default gateways (Основные шлюзы)**.
- В окне **TCP/IP Gateway Address (Адрес шлюза TCP/IP)** введите IP-адрес шлюза по умолчанию в поле **Gateway (Шлюз)**. Чтобы вручную настроить метрику по умолчанию (количество прыжков при передаче), снимите флажок **Automatic metric (Автоматическое назначение метрики)** и введите метрику в поле **Metric (Метрика)**.
- Нажмите кнопку **Add (Добавить)**.
- Повторите три указанных выше действия для добавления каждого шлюза по умолчанию.

- Нажмите кнопку **OK** по завершении.

Рис. 255 Windows XP: Дополнительные параметры TCP/IP

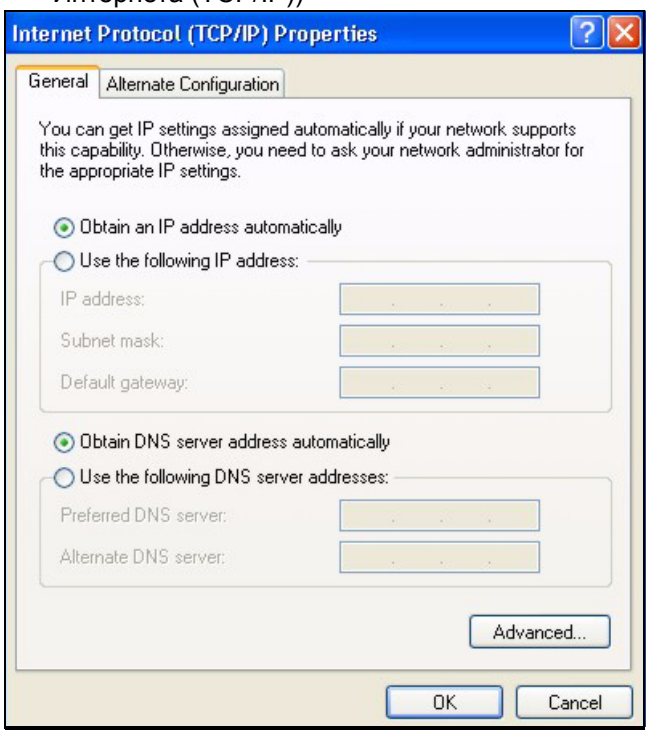


7 В окне **Internet Protocol TCP/IP Properties (Свойства протокола Интернета (TCP/IP))** (вкладка **General (Общие)** в Windows XP) выполните следующее.

- Установите переключатель **Obtain DNS server address automatically (Получить адрес DNS-сервера автоматически)**, если адрес сервера неизвестен.
- Если IP-адрес DNS-сервера известен, установите переключатель **Use the following DNS server addresses (Использовать следующие адреса DNS-серверов)** и введите IP-адрес в полях **Preferred DNS server (Предпочитаемый DNS-сервер)** и **Alternate DNS server (Альтернативный DNS-сервер)**.

  Если DNS-серверы были ранее настроены, нажмите кнопку **Advanced (Дополнительно)** и выберите вкладку **DNS** для их сортировки.

Рис. 256 Windows XP: Internet Protocol (TCP/IP) Properties (Свойства протокола Интернета (TCP/IP))



8 Нажмите кнопку **OK** для закрытия окна **Internet Protocol (TCP/IP) Properties (Свойства протокола Интернета (TCP/IP))**.

9 Нажмите кнопку **Закрыть** (в Windows 2000/NT – **OK**), чтобы закрыть окно **Свойства подключения по локальной сети**.

10 Закройте окно **Сетевые подключения** (в Windows 2000/NT – **Сеть и коммутируемые подключения**).

11 Включите P-793H и перезапустите компьютер (если это будет предложено).

Проверка настроек

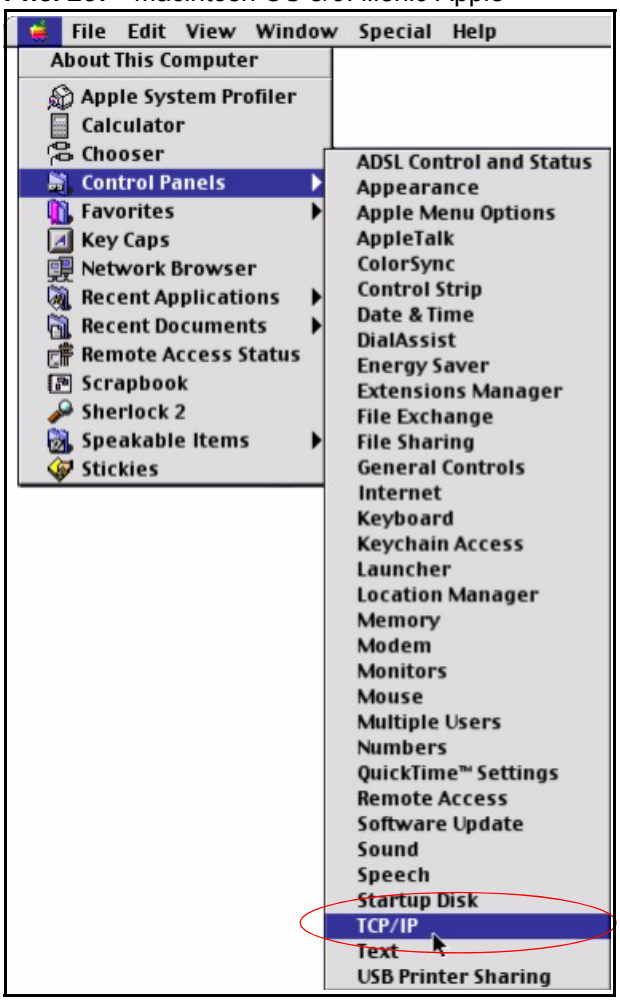
1 Нажмите кнопку **Start (Пуск)**, выберите **All Programs (Все программы)**, **Accessories (Стандартные)**, затем **Command Prompt (Командная строка)**.

2 В окне **Command Prompt (Командная строка)** введите "ipconfig" и затем нажмите кнопку [ENTER] ([ВВОД]). Можно также открыть окно **Network Connections (Сетевые подключения)**, щелкнуть правой кнопкой мыши на сетевом подключении, выбрать пункт **Status (Состояние)**, затем – вкладку **Support (Поддержка)**.

Macintosh OS 8/9

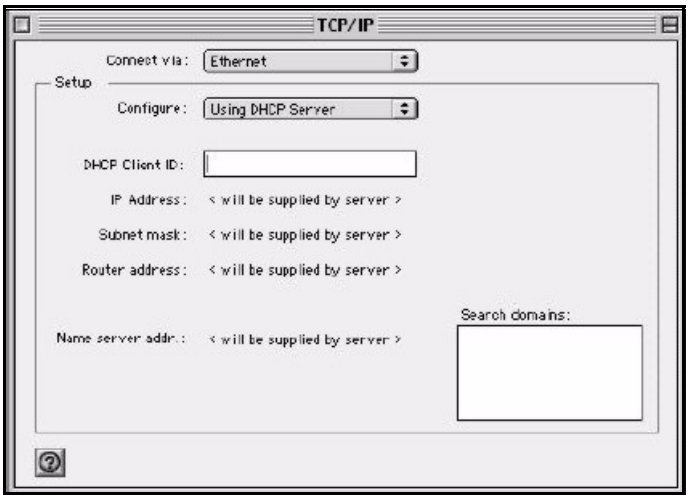
1 Щелкните меню**Apple**, **Control Panel (Панель управления)** и выберите двойным щелчком пункт **TCP/IP**, чтобы открыть **TCP/IP Control Panel (Панель управления TCP/IP)**.

Рис. 257 Macintosh OS 8/9: меню Apple



2 Выберите **Ethernet built-in (Встроенный Ethernet)** в списке **Connect via (Подключиться через)**.

Рис. 258 Macintosh OS 8/9: TCP/IP



3 Для динамически назначаемых параметров выберите пункт **Using DHCP Server (Использование сервера DHCP)** в списке **Configure:** (Конфигурировать).

4 Если параметры назначаются статически, выполните следующие действия.
   - В списке **Configure (Конфигурировать)** выберите пункт **Manually (Вручную)**.
   - Введите свой IP-адрес в поле **IP Address (IP-адрес)**.
   - Введите маску подсети в поле **Subnet mask (Маска подсети)**.
   - Введите IP-адрес P-793H в поле **Router address (Адрес маршрутизатора)**.
5 Закройте **TCP/IP Control Panel (Панель управления TCP/IP)**.
6 При появлении приглашения щелкните **Save (Сохранить)** для сохранения изменений конфигурации.
7 Включите P-793H и перезапустите компьютер (если это будет предложено).

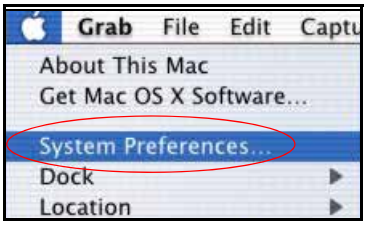
Проверка настроек

Проверьте свойства TCP/IP в окне **TCP/IP Control Panel (Панель управления TCP/IP)**.

Macintosh OS X

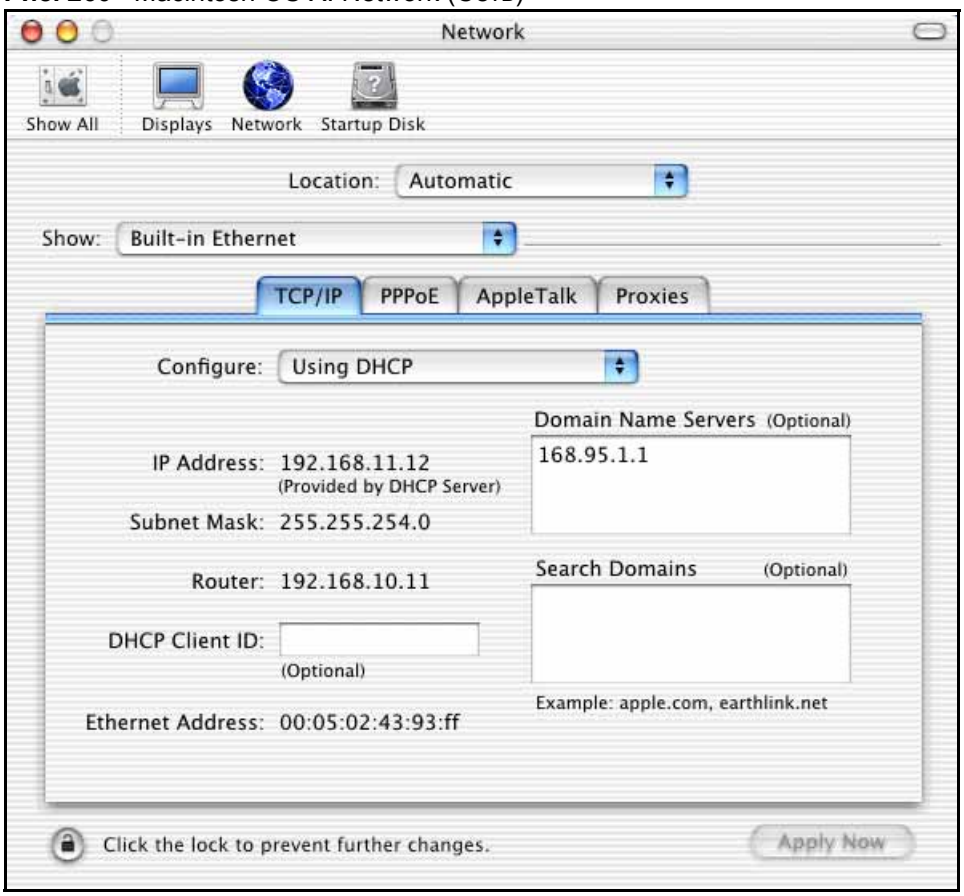
1 Щелкните меню **Apple**, пункт **System Preferences (Параметры системы)** для открытия окна **System Preferences (Параметры системы)**.

Рис. 259 Macintosh OS X: меню Apple



2 Щелкните **Network (Сеть)** на панели иконок.
   - Выберите значение **Automatic (Автоматический)** в списке **Location (Местоположение)**.
   - Выберите пункт **Built-in Ethernet (Встроенный Ethernet)** в списке **Show (Показать)**.
   - Выберите вкладку **TCP/IP**.
3 Если параметры назначаются динамически, выберите пункт **Using DHCP (Использование DHCP)** в списке **Configure**.

Рис. 260 Macintosh OS X: Network (Сеть)



4 Если параметры назначаются статически, выполните следующие действия.
   - В списке **Configure (Конфигурировать)** выберите пункт **Manually (Вручную)**.
   - Введите свой IP-адрес в поле **IP Address (IP-адрес)**.
   - Введите маску подсети в поле **Subnet mask (Маска подсети)**.
   - Введите IP-адрес P-793H в поле **Router address (Адрес маршрутизатора)**.
5 Нажмите кнопку **Apply Now (Применить сейчас)** и закройте окно.
6 Включите P-793H и перезапустите компьютер (если это будет предложено).

Проверка настроек

Проверьте свойства TCP/IP в окне **Network (Сеть)**.

Linux

В этом разделе иллюстрируется настройка параметров TCP/IP в Red Hat Linux 9.0. В зависимости от используемого дистрибутива Linux и его версии методика, вид экранов и местоположение файлов могут различаться.

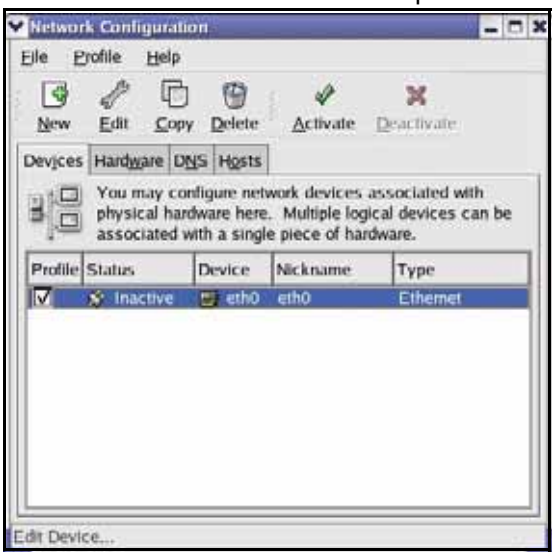
Убедитесь, что вы вошли в систему с правами администратора (root).

Настройка в среде K Desktop Environment (KDE)

Для настройки IP-адреса компьютера в среде KDE выполните следующие операции.

1 Нажмите кнопку Red Hat (в левом нижнем углу экрана), выберите **System Setting** (Системные настройки) и нажмите **Network** (Сеть).

Рис. 261 Red Hat 9.0: KDE: настройка сети: устройства



2 Дважды щелкните на профиле сетевой карты, который вы хотите настроить. Появится показанный ниже экран **Ethernet Device: General** (Устройство Ethernet: Общее).

