P660HWP

Интернет-центр для подключения по ADSL2+ с точкой доступа Wi-Fi 802.11g, 4-портовым коммутатором и адаптером HomePlug AV

Руководство пользователя

Версия 3.40
7/2007
Редакция 1

ZyXEL

www.zyxel.com

О данном Руководстве пользователя

Для кого предназначено данное Руководство

Данное руководство предназначено для тех, кто планирует производить настройку P660HWP с помощью Web-конфигуратора. Для работы с Руководством необходимо обладать основными знаниями о топологии и принципах организации сетей TCP/IP.

Зарегистрируйте ваше изделие ZyXEL через Интернет по адресу *zyxel.ru* для России, *ua.zyxel.com* – для Украины и *zyxel.kz* – для Казахстана. Регистрация изделия дает дополнительный год бесплатной гарантии, персональную техническую поддержку, уведомление по электронной почте об обновлениях, ряд других преимуществ и льгот.**Сопроводительная документация**

- Краткое руководство

  Краткое руководство разработано с целью помочь Вам изучить устройство и начать работать с ним. В нем содержится информация о настройке сети и организации доступа в Интернет.
- Встроенная справка Web-конфигуратора

  Встроенная интерактивная справочная система содержит описания отдельных окон и другую дополнительную информацию.

Рекомендуется выполнять настройку P660HWP с помощью содержащейся на прилагаемом диске программы ZyXEL NetFriend.

- Справочный компакт-диск

  Входящий в комплект компакт диск содержит техническую документацию.
- Web-сайт корпорации ZyXEL
- Сертификаты на изделие, а также дополнительную документацию см. на сайте www.zyxel.ru.

Обратная связь с пользователем

Помогите нам помочь вам. Все комментарии, относящиеся к Руководству пользователя, вопросы и предложения по улучшению направляйте нам через Интерактивную систему консультаций в разделе «Поддержка» на сайте www.zyxel.ru. Спасибо

Обозначения, принятые в документе

Предупреждения и примечания

Предупреждения и примечания в данном руководстве пользователя представлены следующем образом:

Значком "предупреждение" отмечены пункты, содержание которых предупреждает о возможном нанесении вреда пользователю или устройству.

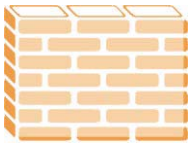
Значком "примечание" помечается важная информация (например, необходимость настройки других параметров или полезные подсказки), рекомендации, относящиеся к теме.

Условные обозначения

- Далее в данном руководстве модель P660HWP может именоваться, как устройство или система P660HWP.
- Надписи на изделии, имена окон, имена полей и пункты меню обозначаются **жирным** шрифтом.
- Название клавиш указаны прописными буквами в квадратных скобках, например, [ENTER] означает клавишу «ввод» или «возврат каретки» на клавиатуре.
- Указание «Введите...» означает, что следует набрать один или несколько символов и затем нажать клавишу [ENTER]. «Выберите» означает, что следует использовать один из предложенных вариантов.
- Правая угловая скобка (>) между названиями окон означает нажатие кнопки мыши. Например, **Maintenance (Сопровождение) > Log (Регистрационный журнал) > Log Setting (Настройки регистрационного журнала)** означает, что сначала необходимо выбрать **Maintenance (Сопровождение)** в панели навигации, затем подменю **Log (Регистрационный журнал)**, а затем закладку **Log Setting**.
- Единицы измерения могут указывать как на «метрические», так и на «научные» величины. Например, приставка «к» (кило) может означать как 1000, так и 1024, приставка «М» – 1000000 или 1048576 и т. д.
- «напр.» – это сокращение для «например», а «т.е.» – для «то есть».

Используемые пиктограммы

В схемах данного руководства используются следующие значки: значок P660HWP является схематичным изображением устройства.

P660HWP 	Компьютер 	Ноутбук 
Сервер 	DSL-коммутатор (DSLAM) 	Межсетевой экран 
Телефон 	Коммутатор 	Маршрутизатор 

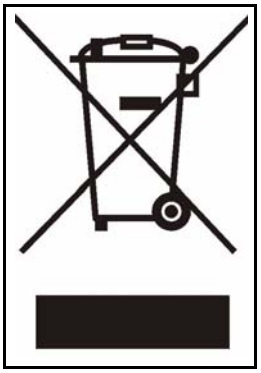
Техника безопасности

Для обеспечения безопасности необходимо ознакомиться и следовать следующим правилам.

- НЕ используйте изделие в непосредственной близости от воды, например, во влажных подвалах или рядом с бассейном.
- НЕ подвергайте устройство воздействию влаги, пыли или агрессивных жидкостей.
- НЕ ставьте на устройство никакие предметы.
- ЗАПРЕЩАЕТСЯ устанавливать, использовать и ремонтировать устройство во время грозы. Существует определенный риск получения удара электрическим током при разряде молнии.
- Подключайте к устройству ТОЛЬКО соответствующие комплектующие.
- НЕ вскрывайте устройство. Не следует открывать или снимать крышку во избежание поражения электрическим током высокого напряжения и других повреждений. Техническое обслуживание и разборка данного устройства должны выполняться только квалифицированным техническим персоналом. Пожалуйста, свяжитесь с местным поставщиком для получения информации о техническом обслуживании.
- Убедитесь, что все кабели подключены к соответствующим портам.
- Прокладывайте соединительные кабели в местах, где никто не будет наступать на них или спотыкаться.
- Всегда отсоединяйте от устройства все кабели перед обслуживанием или разборкой.
- Используйте для устройства ТОЛЬКО соответствующий адаптер или шнур питания.
- Подключите кабель или адаптер питания к сети электропитания с соответствующим напряжением (110 В переменного тока в Северной Америке или 230 В переменного тока в Европе).
- НЕ кладите на кабель или адаптер питания какие-либо предметы и НЕ располагайте его в местах, где на них можно наступить.
- НЕ используйте устройство, если кабель или адаптер питания неисправен, так как это может привести к поражению электрическим током.
- Если кабель или адаптер питания поврежден, отключите его от розетки электропитания.
- НЕ пытайтесь ремонтировать кабель или адаптер питания. Для заказа нового адаптера питания свяжитесь с местным поставщиком.
- НЕ используйте устройство вне помещения и убедитесь, что все соединения также находятся внутри помещения. Существует определенный риск получения удара электрическим током при разряде молнии.
- Не заслоняйте вентиляционные отверстия устройства, так как недостаточный приток воздуха может стать причиной повреждения устройства.

- Используйте только телекоммуникационный кабель №26 AWG (American Wire Gauge – американская система калибровки проводов) или большего размера.
- Предупреждение об использовании антенны: данное устройство соответствует требованиям сертификации ETSI и FCC при использовании с входящей в комплект антенной(ми). используйте ТОЛЬКО антенну(ы) из комплекта поставки.
- Если устройство должно быть закреплено на стене, убедитесь, что при этом не будут повреждены электропроводка, газо- или водопроводы.

Материалы изделия пригодны для переработки. Утилизация должна производиться надлежащим образом.



Содержание

Оглавление

Перечень рисунков

Перечень таблиц

Часть I
Введение

1

Знакомство с P660HWP

В этой главе рассказывается об основных функциях и сферах применения P660HWP, а также о способах управления устройством P660HWP.

1.1 Обзор

Поздравляем вас с приобретением домашнего интернет-центра ZyXEL!

Это высокотехнологичное устройство обеспечивает удобное безопасное подключение вашего дома или офиса к Интернету по ADSL-каналу и делает возможным использование современных услуг интерактивного цифрового телевидения и интернет-телефонии. Установив интернет-центр, вы сможете одновременно выходить в Интернет с нескольких компьютеров, обмениваться между ними фотографиями, музыкой и документами, играть в сетевые игры, совместно использовать принтер. Интернет-центр ZyXEL позволяет использовать высокоскоростное подключение к Интернету для приема интерактивного цифрового телевидения и телефонной связи. Домашний интернет-центр ZyXEL открывает перед вами множество новых возможностей общения, обучения и развлечений.

Встроенный адаптер HomePlug AV позволит вам быстро и качественно подключить свой телевизор к цифровому телевидению в любой точке квартиры без прокладки дополнительных проводов и использования ненадежных беспроводных соединений.

Чтобы настроить подключение к Интернету и цифровому телевидению, не обязательно вдаваться в технические подробности и вызывать на дом специалиста. Достаточно выбрать своего интернет провайдера и тариф из предложенного списка, а все остальное в считаные минуты сделает интеллектуальная технология ZyXEL NetFriend.

Полный список возможностей устройства см. в приложении со спецификациями продукта.

«1» в конце наименования модели (например, P660 серий H/HW-D), обозначает устройство, работающее через аналоговую телефонную систему POTS (Plain Old Telephone Service – Традиционная телефонная сеть общего пользования). «3» в конце наименования модели обозначает устройство, работающее по сети ISDN (Integrated Services Digital Network – Цифровая сеть с предоставлением комплексных услуг).

Модели DSL RJ-11 (ADSL с подключением через POTS) или RJ-45 (ADSL с подключением через ISDN) подключаются к телефонной линии, обеспечивающей подключение по ADSL или ISDN.

Входящие в комплект кабель питания и штепсельная вилка подключаются к домашней сети электропитания.

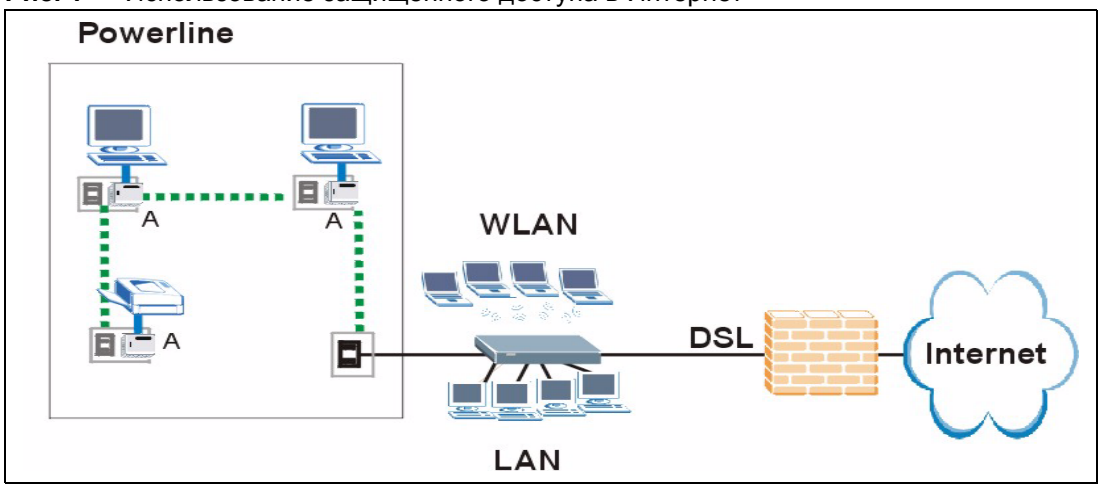
Необходимо использовать микропрограммное обеспечение P660HWP строго в соответствии с конкретной моделью устройства. См. наклейку, находящуюся на нижней панели интернет-центра P660HWP.

Интернет-центр P660HWP является идеальным решением для организации высокоскоростного доступа в Интернет. Он совместим со всеми основными провайдерами ADSL DSLAM (Digital Subscriber Line Access Multiplexer – Мультиплексор цифровых абонентских линий) и поддерживает стандарты ADSL (см. Табл. 1 на с. 37). Кроме того, устройство P660HWP с возможностью беспроводной связи может предоставлять беспроводным клиентам доступ в Интернет и к ресурсам Вашей сети.

Интернет-центр P660HWP обеспечивает защиту от атак, производимых Интернет-хакерами. По умолчанию межсетевой экран блокирует весь входящий трафик из глобальной сети (WAN). Межсетевой экран модема контролирует TCP/UDP, распознает и предотвращает DoS, выдает сигналы тревоги и ведет регистрацию событий и сообщений.

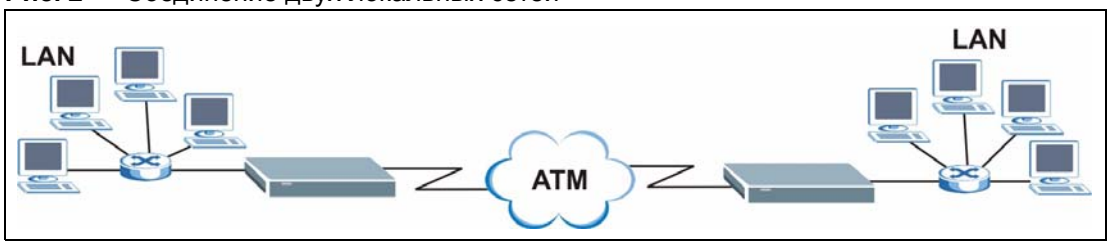
Типичный пример организации доступа в Интернет приводится ниже.

Рис. 1 Использование защищенного доступа в Интернет



P660HWP можно использовать для соединения с помощью линии ADSL двух географически разделенных сетей. Типичный пример соединения двух локальных сетей приводится ниже.

Рис. 2 Соединение двух локальных сетей



P660HWP совместим со стандартами ADSL/ADSL 2/ADSL 2+. В следующей таблице представлены максимально достижимые скорости передачи для каждого стандарта.

Табл. 1 Стандарты ADSL

СТАНДАРТ СКОРОСТИ ПЕРЕДАЧИ ДАННЫХ	ПЕРЕДАЧА ДАННЫХ	ПРИЕМ ДАННЫХ
ADSL	832 Кбит/с	8 Мбит/с
ADSL 2	3,5 Мбит/с	12 Мбит/с
ADSL 2+	3,5 Мбит/с	24 Мбит/с

Если ваше устройство P660HWP не поддерживает дополнительный стандарт Annex M (ADSL 2+M), то максимальная скорость передачи данных для ADSL 2/2+ составит 1,2 Мбит/с. Устройства P660HWP, работающие по ISDN, не поддерживают Annex M (ADSL 2+M).

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

1.2 Способы управления устройством P660HWP

Для управления устройством P660HWP используются следующие средства:

- Web-конфигуратор. Рекомендуется для повседневного управления устройством P660HWP с использованием рекомендуемого Web-браузера.
- Интерфейс командной строки. Управление с помощью команд главным образом используется сервисными инженерами при поиске и устранении неисправностей.
- Обновление микропрограммы и резервное копирование или восстановление конфигурации через FTP (Гл. 21 на с. 319).
- SNMP. Мониторинг устройства можно выполнять через управляющую станцию SNMP. Информацию по этому вопросу см. в главе «SNMP» в данном руководстве.

- SPTGEN. SPTGEN – это текстовый файл конфигурации, который можно загружать в устройство и, таким образом, настраивать его. Особенно удобно его использовать для настройки большого числа однотипных устройств.
- TR-069. Это сервер автоматической удаленной настройки устройств.

1.3 Полезные советы по управлению P660HWP

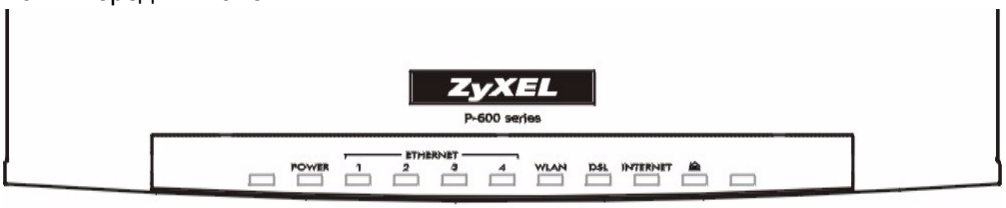
Для обеспечения безопасной и более эффективной работы устройства P660HWP рекомендуется регулярное и правильное выполнение описанных далее процедур для P660HWP.

- Изменение пароля. Необходимо использовать пароль, который не поддается легкому угадыванию и состоит из символов различных типов, например, из букв и цифр.
- Запишите пароль и храните в безопасном месте.
- Сделайте резервное сохранение конфигурации (необходимо знать, как выполнить восстановление конфигурации). В случае, если устройство работает нестабильно или не работает вообще, может помочь восстановление предыдущей рабочей конфигурации. Если пароль утерян, необходимо выполнить сброс параметров P660HWP к настройкам, установленным изготовителем по умолчанию. При наличии файла предыдущей рабочей конфигурации, не придется заново выполнять полную настройку P660HWP. Можно просто восстановить последнюю конфигурацию.

1.4 Светодиоды

На следующем рисунке изображены светодиоды модели P660HWP.

Рис. 3 Передняя панель



Описание светодиодов представлено в следующей таблице.

Табл. 2 Светодиоды передней панели

СВЕТО-ДИОД	ЦВЕТ	СОСТОЯНИЕ	ОПИСАНИЕ
POWER (Питание)	Зеленый	Горит	Питание подается и P660HWP работает нормально.
		Мигает	P660HWP выполняет перезагрузку или диагностику.
	Красный	Горит	Напряжение электропитания, подаваемое на интернет-центр P660HWP, слишком низкое.
		Не горит	Система получает питание, но не работает.
Ethernet (Локальная сеть)	Зеленый	Горит	Устройство P660HWP успешно установило Ethernet-подключение.
		Мигает	P660HWP передает/принимает данные.
		Не горит	Локальная сеть не подключена.
WLAN (Беспро-водная локальная сеть)	Зеленый	Горит	Интернет-центр P660HWP готов, но не передает и не принимает данные по беспроводной сети.
		Мигает	Интернет-центр P660HWP принимает / передает данные по беспроводной сети.
		Не горит	Беспроводная сеть не готова или неисправна.
DSL	Зеленый	Горит	Соединение DSL установлено.
		Мигает	P660HWP инициализирует линию DSL.
		Не горит	Канал DSL не работает.
INTERNET (Интернет)	Зеленый	Горит	Подключение к Интернет установлено, но передачи данных нет.
		Мигает	Устройство P660HWP передает данные через DSL-линию.
		Не горит	Нет подключения.
	Красный	Горит	Устройство P660HWP пыталось подключиться, но не смогло установить соединение.
POWERLINE (Электри-ческая сеть)	Зеленый	Горит	Устройство P660HWP обнаружило другой Ethernet-адаптер в сети электропитания.
		Мигает	Устройство P660HWP передает данные. (Во время управления сетью светодиоды не мигают.)
		Не горит	Устройство P660HWP не обнаружило в сети электропитания другого Ethernet-адаптера.

1.5 Подключение оборудования

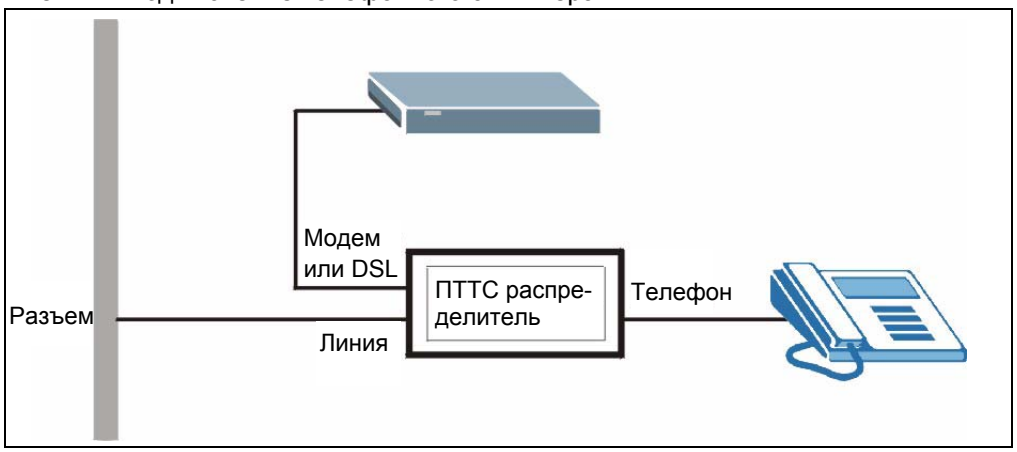
Подключение аппаратных средств описано в Кратком руководстве.

1.5.1 Подключение телефонного сплиттера

При использовании полноскоростного стандарта ADSL (стандарт G.dmt) можно подключить телефонный сплиттер, обеспечивающий разделение телефонных сигналов и сигналов ADSL. Это позволяет одновременно использовать одну телефонную линию для звонков и доступа в Интернет. Кроме того, сплиттер устраняет помехи, вносимые телефонными аппаратами.

Сплиттер устанавливается в точке подвода телефонной линии, как показано на следующем рисунке.

Рис. 4 Подключение телефонного сплиттера



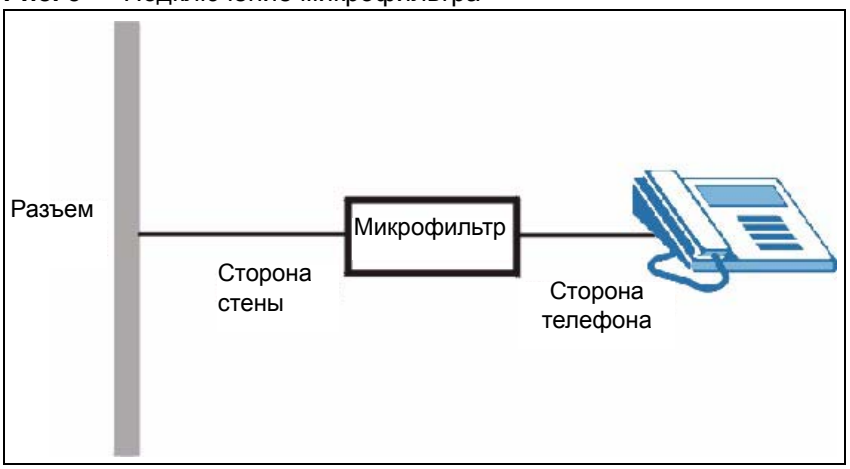
1. Подключите разъем с маркировкой «Phone» к телефону.
2. Подключите разъем с маркировкой «Modem» или «DSL» к устройству P660HWP.
3. Подключите разъем с маркировкой «Line» к настенной телефонной розетке.

1.5.2 Телефонные микрофильтры

Передача голосовых сигналов телефона происходит в более низком диапазоне частот (0 - 4 кГц), в то время как передача сигналов ADSL – в более высоком широкополосном диапазоне (более 4 кГц). Микрофильтр действует как фильтр нижних частот для телефона, что обеспечивает отсутствие влияния сигналов ADSL на передачу телефонных сигналов. Телефонный микрофильтр поставляется отдельно.

1. Найдите и отключите все телефоны.
2. Подключите кабель от телефонной розетки к разъему «wall side» микрофильтра.
3. Подключите разъем «phone side» микрофильтра к телефону, как показано на следующем рисунке.
4. После подключения кабелей проверьте работу телефона. Если телефон не работает, отключите микрофильтр и обратитесь в местную телефонную компанию или к поставщику микрофильтра.

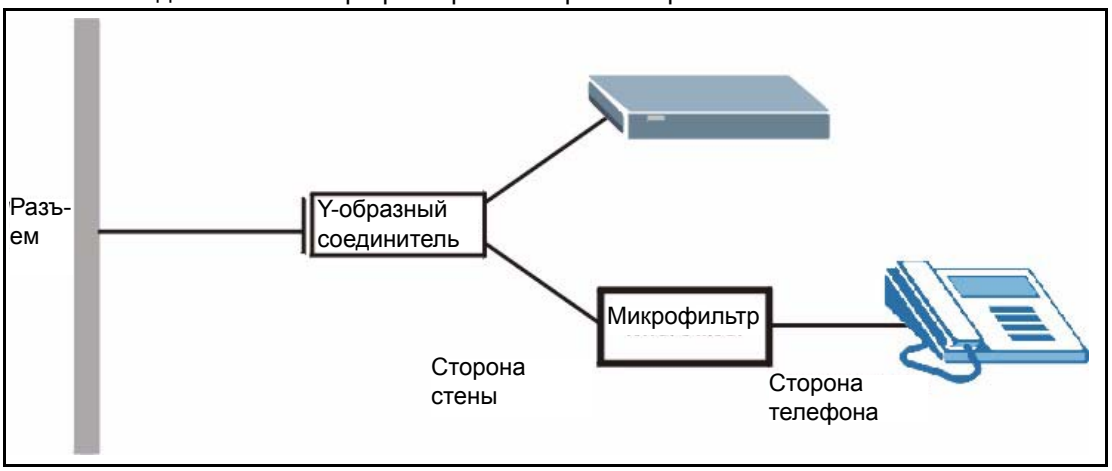
Рис. 5 Подключение микрофильтра



Также можно использовать Y-образный разъем с микрофильтром, чтобы подключить модем и телефон к одной телефонной розетке без использования телефонного разделителя частот.

1. Подключите телефонный кабель от настенной розетки к Y-образному разъему со стороны с одним выводом.
2. Подключите один кабель от Y-образного разъема со стороны с двумя выводами к разъему «wall side» микрофильтра.
3. Подключите другой кабель от конца Y-образного разъема с двумя выводами к P660HWP.
4. Подключите разъем «phone side» микрофильтра к телефону, как показано на следующем рисунке.

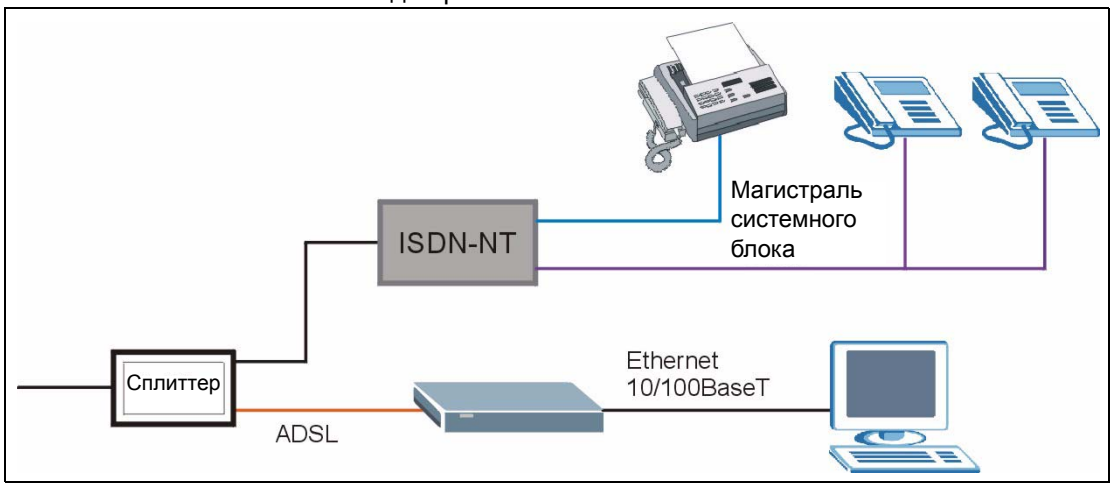
Рис. 6 Подключение микрофильтра и Y-образного разъема



1.5.3 Установка P660HWP для работы по ISDN

Этот раздел предназначен только для тех, кто использует интернет-центр P660HWP с ADSL в сети ISDN (Integrated Services Digital Network – Цифровая сеть с предоставлением комплексных услуг). Ниже приводится пример установки P660HWP для работы по ISDN.

Рис. 7 Установка P660HWP для работы по ISDN



2

Знакомство с Web-конфигуратором

В этой главе описаны способы получения доступа к Web-конфигуратору и методы работы с его интерфейсом.

2.1 Описание Web-конфигуратора

Web-конфигуратор – это интерфейс управления на основе технологии HTML, который позволяет выполнять настройку и управление устройством P660HWP с помощью браузера Интернет. Следует использовать Internet Explorer версии 6.0 и выше либо Netscape Navigator версии 7.0 и выше. Рекомендуемое разрешение экрана: 1024 на 768 пикселей.

Чтобы воспользоваться web-конфигуратором, необходимо включить следующие параметры:

- Всплывающие окна в Интернет-браузере. Блокировка всплывающих окон активирована по умолчанию в Windows XP SP2.
- Поддержка JavaScript (по умолчанию активирована).
- Разрешения Java (Java permissions) (активированы по умолчанию).

Информацию о том, как проверить, действительно ли эти функции включены в браузере Internet Explorer, см. в главе «Поиск и устранение неисправностей».

2.2 Доступ к Web-конфигуратору

Несмотря на то, что существует возможность беспроводного подключения к устройству P660HWP, для начальной настройки рекомендуется подключить компьютер к порту LAN.

1. Убедитесь, что P660HWP подключен правильно (см. Краткое руководство).
2. Подготовьте компьютер/компьютерную сеть для подключения к интернет-центру P660HWP (см. Краткое руководство).

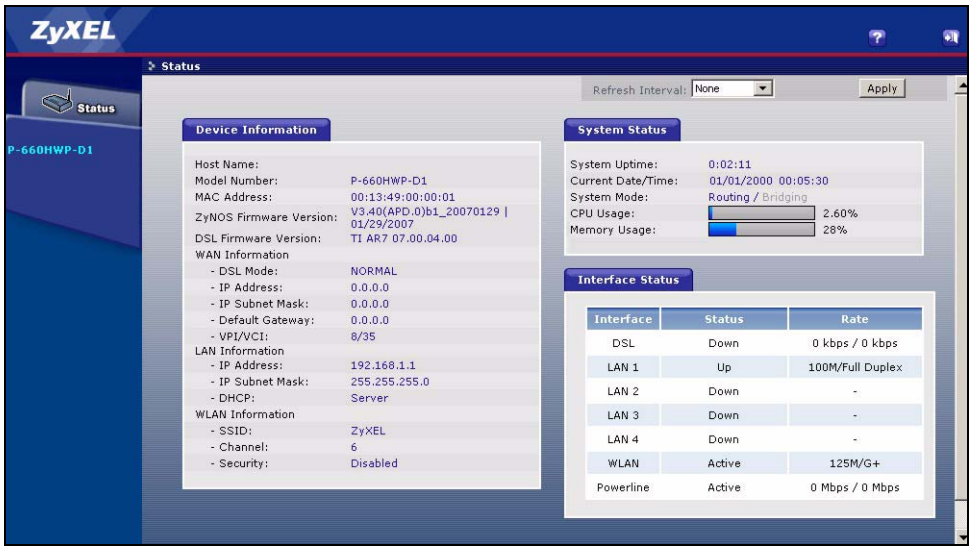
3 Запустите Web-браузер.
4 В адресной строке введите «http://192.168.1.1».
5 Появится следующий экран.

Рис. 8 Окно ввода пароля

2.2.1 Пользовательский доступ

1 Чтобы получить пользовательский доступ только для просмотра состояния, введите стандартный пароль пользователя **user**. Откроется следующее окно.

Рис. 9 Окно состояния



2.2.2 Администраторский доступ

1 Чтобы получить администраторский доступ для настройки мастеров и дополнительных функций, введите стандартный пароль администратора **1234**.
2 Нажмите кнопку **Login (Регистрация)**, чтобы перейти в окно изменения пароля или **Cancel (Отмена)**, чтобы сохранить пароль по умолчанию.
3 Если вы ввели пароль администратора, настоятельно рекомендуется изменить пароль администратора по умолчанию! Введите новый пароль (от 1 до

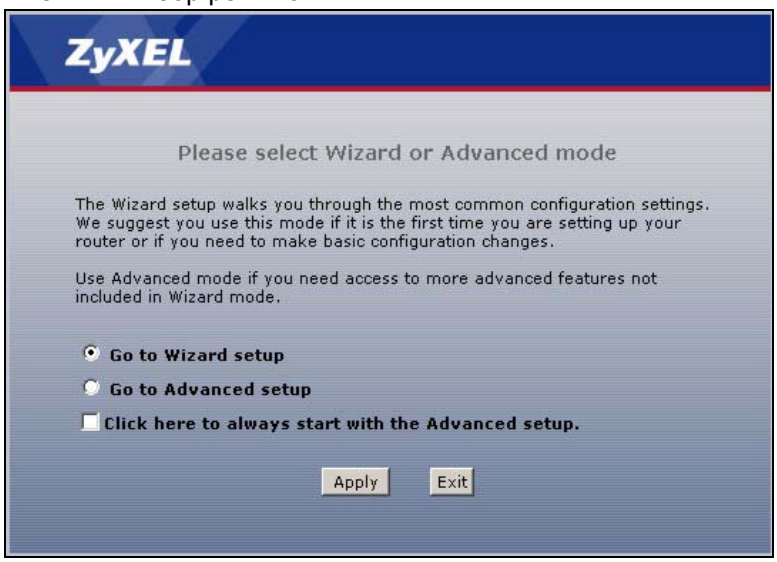
30 символов), еще раз введите его для подтверждения и нажмите кнопку **Apply (Применить)**. Если в настоящее время менять пароль не требуется, щелкните по кнопке **Ignore (Игнорировать)** для перехода в главное меню.

Если вы не изменили пароль, то каждый раз при регистрации с паролем администратора будет появляться следующее окно.

Рис. 10 Изменение пароля при входе

4 Выберите **Go to Wizard setup (Мастер установки)** и нажмите кнопку **Apply (Применить)** для отображения главного окна Мастера установки. В противном случае, выберите **Go to Advanced setup (Дополнительная настройка)** и щелкните **Apply (Применить)** для отображения окна **Status (Статус)**.

Рис. 11 Выбор режима



Сеанс управления будет автоматически завершен по истечении периода времени, установленного в поле Administrator Inactivity Timer (Время простоя в режиме администрирования), по умолчанию – 5 минут. В этом случае следует снова выполнить процедуру регистрации в P660HWP.

2.3 Сброс настроек интернет-центра P660HWP к заводским установкам

Если вы забыли пароль или не можете получить доступ к Web-конфигуратору, необходимо нажать на кнопку **RESET** на задней панели P660HWP для загрузки файла конфигурации, установленного изготовителем по умолчанию. Это означает, что прежняя конфигурация будет полностью потеряна, и пароль будет установлен на значение по умолчанию «1234».

2.3.1 Использование кнопки сброса настроек

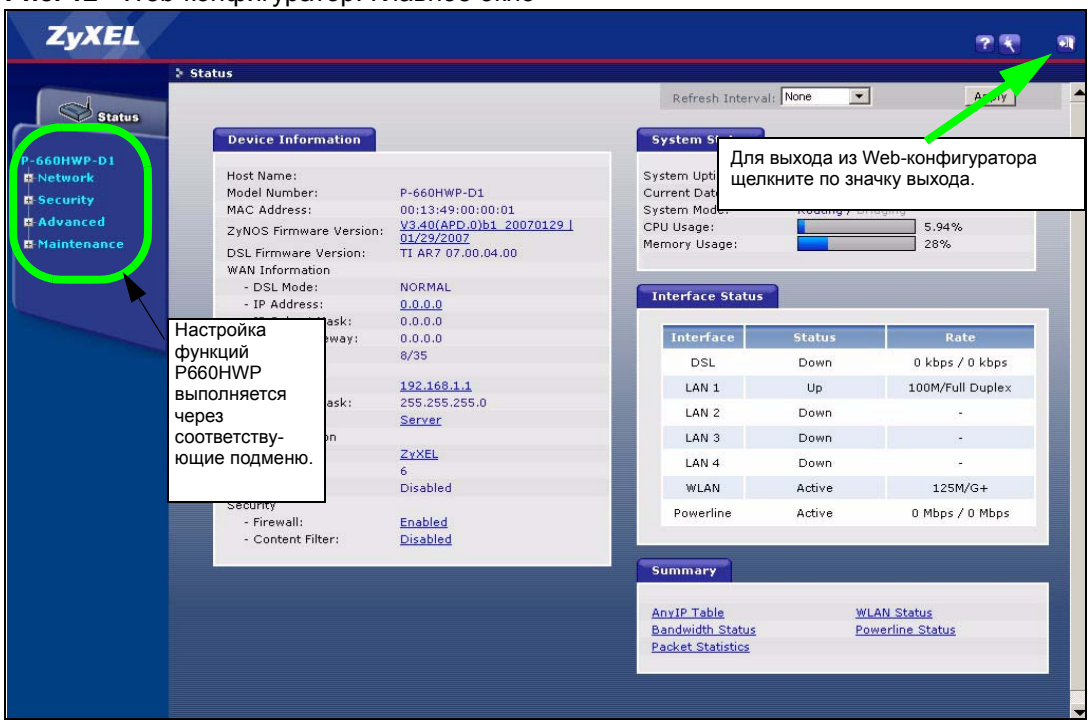
1. Убедитесь, что светодиод **POWER** горит (не мигает).
2. Нажмите и удерживайте кнопку **RESET** в течение 10 секунд или до тех пор, пока светодиод **POWER** не начнет мигать, затем отпустите ее. Когда светодиод **POWER** начинает мигать, это означает, что настройки по умолчанию восстановлены и происходит перезапуск P660HWP.

2.4 Интерфейс Web-конфигуратора

2.4.1 Панель навигации

После ввода пароля администратора отображается главное меню. Для настройки функций P660HWP используются соответствующие подменю в панели навигации. Описание подменю представлено в следующей таблице.

Рис. 12 Web-конфигуратор: Главное окно



Для просмотра встроенной справки щелкните по значку (расположена в верхнем правом углу большинства окон).

Табл. 3 Сводная таблица окон Web-конфигуратора

ССЫЛКА/ ИКОНКА	ПОДРАЗДЕЛ	ФУНКЦИЯ
Wizard (Мастер установки)	INTERNET/ WIRELESS SETUP (НАСТРОЙКА ИНТЕРНЕТА / БЕСПРОВОДНОЙ СЕТИ)	Эти окна используются для первоначальной настройки, включая настройку общих параметров, параметров Интернет-провайдера для доступа в Интернет и назначения IP-адреса в глобальной сети, сервера DNS, MAC-адреса.
	BANDWIDTH MANAGEMENT SETUP (УПРАВЛЕНИЕ ПРОПУСКНОЙ СПОСОБНОСТЬЮ)	Эти окна используются для ограничения пропускной способности для конкретного приложения или типа пакетов.
Logout (Выход)		Для выхода из Web-конфигуратора щелкните по этой иконке.
Status (Состояние)		В этом окне отображается общая информация о состоянии устройства, системы и интерфейсов P660HWP. Это окно открывает доступ к таблицам, содержащим сводную статистику системы.

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

ССЫЛКА/ ИКОНКА	ПОДРАЗДЕЛ	ФУНКЦИЯ
Network (Сеть)		
WAN (Глобальная сеть)	Internet Connection (Подключение к Интернету)	Это окно позволяет назначить IP-адрес устройства в глобальной сети, установить параметры Интернет-провайдера, определить серверы DNS и настроить другие свойства.
	More Connections (Другие соединения)	Это окно используется для просмотра и настройки других соединений для выполнения вызовов на другой удаленный шлюз.
	WAN Backup Setup (Настройка резервного подключения к глобальной сети)	Это окно используется для настройки параметров перенаправления трафика и резервирования глобальной сети.
LAN (Локальная сеть)	IP	Это окно используется для настойки протокола TCP/IP в локальной сети, включения функции «Any IP» (Любой IP), и других свойств.
	DHCP Setup (Настройка DHCP)	Это окно используется для настройки протокола DHCP в локальной сети.
	Client List (Список клиентов)	Это окно используется для просмотра параметров конкретного клиента DHCP и назначения IP-адреса по MAC-адресу (и имени узла).
	IP Alias (Псевдоним IP)	Это окно позволяет разделить локальную сеть на подсети.
Wireless LAN (Беспроводная локальная сеть)	General (Общие)	Это окно используется для настройки беспроводной локальной сети.
	OTIST	Это окно используется для включения функции OTIST.
	MAC Filter (Фильтрация MAC-адресов)	Параметры в этом окне позволяют настроить P660HWP на блокирование доступа к конкретным устройствам или блокирование доступа этих устройств к P660HWP.
	QoS (Качество услуг)	Это окно используется для настройки качества услуги Wi-Fi Multimedia (WMM QoS). Функция WMM QoS позволяет назначать приоритет беспроводному трафику в соответствии с требованиями к доставке со стороны отдельных служб.
Powerline (Электрическая сеть)	Local Setting (Локальные настройки)	Это окно используется для настройки параметров устройства, имеющего поддержку работы через локальную электрическую сеть.
	Remote Setting (Удаленные настройки)	Это окно используется для настройки параметров работы адаптеров электрических линий в электрической сети.
	Status (Состояние)	Это окно используется для просмотра состояния электрической сети.
NAT (Трансляция сетевых адресов)	General (Общие)	Это окно используется для включения функции NAT.
	Port Forwarding (Переадресация портов)	Это окно используется для настройки серверов, находящихся за P660HWP.
Security (Безопасность)		

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

ССЫЛКА/ ИКОНКА	ПОДРАЗДЕЛ	ФУНКЦИЯ
Firewall (Межсетевой экран)	General (Общие)	Это окно используется для активации/деактивации межсетевого экрана и направления сетевого трафика, для которого применяются правила.
	Rules (Правила)	Это окно показывает список правил межсетевого экрана и позволяет редактировать/добавлять правила.
	Anti Probing (Блокирование эхо-тестирования)	Это окно используется для изменения настроек блокирования эхо-тестирования.
	Threshold (Пороговое значение)	Это окно используется для настройки допустимого порога для атаки типа DoS.
Content Filter (Контент-фильтр)	Keyword (Ключевое слово)	Это окно используется для блокировки сайтов, содержащих определенные ключевые слова в URL.
	Schedule (График)	В этом окне устанавливается расписание, по которому P660HWP выполняет фильтрацию содержания.
	Trusted (Доверенные)	В этом окне можно определить группу пользователей локальной сети, для которых P660HWP не будет выполнять фильтрацию содержания.
Certificates (Сертификаты)	My Certificates (Мои сертификаты)	
	Trusted CA's (Доверенные центры сертификации)	
	Trusted Remote Hosts (Доверенные удаленные узлы)	
	Directory Servers (Серверы каталогов)	
Advanced (Дополнительные настройки)		
Static Route (Статический маршрут)	Static Route (Статический маршрут)	Здесь выполняется настройка статических маршрутов IP.
Bandwidth MGMT (Управление пропускной способностью)	Summary (Общие настройки)	Это окно позволяет включить управление пропускной способностью для конкретного интерфейса.
	Rule Setup (Настройка правил)	Это окно позволяет определить правила для пропускной способности интерфейса.
	Monitor (Мониторинг)	В этом окне содержится информация о распределении и использовании пропускной способности P660HWP.
Dynamic DNS (Динамическая система доменных имен)	Dynamic DNS (Динамическая система доменных имен)	Это окно используется для настройки динамической службы DNS.

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

ССЫЛКА/ ИКОНКА	ПОДРАЗДЕЛ	ФУНКЦИЯ
Remote MGMT (Удаленное управление)	WWW	В этом окне можно определить, через какие интерфейсы и с каких IP-адресов пользователям разрешается выполнять управление P660HWP по протоколу HTTPS или HTTP.
	Telnet	В этом окне можно определить, через какие интерфейсы и с каких IP-адресов пользователям разрешается выполнять управление P660HWP по протоколу Telnet.
	FTP	В этом окне можно определить, через какие интерфейсы и с каких IP-адресов пользователям разрешается доступ к P660HWP по протоколу FTP.
	SNMP	В этом окне производятся настройки для управления P660HWP по протоколу SMNP (Простой протокол управления сетью).
	DNS	В этом окне можно определить, через какие интерфейсы и с каких IP-адресов пользователи могут посылать запросы DNS к P660HWP.
	ICMP	Это окно используется для изменения настроек блокирования эхо-тестирования.
UPnP (Универсальная функция Plug and Play)	General (Общие)	Это окно используется для включения в P660HWP функции UPnP (Универсальная функция Plug and Play).
Maintenance (Сопровождение)		
System (Система)	General (Общие)	Это окно служит для отображения административной и общесистемной информации, а также позволяет изменить пароль.
	Time Setting (Установка времени)	Это окно используется для изменения даты и времени в P660HWP.
Logs (Регистра-ционные журналы)	View Log (Просмотр журнала регистрации)	Это окно используется для просмотра журналов регистрации для категорий, которые вы выбрали.
	Log Settings (Настройки журналов)	Это окно используется для изменения настроек регистрационных журналов P660HWP.
Tools (Программные средства)	Firmware (Микропрограмма)	Это окно используется для загрузки микропрограммы в P660HWP.
	Configuration (Конфигурация)	Это окно позволяет выполнять резервное сохранение и восстановление конфигурации или сброс настроек P660HWP к заводским установкам.
	Restart (Перезапуск)	Это окно позволяет выполнить перезагрузку P660HWP без выключения электропитания.
Diagnostic (Диагностика)	General (Общие)	Информация, отображаемая в этих окнах, помогает определить неисправности, связанные с подключением P660HWP.
	DSL Line (Линия DSL)	Информация в этих окнах помогает выявлять неполадки DSL-линии.

2.4.2 Окно состояния

В этом разделе рассказывается, как работать с Web-конфигуратором из окна **Status (Состояние)**. Если в окне ввода пароля вы зарегистрировались с правами пользователя, некоторые поля и ссылки будут недоступны (см. Рис. 8 на с. 44). Некоторые поля недоступны в некоторых моделях .

Рис. 13 Окно состояния

В следующей таблице представлено описание элементов окна **Status (Состояние)**.

Табл. 4 Окно состояния

ПОЛЕ	ОПИСАНИЕ
Refresh Interval (Интервал обновления)	Из выпадающего списка выберите количество секунд для автоматического обновления статистики в окнах по истечении заданного временного интервала или значение **None (Нет)**, чтобы статистика не обновлялась.
Apply (Применить)	Нажмите на эту кнопку для обновления статистических данных в окнах.
Device Information (Информация об устройстве)	
Host Name (Имя узла)	Здесь отображается **системное имя**, которое вводится в окне **Maintenance (Сопровождение)** > **System (Система)** > **General (Общие настройки)**. Это имя используется для идентификации.
Model Number (Номер модели)	Здесь отображается наименование модели P660HWP.
MAC Address (MAC-адрес)	Это уникальный MAC-адрес (Media Access Control – Управление доступом к среде) или адрес Ethernet P660HWP.
ZyNOS Firmware Version (Версия микропрограммы ZyNOS)	Здесь отображается версия и дата создания микропрограммы ZyNOS. ZyNOS – это сетевая операционная система, разработанная ZyXEL.
DSL Firmware Version (Версия микропрограммы DSL)	Это версия микропрограммы DSL, загруженной в P660HWP. Иногда используется техническими специалистами для решения проблем.

Табл. 4 Окно состояния (продолжение)

ПОЛЕ	ОПИСАНИЕ
WAN Information (Параметры глобальной сети)	
DSL Mode (Режим DSL)	Это стандарт, по которому работает P660HWP.
IP Address (IP-адрес)	Здесь отображается IP-адрес порта WAN.
IP Subnet Mask (Маска IP подсети)	Здесь отображается маска IP подсети для порта WAN.
Default Gateway (Шлюз по умолчанию)	Здесь отображается IP-адрес шлюза по умолчанию, если он применяется.
VPI/VCI	Это идентификатор виртуального пути и идентификатор виртуального канала, настраиваемые с помощью Мастера установки или в окне **WAN (Глобальная сеть)**.
LAN Information (Параметры локальной сети)	
IP Address (IP-адрес)	Здесь отображается IP-адрес порта LAN.
IP Subnet Mask (Маска IP подсети)	Здесь отображается маска IP подсети для порта LAN.
DHCP	Это DHCP роль порта WAN. Варианты для выбора: **Server (Сервер)**, **Relay (Ретранслятор)** или **None (Нет)**.
WLAN Information (Параметры беспроводной сети) – только для беспроводных устройств	
SSID (Имя сети)	Это описательное имя, используемое для идентификации P660HWP в беспроводной локальной сети.
Channel (Канал)	Это номер канала, по которому работает P660HWP.
Security (Безопасность)	Показывает уровень безопасности беспроводной сети, выбранный для P660HWP.
Security (Безопасность)	
Firewall (Межсетевой экран)	Это поле показывает, включен ли межсетевой экран P660HWP.
Content Filter (Контент-фильтр)	Это поле показывает, включена ли фильтрация контента для P660HWP.
System Status (Состояние системы)	
System Uptime (Время работы системы)	Здесь отображается время, истекшее с момента запуска P660HWP.
Current Date/ Time (Текущая дата/время)	В этом поле отображается текущая дата и время P660HWP.
System Mode (Режим системы)	В этом поле отображается режим работы P660HWP: маршрутизатор или мост.

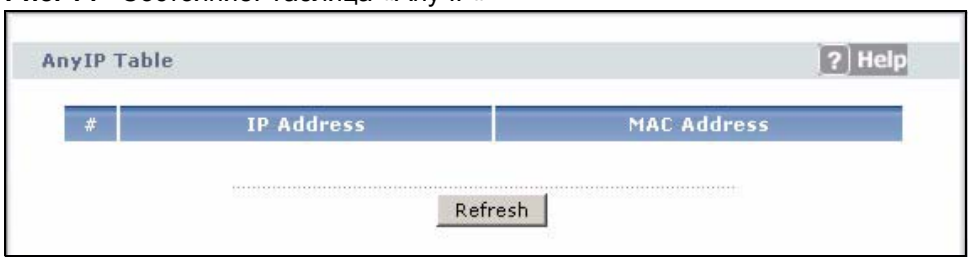
Табл. 4 Окно состояния (продолжение)

ПОЛЕ	ОПИСАНИЕ
CPU Usage (Загрузка центрального процессора)	Здесь отображается использование динамической памяти P660HWP в килобайтах. Операционная система ZyNOS (ZyXEL Network Operating System) не использует динамическую память, т. о., она может использоваться для работы таких функций как NAT, VPN и межсетевой экран. Индикатор показывает процент использования динамической памяти P660HWP. Индикатор меняет свой цвет с зеленого на красный, когда память используется полностью.
Memory Usage (Использование памяти)	Здесь отображается использование всей памяти P660HWP в килобайтах. Индикатор показывает процент использования динамической памяти P660HWP. Индикатор меняет свой цвет с зеленого на красный, когда память используется полностью.
Interface Status (Статус портов)	
Interface (Порт)	В этом поле отображаются типы портов P660HWP.
Status (Состояние)	В этом поле отображается **Down (Нет)** (соединение отсутствует), **Up (Работает)** (соединение установлено и активно), если установлена инкапсуляция Ethernet, или **Down (Нет)** (соединение отсутствует), **Up (Работает)** (соединение установлено и активно), **Idle (Ожидание)** (соединение (ppp) в режиме ожидания), **Dial (Вызов)** (запуск процедуры вызова) и **Drop (Сброс)** (сброс соединения), если установлена инкапсуляция PPPoE.
Rate (Скорость передачи)	Для портов LAN здесь отображается скорость порта и режим дуплексной передачи. Соединения через порт Ethernet могут работать в полудуплексном или дуплексном режиме передачи. В дуплексном режиме передачи устройство однвременно передает и принимает данные, тогда как в полудуплексном режиме в конкретный момент времени трафик передается только в одном направлении. Для установления соединения порт Ethernet должен использовать такие же настройки скорости и режима передачи, как и порт Ethernet клиентской стороны. Для порта WAN здесь отображается скорость приема и передачи данных.
Summary (Общие настройки)	
Any IP Table (Таблица «Any IP»)	В этом окне отображается список IP-адресов и MAC-адресов компьютеров, которые находятся в подсети, отличной от подсети P660HWP.
WLAN Status (Статус беспроводной сети) (только для беспроводных устройств)	В этом окне отображаются MAC-адреса беспроводных станций, подключенных к P660HWP.
Bandwidth Status (Пропускная способность)	В этом окне содержится информация о распределении и использовании пропускной способности P660HWP.
Packet Statistics (Статистика пакетов)	В этом окне отображается статус портов и статистика пакетов.
Powerline Status (Состояние электрической линии)	Показывает состояние подключения через электрическую линию.

2.4.3 Состояние: Таблица «Any IP»

Щелкните по гиперссылке **Any IP Table (Таблица «Any IP»)** в окне **Status (Состояние)**. В таблице «Any IP» отображаются текущие данные в режиме только для чтения (в том числе IP-адрес и MAC-адрес) для всех сетевых устройств, которые используют функцию «Any IP» (Любой IP) для подключения к P660HWP.

Рис. 14 Состояние: Таблица «Any IP»



В следующей таблице даны описания полей этого окна.

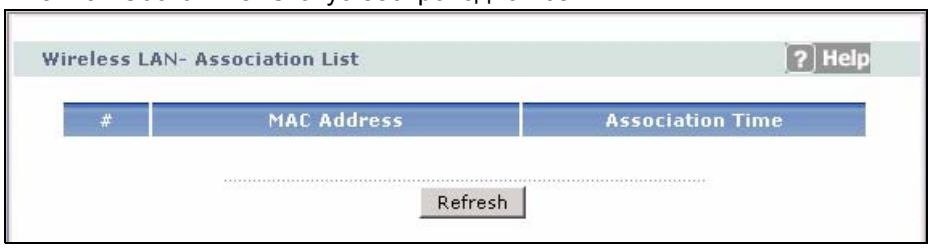
Табл. 5 Состояние: Таблица «Any IP»

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

2.4.4 Состояние: Статус беспроводной сети

Щелкните по гиперссылке **WLAN Status (Статус беспроводной сети)** в окне **Status (Состояние)** для просмотра информации о беспроводных станциях, которые в данный момент подключены к P660HWP.

Рис. 15 Состояние: Статус беспроводной сети



В следующей таблице даны описания полей этого окна.

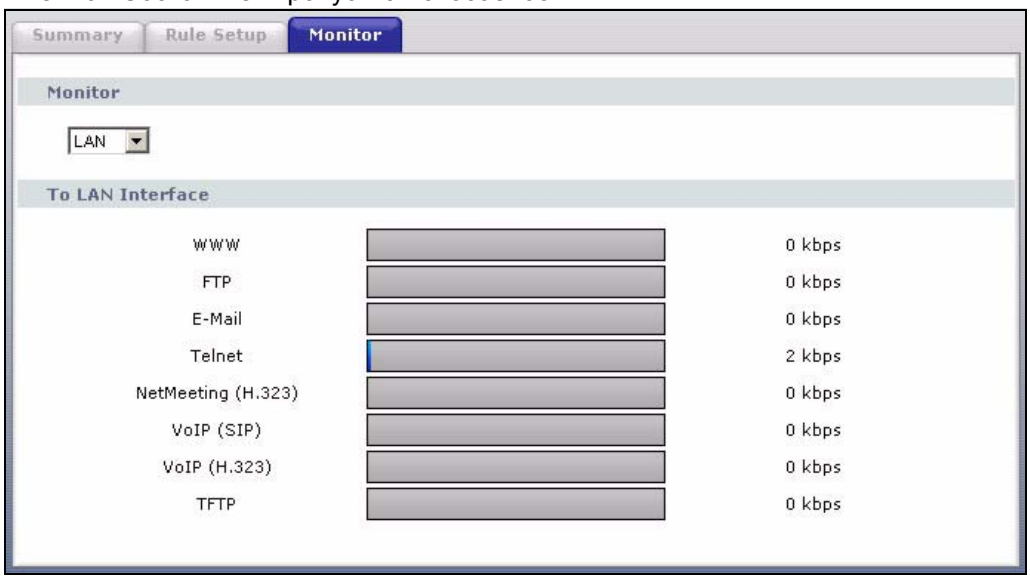
Табл. 6 Состояние: Статус беспроводной сети

ПОЛЕ	ОПИСАНИЕ
#	Это порядковый номер подключенного беспроводного устройства.
MAC Address (MAC-адрес)	В этом поле отображается MAC-адрес (Media Access Control – Управление доступом к среде) соответствующего беспроводного устройства.
Association TIme (Время подключения)	В этом поле отображается время, в течение которого беспроводная станция подключена к интернет-центру P660HWP.
Refresh (Обновить)	Щелкните **Refresh (Обновить)** для обновления информации в этом окне.

2.4.5 Состояние: Пропускная способность

Щелкните по ссылке **Bandwidth Status (Пропускная способность)** в окне **Status (Состояние)**. Из раскрывающегося списка выберите интерфейс, для которого необходимо посмотреть использование пропускной способности по правилам. Серая часть индикатора показывает неиспользуемую пропускную способность в процентах, а оранжевый цвет показывает используемую пропускную способность.

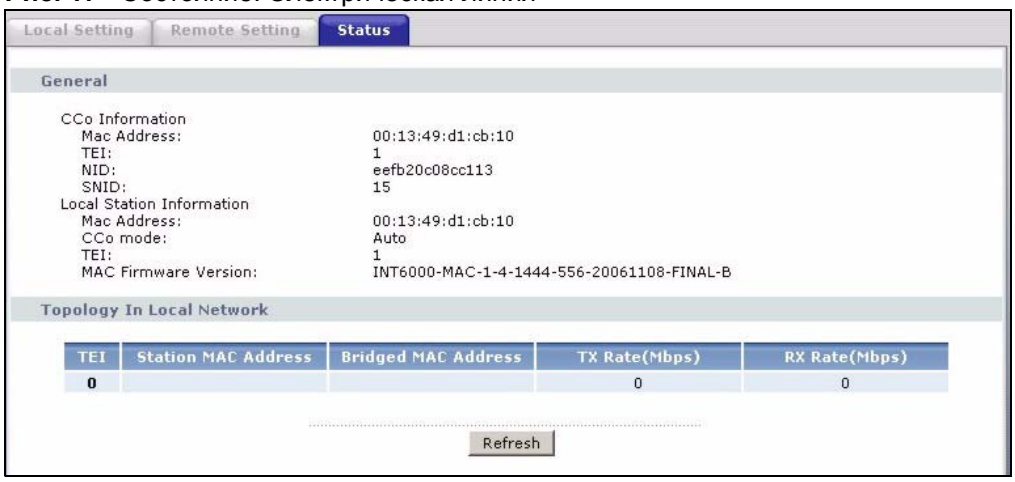
Рис. 16 Состояние: Пропускная способность



2.4.6 Состояние: Статистика электрической линии

Щелкните по ссылке **Powerline Statistics (Статистика электрической линии)** в окне **Status (Состояние)**. Откроется следующее окно.

Рис. 17 Состояние: Электрическая линия

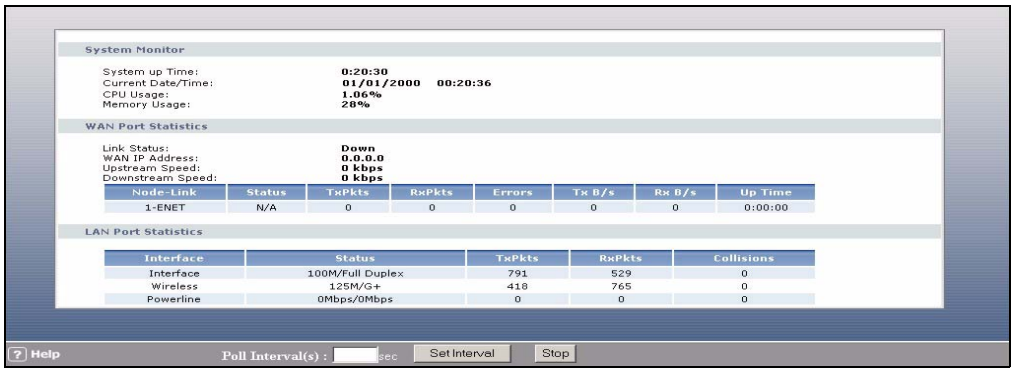


Значение заголовков этого окна см. Рис. 46 на с. 151.

2.4.7 Состояние: Статистика пакетов

Щелкните по гиперссылке **Packet Statistics (Статистика пакетов)** в окне **Status (Состояние)**. Здесь отображается информация о состоянии портов и статистика пакетов в режиме только для чтения. Также здесь отображается время работы системы и интервалы опроса системы. В поле **Poll Interval(s) (Интервал(ы) опроса)** можно изменять значение. Некоторые поля недоступны в некоторых моделях .

Рис. 18 Состояние: Статистика пакетов



В следующей таблице даны описания полей этого окна.

Табл. 7 Состояние: Статистика пакетов

ПОЛЕ	ОПИСАНИЕ
System Monitor (Системный мониторинг)	
System up Time (Время работы системы)	Здесь отображается время, истекшее с момента запуска системы.
Current Date/Time (Текущая дата/ время)	В этом поле отображается текущая дата и время P660HWP.
CPU Usage (Загрузка центрального процессора)	В этом поле отображается процент загрузки процессора модема.

Табл. 7 Состояние: Статистика пакетов (продолжение)

ПОЛЕ	ОПИСАНИЕ
Memory Usage (Использование памяти)	В этом поле отображается использование памяти в процентах.
WAN Port Statistics (Статистика порта WAN)	
Link Status (Состояние канала связи)	Здесь отображается состояние подключения к глобальной сети.
WAN IP Address (IP-адрес в глобальной сети)	IP-адрес в глобальной сети.
Upstream Speed (Скорость исходящего трафика)	В этом поле отображается скорость исходящего трафика P660HWP.
Downstream Speed (Скорость входящего трафика)	В этом поле отображается скорость входящего трафика P660HWP.
Node-Link (Узел – вид соединения)	В этом поле отображается порядковый номер удаленного узла и вид соединения. Виды соединения: PPPoA, ENET, RFC 1483 и PPPoE.
Status (Состояние)	В этом поле отображается **Down (Нет)** (соединение отсутствует), **Up (Работает)** (соединение установлено и активно), если установлена инкапсуляция Ethernet, или **Down (Нет)** (соединение отсутствует), **Up (Работает)** (соединение установлено и активно), **Idle (Ожидание)** (соединение (ppp) в режиме ожидания), Dial (Вызов) (запуск процедуры вызова) и **Drop (Сброс)** (сброс соединения), если установлена инкапсуляция PPPoE.
TxPkts (Передано пакетов)	В этом поле отображается количество пакетов, переданных через этот порт.
RxPkts (Принято пакетов)	В этом поле отображается количество пакетов, принятых через этот порт.
Errors (Ошибки)	В этом поле отображается количество пакетов с ошибками, принятых через этот порт.
Tx B/s (Скорость передачи, байт/с)	В этом поле отображается количество байтов, переданных в последнюю секунду.
Rx B/s (Скорость приема, байт/с)	В этом поле отображается количество байтов, принятых в последнюю секунду.
Up Time (Время соединения)	В этом поле отображается время, истекшее с момента установления соединения через этот порт.
LAN Port Statistics (Статистика порта LAN)	
Interface (Порт)	В данном поле отображается тип порта.
Status (Состояние)	В этом поле отображается **Down (Нет)** (соединение отсутствует), **Up (Работает)** (соединение установлено и активно), если установлена инкапсуляция Ethernet, или **Down (Нет)** (соединение отсутствует), **Up (Работает)** (соединение установлено и активно), **Idle (Ожидание)** (соединение (ppp) в режиме ожидания), Dial (Вызов) (запуск процедуры вызова) и **Drop (Сброс)** (сброс соединения), если установлена инкапсуляция PPPoE.

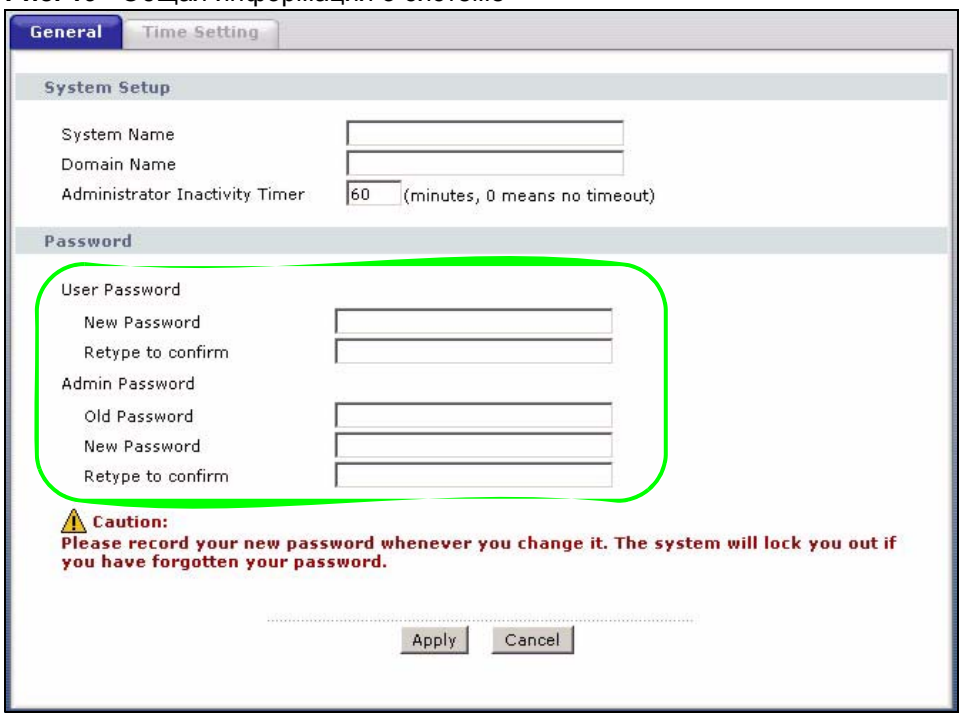
Табл. 7 Состояние: Статистика пакетов (продолжение)

ПОЛЕ	ОПИСАНИЕ
TxPkts (Передано пакетов)	В этом поле отображается количество пакетов, переданных через этот порт.
RxPkts (Принято пакетов)	В этом поле отображается количество пакетов, принятых через этот порт.
Collisions (Конфликты)	Здесь отображается количество конфликтов при передаче через данный порт.
Poll Interval(s) (Интервал(ы) опроса)	Введите интервал времени, через который браузер будет обновлять информацию о системе.
Set Interval (Установить интервал)	Нажмите на эту кнопку, чтобы применить новый интервал опроса, заданный в поле **Poll Interval (Интервал опроса)**.
Stop (Остановить)	Нажмите на эту кнопку, чтобы прекратить обновление информации о системе.

2.4.8 Изменение пароля

Настоятельно рекомендуется периодически изменять пароль доступа к P660HWP. Если после регистрации пароль по умолчанию не был изменен или требуется еще раз изменить пароль, щелкните **Maintenance (Сопровождение)** > **System (Система)** для отображения следующего окна. Подробное описание полей окна см. Табл. 107 на с. 294.

Рис. 19 Общая информация о системе



Часть II
Мастера

3

Мастер настройки доступа в Интернет и беспроводного доступа

В этой главе описываются окна Мастера установки Web-конфигуратора, используемые для настройки доступа в Интернет и беспроводного доступа.

3.1 Введение

Окна Мастера установки используются для настройки системы для доступа в Интернет и беспроводного доступа с помощью ввода параметров, предоставленных Интернет-провайдером.

Более подробная информация об этих полях приведена в главах, посвященных отдельным меню.

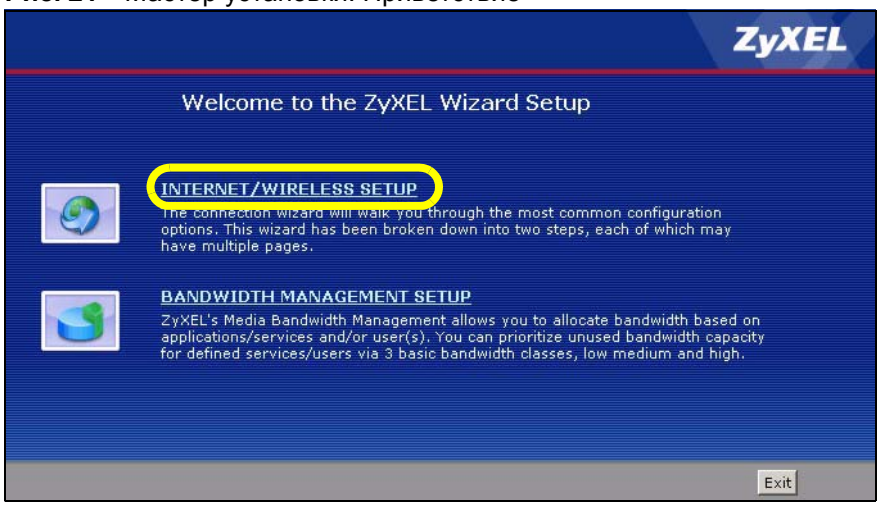
3.2 Настройка мастера доступа в Интернет и беспроводного доступа

1 После ввода пароля администратора и получения доступа к Web-конфигуратору, выберите **Go to Wizard setup (Запуск мастера установки)** и щелкните **Apply (Применить)**. Также для отображения главного окна Мастера установки можно щелкнуть по иконке Мастера установки ( ) в верхнем правом углу Web-конфигуратора.

Рис. 20 Выбор режима

2 Щелкните **INTERNET/WIRELESS SETUP (НАСТРОЙКА ДОСТУПА В ИНТЕРНЕТ И БЕСПРОВОДНОГО ДОСТУПА)**, чтобы настроить доступ в Интернет.

Рис. 21 Мастер установки: Приветствие

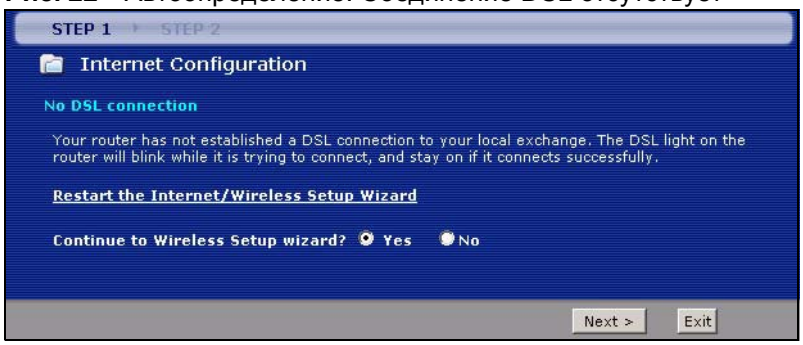


3 Мастер попытается определить, какой тип подключения к глобальной сети используется.