Рис. 262 Red Hat 9.0: KDE: устройство Ethernet: общие настройки

- Если вам выдается динамический IP-адрес, установите флажок **Automatically obtain IP address settings with** (Автоматически получать параметры IP-адреса) и выберите **dhcp**.
- Если вы используете статический IP-адрес, выберите **Statically set IP Addresses** (Статические IP-адреса) и заполните поля **Address** (Адрес), **Subnet mask** (Маска подсети) и **Default Gateway Address** (Шлюз по умолчанию).

3 Чтобы сохранить настройки и закрыть экран **Ethernet Device General**, нажмите кнопку **OK**.

4 Если вам известны IP-адреса DNS-серверов, щелкните на вкладке **DNS** на экране **Network Configuration**. Введите в соответствующих полях параметры DNS-сервера.

Рис. 263 Red Hat 9.0: KDE: настройка сети: DNS

5 Перейдите на вкладку **Devices** (Устройства).

6 Чтобы изменения вступили в силу, нажмите кнопку **Activate** (Активировать). Появится изображенный ниже экран. Для сохранения изменений, выполненных на всех экранах, выберите **Yes** (Да).

Рис. 264 Red Hat 9.0: KDE: настройка сети: активация

7 После повторной инициализации сетевой карты убедитесь, что на экране **Network Configuration** (Настройка сети) в поле **Status** (Статус) **Active** (Активный).

Использование файлов настройки

Чтобы задать IP-адрес компьютера, отредактировав файлы настройки сети, выполните следующие операции.

1 Если в вашем компьютере установлена только одна сетевая карта, найдите файл `ifconfig-eth0` (где `eth0` – обозначение Ethernet-карты). Откройте файл настроек в любом редакторе текстовых файлов.
   - Если IP-адрес назначается вам динамически, в поле `BOOTPROTO=` введите **dhcp**. Пример приведен на следующем рисунке.

Рис. 265 Red Hat 9.0: задание динамического IP-адреса в файле ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

   - Если вы используете статический IP-адрес, в поле `BOOTPROTO=` введите **static**. Наберите `IPADDR=` и укажите ваш IP адрес (в десятичном виде через точку), затем наберите `NETMASK=` и укажите маску подсети. Ниже приведен пример для статического IP-адреса 192.168.1.10 и маски подсети 255.255.255.0.

Рис. 266 Red Hat 9.0: задание статического IP-адреса в файле ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.10
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

2 Если вам известны IP-адреса DNS-серверов, укажите параметры DNS в файле `resolv.conf`, находящемся в каталоге `/etc`. В следующем примере настраиваются IP-адреса двух DNS-серверов.

Рис. 267 Red Hat 9.0: настройка DNS в файле resolv.conf

```
nameserver 172.23.5.1
nameserver 172.23.5.2
```

3 После редактирования и сохранения файлов настройки необходимо переинициализировать сетевую плату. Перейдите в каталог `/etc/rc.d/init.d` и введите `./network restart`. Пример приведен на следующем рисунке.

Рис. 268 Red Hat 9.0: повторная инициализация сетевой платы

```
[root@localhost init.d]# network restart

Shutting down interface eth0:                  [OK]
Shutting down loopback interface:              [OK]
Setting network parameters:                    [OK]
Bringing up loopback interface:                [OK]
Bringing up interface eth0:                    [OK]
```

Проверка настроек

Чтобы проверить настройки TCP/IP, на экране терминала введите `ifconfig`.

Рис. 269 Red Hat 9.0: проверка параметров TCP/IP

```
[root@localhost]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:BA:72:5B:44
          inet addr:172.23.19.129  Bcast:172.23.19.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:717 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:730412 (713.2 Kb)  TX bytes:1570 (1.5 Kb)
          Interrupt:10 Base address:0x1000
[root@localhost]#
```

D

Разрешение всплывающих окон, сценариев JavaScript и апплетов Java

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

- На компьютере в веб-браузере нужно разрешить всплывающие окна.
- Сценарии JavaScript (их выполнение разрешено по умолчанию).
- Разрешения на выполнение Java-кода (включены по умолчанию).

Здесь рассмотрены экраны Internet Explorer 6. Экраны в других версиях Internet Explorer могут отличаться.

Блокирование всплывающих окон в Internet Explorer

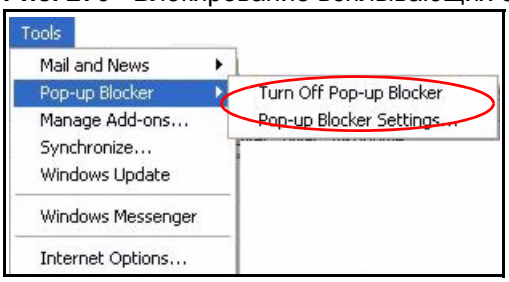
Для входа в устройство может потребоваться отключить блокирование всплывающих окон.

Для этого следует либо полностью отключить блокирование (которое по умолчанию включено Windows XP с пакетом исправлений Service Pack 2), либо включить блокирование, создав исключение для IP-адреса вашего устройства.

Отключение блокирования всплывающих окон

1 В Internet Explorer выберите **Tools** (Сервис), **Pop-up Blocker** (Блокирование всплывающих окон) и выберите **Turn Off Pop-up Blocker** (Отключить блокирование всплывающих окон).

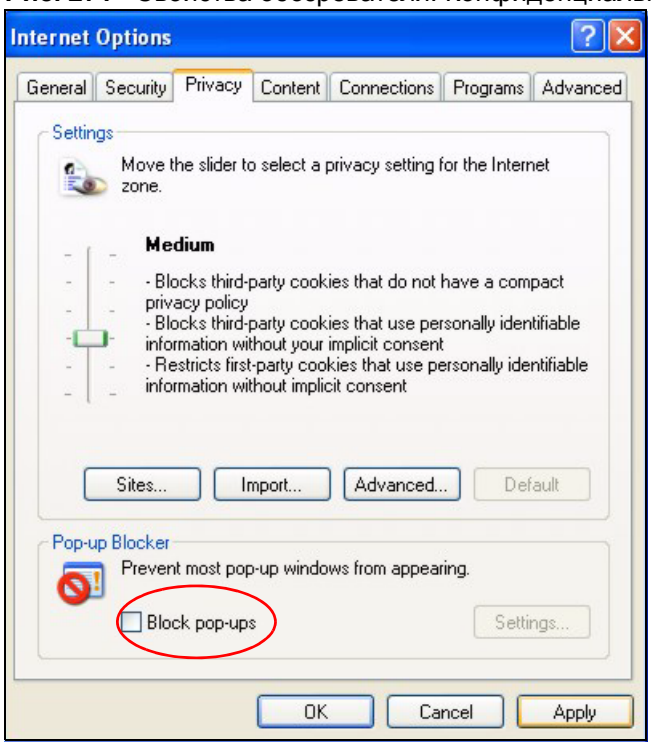
Рис. 270 Блокирование всплывающих окон



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. 271 Свойства обозревателя: Конфиденциальность



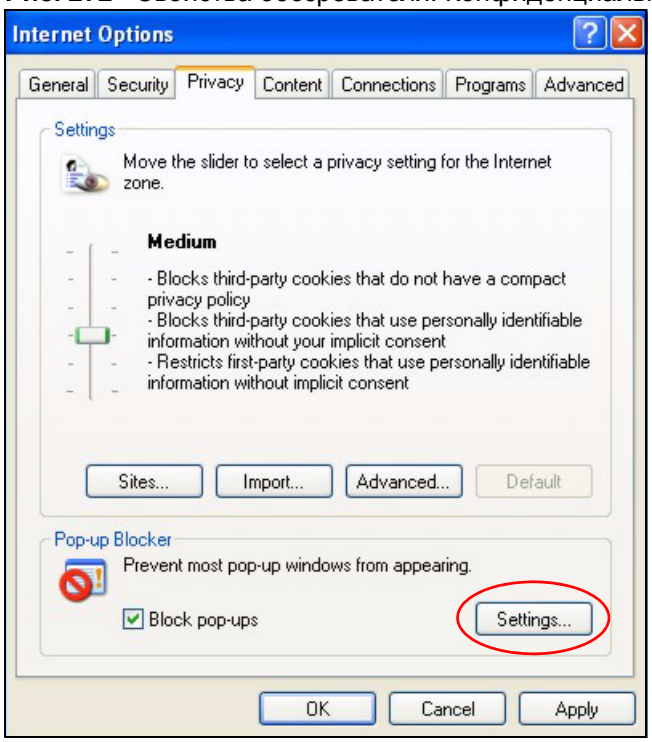
3. Чтобы сохранить настройки, нажмите кнопку **Apply**.

Разрешение всплывающих окон в исключительном порядке

Вместо полного снятия блокирования можно разрешить всплывающие окна только от вашего устройства. Для этого выполните описанные ниже операции.

1. В Internet Explorer выберите **Tools** (Сервис), **Internet Options** (Свойства обозревателя) и перейдите на закладку **Privacy** (Конфиденциальность).
2. Выберите **Settings…** (Параметры), чтобы открыть экран **Pop-up Blocker Settings** (Параметры блокирования всплывающих окон).

Рис. 272 Свойства обозревателя: Конфиденциальность



3 Введите IP-адрес вашего устройства (web-страница, которую Вы не хотите блокировать) с префиксом "http: //". Пример: http://192.168.167.1.

4 Нажмите **Add** (Добавить), чтобы внести IP-адрес в список **Allowed sites** (Разрешенные узлы).

Рис. 273 Параметры блокирования всплывающих окон

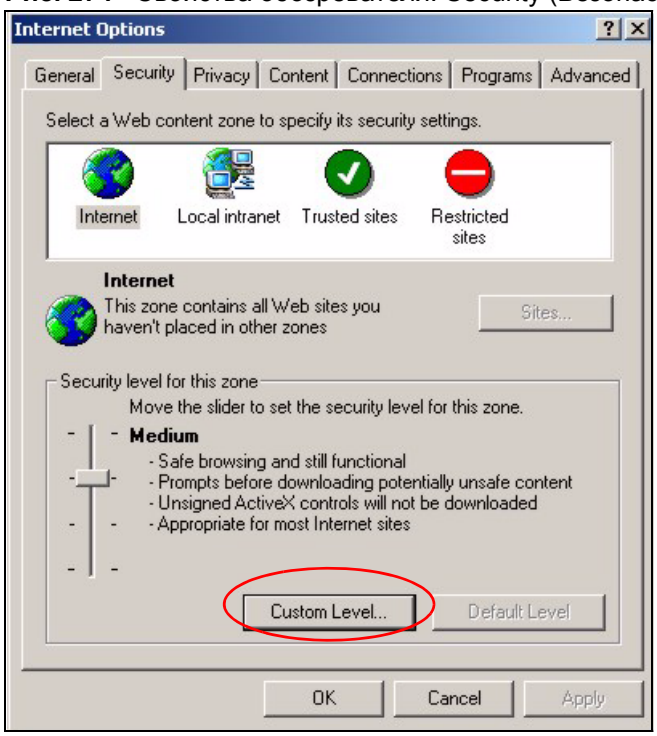
5 Нажмите **Close** (Закрыть), чтобы вернуться на экран **Privacy** (Конфиденциальность).
6 Чтобы сохранить настройки, нажмите кнопку **Apply**.

Сценарии JavaScript

Если страницы веб-конфигуратора в Internet Explorer отображаются неправильно, проверьте, разрешено ли выполнение сценариев JavaScript.

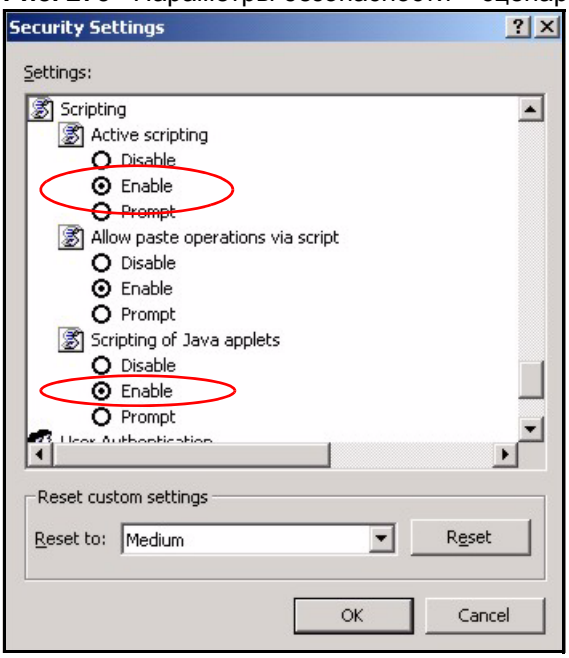
1 В Internet Explorer выберите **Tools** (Сервис), **Internet Options** (Свойства обозревателя) и перейдите на закладку **Security** (Безопасность).

Рис. 274 Свойства обозревателя: Security (Безопасность)



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.

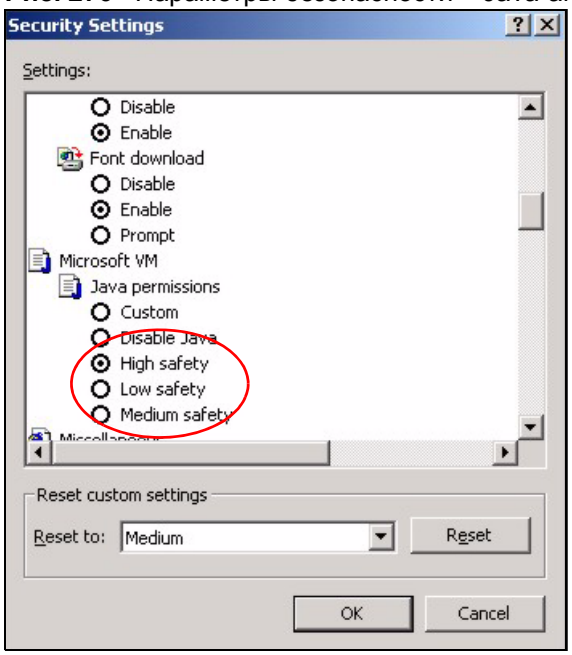
Рис. 275 Параметры безопасности – сценарии JavaScript



Разрешения на выполнение Java-апплетов

1. В Internet Explorer выберите **Tools** (Сервис), **Internet Options** (Свойства обозревателя) и перейдите на закладку **Security** (Безопасность).
2. Нажмите кнопку **Custom Level...** (Другой).
3. Пролистайте список до раздела **Microsoft VM** (Виртуальная машина Microsoft).
4. В подразделе **Java permissions** (Разрешения Java) проверьте, выбран ли уровень безопасности.
5. Нажмите кнопку **OK**, чтобы закрыть окно.

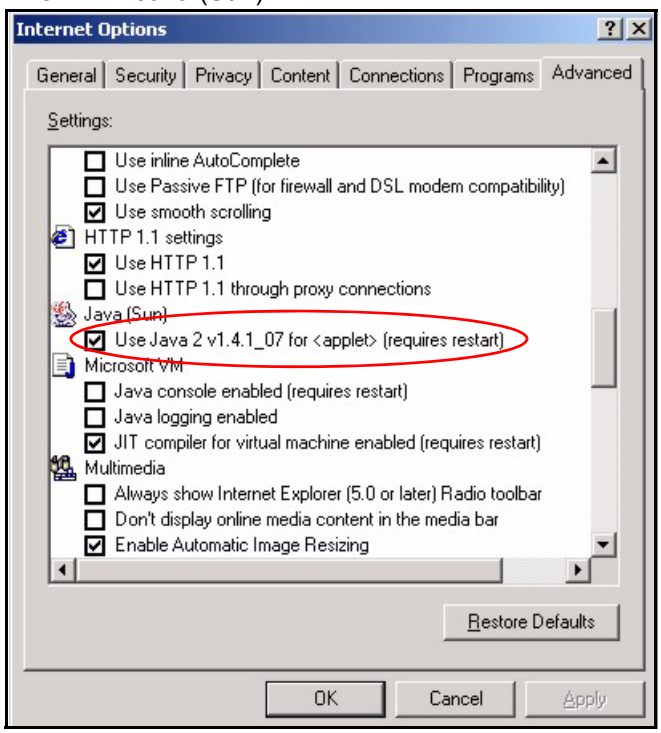
Рис. 276 Параметры безопасности – Java-апплеты



JAVA (Sun)

1. В Internet Explorer выберите **Tools** (Сервис), **Internet Options** (Свойства обозревателя) и перейдите на закладку **Advanced** (Дополнительно).
2. Убедитесь, что в подразделе **Java (Sun)** выбран пункт **Use Java 2 for <applet>**.
3. Нажмите кнопку **OK**, чтобы закрыть окно.

Рис. 277 Java (Sun)



E

IP-адреса и деление на подсети

В этом приложении рассмотрены IP-адреса и маски подсетей.

IP-адреса идентифицируют отдельные устройства в сети. Каждое сетевое устройство (включая компьютеры, серверы, маршрутизаторы, принтеры и т. п.), осуществляющее самостоятельный обмен данными с сетью, должно иметь IP-адрес. Такие сетевые устройства называются хостами.

Маски подсетей определяют максимально возможное число хостов в сети. Маски подсетей можно также использовать для деления одной сети на несколько подсетей.

Общие сведения об IP-адресах

IP-адрес состоит из двух частей: маски подсети и идентификатора хоста. Подобно домам на улице, для которых общим является название улицы, хосты в сети связаны общим номером сети. Уникальным номером, аналогичным номеру дома, в этом случае является идентификатор хоста. Маршрутизаторы ориентируются по номеру подсети для отправки пакетов в соответствующую сеть. Конкретный хост затем находится по идентификатору хоста.

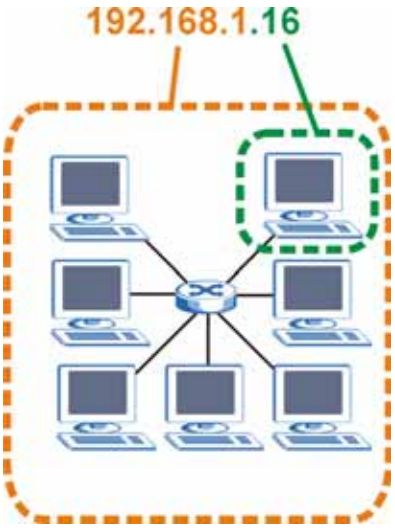
Структура

IP-адрес состоит из четырех частей, которые записываются в десятичной форме через точку, например, 192.168.1.1. Отдельные части называются октетами. Октет – это восьмиразрядное двоичное число (например, 11000000, что в десятичном виде равно 192).

Таким образом каждый октет имеет возможный диапазон значений от 00000000 до 11111111 в двоичном счислении или от 0 до 255 в десятичном счислении.)

На следующем рисунке приведен пример IP-адреса, в котором первые три октета (192.168.1) представляют собой номер сети, а четвертый октет (16) – идентификатор хоста.

Рис. 278 Номер сети и идентификатор хоста



Число разрядов IP-адреса, занимаемое номером подсети или идентификатором хоста, зависит от маски подсети.

Маски подсетей

Маска подсети определяет, какие биты образуют номер сети и какие биты соответствуют идентификатору хоста (с помощью логического "И"). Термин "подсеть" обозначает часть более крупного адресного пространства.

Маска подсети состоит из 32 двоичных разрядов. Если один из разрядов содержит единицу, соответствующий бит в IP-адресе является частью номера сети. Если разряд содержит ноль, соответствующий бит в IP-адресе является частью идентификатора хоста.

В следующем примере приведена маска подсети, в которой отмечены номер сети (жирным шрифтом) и идентификатор хоста в составе IP-адреса (192.168.1.2 в десятичном виде).

Таблица 138 Пример номера сети и идентификатора хоста в IP-адресе

	1-Й ОКТЕТ: (192)	**2-Й ОКТЕТ: (168)**	**3-Й ОКТЕТ: (1)**	**4-Й ОКТЕТ: (2)**
IP-адрес (двоичный)	11000000	10101000	00000001	00000010
Маска подсети (двоичная)	**11111111**	**11111111**	**11111111**	00000000
Номер сети	**11000000**	**10101000**	**00000001**	
Идентификатор хоста				00000010

Маски подсетей принято задавать в виде непрерывной последовательности единиц, начинающейся со старшего бита, за которой следует непрерывная последовательность нулей; обе последовательности в сумме составляют 32 бита.

Маски подсетей часто обозначаются числом разрядов, отводимых под номер сети (т.е. количеством битов, равных единице). Например, термин "8-битная маска" означает, что первые 8 битов маски заполнены единицами, а оставшиеся 24 бита – нулями.

Маски подсетей записываются в десятичном виде через точку, как и IP-адреса. В следующем примере показаны двоичные и десятичные представления для 8-, 16-, 24- и 29-битных масок подсетей.

Таблица 139 Маски подсетей

	ДВОИЧНАЯ				ДЕСЯТИЧНАЯ
	1-Й ОКТЕТ	2-Й ОКТЕТ	3-Й ОКТЕТ	4-Й ОКТЕТ	
8-битная маска	11111111	00000000	00000000	00000000	255.0.0.0
16-битная маска	11111111	11111111	00000000	00000000	255.255.0.0
24-битная маска	11111111	11111111	11111111	00000000	255.255.255.0
29-битная маска	11111111	11111111	11111111	11111000	255.255.255.248

Размер сети

Разрядность номера сети определяет максимальное число хостов, которое может содержаться в сети. Чем больше битов содержит номер, тем меньше битов доступно для использования в качестве идентификаторов хостов.

IP-адрес, в котором идентификатор хоста состоит целиком из нулей, является IP-адресом сети (пример – 192.168.1.0 с 24-битной маской). IP-адрес, в котором идентификатор хоста состоит целиком из единиц, является широковещательным адресом (пример – 192.168.1.255 с 24-битной маской).

Поскольку эти два IP-адреса не могут использоваться конкретными хостами, вычислить максимальное возможное число хостов в сети можно следующим образом:

Таблица 140 Максимально возможное число хостов

МАСКА ПОДСЕТИ		РАЗМЕР ИДЕНТИФИКАТОРА ХОСТА		МАКСИМАЛЬНОЕ ЧИСЛО ХОСТОВ
8 битов	255.0.0.0	24 битов	$2^{24} – 2$	16777214
16 битов	255.255.0.0	16 битов	$2^{16} – 2$	65534
24 битов	255.255.255.0	8 битов	$2^{8} – 2$	254
29 битов	255.255.255.248	3 битов	$2^{3} – 2$	6

Способ записи

Поскольку маска всегда состоит из непрерывной последовательности единиц и непрерывной последовательности нулей, достаточно указывать только число единиц, не записывая значение каждого октета. Для этого обычно после адреса указывается знак "/", за которым следует число единиц в маске подсети.

Например, обозначение 192.1.1.0 /25 соответствует номеру 192.1.1.0 с маской подсети 255.255.255.128.

В следующей таблице представлены некоторые допустимые маски подсетей, записанные обоими способами.

Таблица 141 Альтернативный способ записи маски подсети

МАСКА ПОДСЕТИ	АЛЬТЕРНАТИВНЫЙ СПОСОБ ЗАПИСИ	ПОСЛЕДНИЙ ОКТЕТ (ДВОИЧНЫЙ)	ПОСЛЕДНИЙ ОКТЕТ (ДЕСЯТИЧНЫЙ)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

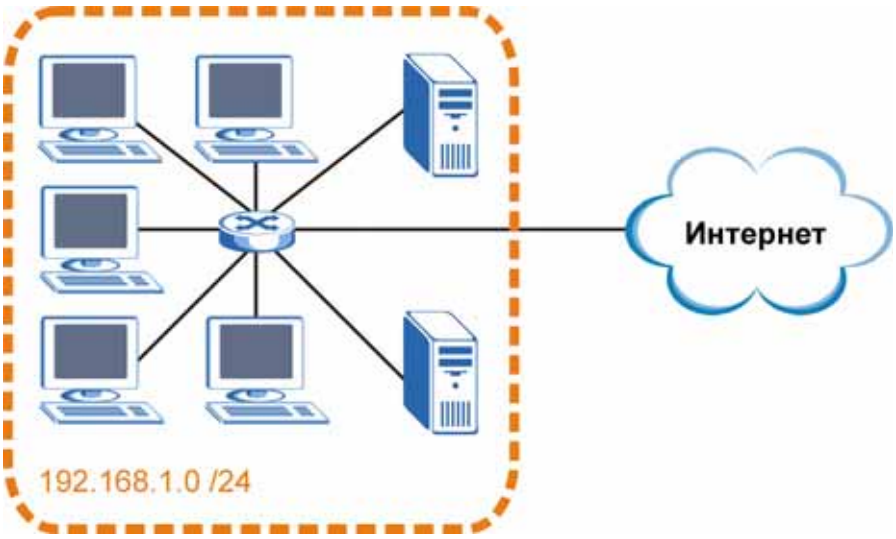
Деление на подсети

Подсети можно использовать для деления одной сети на несколько меньших сегментов. В следующем примере системный администратор создает две подсети, чтобы изолировать группу серверов от остальной части сети по соображениям безопасности.

В этом примере сеть компании имеет адрес 192.168.1.0. Первые три цифры адреса (192.168.1) относятся к номеру подсети, а оставшийся октет содержит идентификатор хоста, обеспечивая до $2^8 – 2 = 254$ возможных хостов.

Структура сети компании до деления на подсети приведена на следующем рисунке.

Рис. 279 Пример деления на подсети: до деления

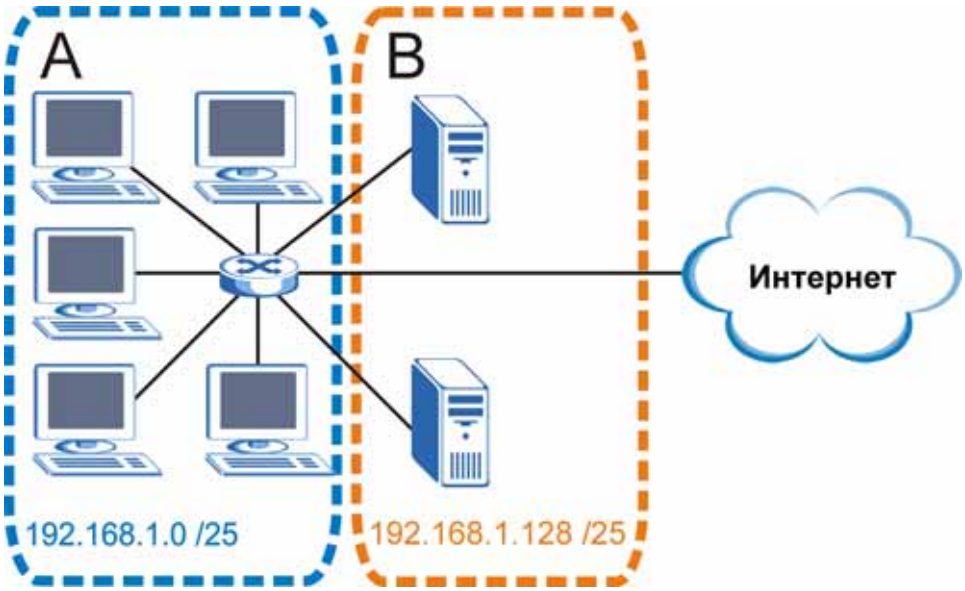


Для деления сети 192.168.1.0 на две логические подсети можно "позаимствовать" один из битов идентификатора хоста. Маска подсети теперь состоит из 25 битов (255.255.255.128 или /25).

"Позаимствованный" бит идентификатора хоста может принимать значения 0 и 1, давая в итоге две подсети: 192.168.1.0 /25 и 192.168.1.128 /25.

Структура сети компании после деления на подсети приведена на следующем рисунке. Теперь имеются две подсети: **A** и **B**.

Рис. 280 Пример деления на подсети: после деления



В 25-битовой подсети идентификатор хоста имеет длину 7 битов, таким образом, каждая подсеть может содержать до $2^7 – 2 = 126$ хостов (идентификатор хоста, целиком состоящий из нулей, используется как адрес подсети, а идентификатор, целиком состоящий из единиц, обозначает широковещательный адрес).

192.168.1.0 с маской 255.255.255.128 - это адрес самой подсети **A**, а 192.168.1.127 с маской 255.255.255.128 - это целевой адрес широковещательной рассылки для данной подсети. Таким образом, непосредственным хостам в подсети **A** могут назначаться адреса от 192.168.1.1 до 192.168.1.126 включительно.

Аналогично, для подсети **B** диапазон адресов хостов – от 192.168.1.129 до 192.168.1.254.

Пример: четыре подсети

В рассмотренном выше примере применялась 25-разрядная маска подсети для деления 24-битного адреса пространства на две подсети. Аналогичным образом 24-битный адрес можно поделить и на четыре подсети; для этого необходимо "позаимствовать" из номера хоста два бита, которые вместе имеют следующие возможные значения: 00, 01, 10 и 11). Маска подсети состоит из 26 битов: 11111111.11111111.11111111.**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 (идентификаторы хостов, целиком состоящие из нулей, идентифицируют саму подсеть, а идентификатор, целиком состоящий из единиц, используется для широковещательной рассылки в подсети).