Если Мастер определяет тип соединения, и ваш Интернет-провайдер использует протокол PPPoE или PPPoA, перейдите к Разд. 3.2.1 на с. 63. Вид окна меняется в зависимости от типа соединения.

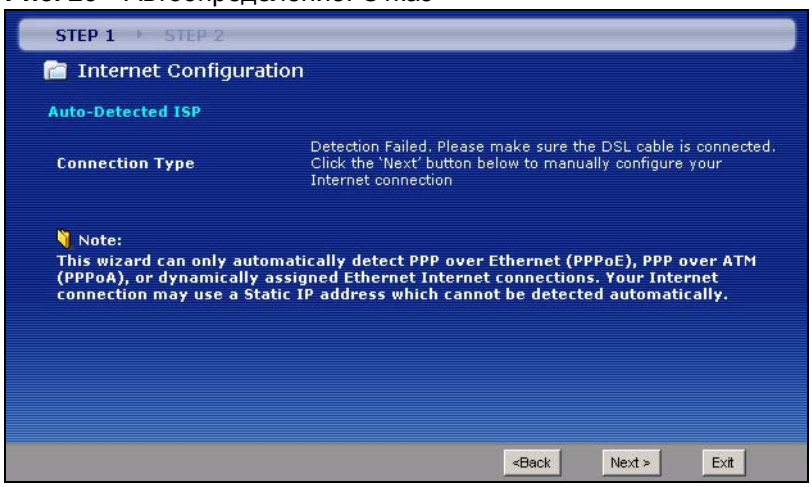
Если Мастер не может определить тип соединения, и появляется следующее окно (см. Рис. 22 на с. 63), проверьте подключение оборудования и щелкните **Restart the Internet/Wireless Setup Wizard (Повторный запуск Мастера установки Интернета / беспроводной сети)**, чтобы P660HWP попытался еще раз определить тип соединения.

Рис. 22 Автоопределение: Соединение DSL отсутствует



Если Мастер установки опять не может определить тип соединения, и появляется следующее окно (см. Рис. 23 на с. 63), щелкните по кнопке **Next (Далее)** и обратитесь к Разд. 3.2.2 на с. 64, где рассказывается, как настроить подключение P660HWP к Интернету вручную.

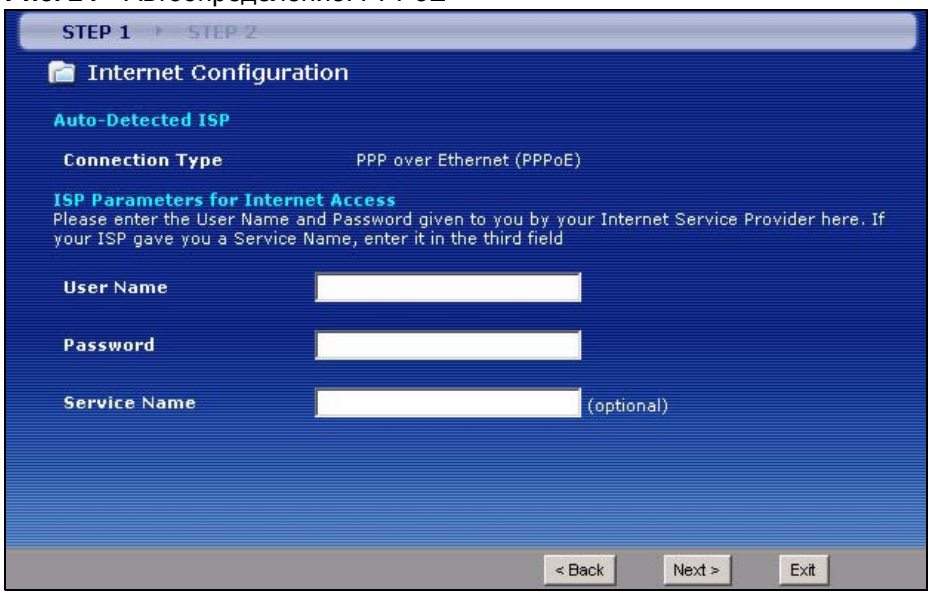
Рис. 23 Автоопределение: Отказ



3.2.1 Автоматическое определение

1. При подключении PPPoE или PPPoA появится окно с запросом на ввод данных учетной записи Интернет. Введите имя пользователя, пароль и/или имя услуги в соответствии с предоставленной провайдером информацией.
2. Нажмите кнопку **Next (Далее)**.

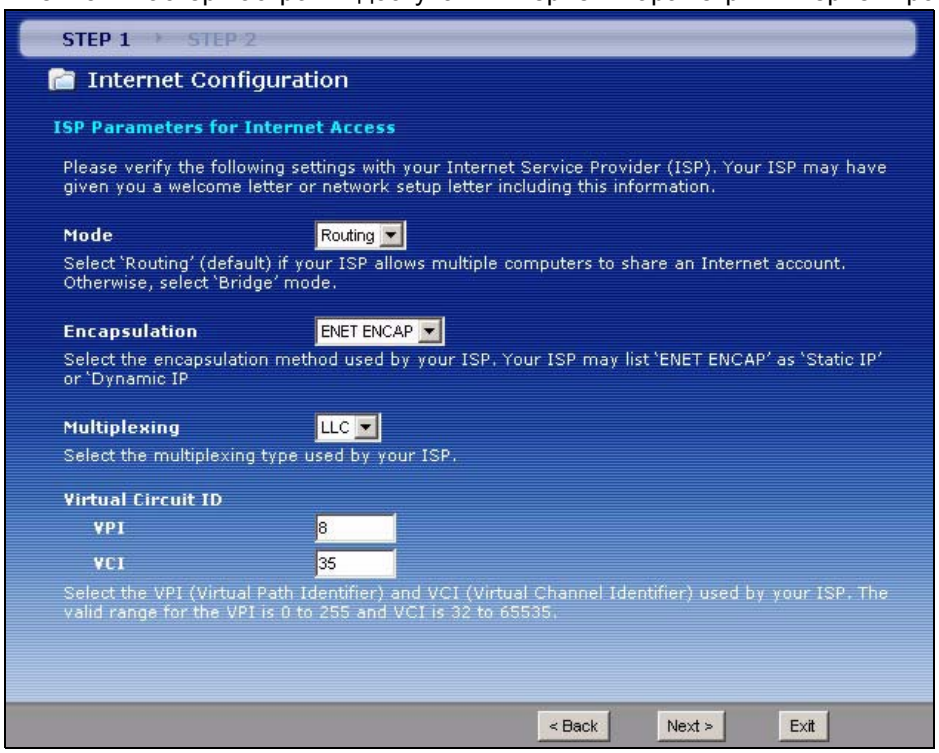
Рис. 24 Автоопределение: PPPoE



3.2.2 Ручная настройка

1 Если P660HWP не удалось определить тип соединения DSL, введите в окне Мастера информацию для доступа в Интернет, предоставленную вашим Интернет-провайдером. Если информация отсутствует, оставьте значения полей по умолчанию.

Рис. 25 Мастер настройки доступа в Интернет: Параметры Интернет-провайдера



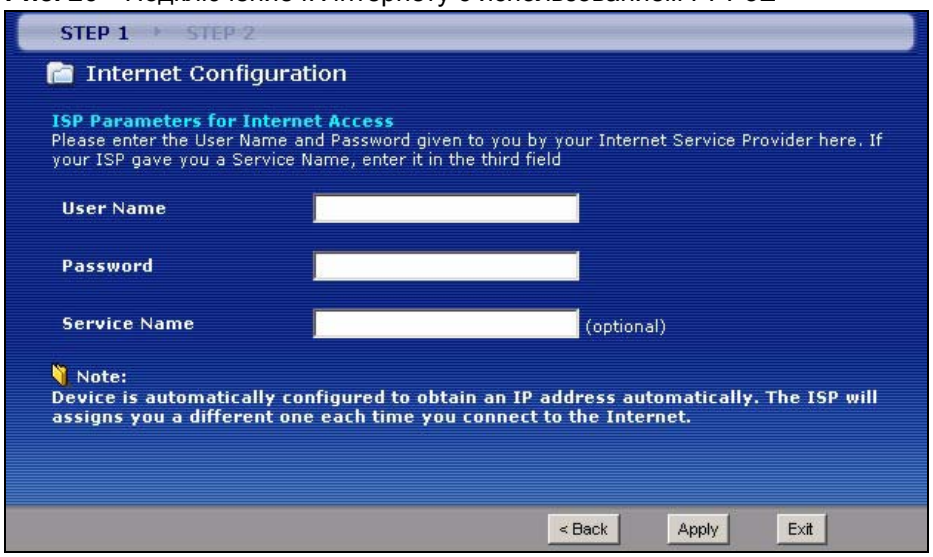
В следующей таблице даны описания полей этого окна.

Табл. 8 Мастер настройки доступа в Интернет: Параметры Интернет-провайдера

ПОЛЕ	ОПИСАНИЕ
Mode (Режим)	Из раскрывающегося списка поля **Mode (Режим)** выберите **Routing (Маршрутизация)** (установлено по умолчанию), если ваш Интернет-провайдер позволяет использовать одну учетную запись для подключения к Интернету нескольких компьютеров. В противном случае выберите **Bridge (Мост)**.
Encapsulation (Инкапсуляция)	Выберите тип инкапсуляции, который использует ваш Интернет-провайдер, из выпадающего списка поля **Encapsulation (Инкапсуляция)**. Опции в списке зависят от значения, установленного в поле **Mode (Режим)**. Если в поле **Mode (Режим)** установлено **Bridge (Мост)**, выберите **PPPoA** или **RFC 1483**. Если в поле **Mode (Режим)** установлено **Routing (Маршрутизация)**, выберите **PPPoA**, **RFC 1483**, **ENET ENCAP** или **PPPoE**.
Multiplex (Мультиплекси-рование)	Из раскрывающегося списка поля **Multiplex (Мультиплексирование)** выберите метод мультиплексирования, который использует ваш Интернет-провайдер: VC-based (на основе VC) или LLC-based (на основе LLC).
Virtual Circuit ID (Идентификатор виртуального канала)	VPI (Virtual Path Identifier – Идентификатор виртуального пути) и VCI (Virtual Channel Identifier – Идентификатор виртуального канала) определяют виртуальную линию передачи. Более подробную информацию см. в приложении.
VPI (Идентификатор виртуального пути)	Введите назначенный вам номер VPI. Это поле может быть уже заполнено.
VCI (Идентификатор виртуального канала)	Введите назначенный вам номер VCI. Это поле может быть уже заполнено.
Back (Назад)	Для возврата к предыдущему окну нажмите кнопку **Back (Назад)**.
Next (Далее)	Для перехода к следующему окну Мастера нажмите кнопку **Next (Далее)**. Вид следующего окна зависит от выбранного выше протокола.
Exit (Выход)	Щелкните по кнопке **Exit (Выход)**, чтобы закрыть окно Мастера без сохранения изменений.

2 Вид следующего окна Мастера установки зависит от выбранного режима и используемого типа инкапсуляции. Во всех представленных экранных окнах используется режим маршрутизации. Заполните поля и нажмите кнопку **Next (Далее)** для продолжения.

Рис. 26 Подключение к Интернету с использованием PPPoE

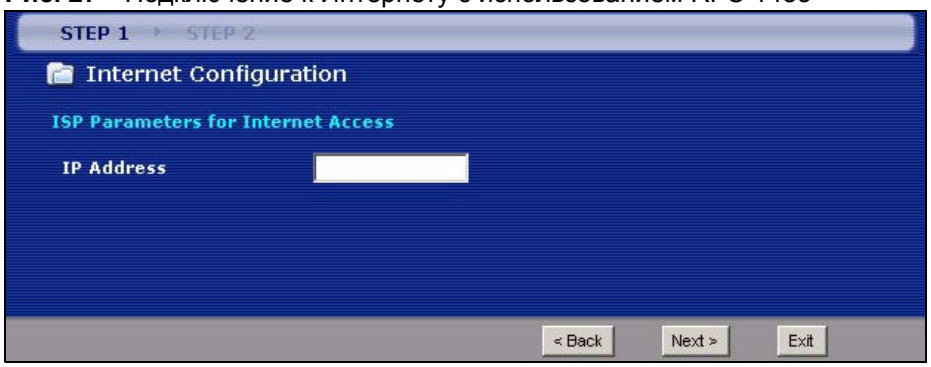


В следующей таблице даны описания полей этого окна.

Табл. 9 Подключение к Интернету с использованием PPPoE

ПОЛЕ	ОПИСАНИЕ
User Name (Имя пользователя)	Введите имя пользователя, предоставленное Интернет-провайдером. Если имя назначается в формате user@domain, где domain означает имя услуги, то вводите оба элемента имени в полном соответствии с данными от провайдера.
Password (Пароль)	Введите пароль для имени пользователя, указанного в предыдущем поле.
Service Name (Имя услуги)	Введите имя провайдера услуг PPPoE.
Back (Назад)	Нажмите кнопку **Back (Назад)** для возвращения к предыдущему окну Мастера установки.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек P660HWP.
Exit (Выход)	Щелкните по кнопке **Exit (Выход)**, чтобы закрыть окно Мастера без сохранения изменений.

Рис. 27 Подключение к Интернету с использованием RFC 1483

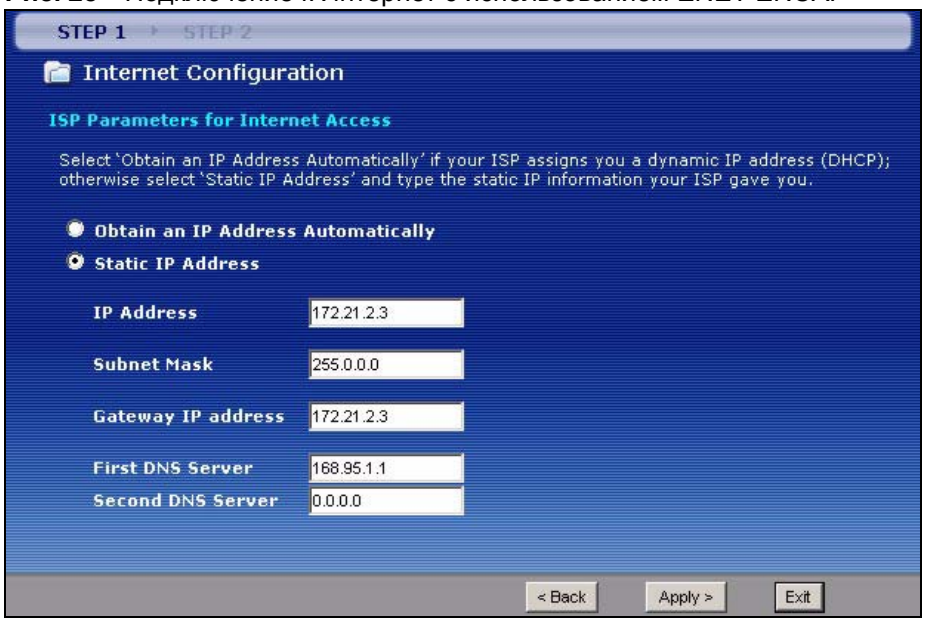


В следующей таблице даны описания полей этого окна.

Табл. 10 Подключение к Интернету с использованием RFC 1483

ПОЛЕ	ОПИСАНИЕ
IP Address (IP-адрес)	Это поле доступно, если в поле **Mode (Режим)** выбран режим **Routing (Маршрутизация)**. Введите в это поле IP-адрес, предоставленный Интернет-провайдером.
Back (Назад)	Нажмите кнопку **Back (Назад)** для возвращения к предыдущему окну Мастера установки.
Next (Далее)	Для перехода к следующему окну Мастера нажмите кнопку **Next (Далее)**.
Exit (Выход)	Щелкните по кнопке **Exit (Выход)**, чтобы закрыть окно Мастера без сохранения изменений.

Рис. 28 Подключение к Интернет с использованием ENET ENCAP

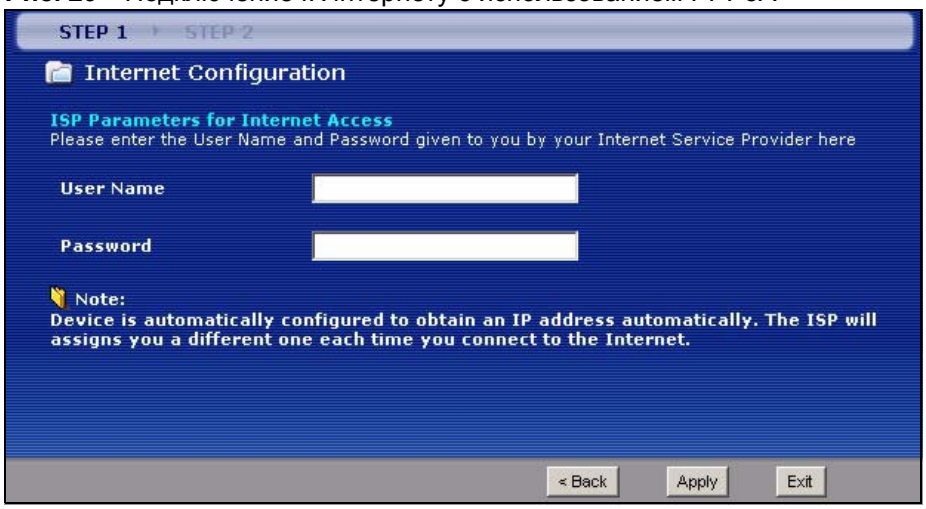


В следующей таблице даны описания полей этого окна.

Табл. 11 Подключение к Интернет с использованием ENET ENCAP

ПОЛЕ	ОПИСАНИЕ
Obtain an IP Address Automatically (Получать IP-адрес автоматически)	Статический IP-адрес – это фиксированный IP-адрес, предоставляемый Интернет-провайдером. Динамический IP-адрес не является фиксированным; Интернет-провайдер назначает вам новый адрес каждый раз, когда вы подключаетесь к Интернету. Если у вас динамический IP-адрес, выберите **Obtain an IP Address Automatically (Получать IP-адрес автоматически)**.
Static IP Address (Статический IP-адрес)	Если Интернет-провайдер назначил вам фиксированный IP-адрес, выберите **Static IP Address (Статический IP-адрес)**.
IP Address (IP-адрес)	Введите IP-адрес, назначенный вашим Интернет-провайдером.
Subnet Mask (Маска подсети)	Введите маску подсети в десятичном формате с разделительными точками. Информацию о расчете маски подсети при создании подсетей см. в приложениях.
Gateway IP Address (IP-адрес шлюза)	Необходимо указать IP-адрес шлюза (предоставленный вашим Интернет-провайдером), если в предыдущем окне в поле **Encapsulation (Инкапсуляция)** установлен тип инкапсуляции **ENET ENCAP**.
First DNS Server (Первый сервер DNS)	Введите IP-адреса серверов DNS. Адреса серверов DNS передаются клиентам DHCP вместе с IP-адресом и маской подсети.
Second DNS Server (Второй сервер DNS)	Аналогично предыдущей записи.
Back (Назад)	Нажмите кнопку **Back (Назад)** для возвращения к предыдущему окну Мастера установки.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек P660HWP.
Exit (Выход)	Щелкните по кнопке **Exit (Выход)**, чтобы закрыть окно Мастера без сохранения изменений.

Рис. 29 Подключение к Интернету с использованием PPPoA



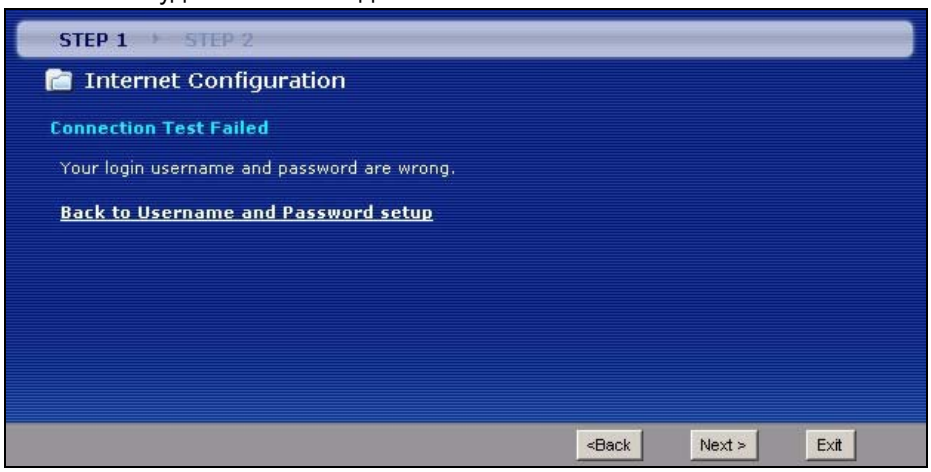
В следующей таблице даны описания полей этого окна.

Табл. 12 Подключение к Интернету с использованием PPPoA

ПОЛЕ	ОПИСАНИЕ
User Name (Имя пользователя)	Введите регистрационное имя, предоставленное Интернет-провайдером.
Password (Пароль)	Введите пароль для имени пользователя, указанного в предыдущем поле.
Back (Назад)	Нажмите кнопку **Back (Назад)** для возвращения к предыдущему окну Мастера установки.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек P660HWP.
Exit (Выход)	Щелкните по кнопке **Exit (Выход)**, чтобы закрыть окно Мастера без сохранения изменений.

- Если вы неправильно ввели имя пользователя и/или пароль для соединения PPPoE или PPPoA, появляется окно, показанное ниже. Нажмите **Back to Username and Password setup (Назад к установке имени пользователя и пароля)**, чтобы вернуться к окну, где можно внести изменения.

Рис. 30 Неудачный тест подключения 1



- Если появляется следующее окно, проверьте, активирована ли ваша учетная запись или нажмите **Restart the Internet/Wireless Setup Wizard (Повторный запуск Мастера установки Интернета / беспроводной сети)**, чтобы проверить параметры доступа в Интернет.

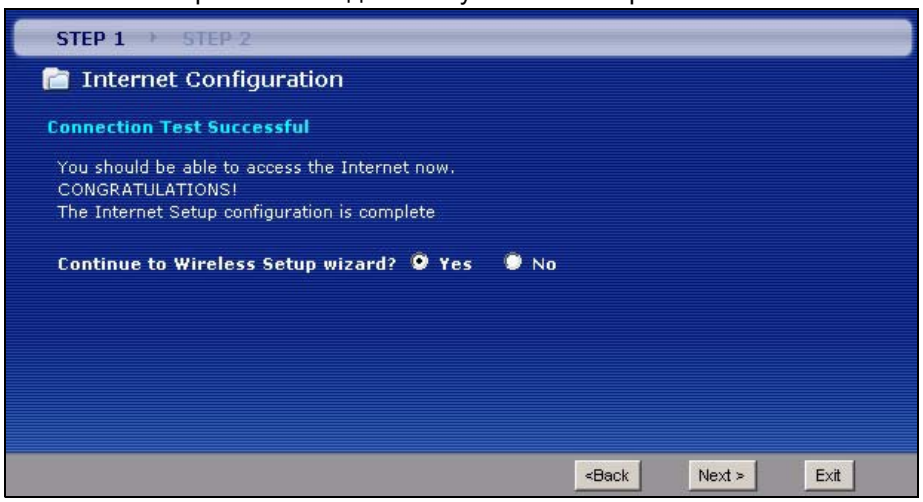
Рис. 31 Неудачный тест подключения 2

3.3 Мастер установки беспроводного подключения

После установки параметров доступа в Интернет, произведите настройку беспроводной локальной сети с помощью следующих окон. Информация, представленная в данном разделе, относится только к беспроводным моделям.

1 Для установки параметров беспроводной сети выберите **Yes (Да)** и щелкните **Next (Далее)**. В противном случае выберите **No (Нет)** и переходите к шагу 6.

Рис. 32 Тестирование соединения успешно завершено



2 Это окно используется для включения функций беспроводной локальной сети и OTIST. Щелкните **Next (Далее)** для продолжения.

Рис. 33 Мастер установки беспроводной локальной сети 1

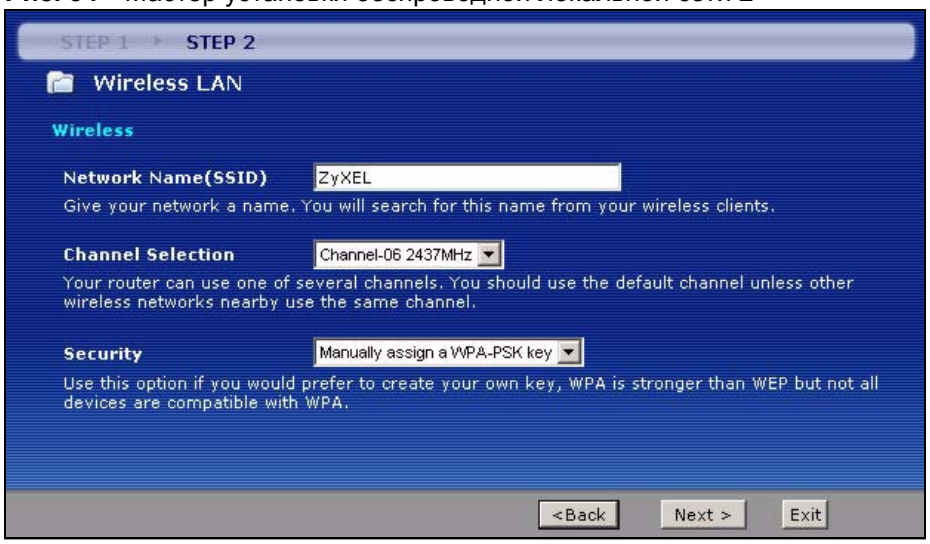
В следующей таблице даны описания полей этого окна.

Табл. 13 Мастер установки беспроводной локальной сети 1

ПОЛЕ	ОПИСАНИЕ
Active (Активировать)	Поставьте флажок, чтобы активировать беспроводную локальную сеть.
Enable OTIST (Включить OTIST)	Поставьте флажок, чтобы включить OTIST, если требуется передавать идентификатор SSID P660HWP и параметры безопасности WPA-PSK беспроводным клиентам, которые поддерживают OTIST и находятся в зоне охвата сети. Одновременно необходимо активировать и запустить OTIST на компьютерах беспроводных клиентов. Для выполнения процедуры потребуется около трех минут. **Примечание:** Включайте OTIST, только если беспроводные клиенты поддерживают WPA и OTIST.
Setup Key (Установочный ключ)	Введите **установочный ключ** OTIST длиной до 8 латинских символов. Убедитесь, что в P660HWP и компьютерах беспроводных клиентов используется один и тот же **установочный ключ**.
Back (Назад)	Для возврата в предыдущее окно нажмите **Back (Назад)**.
Next (Далее)	Нажмите **Next (Далее)** для перехода к следующему экрану.
Exit (Выход)	Нажмите кнопку **Exit (Выход)**, чтобы закрыть окно Мастера без сохранения изменений.

3 Установите параметры беспроводной сети в этом окне. Нажмите кнопку **Next (Далее)**.

Рис. 34 Мастер установки беспроводной локальной сети 2



В следующей таблице даны описания полей этого окна.

Табл. 14 Мастер установки беспроводной локальной сети 2

ПОЛЕ	ОПИСАНИЕ
Network Name (SSID) (Имя сети (SSID))	Введите описательное имя для беспроводной локальной сети (не более 32 семиразрядных печатных латинских символов). При изменении значения этого поля в P660HWP, убедитесь, что на всех беспроводных станциях используется такой же идентификатор SSID, что необходимо для обеспечения доступа в сеть.
Channel Selection (Выбор канала)	Диапазон радиочастот, используемый беспроводными устройствами IEEE 802.11b/g, называется каналом. Выберите идентификатор канала, который не используется соседним устройством.
Security (Безопасность)	Выберите **Automatically assign a WPA key (Recommended) (Автоматически назначить ключ WPA (Рекомендуется))**, чтобы P660HWP автоматически генерировал общий ключ (WPA-PSK) при условии, что беспроводные клиенты поддерживают WPA и OTIST. Это поле доступно, только если в предыдущем окне мастера была включена функция OTIST. Выберите **Manually assign a WPA-PSK key (Назначить ключ WPA-PSK вручную)**, чтобы ввести общий ключ (WPA-PSK). Устанавливайте этот параметр, только если беспроводные клиенты поддерживают WPA. Более подробную информацию см. Разд. 3.3.1 на с. 72. Выберите **Manually assign a WEP key (Назначить ключ WEP вручную)**, чтобы ввести ключ WEP. Более подробную информацию см. Разд. 3.3.2 на с. 73. Выберите **Disable wireless security (Отключить защиту беспроводной сети)** для отключения защиты беспроводной сети. В этом случае сеть будет доступна для любого беспроводного сетевого устройства, находящегося в зоне охвата сети. **Примечание:** Если функция OTIST в предыдущем окне мастера была включена, а в этом окне установлено **Disable wireless security (Отключить защиту беспроводной сети)**, P660HWP все равно будет автоматически генерировать общий ключ (WPA-PSK). Если функция OTIST включена и выбран параметр **Manually assign a WEP key (Назначить ключ WEP вручную)**, P660HWP будет заменять ключ WEP ключом WPA-PSK.

Табл. 14 Мастер установки беспроводной локальной сети 2

ПОЛЕ	ОПИСАНИЕ
Back (Назад)	Для возврата в предыдущее окно нажмите **Back (Назад)**.
Next (Далее)	Нажмите **Next (Далее)** для перехода к следующему экрану.
Exit (Выход)	Нажмите кнопку **Exit (Выход)**, чтобы закрыть окно Мастера без сохранения изменений.

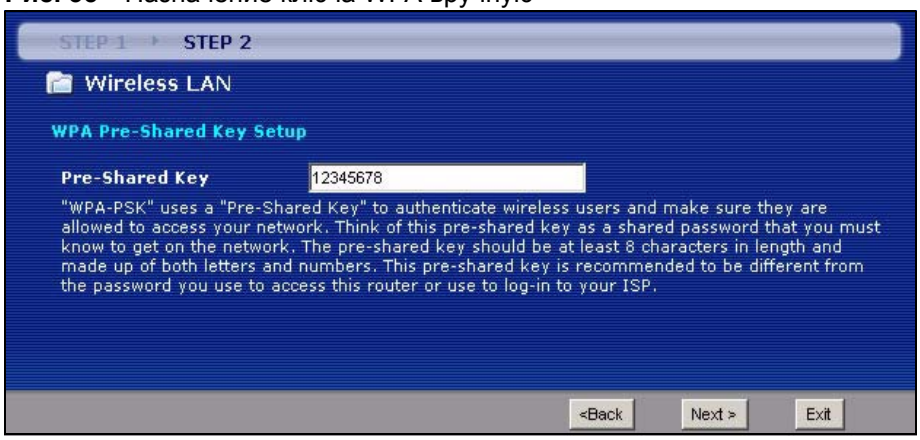
Для обеспечения беспроводного доступа беспроводные станции и P660HWP должны использовать одинаковые идентификаторы SSID, идентификатор канала и ключ шифрования WEP (если включено шифрование WEP) или WPA-PSK (если включено шифрование WPA-PSK).

4 Вид этого окна меняется в зависимости от режима безопасности, установленного в предыдущем окне. Заполните поле (если оно доступно) и щелкните **Next (Далее)**.

3.3.1 Назначение ключа WPA-PSK вручную

В окне настройки беспроводной сети выберите **Manually assign a WPA-PSK key (Назначить ключ WPA-PSK вручную)** для ввода **общего ключа**.

Рис. 35 Назначение ключа WPA вручную



В следующей таблице даны описания полей этого окна.

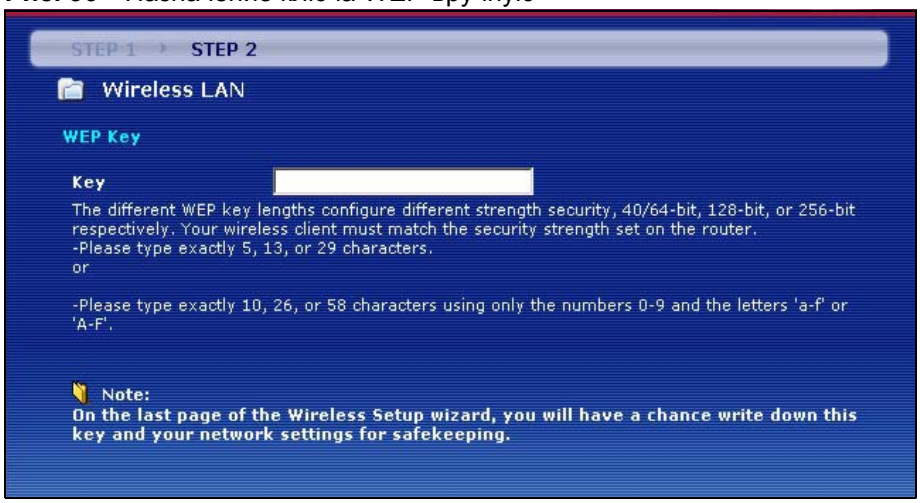
Табл. 15 Назначение ключа WPA вручную

ПОЛЕ	ОПИСАНИЕ
Pre-Shared Key (Общий ключ)	Введите от 8 до 63 латинских символов с учетом регистра. Настройкой WPA в окнах конфигурации беспроводной сети обеспечивается наиболее безопасное беспроводное подключение. Для этого необходимо настроить сервер аутентификации.
Back (Назад)	Для возврата в предыдущее окно нажмите **Back (Назад)**.
Next (Далее)	Нажмите **Next (Далее)** для перехода к следующему экрану.
Exit (Выход)	Нажмите кнопку **Exit (Выход)**, чтобы закрыть окно Мастера без сохранения изменений.

3.3.2 Назначение ключа WEP вручную

Для установки параметров шифрования WEP выберите **Manually assign a WEP key (Назначить ключ WEP вручную)**.

Рис. 36 Назначение ключа WEP вручную



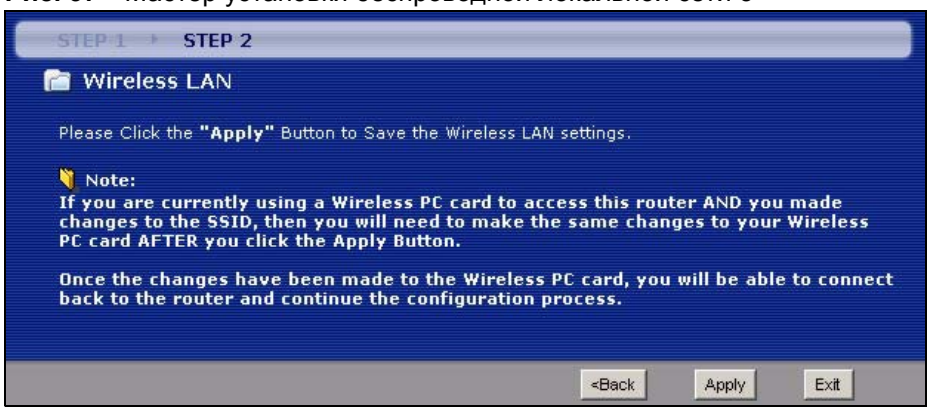
В следующей таблице даны описания полей этого окна.

Табл. 16 Назначение ключа WEP вручную

ПОЛЕ	ОПИСАНИЕ
Key (Ключ)	Ключи WEP используются для шифрования данных. Для обеспечения передачи данных необходимо, чтобы P660HWP и все беспроводные станции использовали одинаковый ключ WEP. Введите любые 5, 13 или 29 символов ASCII или 10, 26 или 58 шестнадцатеричных символов («0-9», «A-F») для установки ключа WEP длиной 64 бита, 128 бит или 256 бит соответственно.
Back (Назад)	Для возврата в предыдущее окно нажмите **Back (Назад)**.
Next (Далее)	Нажмите **Next (Далее)** для перехода к следующему экрану.
Exit (Выход)	Нажмите кнопку **Exit (Выход)**, чтобы закрыть окно Мастера без сохранения изменений.

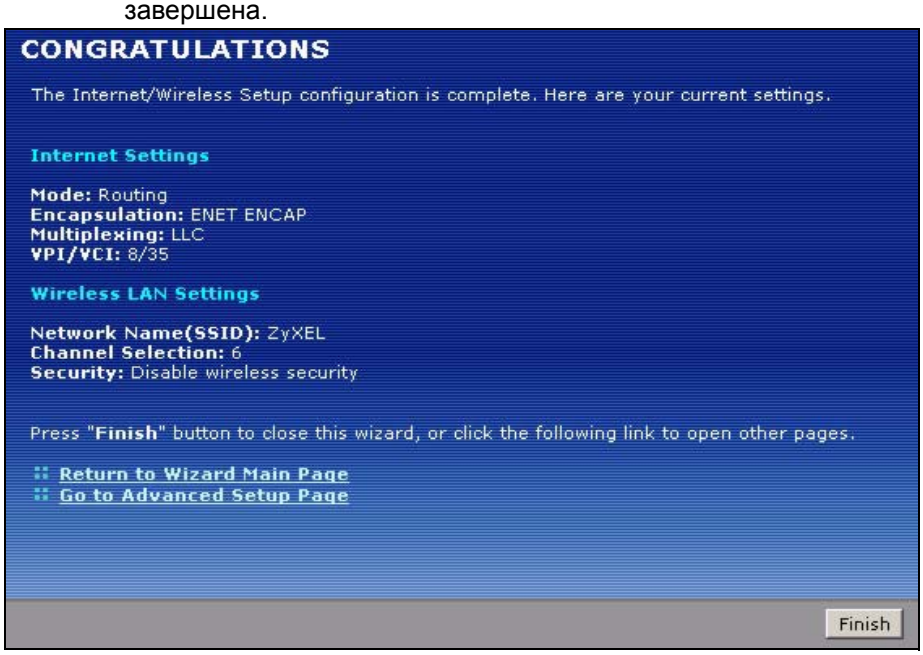
5 Щелкните **Apply (Применить)** для сохранения настроек беспроводной локальной сети.

Рис. 37 Мастер установки беспроводной локальной сети 3



6 Появится сводная таблица, доступная только для чтения, при помощи которой можно проверить правильность установленных параметров. Нажмите кнопку **Finish (Готово)** для завершения работы Мастера установки и сохранения настроек.

Рис. 38 Работа Мастера установкидоступа в Интернет и беспроводного подключения завершена.



7 Запустите Web-браузер и перейдите на сайт www.zyxel.ru. Обеспечение доступа в Интернет – это всего лишь одна из возможностей устройства. Обратитесь к другим разделам данного руководства за подробной информацией обо всех функциях и возможностях P660HWP. Если вы не можете получить доступ в Интернет, снова откройте Web-конфигуратор и проверьте правильность заданных настроек.

4

Мастер управления пропускной способностью

В этой главе рассказывается, как настроить управление пропускной способностью с помощью Мастера.

4.1 Введение

Управление пропускной способностью позволяет управлять скоростью трафика через порт WAN P660HWP и назначать приоритеты для распределения пропускной способности в соответствии с требованиями приложений. Это предотвращает использование одной службой всей доступной пропускной способности и блокирование других пользователей.

4.2 Предварительно определенные службы управления пропускной способностью

Далее приводится описание служб, к которым можно применять управление пропускной способностью с помощью Мастера установки.

Табл. 17 Настройка управления пропускной способностью: Службы

СЛУЖБА	ОПИСАНИЕ
WWW	Всемирная паутина (World Wide Web – WWW) – это система в Интернете, предназначенная для распространения графической и текстовой информации, связанной ссылками, на основе протокола передачи гипертекста (Hyper Text Transfer Protocol – HTTP). HTTP – это протокол типа клиент/сервер, разработанный для WWW. Система Web не является синонимом Интернет; точнее, она является одним из сервисов Интернета. Другими сервисами Интернета являются Интернет-чаты (глобальная система, посредством которой пользователи могут общаться друг с другом в реальном времени) и новостные группы (сетевая служба, рассылающая информацию по определенной теме). К службе Web можно подключиться с помощью браузера.
FTP	Протокол передачи файлов (FTP) позволяет осуществлять быструю передачу файлов, в том числе файлов большого размера, которые невозможно пересылать с помощью электронной почты. Служба FTP использует порт 21.

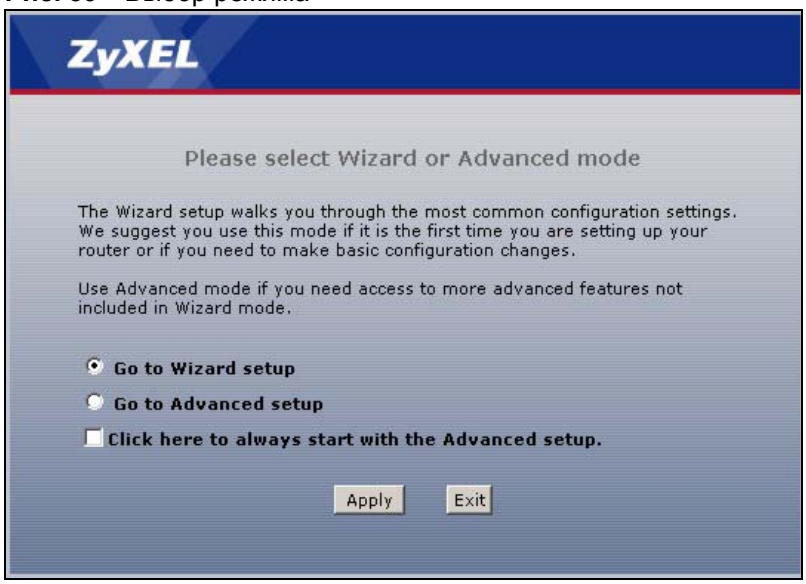
Табл. 17 Настройка управления пропускной способностью: Службы

СЛУЖБА	ОПИСАНИЕ
E-Mail	Электронная почта позволяет передавать сообщения по компьютерной сети конкретному пользователю или группе пользователей. Существует несколько портов, используемых по умолчанию для электронной почты: POP3 – порт 110 IMAP – порт 143 SMTP – порт 25 HTTP – порт 80
Telnet	Telnet – протокол регистрации и эмуляции терминала, общий для среды Интернет и UNIX. Он работает в сетях TCP/IP. Его главная функция заключается в обеспечении регистрации пользователей на удаленных узлах. Telnet использует порт TCP номер 23.
NetMeeting (H.323)	Программное обеспечение Microsoft для обмена данными между мультимедийными приложениями, которое позволяет группам пользователей проводить телеконференции и видеоконференции по сети Интернет. NetMeeting поддерживает протокол VoIP, обмен текстовыми сообщениями в реальном времени, электронные «доски», передачу файлов и совместное использование приложений. NetMeeting использует протокол H.323. H.323 – стандартный протокол для телеконференций, обеспечивающий конференц-связь с обменом аудио, видео и обычными данными. Позволяет осуществлять связь в реальном времени между двумя и несколькими клиентскими компьютерами в сети с пакетным обменом, не гарантирующей качества обслуживания. H.323 в основном передается поверх протокола TCP с использованием порта 1720 по умолчанию.
VoIP (SIP)	Передача речи по Интернет называется Voice over IP или VoIP. Протокол инициирования сеанса связи (Session Initiated Protocol – SIP) является общепризнанным стандартом для обеспечения VoIP. SIP является протоколом уровня приложения (сигнальный протокол), который обеспечивает установку, проведение и завершение голосовых и мультимедиа сеансов связи по Интернет. SIP передается в основном по UDP (Протокол передачи дейтаграмм пользователя), но может передаваться также по TCP с использованием номера порта по умолчанию 5060.
VoIP (H.323)	Передача речи по Интернет называется Voice over IP или VoIP. H.323 – стандартный протокол для телеконференций, обеспечивающий конференц-связь с обменом аудио, видео и обычными данными. Позволяет осуществлять связь в реальном времени между двумя и несколькими клиентскими компьютерами в сети с пакетным обменом, не гарантирующей качества обслуживания. H.323 в основном передается поверх протокола TCP с использованием порта 1720 по умолчанию.
TFTP	Trivial File Transfer Protocol (Упрощенный протокол передачи файлов) – это протокол передачи файлов в Интернет, подобный FTP, но использующий UDP (Протокол передачи дейтаграмм пользователя), а не TCP (Протокол управления передачей).

4.3 Мастер управления пропускной способностью

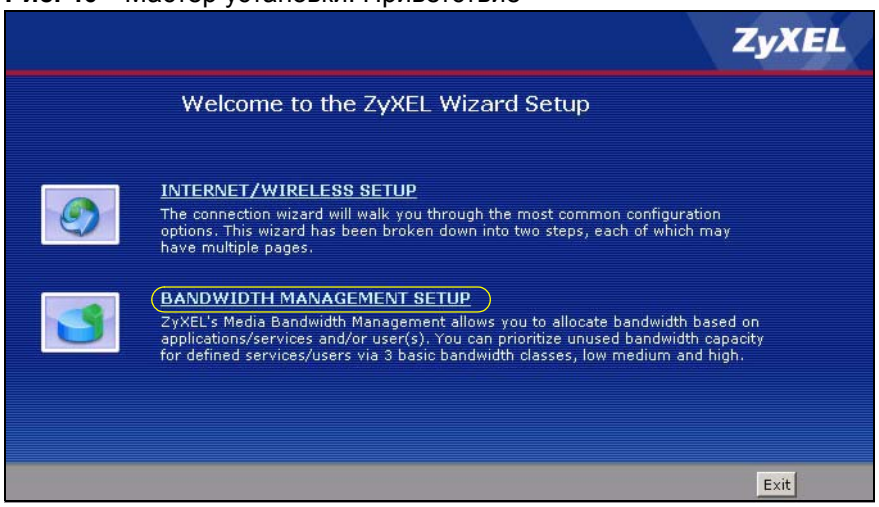
1 После ввода пароля администратора и получения доступа к Web-конфигуратору, выберите **Go to Wizard setup (Запуск мастера установки)** и щелкните **Apply (Применить)**. Также для отображения главного окна Мастера установки можно щелкнуть по иконке Мастера установки () в верхнем правом углу Web-конфигуратора.

Рис. 39 Выбор режима



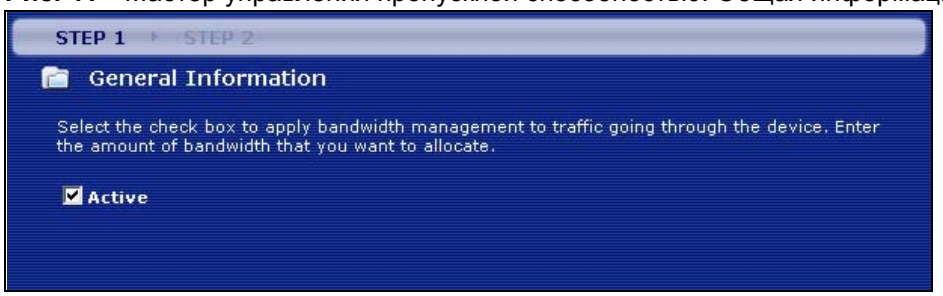
2 Щелкните **BANDWIDTH MANAGEMENT SETUP (НАСТРОЙКА УПРАВЛЕНИЯ ПРОПУСКНОЙ СПОСОБНОСТЬЮ)**, чтобы настроить доступ в Интернет.

Рис. 40 Мастер установки: Приветствие



3 Включите управление пропускной способностью и установите параметры пропускной способности для пакетов различных приложений.

Рис. 41 Мастер управления пропускной способностью: Общая информация



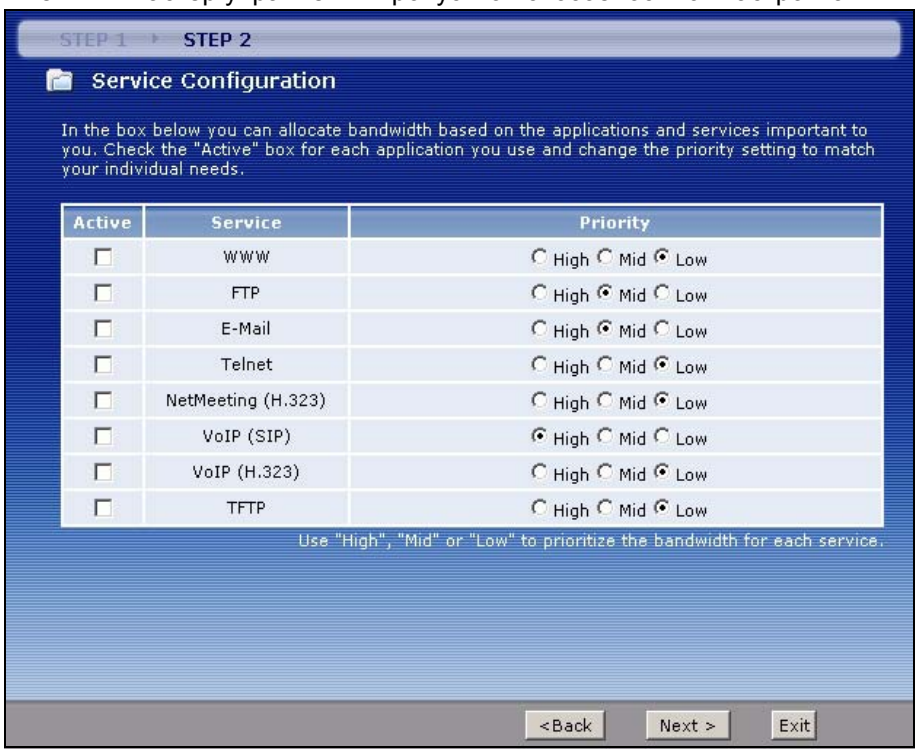
В следующей таблице даны описания полей этого окна.

Табл. 18 Мастер управления пропускной способностью: Общая информация

ПОЛЕ	ОПИСАНИЕ
Active (Активировать)	Установите флажок в поле **Active (Активировать)**, чтобы P660HWP применял управление пропускной способностью к исходящему трафику порта(ов) P660HWP. Выберите **Services Setup (Настройка служб)** для распределения пропускной способности на основе требований, предъявляемых приложениями.
Back (Назад)	Для возврата в предыдущее окно нажмите **Back (Назад)**.
Next (Далее)	Нажмите **Next (Далее)** для перехода к следующему экрану.
Exit (Выход)	Нажмите кнопку **Exit (Выход)**, чтобы закрыть окно Мастера без сохранения изменений.

4 Во втором окне Мастера выберите службы, к которым нужно применить управление пропускной способностью, а также установите приоритет для каждой службы.

Рис. 42 Мастер управления пропускной способностью: Настройка



В следующей таблице даны описания полей этого окна.

Табл. 19 Мастер управления пропускной способностью: Настройка

ПОЛЕ	ОПИСАНИЕ
Active (Активировать)	Поставьте флажок в поле **Active (Активировать)**, чтобы включить управление пропускной способностью для службы или приложения.
Service (Служба)	В этом поле отображается имя службы.

Табл. 19 Мастер управления пропускной способностью: Настройка

ПОЛЕ	ОПИСАНИЕ
Priority (Приоритет)	Установите для каждой службы приоритет **High (Высокий)**, **Mid (Средний)** или **Low (Низкий)**, чтобы P660HWP передавал трафик этой службы в соответствии с ее приоритетом. Службе с приоритетом **High (Высокий)** предоставляется полностью требуемая ей пропускная способность. Если несколько приложений имеет одинаковый приоритет, то пропускная способность делится поровну между этими службами. Приложениям, для которых не установлено управление пропускной способностью, ресурсы предоставляются после удовлетворения требований приоритетных приложений. Если правила, установленные с помощью этого Мастера, изменяются в окне **Advanced (Дополнительно)** > **Bandwidth MGMT (Управление пропускной способностью)** > **Rule Setup (Установка правил)**, то переключатель приоритета службы будет установлен в положение **User Configured (Установлен пользователем)**. В окне **Advanced (Дополнительно)** > **Bandwidth MGMT (Управление пропускной способностью)** > **Rule Setup (Установка правил)** можно редактировать правила.
Back (Назад)	Нажмите кнопку **Back (Назад)** для возвращения к предыдущему окну Мастера установки.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек P660HWP.
Exit (Выход)	Щелкните по кнопке **Exit (Выход)**, чтобы закрыть окно Мастера без сохранения изменений.

5 Следуйте инструкциям на экране и затем нажмите кнопку **Finish (Готово)** для завершения работы Мастера установки и сохранения конфигурации.

Рис. 43 Мастер управления пропускной способностью: Готово

Часть III
Сеть

5

Настройка глобальной сети

В этой главе описывается настройка глобальной сети.

5.1 Общая информация о глобальной сети

WAN (Wide Area Network – Глобальная вычислительная сеть) формируется при наличии подключения к другой сети или к сети Интернет.

5.1.1 Инкапсуляция

Убедитесь, что используется метод инкапсуляции, предписанный Вашим Интернет-провайдером. Ниже перечислены методы инкапсуляции, поддерживаемые P660HWP.

5.1.1.1 Инкапсуляция ENET ENCAP

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

5.1.1.2 Протокол «точка-точка» поверх Ethernet (PPPoE)

PPPoE (Point-to-Point Protocol over Ethernet – Протокол «точка-точка» поверх Ethernet) обеспечивает контроль доступа и учет соединений аналогично коммутируемым линиям связи, использующим PPP. PPPoE – это стандарт IETF (RFC 2516), определяющий, как персональный компьютер (ПК) взаимодействует с широкополосным модемным соединением (DSL, кабель и т.д.).

Для провайдера услуг протокол PPPoE обеспечивает метод доступа и аутентификации, который работает с существующими системами управления доступом (например, RADIUS).

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

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

Так как PPPoE реализован непосредственно в P660HWP (а не на отдельных компьютерах), установка программного обеспечения PPPoE на компьютерах локальной сети не требуется, поскольку эта процедура полностью выполняется интернет-центром P660HWP. Кроме того, при включении функции NAT доступ будут иметь все компьютеры локальной сети.

5.1.1.3 Протокол «точка-точка» поверх ATM (PPPoA)

PPPoA означает Point to Point Protocol over ATM Adaptation Layer 5 (AAL5) (Протокол «точка-точка» поверх адаптации ATM, уровень 5). Соединение PPPoA функционирует подобно коммутируемому подключению к Интернет. P660HWP инкапсулирует сеанс связи PPP на базе RFC1483 и передает его через постоянный виртуальный канал ATM (Permanent Virtual Circuit) на концентратор DSLAM (цифровой мультиплексор доступа) Интернет-провайдера. Для получения дополнительной информации по PPPoA см. комментарий RFC 2364. Информацию по PPP см. в комментарии RFC 1661.

5.1.1.4 RFC 1483

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

5.1.2 Мультиплексирование

Определить, какие протоколы используются для передачи по виртуальному каналу (VC), можно двумя способами. Убедитесь, что вы используете метод мультиплексирования, который поддерживает ваш Интернет-провайдер.

5.1.2.1 Мультиплексирование на базе VC

По предварительному взаимному соглашению за каждым протоколом закрепляется конкретный виртуальный канал, например, VC1 передает IP и т. д. Мультиплексирование на базе VC может быть основным методом в сетевых конфигурациях, где динамическое создание большого количества виртуальных каналов ATM является быстрым и экономичным.

5.1.2.2 Мультиплексирование на базе LLC

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

5.1.3 Сценарии инкапсуляции и мультиплексирования

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

5.1.3.1 Сценарий 1: Один виртуальный канал, множество протоколов

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

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

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

5.1.3.3 Сценарий 3: Несколько виртуальных каналов

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

5.1.4 VPI и VCI

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

5.1.5 Назначение IP-адреса

Статический IP-адрес – это фиксированный IP-адрес, предоставляемый Интернет-провайдером. Динамический IP-адрес не фиксирован. Интернет-провайдер каждый раз назначает новый IP-адрес. Функция учетной записи одиночного пользователя может быть включена или отключена, если вы имеете динамический или статический IP-адрес. Тем не менее, на выбор IP-адреса и шлюза ENET ENCAP влияет назначенный способ инкапсуляции.

5.1.5.1 Назначение IP с инкапсуляцией PPPoA или PPPoE

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

5.1.5.2 Назначение IP с инкапсуляцией RFC 1483

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

5.1.5.3 Назначение IP с инкапсуляцией ENET ENCAP

В этом случае может назначаться как статический, так и динамический IP. Для статического IP-адреса необходимо заполнить оба поля **IP Address (IP-адрес)** и **ENET ENCAP Gateway (Шлюз ENET ENCAP)** в соответствии с параметрами, предоставленными вашим Интернет-провайдером. Однако при назначении динамического IP-адреса P660HWP функционирует как клиент DHCP через WAN-порт и, следовательно, поля **IP Address (IP-адрес)** и **ENET ENCAP Gateway (Шлюз ENET ENCAP)** являются недоступными (N/A), так как эти параметры для P660HWP назначает сервер DHCP.

5.1.6 Постоянное соединение (PPP)

Постоянное соединение – это коммутируемая линия с постоянно установленным соединением независимо от необходимости передачи трафика. P660HWP при постоянном соединении выполняет два действия: во-первых, выключает тайм-аут простоя; во-вторых, P660HWP пытается восстановить соединение при включении питания, а также при разрыве соединения. По очевидным причинам постоянное соединение может быть очень дорогим.

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

5.1.7 Трансляция сетевых адресов (NAT)

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

5.2 Метрика

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

Метрика устанавливает приоритет для маршрутов трафика P660HWP в Интернете. Если два маршрута по умолчанию имеют одинаковую метрику, P660HWP использует следующие заданные приоритеты:

- Стандартный маршрут: назначается Интернет-провайдером (см. Разд. 5.5 на с. 89)
- Маршрут перенаправления трафика (см. Разд. 5.7 на с. 100)
- Резервный маршрут WAN, называемый также резервным коммутируемым подключением (см. Разд. 5.8 на с. 101)

Например, если стандартный маршрут имеет метрику «1», маршрут перенаправления трафика имеет метрику «2», а резервный маршрут имеет метрику «3», то стандартный маршрут используется как основной маршрут по умолчанию. Если по стандартному маршруту не удается подключиться к Интернету, P660HWP пытается использовать маршрут перенаправления трафика. Аналогично, P660HWP использует резервный маршрут, если маршрут переадресации трафика тоже не работает.

Если вы хотите, чтобы резервный маршрут имел приоритет над маршрутом перенаправления трафика или даже над стандартным маршрутом, то необходимо для резервного маршрута установить метрику «1», а для других маршрутов – «2» (или выше).

Политика маршрутизации IP замещает схему маршрутизации по умолчанию и имеет приоритет над всеми маршрутами, описанными выше.

5.3 Формирование трафика

Функция формирования трафика представляет собой соглашение между владельцем сети и абонентом, предназначенное для регулировки средней скорости и колебаний скорости передачи данных через сеть ATM. Такое соглашение помогает устранить перегрузку сети, что важно для передачи данных в реальном времени, таких как аудио- и видеоданные.

PCR (Peak Cell Rate – Пиковая скорость ячеек) – это максимальная скорость, с которой отправитель может передавать ячейки. Данный параметр может быть ниже (но не выше), чем максимальная скорость передачи в линии. Размер одной ячейки ATM составляет 53 байта (424 бита), таким образом при максимальной скорости передачи данных в 832 кбит/с максимальная скорость передачи ячеек PCR будет 1962 ячеек/с. Однако эта скорость не гарантирована, потому что она зависит от скорости передачи линии.

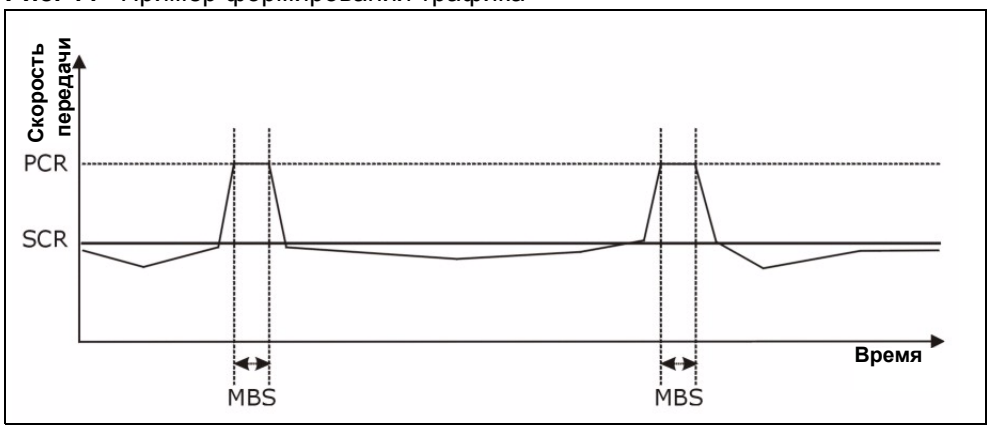
SCR (Sustained Cell Rate – Поддерживаемая скорость ячеек) – это средняя скорость ячеек каждого источника пульсирующего трафика. Она определяет максимальную среднюю скорость, с которой ячейки могут передаваться по виртуальному соединению. Значение SCR не может быть больше, чем PCR.

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

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

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

Рис. 44 Пример формирования трафика



5.3.1 Классы трафика ATM

Существуют основные классы трафика ATM, определяемые в «Спецификации управления трафиком 4.0» в составе Форума ATM.

5.3.1.1 Постоянная скорость передачи (CBR)

Постоянная скорость передачи (CBR) обеспечивает фиксированную пропускную способность, которая всегда доступна, даже если не производится передача данных. Как правило, трафик CBR является чувствительным ко времени (задержка не допускается). CBR используется в соединениях, где постоянно требуется определенная величина пропускной способности. Скорость PCR является заданной, и если скорость трафика превышает эту скорость, ячейки могут отбрасываться. Примерами соединений CBR являются передача речи и видеосигнала с высоким разрешением.

5.3.1.2 Переменная скорость передачи (VBR)

Класс VBR (Variable Bit Rate – Переменная скорость передачи) ATM используется в соединениях с пульсирующим трафиком. Соединения, где используется трафик VBR, могут группироваться в соединения реального времени VBR-RT (real time VBR) или соединения вне реального времени VBR-nRT (non-real time VBR).

Тип трафика VBR-RT (real-time Variable Bit Rate – Переменная скорость передачи в реальном времени) используется для передачи пульсирующего трафика, который требует тщательного контроля задержки и изменений задержки. Здесь также обеспечивается фиксированная пропускная способность (скорость PCR является заданной), но она доступна, только когда производится передача данных. Примером соединения VBR-RT является проведение видеоконференций. Для организации видеоконференций требуется передача данных в реальном времени и предоставление полосы пропускания, меняющейся в зависимости от динамики изменения видеоизображений.

Тип трафика VBR-nRT (non real-time Variable Bit Rate – Переменная скорость передачи вне реального времени) используется для передачи пульсирующего трафика, который не требует тщательного контроля задержки и изменений задержки. Такой тип трафика используется для пульсирующего трафика, типичного для локальных сетей. Скорость PCR и максимальный размер пакета MBS определяют размеры блоков пакетов, SCR определяет минимальный размер блока. Примером соединения VBR-nRT является передача файлов данных, которая не чувствительна к задержкам.

5.3.1.3 Неопределенная скорость передачи (UBR)

Тип трафика UBR ATM (Unspecified Bit Rate – Неопределенная скорость передачи) используется для пакетной передачи данных. Но при использовании UBR не гарантируется величина пропускной способности, и трафик передается, только когда сеть имеет ресурсы. Примером применения UBR является фоновая передача файлов.

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

При включении питания и подключении P660HWP к телефонной розетке, интернет-центр автоматически определяет настройки подключения к Интернету (такие как номера VCI/VPI и метод инкапсуляции), используемые Интернет-провайдером, и производит необходимые изменения в конфигурации. В случаях, когда требуются дополнительные учетные данные для подключения к Интернет (такие как имя и пароль учетной записи пользователя Интернет) или P660HWP не может подключиться к Интернет-провайдеру, на экране появляется окно (окна) для ввода информации или для поиска и устранения неисправностей.

Автоматическая настройка отключается, если:

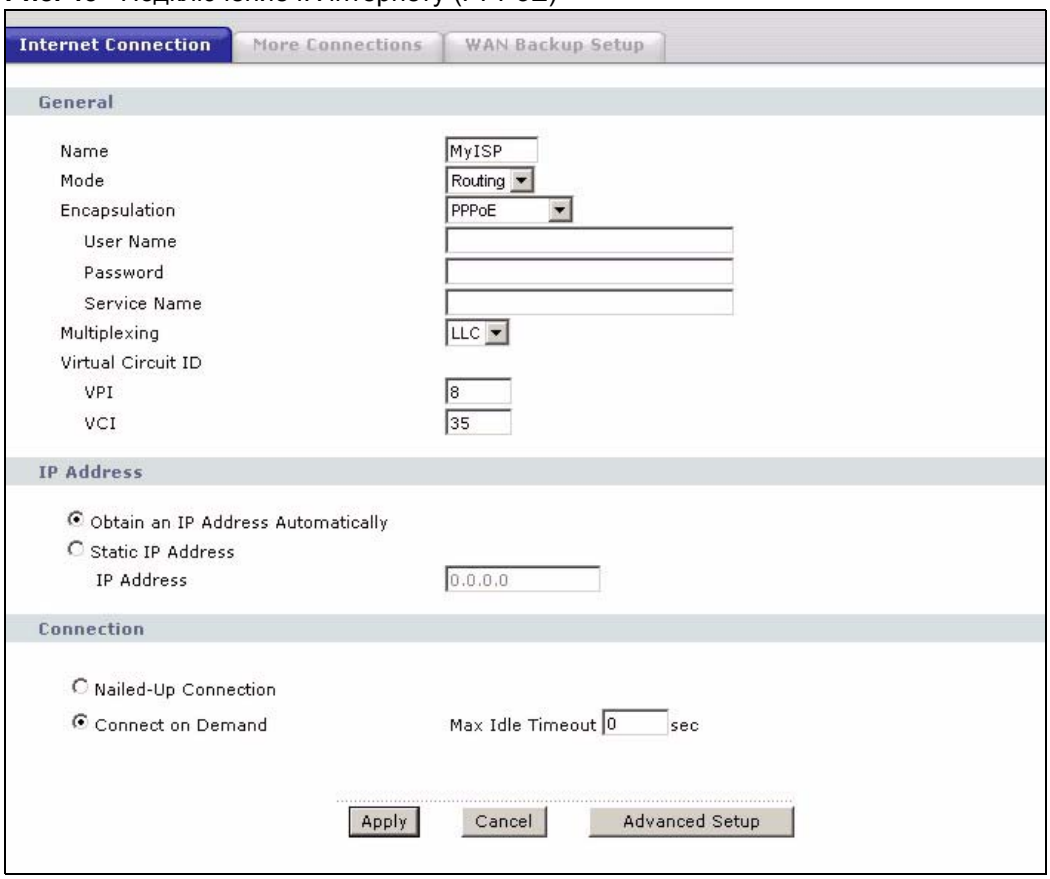
- P660HWP работает в режиме межсетевого моста
- P660HWP установлен в режим использования статического (фиксированного) IP-адреса глобальной сети.

5.5 Подключение к сети Интернет

Для изменения параметров доступа в Интернет порта WAN интернет-центра P660HWP щелкните **Network (Сеть) > WAN (Глобальная сеть)**. Появится окно, вид которого зависит от типа инкапсуляции.

Более подробную информацию см. Разд. 5.1 на с. 83.

Рис. 45 Подключение к Интернету (PPPoE)



В следующей таблице даны описания полей этого окна.

Табл. 20 Подключение к сети Интернет

ПОЛЕ	ОПИСАНИЕ
General (Общие)	
Name (Имя)	Введите имя Интернет-провайдера, например, MyISP. Эта информация используется только в целях идентификации.
Mode (Режим)	Из раскрывающегося списка поля **Mode (Режим)** выберите **Routing (Маршрутизация)** (установлено по умолчанию), если ваш Интернет-провайдер позволяет использовать одни учетные данные для подключения к Интернету нескольких компьютеров. В противном случае выберите **Bridge (Мост)**.
Encapsulation (Инкапсуляция)	Из выпадающего списка выберите метод инкапсуляции, используемый Интернет-провайдером. Варианты в списке зависят от режима, установленного в поле **Mode (Режим)**. Если в поле **Mode (Режим)** установлено **Bridge (Мост)**, то выберите **PPPoA** или **RFC 1483**. Если в поле **Mode (Режим)** установлено **Routing (Маршрутизация)**, то выберите **PPPoA**, **RFC 1483**, **ENET ENCAP** или **PPPoE**.
User Name (Имя пользователя)	Введите имя пользователя, назначенное вашим Интернет-провайдером (только для инкапсуляции PPPoA и PPPoE). Если имя назначается в формате user@domain, где domain означает имя услуги, то вводите оба элемента имени в полном соответствии с данными от провайдера.
Password (Пароль)	Введите пароль для данного имени пользователя (только для инкапсуляции PPPoA и PPPoE).