Таблица 142 Подсеть 1

IP-АДРЕС/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ДВОИЧНОЕ ЗНАЧЕНИЕ ПОСЛЕДНЕГО ОКТЕТА
IP-адрес (десятичный)	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	

Таблица 143 Подсеть 2

IP-АДРЕС/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ДВОИЧНОЕ ЗНАЧЕНИЕ ПОСЛЕДНЕГО ОКТЕТА
IP Address (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	

Таблица 144 Подсеть 3

IP-АДРЕС/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ДВОИЧНОЕ ЗНАЧЕНИЕ ПОСЛЕДНЕГО ОКТЕТА
IP Address (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	

Таблица 145 Подсеть 4

IP-АДРЕС/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ДВОИЧНОЕ ЗНАЧЕНИЕ ПОСЛЕДНЕГО ОКТЕТА
IP Address (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: восемь подсетей

Аналогичным образом можно создать восемь подсетей, используя 27-разрядную маску (000, 001, 010, 011, 100, 101, 110 и 111).

В следующей таблице приведены значения последнего октета IP-адреса для каждой подсети.

Таблица 146 Восемь подсетей

ПОДСЕТЬ	АДРЕС ПОДСЕТИ	ПЕРВЫЙ АДРЕС	ПОСЛЕДНИЙ АДРЕС	ШИРОКОВЕЩАТЕЛЬНЫЙ АДРЕС
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

Планирование структуры подсетей

В следующей таблице перечислены варианты деления на подсети для сети с 24-битным номером.

Таблица 147 Планирование подсетей в сети с 24-битным номером

ЧИСЛО "ЗАИМСТВОВАННЫХ" БИТОВ ИДЕНТИФИКАТОРА ХОСТА	МАСКА ПОДСЕТИ	ЧИСЛО ПОДСЕТЕЙ	КОЛИЧЕСТВО ХОСТОВ В ОДНОЙ ПОДСЕТИ
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

В следующей таблице перечислены варианты деления на подсети для сети с 16-битным номером.

Таблица 148 Планирование подсетей в сети с 16-битным номером

ЧИСЛО "ЗАИМСТВОВАННЫХ" БИТОВ ИДЕНТИФИКАТОРА ХОСТА	МАСКА ПОДСЕТИ	ЧИСЛО ПОДСЕТЕЙ	КОЛИЧЕСТВО ХОСТОВ В ОДНОЙ ПОДСЕТИ
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Настройка IP-адресов

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

Если поставщик услуг Интернета не сообщил вам номер IP-подсети в явном виде, то наиболее вероятно, что вы используете единственную учетную запись пользователя, и поставщик услуг Интернета назначит вам динамический IP-адрес при установлении соединения. В этом случае рекомендуется выбрать номер сети из диапазона от 192.168.0.0 до 192.168.255.0. Комитет по цифровым адресам в Интернете (Internet Assigned Number Authority, IANA) зарезервировал определенные диапазоны адресов специально для частных применений; все адреса, которые не принадлежат этим диапазонам, не должны использоваться без специальных на то указаний. Также необходимо включить на P-793H трансляцию сетевых адресов (NAT).

После выбора номера сети выберите для P-793H легко запоминающийся IP-адрес, например, 192.168.1.1, но убедитесь, что этот адрес не используется никаким другим устройством в вашей сети.

Маска подсети указывает на долю номеров IP-адресов в сети. P-793H автоматически вычисляет маску подсети на основе назначаемого пользователем IP-адреса. В отсутствие специальных указаний изменять маску подсети, предлагаемую P-793H, не следует.

Частные IP-адреса

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

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

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

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

F

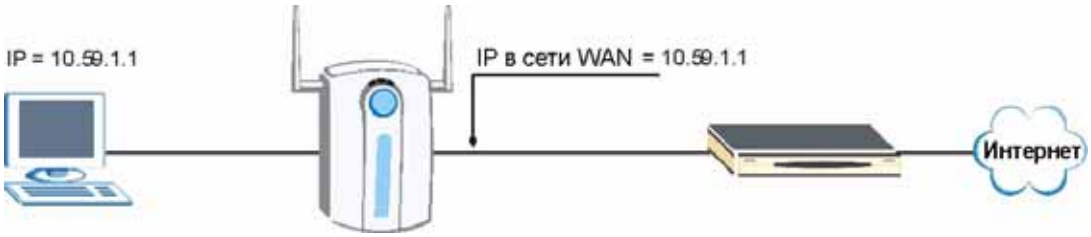
Конфликты в присвоении IP-адресов

В данном приложении рассматриваются ситуации, в которых могут возникнуть конфликты IP-адресов. Абоненты с дублирующимися IP-адресами не смогут выходить в Интернет.

Случай A: P-793H работает с одним и тем же IP-адресом в сетях LAN и WAN

На следующем рисунке показан пример, в котором P-793H использует IP-адрес на стороне WAN, совпадающий с IP-адресом компьютера в сети LAN.

Рис. 281 Конфликты IP-адресов: случай A

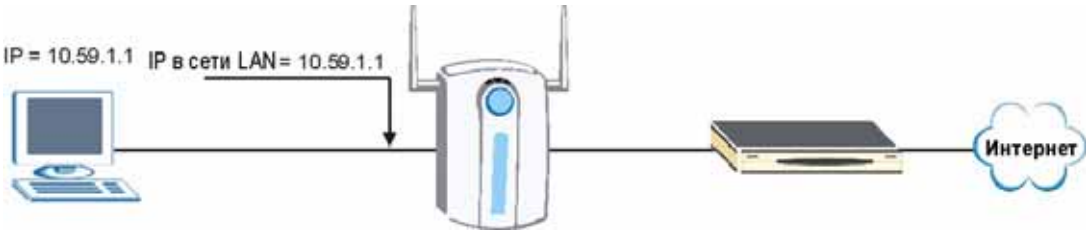


Если в P-793H включен DHCP-сервер, необходимо задать для P-793H различные IP-адреса LAN и WAN из непересекающихся подсетей. Например, в сети WAN можно назначить IP-адрес 192.59.1.1 а в сети LAN - адрес 10.59.1.1. В остальных случаях рекомендуется использовать для P-793H глобальный IP-адрес в сети WAN.

Случай B: IP-адрес P-793H в сети LAN конфликтует с IP-адресом DHCP-клиента

На следующем рисунке рассмотрена работа P-793H в качестве DHCP-сервера. IP-адрес, присвоенный устройством P-793H DHCP-клиенту в локальной сети, совпал с IP-адресом порта LAN.

Рис. 282 Конфликты IP-адресов: случай B

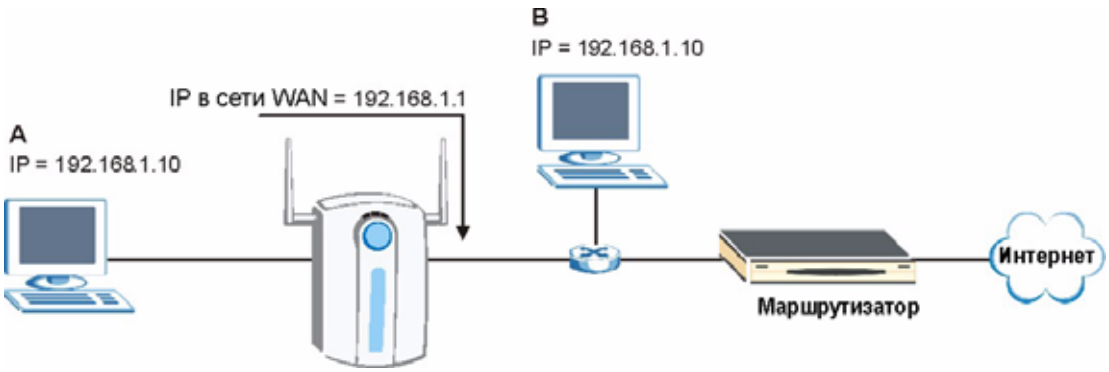


Чтобы разрешить эту проблему, необходимо убедиться, что IP-адрес P-793H на стороне LAN не входит в пул IP-адресов DHCP.

Случай C: IP-адрес абонента совпадает с IP-адресом сетевого устройства

На следующем рисунке приведен пример, в котором IP-адрес абонента совпадает с IP-адресом некоего сетевого устройства, не подключенного напрямую к P-793H.

Рис. 283 Конфликты IP-адресов: случай C



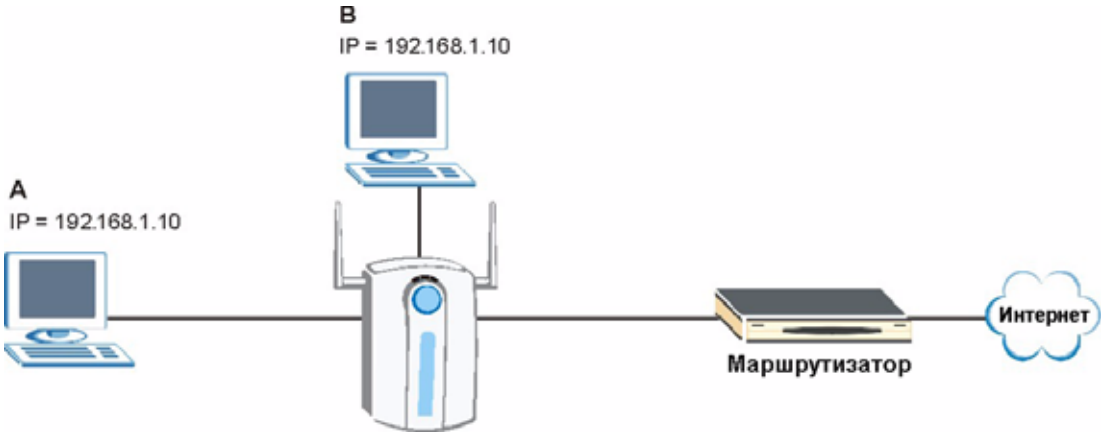
Если в P-793H включен DHCP-сервер, необходимо задать для P-793H различные IP-адреса LAN и WAN из непересекающихся подсетей. Например, в сети WAN можно назначить IP-адрес 192.59.1.1 а в сети LAN - адрес 10.59.1.1. В остальных случаях рекомендуется использовать для P-793H глобальный IP-адрес в сети WAN.

Случай D: двое или несколько абонентов имеют одинаковый IP-адрес.

Преобразуя все частные IP-адреса в IP-адрес, используемый в сети WAN, P-793H обеспечит выход в Интернет пользователям с различными настройками сети. Однако в некоторых ситуациях два или более абонентов могут иметь одинаковый частный IP-адрес. Это происходит, в частности, в тех случаях, когда настроенный у одного из абонентов статический (фиксированный) IP-адрес совпадает с адресом, присвоенным DHCP-сервером устройства P-793H другому абоненту, чей компьютер является клиентом DHCP.

При этом абоненты не смогут выходить в Интернет.

Рис. 284 Конфликты IP-адресов: случай D



Для устранения этой проблемы необходимо включить в сеть коммутатор с поддержкой VLAN или перевести все компьютеры в режим динамического получения IP-адресов.

G

Распространенные сетевые службы

В следующей таблице перечислены часто используемые сетевые службы и соответствующие им типы протоколов и номера портов. Подробный перечень номеров портов и сетевых служб, а также кодов и типов сообщений ICMP см. на сайте IANA (Комитета по цифровым адресам в Интернете).

- **Наименование**: это краткое название службы. Можно использовать это название или указать другое.
- **Протокол**: это тип протокола IP, используемого данной службой. Если в этом поле указано **TCP/UDP**, то для данной службы на одном номере порта используются одновременно TCP и UDP. Если в качестве протокола указан **ПОЛЬЗОВАТЕЛЬСКИЙ**, то в графе **Порт(ы)** указан номер протокола IP, а не номер порта.
- **Порт(ы)**: значение зависит от содержимого поля **Протокол**. Дополнительные сведения о номерах портов см. в документе RFC 1700.
  - Если в графе **Протокол** указан **TCP**, **UDP** или **TCP/UDP**, здесь приводится номер порта IP.
  - Если в графе **Протокол** указан **ПОЛЬЗОВАТЕЛЬСКИЙ**, здесь приводится номер протокола IP.
- **Описание**: ниже приведено краткое описание применений каждой службы и ситуаций, в которых она используется.

Таблица 149 Часто используемые сетевые службы

НАИМЕНОВАНИЕ	ПРОТОКОЛ	ПОРТ(Ы)	ОПИСАНИЕ
AH (IPSEC_TUNNEL)	Пользовательский	51	Эта служба используется протоколом туннелирования IPSEC AH (Authentication Header – заголовок аутентификации).
AIM/New-ICQ	TCP	5190	Служба мгновенного обмена сообщениями America Online. Этот порт также используется ICQ по умолчанию в качестве входного порта.
AUTH	TCP	113	Протокол аутентификации, используемый некоторыми серверами.
BGP	TCP	179	Протокол для граничных маршрутизаторов.
BOOTP_CLIENT	UDP	68	DHCP-клиент.

Таблица 149 Часто используемые сетевые службы (продолжение)

НАИМЕНОВАНИЕ	ПРОТОКОЛ	ПОРТ(Ы)	ОПИСАНИЕ
BOOTP_SERVER	UDP	67	DHCP-сервер.
CU-SEEME	TCP UDP	7648 24032	Популярное решение для видеоконференций, разработанное White Pines Software.
DNS	TCP/UDP	53	Сервер доменных имен. Служба, которая ставит в соответствие буквенным адресам (например, www.zyxel.com) IP-адреса.
ESP (IPSEC_TUNNEL)	Пользовательский	50	Эта служба используется протоколом IPSEC ESP (Encapsulation Security Protocol – протокол защищенного сокрытия содержания).
FINGER	TCP	79	Finger – команда, позволяющая проверять состояние пользователя в системах UNIX или Интернете.
FTP	TCP TCP	20 21	Протокол передачи файлов используется для пересылки файлов, в особенности – больших объемов данных, которые невозможно передать по электронной почте.
H.323	TCP	1720	Этот протокол используется программой NetMeeting.
HTTP	TCP	80	Протокол передачи гипертекста – клиент-серверный протокол для "Всемирной паутины".
HTTPS	TCP	443	HTTPS - защищенный сеанс HTTP, часто используемый в электронной коммерции.
ICMP	Пользовательский	1	Межсетевой протокол контрольных сообщений часто используется в диагностических целях или для установления маршрутов.
ICQ	UDP	4000	Это популярная программа для общения в Интернете.
IGMP (MULTICAST)	Пользовательский	2	Протокол Internet Group Multicast Protocol используется при отправке пакетов отдельной группе хостов.
IKE	UDP	500	Для распространения ключей и управления ключами используется алгоритм IKE (Internet Key Exchange – обмен ключами в Интернете).
IRC	TCP/UDP	6667	Это популярная служба для общения (чата) в Интернете.
MSN Messenger	TCP	1863	Служба мгновенного обмена сообщениями Microsoft Network использует этот протокол.
NEW-ICQ	TCP	5190	Программа для общения в Интернете.
NEWS	TCP	144	Протокол для групп новостей.