Табл. 20 Подключение к сети Интернет (продолжение)

ПОЛЕ	ОПИСАНИЕ
Service Name (Имя услуги)	(Только для PPPoE) Введите имя службы PPPoE в это поле.
Multiplexing (Мультиплексирование)	Из выпадающего списка выберите метод мультиплексирования, используемый Интернет-провайдером. Вариантами являются **VC** или **LLC**.
Virtual Circuit ID (Идентификатор виртуального канала)	VPI (Virtual Path Identifier – Идентификатор виртуального пути) и VCI (Virtual Channel Identifier – Идентификатор виртуального канала) определяют виртуальную линию передачи. Более подробную информацию см. в приложении.
VPI (Идентификатор виртуального пути)	Допустимый диапазон для VPI равен от 0 до 255. Введите назначенный вам номер VPI.
VCI (Идентификатор виртуального канала)	Допустимый диапазон для VCI равен от 32 до 65535 (номера от 0 до 31 зарезервированы для локального управления трафиком ATM). Введите назначенный вам номер VCI.
IP Address (IP-адрес)	Это поле доступно, если в поле **Mode (Режим)** выбран режим **Routing (Маршрутизация)**.
Obtain an IP Address Automatically (Получать IP-адрес автоматически)	Выберите этот вариант, если вы получаете динамический IP-адрес от своего Интернет-провайдера (ISP). Динамический IP-адрес не является фиксированным; Интернет-провайдер назначает вам новый адрес каждый раз, когда вы подключаетесь к Интернету. Это поле недоступно, если выбран вариант **RFC 1483** в поле **Encapsulation (Инкапсуляция)**.
Static IP Address (Статический IP-адрес)	Выберите этот вариант, если Интернет-провайдер предоставил вам фиксированный IP-адрес. Введите полученный IP-адрес в поле **IP Address**.
IP Address (IP-адрес)	Введите сюда IP-адрес, предоставленный Интернет-провайдером.
Subnet Mask (Маска подсети) (Только для инкапсуляции ENET ENCAP)	Введите маску подсети в десятичном формате с разделительными точками. Информацию о расчете маски подсети при создании подсетей см. в приложениях.
Gateway IP Address (IP-адрес шлюза) (Только для инкапсуляции ENET ENCAP)	Необходимо указать IP-адрес шлюза (предоставленный вашим Интернет-провайдером), если в поле **Encapsulation (Инкапсуляция)** установлен тип инкапсуляции **ENET ENCAP**.
Connection (Подключение) (Только для инкапсуляции PPPoA и PPPoE)	
Nailed-up Connection (Постоянное соединение)	Выберите **Nailed-Up Connection (Постоянное соединение)**, если требуется постоянное соединение. При разрыве соединения P660HWP автоматически будет пытаться восстановить его.

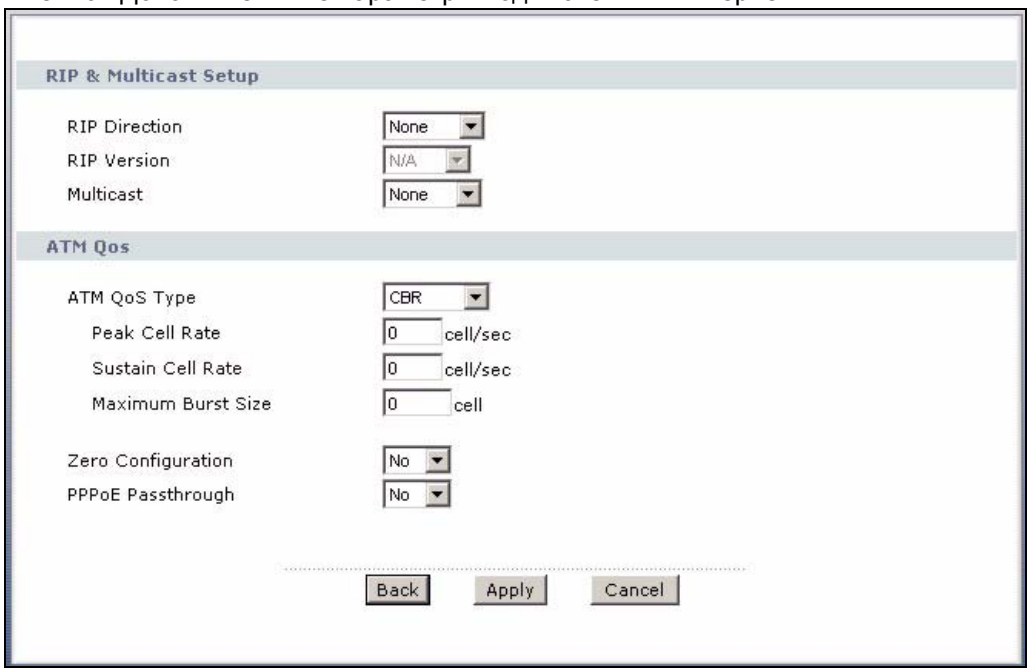
Табл. 20 Подключение к сети Интернет (продолжение)

ПОЛЕ	ОПИСАНИЕ
Connect on Demand (Подключение по требованию)	Выберите **Connect on Demand (Подключение по требованию)**, если постоянное соединение не требуется, и введите в поле **Max. Idle Timeout (Максимальное время простоя)** время простоя (в секундах).
Max Idle Timeout (Максимальное время простоя)	Если вы выбрали **Connect on Demand (Подключение по требованию)**, введите интервал простоя в поле **Max Idle Timeout (Максимальное время простоя)**. По умолчанию установлено 0, что означает, что соединение с Интернет не будет разрываться.
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить изменения.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.
Advanced Setup (Дополнительные настройки)	Щелкните по этой кнопке для отображения окна **Advanced Internet Connection Setup (Дополнительные параметры подключения к Интернет)** и установите дополнительные настройки WAN.

5.5.1 Дополнительные параметры подключения к Интернет

Для изменения в P660HWP дополнительных параметров подключения к глобальной сети, щелкните по кнопке **Advanced Setup (Дополнительная настройка)** в окне **Internet Connection (Подключение к Интернету)**. При этом откроется показанное ниже окно.

Рис. 46 Дополнительные параметры подключения к Интернет



В следующей таблице даны описания полей этого окна.

Табл. 21 Дополнительные параметры подключения к Интернет

ПОЛЕ	ОПИСАНИЕ
RIP & Multicast Setup (Настройка RIP и много-адресной рассылки)	
RIP Direction (Направление RIP)	Выберите направление RIP из раскрывающего списка со значениями **None (Нет)**, **Both (Оба)**, **In Only (Только входящие)** и **Out Only (Только исходящие)**.
RIP Version (Версия RIP)	Выберите версию RIP, где возможны варианты: **RIP-1**, **RIP-2B** и **RIP-2M**.
Multicast (Многоадресная рассылка)	IGMP (Internet Group Multicast Protocol – Протокол многоадресной рассылки) – это протокол сетевого уровня, используемый для установления принадлежности к группе многоадресной рассылки. P660HWP поддерживает обе версии IGMP: **IGMP-v1** и **IGMP-v2**. Выберите **None (Нет)** для отключения IGMP.
ATM QoS (Качество услуг ATM).	
ATM QoS Type (Тип качества услуг ATM)	Выберите **CBR (Постоянная скорость передачи)** для установки постоянной (всегда доступной) пропускной способности для трафика речи или данных. Выберите **UBR (Неопределенная скорость передачи)** для приложений, нечувствительных ко времени, таких как электронная почта. Выберите **VBR-nRT (Переменная скорость передачи вне реального времени)** или **VBR-RT (Переменная скорость передачи в реальном времени)** для передачи пульсирующего трафика и разделения пропускной способности с другими приложениями.
Peak Cell Rate (Пиковая скорость ячеек)	Чтобы найти PCR (Peak Cell Rate – Пиковая скорость ячеек), разделите скорость DSL линии (бит/с) на 424 (размер ячейки ATM). Это и будет максимальная скорость, с которой отправитель может передавать ячейки. Введите в это поле значение PCR.
Sustain Cell Rate (Поддержива-емая скорость ячеек)	Параметр SCR (Sustain Cell Rate – Поддерживаемая скорость ячеек) устанавливает среднюю скорость ячеек (установившаяся скорость), с которой они могут передаваться. Введите значение SCR, оно должно быть меньше, чем PCR. Следует отметить, что по умолчанию установлено 0 ячеек/с.
Maximum Burst Size (Максимальный размер пакета)	MBS (Maximum Burst Size – Максимальный размер пакета) – это максимальное количество ячеек, которое может быть передано на пиковой скорости. Введите значение MBS (должно быть меньше 65535).
Zero Configuration (Автоматическая настройка	Эта функция не применяется / не доступна, если при настройке P660HWP используется статический IP-адрес глобальной сети или режим моста. Выберите **Yes (Да)**, чтобы P660HWP автоматически определял настройки подключения к Интернету (такие как номера VCI/VPI и метод инкапсуляции), используемые Интернет-провайдером и выполнял необходимые изменения в своих настройках. Выберите **No (Нет)** для отключения этой функции. В этом случае для получения доступа в Интернет придется установить настройки P660HWP вручную.

Табл. 21 Дополнительные параметры подключения к Интернет

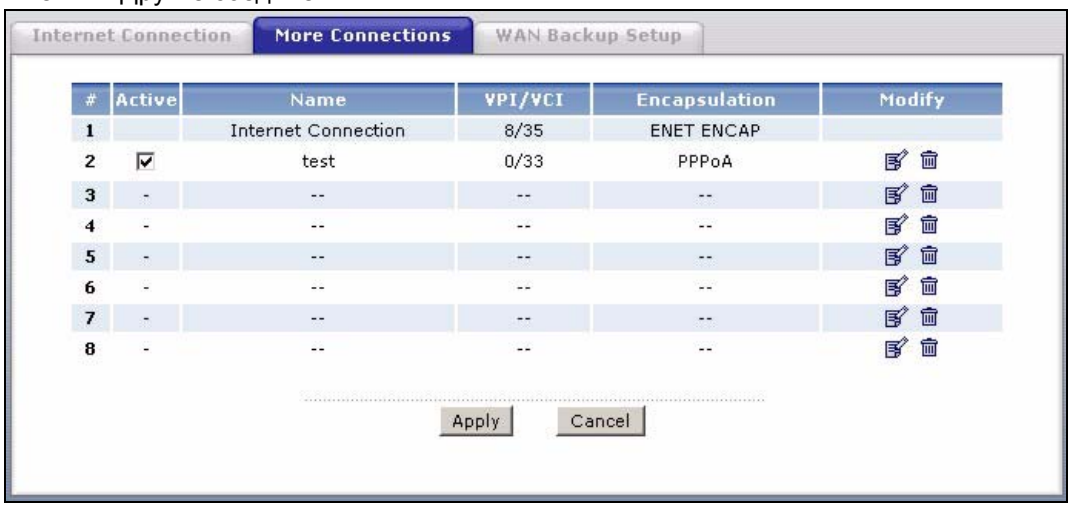
ПОЛЕ	ОПИСАНИЕ
PPPoE PassThrough (Транзит PPPoE-соединений)	Это поле доступно, если выбрана инкапсуляция **PPPoE**. В дополнение к встроенному в P660HWP клиенту PPPoE, можно включить пропускание PPPoE, позволяющее 10 узлам локальной сети с установленным клиентским программным обеспечением PPPoE подключиться к Интернет-провайдеру через P660HWP. Каждый узел может иметь отдельную учетную запись и общедоступный IP-адрес в глобальной сети. Транзит PPPoE-соединений является альтернативой NAT для сфер применения, где использование NAT нецелесообразно. Отключите функцию транзита PPPoE-соединений, если не требуется, чтобы узлы локальной сети использовали программное обеспечение клиента PPPoE для подключения к Интернет-провайдеру.
Back (Назад)	Для возврата к предыдущему окну нажмите кнопку **Back (Назад)**.
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить изменения.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.

5.6 Настройка других соединений

В этом разделе описываются не зависящие от протокола параметры для удаленной сети. Они требуются для выполнения вызовов на удаленный шлюз и расположенную за ним сеть через соединение WAN. При настройке доступа в Интернет в окне **WAN (Глобальная сеть)** > **Internet Connection (Подключение к Интернету)** устанавливается основное подключение к глобальной сети.

Щелкните **Network (Сеть) > WAN (Глобальная сеть) > More Connections (Другие соединения)** для отображения окна, показанного ниже.

Рис. 47 Другие соединения



В следующей таблице даны описания полей этого окна.

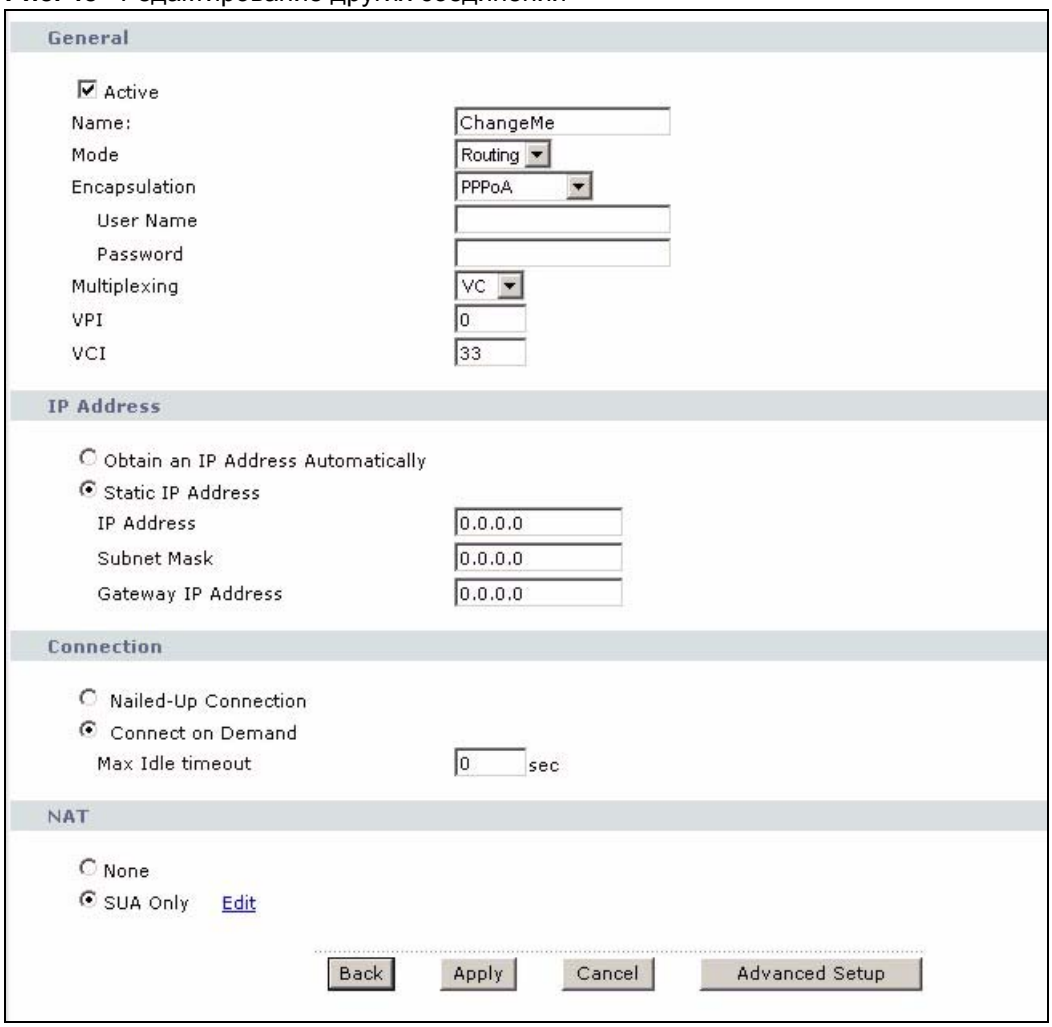
Табл. 22 Другие соединения

ПОЛЕ	ОПИСАНИЕ
#	В этом поле отображается порядковый номер соединения.
Active (Активировать)	В этом поле отображается состояние соединения. Чтобы отключить соединение, снимите флажок. Для включения соединения поставьте флажок.
Name (Имя)	В этом поле отображается описательное имя соединения.
VPI/VCI	В этом поле отображаются значения VPI и VCI для данного соединения.
Encapsulation (Инкапсуляция)	В этом поле отображается метод инкапсуляции для данного соединения.
Modify (Изменить)	В этом окне отображается основное соединение (с Интернет-провайдером) в режиме только для чтения. Изменение его параметров производится в окне **WAN (Глобальная сеть) > Internet Connections (Подключение к Интернету)**. Щелкните по иконке редактирования для перехода к окну, где можно изменить параметры соединения. Для удаления существующего соединения щелкните по иконке удаления. Основное соединение удалить нельзя.
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить изменения.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.

5.6.1 Редактирование других соединений

Щелкните значок редактирования ( ) в окне **More Connections (Другие соединения)** для настройки подключения.

Рис. 48 Редактирование других соединений



В следующей таблице даны описания полей этого окна.

Табл. 23 Редактирование других соединений

ПОЛЕ	ОПИСАНИЕ
Active (Активировать)	Чтобы включить соединение, поставьте флажок в этом поле, чтобы отключить – снимите флажок.
Name (Имя)	Введите уникальное описательное имя для данного соединения длиной до 13 символов латинского алфавита.
Mode (Режим)	Из раскрывающегося списка выберите режим **Routing (Маршрутизация)**, если ваш Интернет-провайдер разрешает подключение нескольких компьютеров по одной учетной записи. При выборе режима **Bridge (Мост)** P660HWP будет пересылать все пакеты, для которых не выполняется маршрутизация, на данный удаленный узел; в противном случае, эти пакеты будут сброшены.
Encapsulation (Инкапсуляция)	Из выпадающего списка выберите метод инкапсуляции, используемый Интернет-провайдером. Вариантами являются: **PPPoA**, **RFC 1483**, **ENET ENCAP** и **PPPoE**.
User Name (Имя пользователя)	Введите имя пользователя, назначенное вашим Интернет-провайдером (только для инкапсуляции PPPoA и PPPoE). Если имя назначается в формате user@domain, где domain означает имя услуги, то вводите оба элемента имени в полном соответствии с данными от провайдера.

Табл. 23 Редактирование других соединений (продолжение)

ПОЛЕ	ОПИСАНИЕ
Password (Пароль)	Введите пароль для данного имени пользователя (только для инкапсуляции PPPoA и PPPoE).
Service Name (Имя услуги)	(Только для PPPoE) Введите имя службы PPPoE в это поле.
Multiplexing (Мультиплексирование)	Из выпадающего списка выберите метод мультиплексирования, используемый Интернет-провайдером. Вариантами являются **VC** или **LLC**. По предварительному соглашению каждому протоколу назначается отдельный виртуальный канал, например, по VC1 передается IP. При выборе VC, необходимо ввести номера VPI и VCI для каждого протокола. При мультиплексировании на базе LLC или инкапсуляции PPP по одному виртуальному каналу передается несколько протоколов вместе с информацией идентификации протоколов, которая содержится в заголовке каждого пакета. В этом случае для всех протоколов нужно указать только один набор номеров VPI и VCI.
VPI (Идентификатор виртуального пути)	Допустимый диапазон для VPI равен от 0 до 255. Введите назначенный вам номер VPI.
VCI (Идентификатор виртуального канала)	Допустимый диапазон для VCI равен от 32 до 65535 (номера от 0 до 31 зарезервированы для локального управления трафиком ATM). Введите назначенный вам номер VCI.
IP Address (IP-адрес)	Это поле доступно, если в поле **Mode (Режим)** выбран режим **Routing (Маршрутизация)**.
Obtain an IP Address Automatically (Получать IP-адрес автоматически)	Выберите этот вариант, если вы получаете динамический IP-адрес от своего Интернет-провайдера (ISP). Динамический IP-адрес не является фиксированным; Интернет-провайдер назначает вам новый адрес каждый раз, когда вы подключаетесь к Интернету. Это поле недоступно, если выбран вариант **RFC 1483** в поле **Encapsulation (Инкапсуляция)**.
Static IP Address (Статический IP-адрес)	Выберите этот вариант, если Интернет-провайдер предоставил вам фиксированный IP-адрес. Введите полученный IP-адрес в поле **IP Address**.
IP Address (IP-адрес)	Введите сюда IP-адрес, предоставленный Интернет-провайдером.
Subnet Mask (Маска подсети)	Введите маску подсети в десятичном формате с разделительными точками. Информацию о расчете маски подсети при создании подсетей см. в приложениях.
Gateway IP Address (IP-адрес шлюза)	Введите IP-адрес шлюза, предоставленный Интернет-провайдером.
Connection (Подключение)	
Nailed-up Connection (Постоянное соединение)	Выберите **Nailed-Up Connection (Постоянное соединение)**, если требуется постоянное соединение. При разрыве соединения P660HWP автоматически будет пытаться восстановить его.
Connect on Demand (Подключение по требованию)	Выберите **Connect on Demand (Подключение по требованию)**, если постоянное соединение не требуется, и введите в поле **Max. Idle Timeout (Максимальное время простоя)** время простоя (в секундах).

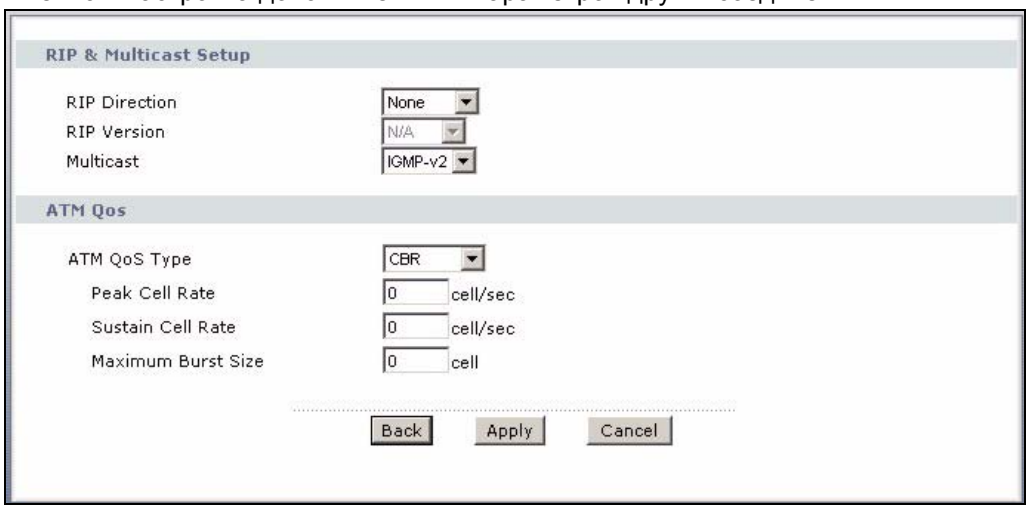
Табл. 23 Редактирование других соединений (продолжение)

ПОЛЕ	ОПИСАНИЕ
Max Idle Timeout (Максимальное время простоя)	Если вы выбрали **Connect on Demand (Подключение по требованию)**, введите интервал простоя в поле **Max Idle Timeout (Максимальное время простоя)**. По умолчанию установлено 0, что означает, что соединение с Интернет не будет разрываться.
NAT (Трансляция сетевых адресов)	NAT - это преобразование IP-адреса узла в пакете, например, адреса источника исходящего пакета, используемого внутри одной сети в другой IP-адрес, известный в другой сети.
None (Нет)	Выберите **None (Нет)** для отключения функции NAT.
SUA Only (Только SUA)	Поле **SUA Only (Только SUA)** доступно, только если в поле **Mode (Режим)** установлено значение **Routing (Маршрутизация)**. Выберите **SUA Only (Только SUA)**, если имеется только один общедоступный IP-адрес и требуется использовать NAT. Щелкните по ссылке **Edit (Редактировать)** для перехода к окну **Port Forwarding (Переадресация портов)** и внесения изменений в таблицу отображения портов сервера.
Back (Назад)	Для возврата к предыдущему окну нажмите кнопку **Back (Назад)**.
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить изменения.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.
Advanced Setup (Дополнительные настройки)	Щелкните по этой кнопке для отображения окна **More Connections Advanced Setup (Дополнительная настройка других соединений)** и установите дополнительные настройки глобальной сети.

5.6.2 Настройка дополнительных параметров других соединений

Для изменения в P660HWP дополнительных параметров подключения к глобальной сети щелкните по кнопке **Advanced Setup (Дополнительная настройка)** в окне **More Connections Edit (Редактирование других соединений)**. При этом откроется показанное ниже окно.

Рис. 49 Настройка дополнительных параметров других соединений



В следующей таблице даны описания полей этого окна.

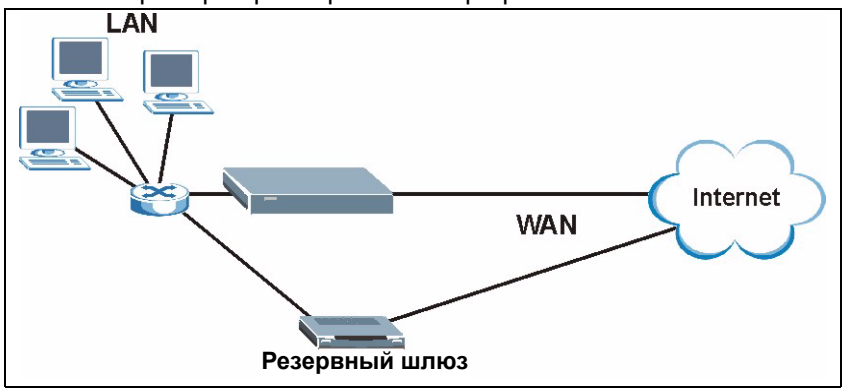
Табл. 24 Настройка дополнительных параметров других соединений

ПОЛЕ	ОПИСАНИЕ
RIP & Multicast Setup (Настройка RIP и многоадресной рассылки)	
RIP Direction (Направление RIP)	Выберите направление RIP из раскрывающего списка со значениями **None (Нет)**, **Both (Оба)**, **In Only (Только входящие)** и **Out Only (Только исходящие)**.
RIP Version (Версия RIP)	Выберите версию RIP, где возможны варианты: **RIP-1**, **RIP-2B** и **RIP-2M**.
Multicast (Многоадресная рассылка)	IGMP (Internet Group Multicast Protocol – Протокол многоадресной рассылки) – это протокол сетевого уровня, используемый для установления принадлежности к группе многоадресной рассылки. P660HWP поддерживает обе версии IGMP: **IGMP-v1** и **IGMP-v2**. Выберите **None (Нет)** для отключения IGMP.
ATM QoS (Качество услуг ATM)	
ATM QoS Type (Тип качества услуг ATM)	Выберите **CBR (Постоянная скорость передачи)** для установки постоянной (всегда доступной) пропускной способности для трафика речи или данных. Выберите **UBR (Неопределенная скорость передачи)** для приложений, нечувствительных ко времени, таких как электронная почта. Выберите **VBR-nRT (Переменная скорость передачи вне реального времени)** или **VBR-RT (Переменная скорость передачи в реальном времени)** для передачи пульсирующего трафика и разделения пропускной способности с другими приложениями.
Peak Cell Rate (Пиковая скорость ячеек)	Чтобы найти PCR (Peak Cell Rate – Пиковая скорость ячеек), разделите скорость DSL линии (бит/с) на 424 (размер ячейки ATM). Это и будет максимальная скорость, с которой отправитель может передавать ячейки. Введите в это поле значение PCR.
Sustain Cell Rate (Поддерживаемая скорость ячеек)	Параметр SCR (Sustain Cell Rate – Поддерживаемая скорость ячеек) устанавливает среднюю скорость ячеек (установившаяся скорость), с которой они могут передаваться. Введите значение SCR, оно должно быть меньше, чем PCR. Следует отметить, что по умолчанию установлено 0 ячеек/с.
Maximum Burst Size (Максимальный размер пакета)	MBS (Maximum Burst Size – Максимальный размер пакета) – это максимальное количество ячеек, которое может быть передано на пиковой скорости. Введите значение MBS (должно быть меньше 65535).
Back (Назад)	Для возврата к предыдущему окну нажмите кнопку **Back (Назад)**.
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить изменения.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.

5.7 Перенаправление трафика

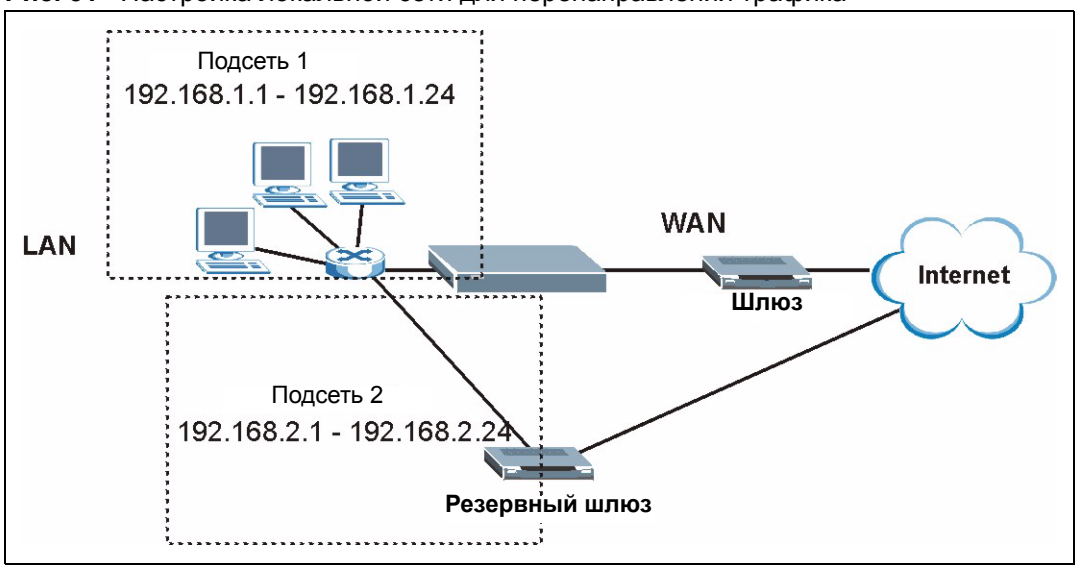
При перенаправлении трафика трафик пересылается на резервный шлюз, если P660HWP не может установить соединение с сетью Интернет. Пример показан на следующем рисунке.

Рис. 50 Пример перенаправления трафика



Топология сети, представленная ниже, позволяет избежать проблем безопасности при треугольном маршруте, если к локальной сети подключен резервный шлюз. С помощью псевдонимов IP локальную сеть можно разделить на 2 или 3 логических сети, и P660HWP будет являться шлюзом для каждой логической сети. Поместите защищенную локальную сеть в одну подсеть (Подсеть 1 на следующем рисунке), а резервный шлюз – в другую подсеть (Подсеть 2). Настройте фильтры, которые пропускают пакеты от защищенной локальной сети (Подсеть 1) к резервному шлюзу (Подсеть 2).

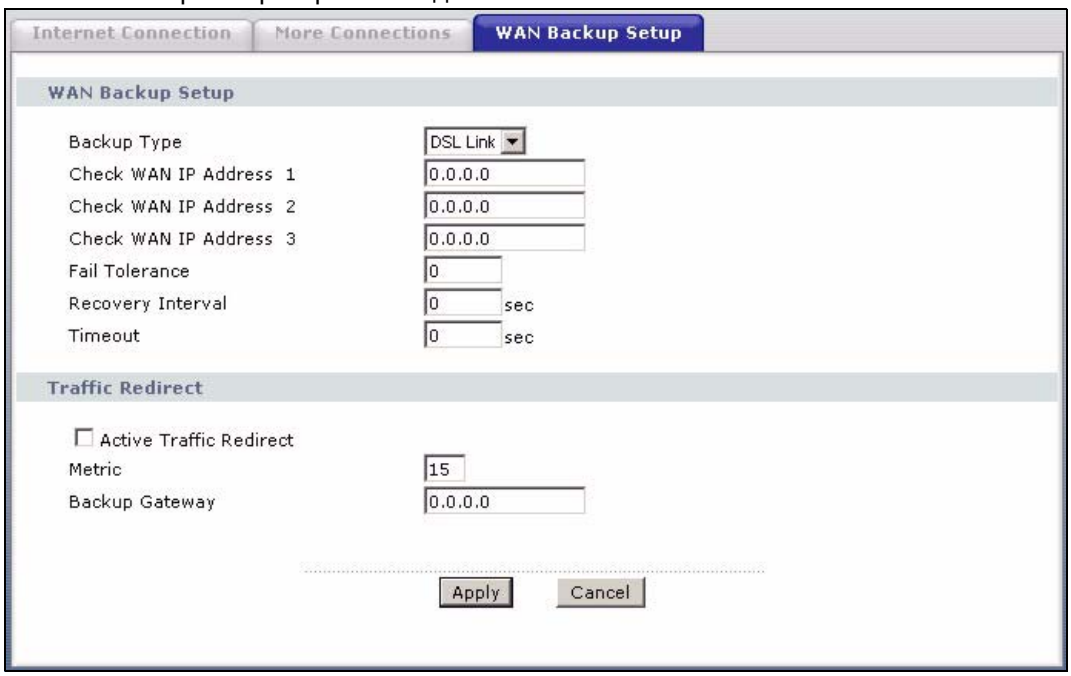
Рис. 51 Настройка локальной сети для перенаправления трафика



5.8 Настройка резервного подключения к глобальной сети

Для изменения параметров резервного подключения порта WAN интернет-центра P660HWP, щелкните **Network (Сеть)** > **WAN (Глобальная сеть)** > **WAN Backup Setup (Настройка резервного подключения WAN)**. При этом откроется показанное ниже окно.

Рис. 52 Настройка резервного подключения к глобальной сети



В следующей таблице даны описания полей этого окна.

Табл. 25 Настройка резервного подключения к глобальной сети

ПОЛЕ	ОПИСАНИЕ
WAN Backup Setup (Настройка резервного подключения к глобальной сети)	
Backup Type (Тип резервирования)	Выберите метод, который P660HWP будет использовать для проверки соединения DSL. Выберите **DSL Link (Канал DSL)**, чтобы P660HWP проверял, установлено ли подключение к DSL-коммутатору. Выберите **ICMP**, чтобы P660HWP периодически посылал эхо-пакеты на IP-адреса, установленные в полях **Check WAN IP Address (Проверять IP-адреса в глобальной сети)**.
Check WAN IP Address1-3 (Проверять IP-адреса глобальной сети 1-3)	Заполните это поле, чтобы P660HWP проверял доступность глобальной сети. Введите IP-адрес ближайшего надежного компьютера (например, адрес сервера DNS Интернет-провайдера). **Примечание: Если включена функция перенаправления трафика или резервного соединения через модем, необходимо настроить по меньшей мере один IP-адрес.** При использовании резервного соединения P660HWP периодически посылает эхо-пакеты на заданные здесь адреса и, если ответ отсутствует, переходит на следующее резевное соединение с WAN (если установлено).

Табл. 25 Настройка резервного подключения к глобальной сети (продолжение)

ПОЛЕ	ОПИСАНИЕ
Fail Tolerance (Максимальное время отсутствия ответа)	Введите время в секундах (рекомендуется 2), в течение которого P660HWP будет посылать эхо-пакеты на IP-адреса, заданные в полях **Check WAN IP Address (Проверять IP-адреса глобальной сети)** при отсутствии ответа, прежде чем перейти на резервное соединение WAN (или другое резервное соединение WAN).
Recovery Interval (Интервал восстановления)	Если P660HWP использует соединение с более низким приоритетом (обычно резервное соединение с WAN), он будет периодически проверять, можно ли перейти на соединение с более высоким приоритетом. Введите время в секундах (рекомендуется 30), в течение которого P660HWP может пребывать в режиме ожидания между проверками. Увеличьте время, если в устройстве с IP-адресом получателя обрабатывается большой объем трафика.
Timeout (Время простоя)	Введите время в секундах (рекомендуется 3), в течение которого P660HWP ожидает ответ на эхо-запрос от одного из IP-адресов, установленных в поле **Check WAN IP Address (Проверять IP-адреса глобальной сети)**, прежде чем повторить запрос. Считается, что подключение P660HWP к глобальной сети отсутствует, после того как пройдет время, установленное в поле **Fail Tolerance (Допуск на отказ)**. Установите в этом поле большее значение, если ваша сеть очень занята или перегружена.
Traffic Redirect (Перенаправление трафика)	При перенаправлении трафика трафик пересылается на резервный шлюз, если P660HWP не может установить соединение с сетью Интернет.
Active Traffic Redirect (Включить перенаправление трафика)	Поставьте в этом поле флажок, чтобы P660HWP использовал перенаправление трафика, если не удается установить нормальное подключение к глобальной сети. **Примечание: При включении функции перенаправления трафика, необходимо сконфигурировать хотя бы одно поле Check WAN IP Address (Проверять IP-адрес глобальной сети).**
Metric (Метрика)	В этом поле устанавливается приоритет маршрута среди маршрутов, используемых P660HWP. Метрика представляет собой «стоимость передачи данных». Маршрутизатор определяет наилучший маршрут для передачи, выбирая путь с самой низкой «стоимостью». Маршрутизация RIP использует счетчик переходов по сети в качестве единицы «стоимости», минимальное значение которой равно 1 и соответствует прямому соединению между сетями. Число должно находиться в интервале от 1 до 15; число больше 15 означает разрыв соединения. Чем меньше число, тем ниже «стоимость».
Backup Gateway (Резервный шлюз)	Введите IP-адрес резервного шлюза в десятичном виде с разделительными точками. P660HWP автоматически пересылает трафик на данный IP-адрес при разрыве соединения с Интернетом.
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить изменения.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.

6

Настройка локальной сети

В этой главе описывается настройка параметров локальной сети.

6.1 Обзор локальной сети

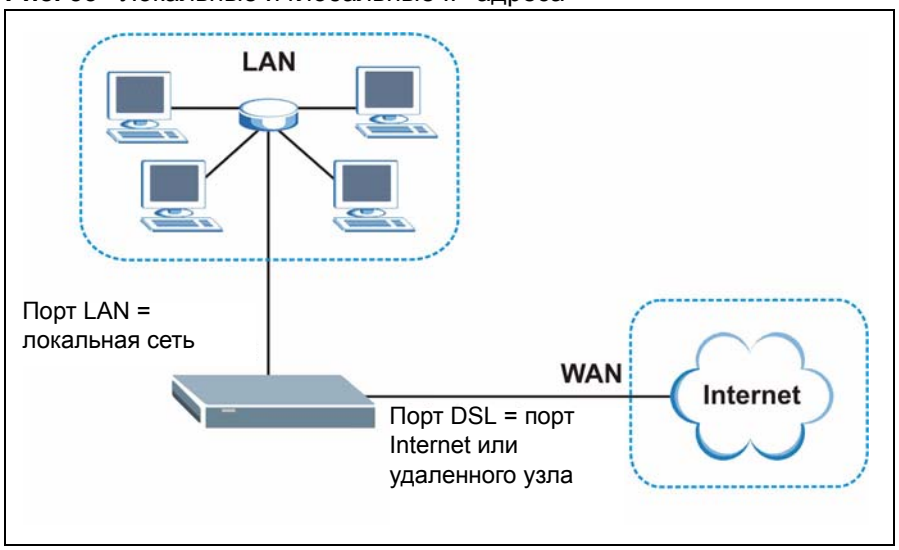
LAN (Local Area Network – Локальная сеть) – это коллективно используемая система связи, к которой подключено множество компьютеров. Локальная сеть представляет собой компьютерную сеть, ограниченную ближайшей территорией, обычно это здание или этаж в здании. Окна настройки LAN используются для настройки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

Информацию об окнах настройки **LAN** см. Разд. 6.3 на с. 109.

6.1.1 Локальные, глобальные сети и P660HWP

Фактическое физическое соединение определяет, являются ли порты P660HWP портами локальной или глобальной сети. Существуют две отдельные IP-сети, одна внутренняя локальная сеть, другая внешняя глобальная сеть, как показано ниже.

Рис. 53 Локальные и глобальные IP-адреса



6.1.2 Настройка DHCP

DHCP (Dynamic Host Configuration Protocol – Протокол динамической настройки узлов, RFC 2131 и RFC 2132) позволяет отдельным клиентским компьютерам получать настройки TCP/IP при загрузке от центрального сервера DHCP. Можно настроить P660HWP как сервер DHCP или отключить эту функцию. При работе в режиме сервера P660HWP предоставляет клиентами DHCP конфигурацию TCP/IP. При отключении службы DHCP требуется наличие другого сервера DHCP в локальной сети или настройка компьютера вручную.

6.1.2.1 Настройка диапазона IP

В P660HWP установлен диапазон IP-адресов клиентов DHCP (диапазон DHCP). См. характеристики изделия в приложениях. Не присваивайте компьютерам локальной сети статических IP-адресов из диапазона DHCP.

6.1.3 Адрес сервера DNS

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

Существует два способа распространения адресов серверов DNS Интернет-провайдером. Первый из них заключается в том, что Интернет-провайдер сообщает клиенту адреса серверов DNS, обычно в виде информационного листка, который клиент подписывает. Если Интернет-провайдер предоставил Вам адреса серверов DNS, следует ввести их в поля **DNS Server (Сервер DNS)** в меню **DHCP Setup (Настройка DHCP)**, в противном случае оставьте эти поля пустыми.

Некоторые Интернет-провайдеры предпочитают передавать адреса серверов DNS после установления соединения с помощью серверных расширений DNS протокола PPP IPCP (IP Control Protocol – Протокол управления IP). Если Интернет-провайдер не предоставляет адресов серверов DNS в явной форме, значит, они передаются в процессе согласования по IPCP. P660HWP поддерживает расширения IPCP сервера DNS посредством функции прокси-сервера DNS.

Если в окне **DHCP Setup (Настройка DHCP)** не заполнены поля **Primary DNS Server (Основной сервер DNS)** и **Secondary DNS Server (Дополнительный сервер DNS)**, т.е., оставлены как **0.0.0.0**, P660HWP сообщает клиентам DHCP, что он сам является сервером DNS. Когда компьютер посылает запрос DNS на P660HWP, то P660HWP пересылает этот запрос на истинный сервер DNS, определенный с помощью IPCP, и ретранслирует ответ компьютеру, пославшему запрос.

Следует отметить, что прокси-сервер DNS может работать, только если Интернет-провайдер использует серверные расширения DNS IPCP. Это не означает, что можно не включать серверы DNS в настройки DHCP при любых обстоятельствах. Если Интернет-провайдер предоставляет адреса серверов DNS в явной форме, убедитесь, что эти IP-адреса установлены в окне **DHCP Setup (Настройка DHCP)**. Таким образом, P660HWP может пропускать к компьютерам ответы серверов DNS, а компьютеры могут посылать запрос прямо на сервер DNS без участия P660HWP.

6.1.4 Назначение адреса сервера DNS

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

Существует два способа распространения адресов серверов DNS Интернет-провайдером.

- Интернет-провайдер сообщает адреса серверов DNS, обычно в виде информационного листка при заключении договора на предоставление услуг. Если Интернет-провайдер предоставляет адреса серверов DNS, введите их в поля для серверов DNS в окне **DHCP Setup (Настройка DHCP)**.
- P660HWP работает как прокси-сервер DNS, если в полях **Primary DNS Server (Основной сервер DNS)** и **Secondary DNS Server (Дополнительный сервер DNS)** в окне **DHCP Setup (Настройка DHCP)** оставлено значение **0.0.0.0**.

6.2 Настройка TCP/IP локальной сети

P660HWP имеет функцию встроенного сервера DHCP, которая позволяет назначать IP-адреса и серверы DNS компьютерам, поддерживающим клиента DHCP.

6.2.1 IP-адрес и маска подсети

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

Номер сети зависит от конкретной ситуации. Если Интернет-провайдер или сетевой администратор назначают блок зарегистрированных IP-адресов, то они также дадут инструкции по выбору IP-адреса и маске подсети.

Если Интернет-провайдер не предоставляет этих данных в явной форме, то вероятнее всего он назначает динамический IP-адрес при установлении соединения. В этом случае рекомендуется выбрать IP-адрес из диапазона 192.168.0.0 – 192.168.255.0 и включить в P660HWP функцию трансляции сетевых адресов (NAT). Агентство по назначению имен и уникальных параметров протоколов Интернет (IANA) зарезервировало этот диапазон специально для частного использования. Если явно не предписано использовать другие адреса, не следует использовать номера за пределами этого диапазона. Если выбрать в качестве номера сети 192.168.1.0, получится 254 индивидуальных адреса от 192.168.1.1 до 192.168.1.254 (числа 0 и 255 зарезервированы). Другими словами, в этом случае первые три числа задают номер сети, а остальные определяют конкретный компьютер в этой сети.

Выбрав номер сети, выберите для P660HWP IP-адрес, который легко запоминается, например, 192.168.1.1, но убедитесь, что никакое другое устройство в вашей сети не использует такой же IP-адрес.

Маска подсети определяет сетевую часть IP-адреса. P660HWP автоматически рассчитывает маску подсети для заданного IP-адреса. Нельзя изменять маску подсети, вычисленную P660HWP, без прямых указаний.

6.2.1.1 IP-адреса для частных сетей

Каждый компьютер в сети Интернет должен иметь уникальный адрес. Если сеть изолирована от Интернета, например, соединяет между собой локальные сети двух филиалов, можно без проблем назначать узлам произвольные IP-адреса. Тем не менее, Агентство по назначению имен и уникальных параметров протоколов Интернет (IANA) зарезервировало следующие три блока IP-адресов специально для частных сетей:

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

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

Независимо от конкретной ситуации не стоит назначать произвольные IP-адреса; лучше следовать приведенным выше указаниям. Для получения более подробной информации по назначению адресов см. RFC 1597, *Address Allocation for Private Internets (Назначение адресов в частных сетях)* и RFC 1466, ***Guidelines for Management of IP Address Space (Руководство по управлению пространством IP-адресов)***.

6.2.2 Настройка RIP

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

- **Both (Оба)** – P660HWP осуществляет периодическую широковещательную рассылку своей маршрутной таблицы и полученных данных RIP.
- **In Only (Только входящие)** – P660HWP не посылает пакеты RIP, но принимает все входящие пакеты RIP.
- **Out Only (Только исходящие)** – P660HWP посылает пакеты RIP, но не принимает входящие пакеты RIP.
- **None (Нет)** – P660HWP не посылает пакеты RIP и игнорирует все входящие пакеты RIP.

Параметр **Version (Версия)** управляет форматом и методом широковещательной рассылки пакетов RIP, которые рассылает P660HWP (оба формата распознаются при приеме). Формат **RIP-1** является общепринятым, но формат RIP-2 содержит больше информации. Формат RIP-1 подходит для большинства сетей, если только сеть не имеет какой-либо специфической топологии.

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

6.2.3 Многоадресная рассылка

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

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

P660HWP поддерживает версии IGMP 1 (**IGMP-v1**) и IGMP 2 (**IGMP-v2**). При запуске P660HWP запрашивает все непосредственно подключенные сети о принадлежности к группе. После получения информации P660HWP периодически обновляет ее. Многоадресную рассылку IP можно включить/отключить для интерфейсов LAN и/или WAN P660HWP с помощью Web-конфигуратора (окна **LAN (Локальная сеть)**, **WAN (Глобальная сеть)**). Для отключения многоадресной рассылки для этих интерфейсов выберите **None (Нет)**.

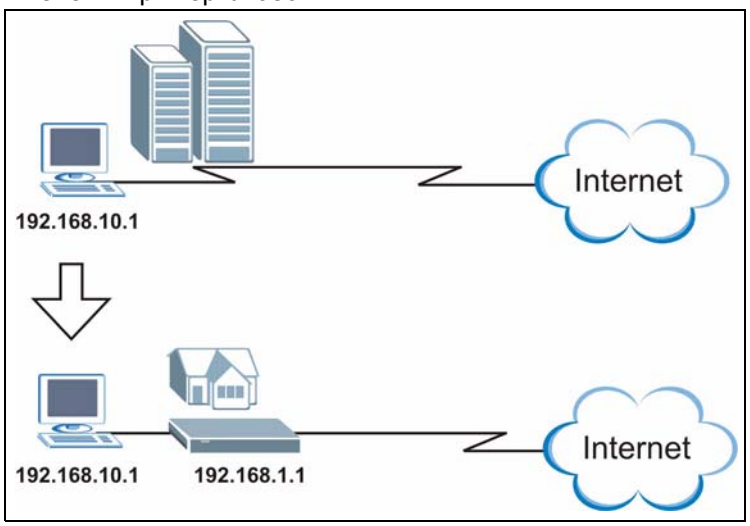
6.2.4 Функция «Any IP» (Любой IP)

Чтобы предоставить компьютеру доступ в Интернет через P660HWP, необходимо, чтобы IP-адреса и маски подсети компьютера и P660HWP находились в одной и той же подсети. В случае, если компьютеру необходимо использовать статический IP-адрес, принадлежащий другой сети, вам придется устанавливать сетевые настройки компьютера вручную каждый раз, когда нужно получить доступ в Интернет через P660HWP.

Если в P660HWP включены функции «Any IP» и NAT, компьютер может получить доступ в Интернет без изменения сетевых настроек (таких как IP-адрес и маска подсети), даже если IP-адреса компьютера и P660HWP находятся в разных подсетях. Независимо от того, динамический или статический IP-адрес назначен компьютеру, вы можете просто подключить компьютер к P660HWP для получения доступа в Интернет.

На следующем рисунке представлен сценарий, где компьютеру назначен статический частный IP-адрес в корпоративной сети. При установке P660HWP в жилом доме можно получить доступ в Интернет без изменения сетевых настроек компьютера, даже если IP-адреса компьютера и P660HWP находятся в разных подсетях.

Рис. 54 Пример: Любой IP



Функция «Any IP» (Любой IP) не применяется к компьютерам с динамическим или статическим IP-адресом, принадлежащим к той же подсети, что и IP-адрес P660HWP.

Для использования в P660HWP функции «Any IP» (Любой IP) *необходимо* включить NAT/SUA.

6.2.4.1 Как работает функция «Any IP» (Любой IP)

ARP (Address Resolution Protocol – Протокол разрешения адресов) служит для установления соответствия между адресом межсетевого протокола IP (IP-адрес) и аппаратным адресом компьютера в локальной сети, известного также как Media Access Control (Управление доступом к среде) или MAC-адрес. Таблица маршрутизации IP для устройства IP Ethernet (P660HWP) определяет следующий транзитный пункт, который необходимо использовать для пересылки данных конкретному адресату.

Когда компьютер пытается в первый раз получить доступ в Интернет через P660HWP, выполняются следующие действия.

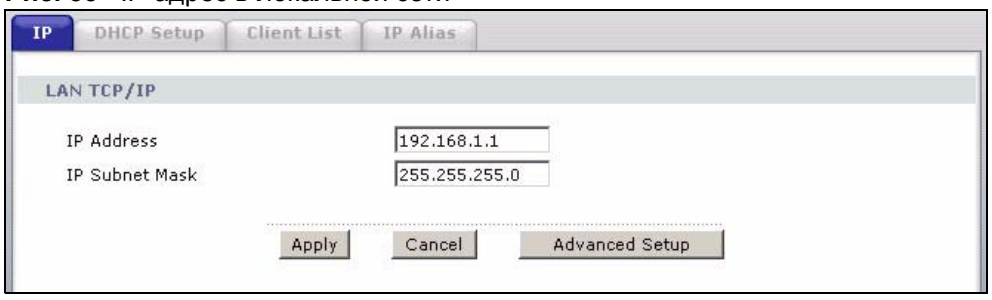
1. Когда компьютер (находящийся в другой подсети) пытается в первый раз получить доступ в Интернет, он посылает пакеты на шлюз по умолчанию (не P660HWP) с помощью поиска его MAC-адреса в своей таблице ARP.
2. Если компьютер не может обнаружить шлюз по умолчанию, посылается широковещательный запрос ARP по локальной сети.
3. P660HWP принимает запрос ARP и отвечает компьютеру, посылая ему свой MAC-адрес.
4. Компьютер обновляет MAC-адрес шлюза по умолчанию в таблице ARP. Обновив таблицу ARP, компьютер может подключаться к Интернету через P660HWP.
5. При получении пакетов от компьютера P660HWP создает запись в таблице маршрутизации IP, с тем чтобы правильно пересылать пакеты, предназначенные для этого компьютера.

После обновления информации о маршрутизации, компьютер получает доступ к P660HWP и к Интернет, как будто он находится в той же подсети, что и P660HWP.

6.3 Настройка IP-адреса в локальной сети

Щелкните **LAN (Локальная сеть)**, чтобы открыть окно **IP**. Более подробную информацию см. Разд. 6.1 на с. 103.

Рис. 55 IP-адрес в локальной сети



В следующей таблице даны описания полей этого окна.

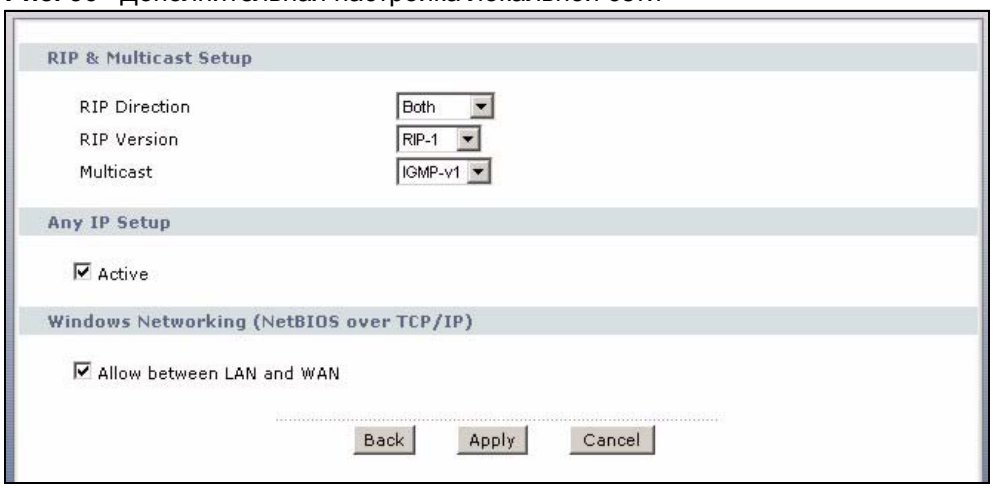
Табл. 26 IP-адрес в локальной сети

ПОЛЕ	ОПИСАНИЕ
LAN TCP/IP (Настройка TCP/IP локальной сети)	
IP Address (IP-адрес)	Введите IP-адрес P660HWP в десятичном виде с разделительными точками, например, 192.168.1.1 (установлен изготовителем по умолчанию).
IP Subnet Mask (Маска IP подсети)	Введите маску подсети, назначенную вашим Интернет-провайдером (если задана).
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек P660HWP.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.
Advanced Setup (Дополнительные настройки)	Щелкните по этой кнопке для отображения окна **Advanced LAN Setup (Дополнительная настройка локальной сети)** и установите дополнительные настройки локальной сети.

6.3.1 Настройка дополнительных параметров локальной сети

Для изменения в P660HWP дополнительных параметров локальной сети, щелкните по кнопке **Advanced Setup (Дополнительная настройка)** в окне **LAN IP (IP-адрес в локальной сети)**. При этом откроется показанное ниже окно.

Рис. 56 Дополнительная настройка локальной сети



В следующей таблице даны описания полей этого окна.

Табл. 27 Дополнительная настройка локальной сети

ПОЛЕ	ОПИСАНИЕ
RIP & Multicast Setup (Настройка RIP и многоадресной рассылки)	
RIP Direction (Направление RIP)	Выберите направление RIP из раскрывающего списка со значениями **None (Нет)**, **Both (Оба)**, **In Only (Только входящие)** и **Out Only (Только исходящие)**.

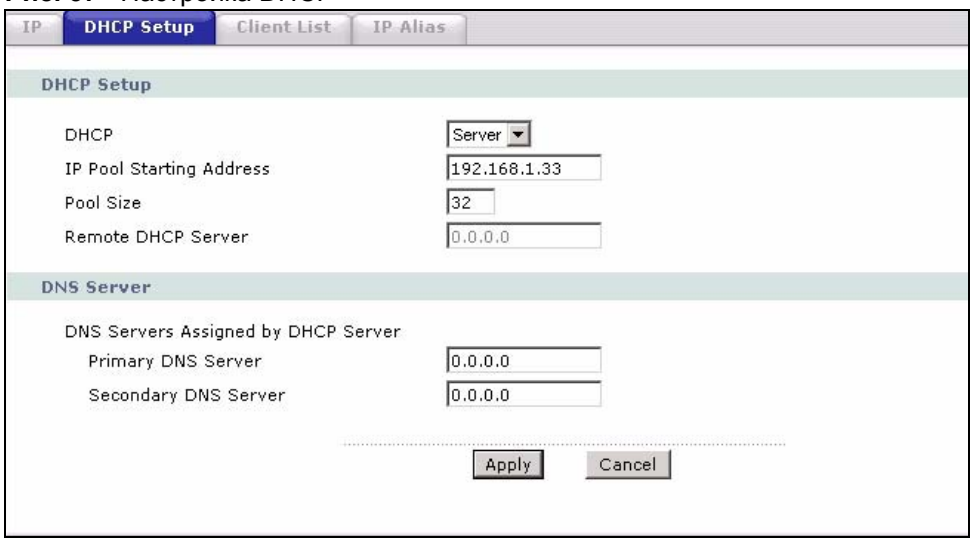
Табл. 27 Дополнительная настройка локальной сети (продолжение)

ПОЛЕ	ОПИСАНИЕ
RIP Version (Версия RIP)	Выберите версию RIP, где возможны варианты: **RIP-1**, **RIP-2B** и **RIP-2M**.
Multicast (Многоадресная рассылка)	IGMP (Internet Group Multicast Protocol – Протокол многоадресной рассылки) – это протокол сетевого уровня, используемый для установления принадлежности к группе многоадресной рассылки. P660HWP поддерживает обе версии IGMP: **IGMP-v1** и **IGMP-v2**. Выберите **None (Нет)** для отключения IGMP.
Any IP Setup (Настройка Any IP)	
Active (Активировать)	Поставьте флажок в поле **Active (Активировать)** для включения функции «Any IP» (Любой IP). Функция Any IP (Любой IP) позволяет компьютеру получить доступ в Интернет без изменения сетевых настроек (таких как IP-адрес и маска подсети), даже если IP-адреса компьютера и P660HWP находятся в разных подсетях. При отключении функции «Any IP» (Любой IP) только компьютеры с динамическими или статическими IP-адресами, принадлежащими той же подсети, что и IP-адрес P660HWP в локальной сети, смогут подключиться к P660HWP или получить доступ в Интернет через P660HWP.
Windows Networking (Средства Windows для удаленного доступа в сеть (NetBIOS по TCP/IP))	Пакеты NetBIOS (Network Basic Input/Output System – Сетевая базовая система ввода-вывода) представляют собой широковещательные пакеты TCP или UDP, позволяющие устанавливать соединение и обмен данными между компьютером и локальной сетью. Для некоторых служб с автоматическим набором номера, например PPPoE или PPTP, пакеты NetBIOS инициируют нежелательные вызовы. Несмотря на это, иногда необходимо разрешить прохождение пакетов NetBIOS в глобальную сеть для того, чтобы найти компьютер в глобальной сети.
Allow between LAN and WAN (Разрешить передачу между LAN и WAN)	Поставьте в этом поле флажок, чтобы разрешить передачу пакетов NetBIOS из локальной сети в глобальную сеть и наоборот. Если в межсетевом экране установлена политика по умолчанию, которая блокирует трафик из глобальной сети в локальную сеть, необходимо включить правило межсетевого экрана, которое пропускает трафик NetBIOS из глобальной сети в локальную. Снимите флажок в этом поле, чтобы блокировать передачу всех пакетов NetBIOS из локальной сети в глобальную сеть и наооборот.
Back (Назад)	Для возврата к предыдущему окну нажмите кнопку **Back (Назад)**.
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить изменения.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.

6.4 Настройка DHCP

В этом окне устанавливаются параметры сервера DNS, которые P660HWP посылает клиентам DHCP в локальной сети.

Рис. 57 Настройка DHCP



В следующей таблице даны описания полей этого окна.

Табл. 28 Настройка DHCP

ПОЛЕ	ОПИСАНИЕ
DHCP Setup (Настройка DHCP)	
DHCP	Если в данном поле установлено значение **Server (Сервер)**, то P660HWP может назначать IP-адреса, IP-шлюз по умолчанию и серверы DNS для Windows 95, Windows NT и других систем, поддерживающих клиента DHCP. Если установлено значение **None (Отключить)**, функция сервера DHCP отключена. Если установлено значение **Relay (Ретранслятор)**, P660HWP выступает в качестве фиктивного DHCP-сервера и передает запросы и ответы между удаленным сервером и клиентами. В этом случае следует ввести IP-адрес фактического удаленного сервера DHCP в поле **Remote DHCP Server (Удаленный сервер DHCP)**. Если функция DHCP включена, необходимо установить следующие параметры:
IP Pool Starting Address (Первый адрес пула IP-адресов)	В этом поле вводится первый адрес из пула непрерывных IP-адресов.
Pool Size (Размер пула)	В этом поле задается размер пула непрерывных IP-адресов.
Remote DHCP Server (Удаленный сервер DHCP)	Если в поле **DHCP** выбрано значение **Relay (Ретранслятор)**, следует ввести IP-адрес фактического удаленного сервера DHCP.
DNS Server (Сервер DNS)	
DNS Servers Assigned by DHCP Server (DNS-сервер, назначенный сервером DHCP)	P660HWP пересылает IP-адрес сервера DNS (Domain Name System – Система доменных имен) клиентам DHCP.

Табл. 28 Настройка DHCP

ПОЛЕ	ОПИСАНИЕ
Primary DNS Server (Основной сервер DNS) Secondary DNS Server (Дополнительный сервер DNS)	Это поле недоступно, если в поле **DHCP** установлено значение **Relay (Ретранслятор)**. Введите IP-адреса серверов DNS. Адреса серверов DNS передаются клиентам DHCP вместе с IP-адресом и маской подсети. Если в этих полях оставлены значения **0.0.0.0**, P660HWP выступает в качестве прокси-сервера DNS и пересылает запросы DNS от клиентов DHCP истинному серверу DNS, определенному с помощью протокола IPCP, и ретранслирует ответ назад компьютеру.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек P660HWP.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.

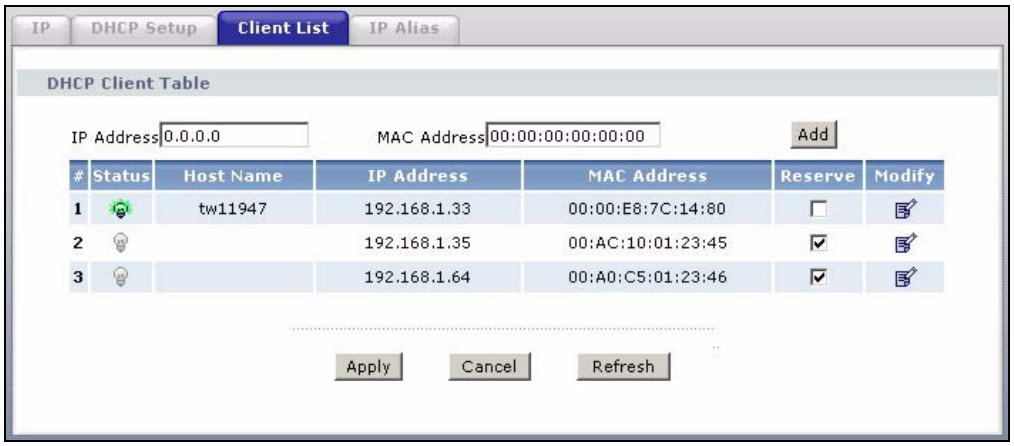
6.5 Список клиентов LAN

С помощью этой таблицы можно назначать IP-адреса отдельным компьютерам локальной сети на основе их MAC-адресов.

Каждое устройство Ethernet имеет уникальный MAC-адрес (Media Access Control – Управление доступом к среде). MAC-адрес назначается изготовителем и состоит из 6 пар шестнадцатеричных символов, например, 00:A0:C5:00:00:02.

Для изменения в P660HWP статических настроек DHCP, нажмите кнопку **Network (Сеть)** > **LAN (Локальная сеть)** > **Client List (Список клиентов)**. При этом откроется показанное ниже окно.

Рис. 58 Список клиентов LAN



В следующей таблице даны описания полей этого окна.

Табл. 29 Список клиентов LAN

ПОЛЕ	ОПИСАНИЕ
IP Address (IP-адрес)	Введите IP-адрес, который вы хотите назначить компьютеру в локальной сети, а также его MAC-адрес в соседнее поле. IP-адрес должен находится в диапазоне IP-адресов, установленном в окне **DHCP Setup (Настройка DHCP)** для клиентов DHCP.
MAC Address (MAC-адрес)	Введите MAC-адрес компьютера локальной сети.
Add (Добавить)	Щелкните по кнопке **Add (Добавить)** для добавления статической записи DHCP.
#	Это порядковый номер записи в таблице статических IP-адресов (строки).
Status (Состояние)	В этом поле отображается, подключен ли данный клиент к P660HWP.
Host Name (Имя узла)	В этом поле отображается имя компьютера.
IP Address (IP-адрес)	В этом поле отображается IP-адрес компьютера с номером, указанном выше.
MAC Address (MAC-адрес)	MAC-адрес (Media Access Control – Управление доступом к среде) или адрес Ethernet в локальной сети является уникальным для каждого компьютера (шесть пар шестнадцатеричных символов). Сетевая интерфейсная карта, такая как Ethernet-адаптер, имеет постоянный адрес, присваиваемый на заводе. Этот адрес отвечает промышленному стандарту, который обеспечивает уникальность этого адреса среди других адаптеров.
Reserve (Резервирование)	Поставьте флажки в этих полях, чтобы P660HWP всегда назначал данные IP-адреса компьютерам с соответствующими MAC-адресами. В данной таблице можно выбрать до 32 записей.
Modify (Изменить)	Щелкните значок **Modify (Изменить)** для изменения **IP-адреса**.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек P660HWP.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.
Refresh (Обновить)	Щелкните по кнопке **Refresh (Обновить)** для перезагрузки таблицы DHCP.

6.6 Псевдоним IP локальной сети

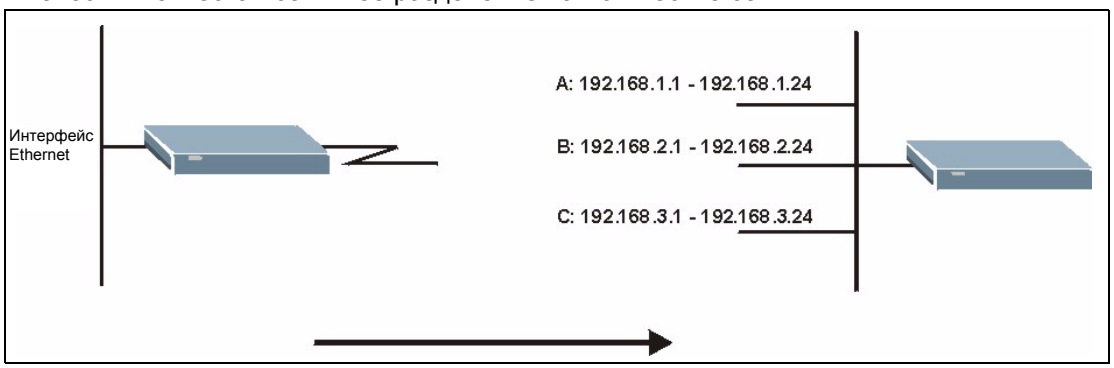
Псевдоним IP позволяет разделить физическую сеть на несколько логических сетей с помощью одного интерфейса Ethernet. P660HWP поддерживает три логических интерфейса локальной сети через один физический интерфейс Ethernet, причем P660HWP является шлюзом для каждой локальной сети.

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

Необходимо следить, чтобы логические сети не перекрывались.

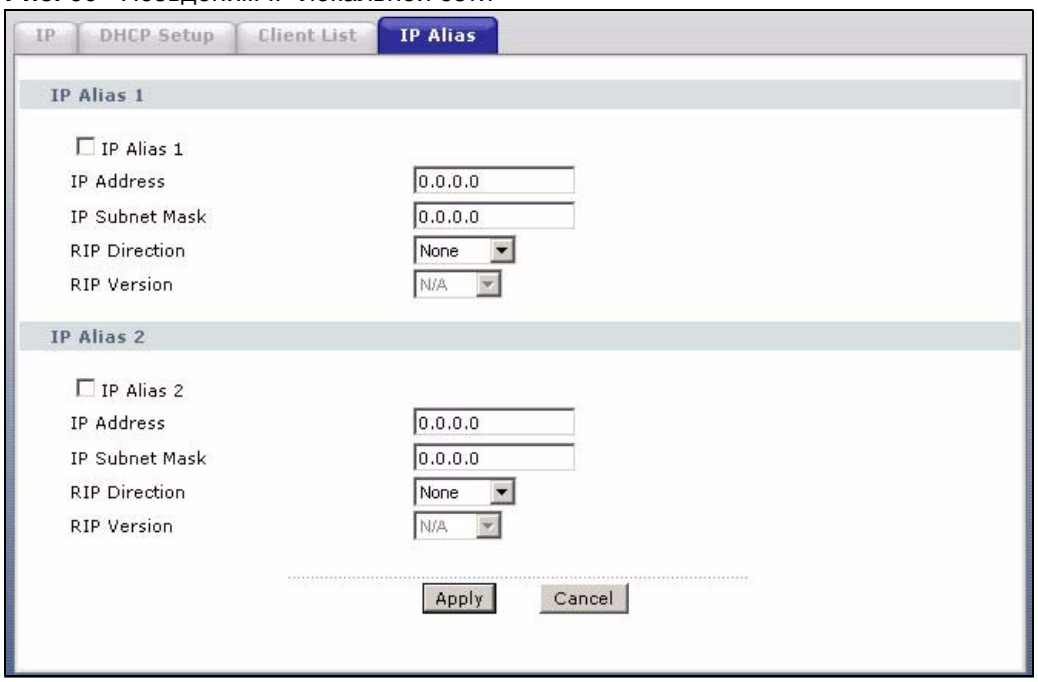
На следующем рисунке показано разделение локальной сети на подсети A, B, и C.

Рис. 59 Физическая сеть и ее разделение на логические сети



Для изменения в P660HWP настроек псевдонимов IP щелкните **Network (Сеть)** > **LAN (Локальная сеть)** > **IP Alias (Псевдоним IP)**. При этом откроется показанное ниже окно.

Рис. 60 Псевдоним IP локальной сети



В следующей таблице даны описания полей этого окна.

Табл. 30 Псевдоним IP локальной сети

ПОЛЕ	ОПИСАНИЕ
IP Alias 1, 2 (Псевдоним IP 1, 2)	Поставьте флажок для настройки другой локальной сети в P660HWP.
IP Address (IP-адрес)	Введите IP-адрес P660HWP в десятичном виде с разделительными точками. Или щелкните правой кнопкой мыши для копирования и/или вставки IP-адреса.
IP Subnet Mask (Маска IP подсети)	P660HWP вычисляет маску подсети автоматически на основании назначенного IP-адреса. Пока не реализована структура подсетей, следует использовать маску подсети, вычисленную P660HWP.

Табл. 30 Псевдоним IP локальной сети

ПОЛЕ	ОПИСАНИЕ
RIP Direction (Направление RIP)	RIP (Routing Information Protocol – Протокол обмена информацией о маршрутизации, RFC 1058 и RFC 1389) позволяет маршрутизатору обмениваться информацией о маршрутизации с другими маршрутизаторами. С помощью настройки поля **RIP Direction (Направление RIP)** производится управление передачей и приемом пакетов RIP. Выберите направление RIP из раскрывающего списка со значениями **Both (Оба) / In Only (Только входящие) / Out Only (Только исходящие) / None (Нет)**. Если установлено **Both (Оба)** или **Out Only (Только исходящие)**, P660HWP будет периодически выполнять широковещательную рассылку своей таблицы маршрутизации. Если установлено **Both (Оба)** или **In Only (Только входящие)**, интернет-центр будет объединять свои данные и полученные данные RIP; при установке **None (Нет)** интернет-центр не будет посылать пакеты RIP и будет игнорировать все входящие пакеты RIP.
RIP Version (Версия RIP)	Параметр **RIP Version (Версия RIP)** управляет форматом и методом широковещательной рассылки пакетов RIP, которые рассылает P660HWP (оба формата распознаются при приеме). Формат **RIP-1** является общепринятым, но формат RIP-2 содержит больше информации. Формат RIP-1 подходит для большинства сетей, если только сеть не имеет какой-либо специфической топологии. Оба формата **RIP-2B** и **RIP-2M** осуществляют отправку данных маршрутизации в формате RIP-2. Их отличие заключается в том, что **RIP-2B** использует циркулярную рассылку для подсети, а **RIP-2M** – многоадресную рассылку. Многоадресная рассылка может способствовать уменьшению нагрузки на машины, которые не являются маршрутизаторами, так как они, как правило, не «прослушивают» групповой адрес пакетов RIP и, следовательно, не получают эти пакеты. Тем не менее, если хотя бы один маршрутизатор в сети использует многоадресную рассылку, остальные маршрутизаторы также должны использовать многоадресную рассылку. По умолчанию для направления RIP установлено значение **Both (Оба)**, а для версии – **RIP-1**.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек P660HWP.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.

7

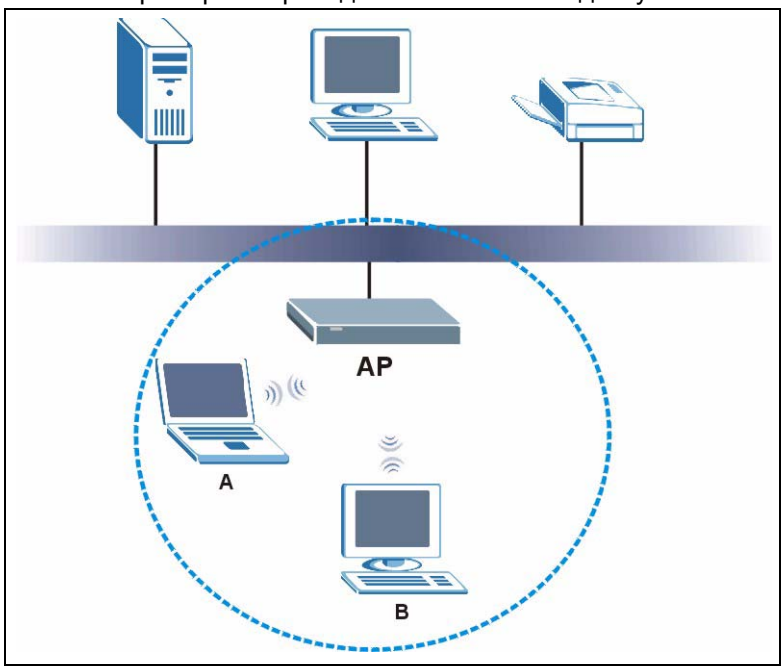
Беспроводная локальная сеть (WLAN)

В этой главе рассказывается, как настроить в P660HWP параметры беспроводной сети. Дополнительную информацию о беспроводных сетях см. в приложениях.

7.1 Обзор беспроводных сетей

На следующем рисунке представлен пример беспроводной сети.

Рис. 61 Пример беспроводной сети с точкой доступа



Беспроводная сеть обозначена синим кругом. Устройства A и B в этой сети называются беспроводными клиентами. Беспроводные клиенты используют точку доступа для подключения к другим устройствам (таким как принтер) или к сети Интернет. P660HWP является точкой доступа.

В любой беспроводной сети должны соблюдаться следующие принципы:

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

  SSID является именем беспроводной сети. SSID – это идентификатор набора служб (Service Set IDentity).
- Если зоны охвата двух беспроводных сетей перекрываются, необходимо, чтобы эти сети использовали разные каналы.

  Подобно радиостанциям или телевизионным каналам, беспроводные сети используют для приема и передачи информации определенные каналы или частоты.
- Все беспроводные устройства, находящиеся в одной беспроводной сети, должны использовать параметры безопасности, совместимые с точкой доступа.

  Настройка безопасности предотвращает доступ неавторизованных устройств к беспроводной сети. Кроме того, таким образом защищается передаваемая по сети информация.

7.2 Настройка беспроводной сети

Для организации беспроводного выхода в сеть Интернет у вас должна быть соответствующая учетная запись.

7.2.1 Требования

Для расширения существующей локальной сети за счет организации беспроводной необходимы следующие элементы:

1. точка доступа (AP; access point) или маршрутизатор с функцией точки доступа
2. как минимум, одна беспроводная сетевая карта или адаптер, в зависимости от вашего компьютера.
   - При использовании настольного компьютера к нему можно подключить беспроводной USB- или PCI-адаптер.
   - При использовании ноутбука к нему можно подключить беспроводной USB- или CardBus-адаптер.
3. сервер RADIUS, если вы хотите использовать стандарт IEEE802.1x, WPA или WPA2

Для организации беспроводной сети без точки доступа или беспроводного маршрутизатора необходимы следующие элементы:

1. две или более беспроводных сетевых карты или адаптера, в зависимости от используемых компьютеров.
   - При использовании настольного компьютера к нему можно подключить беспроводной USB- или PCI-адаптер.
   - При использовании ноутбука к нему можно подключить беспроводной USB- или CardBus-адаптер.

7.2.2 Сведения для установки

Для организации беспроводной сети на основе точки доступа или беспроводного маршрутизатора следует на всех беспроводных устройствах прописать следующие параметры:

- SSID:_____
- Канал: авто или _____
- Тип сети беспроводной сетевой карты/адаптера: с точкой доступа
- Стандарт беспроводной связи: IEEE 802.11b, g, b/g или a
- Безопасность:
  - ( ) Нет
  - ( ) WEP (64-, 128- или 256-битный ключ) (ASCII или Hex):_____
  - ( ) IEEE 802.1x
  - ( ) WPA-PSK (TKIP или AES):_____
  - ( ) WPA (TKIP или AES)
  - ( ) WPA2-PSK (TKIP или AES):_____
  - ( ) WPA2 (TKIP или AES)
- Тип заголовка (если используется): авто, короткий или длинный

Для организации беспроводной сети без точки доступа или беспроводного маршрутизатора следует на всех беспроводных устройствах прописать следующие параметры:

- Тип сети: Ad-Hoc (компьютер-компьютер)
- SSID:_____
- Канал: _____
- Стандарт беспроводной связи: IEEE 802.11b, g, b/g или a
- Безопасность:
  - ( ) Нет
  - ( ) WEP (64-, 128- или 256-битный ключ) (ASCII или Hex):_____

7.3 Защита беспроводной сети – общая информация

В следующих разделах представлены различные виды защиты, которые можно установить для беспроводной сети.

7.3.1 Идентификатор SSID

В стандартном режиме точка доступа работает как радиомаяк, регулярно транслируя в эфир идентификатор SSID. Можно скрыть SSID, и в этом случае точка доступа не будет транслировать SSID. Также можно изменить заданный по умолчанию SSID на трудноугадываемый идентификатор.

Однако этот метод не является достаточным для обеспечения безопасности беспроводной сети, поскольку существуют способы, при помощи которых неавторизованные беспроводные устройства могут получить SSID. Кроме того, неавторизованные беспроводные устройства могут получать информацию, передаваемую по беспроводной сети.

7.3.2 Фильтрация MAC-адресов

Каждый беспроводной клиент имеет уникальный идентификационный номер, называемый MAC-адрес.[1] Обычно MAC-адрес записывается двенадцатью шестнадцатеричными символами[2]; например, 00A0C5000002 или 00-A0-C5-00-00-02. Информацию о MAC-адресе беспроводного клиента см. в руководстве пользователя или другой документации для конкретного устройства.

С помощью фильтра MAC-адресов в точке доступа можно назначить устройства, которым разрешено или не разрешено подключаться к данной беспроводной сети. Если беспроводному клиенту разрешено подключаться к беспроводной сети, ему все равно необходимо иметь правильные настройки (идентификатор SSID, номер канала и параметры безопасности). Если беспроводному клиенту не разрешено подключаться к беспроводной сети, то правильные настройки не имеют значения.

При использовании данного метода безопасности информация, передаваемая по беспроводной сети, не защищается. Более того, существуют способы, при помощи которых неавторизованные устройства могут получить MAC-адрес авторизованного клиента. Затем они могут использовать этот MAC-адрес для включения в беспроводную сеть.

7.3.3 Аутентификация пользователя

Аутентификация – это процедура проверки, которая определяет, может ли беспроводное устройство использовать данную беспроводную сеть. Перед подключением пользователя в беспроводную сеть его необходимо зарегистрировать. Этот процесс называется аутентификацией пользователя. Для прохождения аутентификации все беспроводные устройства в беспроводной сети должны поддерживать стандарт IEEE 802.1x.

В беспроводных сетях имена пользователей и пароли для каждого пользователя обычно хранятся в двух местах.

- В точке доступа: такая функция называется базой данных локальных пользователей или локальной базой данных.
- На сервере RADIUS: такой сервер чаще используется на предприятиях, чем в жилых домах.

1. Некоторые беспроводные устройства, например сканеры, могут определить наличие беспроводной сети, но не могут ее использовать. Такие устройства могут не иметь MAC-адреса.
2. Шестнадцатеричные символы: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F.

Если точка доступа не имеет базы данных локальных пользователей, и сервер RADIUS отсутствует, то невозможно устанавливать имена и пароли для пользователей.

Несанкционированные устройства могут получать информацию, передаваемую в беспроводной сети, даже если они не могут использовать эту беспроводную сеть. Более того, существуют способы получения несанкционированными беспроводными пользователями действующих имени пользователя и пароля. Затем они могут использовать это имя пользователя и пароль для подключения к беспроводной сети.

База данных локальных пользователей также имеет дополнительное ограничение, о котором рассказывается в следующем разделе.

7.3.4 Шифрование

Беспроводные сети могут использовать шифрование для защиты информации, передаваемой по беспроводной сети. Шифрование напоминает секретный код. Не зная кода, нельзя прочесть сообщение.

Виды шифрования выбираются в зависимости от типа аутентификации пользователей. (Дополнительную информацию см. Разд. 7.3.3 на с. 120.)

Табл. 31 Виды шифрования в зависимости от типа аутентификации

	АУТЕНТИФИКАЦИЯ ОТСУТСТВУЕТ	СЕРВЕР RADIUS
Самая слабая защита	Отключение защиты сети	WPA
↕	Статическое шифрование WEP	
	WPA-PSK	
Самая сильная защита	WPA2-PSK	WPA2

Например, если в беспроводной сети есть сервер RADIUS, можно использовать шифрование **WPA** или **WPA2**. Если пользователи не регистрируются в беспроводной сети, вы можете либо отключить шифрование, либо выбрать один из следующих типов шифрования: **статическое шифрование WEP**, **WPA-PSK** или **WPA2-PSK**.

Обычно устанавливается самое сложное шифрование, которое поддерживает каждый клиент в беспроводной сети. Например, предположим, что точка доступа не имеет базы данных локальных пользователей, и сервер RADIUS также отсутствует. Следовательно, аутентификация пользователей отсутствует. Предположим также, что в беспроводной сети находится два беспроводных клиента. Устройство A поддерживает только шифрование WEP, а устройство B поддерживает WEP и WPA. Следовательно, в беспроводной сети следует установить **Статическое шифрование WEP**.

В беспроводной сети рекомендуется использовать шифрование WPA-PSK, WPA или более сложное. Использование шифрования IEEE 802.1x и WEP все же лучше, чем полное отсутствие шифрования, но для несанкционированных устройств существует возможность достаточно быстро вычислить исходные данные для подключения.

При использовании локальной базы данных нельзя применить шифрование **WPA-PSK**, **WPA** или более сложное. В таком случае лучше установить более сложное шифрование без аутентификации, чем использовать простое шифрование вместе с локальной базой данных.

При выборе **WPA2** или **WPA2-PSK** в P660HWP можно также установить параметр **WPA compatible (Совместимость с WPA**) с целью реализации поддержки WPA. В таком случае, если одни беспроводные клиенты поддерживают WPA, а другие WPA2, необходимо установить **WPA2-PSK** или **WPA2** (в зависимости от типа регистрации в беспроводной сети), а также выбрать **WPA compatible (Совместимость с WPA)** в P660HWP.

В большинстве типов шифрования для защиты информации в беспроводной сети используется ключ. Чем длиннее ключ, тем сложнее шифрование. Все беспроводные клиенты в одной беспроводной сети должны использовать одинаковый ключ.

7.3.5 Интеллектуальная технология автонастройки безопасности (OTIST)

Функция OTIST ZyXEL позволяет настроить SSID и WPA-PSK в интернет-центре P660HWP. После этого P660HWP транслирует их устройствам беспроводной сети. В результате не нужно устанавливать SSID и шифрование отдельно на каждом устройстве беспроводной сети.

Устройства в беспроводной сети должны поддерживать функцию OTIST и находится в зоне передачи P660HWP, когда производится их активация. Более подробную информацию см. Разд. 7.5 на с. 132.

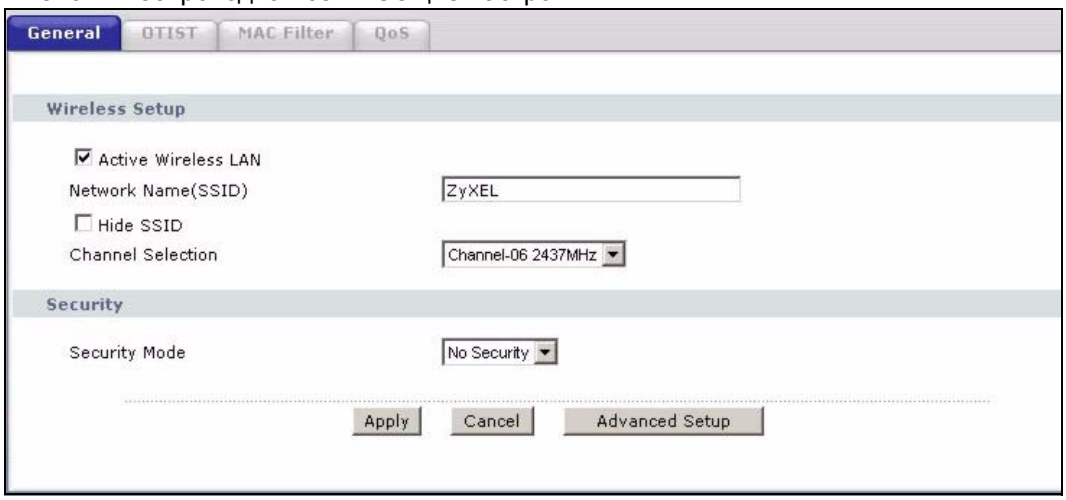
7.4 Окно общих настроек беспроводной сети

Это окно используется для настройки беспроводной локальной сети.

Если вы настраиваете P660HWP с компьютера, подключенного через беспроводную локальную сеть, и при этом изменяете в P660HWP идентификатор SSID или параметры WEP, то при нажатии на кнопку Apply (Применить) беспроводное соединение будет потеряно. В этом случае необходимо изменить беспроводные настройки компьютера для соответствия новым настройкам P660HWP.

Щелкните **Network (Сеть)** > **Wireless LAN (Беспроводная локальная сеть)**, чтобы открыть окно **General (Общие настройки)**.

Рис. 62 Беспроводная сеть: Общие настройки



Приведенная ниже таблица описывает поля общих настроек беспроводной локальной сети.

Табл. 32 Беспроводная сеть: Общие настройки

ПОЛЕ	ОПИСАНИЕ
Wireless Setup (Настройка беспроводной локальной сети)	
Active Wireless LAN (Включить беспроводную локальную сеть)	Поставьте в этом поле флажок, чтобы включить беспроводную локальную сеть.

Табл. 32 Беспроводная сеть: Общие настройки

ПОЛЕ	ОПИСАНИЕ
Network Name (SSID) (Имя сети (SSID))	SSID (Service Set IDentity – Идентификатор набора служб) устанавливает набор служб для беспроводного клиента. Беспроводные клиенты, подключенные к одной точке доступа должны иметь одинаковый SSID. Введите описательное имя для беспроводной локальной сети (не более 32 семиразрядных печатных латинских символов). **Примечание: Если вы настраиваете P660HWP с компьютера, подключенного через беспроводную локальную сеть, и при этом изменяете в P660HWP идентификатор SSID или параметры WEP, то при нажатии на кнопку Apply (Применить) беспроводное соединение будет потеряно. В этом случае необходимо изменить беспроводные настройки компьютера для соответствия новым настройкам P660HWP.**
Hide SSID (Скрыть SSID)	Поставьте флажок в этом поле, чтобы скрыть SSID в исходящем сигнальном кадре, в этом случае станция не сможет получить SSID при сканировании сети программами обзора узлов сети.
Channel Selection (Выбор канала)	Настройте рабочую частоту / канал в зависимости от Вашего региона. Выберите канал из раскрывающегося списка.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек P660HWP.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)** для восстановления предыдущей конфигурации в этом окне.
Advanced Setup (Дополнительные настройки)	Щелкните **Advanced Setup (Дополнительные настройки)** для отображения окна **Wireless Advanced Setup (Дополнительные настройки беспроводного подключения)** и установите дополнительные настройки беспроводной сети.

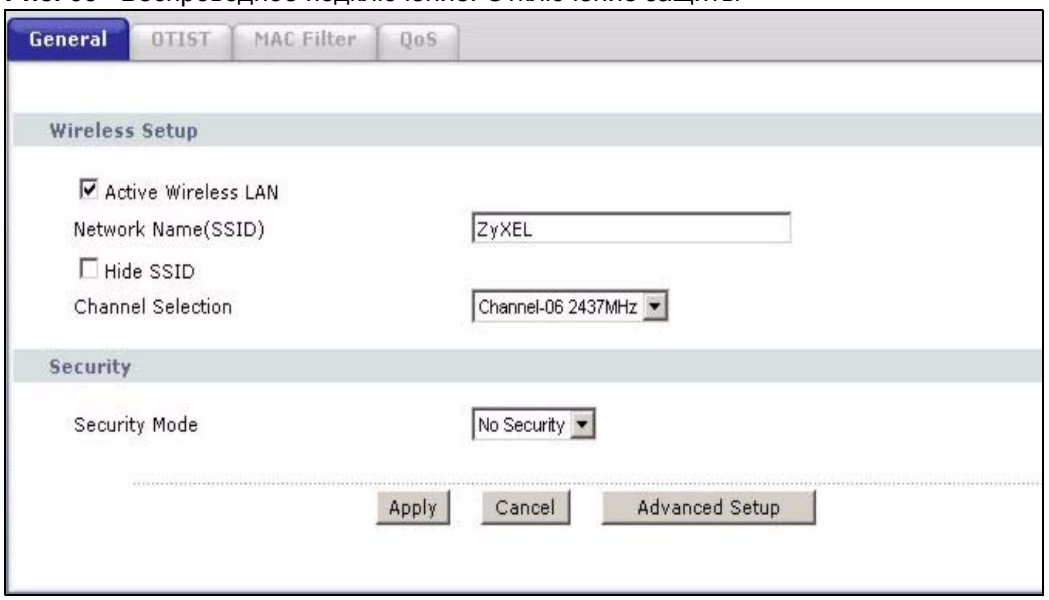
Описание других полей этого окна см. далее в этой главе.

7.4.1 Отключение защиты сети

Выберите **No Security (Отключить защиту)**, чтобы разрешить беспроводным клиентам взаимодействовать с точками доступа без шифрования данных.

Если функция обеспечения беспроводной безопасности в P660HWP отключена, ваша сеть будет доступна для любого беспроводного сетевого устройства, которое находится в зоне охвата сети.

Рис. 63 Беспроводное подключение: Отключение защиты



В следующей таблице даны описания полей этого окна.

Табл. 33 Беспроводное подключение: Отключение защиты

ПОЛЕ	ОПИСАНИЕ
Security Mode (Режим безопасности)	Из выпадающего списка выберите **No Security (Отключить защиту)**.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек P660HWP.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)** для восстановления предыдущей конфигурации в этом окне.
Advanced Setup (Дополнительные настройки)	Щелкните **Advanced Setup (Дополнительные настройки)** для отображения окна **Wireless Advanced Setup (Дополнительные настройки беспроводного подключения)** и установите дополнительные настройки беспроводной сети.

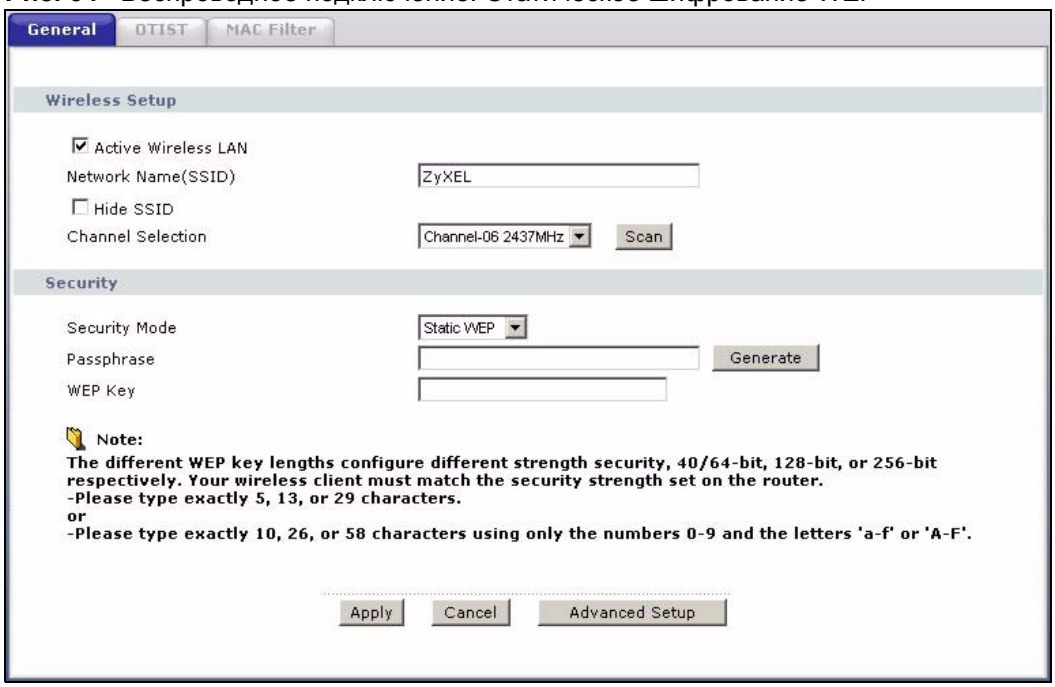
7.4.2 WEP-шифрование

При шифровании WEP данные, передаваемые между беспроводными клиентами и точками доступа, кодируются с целью предотвращения несанкционированного доступа. Шифруются передачи одноадресных и многоадресных рассылок в сети. Беспроводные клиенты и точки доступа должны использовать одинаковый ключ WEP.

P660HWP позволяет создать до четырех ключей WEP длиной 64 бит, 128 бит или 256 бит, но одновременно может использоваться только один ключ.

Чтобы включить и настроить шифрование WEP, щелкните **Network (Сеть)** > **Wireless LAN (Беспроводная локальная сеть)** для отображения окна **General (Общие настройки)**. Выберите **Static WEP (Статическое шифрование WEP)** в списке **Security Mode (Режим безопасности)**.

Рис. 64 Беспроводное подключение: Статическое шифрование WEP



В приведенной ниже таблице описываются поля для настройки безопасности беспроводной локальной сети.

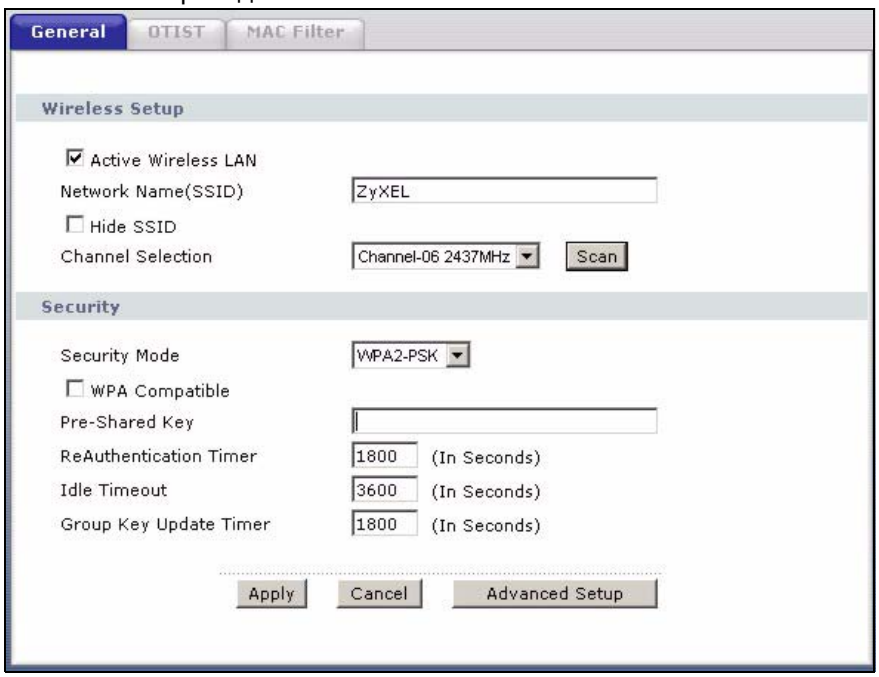
Табл. 34 Беспроводное подключение: Статическое шифрование WEP

ПОЛЕ	ОПИСАНИЕ
Security Mode (Режим безопасности)	Из раскрывающегося списка выберите **Static WEP (Статическое шифрование WEP)**.
Passphrase (Идентификационная фраза)	Введите идентификационную фразу (до 32 печатных знаков) и щелкните **Generate (Генерировать)**. P660HWP автоматически сгенерирует ключ WEP.
WEP Key (Ключ WEP)	Ключи WEP используются для шифрования данных. Для обеспечения передачи данных необходимо, чтобы P660HWP и все беспроводные клиенты использовали одинаковый ключ WEP. Если требуется вручную установить ключ WEP, введите любые 5, 13 или 29 латинских символов или 10, 26 или 58 шестнадцатеричных символов («0-9», «A-F») для генерирования ключа WEP длиной 64 бита, 128 бит или 256 бит соответственно.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек P660HWP.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)** для восстановления предыдущей конфигурации в этом окне.
Advanced Setup (Дополнительные настройки)	Щелкните **Advanced Setup (Дополнительные настройки)** для отображения окна **Wireless Advanced Setup (Дополнительные настройки беспроводного подключения)** и установите дополнительные настройки беспроводной сети.

7.4.3 WPA-PSK/WPA2-PSK

Чтобы включить и настроить аутентификацию WPA(2)-PSK, щелкните **Network (Сеть)** > **Wireless LAN (Беспроводная локальная сеть)** для отображения окна **General (Общие настройки)**. Выберите **WPA-PSK** или **WPA2-PSK** в списке **Security Mode (Режим безопасности)**.

Рис. 65 Беспроводная сеть: WPA-PSK/WPA2-PSK



В приведенной ниже таблице описываются поля для настройки безопасности беспроводной локальной сети.

Табл. 35 Беспроводная сеть: WPA-PSK/WPA2-PSK

ПОЛЕ	ОПИСАНИЕ
Security Mode (Режим безопасности)	Из выпадающего списка выберите **WPA-PSK** или **WPA2-PSK**.
WPA Compatible (Совместимость с WPA)	Это поле доступно, только если в поле **Security Mode (Режим безопасности)** установлено **WPA2-PSK** или **WPA2**. Поставьте в этом поле флажок, чтобы клиенты WPA2 и WPA могли подключаться к P660HWP, даже если в P660HWP используется WPA2-PSK или WPA2.
Pre-Shared Key (Общий ключ)	Механизмы шифрования, используемые для **WPA/WPA2** и **WPA-PSK/WPA2-PSK**, являются одинаковыми. Разница между ними состоит в том, что при **WPA-PSK/WPA2-PSK** используется единственный общий ключ (пароль) для всех пользователей, в то время как WPA предполагает наличие индивидуального пароля у каждого пользователя. Введите общий ключ от 8 до 63 латинских символов с учетом регистра (включая пробелы и знаки).

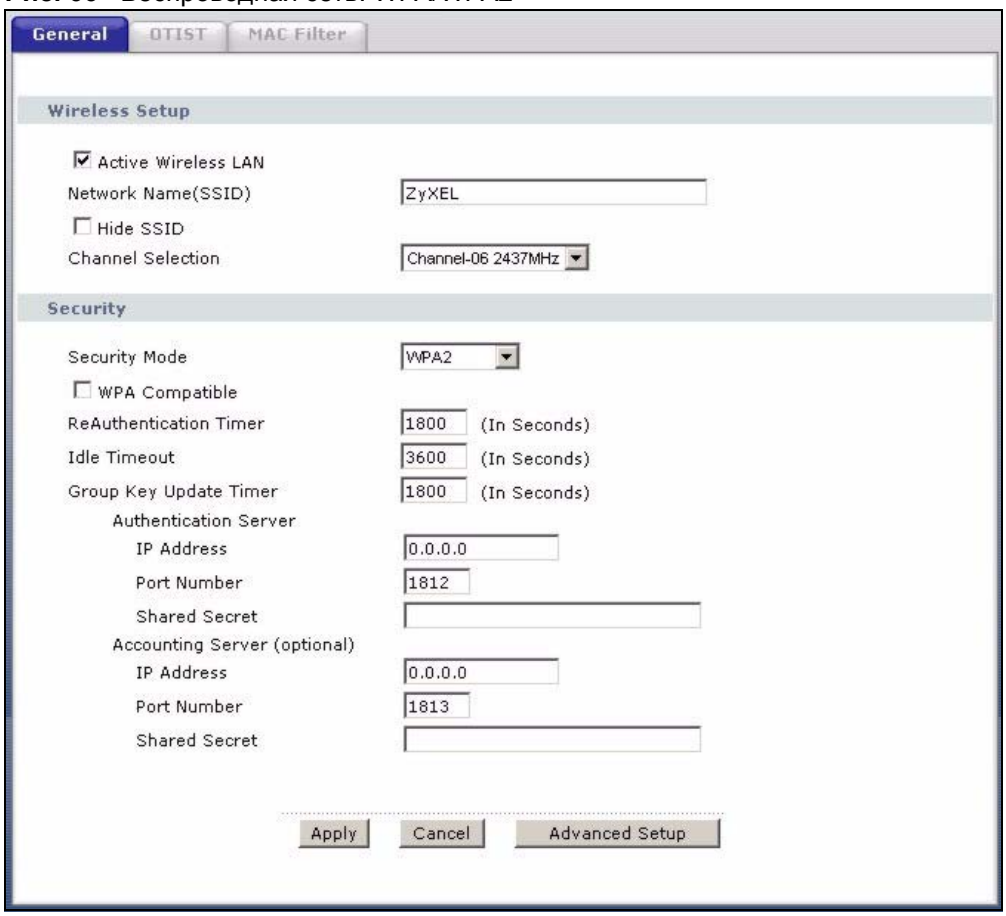
Табл. 35 Беспроводная сеть: WPA-PSK/WPA2-PSK

ПОЛЕ	ОПИСАНИЕ
ReAuthentication Timer (In Seconds) (Интервал повторной аутентификации (в секундах))	Установите время, через которое беспроводные клиенты должны периодически передавать имя пользователя и пароль, для того, чтобы оставаться подключенными к сети. Введите период времени в диапазоне от 10 до 9999 секунд. Временной интервал по умолчанию – 1800 секунд (30 минут). **Примечание: Если аутентификация беспроводного клиента производится с помощью сервера RADIUS, таймер повторной аутентификации на сервере RADIUS имеет приоритет.**
Idle Timeout (in Seconds) (Время простоя (в секундах))	По истечении периода простоя P660HWP автоматически отключает беспроводную станцию от беспроводной сети. Чтобы снова подключиться к беспроводной сети, станции потребуется опять предоставить имя пользователя и пароль. Одни беспроводные клиенты могут подсказывать пользователям имя пользователя и пароль; другие клиенты используют сохраненные регистрационные параметры. В любом случае обычно существует небольшая задержка при повторной регистрации беспроводного клиента в беспроводной сети. Время простоя обычно устанавливается меньше, если беспроводная сеть хранит информацию о том, сколько времени каждая беспроводная станция подключена к беспроводной сети (например, при использовании сервера аутентификации). Если беспроводная сеть не хранит такую информацию, то можно установить большее значение для снижения числа задержек, вызванных повторной регистрацией.
Group Key Update Timer (In Seconds) (Интервал обновления группового ключа (в секундах))	**Group Key Update Timer (Интервал обновления группового ключа)** – это интервал времени, через который точка доступа (если используется управление ключами **WPA-PSK/WPA2-PSK**) или сервер RADIUS (если используется управление ключами WPA(2)) передает новый групповой ключ всем клиентам. Процедура повторной настройки по ключу при WPA(2) является эквивалентом автоматической периодической замены ключей WEP в точке доступа и всех устройствах беспроводной сети. Параметр **Group Key Update Timer (Интервал обновления группового ключа)** также поддерживается в режиме **WPA-PSK/WPA2-PSK**. По умолчанию устанавливается значение в **1800** секунд (30 минут).
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек P660HWP.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)** для восстановления предыдущей конфигурации в этом окне.
Advanced Setup (Дополнительные настройки)	Щелкните **Advanced Setup (Дополнительные настройки)** для отображения окна **Wireless Advanced Setup (Дополнительные настройки беспроводного подключения)** и установите дополнительные настройки беспроводной сети.

7.4.4 WPA/WPA2

Чтобы включить и настроить аутентификацию WPA/WPA2; щелкните по ссылке **Wireless LAN (Беспроводная сеть)** в разделе **Network (Сеть)** для отображения окна **General (Общие параметры)**. Выберите **WPA** или **WPA2** в списке **Security Mode (Режим безопасности)**.

Рис. 66 Беспроводная сеть: WPA/WPA2



В приведенной ниже таблице описываются поля для настройки безопасности беспроводной локальной сети.

Табл. 36 Беспроводная сеть: WPA/WPA2

ПОЛЕ	ОПИСАНИЕ
WPA Compatible (Совместимость с WPA)	Это поле доступно, только если в поле **Security Mode (Режим безопасности)** установлено **WPA2-PSK** или **WPA2**. Поставьте в этом поле флажок, чтобы клиенты WPA2 и WPA могли подключаться к P660HWP, даже если в P660HWP используется WPA2-PSK или WPA2.
ReAuthentication Timer (In Seconds) (Интервал повторной аутентификации (в секундах))	Установите время, через которое беспроводные клиенты должны периодически передавать имя пользователя и пароль, для того, чтобы оставаться подключенными к сети. Введите период времени в диапазоне от 10 до 9999 секунд. Временной интервал по умолчанию – 1800 секунд (30 минут). **Примечание: Если аутентификация беспроводного клиента производится с помощью сервера RADIUS, таймер повторной аутентификации на сервере RADIUS имеет приоритет.**
Idle Timeout (in Seconds) (Время простоя (в секундах))	По истечении периода простоя P660HWP автоматически отключает беспроводного клиента от беспроводной сети. Чтобы снова получить доступ к беспроводной сети, беспроводному клиенту потребуется опять предоставить имя пользователя и пароль. По умолчанию устанавливается значение в 3600 секунд (или 1 час).

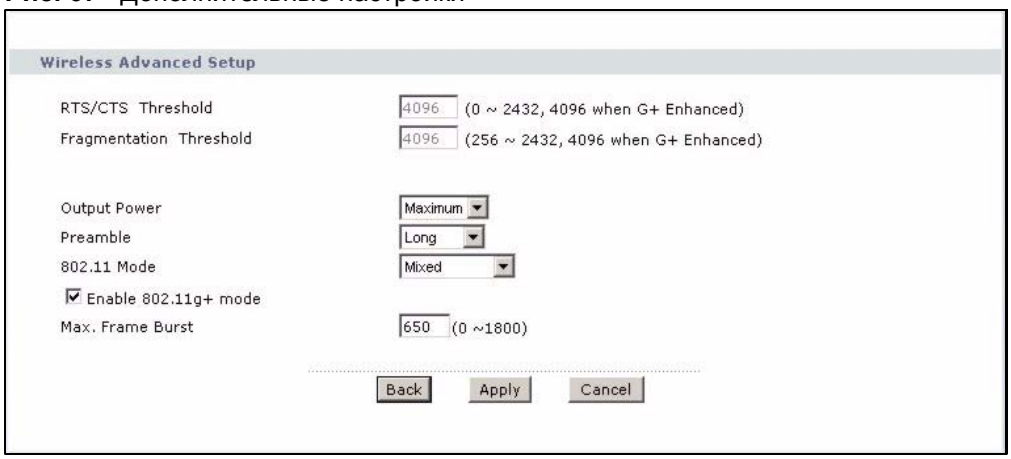
Табл. 36 Беспроводная сеть: WPA/WPA2 (продолжение)

ПОЛЕ	ОПИСАНИЕ
Group Key Update Timer (In Seconds) (Интервал обновления группового ключа (в секундах))	**Group Key Update Timer (Интервал обновления группового ключа)** – это интервал времени, через который точка доступа (если используется управление ключами **WPA-PSK/WPA2-PSK**) или сервер RADIUS (если используется управление ключами WPA(2)) передает новый групповой ключ всем клиентам. Процедура повторной настройки по ключу при WPA(2) является эквивалентом автоматической периодической замены ключей WEP в точке доступа и всех устройствах беспроводной сети. Параметр **Group Key Update Timer (Интервал обновления группового ключа)** также поддерживается в режиме **WPA-PSK/WPA2-PSK**. По умолчанию устанавливается значение в **1800** секунд (30 минут).
Authentication Server (Сервер аутентификации)	
IP Address (IP-адрес)	Введите в этом поле IP-адрес внешнего сервера аутентификации в десятичном виде с разделительными точками.
Port Number (Номер порта)	Введите номер порта сервера внешней аутентификации. Номер порта по умолчанию – **1812**. Не изменяйте это значение, если на то нет специальных указаний и информации от сетевого администратора.
Shared Secret (Общий секретный ключ)	Введите пароль (до 31 буквенно-цифрового символа) для создания ключа, совместно используемого внешним сервером аутентификации и P660HWP. Внешний сервер аутентификации и P660HWP должны использовать одинаковый ключ. Этот ключ не передается по сети.
Сервер учета (не обязательно)	
IP Address (IP-адрес)	Введите в этом поле IP-адрес внешнего сервера учета в десятичном виде с разделительными точками.
Port Number (Номер порта)	Введите номер порта внешнего сервера учета. Номер порта по умолчанию – **1813**. Не изменяйте это значение, если на то нет специальных указаний и информации от сетевого администратора.
Shared Secret (Общий секретный ключ)	Введите пароль (до 31 буквенно-цифрового символа) для создания ключа, совместно используемого внешним сервером учета и P660HWP. Внешний сервер учета и P660HWP должны использовать одинаковый ключ. Этот ключ не передается по сети.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек P660HWP.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)** для восстановления предыдущей конфигурации в этом окне.
Advanced Setup (Дополнительные настройки)	Щелкните **Advanced Setup (Дополнительные настройки)** для отображения окна **Wireless Advanced Setup (Дополнительные настройки беспроводного подключения)** и установите дополнительные настройки беспроводной сети.

7.4.5 Дополнительные настройки беспроводной локальной сети

Для настройки дополнительных параметров беспроводной сети щелкните по кнопке **Advanced Setup (Дополнительные настройки)** в окне **General (Общие настройки)**. При этом откроется показанное ниже окно.

Рис. 67 Дополнительные настройки



В следующей таблице даны описания полей этого окна.

Табл. 37 Беспроводная локальная сеть: Дополнительные настройки

ПОЛЕ	ОПИСАНИЕ
Wireless Advanced Setup (Дополнительные настройки беспроводного подключения)	
RTS/CTS Threshold (RTS/CTS Порог)	Введите значение от 256 до 2346.
Fragmentation Threshold (Порог фрагментации)	Это максимальный размер фрагмента данных для передачи. Введите значение от 256 до 2432.
Output Power (Выходная мощность)	В этом поле устанавливается выходная мощность P660HWP. Это значение определяет коэффициент усиления антенны или мощность передачи P660HWP. С увеличением коэффициента усиления антенны увеличивается зона охвата сети. Более мощное усиление увеличивает дальность сигнала, что обеспечивает лучшую связь. Если в зоне сети высокая плотность точек доступа, следует уменьшить выходную мощность P660HWP, чтобы снизить помехи в других точках доступа. Вариантами являются: **Maximum (Максимальная)**, **Middle (Средняя)** и **Minimum (Минимальная)**.
Preamble (Заголовок)	Выберите **Long (Длинный заголовок)**, если неизвестно, какой режим заголовков поддерживают беспроводные адаптеры, а также для обеспечения более надежной связи в загруженных беспроводных сетях. Выберите **Short (Короткий заголовок)**, если Вы уверены, что этот режим заголовков поддерживается беспроводными адаптерами, а также для обеспечения большей пропускной способности. Выберите **Dynamic (Динамический)**, чтобы P660HWP автоматически использовал короткий заголовок, если он поддерживается всеми беспроводными адаптерами, в противном случае P660HWPбудет использовать длинный заголовок.
802.11 Mode (Режим 802.11)	Выберите **802.11b**, чтобы разрешить подключение к P660HWP только тем беспроводным устройствам, которые совместимы со стандартом IEEE 802.11b. Выберите **802.11g Only (Только 802.11g)**, чтобы разрешить подключение к P660HWP только тем беспроводным устройствам, которые совместимы со стандартом IEEE 802.11g. Выберите **Mixed Mode (Смешаный режим)**, чтобы разрешить подключение к P660HWP беспроводным устройствам, совместимым как со стандартом IEEE802.11b, так и IEEE802.11g. При этом скорость передачи P660HWP может снизиться.

Табл. 37 Беспроводная локальная сеть: Дополнительные настройки (продолжение)

ПОЛЕ	ОПИСАНИЕ
Enable 802.11g+ mode (Включить режим 802.11g+)	При выборе этого параметра включаются режимы Turbo и Super G.
Max. Frame Burst (Максимальный размер серии кадров)	Установка параметра **Maximum Frame Burst (Максимальный размер серии кадров)** помогает устранить конфликты в сетях со смешанным режимом (присутствует оба типа трафика: IEEE 802.11g и IEEE 802.11b), а также увеличить производительность сетей IEEE 802.11g и смешанных сетей IEEE 802.11b/g. **Maximum Frame Burst (Максимальный размер серии кадров)** задает максимальное время в микросекундах, в течение которого P660HWP передает только беспроводной трафик IEEE 802.11g. Введите число от 0 до 1800 (рекомендуется 650, 1000 или 1800). Для отключения этой функции введите 0.
Back (Назад)	Для возврата к предыдущему окну нажмите кнопку **Back (Назад)**.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек P660HWP.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)** для восстановления предыдущей конфигурации в этом окне.

7.5 OTIST

Клиенты беспроводной сети должны иметь то же имя сети (SSID) и те же параметры безопасности, что и точка доступа или беспроводной маршрутизатор, с которыми клиенты устанавливают связь. Раньше это означало необходимость конфигурирования точки доступа, а затем установки тех же параметров вручную в каждом беспроводном клиенте.

Технология OTIST (One-Touch Intelligent Security Technology – Интеллектуальная технология автонастройки безопасности) позволяет передавать идентификатор точки доступа (SSID), а также параметры безопасности WEP или WPA-PSK беспроводным клиентам, которые поддерживают OTIST и находятся в зоне охвата точки доступа. Если ключ WPA-PSK не настроен вручную, устройство, поддерживающее технологию OTIST, может сделать это самостоятельно.

OTIST заменяет предустановленные беспроводные параметры у беспроводных клиентов.

7.5.1 Активация OTIST

Перед началом передачи параметров необходимо активировать OTIST в точке доступа и в беспроводном клиенте.

Точка доступа и беспроводной(-ые**) клиент(-ы) ДОЛЖНЫ использовать один и тот же установочный ключ (Setup key)**.

7.5.1.1 Точка доступа

Функцию OTIST можно включить с помощью кнопки **RESET (Сброс)** или через Web-конфигуратор.

7.5.1.1.1 Кнопка Reset (Сброс)

При использовании кнопки **RESET (Сброс)** для шифрования передаваемых настроек используется **Setup key (Установочный ключ)** по умолчанию (01234567) или последний ключ, установленный с помощью Web-конфигуратора.

Удерживайте кнопку **RESET (Сброс)** 3-8 секунд.

Если удерживать кнопку RESET (Сброс) достаточное время, произойдет восстановление заводских настроек по умолчанию!

7.5.1.1.2 Web-конфигуратор

Щелкните **Network (Сеть) > Wireless LAN (Беспроводная сеть) > OTIST**. Появится следующее окно.

Рис. 68 OTIST

В следующей таблице даны описания полей этого окна.

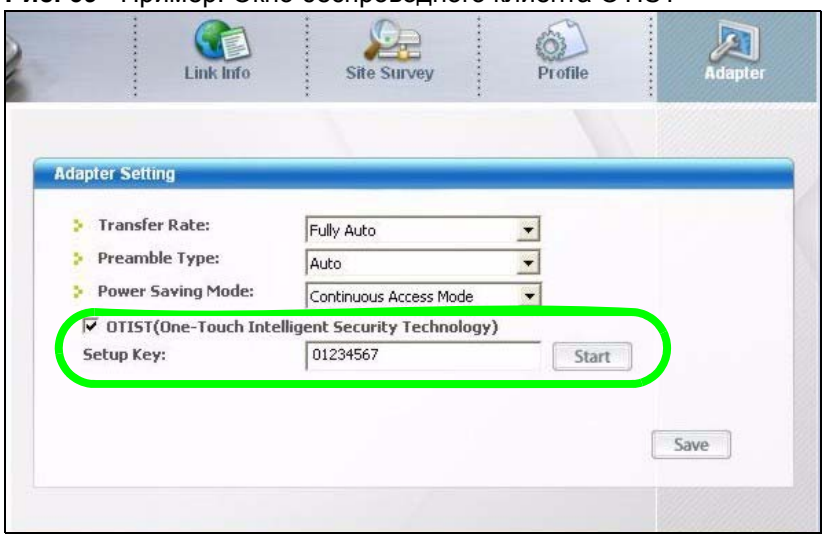
Табл. 38 OTIST

ПОЛЕ	ОПИСАНИЕ
Setup Key (Установочный ключ)	Введите **установочный ключ** OTIST длиной ровно 8 латинских символов. Значение установочного ключа OTIST по умолчанию «01234567». **Примечание: При изменении в этом окне установочного ключа OTIST необходимо произвести те же изменения у беспроводных клиентов.**
Yes! (Да!)	Чтобы OTIST автоматически включал WPA-PSK, необходимо выполнить следующее: • Измените параметры безопасности на отличные от **WPA-PSK** в окне **Wireless LAN (Беспроводная сеть)** > **General (Общие настройки)**. • Установите флажок **Yes! (Да!)** в окне **OTIST** и щелкните **Start (Пуск)**. • В окне будет отображаться автоматически созданная конфигурация WPA-PSK и установлен режим безопасности WPA-PSK. Беспроводным клиентам настройки безопасности WPA-PSK назначаются при запуске OTIST. **Примечание: Если безопасность WPA-PSK уже настроена в окне Wireless LAN (Беспроводная сеть) > General (Общие параметры), и выполнен запуск OTIST с помощью установки флажка Yes! (Да!), OTIST будет использовать существующие настройки WPA-PSK.**
Start (Пуск)	Щелкните **Start (Пуск)**, чтобы выполнять шифрование данных с использованием установочного ключа, и чтобы P660HWP настроил в беспроводных клиентах такие же параметры безопасности, что и в P660HWP. Необходимо также включить и произвести запуск OTIST на всех беспроводных клиентах в течение 3 минут.

7.5.1.2 Беспроводной клиент

Запустите утилиту беспроводного адаптера и перейдите на вкладку **Adapter (Адаптер)**. Поставьте флажок **OTIST**, введите тот же **установочный ключ**, который использует точка доступа, и нажмите **Save (Сохранить)**.

Рис. 69 Пример: Окно беспроводного клиента OTIST

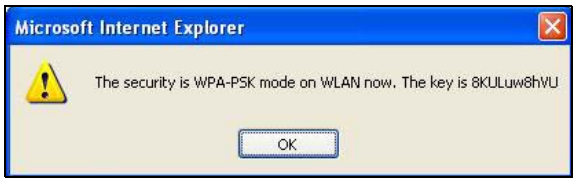


7.5.2 Запуск OTIST

Запуск функции OTIST должен быть произведен на всех устройствах, участвующих в настройке безопасности, в течение трех минут**. Запускать OTIST в беспроводных клиентах и точке доступа можно в любом порядке, но все они должны находиться в зоне доступа, и поддержка OTIST должна быть включена.**

1 В точке доступа отображается окно веб-конфигуратора с параметрами безопасности, подлежащими транслированию. В этом окне можно использовать ключ для установки шифрования WPA-PSK вручную для устройств беспроводной сети, не поддерживающих OTIST. После проверки параметров нажмите **OK**.

Рис. 70 Ключ безопасности



2 Это окно появляется во время передачи параметров по OTIST. Оно закрывается после окончания передачи.

Рис. 71 Выполнение OTIST в точке доступа

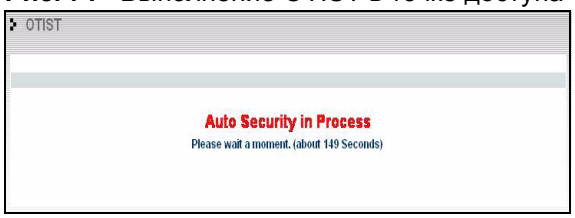
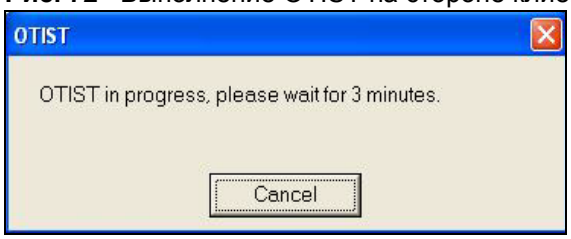
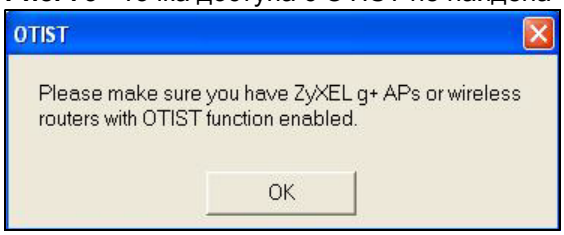


Рис. 72 Выполнение OTIST на стороне клиента



Это окно отображается на стороне беспроводного клиента, если он не может найти точку доступа с включенной функцией OTIST (с таким же **установочным ключом**). Нажмите **OK**, чтобы перейти обратно к главному окну утилиты беспроводного адаптера.

Рис. 73 Точка доступа с OTIST не найдена

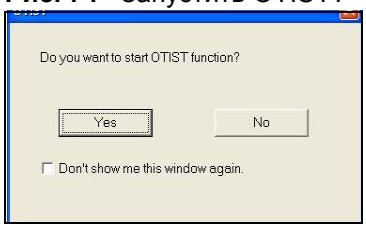


- Если в зоне доступа находятся несколько точек доступа, поддерживающих OTIST, появится экран, предлагающий выбрать точку доступа, от которой будут получены параметры.

7.5.3 Замечания относительно OTIST

1. Если в беспроводном клиенте включена поддержка OTIST, это окно будет появляться каждый раз при запуске утилиты. Нажмите **Yes (Да)**, чтобы начать поиск точки доступа, поддерживающей OTIST.

Рис. 74 Запустить OTIST?



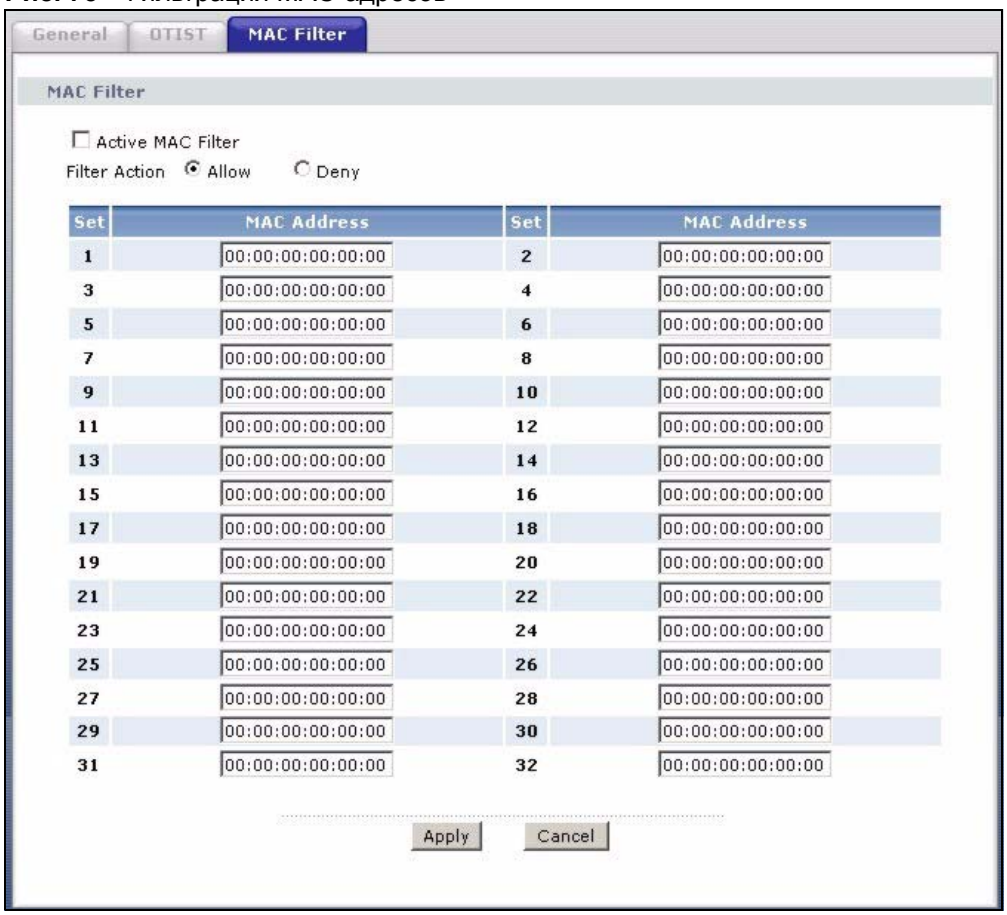
2. Если беспроводной клиент, поддерживающий OTIST, теряет беспроводную связь с точкой доступа более чем на десять секунд, он будет искать точку доступа, поддерживающую OTIST, в течение одной минуты. Если дать беспроводному клиенту команду искать точку доступа, поддерживающую OTIST, поиск не прекратится автоматически; для остановки поиска нажмите **Cancel (Отменить)** в окне выполнения OTIST.
3. Если беспроводной клиент нашел точку доступа, с включенной функцией OTIST, необходимо в точке доступа нажать на кнопку **Start (Пуск)** в окне Web-конфигуратора OTIST или удерживать нажатой кнопку **RESET (Сброс)** (в течение 1-5 секунд), чтобы точка доступа начала передачу параметров безопасности.
4. При изменении идентификатора SSID или ключей в точке доступа после их передачи по OTIST, необходимо повторить передачу параметров по OTIST или ввести их вручную в беспроводном(-ых) клиенте(-ах).
5. Если OTIST настроена на генерацию ключа WPA-PSK, этот ключ меняется каждый раз при запуске OTIST. Поэтому, если к вашей беспроводной сети подключается новый беспроводной клиент, необходимо еще раз запустить OTIST в точке доступа и на ВСЕХ беспроводных клиентах.

7.6 Фильтрация MAC-адресов

Окно MAC-фильтра позволяет настроить P660HWP так, чтобы к нему могло получить монопольный доступ до 32 устройств (опция **Allow (Разрешить)**) или, напротив, запретить доступ к P660HWP для данных устройств (опция **Deny (Запретить)**). Каждое устройство Ethernet имеет уникальный MAC-адрес (Media Access Control – Управление доступом к среде). MAC-адрес назначается изготовителем и состоит из 6 пар шестнадцатеричных символов, например, 00:A0:C5:00:00:02. Для настройки этого окна необходимо знать MAC-адреса устройств.

Для изменения параметров MAC-фильтра P660HWP щелкните **Network (Сеть)** > **Wireless LAN (Беспроводная локальная сеть)** > **MAC Filter (MAC-фильтр)**. При этом откроется показанное ниже окно.

Рис. 75 Фильтрация MAC-адресов



В следующей таблице даны описания полей этого окна.

Табл. 39 Фильтрация MAC-адресов

ПОЛЕ	ОПИСАНИЕ
Active MAC Filter (Включить MAC-фильтр)	Поставьте в этом поле флажок, чтобы включить фильтрацию MAC-адресов.
Filter Action (Действие фильтра)	Определите способ фильтрации для списка MAC-адресов в таблице **MAC Address (MAC-адрес)**. Выберите **Deny (Запретить)**, чтобы заблокировать доступ к P660HWP. Устройствам с MAC-адресами, не перечисленными в данном списке, доступ к P660HWP будет разрешен. Выберите **Allow (Разрешить)**, чтобы открыть доступ к P660HWP. Устройствам с MAC-адресами, не перечисленными в данном списке, доступ к P660HWP будет запрещен.
Set (Устройство)	Это индексный номер MAC-адреса.
MAC Address (MAC-адрес)	Введите в адресные поля MAC-адреса беспроводных клиентов, которым разрешен или запрещен доступ к P660HWP. MAC-адреса необходимо вводить в специальном формате MAC-адресов, т. е., шесть пар шестнадцатеричных символов, например, 12:34:56:78:9a:bc.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек P660HWP.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)** для восстановления предыдущей конфигурации в этом окне.

7.7 Качество предоставления услуг в беспроводной среде передачи

QoS (Quality of Service – качество и класс предоставляемых услуг) для WMM (Wi-Fi MultiMedia – беспроводная мультимедийная передача) позволяет назначать приоритеты беспроводному трафику в соответствии с требованиями доставки трафика конкретных служб.

WMM является расширением QoS в стандарте IEEE 802.11e для аттестованных беспроводных сетей.

7.7.1 Пример WMM QoS

Если функция WMM QoS отключена, всем потокам трафика предоставляется одинаковая пропускная способность для доступа к беспроводной сети. Если при введении еще одного потока создаются требования, которые превышают текущую производительность сети, то из-за нового потока снижается пропускная способность сети для других потоков трафика.

Если функция WMM QoS включена, потокам назначаются приоритеты в соответствии с требованиями приложений. Различным приложениям можно назначать различные приоритеты. Это предотвращает снижение скорости передачи для приложений, чувствительных к этому.

7.7.2 Приоритеты WMM QoS

В следующей таблице представлены приоритеты, применяемые к трафику, который P660HWP пересылает в беспроводную сеть.

Табл. 40 Приоритеты WMM QoS

ПОЛЕ	ОПИСАНИЕ
Самый высокий	Обычно используется для трафика передачи речи или видеоизображений, который очень чувствителен к дрожанию (изменение величины задержки). Самый высокий приоритет используется с целью уменьшить время ожидания для улучшения качества передачи речи.
Высокий	Обычно используется для видеотрафика, который имеет некоторый допуск на дрожание, но требует приоритета над другими видами трафика данных.
Средний	Обычно используется для трафика от приложений или устройств, которым требуются возможности QoS. Средний приоритет используется для трафика, который менее чувствителен к ожиданию, но не допускает больших задержек, как, например, Интернет серфинг.
Низкий	Обычно используется для некритического «фонового» трафика, как, например, групповая пересылка данных и задания на печать, которые допускают задержки и не влияют на другие приложения и пользователей. Низкий приоритет используется для приложений, которые не имеют жестких требований ко времени ожидания и пропускной способности.

7.7.3 Службы

В следующей таблице приведены наиболее часто используемые службы и номера портов. Дополнительную информацию по номерам портов можно получить в RFC 1700. Рядом с названием службы располагаются два поля в скобках. В первом поле указывается тип протокола IP (TCP, UDP или ICMP). Во втором – номер порта IP для данной службы. Следует учесть, что тип протокола IP может быть не один. Например, для службы DNS (UDP/TCP:53) означает UDP-порт 53 и TCP-порт 53.

Табл. 41 Наиболее часто используемые службы

СЛУЖБА	ОПИСАНИЕ
AIM/New-ICQ(TCP:5190)	Система пересылки сообщений в сети Интернет, предоставляемая корпорацией AOL, используется службой ICQ как «слушающий» порт.
AUTH(TCP:113)	Протокол аутентификации, используется некоторыми серверами.
BGP(TCP:179)	Протокол BGP (пограничный межсетевой протокол).
BOOTP_CLIENT(UDP:68)	Клиент DHCP.
BOOTP_SERVER(UDP:67)	Сервер DHCP.
CU-SEEME(TCP/UDP:7648, 24032)	Популярное решение для проведения видеоконференций от White Pines Software.
DNS(UDP/TCP:53)	Сервер имен доменов – служба, определяющая соответствие web-имен (например, www.zyxel.com) и номеров IP.
FINGER(TCP:79)	Finger – команда для UNIX или Интернет, используемая для проверки нахождения пользователя в сети.

Табл. 41 Наиболее часто используемые службы

СЛУЖБА	ОПИСАНИЕ
FTP(TCP:20.21)	Протокол передачи файлов, программа для быстрой передачи файлов, в том числе файлов большого размера, которые невозможно пересылать средствами электронной почты.
H.323(TCP:1720)	Протокол для Net Meeting.
HTTP(TCP:80)	Протокол передачи гипертекста – протокол уровня клиент/сервер для WWW.
HTTPS (TCP:443)	HTTPS - это надежный сеанс связи http, часто используемый в электронной коммерции.
ICQ(UDP:4000)	Популярная система интерактивного общения в Интернет.
IKE(UDP:500)	Алгоритм обмена ключами в Интернет, используется для распределения и управления ключами.
IPSEC_TUNNEL(AH:0)	Эту службу использует протокол туннелирования IPSEC AH (Заголовок аутентификации).
IPSEC_TUNNEL(ESP:0)	Эту службу использует протокол туннелирования IPSEC ESP (Протокол обеспечения безопасности инкапсуляции).
IRC(TCP/UDP:6667)	Еще одна программа интерактивного общения в Интернет.
MSN Messenger(TCP:1863)	Протокол для передачи сообщений в сетях Microsoft.
MULTICAST(IGMP:0)	Internet Group Multicast Protocol (Широковещательный протокол взаимодействия групп в сети Интернет) используется для отправки пакетов определенным группам узлов.
NEW-ICQ(TCP:5190)	Программа для обмена текстовыми сообщениями между абонентами сети Internet в реальном времени.
NEWS(TCP:144)	Протокол для групп новостей.
NFS(UDP:2049)	Сетевая файловая система – NFS, распределенная файловая служба клиент/сервер, обеспечивающая прозрачное совместное использование файлов в сети.
NNTP(TCP:119)	Network News Transport Protocol (Сетевой протокол передачи новостей) – система доставки для групп новостей USENET.
PING(ICMP:0)	Packet INternet Groper (Пакетное эхо-тестирование в Интернет) – это протокол, который посылает эхо-запросы ICMP для проверки достижимости удаленного узла.
POP3(TCP:110)	Почтовый протокол версии 3, позволяет клиентскому компьютеру получать электронную почту с сервера POP3, используя временное соединение (TCP/IP или другое).
PPTP(TCP:1723)	Point-to-Point Tunneling Protocol (Протокол туннелирования «точка-точка») обеспечивает безопасную передачу данных в общедоступных сетях. Это канал управления.
PPTP_TUNNEL(GRE:0)	Point-to-Point Tunneling Protocol (Протокол туннелирования «точка-точка») обеспечивает безопасную передачу данных в общедоступных сетях. Это канал передачи данных.
RCMD(TCP:512)	Удаленное управление командной строкой.
REAL_AUDIO(TCP:7070)	Система прямого воспроизведения звука, обеспечивает передачу аудиопотоков в сети в реальном времени.
REXEC(TCP:514)	Daemon-служба удаленного выполнения команд.
RLOGIN(TCP:513)	Удаленная регистрация.
RTELNET(TCP:107)	Удаленный доступ через Telnet.

Табл. 41 Наиболее часто используемые службы

СЛУЖБА	ОПИСАНИЕ
RTSP(TCP/UDP:554)	Протокол (Real Time Streaming – Протокол воспроизведения в реальном времени) - это удаленное управление для мультимедиа в Интернете.
SFTP(TCP:115)	Простой протокол передачи файлов.
SMTP(TCP:25)	Simple Mail Transfer Protocol (Простой протокол электронной почты) – стандартный протокол обмена сообщениями для сети Интернет. SMTP обеспечивает пересылку сообщений с одного почтового сервера на другой.
SNMP(TCP/UDP:161)	Simple Network Management Program (Простой протокол управления сетью).
SNMP-TRAPS(TCP/UDP:162)	Система регистрации событий в потоке SNMP (RFC:1215).
SQL-NET(TCP:1521)	Structured Query Language (Язык структурированных запросов) представляет собой интерфейс для доступа к данным на различных типах систем баз данных, включая универсальные вычислительные машины, системы средней производительности, системы UNIX и сетевые серверы.
SSH(TCP/UDP:22)	Программа для обеспечения безопасной удаленной регистрации.
STRM WORKS(UDP:1558)	Протокол передачи потоков Stream Works.
SYSLOG(UDP:514)	Syslog (Системный журнал) позволяет отправлять системные журналы на сервер UNIX.
TACACS(UDP:49)	Login Host Protocol (Протокол регистрации узла), используется для TACACS (Terminal Access Controller Access Control System – Система управления доступом на основе контроллера доступа к терминалу).
TELNET(TCP:23)	Telnet – протокол регистрации и эмуляции терминала, общий для среды Интернет и UNIX. Он работает в сетях TCP/IP. Его главная функция заключается в обеспечении регистрации пользователей на удаленных узлах.
TFTP(UDP:69)	Trivial File Transfer Protocol (Упрощенный протокол передачи файлов) – это протокол передачи файлов в Интернет, подобный FTP, но использующий UDP (Протокол передачи дейтаграмм пользователя), а не TCP (Протокол управления передачей).
VDOLIVE(TCP:7000)	Еще одна программа для видеоконференций.