Таблица 149 Часто используемые сетевые службы (продолжение)

НАИМЕНОВАНИЕ	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 Grouper) – это протокол отправки эхозапросов ICMP для проверки доступности удаленного хоста.
POP3	TCP	110	Почтовый протокол версии 3 позволяет клиентскому компьютеру получать электронную почту с сервера POP3 по временному соединению (посредством TCP/IP или другого протокола).
PPTP	TCP	1723	Двухточечный протокол туннелирования обеспечивает защищенную передачу данных по сетям общего пользования. Эта служба соответствует управляющему каналу.
PPTP_TUNNEL (GRE)	Пользовательский	47	Двухточечный протокол туннелирования обеспечивает защищенную передачу данных по сетям общего пользования. Эта служба соответствует каналу данных.
RCMD	TCP	512	Служба удаленного выполнения команд.
REAL_AUDIO	TCP	7070	Протокол поточной передачи аудиоданных, обеспечивающий передачу звука в реальном времени по WWW.
REXEC	TCP	514	Демон удаленного выполнения команд.
RLOGIN	TCP	513	Служба удаленного входа в систему.
RTELNET	TCP	107	Удаленный Telnet.
RTSP	TCP/UDP	554	Протокол поточного вещания в реальном времени (RTSP) – это служба дистанционного управления мультимедиа-вещанием в Интернете.
SFTP	TCP	115	Упрощенный протокол передачи файлов.
SMTP	TCP	25	Простой протокол передачи почты – стандарт обмена почтовыми сообщениями в Интернете. SMTP позволяет передавать сообщения от одного почтового сервера к другому.
SNMP	TCP/UDP	161	Упрощенный протокол управления сетью.
SNMP-TRAPS	TCP/UDP	162	Прерывания, используемые SNMP (RFC:1215).

Таблица 149 Часто используемые сетевые службы (продолжение)

НАИМЕНОВАНИЕ	ПРОТОКОЛ	ПОРТ(Ы)	ОПИСАНИЕ
SQL-NET	TCP	1521	Язык структурированных запросов (SQL) – интерфейс для доступа к данным в различных СУБД, включая СУБД на мейнфреймах, системах среднего уровня, UNIX-системах и сетевых серверах.
SSH	TCP/UDP	22	Программа для защищенного удаленного входа в системную оболочку.
STRM WORKS	UDP	1558	Протокол Stream Works.
SYSLOG	UDP	514	SYSLOG позволяет оставлять сообщения в файле журнала на UNIX-сервере.
TACACS	UDP	49	Протокол хоста регистрации (Terminal Access Controller Access Control System – система управления доступом для контроля доступа к оконечным узлам).
TELNET	TCP	23	Telnet – протокол регистрации в системе и эмуляции терминала, распространенный в Интернете и в среде UNIX. Он предназначен для работы по сетям TCP/IP. Его основное назначение – обеспечить дистанционный доступ пользователей к хостам.
TFTP	UDP	69	TFTP (упрощенный протокол пересылки файлов) – протокол передачи файлов в Интернете, подобный FTP, но использующий UDP (протокол пользовательских датаграмм) вместо TCP (протокол управления передачей).
VDOLIVE	TCP	7000	Альтернативное решение для проведения видеоконференций.

H

Интерпретатор команд

Ниже приведено описание интерпретатора команд. Способ вызова интерпретатора команд из SMT описан в разд. 35.1 на стр. 359. Более подробное описание этих команд см. на сайте www.zyxel.com.

Использование недокументированных команд или некорректное выполнение настроек может нарушить работоспособность устройства или вывести его из строя.

Синтаксис команд

- Ключевые слова команд выделены шрифтом `courier new`.
- Введите ключевые слова команд именно так, как показано ниже, не сокращая.
- Обязательные поля команды заключены в угловые скобки <>.
- Необязательные поля команды заключены в квадратные скобки `[]`.
- Знак " | " означает "или".
  Например,
  sys filter netbios config <type> <on|off>
  означает, что необходимо указать тип фильтра netbios и то, нужно ли его включить или выключить.

Использование команд

Список действительных команд можно найти, введя `help` или `?` в командной строке. Всегда вводите команду полностью. Чтобы завершить сеанс, введите `exit`.

Примеры команд

В этом разделе приведены примеры команд, поддерживаемых P-793H. Этот список приведен для примера и носит ориентировочный характер. Команды, поддерживаемые вашим устройством P-793H, могут отличаться от приведенных примеров. Дополнительные примеры см. в приложениях.

Настройка содержания журнала P-793H

1. Команда `sys logs load` загружает буфер настроек журнала, позволяющий задать типы журналов, которые будет вести устройство P-793H.
2. Список категорий журналов можно просмотреть с помощью команды `sys logs category`.

Рис. 285 Пример просмотра списка категорий журналов

```
ras> sys logs category
8021x           access          attack          display
error           icmp            ike             ipsec
javablocked     mten            packetfilter    ppp
cdr             pki             tls             remote
tcpreset        traffic         upnp            urlblocked
urlforward      wireless
```

3. Чтобы просмотреть список параметров, доступных для конкретной категории, наберите команду `sys logs category`, следом указав тип категории.

Рис. 286 Пример просмотра параметров ведения журнала

```
ras> sys logs category access
Использование: [0:none/1:log/2:alert/3:both] [0:don't show debug type/1:show
debug type]
```

4. Чтобы задать типы журнальных сообщений, наберите команду `sys logs category`, следом указав тип категории и параметр.

   0 отключает ведение журналов для данной категории, 1 указывает регистрировать только журнальные сообщения для данной категории, 2 – регистрировать только предупреждения для данной категории, 3 – регистрировать для данной категории и журнальные сообщения, и предупреждения. Для некоторых категорий определенные параметры могут быть недоступны.
5. Команда `sys logs save` служит для сохранения параметров в P-793H (ее необходимо выполнить для сохранения журналов).

Просмотр журналов

- Команда `sys logs display` служит для просмотра всех сообщений в журнале P-793H.
- Команда `sys logs category display` служит для просмотра настроек журналов или для просмотра всех категорий журналов.
- Команда `sys logs display [log category]` служит для просмотра отдельной категории журналов P-793H.
- Команда `sys logs clear` служит для удаления всех журналов P-793H.

Пример команд для работы с журналами

В этом примере выполняется настройка P-793H для ведения журналов доступа и предупреждений, после чего вызывается просмотр результатов.

```
ras> sys logs load
ras> sys logs category access 3
ras> sys logs save
ras> sys logs display access

#  .time                 source                  destination            notes

    message
  0|06/08/2004 05:58:21 |172.21.4.154          |224.0.1.24            |ACCESS
BLOCK
    Firewall default policy: IGMP (W to W/ZW)
  1|06/08/2004 05:58:20 |172.21.3.56           |239.255.255.250       |ACCESS
BLOCK
    Firewall default policy: IGMP (W to W/ZW)
  2|06/08/2004 05:58:20 |172.21.0.2            |239.255.255.254       |ACCESS
BLOCK
    Firewall default policy: IGMP (W to W/ZW)
  3|06/08/2004 05:58:20 |172.21.3.191          |224.0.1.22            |ACCESS
BLOCK
    Firewall default policy: IGMP (W to W/ZW)
  4|06/08/2004 05:58:20 |172.21.0.254          |224.0.0.1             |ACCESS
BLOCK
    Firewall default policy: IGMP (W to W/ZW)
  5|06/08/2004 05:58:20 |172.21.4.187:137      |172.21.255.255:137    |ACCESS
BLOCK
    Firewall default policy: UDP (W to W/ZW)
```

Команда routing

Синтаксис: `ip nat routing [0:LAN] [0:no|1:yes]`

Эта команда указывает P-793H пересылать через определенный интерфейс весь трафик, не подпадающий под правила NAT. Эта функция может использоваться, например, в том случае, если к локальной сети подключены серверы с глобальными (внешними) IP-адресами.

В следующем примере P-793H пересылает весь трафик, для которого отсутствуют правила NAT, через интерфейс LAN.

Рис. 287 Пример вызова команды routing

```
ras> ip nat routing 2 0
Routing can work in NAT when no NAT rule match.
------------------------------------------------
         LAN : yes
```

Обработка ARP и группа команд ARP ackGratuitous

P-793H не принимает отклики ARP, если от P-793H не был отправлен соответствующий запрос. Это исключает возможность подмены IP- и MAC-адресов в таблицы ARP P-793H путем отправки фальсифицированного отклика ARP. Наличие неверной привязки IP-адреса к MAC-адресу в таблице ARP P-793H может использоваться для пересылки пакетов через P-793H на иные устройства вместо изначального адресата.

Команды для обработки и игнорирования произвольных запросов ARP

Хост может отправить запрос ARP для разрешения своего собственного IP-адреса. Такой запрос называется произвольным (gratuitous). IP-адреса отправителя и получателя в пакете запроса указывают на сам хост. В качестве MAC-адреса получателя в пакете содержится широковещательный адрес Ethernet (FF:FF:FF:FF:FF:FF). Это позволяет определить, имеются ли в сети другие хосты, IP-адреса которых совпадают с IP-адресом изготовителя. Кроме того, другие хосты в сети получают возможность обновить свои таблицы ARP, включив в них IP-адрес хоста и соответствующий ему MAC-адрес.

Команды `ip arp ackGratuitous` задают режим обработки произвольных запросов ARP на P-793H.

- Чтобы указать P-793H игнорировать произвольные запросы ARP, введите команду `ip arp ackGratuitous active no`.
- Чтобы указать P-793H отвечать на произвольные запросы ARP, введите команду `ip arp ackGratuitous active yes`.

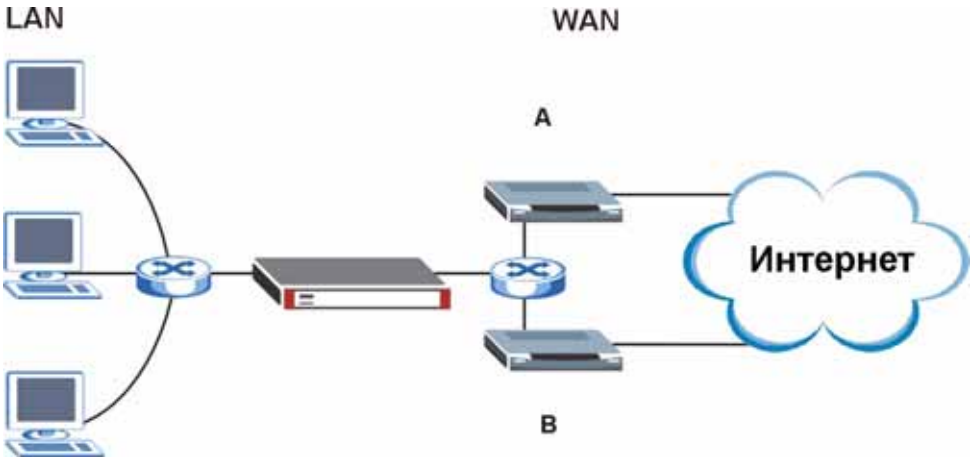
  Рассмотрим следующий пример: обычно используемый шлюз становится недоступен, и резервный шлюз отправляет произвольный запрос ARP. Если IP-адрес, к которому относится запрос, отсутствует в таблице ARP P-793H, то P-793H отправляет запрос ARP, чтобы определить, какой хост использует данный IP-адрес. После получения ответа от резервного шлюза P-793H добавляет новую запись в таблицу ARP.

  Если в таблице ARP P-793H уже содержится запись с соответствующим IP-адресом, то ответ P-793H будет зависеть от режима, выбранного командой `ip arp ackGratuitous forceUpdate`.

  - Команда `ip arp ackGratuitous forceUpdate on` указывает P-793H принудительно заменить MAC-адрес в таблице ARP.
  - Команда `ip arp ackGratuitous forceUpdate off` отключает замену MAC-адреса в таблице ARP P-793H.

Использование резервного шлюза (см. следующий рисунок) является одним из случаев, когда принудительное обновление таблицы ARP в ответ на произвольные запросы необходимо. В определенный момент шлюз A перестает работать, и его место занимает резервный шлюз (B) с тем же статическим IP-адресом, что и у шлюза A. Шлюз B рассылает широковещательный запрос ARP для нахождения хоста, использующего его IP-адрес. Если параметр ackGratuitous включен и установлен в режим принудительного обновления, P-793H примет произвольный запрос ARP и обновит свою таблицу ARP. В результате на P-793H будет храниться актуальная таблица ARP, позволяющая пересылать пакеты через резервный шлюз. Если параметр ackGratuitous отключен или принудительное обновление не выбрано, P-793H не обновит параметры записи в таблице ARP и не сможет пересылать пакеты через шлюз B.

Рис. 288 Резервный шлюз



Обновление записей ARP может сделать сеть более уязвимой к атакам с подменой адресов. Параметр ackGratuitous и принудительное обновление рекомендуется включать только в том случае, если они необходимы, как в рассмотренном примере с резервным шлюзом. Включение принудительного обновления во всех случаях представляет повышенную опасность, поскольку P-793H будет обновлять таблицу ARP даже в том случае, если соответствующая запись в ней уже существует.

Задание длины ключа для шифрования AES на фазе 2 IPSec

Синтаксис: `ipsec ipsecConfig encryKeyLen <0:128 | 1:192 | 2:256>`

По умолчанию для туннелей IPSec на фазе 2 P-793H использует 128-битный ключ AES. Эта команда позволяет отредактировать существующее правило VPN для использования более длинного ключа AES.

См. следующий пример. Предположим, что имеется правило VPN, в котором задано использование AES для шифрования на фазе 2 и его необходимо настроить на шифрование со 192-битным ключом.

- Первая строка начинает редактирование правила VPN.
- Вторая строка задает для правила VPN 1 использование 192-битного шифрования AES на фазе 2.
- Третья строка выводит на экран результаты.

Рис. 289 Пример вызова команды routing

```
ras> ipsec ipsecEdit 1
ras> ipsec ipsecConfig encryKeyLen 1
ras> ipsec ipsecDisplay
---------- IPSec Setup ----------
Index #= 1     Active= No    Multi Pro = No    Protocol= 0 Global SW= 0xA
Bound IKE 9999   NailUp = No   Netbios = No   Name= test

ControlPing = No  LogControlPing = No  Control ping address = 0.0.0.0
Local:  Addr Type= SINGLE      Port Start= 0         End= N/A
        IP Addr Start= 0.0.0.0              Mask= N/A
Remote: Addr Type= SINGLE      Port Start= 0         End= N/A
        IP Addr Start= 0.0.0.0              Mask= N/A
Enable Replay Detection= No    Key Management= IKE
Phase 2 - Active Protocol= ESP
          Encryption Algorithm= AES    Authentication Algorithm= SHA1
          Encryption Key Length = 192
          SA Life Time (Seconds)= 28800
          Encapsulation= Tunnel   Perfect Forward Secrecy (PFS)= None
ras>
```

I

Формат журналов

В этом приложении приведены расшифровки сообщений в журналах.

Таблица 150 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.
`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.