7.8 Окно QoS

Окно QoS по умолчанию позволяет автоматически назначать службе уровень приоритета в соответствии со значением поля ToS в IP-заголовке передаваемых пакетов.

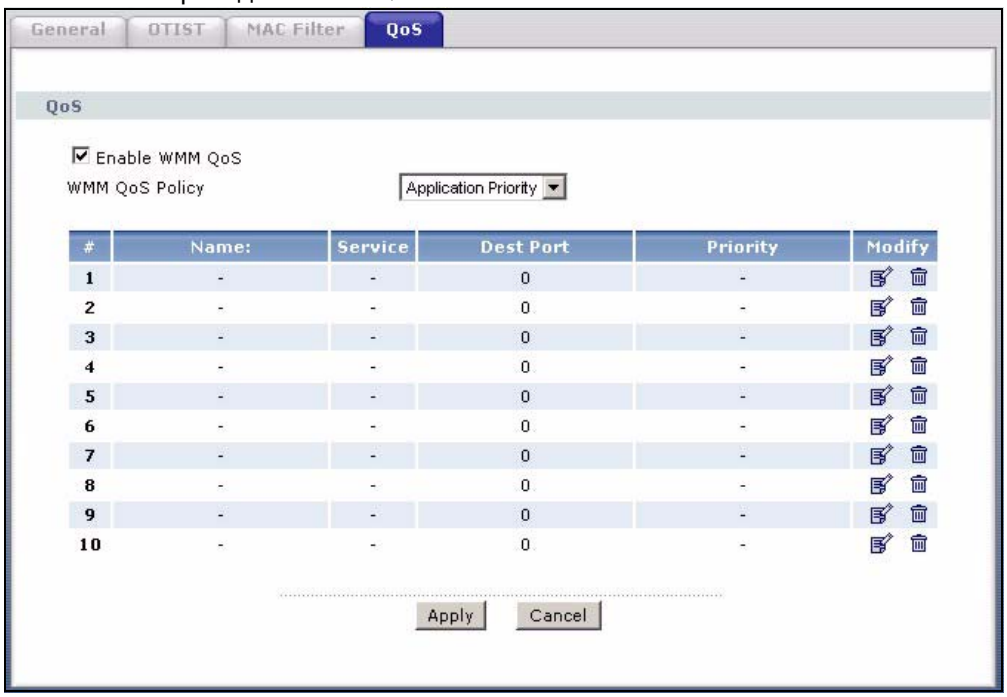
7.8.1 ToS и WMM QoS

ToS (Type of Service – Тип услуги) определяет поле DS (Differentiated Service – Дифференцированная служба) в IP-заголовке пакета. Значение ToS в исходящих пакетах находится интервале от 0 до 255. 0 означает самый низкий приоритет.

При использовании WMM QoS в заголовке передаваемых пакетов данных проверяется поле ToS. В результате приложению назначается приоритет в соответствии с числом в этом поле заголовка. Если значение ToS не указано, передаваемые данные обрабатываются как стандартный трафик или трафик с высоким приоритетом.

Щелкните **Network (Сеть)** > **Wireless LAN (Беспроводная локальная сеть)** > **QoS**. Появится следующее окно.

Рис. 76 Беспроводная сеть: QoS



В следующей таблице даны описания полей этого окна.

Табл. 42 Беспроводная сеть: QoS

ПОЛЕ	ОПИСАНИЕ
QoS (Качество услуг)	
Enable WMM QoS (Включить WMM QoS)	Поставьте флажок, чтобы включить функцию WMM QoS в P660HWP.
WMM QoS Policy (Политика WMM QoS)	Из раскрывающегося списка выберите **Default (По умолчанию)**, чтобы P660HWP автоматически назначал службе уровень приоритета в соответствии со значением поля ToS в IP-заголовке передаваемых пакетов. Выберите **Application Priority (Приоритет приложений)** для перехода к таблице, где отображается информация о названиях приложений, службах, портах и приоритетах для управления с помощью WMM QoS.
#	Это порядковый номер отдельной записи.
Name (Имя)	В этом поле отображается описание данной записи.
Service (Служба)	В этом поле отображается служба: **FTP**, **WWW**, **E-mail** или **User Defined (Определенная пользователем)**, к которой можно применить WMM QoS.

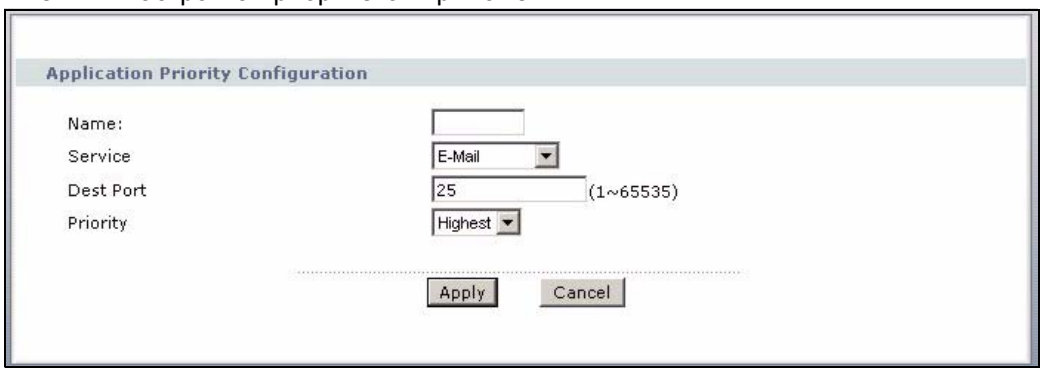
Табл. 42 Беспроводная сеть: QoS (продолжение)

ПОЛЕ	ОПИСАНИЕ
Dest Port (Порт назначения)	В этом поле отображается номер порта назначения, куда приложение отправляет трафик.
Priority (Приоритет)	В этом поле отображается приоритет WMM QoS для назначения трафику пропускной способности.
Modify (Изменить)	Открывает окно **Application Priority Configuration (Настройка приоритетов приложений)**. Внесите изменения в существующую запись или создайте новую запись в окне **Application Priority Configuration (Настройка приоритетов приложений)**. Для удаления записи щелкните по иконке **Remove (Удалить)**.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек P660HWP.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)** для восстановления предыдущей конфигурации в этом окне.

7.8.2 Настройка приоритетов приложений

Для изменения записи WMM QoS щелкните значок редактирования ( ) в столбце **Modify (Изменить)**. Появится следующее окно.

Рис. 77 Настройка приоритетов приложений



В следующей таблице даны описания полей этого окна.

Табл. 43 Настройка приоритетов приложений

ПОЛЕ	ОПИСАНИЕ
Application Priority Configuration (Настройка приоритетов приложений)	
Name (Имя)	Введите описание для приоритета приложения.

Табл. 43 Настройка приоритетов приложений (продолжение)

ПОЛЕ	ОПИСАНИЕ
Service (Служба)	Здесь представлено описание приложений, которым можно назначать приоритет с помощью WMM QoS.Выберите службу из выпадающего списка. • **FTP** Протокол передачи файлов позволяет осуществлять быструю передачу файлов, в том числе файлов большого размера, которые невозможно пересылать с помощью электронной почты. Служба FTP использует порт 21. • **E-Mail** Электронная почта позволяет передавать сообщения по компьютерной сети конкретному пользователю или группе пользователей. Существует несколько портов, используемых по умолчанию для электронной почты: POP3 – порт 110 IMAP – порт 143 SMTP – порт 25 HTTP – порт 80 • **WWW** Всемирная паутина (World Wide Web) – это система в Интернете, предназначенная для распространения графической и текстовой информации, связанной ссылками, на основе протокола передачи гипертекста (Hyper Text Transfer Protocol – HTTP). HTTP – это протокол типа клиент/сервер, разработанный для WWW. Система Web не является синонимом Интернет; точнее, она является одним из сервисов Интернета. Другими сервисами Интернета являются Интернет-чаты (глобальная система, посредством которой пользователи могут общаться друг с другом в реальном времени) и новостные группы (сетевая служба, рассылающая информацию по определенной теме). К службе Web можно подключиться с помощью браузера. • **User-Defined (Определенная пользователем)** Определяемые пользователем службы – это специальные службы пользователя, для их настройки требуется установить номер порта и соответствующее приложение.
Dest Port (Порт назначения)	Здесь отображается номер порта, который использует выбранная служба. Введите в поле номер порта, если необходимо использовать порт, отличный от порта по умолчанию. Информацию о номерах портов см. Табл. 41 на с. 139.
Priority (Приоритет)	Выберите приоритет из выпадающего списка.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек P660HWP.
Cancel (Отменить)	Щелкните «Cancel» (Отменить) для возврата к предыдущему окну без сохранения изменений.

8

Технология Powerline

В этой главе рассказывается об основных функциях и сферах применения технологии Powerline.

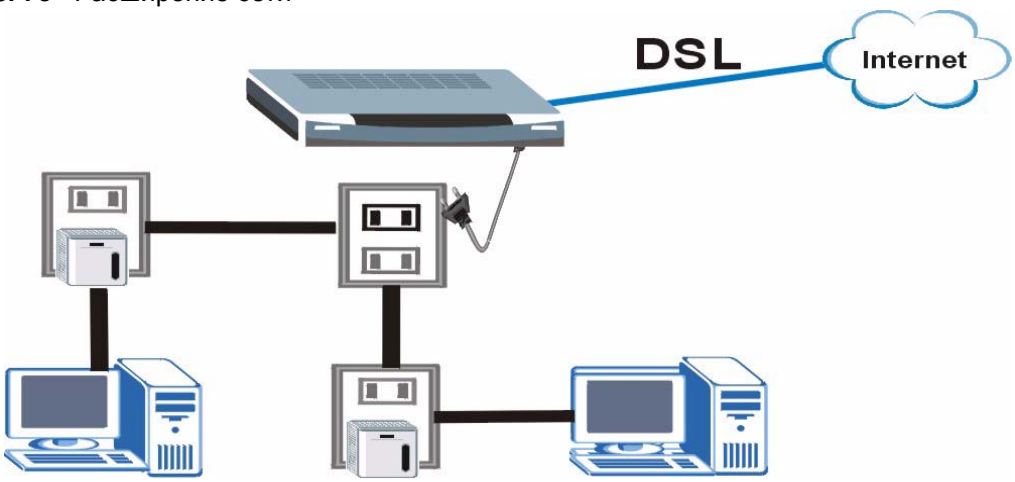
8.1 Обзор

Устройство P660HWP является адаптером стандарта HomePlug AV с интегрированным DSL-модемом. Устройство P660HWP может взаимодействовать с другими Powerline-адаптерами стандарта HomePlug AV путем передачи и получения информации через домашнюю электрическую сеть.

Подключив устройство P660HWP в обычную розетку, можно организовать новую сеть, доступ к которой можно получить из любой домашней розетки, даже если она находится другой комнате.

В следующем разделе приводится пример организации такой сети.

Рис. 78 Расширение сети



1. Подключите устройство P660HWP к сети Интернет.
2. Затем включите P660HWP в розетку и нажмите кнопку включения питания.

Теперь устройство P660HWP готово к организации Powerline-сети.

3. Подключите к компьютеру другой адаптер, поддерживающий стандарт HomePlug AV, и включите его в розетку той же домашней или офисной электрической линии.

После настройки всех адаптеров (см. Разд. 8.3 на с. 148 and Разд. 8.4 на с. 150) с компьютера можно выходить в Интернет через Powerline-сеть. Вы сможете легко расширить свою Powerline-сеть, подключая дополнительные Powerline-адаптеры другие розетки питания в доме и подключая к этим адаптерам другие компьютеры или сетевые устройства (например, принтеры).

Далее в данном руководстве сеть, организованная на основе электрической проводки, будет называться «Powerline-сетью».

8.2 Powerline-адаптеры и конфиденциальность информации

Для обеспечения конфиденциальности информации в сети, организованной P660HWP и другими Powerline-адаптерами HomePlug AV, применяется шифрование. Шифрование напоминает секретный код. Не зная кода нельзя прочесть сообщение. В стандарте HomePlug AV используется шифрование AES с длиной ключа 128 битов (Advanced Encryption Standard – улучшенный стандарт шифрования) для безопасной передачи данных между Powerline-адаптерами.

Чтобы P660HWP и другие Powerline-адаптеры могли взаимодействовать друг с другом, все они должны использовать одинаковый ключ членства в сети (NMK –Network Membership Key). В противном случае, они не смогут расшифровывать данные, передаваемые по Powerline-сети.

Ключ NMK генерируется на основе сетевого пароля, заданного вами для устройства P660HWP и Powerline-адаптеров. По умолчанию для всех Powerline-адаптеров HomePlug AV установлен сетевой пароль **HomePlugAV**. Это позволяет всем Powerline-адаптерам HomePlug AV и устройству P660HWP взаимодействовать друг с другом без каких-либо программных настроек. Однако, если не менять стандартный сетевой пароль, все адаптеры будут видеть данные, передаваемые в вашей сети.

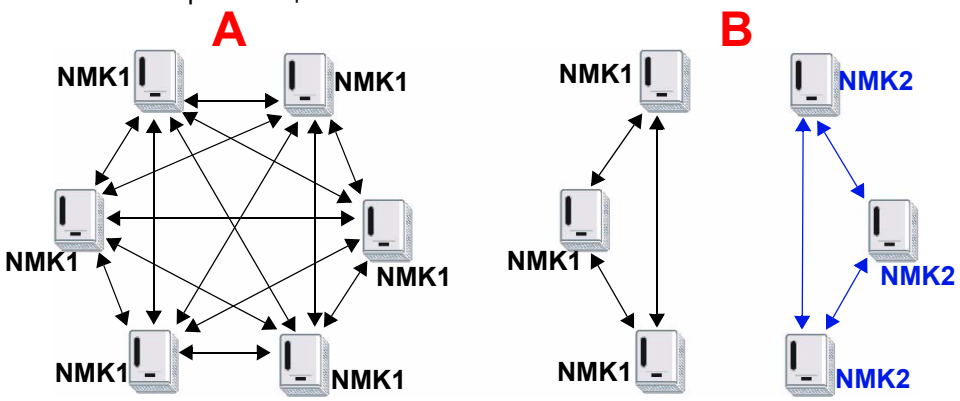
Поменяйте сетевой пароль на всех Powerline-адаптерах, чтобы обеспечить безопасность данных в Powerline-сети.

8.2.1 Организация частной Powerline-сети

Для предотвращения несанкционированного доступа, можно создать частную сеть. Для этого нужно поменять сетевой пароль на тех Powerline-адаптерах, которые должны в нее входить. Устройство P660HWP и другие Powerline-адаптеры преобразуют сетевой пароль в ключ членства в сети (NMK). Поэтому взаимодействовать в частной сети могут только устройства с одинаковыми NMK.

На следующем рисунке показаны две схемы организации Powerline-сети. На схеме **A** все Powerline-адаптеры имеют одинаковый ключ NMK (**NMK1**), а на схеме **B** одни адаптеры используют ключ **NMK1**, а другие – **NMK2**.

Рис. 79 Схема организации Powerline-сети



В обеих схемах адаптеры подключены к одной электрической цепи. В схеме **A** все адаптеры взаимодействуют друг с другом. В схеме **B** взаимодействовать между собой могут только адаптеры с одинаковыми ключами NMK.

8.2.2 Организация нескольких Powerline-сетей.

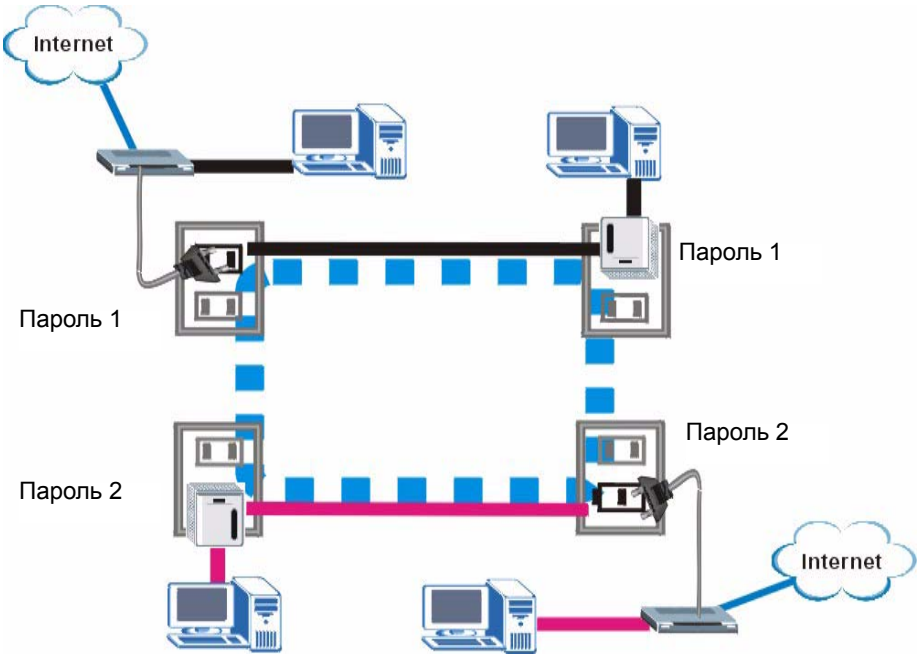
В одной Powerline-сети можно организовать несколько локальных сетей. В небольшом офисе можно создать множество Powerline-сетей при наличии в нем двух отдельных сетей Ethernet.

Подключите один Powerline-адаптер к маршрутизатору или коммутатору первой сети Ethernet и назначьте этому адаптеру пароль (например, «Password1»). Подключите дополнительные Powerline-адаптеры к электрическим розеткам и назначьте им тот же пароль «Password1». На этом настройка первой локальной сети Powerline завершена.

Подключите другой Powerline-адаптер к маршрутизатору или коммутатору второй сети Ethernet и назначьте этому адаптеру другой пароль (например, «Password2»). Подключите дополнительные Powerline-адаптеры к электрическим розеткам и назначьте им пароль «Password2».

Таким образом, в одной сети Powerline организовано две частных локальных сети. Информация между этими сетями не передается, так как взаимодействовать друг с другом могут только Powerline-адаптеры с одинаковым паролем. Схема такой сети показана на следующем рисунке.

Рис. 80 Две частных Powerline-сети в одной электрической цепи



8.3 Настройка локальных параметров

Для ввода сетевого пароля организуемой сети откройте окно **Local Setting (Локальные параметры)**. В этом же окне в поле **Device Access Key (Ключ доступа к устройству)** можно изменить ключ доступа к сети для устройства P660HWP.

Для доступа к параметрам локальной станции щелкните пункт **Network (Сеть)** > **Powerline**.

Рис. 81 Сеть > Powerline > Локальные параметры

В следующей таблице даны описания полей этого окна.

Табл. 44 Сеть > Powerline > Локальные параметры

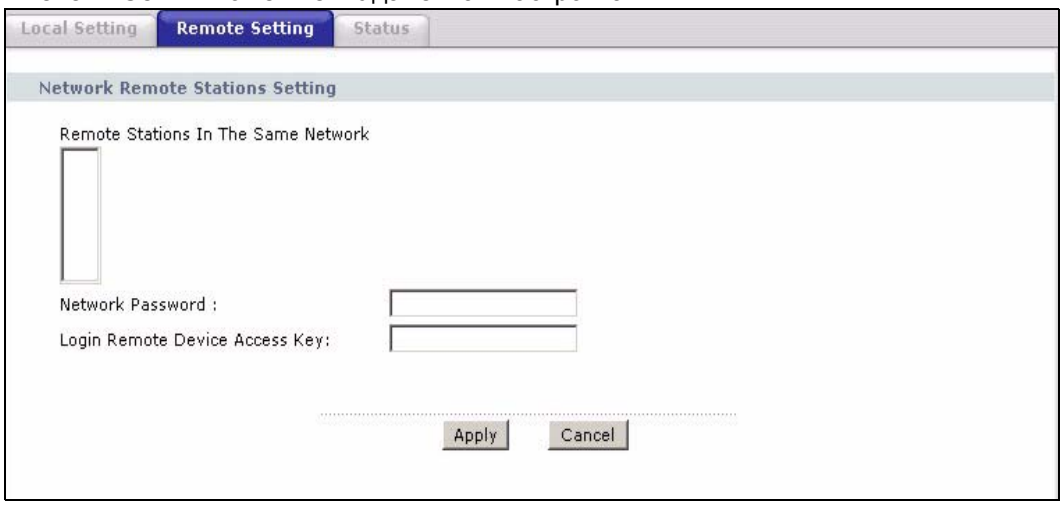
ПОЛЕ	ОПИСАНИЕ
Network Local Station Setting (Параметры сети и локальной станции)	В этом разделе производится настройка адаптера HomePlug AV, используемого для подключения к Powerline-сети.
Enable Powerline (Использовать функцию Powerline)	Позволяет активировать функцию Powerline на вашем устройстве. Она позволяет организовать взаимодействие с другими Powerline-адаптерами через обычные розетки электрической сети.
Network Password (Сетевой пароль)	Сетевой пароль, используемый Powerline-адаптерами для идентификации устройств в Powerline-сети. По умолчанию, в качестве **сетевого пароля** в устройстве P660HWP используется строка **HomePlugAV**. Для взаимодействия с другими адаптерами устройство P660HWP должно использовать одинаковый с ними сетевой пароль. Если изменить пароль в каком-либо устройстве сети, это устройство больше не будет распознаваться как часть этой сети. Если вы захотите поменять **сетевой пароль**, его нужно менять на всех адаптерах, которые должны входить в одну сеть. Длина сетевого пароля составляет от 1 до 64 буквенно-цифровых символов. Пробелы не допускаются.
Device Access Key (Ключ доступа к устройству)	**Ключ доступа к устройству (DAK)** – это пароль, необходимый для внесения изменений в настройки устройства. Пароль DAK указывается на наклейке на нижней панели адаптера HomePlug. Не обязательно вводить пароль **DAK** для доступа у устройству P660HWP, но для повышения безопасности рекомендуется сменить этот **DAK**.
Mask Network Password and Device Access Key (Пароль маскирования сети и ключ доступа к устройству)	Позволяет маскировать **сетевой пароль** и **DAK** при вводе.
Local Station MAC Address (MAC-адрес локальной станции)	Это уникальный идентифицирующий адрес устройства, который вы используете для настройки сети.
Apply (Применить)	Нажмите кнопку, чтобы применить изменения. В результате будут установлены новый **сетевой пароль** и **DAK** для P660HWP. **Примечание: Необходимо ввести правильный ключ доступа к устройству (DAK) для выбранного Powerline-адаптера, прежде чем можно будет его изменить.**
Cancel (Отменить)	Эта кнопка используется для отмены сделанных изменений.

8.4 Удаленная настройка параметров

Это окно используется для доступа к другим Powerline-адаптерам в сети. Эти адаптеры можно настраивать, добавлять или удалять из сети.

Для доступа и настройки адаптеров щелкните пункт **Network (Сеть)** > **Powerline** > **Remote Settings (Удаленная настройка)**.

Рис. 82 Сеть > Powerline > Удаленная настройка



В следующей таблице даны описания полей этого окна.

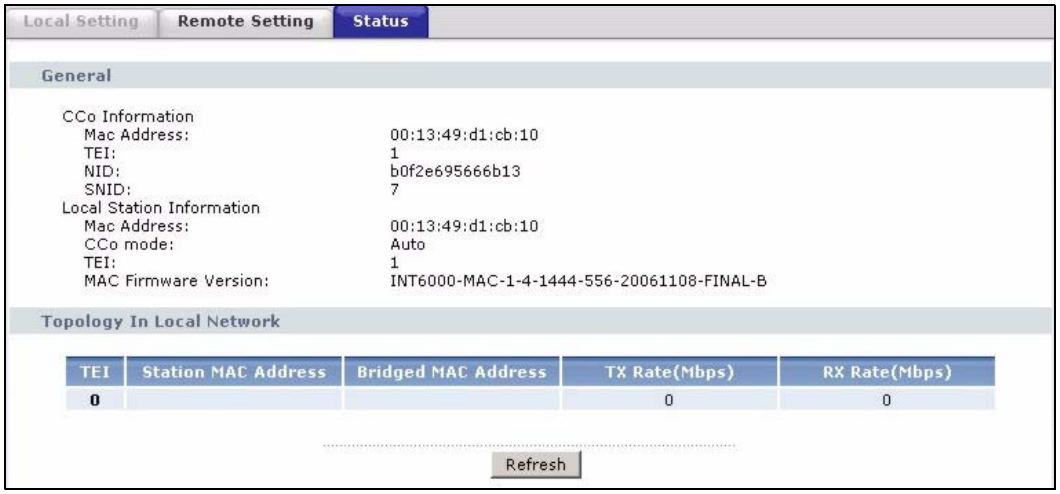
Табл. 45 Сеть > Powerline > Удаленная настройка

ПОЛЕ	ОПИСАНИЕ
Network Remote Stations Setting (Настройка удаленных сетевых станций)	В этом разделе описывается конфигурация других адаптеров HomePlug AV в Powerline-сети.
Remote Stations In The Same Network (Удаленные станции одной сети)	В этом разделе отображаются MAC-адреса адаптеров HomePlug AV в вашей сети. Эти адаптеры используют общий сетевой пароль, установленный в разделе **Local Settings (Локальные параметры)**. Для настройки одного из адаптеров выберите его MAC-адрес и укажите Powerline-сеть.
Network Password (Сетевой пароль)	Введите для выбранного адаптера новый сетевой пароль. Он должен отличаться от стандартного пароля **HomePlugAV**.
Login Remote Device Access Key (Ключ доступа для регистрации на удаленном устройстве)	Введите для выбранного устройства **ключ доступа**. Этот **ключ** написан на самом устройстве.
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы установить новый **сетевой пароль**. MAC-адрес этого устройства не будет отображаться в списке до тех пор, пока не будут изменены **сетевые пароли** на остальных устройствах.
Cancel (Отменить)	Эта кнопка используется для отмены сделанных изменений.

8.5 Состояние Powerline-сети

Это окно используется для проверки состояния Powerline-сети и квалифицированной диагностики неисправностей. Выберите пункт **Network (Сеть)** > **Powerline** > **Status (Состояние)** для получения подробной информации о состоянии Powerline-сети.

Рис. 83 Сеть > Powerline > Состояние



В следующей таблице даны описания полей этого окна.

Табл. 46 Сеть > Powerline > Состояние

ПОЛЕ	ОПИСАНИЕ
General (Общие)	В этом разделе приводится общая информация о вашей сети, которая может оказаться полезной при поиске и устранении неисправностей.
CCo Information (Информация центрального координатора)	Аббревиатура **«CCo»** расшифровывается, как **«Central Coordinator» (Центральный координатор)**. Центральным координатором сети Powerline называется Powerline-адаптер, отслеживающий остальные устройства сети и синхронизирующий их взаимодействие. Адаптеры в сети Powerline автоматически выбирают центрального координатора.
MAC Address (MAC-адрес)	MAC-адрес центрального координатора в сети Powerline. MAC-адрес Powerline-адаптера указывается на этикетке устройства. Он состоит из 6 пар шестнадцатеричных символов (включает цифры «0-9» и буквы «a-f»). Для адаптера P660HWP этикетка находится на нижней панели устройства.
TEI	Аббревиатура **«TEI»** расшифровывается, как **«Terminal Equipment Identifier» (Идентификатор оборудования терминала)**. В данном случае этим номером обозначается **CCo** в Powerline-сети.
NID	Аббревиатура **«NID»** расшифровывается, как **«Network Identifier» (Идентификатор сети)**. Этим номером обозначается сеть с общим паролем.
SNID	Аббревиатура **«SNID»** расшифровывается, как **«Short Network Identifier» (Короткий идентификатор сети)**. Это короткая форма **NID**.
Local Station Information (Информация о локальной станции)	В этом разделе приводится информация по адаптеру (P660HWP), который используется для выхода в Powerline-сеть.
MAC Address (MAC-адрес)	MAC-адрес **локальной станции**. MAC-адрес адаптера указывается на наклейке на нижней панели устройства.

ПОЛЕ	ОПИСАНИЕ
CCo Mode (Режим центрального координатора)	**Центральный координатор** может работать в следующих режимах: **Auto (Автоматический)**, **Always (Постоянно включен)** или **Never (Отключен)**. Эти режимы доступны только для чтения и не могут быть изменены пользователем.
TEI	Аббревиатура **«TEI»** расшифровывается, как **«Terminal Equipment Identifier» (Идентификатор оборудования терминала)**. В данном случае этим номером обозначается P660HWP в Powerline-сети.
MAC Firmware Version (Версия микропрограммы)	В этом поле отображается информация о производителе набора микросхем и номер версии микросхемы.
Topology in Local Network (Топология локальной сети)	В этом разделе описывается организация сети Powerline.
TEI	Этим номером обозначается один из адаптеров в сети Powerline.
Station MAC Address (MAC-адрес станции)	В этом поле отображается MAC-адрес адаптера в вашеей Powerline-сети.
Bridged MAC Address (MAC-адрес для установки соединения типа «мост»)	Устройство P660HWP может подключаться к Ethernet-сети, например, локальной сети или Интернет. При этом через P660HWP может быть организован выход из Powerline-сети в Ethernet-сеть. Таким образом, указанный **MAC-адрес** используется устройством P660HWP для подключения Powerline-сети к сети Ethernet и сети Ethernet к Powerline-сети.
Tx Rate (Скорость передачи)	Это скорость, с которой **локальная станция** передает данные другому адаптеру в сети Powerline**.** Скорость отображается в следующем формате: «скорость передачи данных приложения/ скорость передачи двоичных данных». Данные на уровне приложения более точно отображают скорость передачи трафика между устройствами для данного приложения (напр., трафик IP (Internet Protocol – Протокол Интернета). Данные на физическом уровне показывают количество полезной информации в пакетах, передаваемых по Powerline-сети.
Rx Rate (Скорость приема)	Это скорость, с которой **локальная станция** принимает данные от другого адаптера в сети Powerline**.** Скорость отображается в следующем формате: «скорость передачи данных приложения/ скорость передачи двоичных данных». Данные на уровне приложения более точно отображают скорость передачи трафика между устройствами для данного приложения (напр., трафик IP (Internet Protocol – Протокол Интернета). Данные на физическом уровне показывают количество полезной информации в пакетах, передаваемых по Powerline-сети.
Refresh (Обновить)	Кнопка **Refresh (Обновить)** позволяет обновить информацию на экране.

9

Трансляция сетевых адресов (NAT)

В этой главе рассказывается, как настроить функцию NAT в P660HWP.

9.1 Обзор NAT

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

9.1.1 Определения NAT

«Внутренний/внешний» означает расположение узла относительно P660HWP, например, компьютеры ваших абонентов являются внутренними узлами, тогда как web-серверы Интернета являются внешними узлами.

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

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

Табл. 47 Определения NAT

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

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

9.1.2 Назначение NAT

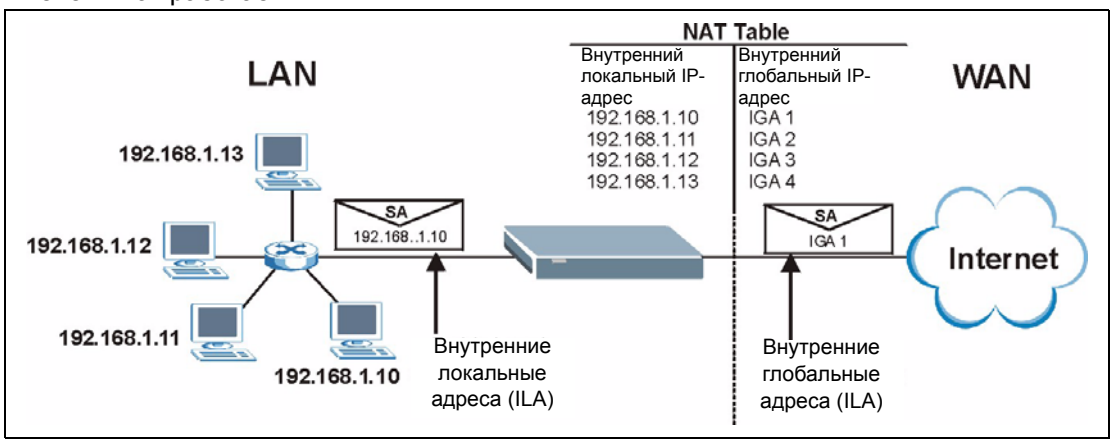
В простейшем случае NAT изменяет IP-адрес источника в пакете, принятом от абонента (внутренний локальный адрес) на другой (внутренний глобальный адрес) перед передачей пакета в глобальную сеть. При получении ответа NAT преобразовывает адрес получателя (внутренний глобальный адрес) обратно во внутренний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

Глобальные IP-адреса внутренних узлов могут быть статическими, или могут динамически назначаться Интернет-провайдером. Кроме того, вы можете определить серверы, например, web-сервер и сервер Telnet, находящиеся в вашей локальной сети, и сделать их доступными для внешних пользователей. Если вы не определили серверы (с отображением «много-к-одному» и «много-ко-многим с перегрузкой» – см. Табл. 48 на с. 156), NAT предлагает дополнительное преимущество защиты сети с помощью межсетевого экрана. Если серверы не установлены, P660HWP отфильтровывает все входящие запросы, таким образом предотвращая зондирование вашей сети злоумышленниками. Дополнительные сведения о трансляции IP-адресов см. в *RFC 1631*, «*Трансляция сетевых IP-адресов (NAT)*».

9.1.3 Как работает NAT

Каждый пакет имеет два адреса – адрес источника и адрес назначения. Для исходящих пакетов, внутренний локальный адрес (ILA) является адресом источника в локальной сети, а внутренний глобальный адрес (IGA) – адресом источника в глобальной сети. Для входящих пакетов, ILA – это адрес получателя в локальной сети, а IGA – адрес получателя в глобальной сети. NAT преобразовывает частные (локальные) IP-адреса в уникальные глобальные, что необходимо для связи с узлами в других сетях. NAT заменяет исходный IP-адрес источника (и номера портов источника TCP или UDP на отображение «много-к-одному» и «много-ко-многим с перегрузкой») в каждом пакете и затем пересылает его в Интернет. P660HWP отслеживает оригинальные адреса и номера портов, и, таким образом, во входящих ответных пакетах восстанавливаются исходные значения. Применение фильтров показано на следующем рисунке.

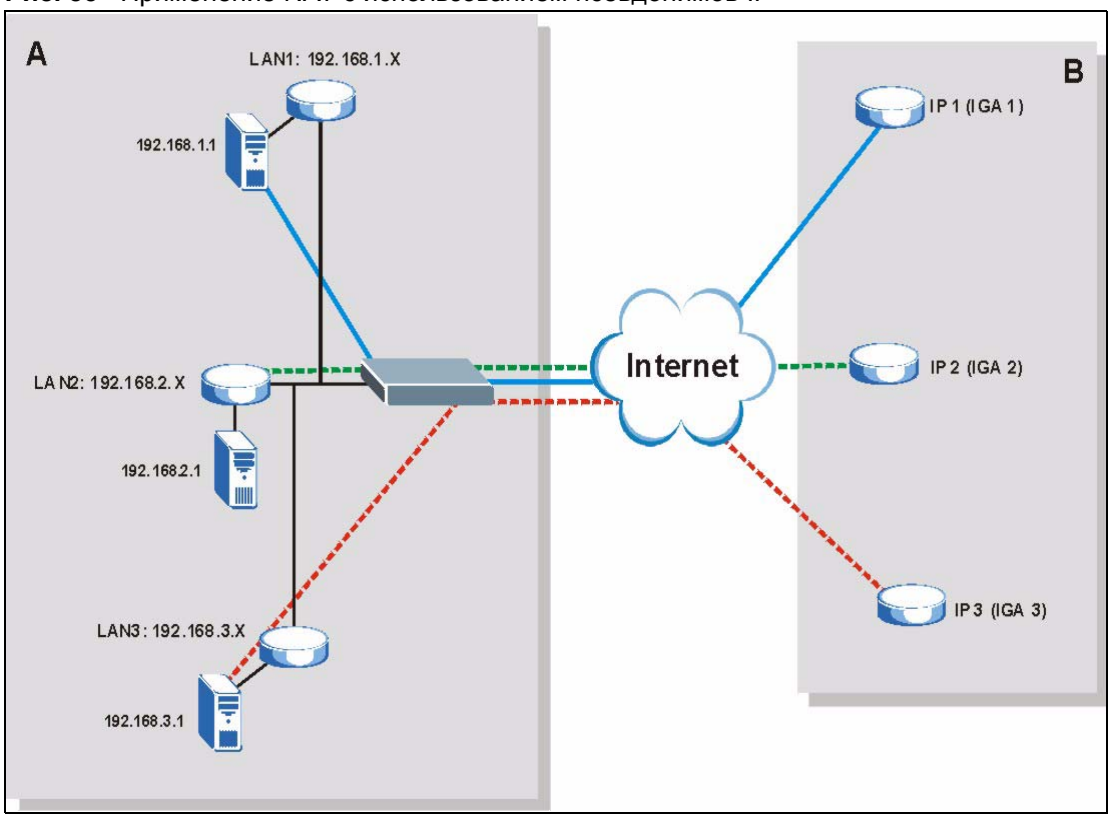
Рис. 84 Как работает NAT



9.1.4 Применение NAT

На следующем рисунке приведен вариант применения NAT, где три внутренних локальных сети (логические локальные сети, образованные с помощью псевдонимов IP), расположенные за P660HWP, взаимодействуют с тремя различными глобальными сетями. Дополнительные примеры приведены в конце данной главы.

Рис. 85 Применение NAT с использованием псевдонимов IP



9.1.5 Типы отображения NAT

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

- **Один к одному**: в режиме **One-to-one (Один-к-одному)** P660HWP преобразовывает один локальный IP-адрес в один глобальный IP-адрес.
- **Много-к-одному**: в режиме **Many-to-One (Много-к-одному)** P660HWP преобразовывает несколько локальных IP-адресов в один глобальный IP-адрес. Эта функция эквивалентна SUA (например, PAT, Port Address Translation – Преобразование адресов портов), т. е. функции ZyXEL «Учетная запись одиночного пользователя», которая поддерживалась в предыдущих моделях маршрутизаторов ZyXEL (опция **SUA Only (Только SUA)** в современных маршрутизаторах).
- **Много-ко-многим с перегрузкой**: в этом режиме P660HWP преобразовывает несколько локальных IP-адресов в несколько общих глобальных IP-адресов.
- **Много-ко-многим без перегрузки**: в этом режиме P660HWP преобразовывает каждый локальный IP-адрес в уникальный глобальный IP-адрес.

- **Сервер**: этот режим позволяет установить внутренние серверы для различных служб, расположенных за NAT, и сделать их доступными для внешних пользователей.

Номера портов НЕ изменяются при использовании типов отображения NAT **One-to-one (Один-к-одному)** и **Many-to-Many No Overload (Много-ко-многим без перегрузки)**.

В следующей таблице приведена сводная информация о типах NAT.

Табл. 48 Типы отображения NAT

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

9.2 SUA (Учетная запись одиночного пользователя) в сравнении с NAT

SUA (Single User Account – Учетная запись одиночного пользователя) – это реализация в операционной системе ZyNOS подмножества NAT, которое поддерживает два типа отображения: **Many-to-One (Много-к-одному)** и **Server (Сервер)**. Кроме того, P660HWP поддерживает преобразование типа **Full Feature (Полный набор функций)**, что обеспечивает преобразование нескольких глобальных IP-адресов в несколько частных локальных IP-адресов клиентов или серверов с использованием типов преобразования согласно Табл. 48 на с. 156.

- Выберите **SUA Only (Только SUA)**, если P660HWP имеет только один общедоступный IP-адрес в глобальной сети.
- Выберите **Full Feature (Полный набор функций)**, если P660HWP имеет несколько общедоступных IP-адресов в глобальной сети.

9.3 Шлюз SIP ALG

Некоторые приложения, например, SIP, не могут работать через NAT (не поддерживают NAT), так как вставляют IP-адреса и номера портов в свои пакеты данных.

Некоторые NAT маршрутизаторы могут включать функцию SIP ALG (Session Initialization Protocol Application Layer Gateway – встроенный программный шлюз для приложений, использующих протокол SIP). Шлюз прикладного уровня (ALG – Application Layer Gateway) управляет специальным протоколом (например, SIP, H.323 или FTP) на уровне приложений.

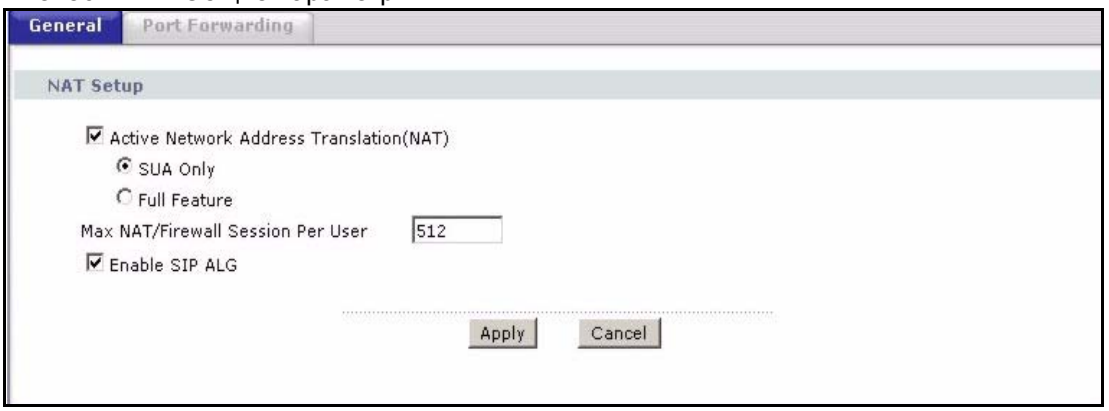
SIP ALG позволяет вызовам SIP проходить через NAT с помощью анализа и преобразования IP-адресов, содержащихся в потоке данных.

Когда P660HWP регистрируется в сервере SIP, шлюз SIP ALG производит преобразование частного IP-адреса P660HWP внутри потока данных SIP в общедоступный IP-адрес. При этом не требуется использовать STUN или исходящий прокси-сервер, если P660HWP находится за шлюзом SIP ALG.

9.4 Настройка общих параметров NAT

Чтобы разрешить прохождение трафика из глобальной сети через P660HWP, необходимо в дополнение к SUA/NAT создать правило межсетевого экрана. Щелкните **Network (Сеть)** > **NAT** для отображения следующего окна.

Рис. 86 NAT: Общие параметры



В следующей таблице даны описания полей этого окна.

Табл. 49 NAT: Общие параметры

ПОЛЕ	ОПИСАНИЕ
Active Network Address Translation (NAT) (Включить трансляцию сетевых адресов)	Поставьте флажок в этом поле, чтобы включить NAT.
SUA Only (Только SUA)	Выберите эту опцию, если P660HWP имеет только один общедоступный IP-адрес в глобальной сети.
Full Feature (Полный набор функций)	Выберите эту опцию, если P660HWP имеет несколько общедоступных IP-адресов в глобальной сети.

Табл. 49 NAT: Общие параметры (продолжение)

ПОЛЕ	ОПИСАНИЕ
Max NAT/Firewall Session Per User (Макс. кол-во сеансов NAT / межсетевой экран для одного пользователя)	Когда компьютеры используют равноправное соединение (без выделенного сервера), например, совместное использование файла, они должны устанавливать сеансы NAT. Если не ограничить количество сеансов, устанавливаемых одним клиентом, это может привести к тому, что все доступные сеансы NAT будут использованы. В таком случае, другие пользователи не смогут установить сеансы NAT и, следовательно, получить доступ в Интернет. При каждом сеансе NAT устанавливается соответствующий сеанс межсетевого экрана. Это поле предназначено для ограничения количества сеансов NAT / межсетевого экрана, которые каждый клиентский компьютер может устанавливать через P660HWP. Если в вашей сети небольшое количество пользователей использует равноправные приложения, это число можно увеличить, чтобы не снижать качество обслуживания из-за ограничения доступных каждому клиенту сеансов NAT. Если в сети большое число пользователей использует равноправные приложения, это число следует уменьшить, чтобы не допустить ситуации, когда один клиент занимает все доступные сеансы NAT.
Enable SIP ALG (Включить SIP ALG)	Установите флажок для корректной работы SIP (VoIP) с правилами переадресации и переключения портов.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек P660HWP.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)** для восстановления предыдущей конфигурации в этом окне.

9.5 Переадресация портов

Набор переадресации портов – это список внутренних серверов (расположенных в локальной сети за NAT), например, web или FTP, которые можно сделать видимыми для внешних пользователей, несмотря на то, что NAT представляет всю внутреннюю сеть для внешних пользователей, как одиночный компьютер.

Можно ввести либо номер одного порта, либо диапазон номеров портов, подлежащих пересылке, и локальный IP-адрес требуемого сервера. Номер порта определяет службу, например, служба web использует порт 80, а FTP – порт 21. В некоторых случаях, когда служба неизвестна или один сервер поддерживает более одной службы (например, FTP и web), лучше указать диапазон номеров портов. Вы можете назначить IP-адрес сервера, который соответствует порту или диапазону портов.

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

9.5.1 IP-адрес сервера по умолчанию

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

Если серверу по умолчанию не назначен IP-адрес, P660HWP сбрасывает все пакеты, принятые для портов, которые не указаны здесь или в настройках удаленного управления.

9.5.2 Переадресация портов: Службы и номера портов

Окно **Port Forwarding (Переадресация портов)** служит для направления входящих запросов служб на соответствующие сервер(ы) локальной сети.

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

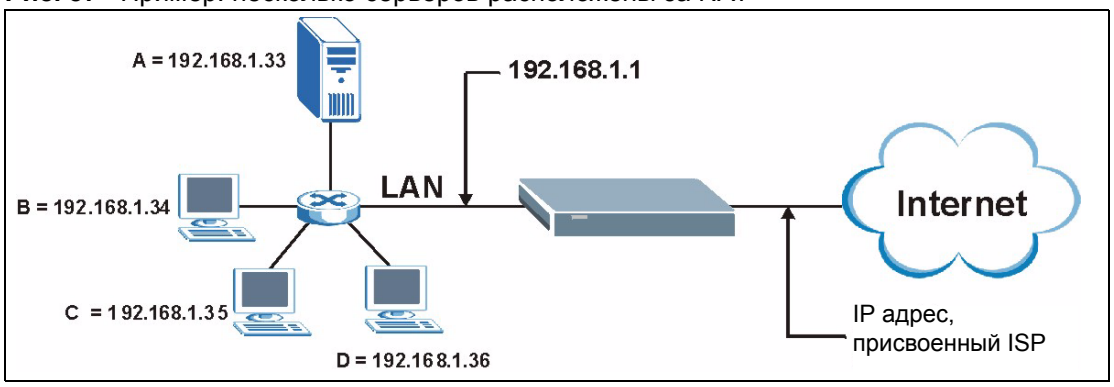
Табл. 50 Службы и номера портов

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

9.5.3 Пример настройки серверов, расположенных после преобразования портов

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

Рис. 87 Пример: несколько серверов расположены за NAT



9.6 Настройка переадресации портов

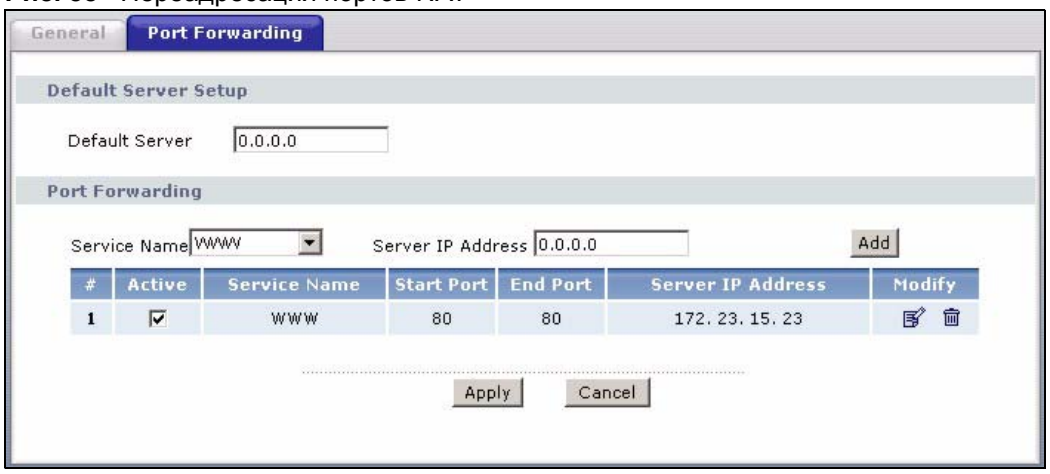
Окно Port Forwarding (Переадресация портов) доступно, только если установлен режим SUA Only (Только SUA) в окне NAT > General (Общие настройки).

Если серверу по умолчанию не назначен IP-адрес, P660HWP сбрасывает все пакеты, принятые для портов, которые не указаны здесь или в настройках удаленного управления.

Щелкните **Network (Сеть)** > **NAT** > **Port Forwarding (Переадресация портов)** для отображения следующего окна.

Информацию по номерам портов, обычно используемых для конкретных служб см. Табл. 50 на с. 159.

Рис. 88 Переадресация портов NAT



В следующей таблице даны описания полей этого окна.

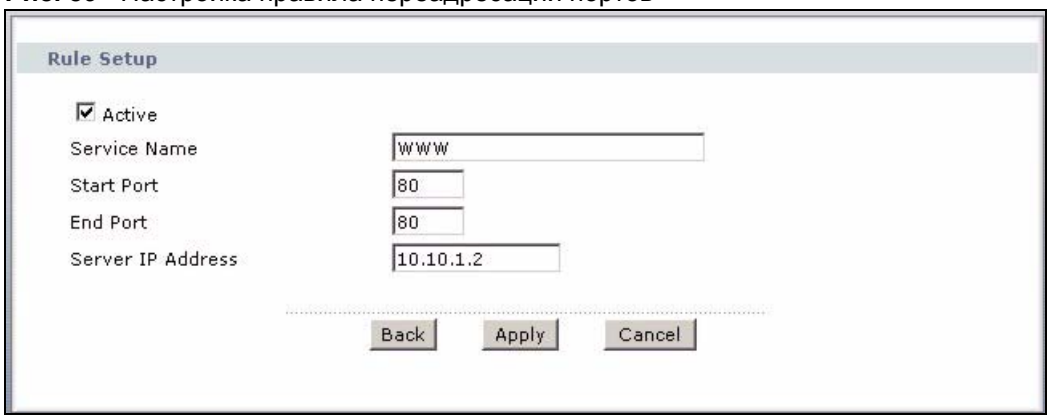
Табл. 51 Переадресация портов NAT

ПОЛЕ	ОПИСАНИЕ
Default Server Setup (Настройка сервера по умолчанию)	
Default Server (Сервер по умолчанию)	Кроме серверов определенных видов служб NAT поддерживает сервер по умолчанию. Сервер по умолчанию принимает пакеты от портов, которые не указаны в представленной ниже таблице. Если **серверу по умолчанию** не назначен IP-адрес, P660HWP сбрасывает все пакеты, принятые для портов, которые не указаны здесь или в настройках удаленного управления.
Port Forwarding (Переадресация портов)	
Service Name (Имя услуги)	Выберите службу из выпадающего списка.
Server IP Address (IP-адрес сервера)	Введите IP-адрес сервера для данной службы.
Add (Добавить)	Щелкните по этой кнопке, чтобы добавить в таблицу новое правило.
#	Это порядковый номер правила (только для чтения).
Active (Активировать)	Поставьте флажок для включения правила.
Service Name (Имя услуги)	Здесь отображается имя услуги.
Start Port (Начальный порт)	Это номер первого порта, определяющего службу.
End Port (Последний порт)	Это номер последнего порта, определяющего службу.
Server IP Address (IP-адрес сервера)	Это IP-адрес сервера.
Modify (Изменить)	Щелкните по иконке редактирования для перехода к окну, где можно изменить параметры правила переадресации портов. Щелкните по иконке удаления, чтобы удалить существующее правило переадресации портов. Следует отметить, что при удалении правила все последующие правила сдвигаются на позицию вверх.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек P660HWP.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы вернуться к предыдущей конфигурации.

9.6.1 Изменение правила переадресации портов

Для внесения изменений в правило переадресации портов щелкните по иконке редактирования в строке правила в окне **Port Forwarding (Переадресация портов)**. Появится следующее окно.

Рис. 89 Настройка правила переадресации портов



В следующей таблице даны описания полей этого окна.

Табл. 52 Настройка правила переадресации портов

ПОЛЕ	ОПИСАНИЕ
Active (Активировать)	Поставьте флажок для включения правила.
Service Name (Имя услуги)	Введите имя для описания правила переадресации портов.
Start Port (Начальный порт)	Введите в это поле номер порта. Для переадресации трафика только одного порта введите его номер еще раз в поле **End Port (Последний порт)**. Для переадресации трафика серии портов введите в это поле номер первого порта, а в поле **End Port (Последний порт)** – номер последнего порта.
End Port (Последний порт)	Введите в это поле номер порта. Для переадресации трафика только одного порта, введите его номер в поле **Start Port (Начальный порт)**, а затем введите этот же номер еще раз в это поле. Для переадресации трафика серии портов введите номер последнего порта серии портов, которая начинается с номера порта, установленного в поле **Start Port (Начальный порт)**.
Server IP Address (IP-адрес сервера)	Введите в это поле внутренний IP-адрес сервера.
Back (Назад)	Для возврата к предыдущему окну нажмите кнопку **Back (Назад)**.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек P660HWP.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.

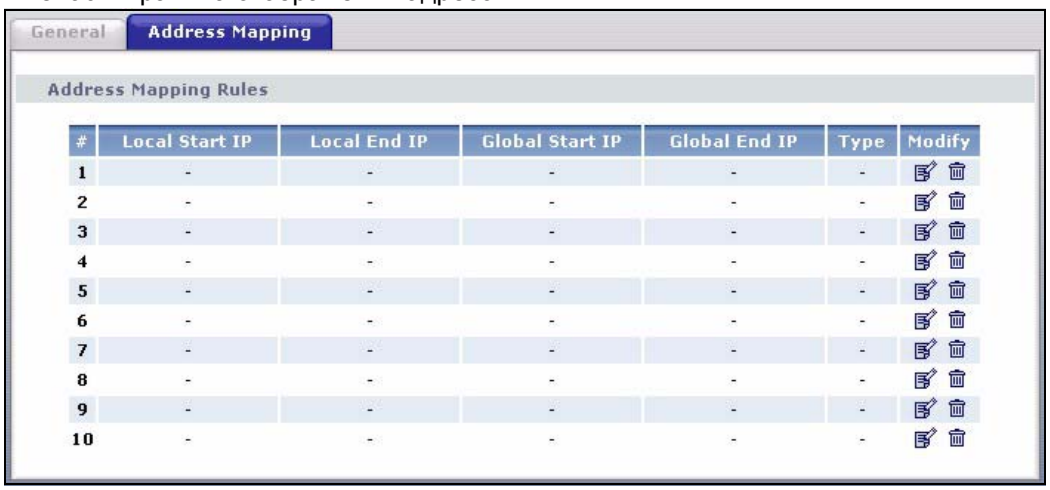
9.7 Отображение адресов

Окно Address Mapping (Отображение адресов) доступно, только если установлен режим Full Feature (Полный набор функций) в окне NAT > General (Общие настройки).

Порядок следования правил имеет большое значение, так как P660HWP применяет правила в установленном порядке. Когда текущий пакет соответствует какому-либо правилу P660HWP выполняет соответствующее действие и игнорирует остальные правила. Если в таблице существуют пустые правила перед новым создаваемым правилом, это правило перемещается вверх на количество позиций, равное числу пустых правил. Например, вы уже настроили правила с 1-го по 6-е в текущем наборе и теперь хотите настроить правило 9. В общем окне набора правил новое правило будет иметь номер 7, но не 9. Теперь, если удалить правило 4, то правила с 5-го по 7-е переместятся вверх на 1 позицию, так что старые правила 5, 6 и 7 будут иметь номера 4, 5 и 6.

Для изменения в P660HWP параметров отображения адресов, щелкните **Network (Сеть)** > **NAT** > **Address Mapping (Отображение адресов)**. Появится следующее окно.

Рис. 90 Правила отображения адресов



В следующей таблице даны описания полей этого окна.

Табл. 53 Правила отображения адресов

ПОЛЕ	ОПИСАНИЕ
#	Это порядковый номер правила.
Local Start IP (Начальный локальный IP-адрес)	Это начальный внутренний локальный IP-адрес (начальный ILA). Локальные IP-адреса недоступны (**N/A**) для типа отображения портов **Server (Сервер)**.
Local End IP (Конечный локальный IP-адрес)	Это конечный внутренний локальный IP-адрес (ILA). Если правило предназначено для всех локальных IP-адресов, то в поле **Local Start IP (Начальный локальный IP-адрес)** отображается 0.0.0.0, а в поле **Local End IP (Конечный локальный IP-адрес)** отображается 255.255.255.255. В этом поле отображается **N/A (Не применяется)** для типов отображения **One-to-one (Один-к-одному)** и **Server (Сервер)**.
Global Start IP (Начальный глобальный IP-адрес)	Это начальный внутренний глобальный IP-адрес (IGA). Если вы используете динамический IP-адрес, назначаемый Интернет-провайдером, введите в это поле 0.0.0.0. В этом случае используются только отображения **много-к-одному** и **сервер**.
Global End IP (Конечный глобальный IP-адрес)	Это конечный внутренний глобальный IP-адрес (IGA). В этом поле отображается **N/A (Не применяется)** для типов отображения **One-to-one (Один-к-одному)**, **Many-to-One (Много-к-одному)** и **Server (Сервер)**.

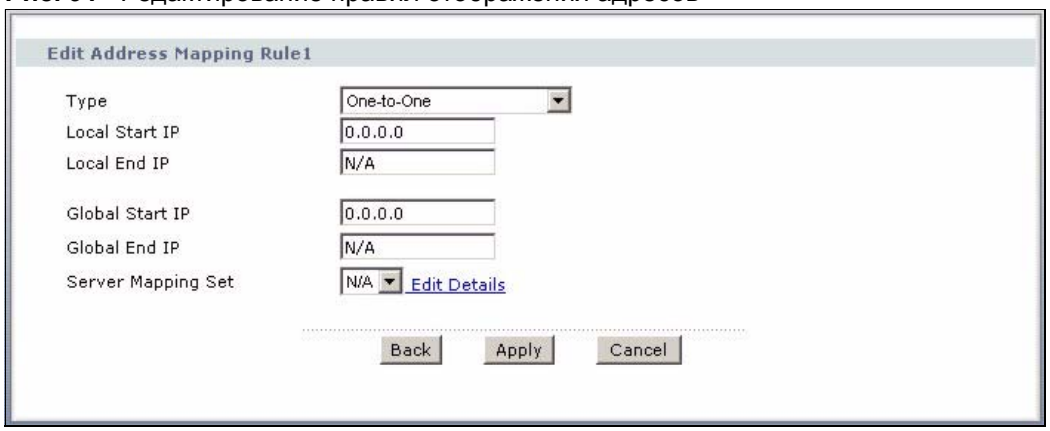
Табл. 53 Правила отображения адресов (продолжение)

ПОЛЕ	ОПИСАНИЕ
Type (Тип)	**1-1**: в режиме **One-to-one (Один-к-одному)** один локальный IP-адрес отображается на один глобальный IP-адрес. Следует отметить, что в данном режиме отображения NAT номера портов не изменяются. **M-1**: в режиме **Many-to-One (Много-к-одному)** несколько локальных IP-адресов отображаются на один глобальный IP-адрес. Этот режим аналогичен SUA (т.е., PAT, port address translation – преобразование адресов портов) – функции ZyXEL «Учетная запись одиночного пользователя», которую поддерживали предыдущие модели маршрутизаторов ZyXEL. **M-M Ov (Overload)**: в режиме **Many-to-Many Overload (Много-ко-многим с перегрузкой)** несколько локальных IP-адресов отображаются на несколько общих глобальных IP-адресов. **MM No (No Overload)**: в режиме **Many-to-Many No Overload (Много-ко-многим без перегрузки)** каждый локальный IP-адресов отображается на уникальный глобальный IP-адрес. **Server (Сервер)**: этот режим позволяет установить внутренние серверы для различных служб, расположенных за NAT, и сделать их доступными для внешних пользователей.
Modify (Изменить)	Щелкните по иконке редактирования для перехода к окну, где можно изменить правило отображения адресов. Щелкните по иконке удаления, чтобы удалить существующее правило отображения портов. Следует отметить, что при удалении правила все последующие правила сдвигаются на позицию вверх.

9.7.1 Редактирование правил отображения адресов

Для внесения изменений в правило отображения адресов щелкните по иконке редактирования в строке правила в окне **Address Mapping (Отображение адресов)**. Появится следующее окно.

Рис. 91 Редактирование правил отображения адресов



В следующей таблице даны описания полей этого окна.

Табл. 54 Редактирование правил отображения адресов

ПОЛЕ	ОПИСАНИЕ
Type (Тип)	Выберите тип отображения портов из следующих вариантов. • **One-to-one (Один к одному)**: в этом режиме один локальный IP-адрес отображается на один глобальный IP-адрес. Следует отметить, что в данном режиме отображения NAT номера портов не изменяются. • **Many-to-One (Много-к-одному)**: в этом режиме несколько локальных IP-адресов отображается на один глобальный IP-адрес. Этот режим аналогичен SUA (т.е., PAT, port address translation – преобразование адресов портов) – функции ZyXEL «Учетная запись одиночного пользователя», которую поддерживали предыдущие модели маршрутизаторов ZyXEL. • **Many-to-Many Overload (Много-ко-многим с перегрузкой)**: в этом режиме несколько локальных IP-адресов отображается на несколько общих глобальных IP-адресов. • **Many-to-Many No Overload (Много-ко-многим без перегрузки)**: в этом режиме каждый локальный IP-адрес отображается на уникальный глобальный IP-адрес. • **Server (Сервер)**: этот режим позволяет установить внутренние серверы для различных служб, расположенных за NAT, и сделать их доступными для внешних пользователей.
Local Start IP (Начальный локальный IP-адрес)	Это начальный локальный IP-адрес (ILA). Локальные IP-адреса недоступны (**N/A**) для типа отображения портов **Server (Сервер)**.
Local End IP (Конечный локальный IP-адрес)	Это конечный локальный IP-адрес (ILA). Если правило предназначено для всех локальных IP-адресов, то в поле **Local Start IP (Начальный локальный IP-адрес)** введите 0.0.0.0, а в поле **Local End IP (Конечный локальный IP-адрес)** введите 255.255.255.255. В этом поле отображается **N/A (Не применяется)** для типов отображения **One-to-one (Один-к-одному)** и **Server (Сервер)**.
Global Start IP (Начальный глобальный IP-адрес)	Это начальный глобальный IP-адрес (начальный IGA). Если вы используете динамический IP-адрес, назначаемый Интернет-провайдером, введите в это поле 0.0.0.0.
Global End IP (Конечный глобальный IP-адрес)	Это конечный глобальный IP-адрес (конечный IGA). В этом поле отображается **N/A (Не применяется)** для типов отображения **One-to-one (Один-к-одному)**, **Many-to-One (Много-к-одному)** и **Server (Сервер)**.
Server Mapping Set (Набор отображения серверов)	Это поле доступно, только если в поле **Type (Тип)** установлено значение **Server (Сервер)**. Выберите число из выпадающего списка, чтобы установить набор отображения серверов.
Edit Details (Редактировать параметры)	Щелкните по этой ссылке для перехода к окну **Port Forwarding (Переадресация портов)** для внесения изменений в набор отображения серверов, установленный в поле **Server Mapping Set (Набор отображения серверов)**.
Back (Назад)	Для возврата к предыдущему окну нажмите кнопку **Back (Назад)**.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек P660HWP.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.

Часть IV
Безопасность

10

Межсетевые экраны

В этой главе представлена вводная информация о межсетевых экранах и рассказывается о межсетевом экране интернет-центра P660HWP.

10.1 Межсетевой экран – общая информация

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

Настройки межсетевого экрана по умолчанию – см. Разд. 11.5 на с. 186.

Просмотр правил межсетевых экранов – см. Разд. 11.6 на с. 188.

Настройка правил межсетевых экранов – см. Разд. 11.6.1 на с. 190.

Настройка пользовательских служб – см. Разд. 11.6.2 на с. 193.

Настройка порогов межсетевых экранов – см. Разд. 11.10.3 на с. 204.

10.2 Типы межсетевых экранов

Существует три основных вида межсетевых экранов:

- Межсетевые экраны с фильтрацией пакетов
- Межсетевые экраны на уровне приложений
- Межсетевые экраны с инспекцией пакетов с учетом состояния

10.2.1 Межсетевые экраны с фильтрацией пакетов

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

10.2.2 Межсетевые экраны на уровне приложений

Межсетевые экраны на уровне приложений ограничивают доступ, выступая в качестве прокси-серверов для внешних серверов. В связи с тем, что они используют программы, написанные для конкретных служб Интернет, таких как HTTP, FTP и telnet, они могут инспектировать пакеты на предмет достоверности относящихся к приложению данных. У шлюзов приложений имеется ряд преимуществ общего характера по сравнению с режимом (по умолчанию) разрешения передачи трафика приложений непосредственно к внутренним узлам.

Функция намеренного скрытия информации не позволяет внешним системам получить имена внутренних узлов через DNS, так как шлюз приложения – это единственный узел, имя которого должно быть известно внешним системам.

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

10.2.3 Межсетевые экраны с инспекцией пакетов с учетом состояния

Межсетевые экраны с инспекцией пакетов с учетом состояния ограничивают доступ путем отбраковки пакетов, не удовлетворяющих установленным правилам доступа. Решения о доступе принимаются в зависимости от IP-адреса и протокола. Такие межсетевые экраны также «инспектируют» данные сеансов связи для обеспечения целостности соединения и адаптации к динамическим протоколам. Как правило, такие экраны обеспечивают лучшую скорость и прозрачность, однако проигрывают в таких аспектах, как управление доступом на уровне приложений и кэширование, которые поддерживаются некоторыми прокси. Для получения более подробной информации об инспекции пакетов с учетом состояния см. Разд. 10.5 на с. 175.

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

10.3 Знакомство с межсетевым экраном ZyXEL

Межсетевой экран P660HWP относится к типу экранов с инспекцией пакетов с учетом состояния и предназначен для защиты от атак типа «Denial of Service» (отказ в обслуживании). Задачей межсетевого экрана P660HWP является обеспечение безопасного подключения частной локальной сети (LAN) к Интернету. P660HWP также

можно использовать для предотвращения несанкционированного копирования, уничтожения и изменения данных или регистрационных журналов, что важно с точки зрения безопасности локальной сети. Также P660HWP выполняет функции фильтрации пакетов.

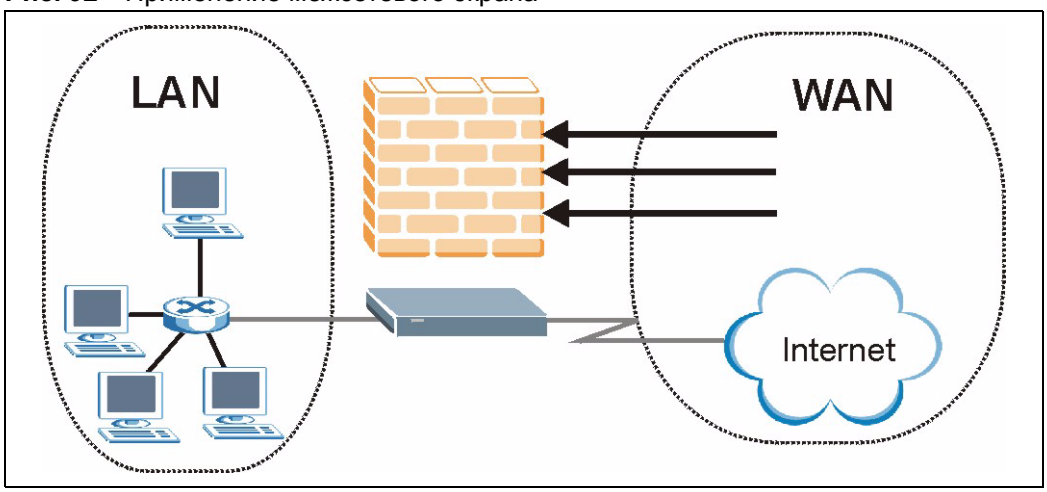
Интернет-центр P660HWP устанавливается между локальной сетью и Интернетом. Это позволяет ему выступать в качестве безопасного шлюза для данных, пересылаемых из локальной сети в Интернет и наоборот.

P660HWP имеет один порт DSL/ISDN и один порт Ethernet для подключения локальной сети. Порты физически разделяют сеть на две области.

- Порт DSL/ISDN подключается к Интернету.
- Порт локальной сети подключается к компьютерной сети, для которой необходимо обеспечить защиту от внешнего мира. Компьютеры сети будут иметь доступ к Интернет-службам, таким как электронная почта, FTP, и WWW. Однако, «входящий доступ» не будет разрешен, если не настроено удаленное управление или не создано правило межсетевого экрана, позволяющее удаленному узлу использовать конкретную службу.

10.3.1 Атаки типа «Отказ в обслуживании» (DoS)

Рис. 92 Применение межсетевого экрана



10.4 Отказ в обслуживании (DoS)

Атаки типа «Отказ в обслуживании» (DoS) нацелены на устройства и сети, подключенные к Интернету. Эти атаки нацелены не на несанкционированное получение информации, а имеют своей целью вывести из строя какое-либо устройство или сеть, таким образом лишая пользователя дальнейшего доступа к ресурсам сети. Предварительная настройка межсетевого экрана P660HWP обеспечивает автоматическое обнаружение и устранение всех известных атак DoS.

10.4.1 Основные сведения

Компьютеры обмениваются информацией через Интернет, используя общий «универсальный язык» под названием TCP/IP. TCP/IP, в свою очередь, представляет собой набор протоколов уровня приложений, выполняющих определенные функции. «Добавочный номер», называемый «порт TCP» или «порт UDP» идентифицирует эти протоколы, а именно HTTP (Web), FTP (File Transfer Protocol – Протокол передачи файлов), POP3 (E-mail) и т. д. Например, Web-трафик по умолчанию использует порт 80 TCP.

При взаимодействии компьютеров в сети Интернет используется модель клиент-сервер, при которой сервер «прослушивает» через конкретный порт TCP/UDP запросы на информацию, поступающие от удаленных клиентских компьютеров сети. Например, web-сервер обычно «слушает» через порт 80. Следует отметить, что на данном компьютере может быть задействован не единственный порт (например, порт 80 для web), но и остальные тоже будут активны. При недостаточной осторожности лица, осуществляющего настройку и управление данным компьютером, компьютер может подвергнуться атаке хакера через незащищенный порт.

Некоторые наиболее общепринятые порты IP:

Табл. 55 Общепринятые порты IP

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

10.4.2 Типы атак DoS

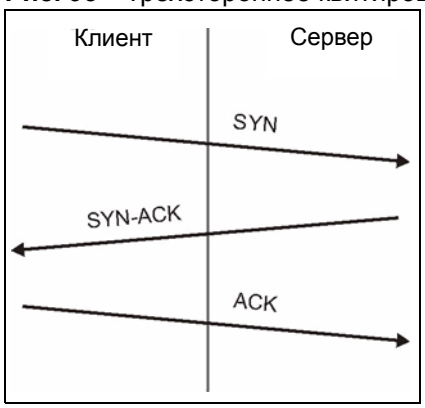
Существуют четыре категории атак типа DoS:

1. Атаки, использующие недостатки реализации TCP/IP.
2. Атаки, использующие слабые места спецификации TCP/IP.
3. Атаки грубой силой, наполняющие сеть бесполезными данными.
4. Подстановка IP-адреса.
5. Атаки **Ping of Death** и **Teardrop** используют недостатки реализации TCP/IP на различных компьютерных и хост-системах.

- Атака «Ping of Death» использует утилиту эхо-тестирования (ping) для создания IP-пакета, превышающего максимальный размер в 65 536 байт, разрешенный спецификацией IP. Пакет большого размера посылается в систему, что вызывает ее отказ, зависание или перезагрузку.
- Атака «Teardrop» использует слабости в перекомпоновке фрагментов пакета IP. При передаче данных в сети IP-пакеты разбиваются на более мелкие фрагменты. Каждый фрагмент выглядит как первоначальный пакет IP, но содержит поле смещения, несущее информацию, например, о том, что «Данный фрагмент несет байты с 200 по 400 первоначального (нефрагментированного) пакета IP.» Программа Teardrop создает серию IP-фрагментов с перекрывающимися полями смещения. Когда при достижении адресата пакет восстанавливается из фрагментов, это может привести к остановке, зависанию и перезагрузке системы.

6. Слабости в спецификации TCP/IP оставляют ее открытой для атак **SYN Flood** и **LAND**. Эти атаки происходят во время квитирования, инициирующего сеанс связи между двумя приложениями.

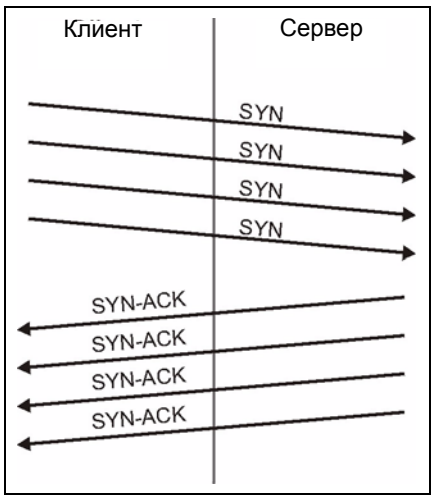
Рис. 93 Трехстороннее квитирование



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

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

Рис. 94 SYN Flood

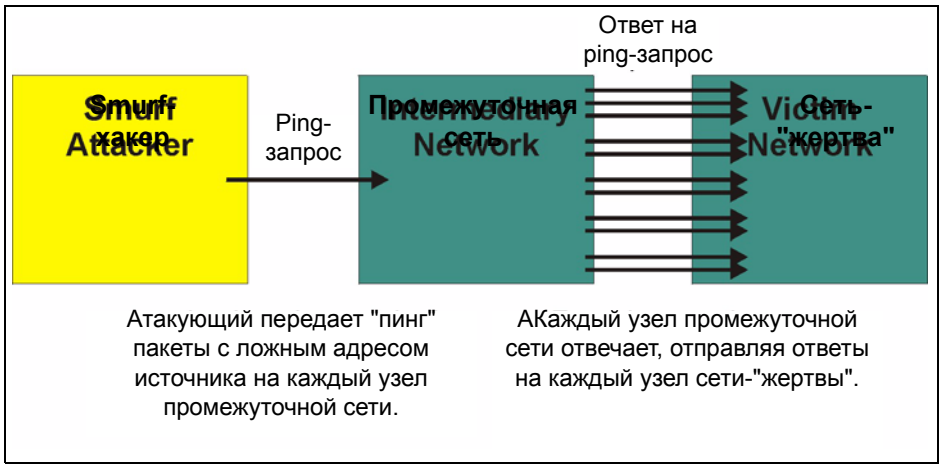


- Используя атаку **LAND**, хакер затопляет сеть SYN-пакетами с ложным IP-адресом источника, равным IP-адресу атакуемой системы. В результате компьютер-узел посылает пакеты сам себе, и система становится недоступной, пытаясь отвечать на запросы самой себе.

7 Атака **грубой силой**, например «Smurf», использует особенность спецификации IP, известную как направленная рассылка или циркулярная рассылка для подсети, для того, чтобы затопить атакуемую сеть бесполезными данными. Хакер, использующий этот вид атаки, переполняет маршрутизатор пакетами – эхо-

запросами протокола ICMP (протокол управляющих сообщений в сети Интернет). Так как IP-адрес получателя каждого пакета является широковещательным адресом сети, маршрутизатор рассылает такой пакет ICMP всем узлам сети. Если узлов много, это приводит к большому объему трафика состоящего из запросов и ответов ICMP. Если хакер решает подменить IP-адрес источника эхо-запроса ICMP, то в результате трафик ICMP не только переполнит сеть-«посредник», но и перегрузит сеть подмененного IP-адреса, именуемую сетью-«жертвой». Такое переполнение широковещательным трафиком использует весь имеющийся ресурс пропускной способности, делая связь с системой недоступной.

Рис. 95 Атака Smurf



10.4.2.1 Уязвимость ICMP

ICMP является протоколом с оповещением об ошибках, работающим совместно с IP. Следующие типы ICMP выдают предупреждение:

Табл. 56 Команды ICMP, выдающие предупреждение

5	REDIRECT
13	TIMESTAMP_REQUEST
14	TIMESTAMP_REPLY
17	ADDRESS_MASK_REQUEST
18	ADDRESS_MASK_REPLY

10.4.2.2 Недопустимые команды (NetBIOS и SMTP)

Единственно допустимыми командами NetBIOS являются приведенные ниже, все остальные – недопустимы.

Табл. 57 Команды NetBIOS

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

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

Табл. 58 Команды SMTP

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

10.4.2.3 Traceroute

Traceroute – это утилита, предназначенная для определения маршрута, проходимого пакетом между двумя конечными точками. Иногда при некорректной установке межсетевого экрана у хакера появляется возможность проследить его путь и получить данные о топологии сети, находящейся за экраном.

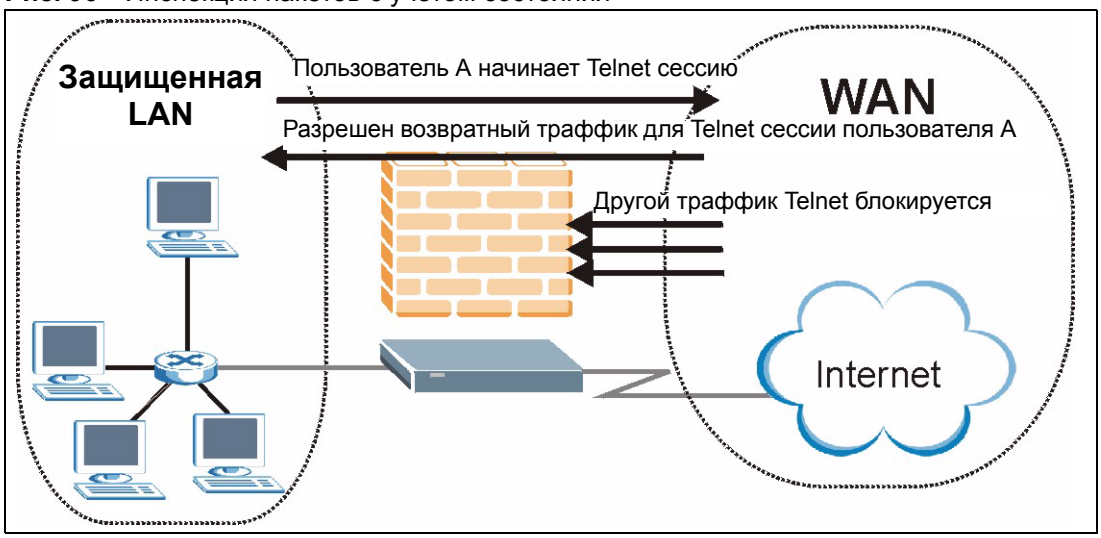
Часто, многие атаки DoS также применяют, как часть своей атаки метод, известный как **IP Spoofing** (подстановка IP-адреса). Подстановка IP-адреса может использоваться с целью проникновения в системы, чтобы исключить возможность идентифицировать хакера или увеличить эффект атаки DoS. Подстановка IP-адреса применяется для получения несанкционированного доступа к компьютерам путем создания ситуации, когда межсетевой экран или маршрутизатор получают информацию о том, что обмен данными происходит якобы с надежной (в отношении безопасности) сетью. При использовании данного способа хакер должен видоизменить заголовки пакетов так, чтобы складывалось впечатление, что пакеты поступают с надежного (доверенного) узла и должны беспрепятственно пропускаться сетевым экраном или маршрутизатором. P660HWP блокирует все попытки имитации IP-адреса.

10.5 Инспекция пакетов с учетом состояния

Инспекция с учетом состояния означает, что поля пакетов сравниваются с теми пакетами, которые уже считаются достоверными. Например, при доступе к внешнему серверу прокси-сервер запоминает параметры первоначального запроса, такие как номер порта и адрес источника и получателя. Такое «запоминание» называется *сохранением состояния*. Когда внешняя система отвечает на запрос, межсетевой экран сравнивает параметры получаемых пакетов с параметрами сохраненного состояния и принимает решение о допуске. В P660HWP инспекция пакетов с учетом состояния используется для защиты частной локальной сети от хакеров и вандалов в Интернете. По умолчанию в P660HWP при инспекции пакетов с учетом состояния разрешается прохождение трафика из локальной сети в Интернет, если источником этого трафика является локальная сеть, и блокируется весь трафик в локальную сеть из Интернета, если этот трафик инициирует Интернет. В целом, основные функции инспекции пакетов с учетом состояния таковы:

- Разрешаются все сеансы связи с глобальной сетью (Интернет, WAN) со стороны локальной (LAN).
- Запрещаются сеансы связи с локальной сетью со стороны глобальной.

Рис. 96 Инспекция пакетов с учетом состояния



На предыдущем рисунке демонстрируется действие правил межсетевого экрана P660HWP по умолчанию, а также показано, как работает функция инспекции пакетов с учетом состояния. Пользователь A может инициировать Telnet-соединение из локальной сети, и ответы на его запросы разрешаются. Однако всякий иной трафик Telnet, поступающий из глобальной сети, блокируется.

10.5.1 Действие функции инспекции пакетов с учетом состояния

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

1. Пакет поступает из локальной сети (где находится сетевой экран) в глобальную сеть.
2. Происходит проверка пакета по существующему списку контроля исходящего доступа для данного порта и дается разрешение (недопущенный пакет сбрасывается уже на данном этапе).
3. Происходит инспекция пакета в соответствии с правилом сетевого экрана для выявления и записи информации о состоянии подключения для данного пакета. Эта информация записывается в виде нового элемента таблицы состояний, созданной для данного подключения. Если для данного пакета нет соответствующего правила межсетевого экрана и, следовательно, он не является атакой, то действия в отношении этого пакета определяются настройками в окне **Firewall General (Общие настройки межсетевого экрана)**.
4. В зависимости от полученной информации о состоянии, правило межсетевого экрана создает временную запись в списке контроля доступа, которая вставляется в начало расширенного списка контроля входящего доступа для порта WAN. Эта временная запись в списке контроля доступа предназначена для разрешения пропуска входящих пакетов с того же соединения, что и уже проинспектированные исходящие пакеты.
5. Исходящий пакет пересылается через данный порт.

6 Далее, входящий пакет достигает порта. Этот пакет является частью соединения уже установленного исходящим пакетом. Происходит сверка входящего пакета со списком контроля входящего доступа и дается разрешение, так как ранее была добавлена временная запись в список контроля доступа.
7 Пакет проверяется на соответствие правилом межсетевого экрана, а таблица состояний для данного соединения по необходимости обновляется. На основании обновленной информации о состоянии временные записи расширенного списка контроля входящего доступа могут быть изменены, чтобы разрешать только пропуск пакетов, действительных для текущего состояния данного соединения.
8 Проверяются дополнительные входящие или исходящие пакеты для данного соединения, таким образом обновляется таблица состояний и, соответственно, временные записи в списке контроля исходящего доступа; пакеты пересылаются через порт.
9 При прекращении связи или истечении времени ожидания, таблица состояний для данного соединения и временные записи в списке контроля доступа удаляются.

10.5.2 Инспекция пакетов с учетом состояния и P660HWP

Дополнительные правила могут расширять или замещать установленные по умолчанию. Например, можно создать правило, которое будет выполнять следующее:

- Блокировать трафик определенного типа, например IRC (Internet Relay Chat), исходящий из локальной сети в Интернет.
- Разрешить трафик определенного типа из Интернета к конкретным компьютерам-узлам локальной сети.
- Разрешить доступ к web-серверу всем, кроме конкурентов.
- Разрешить использование определенных протоколов, например Telnet, лишь полномочным пользователям локальной сети.

Эти определяемые пользователями правила работают, используя принцип проверки IP-адреса источника и IP-адреса получателя сетевого трафика, типа протокола IP, и сравнения с правилами, установленными администратором.

Возможность устанавливать правила межсетевого экрана является очень мощным инструментом. С помощью этих правил можно отключить межсетевой экран или полностью заблокировать доступ в Интернет. Создание и удаление правил межсетевого экрана требует большой осторожности. После создания новых правил необходимо проверить их на правильность работы.

Ниже дается краткое техническое описание отслеживания таких соединений. Соединения могут определяться или протоколами верхнего уровня (например, TCP) или самим интернет-центром P660HWP (как и в случае «виртуальных соединений», создаваемых для UDP и ICMP).

10.5.3 Безопасность TCP

P660HWP использует информацию о состоянии, вложенную в пакеты TCP. В первом пакете любого нового соединения флаг SYN (синхронизация) установлен, а флаг ACK (подтверждение приема) отсутствует; это пакеты-инициаторы. Пакеты, не содержащие таких флажков, называются «последующими», так как несут данные, возникающие затем в потоке TCP.

Если пакет-инициатор исходит из глобальной сети, это значит, что кто-то в Интернете пытается установить соединение с локальной сетью. За исключением особых случаев (см. далее «протоколы верхнего уровня»), такие пакеты сбрасываются и вносятся в журнал.

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

При получении интернет-центром P660HWP пакета типа «последующий» (из Интернета или локальной сети) из него извлекается информация о подключении и проверяется по содержанию кэша. Прохождение пакета разрешается, только если он соответствует данному соединению (то есть, если он является ответом на запрос соединения из локальной сети).

10.5.4 Безопасность UDP/ICMP

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

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

Подобная ситуация имеет место и для ICMP, но в этом случае P660HWP налагает более строгие ограничения. В частности, лишь в ответ на исходящие эхо-запросы разрешены входящие эхо-отклики, на исходящий запрос маски подсети – входящий ответ, а входящий ответ временной метки разрешен только на исходящий запрос. Межсетевой экран не пропускает никакие другие пакеты ICMP, так как они представляют собой большую опасность и содержат слишком мало информации о маршруте. Например, прием ICMP-пакетов переадресации запрещен, так как с их помощью можно перенаправить трафик через атакующие компьютеры.

10.5.5 Протоколы верхнего уровня

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

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

Чтобы достичь этого, P660HWP анализирует данные FTP на прикладном уровне. В частности, ищет выходную команду PORT, и если таковая имеется, добавляет в кэш запись об ожидаемом соединении для передачи данных. Эта операция безопасна, поскольку команда PORT содержит адрес и порт, по которым идентифицируется соединение.

Любой протокол, работающий таким образом, необходимо поддерживать отдельно по каждому случаю. Для этого можно использовать функцию Web-конфигуратора «Custom Ports» (Назначение портов пользователем).

10.6 Методы усиления безопасности при помощи межсетевого экрана

- Измените пароль по умолчанию с помощью CLI (Command Line Interpreter – интерпретатор командной строки) или Web-конфигуратора.
- Ограничьте круг лиц, имеющих право telnet-подключения к маршрутизатору.
- Не подключайте неиспользуемые локальные службы (SNMP или NTP). Любое такое лишнее подключение может представлять потенциальную угрозу безопасности. Находчивый хакер может отыскать оригинальные способы злоупотребления подключенными службами для получения доступа к межсетевому экрану или сети.
- Подключенные локальные серверы необходимо обезопасить. Защита обеспечивается путем ограничения взаимодействия до конкретных клиентских устройств и назначения правил блокировки пакетов, поступающих через конкретный порт.
- Активированный межсетевой экран обеспечит защиту от подмены IP-адресов.
- Само устройство межсетевого экрана должно находиться в недоступном (закрытом) помещении.

10.6.1 Общая безопасность

Предусмотреть все возможные случаи невозможно. Многие факторы, контроль над которыми выходит за пределы возможностей межсетевого экрана, фильтрации или трансляции сетевых адресов, могут создать бреши в системе защиты. Ниже приводятся некоторые общие рекомендации, выполнение которых позволит свести риск к минимуму.

- Организация/компания должна разработать комплексный план по защите. Качественное сетевое администрирование предполагает учет возможностей хакеров и предвидение атак. Лучшей защитой от хакеров и взломщиков является информированность. Все сотрудники компании должны быть осведомлены о том, как важна безопасность и как минимизировать риск. Рекомендуется составить перечни, подобные этому.

- Подключения с помощью DSL или кабельного модема являются соединениями типа «always-on» (всегда включено) и особенно уязвимы, так как предоставляют хакерам возможность взлома системы. Компьютеры, не используемые в данный момент, необходимо выключать.
- Никогда не сообщайте пароль или другие секретные данные, отвечая на телефонные звонки или сообщения по электронной почте от неизвестных лиц.
- Никогда не отправляйте секретные сведения, такие как пароли, данные о кредитных картах и т. д. в незашифрованном виде.
- Не публикуйте секретные данные на веб-страницах, если веб-сайт не использует безопасные подключения. Безопасное подключение можно идентифицировать по иконке в виде ключа в нижней панели браузера (Internet Explorer версии 3.02 и выше или Netscape версии 3.0 и выше). Если веб-сайт использует безопасное подключение, предоставление информации безопасно. Безопасные веб-транзакции довольно сложно взламывать.
- Не сообщайте IP-адрес и прочие системные данные о сети людям, не имеющим отношения к вашей организации. Обращайте внимание на файлы, присылаемые по электронной почте неизвестными отправителями. Общеизвестный способ получения вируса BackOrifice – получение его в составе другого файла в качестве «троянского коня».
- Время от времени меняйте пароли. Используйте пароли, которые невозможно угадать. Наиболее трудно взламывать пароли, содержащие буквы нижнего и верхнего регистров, числа и символы типа % или # одновременно.
- Регулярно обновляйте программное обеспечение. Многие старые версии программ, особенно Web-браузеры, имеют недостатки в системе защиты. Последние версии программ, как правило, содержат самые последние обновления и исправления.
- При участии в чатах или сеансах IRC необходимо тщательно следить за информацией, сообщаемой незнакомым людям.
- При подозрительном поведении системы необходимо обратиться к своему Интернет-провайдеру. Некоторые хакеры используют средства, заставляющие систему со временем становиться все менее устойчивой или прекращать нормальное функционирование.
- Уничтожайте документы, содержащие конфиденциальную информацию, особенно о компьютере, перед тем как их выбросить. Некоторые хакеры могут получить нужную им информацию, исследуя выбрасываемые организацией или отдельными людьми ненужные документы.

10.7 Сравнение функций фильтрации пакетов и межсетевого экрана

Ниже представлено сравнение функций фильтрации и межсетевого экрана в P660HWP.

10.7.1 Фильтрация пакетов

- Маршрутизатор производит фильтрацию пакетов во время их прохождения через порт маршрутизатора в соответствии с назначенными правилами фильтрации.

- Фильтрация пакетов является мощным инструментом, однако, могут возникнуть сложности с ее настройкой и управлением, особенно если нужно задать цепочку правил для фильтрации какой-либо службы.
- Фильтрация пакетов проверяет лишь заголовки пакетов IP.

10.7.1.1 Случаи использования фильтрации

- Для блокировки/допуска пакетов LAN по их MAC-адресам.
- Для блокировки/допуска пакетов с особым IP, не являющихся пакетами TCP, UDP, или ICMP.
- Для блокировки/допуска как входящего (из WAN в LAN), так и исходящего (из LAN в WAN) трафика между конкретным внутренним узлом/сетью «A» и внешним узлом/сетью «B». Если фильтр блокирует трафик из A в B, то также блокируется и трафик из B в A. Фильтры не могут различать трафик, исходящий от внутреннего или внешнего узла по IP-адресу.
- Для блокировки/допуска отслеживания маршрута по сети IP.

10.7.2 Межсетевой экран

- Межсетевой экран проверяет содержание пакетов и адреса их источника и получателя. Экраны такого типа используют модуль контроля, подходящий ко всем протоколам, и распознающий данные пакета разных уровней, от сетевого уровня (заголовки IP) до уровня приложений.
- Межсетевой экран выполняет инспекцию пакетов с учетом состояния. Он учитывает состояние обрабатываемых подключений, например, легальный входящий пакет можно сопоставить с исходящим запросом на этот пакет и разрешить его получение. Напротив, входящий пакет, маскирующийся под ответ на несуществующий исходящий запрос, блокируется.
- Межсетевой экран применяет фильтрацию сеансов связи, т. е. использует сложные правила, расширяющие процесс фильтрации с проверки отдельных пакетов в рамках сеанса связи до контроля сеанса связи в целом.
- Межсетевой экран имеет службу электронной почты, с помощью которой отсылаются отчеты и извещения.

10.7.2.1 Случаи использования межсетевого экрана

- Для защиты от атак типа DoS и предотвращения проникновения в сеть хакеров.
- Возможность в рамках одного правила задать ряд IP-адресов источника и получателя, а также номера портов делает использование экрана более предпочтительным в случаях, когда необходимы сложные правила.
- Для выборочной блокировки/допуска входящего и исходящего трафика между внутренними и внешними узлами/сетями. Напомним, что фильтры не в состоянии отличать трафик, исходящий от внутреннего или внешнего узла, по IP-адресу.
- Межсетевой экран предпочтительнее, чем фильтрация, если необходима проверка на соответствие нескольким правилам.
- Лучше использовать межсетевой экран, если есть необходимость получать плановые отчеты о системе или сообщения об атаках по электронной почте.
- Межсетевой экран позволяет блокировать трафик от конкретного URL при появении такового. Указатели URL сохраняются в базе данных списка контроля доступа.

11

Настройка межсетевого экрана

В этой главе рассказывается, как включить и настроить межсетевой экран интернет-центра P660HWP.

11.1 Способы настройки

Web-конфигуратор обеспечивает все необходимые средства для настройки межсетевого экрана интернет-центра P660HWP. Поэтому рекомендуется выполнять настройку межсетевого экрана с помощью Web-конфигуратора. CLI (Command Line Interpreter – интерфейс командной строки) обеспечивает настройку ограниченного числа параметров и рекомендуется только для опытных пользователей.

11.2 Обзор правил межсетевого экрана

Правила межсетевого экрана группируются по направлениям движения пакетов, к которым они применяются.

- Лок. сеть – лок. сеть/маршрутизатор
- Лок. сеть – глоб. сеть
- Глоб. сеть – лок. сеть
- Глоб. сеть – глоб. сеть/маршрутизатор

По умолчанию выполняемая интернет-центром P660HWP инспекция пакетов с учетом состояния разрешает прохождение пакетов в следующих направлениях:

- Лок. сеть – лок. сеть/маршрутизатор

  Это позволяет компьютерам локальной сети выполнять управление интернет-центром P660HWP и обмениваться данными с сетями и подсетями, подключенными к порту локальной сети
- Лок. сеть – глоб. сеть

По умолчанию выполняемая интернет-центром P660HWP инспекция пакетов с учетом состояния отбрасывает пакеты, передаваемые в следующих направлениях:

- Глоб. сеть – лок. сеть
- Глоб. сеть – глоб. сеть/маршрутизатор

  Это предотвращает использование P660HWP в качестве шлюза компьютерами глобальной сети для связи с другими компьютерами в глобальной сети, а также для управления P660HWP.

  Можно определить дополнительные правила и установить или модифицировать существующие, но соблюдайте при этом крайнюю осторожность.

Вы можете неумышленно подвергнуть межсетевой экран и защищенную сеть риску, если попытаетесь настроить правила, не имея четкого представления о том, как они работают. После настройки правила необходимо протестировать.

Например, можно назначить следующие правила:

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

Эти определяемые пользователем правила работают на основе принципа проверки IP-адреса источника, IP-адреса получателя сетевого трафика и типа протокола IP на соответствие правилам, установленным администратором. Правила, установленные пользователем, имеют более высокий приоритет по отношению к правилам по умолчанию P660HWP и замещают их.

11.3 Обзор логики правил

Прежде чем назначать правила, необходимо тщательно изучить данные указания.

11.3.1 Список вопросов для составления правил

Сформулируйте назначение правила. Например: «ограничить доступ IRC из локальной сети в сеть Интернет». Или: «позволить удаленному серверу Lotus Notes синхронизацию с внутренним сервером Notes через Интернет».

1. Трафик должен пересылаться или блокироваться согласно правилу?
2. К какому направлению трафика применяется правило?
3. Какие службы IP попадут под действие правила?
4. На каких компьютерах локальной сети отразится выполнение этого правила?
5. На каких компьютерах в Интернете отразится выполнение этого правила? Эти сведения должны быть по возможности конкретны. Например, если разрешается пересылка трафика из сети Интернет в локальную сеть, лучше указать определенные серверы в Интернете, которые будут иметь доступ к локальной сети.

11.3.2 Правила с точки зрения безопасности

1. Когда правило составлено, очень важно рассмотреть те последствия, которые оно будет иметь для безопасности сети.
2. Не мешает ли данное правило пользователям локальной сети иметь доступ к каким-либо важным ресурсам Интернета? Например, если блокируется IRC, есть ли пользователи, которым необходима эта служба?
3. Нельзя ли видоизменить правило так, чтобы оно стало более конкретным? Например, если IRC заблокирован для всех пользователей, возможно, будет целесообразнее задать правило, которое блокирует доступ только для определенных пользователей.
4. Не является ли правило, позволяющее пользователям Интернета иметь доступ к ресурсам локальной сети, причиной появления слабых мест в системе защиты? Например, если соединение с локальной сетью через порт FTP (TCP 20, 21) возможно из Интернета, пользователи Интернета могут получить доступ к работающим FTP-серверам.
5. Нет ли конфликта между данным правилом и другими имеющимися правилами?
6. Если ответы на эти вопросы известны, то добавление правил сведется к простому внесению данных в нужные поля в окнах Web-конфигуратора.

11.3.3 Основные поля для настройки правил

11.3.3.1 Action (Действие)

Выполняемое действие: **Drop (Сбросить)**, **Reject (Отказать)** или **Permit (Пропустить)**.

Drop (Сбросить) означает, что межсетевой экран сбрасывает пакеты без предупреждения. Reject (Отказать) означает, что межсетевой экран сбрасывает пакеты и посылает отправителю сообщение ICMP о недоступности адресата.

11.3.3.2 Service (Служба)

Выберите службу из прокручиваемого окна списка **Service (Служба)**. Если нужной службы нет в списке, необходимо сначала ее определить. Для получения более подробной информации о предварительно заданных службах см. Разд. Табл. 64 на с. 199.

11.3.3.3 Source Address (Адрес источника)

Это адрес источника соединения: локальная или глобальная сеть, одиночный IP-адрес, диапазон IP-адресов или подсеть.

11.3.3.4 Destination Address (Адрес назначения)

Это адрес назначения соединения: локальная или глобальная сеть, одиночный IP-адрес, диапазон IP-адресов или подсеть.

11.4 Направление связи

В этом разделе приведены примеры правил межсетевого экрана для соединений «LAN – WAN» и «WAN – LAN».

Правила для соединений «LAN – LAN/маршрутизатор» и «WAN – WAN/маршрутизатор» применяются к пакетам, поступающим на соответствующий порт (LAN или WAN). «LAN – LAN/маршрутизатор» – это правила для соединений «LAN – P660HWP» (правила для управления P660HWP через порт LAN) и правила для соединений «LAN – LAN» (правила для управления маршрутизацией между двумя подсетями в локальной сети). Аналогично, правила для соединений "WAN–WAN/маршрутизатор" применяются к порту WAN.

11.4.1 Правила LAN – WAN

Правило, устанавливаемое по умолчанию для трафика «LAN – WAN», разрешает всем пользователям в локальной сети неограниченный доступ к глобальной. Назначение правил «LAN – WAN» обычно подразумевает запрет для некоторых или всех пользователей доступа к определенным службам глобальной сети. Правила WAN – LAN

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

11.4.2 Предупреждения

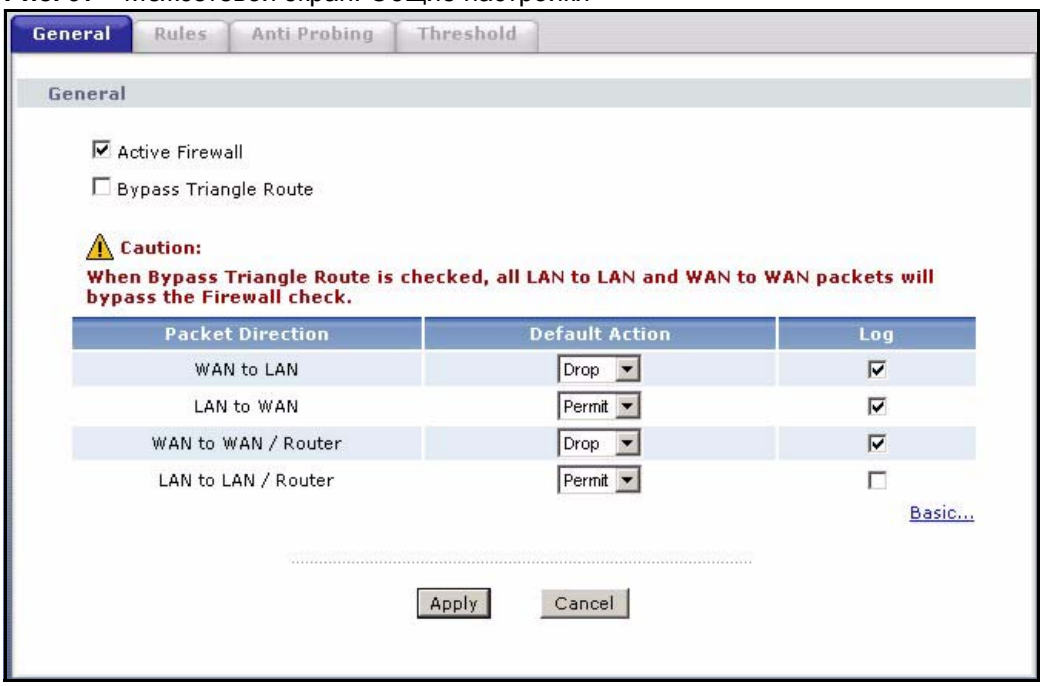
Предупреждения – это сообщения о событиях (таких как атаки), информация о которых может быть необходима пользователю немедленно. Чтобы устройство генерировало извещение при обнаружении события, соответствующего правилу, необходимо установить эту функцию в окне **Edit Rule (Изменить правило)** (см. Рис. 99 на с. 191). Если происходит событие, которое генерирует извещение, то по электронной почте немедленно отправляется сообщение по адресу, установленному в окне **Log Settings (Настройки регистрационного журнала)**. Для дополнительной информации см. главу, посвященную регистрационным журналам.

11.5 Основная политика межсетевого экрана

Щелкните **Security (Безопасность)** > **Firewall (Межсетевой экран)** для отображения следующего окна. Межсетевой экран включается с помощью установки флажка в поле **Active Firewall (Включить межсетевой экран)**, как показано на следующем рисунке.

Более подробную информацию см. Разд. 10.1 на с. 169.

Рис. 97 Межсетевой экран: Общие настройки



В следующей таблице даны описания полей этого окна.

Табл. 59 Межсетевой экран: Общие настройки

ПОЛЕ	ОПИСАНИЕ
Active Firewall (Включить межсетевой экран)	Выберите эту опцию, чтобы включить межсетевой экран. Если межсетевой экран включен, P660HWP осуществляет управление доступом и защиту от атак типа «Отказ в обслуживания» (DoS).
Bypass Triangle Route (Обходной треугольный маршрут)	Поставьте в этом поле флажок, чтобы межсетевой экран P660HWP разрешал использование треугольной топологии маршрутов в сети. Дополнительную информацию о треугольной топологии маршрутов см. в *приложении*. **Примечание: Использование несимметричных маршрутов позволяет пропускать трафик из глобальной сети прямо к компьютеру локальной сети без прохождения через маршрутизатор. См. Прил. J на с. 419, где более подробно описывается треугольная топология маршрутов, а также ее использование.**
Packet Direction (Направление пакетов)	Это направление движения пакетов: **LAN to LAN / Router (Лок. сеть – лок. сеть/маршрутизатор)**, **LAN to WAN (Лок. сеть – глоб. сеть)**, **WAN to WAN / Router (Глоб. сеть – глоб. сеть/маршрутизатор)**, **WAN to LAN (Глоб. сеть – лок. сеть)**. Правила межсетевого экрана группируются по направлениям движения пакетов, к которым они применяются. Например, направление **LAN to LAN / Router (Лок. сеть – лок. сеть/маршрутизатор** означает, что пакеты передаются от компьютера/подсети в локальной сети к другому компьютеру/подсети, подключенному к интерфейсу LAN P660HWP или к самому интернет-центру P660HWP.

Табл. 59 Межсетевой экран: Общие настройки (продолжение)

ПОЛЕ	ОПИСАНИЕ
Default Action (Действия по умолчанию)	Из выпадающего списка выберите действие по умолчанию, которое межсетевой экран выполняет для пакетов, которые перемещаются в выбранном направлении и не соответствуют ни одному из правил межсетевого экрана. Выберите **Drop (Сбросить)** для сброса пакетов без предупреждения и без отправки пакета сброса TCP или сообщения ICMP отправителю о недоступности адресата. Выберите **Reject (Отказать)**, чтобы не принимать пакеты и отправить пакет сброса TCP (для пакетов TCP) или сообщение ICMP отправителю о недоступности адресата (для пакетов UDP). Выберите **Permit (Пропустить)**, чтобы разрешить прохождение пакетов.
Log (Регистрационный журнал)	Установите флажок для ведения регистрационного журнала (когда производится выбранное выше действие) для пакетов, которые перемещаются в выбранном направлении и не соответствуют ни одному из правил межсетевого экрана.
Expand... (Больше...)	Щелкните по этой кнопке для отображения дополнительных параметров.
Basic... (Меньше...)	Щелкните по этой кнопке для отображения только основных параметров.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек P660HWP.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.

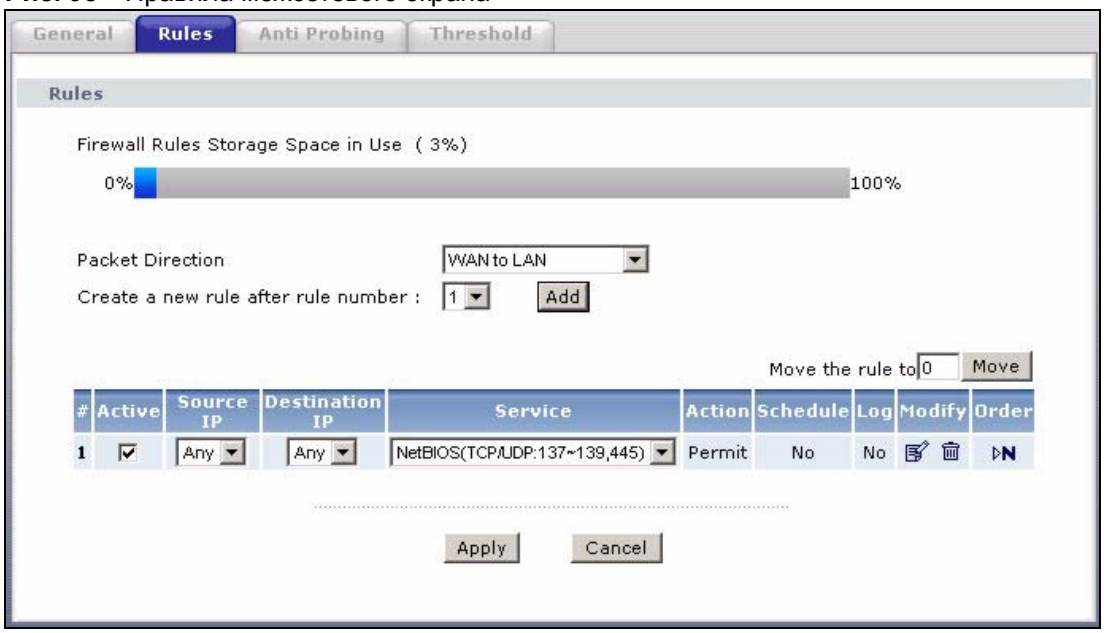
11.6 Сводка правил межсетевого экрана

Очередность правил очень важна, так как правила применяются одно за другим.

Более подробную информацию см. Разд. 10.1 на с. 169.

Щелкните **Security (Безопасность)** > **Firewall (Межсетевой экран)** > **Rules (Правила)** для отображения следующего окна. В этом окне отображается список установленных правил межсетевого экрана. Следует обратить внимание на порядок, в котором они перечислены.

Рис. 98 Правила межсетевого экрана



В следующей таблице даны описания полей этого окна.

Табл. 60 Правила межсетевого экрана

ПОЛЕ	ОПИСАНИЕ
Firewall Rules Storage Space in Use (Память, занятая правилами межсетевого экрана)	Этот информационный индикатор показывает, какая часть памяти интернет-центра P660HWP, предназначенная для записи правил межсетевого экрана, находится в использовании. Если занято 80% или менее доступной памяти, индикатор остается зеленым. Если занято более 80% памяти, индикатор становится красным.
Packet Direction (Направление пакетов)	Выберите из раскрывающегося списка направление движения пакетов, для которого вы хотите определить правила межсетевого экрана.
Create a new rule after rule number (Создать новое правило после правила номер)	Выберите порядковый номер и щелкните **Add (Добавить)**, чтобы добавить новое правило межсетевого экрана с порядковым номером, следующим после выбранного в соседнем поле. Например, если вы выберете «6», новое правило будет иметь номер 7, а старое правило под номером 7 (если есть) будет иметь номер 8.
	Следующие поля, предназначенные только для чтения, содержат информацию о правилах, определенных для трафика в выбранном направлении. Установленные правила межсетевого экрана (в таблице ниже) имеют приоритет над общими настройками межсетевого экрана, установленными в окне **General (Общие настройки)**.
#	Номер правила. Порядок расположения правил имеет большое значение, так как правила выполняются по очереди.
Active (Активировать)	В этом поле отображается состояние межсетевого экрана: включен или отключен. Поставьте флажок в этом поле для включения данного правила. Чтобы отключить данное правило, снимите флажок.
Source IP (IP-адрес источника)	Этот раскрывающийся список содержит адреса или диапазоны адресов источника, к которым применяется данное правило межсетевого экрана. Заметьте, что отсутствие адреса источника или получателя эквивалентно выбору **Any (Любой)**.

Табл. 60 Правила межсетевого экрана (продолжение)

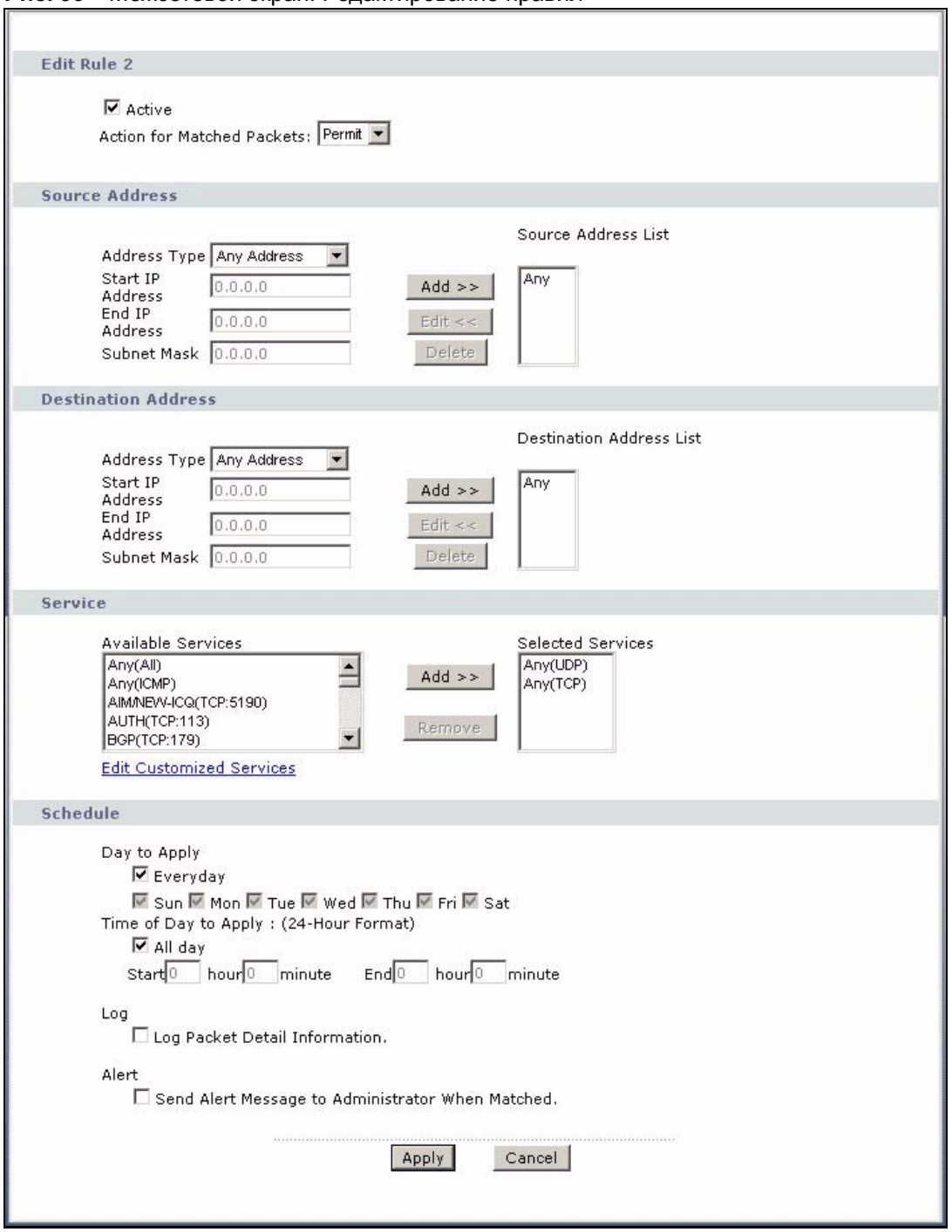
ПОЛЕ	ОПИСАНИЕ
Destination IP (IP-адрес назначения)	Этот раскрывающийся список содержит адреса или диапазоны адресов получателя, к которым применяется данное правило межсетевого экрана. Заметьте, что отсутствие адреса источника или получателя эквивалентно выбору **Any (Любой)**.
Service (Служба)	Этот раскрывающийся список содержит службы, к которым применяется данное правило межсетевого экрана. Более подробную информацию см. Разд. 11.8 на с. 199.
Action (Действие)	В этом поле отображается одно из следующих значений: **Drop (Сбросить)** – межсетевой экран сбрасывает пакеты без предупреждения, **Reject (Отказать)** – межсетевой экран сбрасывает пакеты и отправляет пакет сброса TCP или сообщение ICMP отправителю о недоступности адресата, **Permit (Пропустить)** – межсетевой экран разрешает прохождение пакетов.
Schedule (График)	Это поле показывает, определено (**Yes**) или нет (**No**) расписание.
Log (Регистрационный журнал)	Это поле показывает, создается ли запись в регистрационном журнале, при соответствии пакетов данному правилу: **Yes (Да)** или **No (Нет)**.
Modify (Изменить)	Щелкните по иконке редактирования для перехода к окну, где можно менять параметры правила. Для удаления существующего правила межсетевого экрана щелкните по иконке удаления. Появляется окно с запросом на подтверждение операции удаления правила межсетевого экрана. Следует помнить, что при удалении одного правила все последующие сдвигаются на позицию вверх.
Order (Порядок)	Щелкните по иконке перемещения для отображения поля **Move the rule to (Переместить правило на)**. В поле **Move the rule to (Переместить правило на)** введите число и щелкните по кнопке **Move (Переместить)**, чтобы переместить правило на позицию с указанным номером. Порядок расположения правил имеет большое значение, так как правила выполняются по очереди.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек P660HWP.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.

11.6.1 Настройка правил межсетевого экрана

Более подробную информацию см. Разд. 10.1 на с. 169.

В окне **Rules (Правила)** выберите порядковый номер и щелкните по кнопке **Add (Добавить)** или щелкните по иконке редактирования правила для отображения окна, показанного ниже. В таблице представлена информация по заполнению полей этого окна.

Рис. 99 Межсетевой экран: Редактирование правил



В следующей таблице даны описания полей этого окна.

Табл. 61 Межсетевой экран: Редактирование правил

ПОЛЕ	ОПИСАНИЕ
Active (Активировать)	Выберите эту опцию, чтобы задействовать данное правило межсетевого экрана.
Action for Matched Packet (Действие для соответствующего пакета)	Из выпадающего списка выберите действие, которое должен выполнить межсетевой экран по отношению к пакетам, которые соответствуют данному правилу. Выберите **Drop (Сбросить)** для сброса пакетов без предупреждения и без отправки пакета сброса TCP или сообщения ICMP отправителю о недоступности адресата. Выберите **Reject (Отказать)**, чтобы не принимать пакеты и отправить пакет сброса TCP (для пакетов TCP) или сообщение ICMP отправителю о недоступности адресата (для пакетов UDP). Выберите **Permit (Пропустить)**, чтобы разрешить прохождение пакетов.
Source/Destination Address (Адрес источника/ назначения)	
Address Type (Тип адреса)	Хотите ли вы, чтобы это правило применялось к пакетам с (одним) определенным IP-адресом, любым из диапазона IP-адресов (например, от 192.168.1.10 до 192.169.1.50), подсети или любому IP-адресу? Из выпадающего списка выберите тип: **Single Address (Одиночный адрес)**, **Range Address (Диапазон адресов)**, **Subnet Address (Адрес подсети)** или **Any** Address (Любой адрес).
Start IP Address (Начальный IP-адрес)	Введите одиночный IP-адрес или начальный IP-адрес группы.
End IP Address (Конечный IP-адрес)	Введите конечный IP-адрес группы.
Subnet Mask (Маска подсети)	Введите маску подсети, если таковая имеется.
Add (Добавить) >>	Нажмите кнопку **Add (Добавить)** >>, чтобы добавить новый адрес в поле **Source Address (Адрес источника)** или **Destination Address (Адрес назначения)**. Добавлять можно группы адресов, диапазоны адресов и/или подсети.
Edit (Редактировать) <<	Чтобы изменить существующий адрес источника или назначения, выделите его в соответствующем поле и щелкните по кнопке **Edit (Редактировать)** <<.
Delete (Удалить)	Выделите существующий адрес источника или получателя в поле **Source Address (Адрес источника)** или **Destination Address (Адрес назначения)** и нажмите на **Delete (Удалить)**, чтобы удалить его.
Services (Службы)	
Available/Selected Services (Доступные/ Выбранные службы)	Более подробную информацию об имеющихся службах см. Разд. 11.8 на с. 199. Выделите одну из служб в списке **Available Services (Доступные службы)** слева, затем нажмите **Add (Добавить)>>**, чтобы добавить ее в список **Selected Services (Выбранные службы)** справа. Чтобы удалить службу, выделите ее в списке **Selected Services (Выбранные службы)** справа и нажмите **Remove (Удалить)**.
Edit Customized Service (Редактирование пользовательских служб)	Щелкните по ссылке **Edit Customized Services (Редактирование пользовательских служб)**, чтобы открыть окно, позволяющее настроить новую службу, отсутствующую в стандартном списке служб.

Табл. 61 Межсетевой экран: Редактирование правил (продолжение)

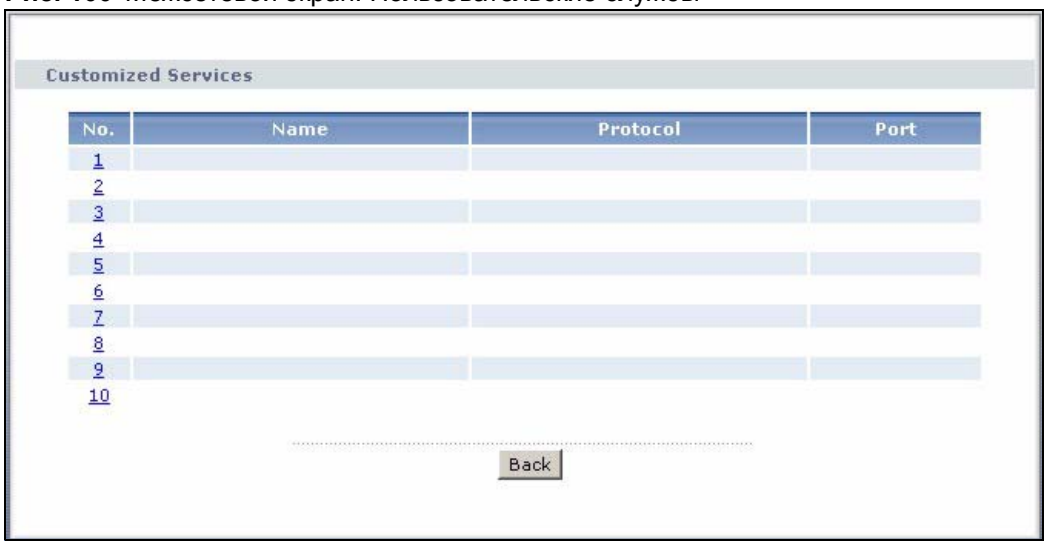
ПОЛЕ	ОПИСАНИЕ
Schedule (График)	
Day to Apply (День применения)	Выберите, должно ли правило применяться каждый день (Everyday) или в определенные дни недели.
Time of Day to Apply (24-Hour Format) (Время применения в 24-часовом формате)	Выберите **All Day (Круглосуточно)** или введите время начала и окончания применения правила в часах и минутах.
Log (Регистрационный журнал)	
Log Packet Detail Information (Регистрировать подробную информацию о пакете)	Это поле определяет, создается или нет запись в регистрационном журнале для пакетов, соответствующих данному правилу. Перейдите на страницу **Log Settings (Настройки регистрационного журнала)** и выберите категорию **Access Control (Управление доступом)**, чтобы включить ведение журналов регистрации P660HWP.
Alert (Предупреждение)	
Send Alert Message to Administrator When Matched (Посылать администратору предупреждение при совпадении)	Поставьте флажок, чтобы P660HWP генерировал извещение, если происходит событие, соответствующее условиям данного правила.
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить измененные настройки и выйти из этого окна.
Cancel (Отменить)	Нажмите кнопку **Cancel**, чтобы выйти из этого окна без сохранения изменений.

11.6.2 Пользовательские службы

В межсетевом экране P660HWP можно настроить пользовательские службы и соответствующие им номера портов. Полный перечень номеров портов и служб приведен на сайте IANA (Internet Assigned Number Authority – Агентство по назначению имен и уникальных параметров протоколов Интернет). Дополнительную информацию по службам см. Разд. 11.8 на с. 199. Щелкните по ссылке **Edit Customized Services (Редактирование пользовательских служб)** в окне редактирования правил межсетевого экрана, чтобы установить для пользовательской службы номер порта. При этом откроется следующее окно.

Более подробную информацию см. Разд. 10.1 на с. 169.

Рис. 100 Межсетевой экран: Пользовательские службы



В следующей таблице даны описания полей этого окна.

Табл. 62 Пользовательские службы

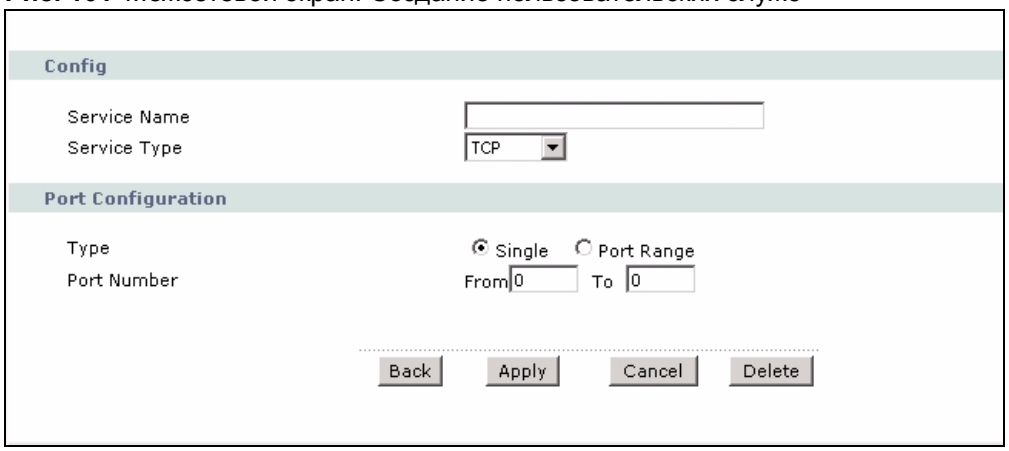
ПОЛЕ	ОПИСАНИЕ
No. (Номер)	Номер дополнительно назначаемого пользовательского порта. Щелкните по номеру правила службы для перехода к окну, где можно создать новую службу или изменить существующую. Более подробную информацию см. Разд. 11.6.3 на с. 194.
Name (Имя)	В этом поле отображается название пользовательской службы.
Protocol (Протокол)	В этом поле отображается протокол IP (**TCP**, **UDP** или **TCP/UDP**), определяющий пользовательскую службу.
Port (Порт)	В этом поле отображается номер порта или диапазон, определяющий пользовательскую службу.
Back (Назад)	Нажмите кнопку **Back (Назад)** для возвращения к экрану **Firewall Edit Rule (Редактирование правил межсетевого экрана)**.

11.6.3 Настройка пользовательских служб

Выберите номер правила в окне **Firewall Customized Services (Межсетевой экран: Пользовательские службы)**, чтобы создать новый пользовательский порт или отредактировать существующий. Появится следующий экран.

Более подробную информацию см. Разд. 10.1 на с. 169.

Рис. 101 Межсетевой экран: Создание пользовательских служб



В следующей таблице даны описания полей этого окна.

Табл. 63 Межсетевой экран: Создание пользовательских служб

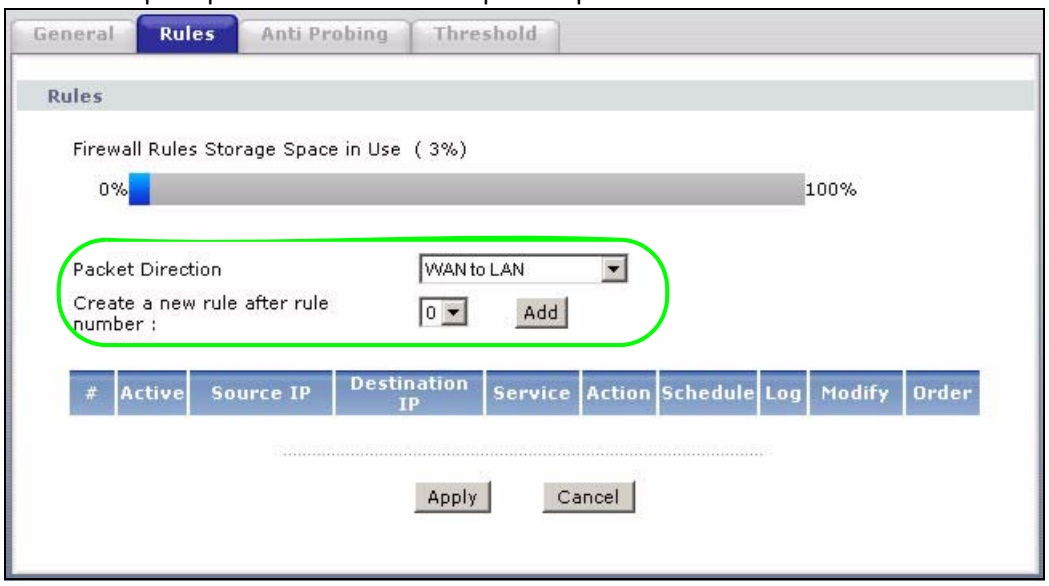
ПОЛЕ	ОПИСАНИЕ
Service Name (Имя услуги)	Введите уникальное имя для пользовательского порта.
Service Type (Тип службы)	Выберите из выпадающего списка порт IP (**TCP**, **UDP** или **TCP/UDP**) для пользовательского порта.
Port Configuration (Настройка порта)	
Type (Тип)	Выберите **Single (Одиночный)** для одного порта или **Range (Диапазон)** для диапазона из нескольких портов, связанных с пользовательской службой.
Port Number (Номер порта)	Введите один номер или диапазон номеров портов, связанных с пользовательской службой.
Back (Назад)	Для возврата к предыдущему окну нажмите кнопку **Back (Назад)**.
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить измененные настройки и выйти из этого окна.
Cancel (Отменить)	Для возврата к предыдущему окну щелкните по кнопке **Cancel (Отменить)**.
Delete (Удалить)	Нажмите кнопку **Delete (Удалить)** для удаления текущего правила и возвращения к предыдущему экрану.

11.7 Пример правила межсетевого экрана

В следующем примере правило межсетевого экрана для Интернета разрешает гипотетическое соединение «MyService» из Интернета.

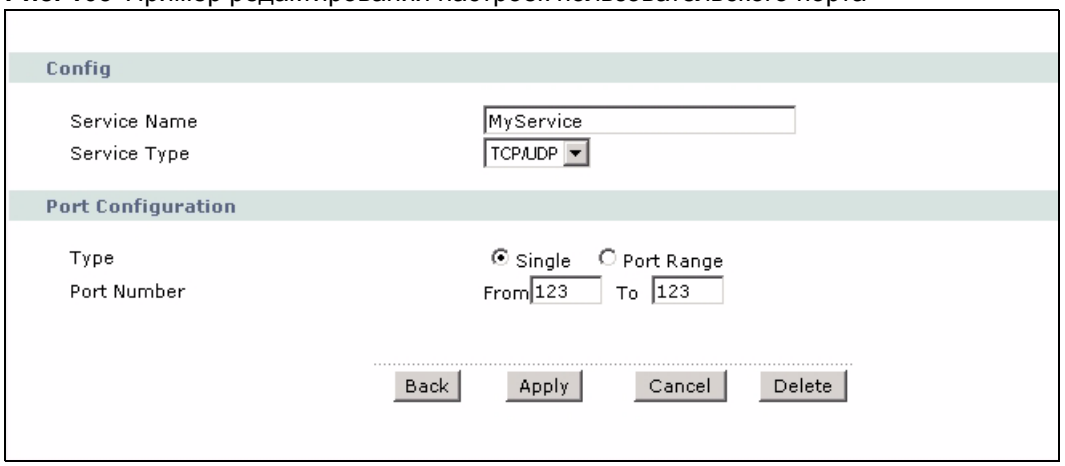
1. Щелкните **Security (Безопасность)** > **Firewall (Межсетевой экран)** > **Rules (Правила)**.
2. Выберите **WAN to LAN (Глоб. сеть – лок. сеть)** в поле **Packet Direction (Маршрут пакета)**.

Рис. 102 Пример окна межсетевого экрана: Правила



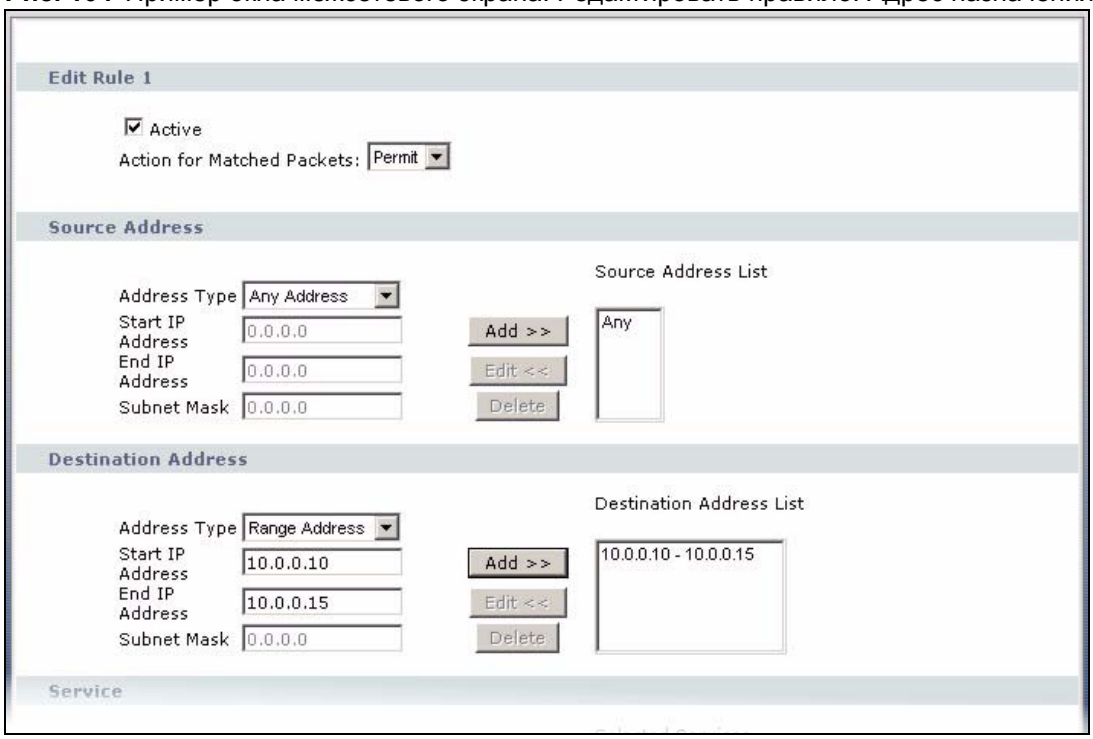
3. В окне **Rules (Правила)** выберите порядковый номер правила, после которого должно разместиться новое правило. Например, если вы выберете «6», новое правило будет иметь номер 7, а старое правило под номером 7 (если есть) будет иметь номер 8.
4. Нажмите кнопку **Add (Добавить)** для отображения окна настройки правила межсетевого экрана.
5. В окне **Edit Rule (Редактировать правило)** щелкните по ссылке **Edit Customized Services (Редактирование пользовательских служб)** для отображения окна **Customized Service (Пользовательские службы)**.
6. Щелкните по номеру правила для отображения окна **Customized Services Config (Настройка пользовательских служб)**, установите параметры, как показано ниже, и нажмите кнопку **Apply (Применить)**.

Рис. 103 Пример редактирования настроек пользовательского порта



7. В окне **Destination Address (Адрес назначения)** выберите **Any (любой)**, а затем нажмите **Delete (Удалить)**.
8. Выполните настройки в окне адреса получателя, как показано ниже, и нажмите кнопку **Add (Добавить)**.

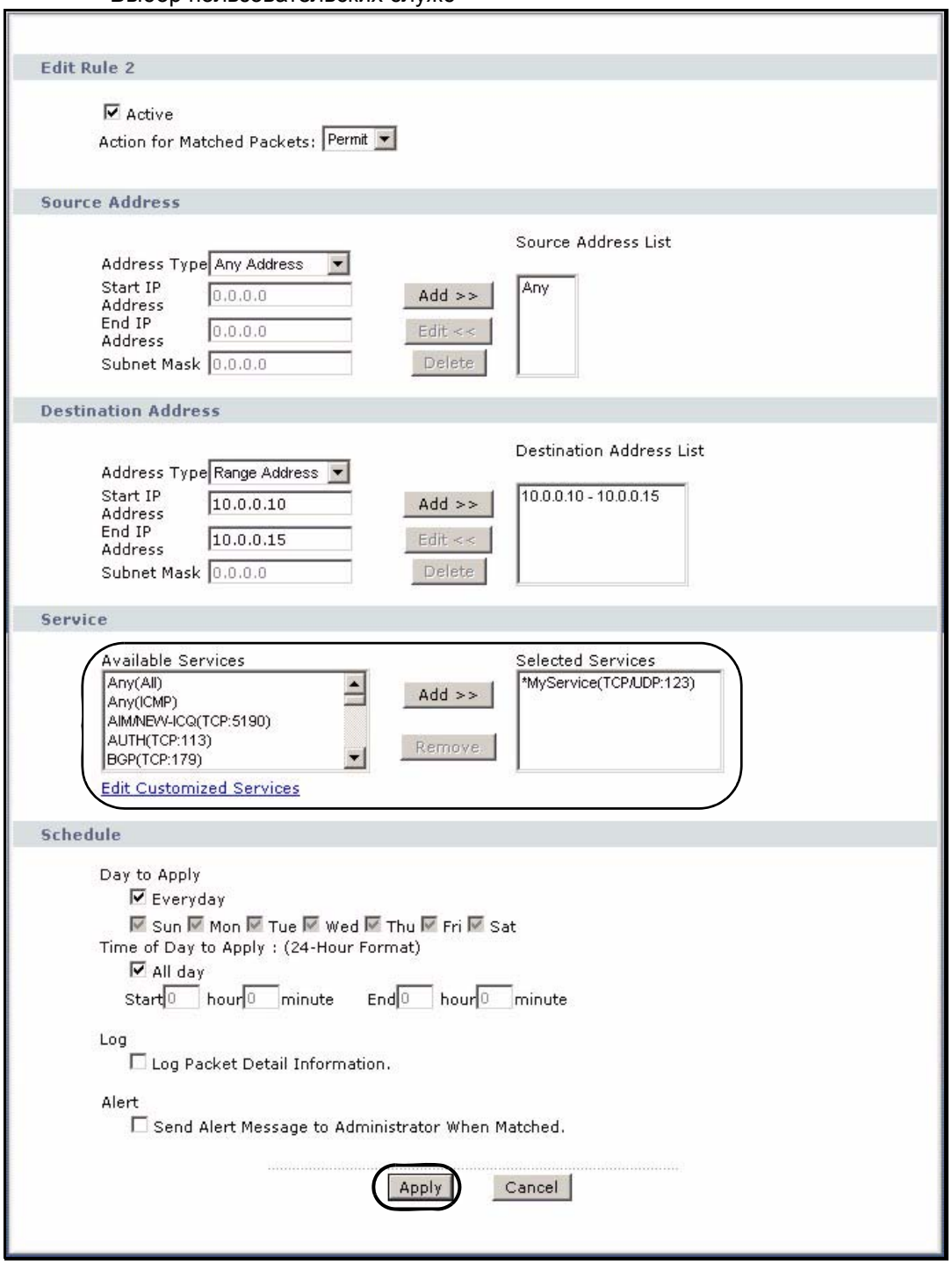
Рис. 104 Пример окна межсетевого экрана: Редактировать правило: Адрес назначения



9 С помощью кнопок **Add (Добавить)** >> и **Remove (Удалить)** между полями со списками **Available Services (Доступные службы)** и **Selected Services (Выбранные службы)** установите параметры, как показано ниже. По окончании нажмите **Apply (Применить)**.