Таблица 150 Журналы обслуживания системы (продолжение)

СООБЩЕНИЕ	ОПИСАНИЕ
SSH login failed	Пользователю не удалось войти в маршрутизатор через встроенный SSH-сервер.
Successful HTTPS login	Пользователь вошел в веб-конфигуратор маршрутизатора по протоколу HTTPS.
HTTPS login failed	Пользователю не удалось войти в веб-конфигуратор маршрутизатора по протоколу HTTPS.

Таблица 151 Системные журналы ошибок

СООБЩЕНИЕ	ОПИСАНИЕ
%s exceeds the max. number of session per host!	При очередной попытке создания сеанса NAT было превышено ограничение на емкость таблицы сеансов NAT для конкретного хоста.
setNetBIOSFilter: calloc error	Маршрутизатор не смог выделить память для параметров настройки фильтра NetBIOS.
readNetBIOSFilter: calloc error	Маршрутизатор не смог выделить память для параметров настройки фильтра NetBIOS.
WAN connection is down.	Соединение с WAN отсутствует. Вы не можете получить доступ к сети через этот интерфейс.

Таблица 152 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.
Packet without a NAT table entry blocked: [TCP | UDP | IGMP | ESP | GRE | OSPF]	Маршрутизатор заблокировал пакет, для которого отсутствует соответствующая запись в таблице NAT.
Router sent blocked web site message: TCP	Маршрутизатор отправил сообщение, уведомляющее пользователя о том, что в маршрутизаторе заблокирован доступ к запрошенному пользователем веб-сайту.

Таблица 153 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 времени ожидания динамического сеанса межсетевого экрана: По умолчанию приняты следующие периоды ожидания: Время ожидания ICMP: 3 минуты. Время ожидания UDP: 3 минуты. Время ожидания TCP-соединения (трехэтапное согласование): 270 секунд. Время ожидания TCP FIN: 2 MSL (максимальных периода существования сегмента, установленных в заголовке TCP). Период неактивности установленного TCP-соединения: 150 минут. Время ожидания сброса TCP-соединения: 10 секунд.
`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").

Таблица 154 Журналы фильтрации пакетов

СООБЩЕНИЕ	ОПИСАНИЕ
`[TCP | UDP | ICMP | IGMP | Generic] packet filter matched (set:%d, rule:%d)`	Попытка доступа совпала с настроенным правилом фильтра (набор и номер правила указаны в скобках) и была заблокирована или разрешена согласно правилу.

Таблица 155 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. Расшифровку типов и кодов см. в таб. 167 на стр. 451.
`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. Расшифровку типов и кодов см. в таб. 167 на стр. 451.
`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.

Таблица 156 Журналы вызовов (CDR)

СООБЩЕНИЕ	ОПИСАНИЕ
`board%d line%d channel%d, call%d,%s C01 Outgoing Call dev=%x ch=%x%s`	Маршрутизатор получил требования для подготовки вызова. "call" – учетный (порядковый) номер вызова. "dev" – тип устройства (3 – коммутируемый доступ, 6 – PPPoE, 10 – PPTP). "channel" или "ch" – идентификатор канала вызова. Например, запись "board 0 line 0 channel 0, call 3, C01 Outgoing Call dev=6 ch=0" означает, что маршрутизатор три раза вызывал сервер PPPoE.
`board%d line%d channel%d, call%d,%s C02 OutCall Connected%d%s`	Установлено соединение при вызове посредством PPPoE, PPTP или коммутируемого доступа.
`board%d line%d channel%d, call%d,%s C02 Call Terminated`	Вызов PPPoE, PPTP или коммутируемого доступа разъединен.

Таблица 157 Журналы PPP

СООБЩЕНИЕ	ОПИСАНИЕ
`ppp:LCP Starting`	Начат этап PPP-соединения с использованием протокола управления соединением (LCP).
`ppp:LCP Opening`	Открывается этап PPP-соединения с использованием протокола управления соединением (LCP).
`ppp:CHAP Opening`	Открывается этап PPP-соединения с использованием протокола аутентификации с предварительным согласованием вызова (CHAP).
`ppp:IPCP Starting`	Начат этап PPP-соединения с использованием протокола управления протоколом IP (IPCP).
`ppp:IPCP Opening`	Открывается этап PPP-соединения с использованием протокола управления протоколом IP (IPCP).
`ppp:LCP Closing`	Закрывается этап PPP-соединения с использованием протокола управления соединением (LCP).
`ppp:IPCP Closing`	Закрывается этап PPP-соединения с использованием протокола управления протоколом IP (IPCP).

Таблица 158 Журналы UPnP

СООБЩЕНИЕ	ОПИСАНИЕ
UPnP pass through Firewall	Пакетам UPnP разрешено проходить через межсетевой экран.

Таблица 159 Журналы фильтрации содержания

СООБЩЕНИЕ	ОПИСАНИЕ
%s: Keyword blocking	Содержание запрошенной веб-страницы совпало с ключевым словом, заданным пользователем.
%s: Not in trusted web list	Сайт не принадлежит доверенному домену, и маршрутизатор блокирует весь трафик, не относящийся к сайтам в доверенных доменах.
%s: Forbidden Web site	Сайт находится в списке запрещенных.
%s: Contains ActiveX	Сайт содержит элементы ActiveX.
%s: Contains Java applet	Сайт содержит Java-апплет.
%s: Contains cookie	Сайт содержит cookie (сеансовый идентификатор).
%s: Proxy mode detected	Маршрутизатор обнаружил в пакете режим прокси-сервера.
%s	Сервер фильтрации содержания сообщил о принадлежности сайта к одной из блокируемых категорий, но не указал тип категории.
%s:%s	Сервер фильтрации содержания сообщил о принадлежности сайта к блокируемой категории и возвратил тип категории.
%s(cache hit)	Система обнаружила, что сайт принадлежит к списку блокирования в локальном кэше, но тип категории неизвестен.
%s:%s(cache hit)	Система обнаружила, что сайт принадлежит к списку блокирования в локальном кэше, и тип категории известен.
%s: Trusted Web site	Веб-сайт находится в доверенном домене.
%s	Если фильтр содержания в соответствии с расписанием отключен или флажок "Block Matched Web Site" не отмечен, система будет пересылать сайты с любым содержанием.
Waiting content filter server timeout	От внешнего сервера фильтрации содержания не поступило ответа за установленное время ожидания.
DNS resolving failed	Устройству P-793H не удалось получить IP-адрес внешнего сервера фильтрации содержания посредством DNS-запроса.
Creating socket failed	P-793H не может сформировать запрос из-за ошибки создания сокета TCP/IP на указанном порту.
Connecting to content filter server fail	Не удалось соединиться с внешним сервером фильтрации содержания.
License key is invalid	Лицензионный ключ внешней службы фильтрации содержания недействителен.

Таблица 160 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. Расшифровку типов и кодов см. в таб. 167 на стр. 451.
`land [ TCP | UDP | IGMP | ESP | GRE | OSPF ]`	Межсетевой экран обнаружил LAND-атаку по протоколу TCP/UDP/IGMP/ESP/GRE/OSPF.
`land ICMP (type:%d, code:%d)`	Межсетевой экран обнаружил LAND-атаку по протоколу ICMP. Расшифровку типов и кодов см. в таб. 167 на стр. 451.
`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. Расшифровку типов и кодов см. в таб. 167 на стр. 451.
`icmp echo : ICMP (type:%d, code:%d)`	Межсетевой экран обнаружил атаку посредством эхозапроса ICMP. Расшифровку типов и кодов см. в таб. 167 на стр. 451.
`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. Расшифровку типов и кодов см. в таб. 167 на стр. 451.
`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. Расшифровку типов и кодов см. в таб. 167 на стр. 451.
`traceroute ICMP (type:%d, code:%d)`	Межсетевой экран обнаружил атаку с использованием ICMP-запроса для трассировки маршрута. Расшифровку типов и кодов см. в таб. 167 на стр. 451.

Таблица 161 Журналы IPSec

СООБЩЕНИЕ	ОПИСАНИЕ
Discard REPLAY packet	Маршрутизатор удалил полученный пакет с неверным порядковым номером.
Inbound packet authentication failed	Маршрутизатор получил измененный пакет, что может быть признаком его правки или подмены посторонними лицами.
Receive IPSec packet, but no corresponding tunnel exists	Маршрутизатор запретил входящий пакет, для которого не удалось найти соответствующую фазу 2 SA посредством SPI.
Rule <%d> idle time out, disconnect	Маршрутизатор разорвал соединение, по которому в течение установленного периода отсутствовал входящий и исходящий трафик. Для задания этого периода можно воспользоваться командой КС "ipsec timer chk_conn". Значение по умолчанию – 2 минуты.
WAN IP changed to <IP>	Маршрутизатор разорвал все соединения с адресом "MyIP", настроенным как "0.0.0.0", при изменении IP-адреса в сети WAN.

Таблица 162 Журналы IKE

СООБЩЕНИЕ	ОПИСАНИЕ
Active connection allowed exceeded	Процесс IKE для нового соединения не выполнен из-за превышения предельного числа SA для фазы 2.
Start Phase 2: Quick Mode	Начата фаза 2 в быстром режиме.
Verifying Remote ID failed:	Соединение на фазе 2 IKE не установлено, поскольку локальные/удаленные адреса маршрутизатора и противоположной стороны соединения не совпали.
Verifying Local ID failed:	Соединение на фазе 2 IKE не установлено, поскольку локальные/удаленные адреса маршрутизатора и противоположной стороны соединения не совпали.
IKE Packet Retransmit	Маршрутизатор повторно отправил последний отправленный пакет из-за отсутствия отклика удаленной стороны.
Failed to send IKE Packet	Ошибка Ethernet не позволила маршрутизатору отправить пакеты IKE.
Too many errors! Deleting SA	SA удалена из-за недопустимо высокого числа ошибок.
Phase 1 IKE SA process done	Фаза 1 процесса IKE SA завершена.
Duplicate requests with the same cookie	Маршрутизатор получил несколько запросов от одной удаленной стороны, не успев обработать первый полученный от нее пакет IKE.
IKE Negotiation is in process	Маршрутизатор уже начал согласование соединения с удаленной стороной, но процесс IKE пока не завершен.
No proposal chosen	Параметры фазы 1 или фазы 2 не совпадают. Проверьте все протоколы и настройки. В частности, соединение невозможно, если в одном устройстве выбран алгоритм шифрования 3DES, а в другом – DES.
Local / remote IPs of incoming request conflict with rule <%d>	В качестве адреса защищенного шлюза выбран "0.0.0.0". Маршрутизатор, приняв в качестве адреса удаленной стороны локальный адрес противоположной стороны соединения, нарушил статическое правило с номером %d, и соединение было запрещено.

Таблица 162 Журналы IKE (продолжение)

СООБЩЕНИЕ	ОПИСАНИЕ
Cannot resolve Secure Gateway Addr for rule <%d>	Маршрутизатор не смог получить IP-адрес из доменного имени, указанного в качестве адреса защищенного маршрутизатора.
Peer ID: <код удаленной стороны> <наш удаленный тип> - <наш локальный тип>	Указанные коды не совпадают у двух сторон соединения.
vs. My Remote <наш удаленный код> -<наш локальный код>	Указанные коды не совпадают у двух сторон соединения.
vs. My Local <наш локальный код>-<наш локальный код>	Указанные коды не совпадают у двух сторон соединения.
Send <пакет>	Отправлен пакет.
Recv <пакет>	Для передачи данных в IKE используется протокол ISAKMP. Каждый пакет ISAKMP содержит несколько типов полезных нагрузок. Сведения о всех них отражаются в журнале. Полный список типов полезных нагрузок ISAKMP см. в документе RFC2408.
Recv <режим: Main или Aggressive> Mode request from <IP>	С указанного адреса удаленной стороны маршрутизатор получил запрос согласования IKE.
Send <режим: Main или Aggressive> Mode request to <IP>	Маршрутизатор начал согласование с удаленной стороной.
Invalid IP <локальный адрес удаленной стороны> / <локальный адрес удаленной стороны>	Локальный IP-адрес удаленной стороны настроен неверно.
Remote IP <IP-адрес удаленной стороны> / <IP-адрес удаленной стороны> conflicts	В качестве адреса защищенного шлюза выбран "0.0.0.0". Маршрутизатор, приняв в качестве адреса удаленной стороны локальный адрес противоположной стороны соединения, нарушил статическое правило с номером %d, и соединение было запрещено.
Phase 1 ID type mismatch	Тип удаленного идентификатора на этом маршрутизаторе отличается от типа локального идентификатора на удаленном маршрутизаторе IPSec.
Phase 1 ID content mismatch	Содержание удаленного идентификатора на этом маршрутизаторе отличается от содержания локального идентификатора на удаленном маршрутизаторе IPSec.
No known phase 1 ID type found	Маршрутизатор не смог найти известный идентификатор фазы 1 при попытке соединения.
ID type mismatch. Local / Peer: <тип локального идентификатора/тип удаленного идентификатора>	Типы идентификаторов для фазы 1 не совпали.
ID content mismatch	Содержание идентификаторов для фазы 1 не совпало.
Configured Peer ID Content: <содержание настроенного идентификатора удаленной стороны>	Содержание идентификаторов для фазы 1 не совпало. Приведено настроенное содержание идентификатора удаленной стороны.
Incoming ID Content: <содержание входящего идентификатора удаленной стороны>	Содержание идентификаторов для фазы 1 не совпало. Приведено содержание идентификатора из входящего пакета.