В списках Services (Службы) и Rules (Правила) пользовательские службы отмечены символом «*»” перед именем.

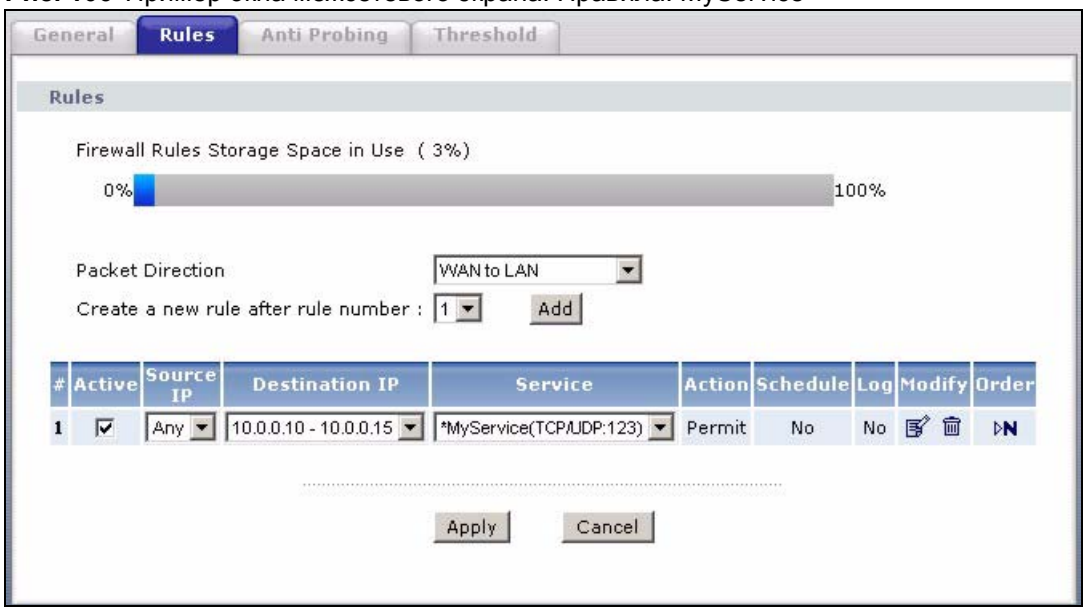
Рис. 105 Пример окна межсетевого экрана: Редактировать правило: Выбор пользовательских служб



По завершении настройки правила межсетевого экрана для Интернета, окно **Rules (Правила)** должно выглядеть следующим образом.

Правило 1 разрешает соединение «MyService» между глобальной сетью и диапазоном IP-адресов локальной сети 10.0.0.10–10.0.0.15.

Рис. 106 Пример окна межсетевого экрана: Правила: MyService



11.8 Предварительно настроенные службы

Список **Available Services (Доступные службы)** в окне **Edit Rule (Редактировать правило)** (см. Разд. 11.6.1 на с. 190) содержит все предварительно настроенные службы, которые интернет-центр P660HWP уже поддерживает. Рядом с названием службы располагаются два поля в скобках. В первом поле указывается тип протокола IP (TCP, UDP или ICMP). Во втором – номер порта IP для данной службы. Следует учесть, что тип протокола IP может быть не один. В качестве примера можно привести конфигурацию по умолчанию с обозначением «(**DNS**)». **(UDP/TCP:53)** означает UDP-порт 53 и TCP-порт 53. Возможно до 128 записей. Порты пользовательских служб можно настроить также с помощью функции **Edit Customized Services (Редактирование пользовательских служб)**, о которой было рассказано выше.

Табл. 64 Предварительно настроенные службы

СЛУЖБА	ОПИСАНИЕ
AIM/NEW_ICQ(TCP:5190)	Система пересылки сообщений в сети Интернет, предоставляемая корпорацией AOL, используется службой ICQ как «слушающий» порт.
AUTH(TCP:113)	Протокол аутентификации, используется некоторыми серверами.
BGP(TCP:179)	Протокол BGP (пограничный межсетевой протокол).
BOOTP_CLIENT(UDP:68)	Клиент DHCP.
BOOTP_SERVER(UDP:67)	Сервер DHCP.
CU-SEEME(TCP/UDP:7648, 24032)	Популярное решение для проведения видеоконференций от White Pines Software.
DNS(UDP/TCP:53)	Сервер имен доменов – служба, определяющая соответствие web-имен (например, www.zyxel.com) и номеров IP.
FINGER(TCP:79)	Finger – команда для UNIX или Интернет, используемая для проверки нахождения пользователя в сети.

Табл. 64 Предварительно настроенные службы (продолжение)

СЛУЖБА	ОПИСАНИЕ
FTP(TCP:20.21)	Протокол передачи файлов, программа для быстрой передачи файлов, в том числе файлов большого размера, которые невозможно пересылать средствами электронной почты.
H.323(TCP:1720)	Протокол для Net Meeting.
HTTP(TCP:80)	Протокол передачи гипертекста – протокол уровня клиент/сервер для WWW.
HTTPS	HTTPS - это надежный сеанс связи http, часто используемый в электронной коммерции.
ICQ(UDP:4000)	Популярная система интерактивного общения в Интернет.
IPSEC_TRANSPORT/ TUNNEL(AH:0)	Эту службу использует протокол туннелирования IPSEC AH (Заголовок аутентификации).
IPSEC_TUNNEL(ESP:0)	Эту службу использует протокол туннелирования IPSEC ESP (Протокол обеспечения безопасности инкапсуляции).
IRC(TCP/UDP:6667)	Еще одна программа интерактивного общения в Интернет.
MSN Messenger(TCP:1863)	Протокол для передачи сообщений в сетях Microsoft.
MULTICAST(IGMP:0)	Internet Group Multicast Protocol (Широковещательный протокол взаимодействия групп в сети Интернет) используется для отправки пакетов определенным группам узлов.
NEWS(TCP:144)	Протокол для групп новостей.
NFS(UDP:2049)	Сетевая файловая система – NFS, распределенная файловая система клиент/сервер, обеспечивающая прозрачное совместное использование файлов в сетевом окружении.
NNTP(TCP:119)	Network News Transport Protocol (Сетевой протокол передачи новостей) – система доставки для групп новостей USENET.
PING(ICMP:0)	Packet INternet Groper (Пакетное эхо-тестирование в Интернет) – это протокол, который посылает эхо-запросы ICMP для проверки достижимости удаленного узла.
POP3(TCP:110)	Почтовый протокол версии 3, позволяет клиентскому компьютеру получать электронную почту с сервера POP3, используя временное соединение (TCP/IP или другое).
PPTP(TCP:1723)	Point-to-Point Tunneling Protocol (Протокол туннелирования «точка-точка») обеспечивает безопасную передачу данных в общедоступных сетях. Это канал управления.
PPTP_TUNNEL(GRE:0)	Point-to-Point Tunneling Protocol (Протокол туннелирования «точка-точка») обеспечивает безопасную передачу данных в общедоступных сетях. Это канал передачи данных.
RCMD(TCP:512)	Удаленное управление командной строкой.
REAL_AUDIO(TCP:7070)	Система прямого воспроизведения звука, обеспечивает передачу аудиопотоков в сети в реальном времени.
REXEC(TCP:514)	Daemon-служба удаленного выполнения команд.
RLOGIN(TCP:513)	Удаленная регистрация.
RTELNET(TCP:107)	Удаленный доступ через Telnet.
RTSP(TCP/UDP:554)	Протокол (Real Time Streaming – Протокол воспроизведения в реальном времени) – это удаленное управление для мультимедиа в Интернете.
SFTP(TCP:115)	Простой протокол передачи файлов.

Табл. 64 Предварительно настроенные службы (продолжение)

СЛУЖБА	ОПИСАНИЕ
SMTP(TCP:25)	Simple Mail Transfer Protocol (Простой протокол электронной почты) – стандартный протокол обмена сообщениями для сети Интернет. SMTP обеспечивает пересылку сообщений с одного почтового сервера на другой.
SNMP(TCP/UDP:161)	Simple Network Management Program (Простой протокол управления сетью).
SNMP-TRAPS (TCP/ UDP:162)	Система регистрации событий в потоке SNMP (RFC:1215).
SQL-NET(TCP:1521)	Structured Query Language (Язык структурированных запросов) представляет собой интерфейс для доступа к данным на различных типах систем баз данных, включая универсальные вычислительные машины, системы средней производительности, системы UNIX и сетевые серверы.
SSDP(UDP:1900)	Протокол упрощенной службы обнаружения (SSDP) – это служба обнаружения, отыскивающая устройства типа Plug and Play в домашней сети или шлюзы в Интернете для предачи данных при помощи порта 1900 протокола DUDP.
SSH(TCP/UDP:22)	Программа для обеспечения безопасной удаленной регистрации.
STRMWORKS(UDP:1558)	Протокол передачи потоков Stream Works.
SYSLOG(UDP:514)	Syslog (Системный журнал) позволяет отправлять системные журналы на сервер UNIX.
TACACS(UDP:49)	Login Host Protocol (Протокол регистрации узла), используется для TACACS (Terminal Access Controller Access Control System – Система управления доступом на основе контроллера доступа к терминалу).
TELNET(TCP:23)	Telnet – протокол регистрации и эмуляции терминала, общий для среды Интернет и UNIX. Он работает в сетях TCP/IP. Его главная функция заключается в обеспечении регистрации пользователей на удаленных узлах.
TFTP(UDP:69)	Trivial File Transfer Protocol (Упрощенный протокол передачи файлов) – это протокол передачи файлов в Интернет, подобный FTP, но использующий UDP (Протокол передачи дейтаграмм пользователя), а не TCP (Протокол управления передачей).
VDOLIVE(TCP:7000)	Еще одна программа для видеоконференций.

11.9 Предотвращение зондирования

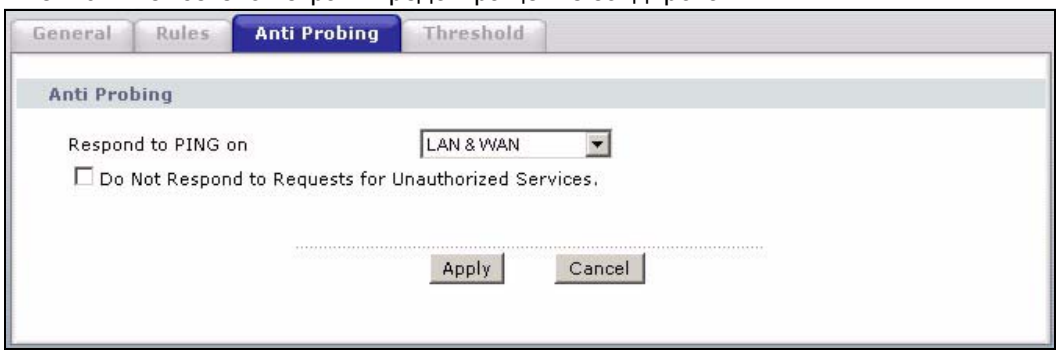
Если внешний пользователь попытается прозондировать неподдерживаемый порт P660HWP, ему будет автоматически отправлен ответный пакет ICMP. Это позволяет внешнему пользователю узнать о существовании интернет-центра P660HWP. Также P660HWP поддерживает предотвращение зондирования без отправки ответного пакета ICMP. Это позволяет скрыть существование P660HWP от посторонних лиц при попытке эхо-тестирования неподдерживаемого порта.

Протокол управляющих сообщений в сети Интернет (ICMP) является протоколом управляющих сообщений и сообщений об ошибках между сервером-узлом и шлюзом выхода в Интернет. ICMP использует дейтаграммы протокола Интернета (IP), но сообщения обрабатываются программным обеспечением TCP/IP, и невидимы для пользователей приложений.

Более подробную информацию см. Разд. 10.1 на с. 169.

Щелкните **Security (Безопасность)** > **Firewall (Межсетевой экран)** > **Anti Probing (Блокирование эхо-тестирования)** для отображения окна, как показано ниже.

Рис. 107 Межсетевой экран: Предотвращение зондирования



В следующей таблице даны описания полей этого окна.

Табл. 65 Межсетевой экран: Предотвращение зондирования

ПОЛЕ	ОПИСАНИЕ
Respond to PING on (Отвечать на PING-запросы)	Интернет-центр P660HWP не отвечает на входящие Ping-запросы, если в поле **Disable (Отключить)** установлен флажок. Выберите **LAN** для ответа на входящие Ping-запросы из локальной сети. Выберите **WAN** для ответа на входящие Ping-запросы по глобальной сети. В противном случае выберите **LAN & WAN** для ответа на Ping-запросы как по локальной, так и глобальной сети.
Do not respond to requests for unauthorized services (Не отвечать на запросы для запрещеных служб).	Установите флажок, чтобы предотвратить обнаружение хакерами интернет-центра P660HWP посредством эхо-тестирования неиспользуемых портов. Если флажок установлен, P660HWP не будет отвечать на запросы на неиспользуемые порты. Таким образом, неиспользуемые порты и интернет-центр P660HWP остаются невидимыми. По умолчанию флажок снят и P660HWP посылает пакет ICMP «Port Unreachable» (Порт недоступен) в ответ на зондирование неиспользуемых портов UDP, а в ответ на зондирование неиспользуемых портов TCP – пакет «TCP Reset» (Сброс TCP). Следует отметить, что прежде чем зондирующие пакеты достигнут механизма блокирования эхо-тестирования, они сначала должны пройти через межсетевой экран P660HWP. Следовательно, если механизм межсетевого экрана блокирует зондирующий пакет, реакция P660HWP производится на основе политики межсетевого экрана: в ответ на заблокированный пакет TCP посылается пакет «сброс TCP», на заблокированный пакет UDP – пакет ICMP «порт недоступен», или пакеты просто сбрасываются без отправки ответных пакетов.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек P660HWP.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.

11.10 Допустимые пороги для атак «Отказ в обслуживании» (DoS)

Для атак типа DoS интернет-центр P660HWP применяет пороги, которые определяют, когда следует сбросить сеанс связи, находящийся в процессе установления соединения. Данные допустимые пороги относятся в целом ко всем сессиям.

Можно использовать значения допустимых порогов по умолчанию или установить собственные в соответствиями с требованиями безопасности.

Настройка порогов – см. Разд. 11.10.3 на с. 204.

11.10.1 Значения допустимых порогов

Если что-то не работает и счетчики сетевого экрана проверены, необходимо настроить данные параметры. Значения, установленные по умолчанию, хорошо подходят для небольших офисов. Выбор значений допустимых порогов зависит от следующих величин:

- Максимальное количество открытых сессий.
- Минимальное количество возможных незавершенных заданий на сервере локальной сети.
- Возможности центральных процессоров серверов локальной сети.
- Пропускная способность сети.
- Тип трафика для отдельных серверов.

Если по причинам, зависящим от каких-то из вышеперечисленных факторов, сеть работает медленнее, чем обычно (особенно если имеются медленные серверы или серверы, обрабатывающие большое количество задач, которые часто перегружены), значения по умолчанию необходимо уменьшить.

Изменять значения допустимых порогов необходимо до продолжения работы по настройке параметров межсетевого экрана.

11.10.2 Полуоткрытые сеансы связи

Слишком большое количество полуоткрытых сеансов связи (выраженное конкретным числом или в виде частоты поступлений) может означать наличие атаки DoS. Применительно к TCP, «полуоткрытые» сеансы – это сеансы связи, не дошедшие до состояния установленных, т. е. когда не завершено трехстороннее квитирование по TCP (см. Рис. 93 на с. 173). Для UDP «полуоткрытое» состояние означает, что межсетевой экран не обнаружил ответный трафик.

P660HWP измеряет общее количество существующих полуоткрытых сеансов и интенсивность попыток установления сеансов. Для обоих типов соединений, TCP и UDP, считается количество полуоткрытых соединений и интенсивность поступлений. Подсчеты производятся поминутно.

Когда число существующих полуоткрытых сеансов связи превышает порог **max-incomplete high (верхний предел полуоткрытых сеансов)**, интернет-центр P660HWP начинает удалять полуоткрытые сеансы связи для выполнения новых запросов на установление соединение. P660HWP удаляет полуоткрытые сеансы до тех пор, пока их количество не станет меньше, чем значение порога **max-incomplete low (нижний предел полуоткрытых сеансов)**.

Когда интенсивность новых попыток установления соединения превышает порог **one-minute high (верхний порог интенсивности)**, P660HWP начинает удалять полуоткрытые сеансы связи для выполнения новых запросов на установление соединение. The P660HWP удаляет полуоткрытые сеансы до тех пор, пока значение интенсивности новых попыток установления соединения не станет меньше, чем значение порога **one-minute low (нижний порог интенсивности)**. Частота соединений – это количество новых попыток, обнаруженное за последний установленный период выборки длительностью в одну минуту.

11.10.2.1 Максимум неполных TCP-соединений и время блокирования

Слишком большое количество полуоткрытых соединений с одним и тем же адресом узла получателя может означать атаку DoS, направленную на данный компьютер-узел.

Пока количество полуоткрытых соединений с одним и тем же адресом назначения превышает допустимый порог **TCP Maximum Incomplete (Максимум неполных TCP)** P660HWP удаляет полуоткрытые соединения одним из следующих способов:

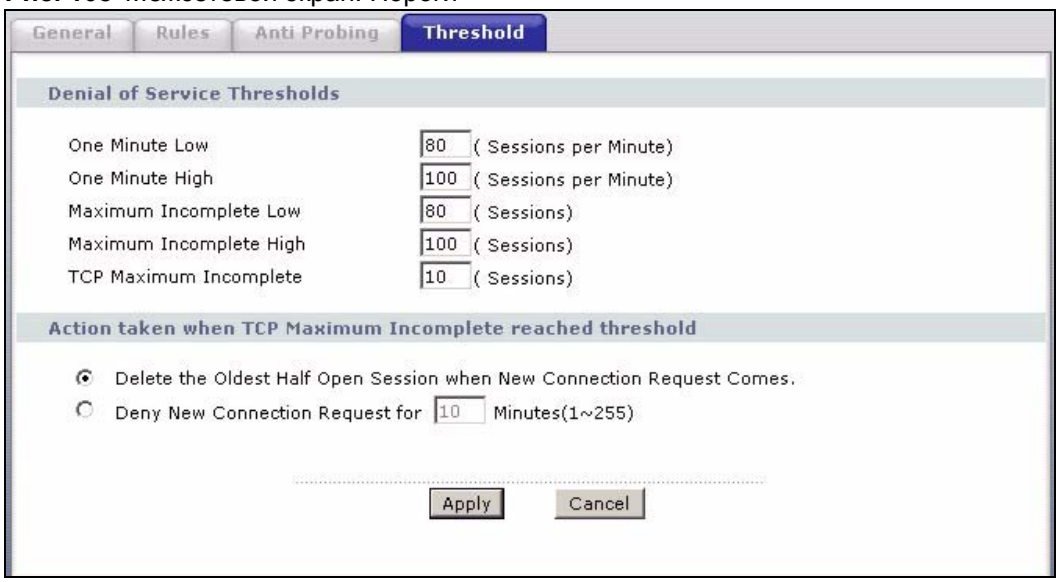
- Если значение **Blocking Time (Время блокирования)** установлено на 0 (по умолчанию), P660HWP удаляет самый старый из существующих полуоткрытых сеансов для данного узла при каждом новом запросе на установление соединения. В этом случае количество полуоткрытых соединений для данного узла не может превысить допустимый порог.
- Если значение **Blocking Time (Время блокирования)** больше 0, P660HWP блокирует все вновь поступающие на данный узел запросы на установление соединения, оставляя серверу время обработать текущие запросы. Интернет-центр P660HWP блокирует все новые запросы на установление соединения до тех пор, пока не истечет время, установленное в поле **Blocking Time (Время блокирования)**.

11.10.3 Настройка порогов межсетевого экрана

Интернет-центр P660HWP также посылает извещения, каждый раз, когда превышается значение **TCP Maximum Incomplete (Максимум неполных TCP)**. Глобальные значения допустимого порога и времени ожидания действительны для всех TCP-соединений.

Нажмите кнопку **Firewall (Межсетевой экран)**, а затем **Threshold (Пороги)**, чтобы открыть следующее окно.

Рис. 108 Межсетевой экран: Пороги



В следующей таблице даны описания полей этого окна.

Табл. 66 Межсетевой экран: Пороги

ПОЛЕ	ОПИСАНИЕ	ЗНАЧЕНИЯ ПО УМОЛЧАНИЮ
Denial of Service Thresholds (Значения допустимых порогов для атак DoS)		
One Minute Low (Нижний порог интенсивности)	Частота появления новых полуоткрытых соединений, при которой межсетевой экран прекращает удалять полуоткрытые соединения. P660HWP удаляет полуоткрытые сеансы до тех пор, пока значение интенсивности новых попыток установления соединения не станет меньше, чем это число.	80 существующих полуоткрытых соединений.
One Minute High (Верхний порог интенсивности)	Частота появления новых полуоткрытых соединений, при которой межсетевой экран начинает удалять полуоткрытые соединения. Когда интенсивность новых попыток установления соединения превышает это число, P660HWP начинает удалять полуоткрытые сеансы связи для выполнения новых запросов на установление соединения.	100 полуоткрытых соединений в минуту. Указанные выше величины означают, что интернет-центр P660HWP начнет удалять полуоткрытые соединения, как только в течении последней минуты будет зафиксировано более 100 попыток установки соединения, и прекратит удалять полуоткрытые соединения, когда в течение последней минуты будет зафиксировано менее 80 попыток.
Maximum Incomplete Low (Нижний предел полуоткрытых сеансов)	Количество существующих полуоткрытых соединений при котором межсетевой экран прекращает удалять полуоткрытые соединения. P660HWP удаляет полуоткрытые сеансы до тех пор, пока количество существующих полуоткрытых соединений не станет меньше, чем это число.	80 существующих полуоткрытых соединений.

Табл. 66 Межсетевой экран: Пороги (продолжение)

ПОЛЕ	ОПИСАНИЕ	ЗНАЧЕНИЯ ПО УМОЛЧАНИЮ
Maximum Incomplete High (Верхний предел полуоткрытых сеансов)	Количество существующих полуоткрытых соединений, при котором межсетевой экран начинает удалять полуоткрытые соединения. Когда количество существующих полуоткрытых сеансов связи превышает это число, интернет-центр P660HWP начинает удалять полуоткрытые сеансы связи для выполнения новых запросов на установление соединений. Нельзя устанавливать значение верхнего предела полуоткккрытых сеансов ниже текущего значения нижнего предела.	100 существующих полуоткрытых соединений. Указанные выше величины означают, что интернет-центр P660HWP начнет удалять полуоткрытые соединения, как только количество существующих полуоткрытых соединений превысит 100, и прекратит удалять полуоткрытые соединения, если количество текущих сеансов станет меньше 80.
TCP Maximum Incomplete (Максимум полуоткрытых TCP соединений)	Количество существующих полуоткрытых соединений через TCP с одним и тем же IP-адресом получателя, при котором межсетевой экран начинает сбрасывать полуоткрытые соединения с адресатом по данному IP-адресу. Введите число от 1 до 256. Обычно в случае небольшой сети, медленной системы или ограниченной пропускной способности выбирается небольшое количество.	10 существующих полуоткрытых TCP-соединений.
Action taken when the TCP Maximum Incomplete threshold is reached (Действия при достижении максимального количества полуоткрытых TCP-соединений).		
Delete the oldest half open session when new connection request comes (Удалить самое старое полуоткрытое соединение при получении запроса на новое соединение)	Выберите эту опцию для удаления самого старого полуоткрытого соединения при получении запроса на новое соединение.	
Deny new connection request for (Не принимать новые запросы в течение)	Выберите эту опцию и укажите, как долго интернет-центр P660HWP должен блокировать запросы на новое соединение при достижении порога **TCP Maximum Incomplete (Максимум неполных TCP)**. Введите длительность блокировки в минутах (от 1 до 256).	
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек P660HWP.	
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.	

12

Фильтрация на основе содержания (контентная фильтрация)

В этой части дается обзор настройки контент-фильтрования.

12.1 Фильтрация на основе содержания – общая информация

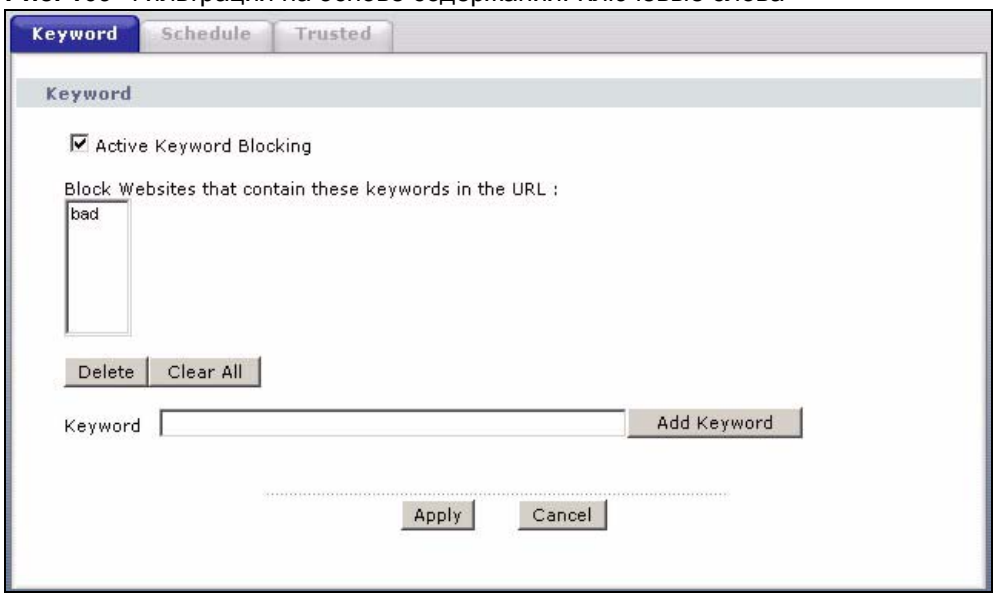
Фильтрация информации, поступающей из Интернета позволяет создавать и реализовывать правила доступа в Интернет, настроенные под конкретные потребности. Фильтрация на основе содержания дает возможность блокировать сайты по определенным ключевым словам в URL. Можно установить расписание, по которому P660HWP будет выполнять фильтрацию. Также можно задать доверенные IP-адреса в локальной сети, для которых P660HWP не будет выполнять фильтрацию.

12.2 Настройка блокировки по ключевым словам

Это окно используется для блокировки сайтов, содержащих определенные ключевые слова в URL. Например, если установить ключевое слово «bad», то интернет-центр P660HWP заблокирует доступ по всем сайтам, содержащим это слово, в том числе URL http://www.website.com/bad.html, даже если он не включен в список фильтрации.

Для того, чтобы интернет-центр P660HWP блокировал Web-сайты, содержащие ключевые слова в URL, щелкните **Security (Безопасность)** > **Content Filter (Фильтрация на основе содержания)**. При этом откроется показанное ниже окно.

Рис. 109 Фильтрация на основе содержания: Ключевые слова



В следующей таблице даны описания полей этого окна.

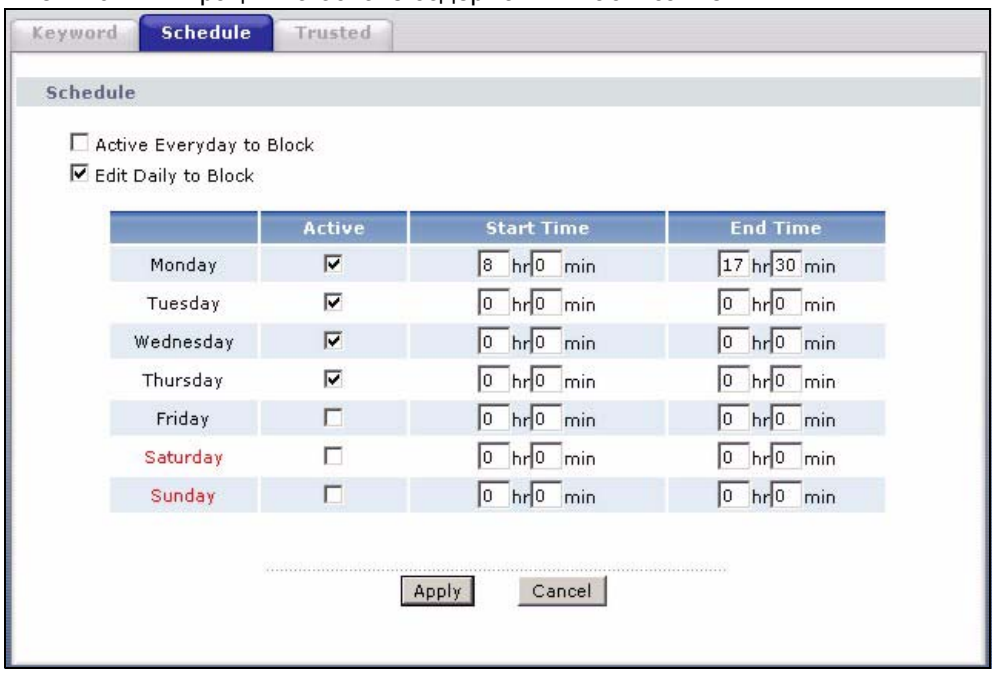
Табл. 67 Фильтрация на основе содержания: Ключевые слова

ПОЛЕ	ОПИСАНИЕ
Active Keyword Blocking (Включить блокирование по ключевым словам)	Поставьте флажок в этом поле для включения функции.
Block Websites that contain these keywords in the URL: (Блокирование Web-сайтов, содержащих в URL ключевые слова:)	Это поле содержит список всех установленных ключевых слов, по которым P660HWP будет производить блокирование сайтов.
Delete (Удалить)	Выделите ключевое слово в списке и нажмите **Delete (Удалить)**, чтобы удалить его.
Clear All (Очистить все)	Нажмите **Clear All (Очистить все)**, чтобы удалить все ключевые слова из этого списка.
Keyword (Ключевое слово)	Введите в это поле ключевое слово. Допускается использование любых символов (количеством до 127). Использование знаков препинания не допускается.
Add Keyword (Добавить ключевое слово)	Нажмите **Add Keyword (Добавить ключевое слово)** после ввода ключевого слова. Повторите эту процедуру, если нужно добавить другие ключевые слова. Допускается до 64 ключевых слов. При попытке доступа к web-странице, содержащей ключевое слово, будет выведено сообщение о том, что контент-фильтр заблокировал запрос.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек P660HWP.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)** для возврата к предыдущим сохраненным настройкам.

12.3 Настройка расписания фильтрации

Чтобы установить дату и время, когда P660HWP должен выполнять фильтрацию контента, щелкните **Security (Безопасность)** > **Content Filter (Фильтрация на основе содержания)** > **Schedule (Расписание)**. При этом откроется показанное ниже окно.

Рис. 110 Фильтрация на основе содержания: Расписание



В следующей таблице даны описания полей этого окна.

Табл. 68 Фильтрация на основе содержания: Расписание

ПОЛЕ	ОПИСАНИЕ
Schedule (График)	Установите флажок в поле **Active Everyday to Block (Выполнять блокирование каждый день)**, чтобы фильтрация контента выполнялась каждый день. В другом случае, установите флажок в поле **Edit Daily to Block (Установить дни для блокирования)** и выберите дни недели (или каждый день), а также время дня, когда необходимо выполнять фильтрацию контента.
Active Everyday to Block (Активировать ежедневное блокирование	Установите флажок в это поле для включения непрерывной фильтрации веб-сайтов по выбранным ключевым словам.
Edit Daily to Block (Редактировать ежедневное блокирование)	Установите флажок в это поле для включения фильтрации веб-сайтов по указанным дням и времени.
Active (Активировать)	Установите флажок, чтобы выполнять фильтрацию контента в выбранный день.
Start Time (Начальное время)	Введите время, когда необходимо начать выполнение фильтрации контента в формате «часы - минуты».

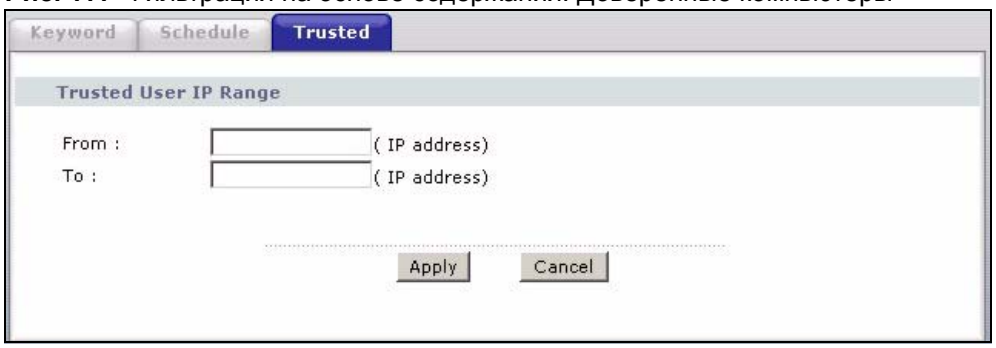
Табл. 68 Фильтрация на основе содержания: Расписание (продолжение)

ПОЛЕ	ОПИСАНИЕ
End Time (Конечное время)	Введите время, когда необходимо прекратить выполнение фильтрации контента в формате «часы - минуты».
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить изменения.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)** для возврата к предыдущим сохраненным настройкам.

12.4 Настройка списка доверенных компьютеров

Чтобы P660HWP не выполнял фильтрацию контента для определенных пользователей в локальной сети, щелкните **Security (Безопасность)** > **Content Filter (Фильтрация на основе содержания)** > **Trusted (Доверенные компьютеры)**. При этом откроется показанное ниже окно.

Рис. 111 Фильтрация на основе содержания: Доверенные компьютеры



В следующей таблице даны описания полей этого окна.

Табл. 69 Фильтрация на основе содержания: Доверенные компьютеры

ПОЛЕ	ОПИСАНИЕ
Trusted User IP Range (Диапазон IP-адресов доверенных пользователей)	
From (От)	Введите IP-адрес компьютера локальной сети (или начальный IP-адрес конкретного диапазона компьютеров), который необходимо исключить из контент-фильтрования.
To (До)	Введите конечный IP-адрес конкретного диапазона пользователей локальной сети, которых необходимо исключить из контент-фильтрования. Оставьте это поле не заполненным, если необходимо исключить отдельный компьютер.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек P660HWP.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)** для возврата к предыдущим сохраненным настройкам.

13

Сертификаты

В этой главе представлена вводная информация о сертификатах открытого ключа и рассказывается об их использовании.

13.1 Сертификаты – общее описание

В интернет-центре P660HWP для аутентификации пользователей можно использовать сертификаты, называемые также цифровыми идентификаторами. Сертификаты основываются на парах открытых секретных ключей. Каждый сертификат содержит идентификатор владельца и открытый ключ. Сертификаты обеспечивают обмен открытыми ключами для проведения аутентификации.

Центр сертификации (Certification Authority – CA) выдает сертификаты и гарантирует подлинность владельца сертификата. Существуют коммерческие центры сертификации, такие как CyberTrust и VeriSign, а также правительственные центры сертификации. Интернет-центр P660HWP может генерировать запросы на сертификацию, содержащие идентифицирующую информацию и открытые ключи, и затем отправлять эти запросы в центр сертификации.

При использовании аутентификации по открытому ключу каждый узел имеет два ключа. Первый ключ является открытым и доступным; второй ключ является секретным и должен храниться в тайне. Шифрование для аутентификации с использованием открытого ключа производится следующим образом.

1. Тим хочет отправить Дженни конфиденциальное сообщение. Тим создает открытый и секретный ключи. Данные, зашифрованные с помощью первого ключа, могут быть расшифрованы только с помощью второго ключа.
2. Тим хранит у себя секретный ключ и предоставляет открытый ключ.
3. Тим зашифровывает сообщение с помощью секретного ключа и отправляет сообщение Дженни.
4. Дженни получает сообщение и использует открытый ключ Тима для расшифровывания сообщения.
5. Кроме того, Дженни использует свой секретный ключ для шифрования сообщения, а Тим использует открытый ключ Дженни для расшифровывания сообщения.

Для идентификации пользователей, пытающихся установить подключение, устройство P660HWP использует сертификаты на основе технологии открытого ключа. Способ защиты данных, которые пересылаются по установленному соединению, зависит от типа соединения. Например, в туннеле VPN может использоваться алгоритм шифрования Triple DES.

В центре сертификации для подписи сертификатов используются свои секретные ключи. Открытые ключи центра сертификации используются для проверки сертификатов.

Путь к сертификату – это иерархия сертификатов центра сертификации, подтверждающая достоверность сертификата. Интернет-центр P660HWP считает сертификат ненадежным, если срок действия этого сетификата в иерархии закончился или сертификат аннулирован.

Центры сертификации поддерживают серверы каталогов, содержащих базы данных действительных и аннулированных сертификатов. Каталог сертификатов, которые были аннулированы до запланированного окончания срока действия, называется CRL (Certificate Revocation List – Список аннулированных сертификатов). Интернет-центр P660HWP может проверить сертификат удаленного устройства по списку аннулированных сертификатов на сервере каталогов. Структура серверов, программного обеспечения, методик и правил для обработки ключей называется PKI (Public-key infrastructure – Инфраструктура открытого ключа).

13.1.1 Преимущества сертификатов

Сертификаты имеют следующие преимущества.

- Интернет-центр P660HWP хранит только сертификаты из центра сертификации, которые попали в категорию доверенных, вне зависимости от того, сколько устройств должны проходить аутентификацию.
- Распределение ключей является простой и очень надежной процедурой, так как открытые ключи распространяются открыто, а секретные ключи никогда не передаются.

13.2 Самостоятельно подписанные сертификаты

Интернет-центр P660HWP может выступать в качестве центра сертификации и подписывать свои сертификаты.

13.3 Проверка сертификатов

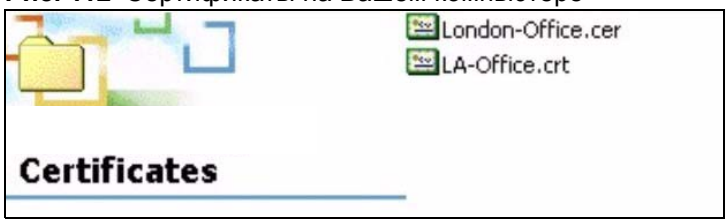
Перед загрузкой в P660HWP сертификата доверенного центра сертификации или удаленного доверенного узла следует проверить наличие текущего сертификата. Это особенно актуально для сертификатов доверенных центров сертификации, т.к. устройство P660HWP доверяет любому верному сертификату, подписанному любым из загруженных доверенных центров сертификации.

13.3.1 Проверка сигнатуры локального сертификата

Сигнатуры сертификатов – это профили сообщений, рассчитанные с использованием алгоритма MD5 или SHA1. Для проверки сигнатуры сертификата с целью определения его действительности используется следующая процедура.

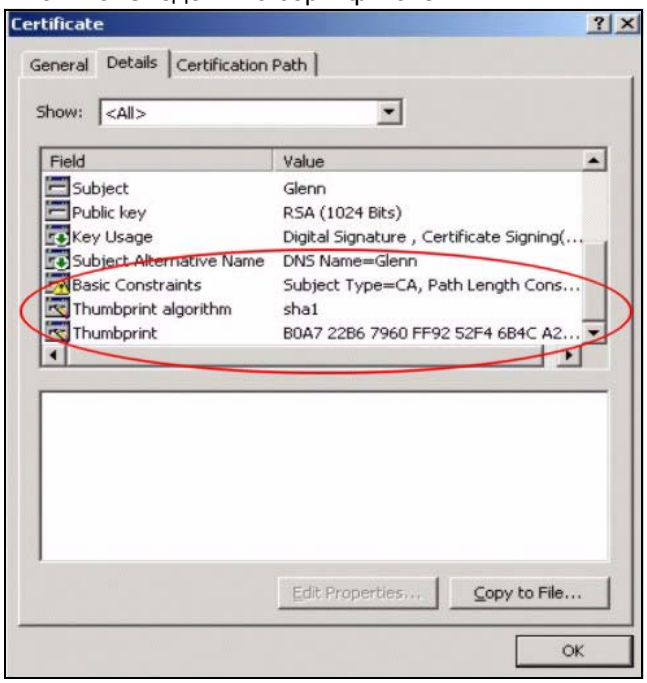
1. Откройте на компьютере папку с сохраненным сертификатом.
2. Убедитесь, что файл сертификата имеет расширение «.cer» или «.crt».

Рис. 112 Сертификаты на Вашем компьютере



3 Дважды щелкните по иконке сертификата, чтобы открыть окно **Certificate (Сертификат)**. Щелкните по закладке **Details (Сведения)** и прокрутите окно вниз, чтобы отображались поля **Thumbprint Algorithm (Алгоритм отпечатка)** и **Thumbprint (Отпечаток)**.

Рис. 113 Сведения о сертификате

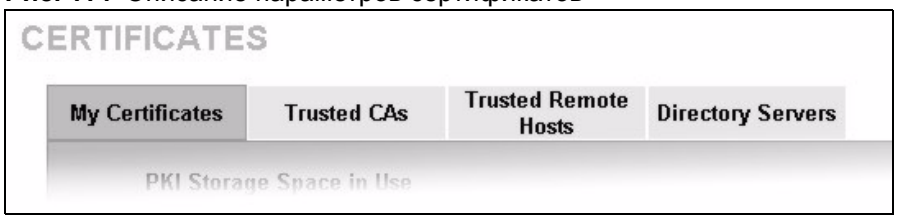


4 Используйте безопасный метод для проверки того, что владелец сертификата обладает той же информацией, которая отображена в полях **Thumbprint Algorithm (Алгоритм отпечатка)** и **Thumbprint (Отпечаток)**. В зависимости от ситуации безопасными могут быть разные методы. Например, по телефону или через HTTPS-подключение.

13.4 Описание параметров

В этой главе рассказывается об управлении сертификатами в интернет-центре P660HWP.

Рис. 114 Описание параметров сертификатов



Окна **My Certificate (Мой сертификат)** используются для создания и экспорта самостоятельно подписанных сертификатов или запросов на сертификацию, а также импорта сертификатов P660HWP, подписанных центром сертификации.

Окна **Trusted CA (Доверенные центры сертификации)** используются для сохранения сертификатов, выданных доверенными центрами сертификации, в устройстве P660HWP. Сертификаты можно также выгружать в компьютер.

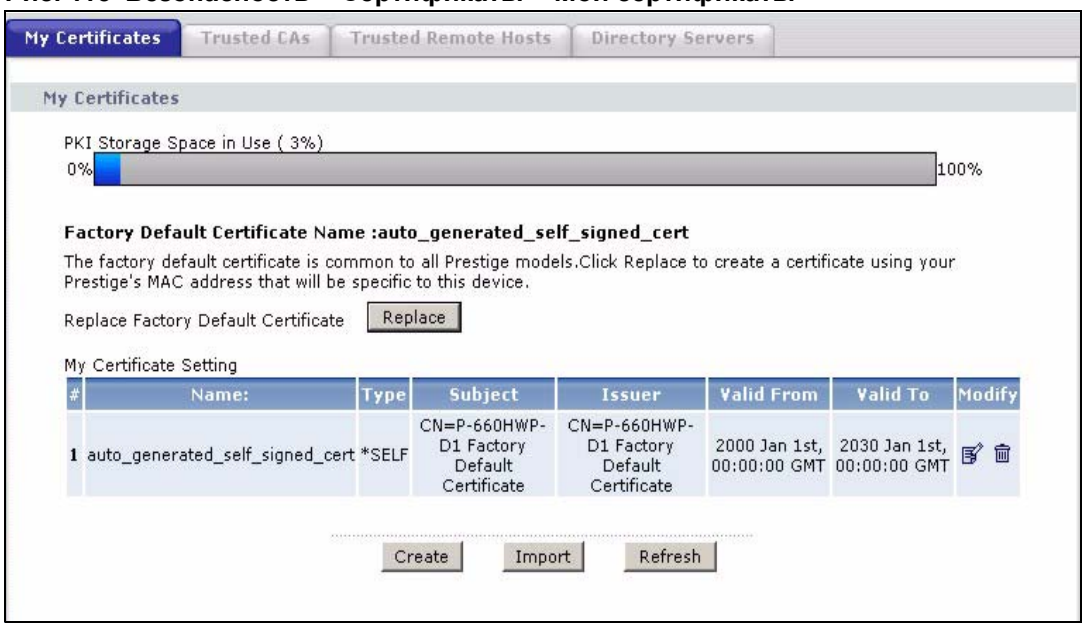
Для импорта самостоятельно подписанных сертификатов с удаленных доверенных узлов используются окна **Trusted Remote Hosts (Доверенные узлы)**.

Окно **Directory Servers (Серверы каталогов)** используется для создания списка адресов серверов каталогов, которые содержат списки действующих и аннулированных сертификатов.

13.5 Мои сертификаты

Щелкните **Security (Безопасность)** > **Certificates (Сертификаты)** > **My Certificates (Мои сертификаты)** для отображения окна **My Certificates (Мои сертификаты)**. Окно содержит сводный список сертификатов P660HWP и запросов на сертификацию. Сертификаты отображаются черным шрифтом, а запросы на сертификацию – серым.

Рис. 115 Безопасность > Сертификаты > Мои сертификаты



В следующей таблице даны описания полей этого окна.

Табл. 70 Безопасность > Сертификаты > Мои сертификаты

ПОЛЕ	ОПИСАНИЕ
PKI Storage Space in Use (Использованная память для хранения инфраструктуры открытого ключа)	Этот индикатор показывает находящуюся в использовании память P660HWP в процентах для хранения инфраструктуры открытого ключа. Когда место для хранения заканчивается, необходимо удалить просроченные или ненужные сертификаты перед добавлением новых сертификатов.
Replace (Заменить)	Эта кнопка отображается, когда в P660HWP имеется сертификат, установленный изготовителем по умолчанию. Установленный изготовителем по умолчанию сертификат является общим для всех устройств P660HWP, в которых используются сертификаты. Корпорация ZyXEL настоятельно рекомендует с помощью этой кнопки заменить сертификат, установленный изготовителем по умолчанию, на сертификат, в котором используется MAC-адрес устройства P660HWP.
Настройки сертификатов	
#	В этом поле отображается порядковый номер сертификата. Сертификаты отображаются в алфавитном порядке.
Name (Имя)	В этом поле отображается описательное имя сертификата. Рекомендуется давать каждому сертификату уникальное имя.
Type (Тип)	В этом поле отображается тип сертификата. **REQ** обозначает запрос на сертификацию и не является действующим сертификатом. Необходимо отправить запрос на сертификацию в центр сертификации, который затем выдаст сертификат. Окно **My Certificate Import (Импорт сертификатов)** используется для импорта сертификатов и замены запросов. **SELF** обозначает самостоятельно подписанный сертификат. ***SELF** обозначает самостоятельно подписанный сертификат по умолчанию, который используется интернет-центром P660HWP для подписи сертификатов, импортированных из доверенных удаленных узлов. **CERT** обозначает сертификат, выданный центром сертификации.
Subject (Владелец)	В этом поле отображается идентифицирующая информация о владельце сертификата, такая как CN (Common Name – Общее имя), OU (Organizational Unit or department – Организационная единица или отдел), O (Organization or company – Организация или компания) и C (Country – Страна). Рекомендуется для каждого сертификата указывать уникальную информацию о владельце.
Issuer (Издатель)	В этом поле отображается идентифицирующая информация о центре сертификации, выдавшем сертификат: общее имя, организационная единица или отдел, компания и страна. Для самостоятельно подписанного сертификата в этом поле отображается такая же информация, как и в поле **Subject (Владелец)**.
Valid From (Действителен с)	В этом поле отображается дата, начиная с которой применяется сертификат. Если сертификат еще не может применяться, то текст в этом поле отображается красным шрифтом и содержит сообщение «Not Yet Valid!» (Еще не действителен!).
Valid To (Действителен до)	В этом поле отображается дата, после которой срок действия сертификата заканчивается. Если срок действия сертификата подходит к концу или уже закончился, то текст в этом поле отображается красным шрифтом и содержит сообщение «Expiring!» (Срок заканчивается) или «Expired!» (Срок истек).

Табл. 70 Безопасность > Сертификаты > Мои сертификаты

ПОЛЕ	ОПИСАНИЕ
Modify (Изменить)	Щелкните по значку дополнительной информации, чтобы открыть окно, содержащее полную информацию о сертификате (или запросе о сертификате). Для сохранения сертификата на компьютере следует щелкнуть значок экспорта. Для запроса на сертификат следует щелкнуть значок экспорта, а затем в окне **File Download (Загрузка файла)** значок **Save (Сохранить)**. Откроется окно **Save As (Сохранить как)**. Выберите местонахождение файла и щелкните **Save (Сохранить)**. Для удаления сертификата (или запроса на сертификат) нужно щелкнуть значок удаления. Появляется окно с запросом на подтверждение операции удаления сертификата. Нельзя удалить сертификат, который используется одной или более службами. Для удаления сертификата со значением ***SELF** в поле **Type (Тип)** выполните следующие действия. 1. Убедитесь, что этот сертификат ***SELF** не используется в настройках ни одной из служб, например, HTTPS, VPN, SSH. 2. Щелкните по иконке дополнительной информации в строке другого самостоятельно подписанного сертификата (если требуется создать самостоятельно подписанный сертификат, см. описание кнопки **Create (Создать)**. 3. Установите флажок в поле **Default self-signed certificate which signs the imported remote host certificates (Самостоятельно подписанный сертификат по умолчанию, используемый для подписи импортированных сертификатов от доверенных удаленных узлов)**. 4. Щелкните по кнопке **Apply (Применить)** для сохранения изменений и возврата к окну **My Certificates (Мои сертификаты)**. 5. Сертификат, который первоначально отображался как ***SELF**, сейчас отображается **SELF** и его можно удалить. Следует помнить, что при удалении сертификата все последующие сдвигаются на позицию вверх.
Create (Создать)	Щелкните по кнопке **Create (Создать)** для перехода к окну, в котором P660HWP генерирует сертификат или запрос на сертификацию.
Import (Импорт)	Щелкните по кнопке **Import (Импорт)** для отображения окна, где можно перенести сертификат, полученный из центра сертификации, с вашего компьютера в интернет-центр P660HWP.
Refresh (Обновить)	Щелкните по кнопке **Refresh (Обновить)** для обновления информации о текущем статусе сертификатов.

13.6 Мои сертификаты > Сведения

Щелкните **Security (Безопасность) > Certificates (Сертификаты) > My Certificates (Мои сертификаты)** для отображения окна **My Certificates (Мои сертификаты)** (см. Рис. 115 на с. 214). Щелкните значок редактирования для перехода к окну **My Certificate Details (Сведения о сертификате)**. В этом окне можно просмотреть подробную информацию о данном сертификате или изменить его имя.

Если сертификат является самоподписанным, можно настроить устройство P660HWP на использование этого сертификата для подписывания загруженных сертификатов удаленного доверенного узла.

Табл. 71 Безопасность > Сертификаты > Мои сертификаты > Правка

В следующей таблице даны описания полей этого окна.

Табл. 72 Безопасность > Сертификаты > Мои сертификаты > Сведения

ПОЛЕ	ОПИСАНИЕ
Certificate Name (Имя сертификата)	В этом поле отображается описательное имя для данного сертификата. Для изменения имени введите до 31 символа с целью описания сертификата. Допускается использовать любые символы, кроме пробелов.
Property (Свойства) Default self-signed certificate which signs the imported remote host certificates (Самостоятельно подписанный сертификат по умолчанию, используемый для подписи импортированных сертификатов от доверенных удаленных узлов).	Установите в этом поле флажок, чтобы P660HWP использовал этот сертификат для подписи сертификатов от доверенных удаленных узлов, которые импортируются в P660HWP. Это поле доступно только при использовании самостоятельно подписанных сертификатов. Если здесь флажок уже установлен, то в этом окне его снять нельзя, флажок необходимо установить в окне с параметрами другого самостоятельно подписанного сертификата. Тогда флажок автоматически будет снят в окне с параметрами сертификата, который ранее был установлен для подписи импортированных сертификатов от доверенных удаленных узлов.
Refresh (Обновить)	Щелкните по кнопке **Refresh (Обновить)** для отображения пути к сертификату.

Табл. 72 Безопасность > Сертификаты > Мои сертификаты > Сведения (продолжение)

ПОЛЕ	ОПИСАНИЕ
Certification Path (Путь к файлу сертификата)	Щелкните по кнопке **Refresh (Обновить)** для вывода в текстовом поле, которое отображается в режиме только для чтения, иерархии центров сертификации, которые подтверждают достоверность сертификата, а также сам сертификат. Если центр сертификации, выпускающий сертификат, является импортированным в качестве доверенного центра сертификации, он может быть единственным центром сертификации в списке (среди сертификатов). Если сертификат является самостоятельно подписанным, то он будет единственным в этом списке. Если при проверке в иерархии срок какого-либо сертификата закончился или сертификат был отозван, интернет-центр P660HWP считает такой сертификат непроверенным, и в этом поле появляется сообщение **Not trusted (Не подтвержден)**.
Certificate Information (Параметры сертификата)	В следующих полях отображается подробная информация о сертификате в режиме только для чтения.
Type (Тип)	В этом поле отображается общая информация о сертификате. «CA-signed» означает, что сертификат подписан центром сертификации. «Self-signed» означает, что сертификат подписан владельцем сертификата (не центром сертификации). «X.509» означает, что сертификат был создан и подписан в соответствии с правилами ITU-T X.509, которые определяют форматы для сертификатов открытого ключа.
Version (версия)	В этом поле отображается номер версии X.509.
Serial Number (Серийный номер)	В этом поле отображается идентификационный номер сертификата, выданного центром сертификации или сгенерированного интернет-центром P660HWP.
Subject (Владелец)	В этом поле отображается идентифицирующая информация о владельце сертификата, такая как CN (Common Name – Общее имя), OU (Organizational Unit – Организационная единица), O (Organization – Организация) и C (Country – Страна).
Issuer (Издатель)	В этом поле отображается идентифицирующая информация о центре сертификации, выдавшем сертификат: общее имя, организационная единица, компания и страна. Для самостоятельно подписанного сертификата в этом поле отображается такая же информация, как и в поле **Subject (Владелец)**.
Signature Algorithm (Алгоритм подписи)	В этом поле отображается тип алгоритма, использованного для подписи сертификата. В интернет-центре P660HWP используется алгоритм rsa-pkcs1-sha1 (алгоритм шифрования с использованием открытого-секретного ключа RSA и алгоритм с использованием хэш-функции SHA1). Некоторые центры сертификации используют алгоритм rsa-pkcs1-md5 (алгоритм шифрования с использованием открытого-секретного ключа RSA и алгоритм с использованием хэш-функции MD5).
Valid From (Действителен с)	В этом поле отображается дата, начиная с которой применяется сертификат. Если сертификат еще не может применяться, то текст в этом поле отображается красным шрифтом и содержит сообщение «Not Yet Valid!» (Еще не действителен!).
Valid To (Действителен до)	В этом поле отображается дата, после которой срок действия сертификата заканчивается. Если срок действия сертификата подходит к концу или уже закончился, то текст в этом поле отображается красным шрифтом и содержит сообщение «Expiring!» (Срок заканчивается) или «Expired!» (Срок истек).
Key Algorithm (Алгоритм ключа)	В этом поле отображается тип алгоритма, который используется для генерирования пар ключей сертификатов (в P660HWP используется шифрование RSA), и длина ключа в битах (в примере 1024 бит).

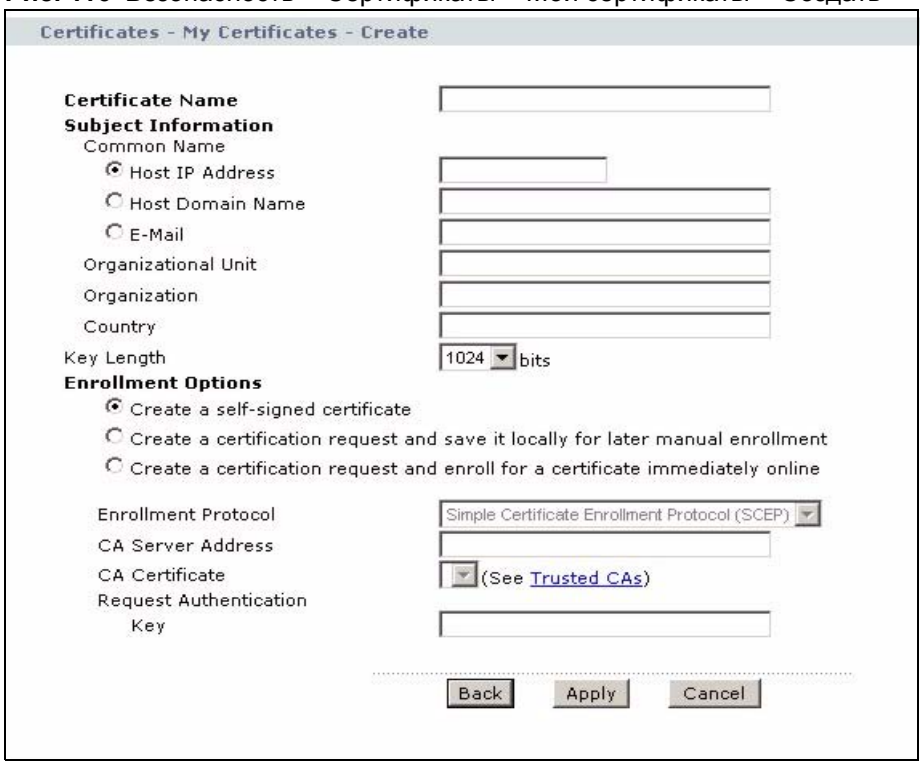
Табл. 72 Безопасность > Сертификаты > Мои сертификаты > Сведения (продолжение)

ПОЛЕ	ОПИСАНИЕ
Subject Alternative Name (Сведения о владельце)	В этом поле отображается IP-адрес (IP), доменное имя (DNS) или адрес электронной почты (EMAIL) владельца сертификата.
Key Usage (Функции ключа)	В этом поле отображаются функции, для которых применяется ключ сертификата. Например, «DigitalSignature» (Цифровая подпись) означает, что ключ может использоваться для подписи сертификатов, а «KeyEncipherment» (Шифрование с использованием ключа) означает, что ключ может использоваться для шифрования текста.
Basic Constraint (Основные параметры)	В этом поле отображается общая информация о сертификате. Например, «Subject Type=CA» означает, что этот сертификат выдан центром сертификации, а «Path Length Constraint=1» означает, что путь к сертификату содержит только один центр сертификации.
MD5 Fingerprint (Сигнатура MD5)	Это профиль сообщения сертификата, который устройство P660HWP вычислило с использованием алгоритма MD5.
SHA1 Fingerprint (Сигнатура SHA1)	Это профиль сообщения сертификата, который интернет-центр P660HWP вычислил с использованием алгоритма SHA1.
Certificate in PEM (Base-64) Encoded Format (Сертификат в зашифрованном формате PEM (Base-64))	В этом текстовом поле отображается сертификат или запрос на сертификат в формате PEM (Privacy Enhanced Mail – Электронная почта с усовершенствованной защитой) в режиме только для чтения. В формате PEM для преобразования бинарного сертификата в печатную форму используется 64 символа ASCII. Запрос на сертификат можно скопировать и перенести в веб-страницу центра сертификации, почтовое сообщение для отправки в центр сертификации или текстовый редактор, а также сохранить в файле на управляющем компьютере, чтобы позже зарегистрировать вручную. Сертификат можно скопировать и перенести в почтовое сообщение для отправки друзьям или коллегам, а также перенести в текстовый редактор для сохранения в файле на управляющем компьютере для последующего распространения (например, с помощью дискеты).
Back (Назад)	Для возврата к предыдущему окну нажмите кнопку **Back (Назад)**.
Export (Экспорт)	Для экспорта файла со сведениями о сертификате нажмите кнопку **Export (Экспорт)**.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек P660HWP. Изменить можно только имя, исключение составляет самостоятельно подписанный сертификат, который можно установить как сертификат по умолчанию для подписи импортированных сертификатов доверенных удаленных узлов.
Cancel (Отменить)	Щелкните **Cancel (Отмена)** для выхода и возврата к окну **My Certificates (Мои сертификаты)**.

13.7 Мои сертификаты > Создать

Щелкните **Security (Безопасность) > Certificates (Сертификаты) > My Certificates (Мои сертификаты) > Create (Создать)** для отображения окна **My Certificate Create (Создание сертификатов)**. В этом окне P660HWP может создать самостоятельно подписанный сертификат, зарегистрировать сертификат от центра сертификации или сгенерировать запрос на сертификацию.

Рис. 116 Безопасность > Сертификаты > Мои сертификаты > Создать



В следующей таблице даны описания полей этого окна.

Табл. 73 Безопасность > Сертификаты > Мои сертификаты > Создать

ПОЛЕ	ОПИСАНИЕ
Certificate Name (Имя сертификата)	Введите до 31 символа ASCII (пробелы исключаются) для описания сертификата.
Subject Information (Информация о владельце)	В эти поля заполняется информация, идентифицирующая владельца сертификата. Не обязательно заполнять все поля, но поле **Common Name (Общее имя)** является обязательным. Центр сертификации при выпуске сертификата может добавлять поля к информации о владельце (например, серийный номер). Рекомендуется для каждого сертификата указывать уникальную информацию о владельце.
Common Name (Общее имя)	Установите переключатель, чтобы идентифицировать владельца сертификата по IP-адресу, доменному имени или адресу электронной почты.
Host IP Address (IP-адрес узла)	Введите IP-адрес (в десятичном формате с разделительными точками), доменное имя или адрес электронной почты в соответствующее поле.
Host Domain Name (Доменное имя узла)	Введите доменное имя. Имя может иметь длину до 31 латинского символа. Оно используется исключительно в целях идентификации и может быть любым.
Email (Электронная почта)	Введите адрес электронной почты. Имя может иметь длину до 31 латинского символа. Оно используется исключительно в целях идентификации и может быть любым.
Organizational Unit (Организационная единица)	Введите до 127 символов для описания организационной единицы или отдела, к которому относится владелец сертификата. Допускается вводить любые символы, включая пробелы, однако P660HWP отбрасывает пробелы в конце строки.

Табл. 73 Безопасность > Сертификаты > Мои сертификаты > Создать (продолжение)

ПОЛЕ	ОПИСАНИЕ
Organization (Компания)	Введите до 127 символов для описания компании или группы, к которому относится владелец сертификата. Допускается вводить любые символы, включая пробелы, однако P660HWP отбрасывает пробелы в конце строки.
Country (Страна)	Введите до 127 символов для описания страны, где находится владелец сертификата. Допускается вводить любые символы, включая пробелы, однако P660HWP отбрасывает пробелы в конце строки.
Key Length (Длина ключа)	Из выпадающего списка выберите число, чтобы установить длину ключа в битах (от 512 до 2048). Чем больше длина ключа, тем выше уровень защиты. Чем длиннее ключ, тем больше памяти используется для хранения PKI.
Enrollment Options (Регистрация)	Здесь определяется способ создания сертификата.
Create a self-signed certificate (Создать самостоятельно подписанный сертификат)	Выберите **Create a self-signed certificate (Создать самостоятельно подписанный сертификат)**, чтобы интернет-центр P660HWP выступал в качестве центра сертификации и генерировал сертификаты. В этом случае не требуется делать запрос на получение сертификата в центр сертификации.
Create a certification request and save it locally for later manual enrollment (Создать запрос на сертификацию и сохранить его локально с целью выполнить регистрацию вручную позже)	Выберите **Create a certification request and save it locally for later manual enrollment (Создать запрос на сертификацию и сохранить его локально с целью выполнить регистрацию вручную позже)**, чтобы интернет-центр P660HWP генерировал и сохранял запросы на сертификаты. Просмотр и копирование запросов на сертификат, а также их отправка в центр сертификации производится в окне **My Certificate Details (Сведения о сертификате)**. Скопируйте запрос на сертификат в окне **My Certificate Details (Сведения о сертификате)** (см. Разд. 13.6 на с. 216) и затем отправьте его в центр сертификации.
Create a certification request and enroll for a certificate immediately online (Создать запрос на сертификат и зарегистрировать сертификат в режиме online)	Выберите **Create a certification request and enroll for a certificate immediately online (Создать запрос на сертификат и зарегистрировать сертификат в режиме online)**, чтобы интернет-центр P660HWP сгенерировал запрос на сертификат и отправил этот запрос в центр сертификации. Заранее необходимо выполнить импорт сертификата, выданного центром сертификации, в окне **Trusted CAs (Доверенные центры сертификации)**. При выборе этого варианта необходимо установить протокол регистрации и сертификат центра сертификации из выпадающих списков, а также адрес сервера центра сертификации. Также необходимо заполнить поля **Reference Number (Регистрационный номер)** и **Key (Ключ)**, если эта информация требуется центру сертификации.
Enrollment Protocol (Протокол регистрации)	Из выпадающего списка выберите протокол регистрации, используемый центром сертификации **SCEP (Simple Certificate Enrollment Protocol – Простой протокол регистрации сертификатов)** – это протокол регистрации на основе протокола TCP, разработанный компаниями VeriSign и Cisco. **CMP (Certificate Management Protocol – Протокол управления сертификатами)** – это протокол регистрации на основе протокола TCP, разработанный рабочей группой Public Key Infrastructure X.509 (Инфраструктура открытого ключа X.509) в составе IETF (Internet Engineering Task Force – Рабочая группа проектирования сети Интернет) и описываемый в комментариях RFC 2510.

Табл. 73 Безопасность > Сертификаты > Мои сертификаты > Создать (продолжение)

ПОЛЕ	ОПИСАНИЕ
CA Server Address (Адрес сервера центра сертификации)	Введите IP-адрес или URL сервера центра сертификации.
CA Certificate (Сертификат центра сертификации)	Из выпадающего списка поля **CA Certificate (Сертификат центра сертификации)** выберите сертификат центра сертификации. Заранее необходимо выполнить импорт сертификата, выданного центром сертификации, в окне **Trusted CAs (Доверенные центры сертификации)**. Щелкните по ссылке **Trusted CAs (Доверенные центры сертификации)** для перехода к окну **Trusted CAs (Доверенные центры сертификации)**, где можно выполнять просмотр и управление списком сертификатов P660HWP от доверенных центров сертификации.
Request Authentication (Запрос на аутентификацию)	При выборе поля **Create a certification request and enroll for a certificate immediately online (Создать запрос на сертификат и зарегистрировать сертификат в режиме online)** центр сертификации может запросить данные о регистрационном номере и ключе для проведения идентифицикации во время получения вашего запроса на сертификат. Заполните поля **Reference Number (Регистрационный номер)** и **Key (Ключ)**, если ваш центр сертификации применяет протокол регистрации CMP. Если ваш центр сертификации применяет протокол регистрации SCEP, заполните только поле **Key (Ключ)**.
Key (Ключ)	Введите ключ, предоставленный центром сертификации.
Back (Назад)	Для возврата к предыдущему окну нажмите кнопку **Back (Назад)**.
Apply (Применить)	Щелкните по кнопке **Apply (Применить)**, чтобы начать генерирование сертификата или запроса на сертификат.
Cancel (Отменить)	Щелкните **Cancel (Отмена)** для выхода и возврата к окну **My Certificates (Мои сертификаты)**.

После щелчка по кнопке **Apply (Применить)** в окне **My Certificate Create (Создание сертификатов)** появляется окно с сообщением о том, что P660HWP генерирует самостоятельно подписанный сертификат или запрос на сертификат.

После того как P660HWP успешно зарегистрирует сертификат или сгенерирует запрос или самостоятельно подписанный сертификат, появляется окно с кнопкой **Return (Возврат)**, при нажатии на которую происходит возврат к окну **My Certificates (Мои сертификаты)**.

Если в окне **My Certificate Create (Создание сертификатов)** производилась регистрация сертификата, и P660HWP не смог ее выполнить успешно, появляется окно с кнопкой **Return (Возврат)**, при нажатии на которую происходит возврат к окну **My Certificate Create (Создание сертификатов)**. Щелкните по кнопке **Return (Возврат)** и проверьте настройки в окне **My Certificate Create (Создание сертификатов)**. Убедитесь, что параметры центра сертификации установлены правильно и подключение к Интернету работает нормально, чтобы P660HWP зарегистрировал сертификат в режиме online.

13.8 Мои сертификаты > Импорт

Щелкните **Security (Безопасность) > Certificates (Сертификаты) > My Certificates (Мои сертификаты)** и затем **Import (Импорт)** для отображения окна **My Certificate Import (Импорт сертификатов)**. Следуйте указаниям в этом окне для загрузки сертификата с компьютера в устройство P660HWP.