Таблица 162 Журналы IKE (продолжение)

СООБЩЕНИЕ	ОПИСАНИЕ
Unsupported local ID Type: <%d>	Типы идентификатора для фазы 1 не поддерживается данным маршрутизатором.
Build Phase 1 ID	Маршрутизатор начал формировать идентификатор для фазы 1.
Adjust TCP MSS to%d	Маршрутизатор автоматически изменил максимальный размер сегмента TCP после установления туннеля.
Rule <%d> input idle time out, disconnect	Туннель для указанного правила удален, поскольку в течение заданного интервала отсутствовал входящий трафик.
XAUTH succeed! Username : <пользователь>	Маршрутизатор разрешил указанное имя пользователя с помощью расширенной аутентификации.
XAUTH fail! Username : <пользователь>	Маршрутизатор не смог разрешить указанное имя пользователя с помощью расширенной аутентификации.
Rule[%d] Phase 1 negotiation mode mismatch	В указанном правиле режим согласования для фазы 1 IKE не совпадает у маршрутизатора и удаленной стороны.
Rule [%d] Phase 1 encryption algorithm mismatch	В указанном правиле алгоритм шифрования для фазы 1 IKE не совпадает у маршрутизатора и удаленной стороны.
Rule [%d] Phase 1 authentication algorithm mismatch	В указанном правиле алгоритм аутентификации для фазы 1 IKE не совпадает у маршрутизатора и удаленной стороны.
Rule [%d] Phase 1 authentication method mismatch	В указанном правиле метод аутентификации для фазы 1 IKE не совпадает у маршрутизатора и удаленной стороны.
Rule [%d] Phase 1 key group mismatch	В указанном правиле группа ключей для фазы 1 IKE не совпадает у маршрутизатора и удаленной стороны.
Rule [%d] Phase 2 protocol mismatch	В указанном правиле протокол аутентификации для фазы 2 IKE не совпадает у маршрутизатора и удаленной стороны.
Rule [%d] Phase 2 encryption algorithm mismatch	В указанном правиле алгоритм шифрования для фазы 2 IKE не совпадает у маршрутизатора и удаленной стороны.
Rule [%d] Phase 2 authentication algorithm mismatch	В указанном правиле алгоритм аутентификации для фазы 2 IKE не совпадает у маршрутизатора и удаленной стороны.
Rule [%d] Phase 2 encapsulation mismatch	В указанном правиле тип инкапсуляции для фазы 2 IKE не совпадает у маршрутизатора и удаленной стороны.
Rule [%d]> Phase 2 pfs mismatch	В указанном правиле параметр защиты от разглашения использованных ключей (pfs) для фазы 2 не совпадает у маршрутизатора и удаленной стороны.
Rule [%d] Phase 1 ID mismatch	В указанном правиле идентификатор для фазы 1 IKE не совпадает у маршрутизатора и удаленной стороны.
Rule [%d] Phase 1 hash mismatch	В указанном правиле хэш для фазы 1 IKE не совпадает у маршрутизатора и удаленной стороны.
Rule [%d] Phase 1 preshared key mismatch	В указанном правиле предварительно согласованный ключ для фазы 1 IKE не совпадает у маршрутизатора и удаленной стороны.
Rule [%d] Tunnel built successfully	Туннель IPSec для указанного правила успешно создан.
Rule [%d] Peer's public key not found	Открытый ключ удаленной стороны для фазы 1 IKE не найден для указанного правила.
Rule [%d] Verify peer's signature failed	Не удалось проверить подпись удаленной стороны на фазе 1 IKE для указанного правила.
Rule [%d] Sending IKE request	IKE направляет запрос для указанного правила.

Таблица 162 Журналы IKE (продолжение)

СООБЩЕНИЕ	ОПИСАНИЕ
`Rule [%d] Receiving IKE request`	IKE принимает запрос для указанного правила.
`Swap rule to rule [%d]`	Маршрутизатор переключился на указанное правило.
`Rule [%d] Phase 1 key length mismatch`	В указанном правиле длина ключа (для алгоритма шифрования AES) для фазы 1 IKE не совпадает у маршрутизатора и удаленной стороны.
`Rule [%d] phase 1 mismatch`	В указанном правиле параметры фазы 1 IKE не совпадают у маршрутизатора и удаленной стороны.
`Rule [%d] phase 2 mismatch`	В указанном правиле параметры фазы 2 IKE не совпадают у маршрутизатора и удаленной стороны.
`Rule [%d] Phase 2 key length mismatch`	В указанном правиле длина ключа (для алгоритма шифрования AES) для фазы 2 IKE не совпадает у маршрутизатора и удаленной стороны.

Таблица 163 Журналы PKI

СООБЩЕНИЕ	ОПИСАНИЕ
`Enrollment successful`	Онлайновая регистрация сертификата по протоколу SCEP выполнена успешно. В поле получателя указывается IP-адрес и номер порта на сервере центра сертификации.
`Enrollment failed`	Не удалось выполнить онлайновую регистрацию сертификата по протоколу SCEP. В поле получателя указывается IP-адрес и номер порта на сервере центра сертификации.
`Failed to resolve <URL сервера SCEP CA>`	Онлайновая регистрация сертификата на сервере SCEP не выполнена, поскольку не удалось разрешить адрес сервера центра сертификации.
`Enrollment successful`	Онлайновая регистрация сертификата по протоколу CMP выполнена успешно. В поле получателя указывается IP-адрес и номер порта на сервере центра сертификации.
`Enrollment failed`	Не удалось выполнить онлайновую регистрацию сертификата по протоколу CMP. В поле получателя указывается IP-адрес и номер порта на сервере центра сертификации.
`Failed to resolve <URL сервера CMP CA>`	Онлайновая регистрация сертификата на сервере CMP не выполнена, поскольку не удалось разрешить адрес сервера центра сертификации.
`Rcvd ca cert: <заголовок>`	Маршрутизатор получил сертификат центра сертификации с указанным заголовком с сервера LDAP, IP-адрес и номер порта которого указаны в поле источника.
`Rcvd user cert: <заголовок>`	Маршрутизатор получил сертификат пользователя с указанным заголовком с сервера LDAP, IP-адрес и номер порта которого указаны в поле источника.
`Rcvd CRL <размер>: <выпускающий>`	Маршрутизатор получил с сервера LDAP, IP-адрес и номер порта которого указаны в поле источника, список CRL (отзываемых сертификатов) с указанным размером и именем выпускающего.
`Rcvd ARL <размер>: <выпускающий>`	Маршрутизатор получил с сервера LDAP, IP-адрес и номер порта которого указаны в поле источника, список ARL (отзываемых центров сертификации) с указанным размером и именем выпускающего.
`Failed to decode the received ca cert`	Маршрутизатор получил поврежденный сертификат центра сертификации с сервера LDAP, адрес и номер порта которого указаны в поле источника.
`Failed to decode the received user cert`	Маршрутизатор получил поврежденный сертификат пользователя с сервера LDAP, адрес и номер порта которого указаны в поле источника.

Таблица 163 Журналы PKI (продолжение)

СООБЩЕНИЕ	ОПИСАНИЕ
`Failed to decode the received CRL`	Маршрутизатор получил поврежденный CRL (список отзываемых сертификатов) с сервера LDAP, адрес и номер порта которого указаны в поле источника.
`Failed to decode the received ARL`	Маршрутизатор получил поврежденный ARL (список отзываемых центров сертификации) с сервера LDAP, адрес и номер порта которого указаны в поле источника.
`Rcvd data <размер> too large! Max size allowed: <макс. размер>`	Маршрутизатор получил каталог недопустимо большого размера (размер указан) с сервера LDAP, адрес и номер порта которого указаны в поле источника. Также приводится максимальный размер сведений из каталога, разрешенный маршрутизатором.
`Cert trusted: <заголовок>`	Маршрутизатор проверил путь сертификата с указанным заголовком.
`Due to <коды причин>, cert not trusted: <заголовок>`	По перечисленным причинам сертификат с указанным заголовком не прошел проверку пути. Эти коды причин носят ориентировочный характер, отмечая подозрительные свойства сертификата. Расшифровку кодов см. в таб. 164 на стр. 449.

Таблица 164 Коды причин непрохождения проверки сертификата

КОД	ОПИСАНИЕ
1	Несовпадение алгоритма сертификата с условиями поиска.
2	Несовпадение используемых ключей сертификата с условиями поиска.
3	Сертификат недействителен на соответствующем отрезке времени.
4	(Не используется).
5	Сертификат недействителен.
6	Сертификат не прошел проверку подписи.
7	Сертификат отозван списком CRL.
8	Сертификат не был добавлен в кэш.
9	Сертификат не удалось декодировать.
10	Сертификат не найден (где-либо).
11	Кольцевая цепь сертификатов (невозможно найти доверенный корневой элемент)
12	Сертификат содержит важное расширение, которое не удалось обработать.
13	Выпускающий сертификата недействителен (отсутствуют характеристики CA).
14	(Не используется).
15	Список CRL устарел.
16	Список CRL недействителен.
17	Список CRL не прошел проверку подписи.
18	Список CRL не найден (где-либо).
19	Список CRL не был добавлен в кэш.
20	Список CRL не удалось декодировать.
21	Список CRL недействителен в данный момент (но вступит в силу позднее).
22	Список CRL содержит повторяющиеся серийные номера.
23	Интервал времени не непрерывен.
24	Отсутствуют сведения о времени.
25	Истекло время выполнения метода базы данных.

Таблица 164 Коды причин непрохождения проверки сертификата (продолжение)

КОД	ОПИСАНИЕ
26	Не удалось выполнить метод базы данных.
27	Не удалось проверить путь.
28	Достигнута максимальная длина пути.

Таблица 165 802.1X Logs

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.
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.
Локальная база данных пользователей не поддерживает метод аутентификации.	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.

Таблица 165 802.1X Logs (продолжение)

СООБЩЕНИЕ	ОПИСАНИЕ
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.

Таблица 166 Замечания по заданию ACL

НАПРАВЛЕНИЕ ДВИЖЕНИЯ ПАКЕТОВ	НАПРАВЛЕНИЕ	ОПИСАНИЕ
(L to W)	Для трафика из LAN в WAN	ACL задается для пакетов, пересылаемых из LAN в WAN.
(W to L)	Из WAN в LAN (WAN to LAN)	ACL задается для пакетов, пересылаемых из WAN в LAN.
(L to L)	Из LAN в LAN/P-793H	ACL задается для пакетов, пересылаемых из LAN в LAN или на P-793H.
(W to W)	Из WAN в WAN/ P-793H	ACL задается для пакетов, пересылаемых из WAN в WAN или на P-793H.

Таблица 167 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		Переадресация
	0	Переадресация датаграмм для сети
	1	Переадресация датаграмм для хоста
	2	Переадресация датаграмм для типа службы и сети
	3	Переадресация датаграмм для типа службы и хоста
8		Эхозапрос
	0	Сообщение эхозапроса

Таблица 167 Пояснения к кодам ICMP (продолжение)

ТИП	КОД	ОПИСАНИЕ
11		Превышено допустимое время
	0	На маршруте превышено время жизни пакета (TTL)
	1	Превышено время сборки фрагментов
12		Ошибка в параметре
	0	Ошибка отмечена указателем
13		Метка времени
	0	Сообщение запроса метки времени
14		Отклик метки времени
	0	Сообщение с откликом метки времени
15		Информационный запрос
	0	Сообщение с информационным запросом
16		Информационный отклик
	0	Сообщение с информационным откликом

Таблица 168 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.

В следующей таблице приведены типы полезной нагрузки ISAKMP по стандарту RFC 2408 , отображаемые в журнале. Подробное описание каждого типа см. в соответствующем документе RFC.

Таблица 169 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

Таблица 169 Типы полезной нагрузки ISAKMP по стандарту RFC-2408 (продолжение)

СОДЕРЖАНИЕ ЖУРНАЛА	ТИП ПОЛЕЗНОЙ НАГРУЗКИ
SIG	Подпись
NONCE	Псевдослучайное число
NOTFY	Уведомление
DEL	Удаление
VID	Код поставщика оборудования

Команды для управления журналом

В этом разделе приведены общие примеры использования команд для работы с журналами. Вывод на экран для вашего устройства может отличаться, но общий принцип работы аналогичен.

В описании интерфейса командной строки (Приложение H на стр. 433) поясняется вызов и использование команд.

Настройка содержания журнала P-793H

1. Для загрузки буфера настроек журналов, позволяющего задать состав журналов, формируемых P-793H, используется команда sys logs load.
2. Для просмотра категорий журналов служит команда sys logs category.

Рис. 290 Пример просмотра списка категорий журналов

```
ras>?
Действительными командами являются следующие:
sys             exit            ether           aux
ip              ipsec           bridge          bm
certificates    cnm             8021x           radius
ras>
```

3. Чтобы просмотреть список параметров, доступных для конкретной категории, наберите команду sys logs category, следом указав тип категории.

Рис. 291 Пример просмотра параметров ведения журнала

```
ras> sys logs category access
Использование: [0:none/1:log/2:alert/3:both]
```

4. Чтобы задать типы журнальных сообщений, наберите команду sys logs category, следом указав тип категории и параметр.

0 отключает ведение журналов для данной категории, 1 указывает регистрировать только журнальные сообщения для данной категории, 2 – регистрировать только предупреждения для данной категории, 3 – регистрировать для данной категории и журнальные сообщения, и предупреждения. Для некоторых категорий определенные параметры могут быть недоступны.

5. Шаг 5. Запишите настройки в P-793H командой sys logs save (эту операцию необходимо выполнить, чтобы включить ведение журналов).

Просмотр журналов

- Команда sys logs display служит для просмотра всех сообщений в журнале P-793H.
- 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-793H.
- Команда sys logs clear служит для удаления всех журналов из P-793H.

Пример команд для работы с журналами

В этом примере выполняется настройка P-793H для ведения журналов доступа и предупреждений, после чего вызывается просмотр результатов.

```
ras> sys logs load
ras> sys logs category access 3
ras> sys logs save
ras> sys logs display access

#  .time                source                destination           notes

    message
 0|06/08/2004 05:58:21 |172.21.4.154         |224.0.1.24           |ACCESS
BLOCK
    Firewall default policy: IGMP (W to W/ZW)
 1|06/08/2004 05:58:20 |172.21.3.56          |239.255.255.250      |ACCESS
BLOCK
    Firewall default policy: IGMP (W to W/ZW)
 2|06/08/2004 05:58:20 |172.21.0.2           |239.255.255.254      |ACCESS
BLOCK
    Firewall default policy: IGMP (W to W/ZW)
 3|06/08/2004 05:58:20 |172.21.3.191         |224.0.1.22           |ACCESS
BLOCK
    Firewall default policy: IGMP (W to W/ZW)
 4|06/08/2004 05:58:20 |172.21.0.254         |224.0.0.1            |ACCESS
BLOCK
    Firewall default policy: IGMP (W to W/ZW)
 5|06/08/2004 05:58:20 |172.21.4.187:137     |172.21.255.255:137   |ACCESS
BLOCK
    Firewall default policy: UDP (W to W/ZW)
```

J

Команды фильтрации NetBIOS

Ниже описаны команды для фильтрации пакетов NetBIOS. Подробнее о структуре команд см. Приложение H на стр. 433.

Введение

NetBIOS (базовая сетевая система ввода-вывода) представляет собой широковещательные пакеты TCP или UDP, позволяющие компьютеру подключаться и взаимодействовать с локальной сетью.

Пакеты NetBIOS могут приводить к вызову служб коммутируемого доступа посредством PPPoE или PPTP, даже если эти службы не были запрошены пользователем.

Для загрузки фильтров NetBIOS выполните следующие действия:

- Разрешать или запрещать пересылку пакетов NetBIOS из LAN в WAN и из WAN в LAN.
- Разрешать или запрещать пересылку пакетов NetBIOS по VPN-соединениям.
- Разрешать или запрещать осуществление вызовов с помощью пакетов NetBIOS.

Просматривать настройки фильтра NetBIOS.

Синтаксис: `sys filter netbios disp`

Эта команда выводит (неизменяемый) список текущих режимов фильтрования в P-793H.

Пример вызова команды для просмотра настроек фильтра NetBIOS

```
=========== NetBIOS Filter Status ===========
        Between LAN and WAN: Block
              IPSec Packets: Forward
        Trigger Dial: Disabled
```

Типы имеющихся фильтров и настройки по умолчанию для них приведены ниже.

Таблица 170 Настройки фильтра NetBIOS по умолчанию

НАИМЕНОВАНИЕ	ОПИСАНИЕ	ПРИМЕР
Between LAN and WAN	В этом поле отображается действие, выполняемое над пакетами NetBIOS при перемещении между сетями LAN и WAN: блокирование или пересылка.	Block
IPSec Packets	В этом поле отображается действие (block - блокирование, forward - пересылка), выполняемое над пакетами NetBIOS при перемещении по VPN-соединению.	Forward
Trigger dial	В этом поле указывается. разрешено ли осуществлять вызовы с помощью пакетов NetBIOS. Если этот режим отключен (disabled), пакеты NetBIOS не могут использоваться для осуществления вызовов.	Disabled

Настройка фильтра NetBIOS

```
Синтаксис: sys filter netbios config <тип> <on|off>
```

где

`<тип>` = номер настраиваемого фильтра (0-3).

0 = переход между сетями LAN и WAN

3 = пересылка пакетов по IPSec

4 = разрешение вызова

`<on|off>` = Для типов 0 и 1 значение "on" активирует фильтр, блокируя пересылку пакетов NetBIOS. Значение "off" отключает фильтр, разрешая пересылку пакетов NetBIOS.

Для типа 3 значение "on" указывает блокировать пересылку пакетов NetBIOS по VPN-соединению. Значение "off" разрешает пересылку пакетов NetBIOS по VPN-соединению.

Для типа 4 значение "on" разрешает пакетам NetBIOS инициировать вызов по коммутируемому резервному каналу. Значение "off" запрещает пакетам NetBIOS инициировать вызов по коммутируемому резервному каналу.

Примеры команд

`sys filter netbios config 0 on`	Эта команда блокирует переход пакетов NetBIOS из сети LAN в сеть WAN и в обратном направлении.
`sys filter netbios config 3 on`	Эта команда блокирует пересылку пакетов NetBIOS по IPSec.
`sys filter netbios config 4 off`	Эта команда запрещает инициировать вызов по коммутируемому резервному каналу в ответ на пакеты NetBIOS.

K

Важная информация

Регистрация покупки

По завершении установки мы рекомендуем зарегистрировать ваше изделие ZyXEL через Интернет. Регистрация дает дополнительный год бесплатной гарантии, персональную техническую поддержку, уведомление по электронной почте об обновлениях, ряд других преимуществ. Адрес сайта для регистрации в вашей стране указан в главе "Гарантийное обслуживание ZyXEL".

Информация о сертификации

Интернет-центр P-793H одобрен для применения государственными органами по сертификации. Копии действующих в вашей стране сертификатов можно получить через Интернет на домашней странице изделия в каталоге продукции.

Система сертификации ГОСТ Р, Госстандарт России

Сертификат соответствия № РОСС TW.АЯ46.В08942.
Срок действия с 13.09.2006 по 13.09.2008.
Соответствует требованиям: ГОСТ Р МЭК 60950-2002, ГОСТ Р 51318.22-99, ГОСТ Р 51318.24-99, ГОСТ Р 51317.3.2-99, ГОСТ Р 51318.3.3-99.

Государственная санитарно-эпидемиологическая служба РФ

Санитарно-эпидемиологическое заключение № 77.01.09.401.П.087979.12.06.
Срок действия с 26.12.2006 по 18.12.2011.
Соответствует требованиям: СанПиН 2.2.2./2.4.1340-03, СанПиН 2.1.8./2.2.4.1190-03.

Юридический адрес изготовителя

Зайксел Коммуникэйшнз Корп., Инновэйшн Роад II, 6,
Сайнс-бейсд Индастриал Парк, Син-Чу, Тайвань
ZyXEL Communications Corporation, 6, Innovation Road II,
Science-Based Industrial Park, Hsin-Chu, Taiwan, R.O.C.

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

© ZyXEL Communications Corp., 2007. Все права защищены

Гарантийное обслуживание ZyXEL

Мы гордимся надежностью и качеством нашей продукции и верим, что она прослужит вам безотказно долгие годы. Тем не менее, если у вас возникнут вопросы при использовании этого изделия, пожалуйста, обратитесь за помощью в региональное представительство ZyXEL.

Гарантийные обязательства

1. Настоящая гарантия действует в течение трех лет с даты приобретения изделия ZyXEL и подразумевает гарантийное обслуживание при обнаружении дефектов, связанных с материалами и сборкой. В этом случае потребитель имеет право на бесплатный ремонт изделия.
2. При регистрации приобретенного изделия через Интернет на сайте, указанном далее в таблице "Контактная информация", потребитель получает дополнительный год гарантийного обслуживания.
3. Максимальный срок гарантии, предоставляемой компанией ZyXEL, исчисляется с даты производства изделия и составляет четыре с половиной года. Дата производства определяется по серийному номеру на корпусе изделия: 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, если:

- серийный номер на изделии изменен, стерт, удален или неразборчив;
- изделие переделывалось без предварительного письменного согласия ZyXEL;
- изделие неправильно эксплуатировалось, в том числе:
  a)использовалось не по назначению или не в соответствии с руководством пользователя,
  b)устанавливалось или эксплуатировалось в условиях, не соответствующих стандартам и нормам безопасности, действующим в стране использования;
- изделие ремонтировалось не уполномоченными на то сервисными центрами или дилерами;
- изделие вышло из строя по причине несчастного случая, удара молнии, затопления, пожара, неправильной вентиляции и иных причин, находящихся вне контроля ZyXEL;
- изделие пострадало при транспортировке, за исключением случаев, когда она производится авторизованным сервисным центром;
- изделие использовалось в дефектной системе.

Контактная информация

	Россия	Украина	Казахстан
Веб-сайт	zyxel.ru	ua.zyxel.com	zyxel.kz
Поддержка в Интернете	zyxel.ru/help	ua.zyxel.com/help	zyxel.kz/help
Поддержка по телефону			
Бесплатный номер	(800) 200-8929	(800) 504-0040	(800) 080-0055
Дополнительный номер	(495) 542-8929	(044) 247-6978	(3272) 590-689
Представительство ZyXEL	ZyXEL Россия 117279, Москва, ул. Островитянова, дом 37а (495) 542-8920	ZyXEL Украина 04050, Киев, ул. Пимоненко, дом 13 (044) 494-4931	ZyXEL Казахстан 050010, Алматы, пр. Достык, 43, офис 414 (3272) 590-699

О компании ZyXEL

С момента основания в 1989 году компания ZyXEL Communications самостоятельно разрабатывает и создает решения, обеспечивающие надежный и удобный доступ в Интернет. Находясь на переднем крае технологий связи, в каждом поколении своей продукции ZyXEL неизменно предлагает оптимальную реализацию промышленных стандартов. Добившись мирового признания в области модемов для коммутируемого доступа, компания предложила линейку революционных устройств широкополосного доступа и первой раскрыла тему аппаратных средств интернет-безопасности для массового пользователя. Последовательно развивая скорость связи и удобство абонентской интернет-техники, сейчас компания лидирует на рынке DSL и кропотливо работает в перспективных технологических направлениях, таких как ETTH и WiMAX. Наряду с этим ZyXEL поставляет передовые инфраструктурные решения интернет-провайдерам и корпоративным заказчикам, в том числе для проектов национального масштаба. В создании новой продукции, которая сегодня поставляется в семьдесят стран мира, участвуют три научно-исследовательских центра.

На территории СНГ компания ZyXEL работает с 1992 года, взяв курс на полную адаптацию продукции к местным условиям. Подготовка сертифицированных инженеров ведется в трех авторизованных учебных центрах, услуги по обслуживанию оборудования ZyXEL осуществляет сеть авторизованных сервисных центров во всех крупных городах стран СНГ. На региональных веб-сайтах ZyXEL действует уникальная интерактивная система консультаций, а прямая бесплатная связь с Центром информации и поддержки доступна в любом населенном пункте, где есть телефон. Интернет-техникой ZyXEL пользуются миллионы домашних пользователей, и имя компании для них стало синонимом надежной связи и выхода в Интернет с первой попытки.

L

Поддержка покупателей

Обращаясь за поддержкой, предоставьте следующую информацию.

Необходимые сведения

- Модель и серийный номер изделия.
- Информация о гарантии.
- Дата получения устройства.
- Краткое описание проблемы и мер, которые предпринимались для ее разрешения.

Центральный офис корпорации (для всех стран)

- Служба поддержки: support@zyxel.com.tw
- Отдел продаж: sales@zyxel.com.tw
- Телефон: +886-3-578-3942
- Факс: +886-3-578-2439
- Веб-сайт: www.zyxel.com, www.europe.zyxel.com
- FTP-сервер: ftp.zyxel.com, ftp.europe.zyxel.com
- Обычная почта: ZyXEL Communications Corp., 6 Innovation Road II, Science Park, Hsinchu 300, Taiwan

Коста-Рика

- Служба поддержки: soporte@zyxel.co.cr
- Отдел продаж: sales@zyxel.co.cr
- Телефон: +506-2017878
- Факс: +506-2015098
- Веб-сайт: www.zyxel.co.cr
- FTP-сервер: ftp.zyxel.co.cr
- Обычная почта: ZyXEL Costa Rica, Plaza Roble Escazu, Etapa El Patio, Tercer Piso, San Jose, Costa Rica

Чехия

- E-mail: info@cz.zyxel.com
- Телефон: +420-241-091-350
- Факс: +420-241-091-359
- Веб-сайт: www.zyxel.cz
- Обычная почта: ZyXEL Communications, Czech s.r.o., Modranska 621, 143 01 Praha 4 - Modrany, Ceska Republika

Дания

- Служба поддержки: support@zyxel.dk
- Отдел продаж: sales@zyxel.dk
- Телефон: +45-39-55-07-00
- Факс: +45-39-55-07-07
- Веб-сайт: www.zyxel.dk
- Обычная почта: ZyXEL Communications A/S, Columbusvej, 2860 Soeborg, Denmark

Финляндия

- Служба поддержки: support@zyxel.fi
- Отдел продаж: sales@zyxel.fi
- Телефон: +358-9-4780-8411
- Факс: +358-9-4780 8448
- Веб-сайт: www.zyxel.fi
- Обычная почта: ZyXEL Communications Oy, Malminkaari 10, 00700 Helsinki, Finland

Франция

- E-mail: info@zyxel.fr
- Телефон: +33-4-72-52-97-97
- Факс: +33-4-72-52-19-20
- Веб-сайт: www.zyxel.fr
- Обычная почта: ZyXEL France, 1 rue des Vergers, Bat. 1 / C, 69760 Limonest, France

Германия

- Служба поддержки: support@zyxel.de
- Отдел продаж: sales@zyxel.de
- Телефон: +49-2405-6909-0
- Факс: +49-2405-6909-99
- Веб-сайт: www.zyxel.de
- Обычная почта: ZyXEL Deutschland GmbH., Adenauerstr. 20/A2 D-52146, Wuerselen, Germany

Венгрия

- Служба поддержки: support@zyxel.hu
- Отдел продаж: info@zyxel.hu
- Телефон: +36-1-3361649
- Факс: +36-1-3259100
- Веб-сайт: www.zyxel.hu
- Обычная почта: ZyXEL Hungary, 48, Zoldlomb Str., H-1025, Budapest, Hungary

Казахстан

- Служба поддержки: http://zyxel.kz/support
- Отдел продаж: sales@zyxel.kz
- Телефон: +7-3272-590-698
- Факс: +7-3272-590-689
- Веб-сайт: www.zyxel.kz
- Обычная почта: ZyXEL Kazakhstan, 43, Dostyk ave.,Office 414, Dostyk Business Centre, 050010, Almaty, Republic of Kazakhstan

Северная Америка

- Служба поддержки: support@zyxel.com
- Отдел продаж: sales@zyxel.com
- Телефон: +1-800-255-4101, +1-714-632-0882
- Факс: +1-714-632-0858
- Веб-сайт: www.us.zyxel.com
- FTP-сервер: ftp.us.zyxel.com
- Обычная почта: ZyXEL Communications Inc., 1130 N. Miller St., Anaheim, CA 92806-2001, U.S.A.

Норвегия

- Служба поддержки: support@zyxel.no
- Отдел продаж: sales@zyxel.no
- Телефон: +47-22-80-61-80
- Факс: +47-22-80-61-81
- Веб-сайт: www.zyxel.no
- Обычная почта: ZyXEL Communications A/S, Nils Hansens vei 13, 0667 Oslo, Norway

Польша

- E-mail: info@pl.zyxel.com
- Телефон: +48 (22) 333 8250
- Факс: +48 (22) 333 8251
- Веб-сайт: www.pl.zyxel.com
- Обычная почта: ZyXEL Communications, ul. Okrzei 1A, 03-715 Warszawa, Poland

Россия

- Служба поддержки: http://zyxel.ru/support
- Отдел продаж: sales@zyxel.ru
- Телефон: +7-095-542-89-29
- Факс: +7-095-542-89-25
- Веб-сайт: www.zyxel.ru
- Обычная почта: ZyXEL Россия, 117279, Москва, ул. Островитянова, д. 37а

Испания

- Служба поддержки: support@zyxel.es
- Отдел продаж: sales@zyxel.es
- Телефон: +34-902-195-420
- Факс: +34-913-005-345
- Веб-сайт: www.zyxel.es
- Обычная почта: ZyXEL Communications, Arte, 21 5Є planta, 28033 Madrid, Spain

Швеция

- Служба поддержки: support@zyxel.se
- Отдел продаж: sales@zyxel.se
- Телефон: +46-31-744-7700
- Факс: +46-31-744-7701
- Веб-сайт: www.zyxel.se
- Обычная почта: ZyXEL Communications A/S, Sjoporten 4, 41764 Goteborg, Sweden

Украина

- Служба поддержки: support@ua.zyxel.com
- Отдел продаж: sales@ua.zyxel.com
- Телефон: +380-44-247-69-78
- Факс: +380-44-494-49-32
- Веб-сайт: www.ua.zyxel.com
- Обычная почта: ZyXEL Украина, 04050, Киев, ул. Пимоненко, д. 13

Великобритания

- Служба поддержки: support@zyxel.co.uk
- Отдел продаж: sales@zyxel.co.uk
- Телефон: +44-1344 303044, 08707 555779 (только для звонков из Великобритании)
- Факс: +44-1344 303034
- Веб-сайт: www.zyxel.co.uk
- FTP-сервер: ftp.zyxel.co.uk
- Обычная почта: ZyXEL Communications UK, Ltd.,11 The Courtyard, Eastern Road, Bracknell, Berkshire, RG12 2XB, United Kingdom (UK)

Знак "+" указывается перед кодом страны, который нужно набрать, чтобы позвонить из другой страны.

Указатель

Л

М

Н

О

П

С

Т

У

Ф

X

Э

A

D

E

F

I

L

M

N

P

R

S

T

U

V

W

Z