- Загрузить можно только сертификат, соответствующий запросу сертификации, созданному устройством P660HWP (запрос сертификации содержит секретный ключ). Импортированный сертификат замещает соответствующий запрос в окне **My Certificates (Мои сертификаты)**. Исключение составляет сертификат формата PKCS#12 без соответствующего запроса на сертификацию, поскольку он содержит секретный ключ.
- Перед импортом необходимо удалить все пробелы в имени файла сертификата.

13.8.1 Форматы файлов сертификатов

Файл сертификата от центра сертификации, который необходимо импортировать, должен иметь один из следующих форматов:

- Бинарный X.509 – это правила ITU-T, которые определяют форматы для сертификатов X.509.
- X.509, зашифрованный PEM (Base-64) – в формате PEM (Privacy Enhanced Mail – Электронная почта с усовершенствованной защитой) используются 64 символа ASCII для преобразования бинарного сертификата X.509 в печатную форму.
- Бинарный PKCS#7 – это стандарт, в котором определяется основной синтаксис для данных (включая цифровые подписи), которые подлежат шифрованию. В настоящее время P660HWP позволяет выполнять импорт файла PKS#7, который содержит один сертификат.
- PKCS#7, зашифрованный PEM (Base-64) – в формате PEM (Privacy Enhanced Mail – Электронная почта с усовершенствованной защитой) используются 64 символа ASCII для преобразования бинарного сертификата PKCS#7 в печатную форму.

В процессе переноса не следует преобразовывать двоичный файл в текстовый. Это вполне вероятно, поскольку многие программы по умолчанию работают с текстовыми файлами.

Рис. 117 Безопасность > Сертификаты > Мои сертификаты > Импорт

В следующей таблице даны описания полей этого окна.

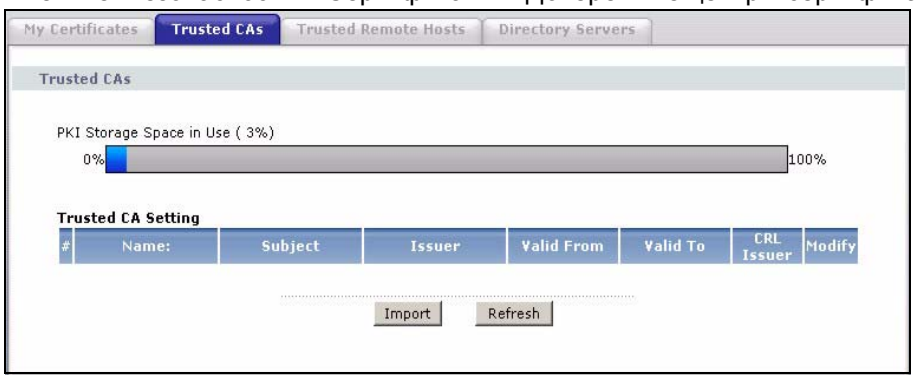
Табл. 74 Безопасность > Сертификаты > Мои сертификаты > Импорт

ПОЛЕ	ОПИСАНИЕ
File Path (Путь к файлу)	Введите в это поле путь к файлу, который требуется загрузить, или щелкните **Browse (Обзор)** для его поиска.
Browse (Обзор)	Щелкните **Browse (Обзор)** для поиска файла сертификата, который требуется загрузить.
Back (Назад)	Для возврата к предыдущему окну нажмите кнопку **Back (Назад)**.
Apply (Применить)	Щелкните **Apply (Применить)** для сохранения сертификата в P660HWP.
Cancel (Отменить)	Щелкните **Cancel (Отмена)** для выхода и возврата к окну **My Certificates (Мои сертификаты)**.

13.9 Доверенные центры сертификации

Щелкните **Security (Безопасность) > Certificates (Сертификаты) > Trusted CAs (Доверенные центры сертификации)** для отображения окна **Trusted CAs (Доверенные центры сертификации)**. В этом окне отображается сводный список сертификатов от центров сертификации, которые установлены в интернет-центре P660HWP как доверенные. Любой действительный сертификат из этого списка, подписанный центром сертификации, P660HWP принимает как надежный, поэтому импорт сертификата, подписанного одним из этих центров сертификации, выполнять не требуется.

Рис. 118 Безопасность > Сертификаты > Доверенные центры сертификации



В следующей таблице даны описания полей этого окна.

Табл. 75 Безопасность > Сертификаты > Доверенные центры сертификации

ПОЛЕ	ОПИСАНИЕ
PKI Storage Space in Use (Использованная память для хранения инфраструктуры открытого ключа)	Этот индикатор показывает находящуюся в использовании память P660HWP в процентах для хранения инфраструктуры открытого ключа. Когда место для хранения заканчивается, необходимо удалить просроченные или ненужные сертификаты перед добавлением новых сертификатов.
Trusted CAs Setting (Настройка доверенных центров сертификации)	
#	В этом поле отображается порядковый номер сертификата. Сертификаты отображаются в алфавитном порядке.
Name (Имя)	В этом поле отображается описательное имя сертификата.
Subject (Владелец)	В этом поле отображается идентифицирующая информация о владельце сертификата, такая как CN (Common Name – Общее имя), OU (Organizational Unit or department – Организационная единица или отдел), O (Organization or company – Организация или компания) и C (Country – Страна). Рекомендуется для каждого сертификата указывать уникальную информацию о владельце.
Issuer (Издатель)	В этом поле отображается идентифицирующая информация о центре сертификации, выдавшем сертификат: общее имя, организационная единица или отдел, компания и страна. Для самостоятельно подписанного сертификата в этом поле отображается такая же информация, как и в поле **Subject (Владелец)**.
Valid From (Действителен с)	В этом поле отображается дата, начиная с которой применяется сертификат. Если сертификат еще не может применяться, то текст в этом поле отображается красным шрифтом и содержит сообщение «Not Yet Valid!» (Еще не действителен!).
Valid To (Действителен до)	В этом поле отображается дата, после которой срок действия сертификата заканчивается. Если срок действия сертификата подходит к концу или уже закончился, то текст в этом поле отображается красным шрифтом и содержит сообщение «Expiring!» (Срок заканчивается) или «Expired!» (Срок истек).
CRL Issuer (Издатель CRL)	В этом поле отображается **Yes (Да)**, если центр сертификации выпускает списки CRL (Certificate Revocation List – Список аннулированных сертификатов) для изданных им сертификатов и в поле **Issues certificate revocation lists (CRL) (Издает списки аннулированных сертификатов)** в окне с параметрами сертификата установлен флажок, чтобы P660HWP проверял списки CRL, прежде чем принимать какой-либо сертификат от этого центра сертификации как надежный. В противном случае в этом поле отображается **No (Нет)**.
Modify (Изменить)	Щелкните по иконке дополнительной информации, чтобы открыть окно, содержащее полную информацию о сертификате. Для сохранения сертификата на компьютере следует щелкнуть значок экспорта. Щелкните по этому значку, затем в окне **File Download (Загрузка файла)** щелкните **Save (Сохранить)**. Откроется окно **Save As (Сохранить как)**. Выберите местонахождение файла и щелкните **Save (Сохранить)**. Для удаления сертификата щелкните по иконке удаления. Появляется окно с запросом на подтверждение операции удаления сертификатов. Следует помнить, что при удалении сертификата все последующие сдвигаются на позицию вверх.

Табл. 75 Безопасность > Сертификаты > Доверенные центры сертификации

ПОЛЕ	ОПИСАНИЕ
Import (Импорт)	Щелкните по кнопке **Import (Импорт)** для отображения окна, где можно перенести сертификат от центра сертификации, который рассматривается как надежный, с вашего компьютера в интернет-центр P660HWP.
Refresh (Обновить)	Щелкните по кнопке **Refresh (Обновить)** для обновления информации о текущем статусе сертификатов.

13.10 Сведения о доверенном центре сертификации

Щелкните **Security (Безопасность) > Certificates (Сертификаты) > Trusted CAs (Доверенные центры сертификации)** для отображения окна **Trusted CAs (Доверенные центры сертификации)**. Щелкните значок правки для перехода к окну **Trusted CA Details (Сведения о доверенном центре сертификации)**. В этом окне отображается подробная информация о сертификате центра сертификации. Здесь также можно измененить имя сертификата и указать, будет ли P660HWP проверять список аннулированных сертификатов этого центра, прежде чем принимать какой-либо сертификат от этого центра сертификации как надежный.

Рис. 119 Безопасность > Сертификаты > Доверенные центры сертификации > Сведения

В следующей таблице даны описания полей этого окна.

Табл. 76 Безопасность > Сертификаты > Доверенные центры сертификации > Сведения

ПОЛЕ	ОПИСАНИЕ
Certificate Name (Имя сертификата)	В этом поле отображается описательное имя для данного сертификата. Для изменения имени введите до 31 символа с целью описания этого сертификата. Допускается использовать любые символы, кроме пробелов.
Property (Свойства) Check incoming certificates issued by this CA against a CRL (Проверка входящих сертификатов, изданных этим центром сертификации, по списку CRL)	Установите в этом поле флажок, чтобы P660HWP проверял входящие сертификаты, изданные этим центром сертификации, по списку CRL (Certificate Revocation List – Список аннулированных сертификатов). Снимите флажок в этом поле, чтобы P660HWP не выполнял проверку входящих сертификатов, изданных этим центром сертификации, по списку CRL (Certificate Revocation List – Список аннулированных сертификатов).
Certification Path (Путь к файлу сертификата)	Щелкните по кнопке **Refresh (Обновить)** для отображения в текстовом поле сертификата последнего объекта и списка сертификатов центра сертификации, который показывает иерархию центров сертификации, подтверждающую сертификат последнего объекта. Если центр сертификации, выпускающий сертификат, является импортированным в качестве доверенного центра сертификации, он может быть единственным центром сертификации в списке (кроме самого сертификата). Если при проверке в иерархии срок какого-либо сертификата закончился или он был отозван, интернет-центр P660HWP считает сертификат последнего объекта непроверенным, и в этом поле появляется сообщение «Not trusted» (Не подтвержден).
Refresh (Обновить)	Щелкните по кнопке **Refresh (Обновить)** для отображения пути к сертификату.
Certificate Information (Параметры сертификата)	В следующих полях отображается подробная информация о сертификате в режиме только для чтения.
Type (Тип)	В этом поле отображается общая информация о сертификате. «CA-signed» означает, что сертификат подписан центром сертификации. «Self-signed» означает, что сертификат подписан владельцем сертификата (не центром сертификации). «X.509» означает, что сертификат был создан и подписан в соответствии с правилами ITU-T X.509, которые определяют форматы для сертификатов открытого ключа.
Version (версия)	В этом поле отображается номер версии X.509.
Serial Number (Серийный номер)	В этом поле отображается идентификационный номер сертификата, выданного центром сертификации.
Subject (Владелец)	В этом поле отображается идентифицирующая информация о владельце сертификата, такая как CN (Common Name – Общее имя), OU (Organizational Unit – Организационная единица), O (Organization – Организация) и C (Country – Страна).
Issuer (Издатель)	В этом поле отображается идентифицирующая информация о центре сертификации, выдавшем сертификат: общее имя, организационная единица, компания и страна. Для самостоятельно подписанного сертификата в этом поле отображается такая же информация, как и в поле **Subject (Владелец)**.

Табл. 76 Безопасность > Сертификаты > Доверенные центры сертификации > Сведения

ПОЛЕ	ОПИСАНИЕ
Signature Algorithm (Алгоритм подписи)	В этом поле отображается тип алгоритма, использованного для подписи сертификата. Некоторые центры сертификации используют алгоритм rsa-pkcs1-sha1 (алгоритм шифрования с использованием открытого-секретного ключа RSA и алгоритм с использованием хэш-функции SHA1). Другие центры сертификации используют алгоритм rsa-pkcs1-md5 (алгоритм шифрования с использованием открытого-секретного ключа RSA и алгоритм с использованием хэш-функции MD5).
Valid From (Действителен с)	В этом поле отображается дата, начиная с которой применяется сертификат. Если сертификат еще не может применяться, то текст в этом поле отображается красным шрифтом и содержит сообщение «Not Yet Valid!» (Еще не действителен!).
Valid To (Действителен до)	В этом поле отображается дата, после которой срок действия сертификата заканчивается. Если срок действия сертификата подходит к концу или уже закончился, то текст в этом поле отображается красным шрифтом и содержит сообщение «Expiring!» (Срок заканчивается) или «Expired!» (Срок истек).
Key Algorithm (Алгоритм ключа)	В этом поле отображается тип алгоритма, который используется для генерирования пар ключей сертификатов (в P660HWP используется шифрование RSA), и длина ключа в битах (в примере 1024 бит).
Subject Alternative Name (Сведения о владельце)	В этом поле отображается IP-адрес (IP), доменное имя (DNS) или адрес электронной почты (EMAIL) владельца сертификата.
Key Usage (Функции ключа)	В этом поле отображаются функции, для которых применяется ключ сертификата. Например, «DigitalSignature» (Цифровая подпись) означает, что ключ может использоваться для подписи сертификатов, а «KeyEncipherment» (Шифрование с использованием ключа) означает, что ключ может использоваться для шифрования текста.
Basic Constraint (Основные параметры)	В этом поле отображается общая информация о сертификате. Например, «Subject Type=CA» означает, что этот сертификат выдан центром сертификации, а «Path Length Constraint=1» означает, что путь к сертификату содержит только один центр сертификации.
CRL Distribution Points (Пункты распределения CRL)	В этом поле отображается количество доступных серверов каталогов со списками аннулированных сертификатов, которые предоставляются центром сертификации, выпустившим этот сертификат. В этом поле также отображаются доменные имена или IP-адреса этих серверов.
MD5 Fingerprint (Сигнатура MD5)	Это профиль сообщения сертификата, который устройство P660HWP вычислило с использованием алгоритма MD5. По этому значению через центр сертификации можно проверить, действительно ли это выданный им сертификат (например, по телефону).
SHA1 Fingerprint (Сигнатура SHA1)	Это профиль сообщения сертификата, который интернет-центр P660HWP вычислил с использованием алгоритма SHA1. По этому значению через центр сертификации можно проверить, действительно ли это выданный им сертификат (например, по телефону).
Certificate in PEM (Base-64) Encoded Format (Сертификат в зашифрованном формате PEM (Base-64))	В этом текстовом поле отображается сертификат или запрос на сертификат в формате PEM (Privacy Enhanced Mail – Электронная почта с усовершенствованной защитой) в режиме только для чтения. В формате PEM для преобразования бинарного сертификата в печатную форму используется 64 символа ASCII. Сертификат можно скопировать и перенести в почтовое сообщение для отправки друзьям или коллегам, а также перенести в текстовый редактор для сохранения в файле на управляющем компьютере для последующего распространения (например, с помощью дискеты).
Back (Назад)	Для возврата к предыдущему окну нажмите кнопку **Back (Назад)**.

Табл. 76 Безопасность > Сертификаты > Доверенные центры сертификации > Сведения

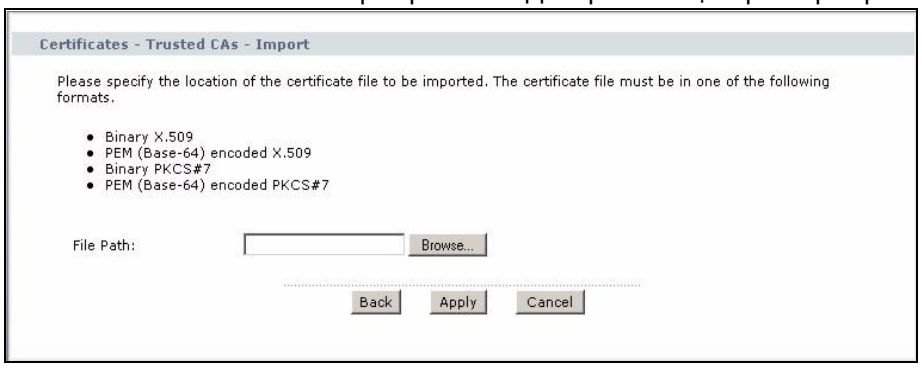
ПОЛЕ	ОПИСАНИЕ
Export (Экспорт)	Для экспорта файла со сведениями о сертификате нажмите кнопку **Export (Экспорт)**.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек P660HWP. Можно изменить только имя сертификата и/или указать, будет ли P660HWP проверять список CRL, издаваемый этим центром сертификации, прежде чем принимать сертификат от этого центра сертификации как надежный.
Cancel (Отменить)	Щелкните **Cancel (Отмена)** для выхода и возврата к окну **Trusted CAs (Доверенные центры сертификации)**.

13.11 Доверенный центр сертификации > Импорт

Щелкните **Security (Безопасность) > Certificates (Сертификаты) > Trusted CAs (Доверенные центры сертификации)** для отображения окна **Trusted CAs (Доверенные центры сертификации)**. В этом окне щелкните по кнопке **Import (Импорт)** для отображения окна **Trusted CA Import (Импорт доверенного центра сертификации)**. Следуйте указаниям в этом окне для загрузки сертификата доверенного центра сертификации из компьютера в P660HWP. Устройство P660HWP доверяет любому действующему сертификату, подписанному любым из загруженных в него сертификатов, выданных доверенными центрами сертификации.

Перед импортом необходимо удалить все пробелы в имени файла сертификата.

Рис. 120 Безопасность > Сертификаты > Доверенные центры сертификации > Импорт



В следующей таблице даны описания полей этого окна.

Табл. 77 Безопасность > Сертификаты > Импорт доверенных центров сертификации

ПОЛЕ	ОПИСАНИЕ
File Path (Путь к файлу)	Введите в это поле путь к файлу, который требуется загрузить, или щелкните **Browse (Обзор)** для его поиска.
Browse (Обзор)	Щелкните **Browse (Обзор)** для поиска файла сертификата, который требуется загрузить.

Табл. 77 Безопасность > Сертификаты > Импорт доверенных центров сертификации

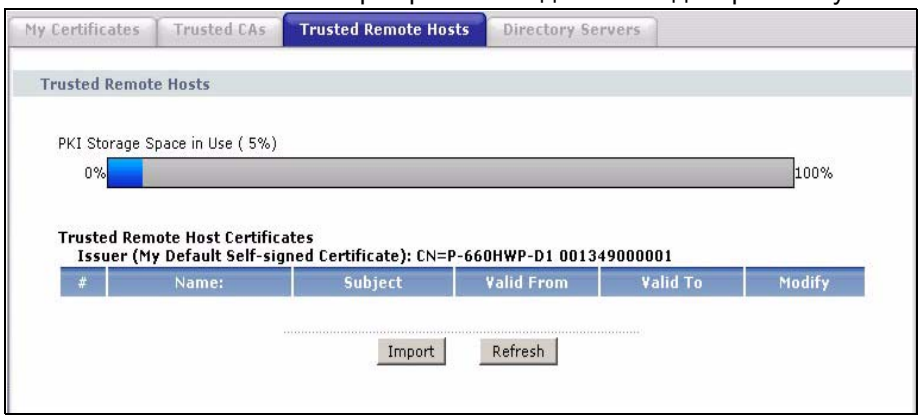
ПОЛЕ	ОПИСАНИЕ
Back (Назад)	Для возврата к предыдущему окну нажмите кнопку **Back (Назад)**.
Apply (Применить)	Щелкните **Apply (Применить)** для сохранения сертификата в P660HWP.
Cancel (Отменить)	Щелкните **Cancel (Отмена)** для выхода и возврата к окну **Trusted CAs (Доверенные центры сертификации)**.

13.12 Доверенные удаленные узлы

Щелкните **Security (Безопасность) > Certificates (Сертификаты) > Trusted Remote Hosts (Доверенные удаленные узлы)** для отображения окна **Trusted Remote Hosts (Доверенные удаленные узлы)**. В этом окне отображается список сертификатов узлов сети, которым вы доверяете, но не подписанных ни одним из центров сертификации, перечисленных в окне **Trusted CAs (Доверенные центры сертификации)**.

Любой действительный сертификат, подписанный доверенным центром сертификации, P660HWP автоматически принимает как надежный, поэтому добавлять сертификат, подписанный центром сертификации, из списка в окне **Trusted CAs (Доверенные центры сертификации)** не требуется.

Рис. 121 Безопасность > Сертификаты > Удаленные доверенные узлы



В следующей таблице даны описания полей этого окна.

Табл. 78 Безопасность > Сертификаты > Удаленные доверенные узлы

ПОЛЕ	ОПИСАНИЕ
PKI Storage Space in Use (Использованная память для хранения инфраструктуры открытого ключа)	Этот индикатор показывает находящуюся в использовании память P660HWP в процентах для хранения инфраструктуры открытого ключа. Когда место для хранения заканчивается, необходимо удалить просроченные или ненужные сертификаты перед добавлением новых сертификатов.
Issuer (My Default Self-signed Certificate) (Издатель (Мой самостоятельно подписанный сертификат по умолчанию))	В этом поле отображается идентифицирующая информация о самостоятельно подписанном сертификате по умолчанию, установленном в P660HWP и использующемся для подписи сертификатов доверенных удаленных узлов.
#	В этом поле отображается порядковый номер сертификата. Сертификаты отображаются в алфавитном порядке.
Name (Имя)	В этом поле отображается описательное имя сертификата.
Subject (Владелец)	В этом поле отображается идентифицирующая информация о владельце сертификата, такая как CN (Common Name – Общее имя), OU (Organizational Unit or department – Организационная единица или отдел), O (Organization or company – Организация или компания) и C (Country – Страна). Рекомендуется для каждого сертификата указывать уникальную информацию о владельце.
Valid From (Действителен с)	В этом поле отображается дата, начиная с которой применяется сертификат. Если сертификат еще не может применяться, то текст в этом поле отображается красным шрифтом и содержит сообщение «Not Yet Valid!» (Еще не действителен!).
Valid To (Действителен до)	В этом поле отображается дата, после которой срок действия сертификата заканчивается. Если срок действия сертификата подходит к концу или уже закончился, то текст в этом поле отображается красным шрифтом и содержит сообщение «Expiring!» (Срок заканчивается) или «Expired!» (Срок истек).
Modify (Изменить)	Щелкните по иконке дополнительной информации, чтобы открыть окно, содержащее полную информацию о сертификате. Для сохранения сертификата на компьютере следует щелкнуть значок экспорта. Щелкните по этому значку, затем в окне **File Download (Загрузка файла)** щелкните **Save (Сохранить)**. Откроется окно **Save As (Сохранить как)**. Выберите местонахождение файла и щелкните **Save (Сохранить)**. Для удаления сертификата щелкните по иконке удаления. Появляется окно с запросом на подтверждение операции удаления сертификата. Следует помнить, что при удалении сертификата все последующие сдвигаются на позицию вверх.
Import (Импорт)	Щелкните по кнопке **Import (Импорт)** для отображения окна, где можно перенести сертификат удаленного узла, который рассматривается как надежный, с вашего компьютера в интернет-центр P660HWP.
Refresh (Обновить)	Щелкните по кнопке **Refresh (Обновить)** для обновления информации о текущем статусе сертификатов.

13.13 Доверенные удаленные узлы > Импорт

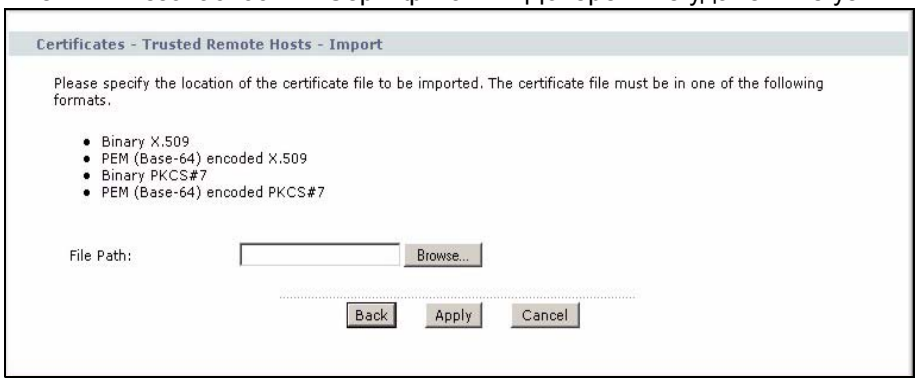
Щелкните **Security (Безопасность) > Certificates (Сертификаты) > Trusted Remote Hosts (Доверенные удаленные узлы)** для отображения окна **Trusted Remote Hosts (Доверенные удаленные узлы)** и затем щелкните по кнопке **Import (Импорт)**, чтобы открыть окно **Trusted Remote Host Import (Импорт доверенных удаленных узлов)**.

У вас могут быть узлы с сертификатами, которым вы можете доверять, но их сертификаты не подписаны ни одним из центров сертификации, перечисленным в окне **Trusted CAs (Доверенные центры сертификации)**. Следуйте указаниям в этом окне для загрузки сертификата узла из компьютера в P660HWP.

Любой действительный сертификат, подписанный доверенным центром сертификации, P660HWP автоматически принимает как надежный, поэтому добавлять сертификат, подписанный центром сертификации, из списка в окне **Trusted CAs (Доверенные центры сертификации)** не требуется.

Сертификат доверенного удаленного узла должен быть самостоятельно подписанным, поэтому прежде чем выполнять импорт этого сертификата, необходимо удалить все пробелы из его имени файла.

Рис. 122 Безопасность > Сертификаты > Доверенные удаленные узлы > Импорт



В следующей таблице даны описания полей этого окна.

Табл. 79 Безопасность > Сертификаты > Доверенные удаленные узлы > Импорт

ПОЛЕ	ОПИСАНИЕ
File Path (Путь к файлу)	Введите в это поле путь к файлу, который требуется загрузить, или щелкните **Browse (Обзор)** для его поиска.
Browse (Обзор)	Щелкните **Browse (Обзор)** для поиска файла сертификата, который требуется загрузить.
Back (Назад)	Для возврата к предыдущему окну нажмите кнопку **Back (Назад)**.
Apply (Применить)	Щелкните **Apply (Применить)** для сохранения сертификата в P660HWP.
Cancel (Отменить)	Щелкните **Cancel (Отмена)** для выхода и возврата к окну **Trusted Remote Hosts (Доверенные удаленные узлы)**.

13.14 Сведения о сертификате доверенного удаленного узла

Щелкните **Security (Безопасность) > Certificates (Сертификаты) > Trusted Remote Hosts (Доверенные удаленные узлы)** для отображения окна **Trusted Remote Hosts (Доверенные удаленные узлы)**. Щелкните по иконке дополнительной информации для перехода к окну **Trusted Remote Host Details (Сведения о доверенном удаленном узле)**. В этом окне можно просмотреть подробную информацию о сертификате доверенного удаленного узла и/или изменить имя сертификата.

Рис. 123 Безопасность > Сертификаты > Удаленные доверенные узлы > Сведения

В следующей таблице даны описания полей этого окна.

Табл. 80 Безопасность > Сертификаты > Удаленные доверенные узлы > Сведения

ПОЛЕ	ОПИСАНИЕ
Certification Name (Название сертификата)	В этом поле отображается описательное имя для данного сертификата. Для изменения имени введите до 31 символа с целью описания этого сертификата. Допускается использовать любые символы, кроме пробелов.
Certificate Path (Путь к сертификату)	Щелкните по кнопке **Refresh (Обновить)** для отображения в текстовом поле собственного сертификата последнего объекта и списка сертификатов центра сертификации в иерархии центров сертификации, который подтверждает центр сертификации, выдавший сертификат. Для доверенного узла этот список содержит собственный сертификат последнего объекта и самостоятельно подписанный сертификат по умолчанию, который используется интернет-центром P660HWP для подписи сертификатов удаленных узлов.
Refresh (Обновить)	Щелкните по кнопке **Refresh (Обновить)** для отображения пути к сертификату.
Certificate Information (Параметры сертификата)	В следующих полях отображается подробная информация о сертификате в режиме только для чтения.
Type (Тип)	В этом поле отображается общая информация о сертификате. Для сертификатов доверенных удаленных хостов в этом поле всегда отображается «CA-signed». Центром сертификации является интернет-центр P660HWP, который подписал этот сертификат. «X.509» означает, что сертификат был создан и подписан в соответствии с правилами ITU-T X.509, которые определяют форматы для сертификатов открытого ключа.
Version (версия)	В этом поле отображается номер версии X.509.
Serial Number (Серийный номер)	В этом поле отображается идентификационный номер сертификата, выданного устройством, которое создало сертификат.
Subject (Владелец)	В этом поле отображается идентифицирующая информация о владельце сертификата, такая как CN (Common Name – Общее имя), OU (Organizational Unit – Организационная единица), O (Organization – Организация) и C (Country – Страна).
Issuer (Издатель)	В этом поле отображается идентифицирующая информация о самостоятельно подписанном сертификате по умолчанию, установленном в P660HWP и использующемся для подписи сертификатов доверенных удаленных узлов.
Signature Algorithm (Алгоритм подписи)	В этом поле отображается тип алгоритма, с помощью которого P660HWP подписал сертификат, например, rsa-pkcs1-sha1 (алгоритм шифрования с использованием открытого-секретного ключа RSA и алгоритм с использованием хэш-функции SHA1).
Valid From (Действителен с)	В этом поле отображается дата, начиная с которой применяется сертификат. Если сертификат еще не может применяться, то текст в этом поле отображается красным шрифтом и содержит сообщение «Not Yet Valid!» (Еще не действителен!).
Valid To (Действителен до)	В этом поле отображается дата, после которой срок действия сертификата заканчивается. Если срок действия сертификата подходит к концу или уже закончился, то текст в этом поле отображается красным шрифтом и содержит сообщение «Expiring!» (Срок заканчивается) или «Expired!» (Срок истек).
Key Algorithm (Алгоритм ключа)	В этом поле отображается тип алгоритма, который используется для генерирования пар ключей сертификатов (в P660HWP используется шифрование RSA), и длина ключа в битах (в примере 1024 бит).

Табл. 80 Безопасность > Сертификаты > Удаленные доверенные узлы > Сведения

ПОЛЕ	ОПИСАНИЕ
Subject Alternative Name (Сведения о владельце)	В этом поле отображается IP-адрес (IP), доменное имя (DNS) или адрес электронной почты (EMAIL) владельца сертификата.
Key Usage (Функции ключа)	В этом поле отображаются функции, для которых применяется ключ сертификата. Например, «DigitalSignature» (Цифровая подпись) означает, что ключ может использоваться для подписи сертификатов, а «KeyEncipherment» (Шифрование с использованием ключа) означает, что ключ может использоваться для шифрования текста.
Basic Constraint (Основные параметры)	В этом поле отображается общая информация о сертификате. Например, «Subject Type=CA» означает, что этот сертификат выдан центром сертификации, а «Path Length Constraint=1» означает, что путь к сертификату содержит только один центр сертификации.
MD5 Fingerprint (Сигнатура MD5)	Это профиль сообщения сертификата, который устройство P660HWP вычислило с использованием алгоритма MD5. Для подписания загружаемых в него сертификатов удаленных доверенных узлов устройство P660HWP использует один из собственных самоподписанных сертификатов. Это приводит к изменению значения отображаемой здесь сигнатуры (она не соответствует оригиналу). См. Разд. 13.3 на с. 212, чтобы узнать, как проверить сертификаты удаленных узлов до загрузки в устройство P660HWP.
SHA1 Fingerprint (Сигнатура SHA1)	Это профиль сообщения сертификата, который интернет-центр P660HWP вычислил с использованием алгоритма SHA1. Для подписания загружаемых в него сертификатов удаленных доверенных узлов устройство P660HWP использует один из собственных самоподписанных сертификатов. Это приводит к изменению значения отображаемой здесь сигнатуры (она не соответствует оригиналу). См. Разд. 13.3 на с. 212, чтобы узнать, как проверить сертификаты удаленных узлов до загрузки в устройство P660HWP.
Certificate in PEM (Base-64) Encoded Format (Сертификат в зашифрованном формате PEM (Base-64))	В этом текстовом поле отображается сертификат или запрос на сертификат в формате PEM (Privacy Enhanced Mail – Электронная почта с усовершенствованной защитой) в режиме только для чтения. В формате PEM для преобразования бинарного сертификата в печатную форму используется 64 символа ASCII. Сертификат можно скопировать и перенести в почтовое сообщение для отправки друзьям или коллегам, а также перенести в текстовый редактор для сохранения в файле на управляющем компьютере для последующего распространения (например, с помощью дискеты).
Back (Назад)	Для возврата к предыдущему окну нажмите кнопку **Back (Назад)**.
Export (Экспорт)	Для экспорта файла со сведениями о сертификате нажмите кнопку **Export (Экспорт)**.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек P660HWP. Изменить можно только имя сертификата.
Cancel (Отменить)	Щелкните **Cancel (Отмена)** для выхода и возврата к окну **Trusted Remote Hosts (Доверенные удаленные хосты)**.

13.15 Серверы каталогов

Щелкните **Security (Безопасность) > Certificate (Сертификаты) > Directory Servers (Серверы каталогов)** для отображения окна **Directory Servers (Серверы каталогов)**. В этом окне отображается сводный список серверов каталогов (которые содержат списки действительных и аннулированных сертификатов), сохраненный в P660HWP.

Если требуется, чтобы P660HWP проверял входящие сертификаты по списку аннулированных сертификатов, выдавшего сертификат центра сертификации, то сначала P660HWP проверяет список серверов в поле **CRL Distribution Points (Пункты распределения CRL)** входящего сертификата. Если в сертификате сервер не указан или указанный сервер недоступен, P660HWP проверяет серверы, перечисленные в этом поле.

Рис. 124 Безопасность > Сертификаты > Серверы каталогов

В следующей таблице даны описания полей этого окна.

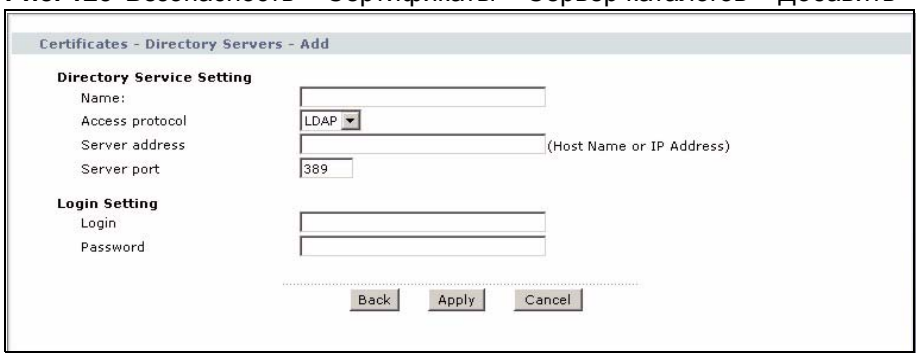
Табл. 81 Безопасность > Сертификаты > Серверы каталогов

ПОЛЕ	ОПИСАНИЕ
PKI Storage Space in Use (Использованная память для хранения инфраструктуры открытого ключа)	Этот индикатор показывает находящуюся в использовании память P660HWP в процентах для хранения инфраструктуры открытого ключа. Когда место для хранения заканчивается, необходимо удалить просроченные или ненужные сертификаты перед добавлением новых сертификатов.
#	Порядковый номер сервера каталогов. Серверы отображаются в алфавитном порядке.
Name (Имя)	В этом поле отображается описательное имя сервера каталогов.
Address (Адрес)	В этом поле отображается IP-адрес или доменное имя сервера каталогов.
Port (Порт)	В этом поле отображается номер порта, который используется сервером каталогов.
Protocol (Протокол)	В этом поле отображается протокол, который используется сервером каталогов.
Modify (Изменить)	Щелкните по иконке дополнительной информации для отображения окна, где можно изменить параметры сервера каталогов. Щелкните по иконке удаления для удаления записи сервера каталогов. Появляется окно с запросом на подтверждение операции удаления сервера каталога. Следует помнить, что при удалении сертификата все последующие сдвигаются на позицию вверх.
Add (Добавить)	Щелкните **Add (Добавить)** для отображения окна, в котором можно изменить параметры сервера каталогов, чтобы обеспечить к нему доступ P660HWP.

13.16 Добавление и удаление сервера каталогов

Щелкните **Security (Безопасность) > Certificate (Сертификаты) > Directory Servers (Серверы каталогов)** для отображения окна **Directory Servers (Серверы каталогов)**. Щелкните по кнопке **Add (Добавить)** (или по иконке дополнительной информации) для отображения окна **Directory Server Add (Добавление сервера каталогов)**. Это окно служит для настройки параметров сервера каталогов для обеспечения доступа к этому серверу P660HWP.

Рис. 125 Безопасность > Сертификаты > Сервер каталогов > Добавить



В следующей таблице даны описания полей этого окна.

Табл. 82 Безопасность > Сертификаты > Сервер каталогов > Добавить

ПОЛЕ	ОПИСАНИЕ
Directory Service Setting (Параметры сервера каталогов)	
Name (Имя)	Введите до 31 символа ASCII (пробелы исключаются) для описания сервера каталогов.
Access Protocol (Протокол доступа)	Из выпадающего списка выберите протокол доступа, который используется сервером каталогов. LDAP (Lightweight Directory Access Protocol – Облегченный протокол службы каталогов) – это протокол поверх TCP, определяющий процедуру доступа клиентов к каталогам сертификатов и спискам аннулированных сертификатов.[A]
Server Address (Адрес сервера)	Введите IP-адрес (в десятичном виде с разделительными точками) или доменное имя сервера каталогов.
Server Port (Порт сервера)	В этом поле отображается номер порта сервера по умолчанию, используемый протоколом, который установлен в поле **Access Protocol (Протокол доступа)**. Если требуется, номер порта сервера можно изменить, но необходимо, чтобы установленный номер порта был такой же, как порт сервера. 389 – номер порта сервера по умолчанию для протокола LDAP.
Login Setting (Параметры регистрации)	
Login (Регистрационное имя)	Чтобы получить доступ к серверу каталогов, интернет-центру P660HWP необходимо пройти аутентификацию. Введите регистрационное имя (до 31 символа ASCII) с объекта, управляющего сервером каталогов (обычно центр сертификации).

Табл. 82 Безопасность > Сертификаты > Сервер каталогов > Добавить

ПОЛЕ	ОПИСАНИЕ
Password (Пароль)	Введите пароль (до 31 символа ASCII) с объекта, управляющего сервером каталогов (обычно центр сертификации).
Back (Назад)	Для возврата к предыдущему окну нажмите кнопку **Back (Назад)**.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек P660HWP.
Cancel (Отменить)	Щелкните **Cancel (Отмена)** для выхода и возврата к окну **Directory Servers (Серверы каталогов)**.

A. На момент написания руководства LDAP является единственным протоколом доступа к серверу каталогов.

Часть V
Дополнительные настройки

14

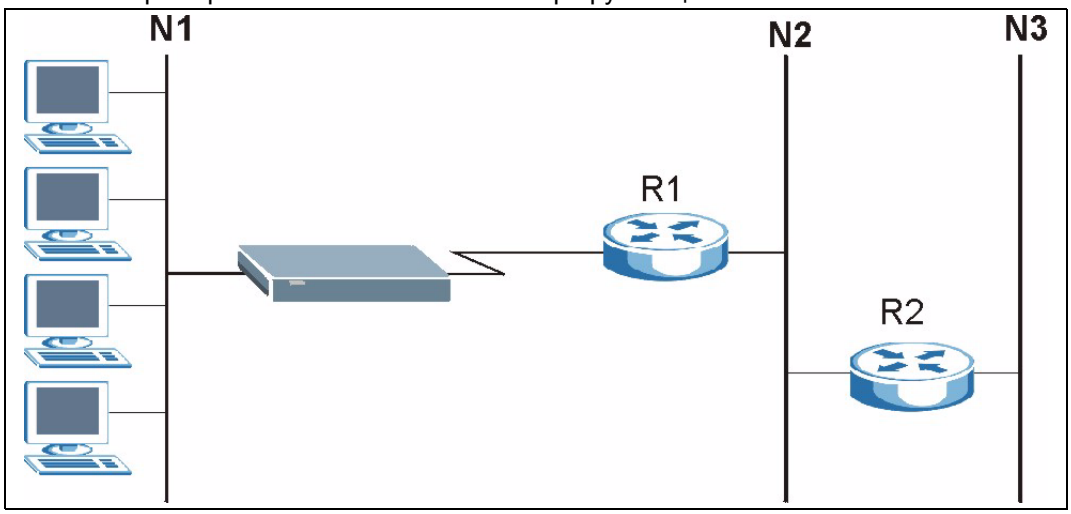
Статический маршрут

В этой главе рассказывается о настройке статических маршрутов P660HWP.

14.1 Статический маршрут

Каждый удаленный узел определяет только ту сеть, к шлюзу которой он непосредственно подключается. Аналогично и P660HWP не имеет никакой информации о сетях, находящихся за ним. В примере на следующем рисунке P660HWP получает информацию о сети N2 через маршрутизатор R1 удаленного узла. Несмотря на это, P660HWP не может отправить пакет в сеть N3, так как он «не знает», что существует маршрут через маршрутизатор R1 удаленного узла и маршрутизатор R2. Статические маршруты предназначены для того, чтобы предоставлять P660HWP информацию о сетях за пределами удаленных узлов.

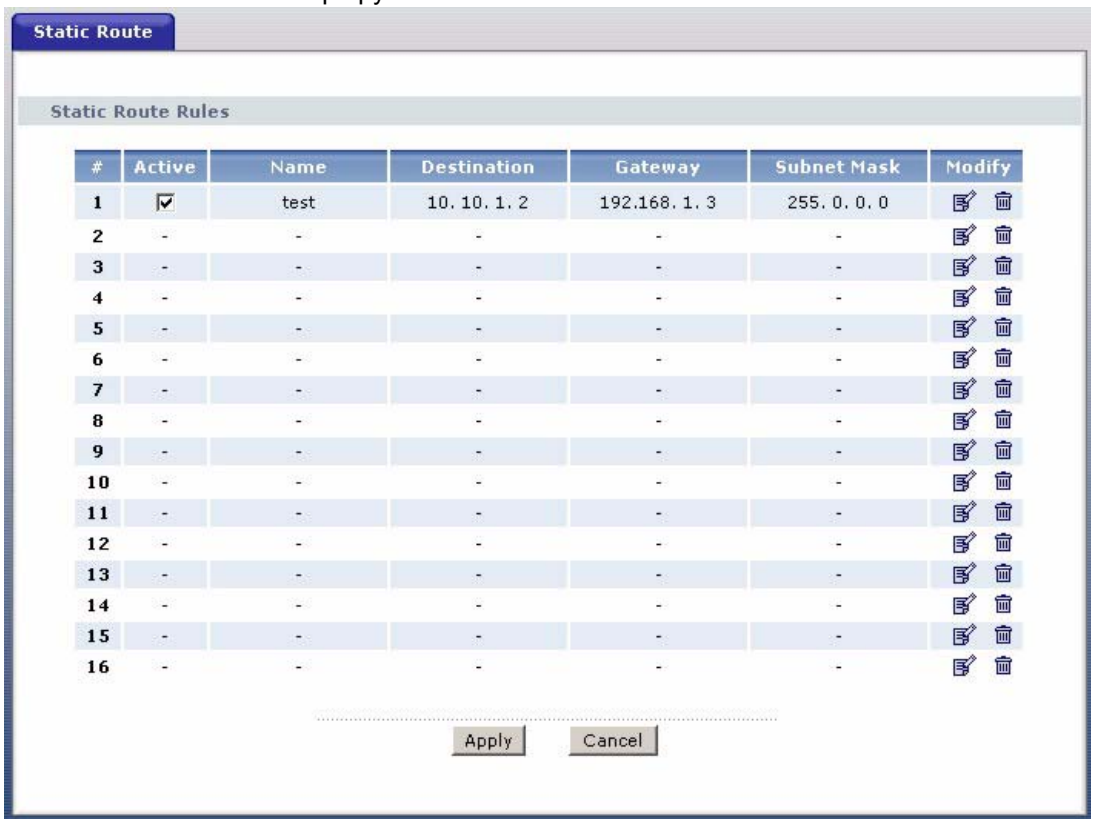
Рис. 126 Пример топологии статической маршрутизации



14.2 Настройка статических маршрутов

Щелкните **Advanced (Дополнительно) > Static Route (Статический маршрут)** для отображения окна **Static Route (Статический маршрут)**.

Рис. 127 Статический маршрут



В следующей таблице даны описания полей этого окна.

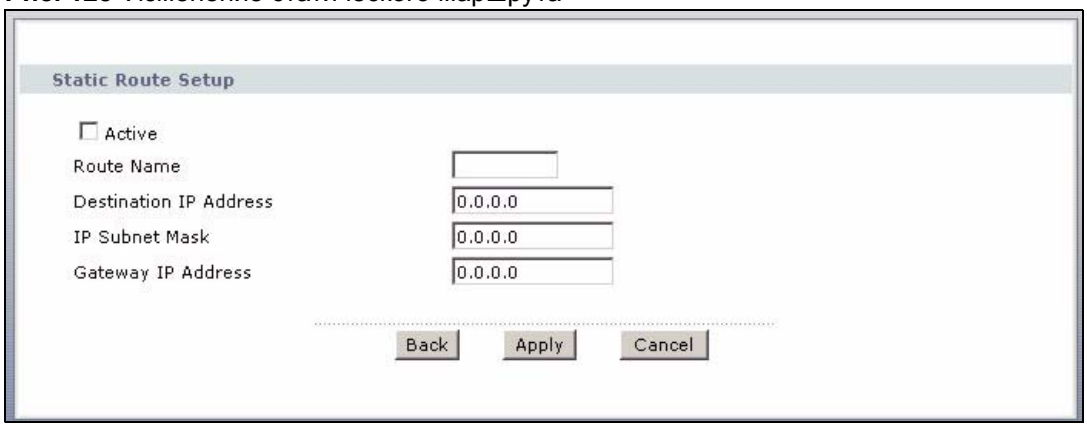
Табл. 83 Статический маршрут

ПОЛЕ	ОПИСАНИЕ
#	Это номер конкретного маршрута.
Active (Активировать)	Установите флажок, чтобы включить данный статический маршрут. В другом случае, снимите флажок.
Name (Имя)	Это описательное имя данного маршрута.
Destination (Адрес назначения)	Данный параметр определяет сетевой IP-адрес конечного получателя. Маршрутизация всегда выполняется на основе номера сети.
Gateway (Шлюз)	В этом поле отображается IP-адрес шлюза. Шлюз – это маршрутизатор или коммутатор, находящийся в том же сегменте сети, что и порт LAN или WAN устройства. Шлюз помогает пересылать пакеты их адресатам.
Subnet Mask (Маска подсети)	Это маска IP подсети.
Modify (Изменить)	Щелкните по иконке редактирования для перехода к окну, где можно изменить параметры статического маршрута P660HWP. Щелкните по иконке удаления для удаления статического маршрута P660HWP. Появится окно с запросом на подтверждение операции удаления маршрута.

14.2.1 Изменение статического маршрута

Выберите номер статического маршрута и щелкните по иконке редактирования ( ). При этом откроется показанное ниже окно. В этом окне выполняется настройка параметров статического маршрута.

Рис. 128 Изменение статического маршрута



В следующей таблице даны описания полей этого окна.

Табл. 84 Изменение статического маршрута

ПОЛЕ	ОПИСАНИЕ
Active (Активировать)	Это поле служит для включения/отключения данного статического маршрута.
Route Name (Имя маршрута)	Введите имя статического маршрута IP. Чтобы удалить данный статический маршрут, оставьте это поле пустым.
Destination IP Address (IP-адрес назначения)	Данный параметр определяет сетевой IP-адрес конечного получателя. Маршрутизация всегда выполняется на основе номера сети. Если нужно определить маршрут к одиночному узлу, в поле маски подсети используйте маску подсети 255.255.255.255, чтобы номер сети и адрес узла были одинаковыми.
IP Subnet Mask (Маска IP подсети)	Введите маску подсети IP.
Gateway IP Address (IP-адрес шлюза)	Введите IP-адрес шлюза. Шлюз – это маршрутизатор или коммутатор, находящийся в том же сегменте сети, что и порт LAN или WAN устройства. Шлюз помогает пересылать пакеты их адресатам.
Back (Назад)	Для возврата к предыдущему окну без сохранения изменений нажмите кнопку **Back (Назад)**.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек P660HWP.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.

15

Управление пропускной способностью

В этой главе рассказывается о настройке управления пропускной способностью P660HWP, изменении правил и просмотре регистрационных журналов управления пропускной способностью.

15.1 Обзор управления пропускной способностью

Управление пропускной способностью ZyXEL позволяет устанавливать правила управления пропускной способностью для отдельных приложений и/или подсетей. В правилах можно устанавливать определенную величину пропускной способности (бюджет).

Управление пропускной способностью применяется к трафику, выходящему через интерфейс P660HWP. P660HWP не управляет пропускной способностью входящего трафика.

Управление пропускной способностью применяется ко всему трафику, выходящему через порт маршрутизатора, независимо от источника этого трафика.

Перенаправление трафика и псевдонимы IP могут вызвать трафик между локальными сетями, который проходит через P660HWP, и, следовательно, регулируется системой управления пропускной способностью.

Сумма распределенной пропускной способности по разным типам трафика на каждом интерфейсе должна быть меньше или равна скорости, установленной для этого интерфейса в окне **Bandwidth Management (Управление пропускной способностью) > Summary (Общие настройки)**.

15.2 Управление пропускной способностью на основе приложений

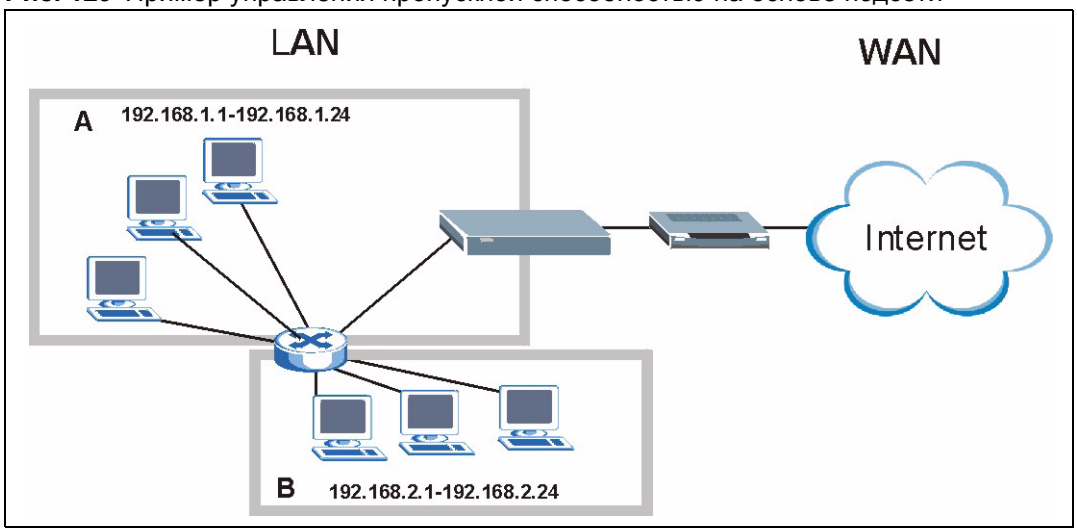
Вы можете создавать классы пропускной способности на основе конкретных приложений (например, VoIP, Web, FTP, E-mail и передача видеосигналов).

15.3 Управление пропускной способностью на основе подсетей

Вы можете создавать классы пропускной способности на основе подсетей.

На следующем рисунке показаны локальные подсети. Можно установить один класс пропускной способности для подсети **A**, а другой – для подсети **B**.

Рис. 129 Пример управления пропускной способностью на основе подсети



15.4 Управление пропускной способностью на основе приложений и подсетей

Также можно создавать классы пропускной способности на основе комбинирования подсетей и приложений. В следующей таблице приводится пример распределения пропускной способности для трафика конкретных приложениий из разных локальных подсетей.

Табл. 85 Пример управления пропускной способностью на основе приложения и подсети

ТИП ТРАФИКА	ИЗ ПОДСЕТИ A	ИЗ ПОДСЕТИ B
VoIP	64 Кбит/с	64 Кбит/с
Web	64 Кбит/с	64 Кбит/с
FTP	64 Кбит/с	64 Кбит/с
E-Mail	64 Кбит/с	64 Кбит/с
Video	64 Кбит/с	64 Кбит/с

15.5 Планировщик

Планировщик распределяет пропускную способность интерфейса по классам пропускной способности. В интернет-центре P660HWP есть планировщик двух видов: на основе равномерного распределения и на основе приоритетов.

15.5.1 Планировщик на основе приоритетов

При использовании планировщика на основе приоритетов интернет-центр P660HWP пересылает трафик различных классов пропускной способности в соответствии с назначенными этим классам приоритетами. Чем больше значение приоритета у того или иного класса, тем выше его приоритет. Для обеспечения более надежной работы приложениям реального времени (где используется аудио или видео) следует присваивать большие приоритеты.

15.5.2 Планировщик на основе равномерного распределения

При использовании планировщика на основе равномерного распределения интернет-центр P660HWP распределяет пропускную способность между всеми классами поровну, что предотвращает использование всей пропускной способности интерфейса одним классом пропускной способности.

15.6 Увеличение пропускной способности

Функция увеличения использования пропускной способности (см. Рис. 130 на с. 251) позволяет интернет-центру P660HWP распределять доступную пропускную способность интерфейса (в т.ч. незарезервированную и зарезервированную, но не используемую) между классами, требующими увеличения пропускной способности.

Если эта функция включена, интернет-центр P660HWP сначала проверяет, что каждому классу выделена установленная ему пропускная способность. Затем интернет-центр P660HWP распределяет доступную пропускную способность интерфейса (нераспределенную или неиспользуемую классами) между классами, требующими увеличения пропускной способности, в зависимости от количества этих классов и от уровней их приоритетов. Если увеличение пропускной способности требуется только одному классу, P660HWP выделяет дополнительную пропускную способность этому классу полностью.

Если дополнительная пропускная способность требуется нескольким классам, интернет-центр P660HWP сначала предоставляет доступную пропускную способность классам с более высоким приоритетом (столько, сколько им нужно, если достаточно имеющейся пропускной способности), а затем – классам с более низким приоритетом из оставшихся ресурсов. Интернет-центр P660HWP равномерно распределяет доступную пропускную способность между классами с одинаковым уровнем приоритетов.

15.6.1 Резервирование пропускной способности для трафика, не относящегося к классам пропускной способности

Чтобы интернет-центр P660HWP выделял пропускную способность для типа трафика, который не прописан в фильтре пропускной способности, выполните следующие действия.

1. Оставьте часть пропускной способности порта нераспределенной.
2. Не включайте опцию **Maximize Bandwidth Usage (Увеличение использования пропускной способности)**.
3. Не активируйте заимствование пропускной способности для подклассов, исходным классом которых является корневой класс (см. Разд. 15.9 на с. 252).

15.6.2 Пример увеличения использования пропускной способности

Здесь приводится пример увеличения пропускной способности P660HWP, установленной для данного интерфейса. В следующей таблице показано распределение пропускной способности по классам. Классы построены на основе подсетей. Пропускная способность интерфейса составляет 10240 кбит/с. Каждой подсети выделяется по 2048 кбит/с. Небюджетированные 2048 кбит/с позволяют пропускать трафик, не определенный ни в одном фильтре, если не активировано увеличение пропускной способности.

Табл. 86 Пример увеличения использования пропускной способности

КЛАССЫ И РАСПРЕДЕЛЕНИЕ ПРОПУСКНОЙ СПОСОБНОСТИ	
Корневой класс: 10240 кбит/с	Администрация: 2048 кбит/с
	Отдел продаж: 2048 кбит/с
	Отдел маркетинга: 2048 кбит/с
	Исследовательский отдел: 2048 кбит/с

Интернет-центр P660HWP распределяет оставшиеся 2048 кбит/с между классами, которым требуется дополнительная пропускная способность. Если административный отдел использует только 1024 кбит/с из выделенных ему 2048 кбит/с, то интернет-центр P660HWP также распределяет оставшиеся 1024 кбит/с между классами, которым требуется дополнительная пропускная способность. Поэтому интернет-центр P660HWP распределит между классами, испытывающими недостаток пропускной способности, в общей сложности 3072 кбит/с из небюджетированной и неиспользуемой пропускной способности.

15.6.2.1 Распределение неиспользуемой и небюджетированной пропускной способности на основе приоритета

В следующей таблице показаны приоритеты классов пропускной способности и величина пропускной способности, установленная для каждого класса.

Табл. 87 Пример распределения неиспользуемой и небюджетированной пропускной способности на основе приоритета

КЛАССЫ, ПРИОРИТЕТЫ И РАСПРЕДЕЛЕНИЕ ПРОПУСКНОЙ СПОСОБНОСТИ	
Корневой класс: 10240 кбит/с	Администрация: приоритет 4, 1024 кбит/с
	Отдел продаж: приоритет 6, 3584 кбит/с
	Отдел маркетинга: приоритет 6, 3584 кбит/с
	Исследовательский отдел: приоритет 5, 2048 кбит/с

Предположим, что дополнительная пропускная способность требуется всем классам, за исключением класса «Администрация».

- Каждый класс получает свою запланированную долю пропускной способности (т. н. бюджет). Администрацией используется только 1024 кбит/с из выделенных ей 2048 кбит/с.
- Отделы продаж и маркетинга получат дополнительную пропускную способность первыми, поскольку имеют самый высокий приоритет (6). Если обоим отделам нужно дополнительно по 1536 кбит/с или более, то интернет-центр P660HWP распределит 3072 кбит/с из небюджетированной и неиспользованной пропускной между ними поровну (добавит по 1536 кбит/с каждому отделу, так что у каждого отдела будет по 3584 кбит/с), поскольку оба отдела имеют одинаковый и самый высокий приоритет.
- Исследовательскому отделу также требуется дополнительная пропускная способность, но он получает только выделенные ему 2048 кбит/с, так как вся небюджетированная и неиспользованная пропускная способность выделяется отделам продаж и маркетинга, имеющим более высокий приоритет.

15.6.2.2 Распределение неиспользуемой и небюджетированной пропускной способности на основе равномерного распределения

В следующей таблице показана величина пропускной способности, назначенная каждому классу.

Табл. 88 Пример распределения неиспользуемой и небюджетированной пропускной способности на основе равномерного распределения

КЛАССЫ И РАСПРЕДЕЛЕНИЕ ПРОПУСКНОЙ СПОСОБНОСТИ	
Корневой класс: 10240 кбит/с	Администрация: 1024 кбит/с
	Отдел продаж: 3072 кбит/с
	Отдел маркетинга: 3072 кбит/с
	Исследовательский отдел: 3072 кбит/с

Предположим, что дополнительная пропускная способность требуется всем классам, за исключением класса «Администрация».

- Каждый класс получает свою запланированную долю пропускной способности (т. н. бюджет). Администрацией используется только 1024 кбит/с из выделенных ей 2048 кбит/с.

- Интернет-центр P660HWP распределяет 3072 кбит/с из небюджетированной и неиспользованной пропускной способности поровну между всеми остальными классами. Каждый класс получает дополнительно 1024 кбит/с, таким образом, общая пропускная способность для каждого класса составит 3072 кбит/с.

15.6.3 Приоритеты при управлении пропускной способностью

В следующей таблице представлены приоритеты, применяемые к трафику, проходящему через интерфейс P660HWP.

Табл. 89 Приоритеты при управлении пропускной способностью

УРОВНИ ПРИОРИТЕТОВ: ТРАФИК С БОЛЕЕ ВЫСОКИМ ПРИОРИТЕТОМ ПРОПУСКАЕТСЯ ГОРАЗДО БЫСТРЕЕ, ТОГДА КАК ТРАФИК С БОЛЕЕ НИЗКИМ ПРИОРИТЕТОМ СБРАСЫВАЕТСЯ, ЕСЛИ СЕТЬ ПЕРЕГРУЖЕНА.	
Высокий	Обычно используется для трафика передачи речи или видеоизображений, который очень чувствителен к дрожанию (дрожание – это изменение величины задержки).
Средний	Обычно используется для трафика «excellent effort» или выше по приоритету, чем «best effort», и может включать важный деловой трафик, который допускает некоторую задержку.
Низкий	Обычно используется для второстепенного «низкоприоритетного» трафика, такого как основная масса данных, которая передается, но не влияет на другие приложения и пользователей.

15.7 Предоставление пропускной способности свыше назначенной

Можно установить пропускную способность конкретного интерфейса выше, чем фактическая скорость передачи этого интерфейса. Трафик с более высоким приоритетом при необходимости сможет использовать всю назначенную пропускную способность, даже если при этом будет использована вся доступная пропускная способность этого интерфейса. При этом передача трафика с более низким приоритетом будет остановлена. Рассмотрим следующий пример.

Табл. 90 Предоставление пропускной способности свыше назначенной

КЛАССЫ ПРОПУСКНОЙ СПОСОБНОСТИ, РАСПРЕДЕЛЕНИЕ		**ПРИОРИТЕТЫ**
Фактическая пропускная способность исходящего трафика, доступная для интерфейса: 1000 кбит/с		
Корневой класс: 1500 кбит/с (такая же как скорость)	Трафик VoIP (Служба = SIP): 500 кбит/с	Высокий
	Трафик NetMeeting (Служба = H.323): 500 кбит/с	Высокий
	FTP (Служба = FTP): 500 кбит/с	Средний

Если одновременно передается трафик VoIP и NetMeeting, устройство сначала предоставляет пропускную способность до 500 кбит/с для каждого трафика, а оставшуюся пропускную способность предоставляет трафику FTP. В результате, трафик FTP будет передаваться только тогда, когда скорость трафиков VoIP и NetMeeting меньше, чем предоставленная им пропускная способность.

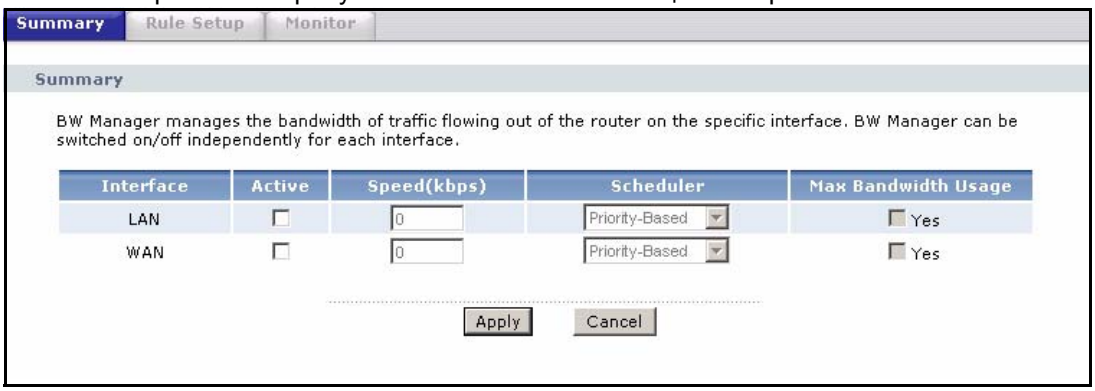
Предположим, что также требуется использовать службу web. В этом случае, трафики VoIP, NetMeeting и FTP имеют более высокий приоритет, поэтому пропускная способность им предоставляется в первую очередь. Трафик web будет передаваться только тогда, когда трафики VoIP, NetMeeting и FTP не будут использовать полностью 1000 кбит/с доступной пропускной способности.

15.8 Общие настройки

Щелкните **Advanced (Дополнительно)** > **Bandwidth MGMT (Управление пропускной способностью)** для отображения окна, показанного ниже.

Активируйте управление пропускной способностью порта и установите максимально допустимую пропускную способность для данного порта.

Рис. 130 Управление пропускной способностью: Общие настройки



В следующей таблице даны описания полей этого окна.

Табл. 91 Управление пропускной способностью: Общие настройки

ПОЛЕ	ОПИСАНИЕ
Interface (Интерфейс)	Эти поля «только для чтения» обозначают физические порты. Для включения управления пропускной способностью того или иного порта поставьте флажок напротив его названия. Управление пропускной способностью применяется ко всему трафику, выходящему через порт маршрутизатора, независимо от источника этого трафика. Перенаправление трафика и псевдонимы IP могут вызвать трафик между локальными сетями, который проходит через P660HWP, и, следовательно, регулируется системой управления пропускной способностью.
Active (Активировать)	Для включения управления пропускной способностью того или иного порта поставьте флажок напротив его названия.

Табл. 91 Управление пропускной способностью: Общие настройки (продолжение)

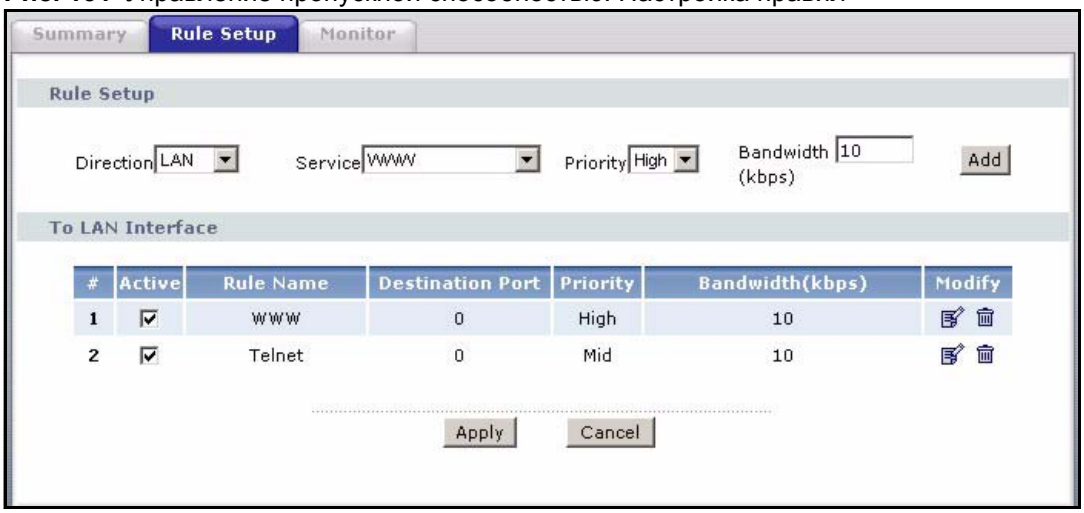
ПОЛЕ	ОПИСАНИЕ
Speed (kbps) (Скорость, кбит/с)	Введите пропускную способность данного порта, которую необходимо назначить с помощью управления пропускной способностью. Рекомендуется установить скорость, соответствующую фактической скорости передачи интерфейса. Например, установите скорость порта WAN равной 1000 кбит/с, если подключение к Интернету имеет скорость исходящего потока 1 Мбит/с. Это значение можно установить выше, чем фактическая скорость передачи интерфейса. При этом передача трафика с более низким приоритетом может быть остановлена, если трафик с более высоким приоритетом использует всю пропускную способность. Также это значение можно установить ниже, чем фактическая скорость передачи интерфейса. Если при этом флажок **Max Bandwidth Usage (Максимизировать использование пропускной способности)** не установлен, это может привести к тому, что P660HWP не будет использовать часть доступной пропускной способности интерфейса.
Scheduler (Планировщик)	Из раскрывающегося меню выберите **Priority-Based (Согласно приоритетам)** или **Fairness-Based (На основе равномерного распределения)**. Опцию **Priority-Based** следует выбрать, если нужно отдать предпочтение более приоритетным классам. Выберите опцию **Fairness-Based**, если все классы должны иметь равные приоритеты.
Max Bandwidth Usage (Увеличение пропускной способности)	Установите в этом поле флажок, чтобы интернет-центр P660HWP распределял всю незарезервированную и/или неиспользуемую пропускную способность интерфейса между классами, которым требуется дополнительная пропускная способность. Не отмечайте опцию, если нужно зарезервировать пропускную способность для трафика, не подпадающего ни под один класс, или если необходимо ограничить скорость порта (см. описание поля **Speed (Скорость)**).
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек P660HWP.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.

15.9 Настройка правил управления пропускной способностью

Прежде чем устанавливать правила для конкретного интерфейса, необходимо включить управление пропускной способностью этого интерфейса в окне **Bandwidth Management Summary (Управление пропускной способностью – Общие настройки)**.

Щелкните **Advanced (Дополнительно) > Bandwidth MGMT (Управление пропускной способностью)** > **Rule Setup (Настройка правил)** для отображения окна, показанного ниже.

Рис. 131 Управление пропускной способностью: Настройка правил



В следующей таблице даны описания полей этого окна.

Табл. 92 Управление пропускной способностью: Настройка правил

ПОЛЕ	ОПИСАНИЕ
Direction (Направление)	Выберите направление трафика, к которому необходимо применять управление пропускной способностью.
Service (Служба)	Установите службу для данного правила или выберите **User Defined (Определяется пользователем)** для перехода к окну, где можно настроить службу.
Priority (Приоритет)	Выберите приоритет из раскрывающегося списка. Вариантами являются: **High (Высокий)**, **Mid (Средний)** или **Low (Низкий)**.
Bandwidth (Пропускная способность, кбит/с)	Установите максимально допустимую для данного правила пропускную способность в кбит/с. Для отдельных правил рекомендуется устанавливать скорость от 20 до 20 000 кбит/с.
Add (Добавить)	Щелкните по этой кнопке, чтобы добавить в таблицу новое правило.
#	Это номер конкретного правила управления пропускной способностью.
Active (Активировать)	Это поле показывает, включено ли данное правило. Установите в этом поле флажок, чтобы P660HWP применял данное правило управления пропускной способностью. Включите правило управления пропускной способностью, чтобы назначить трафику, который соответствует данному правилу, приоритет над трафиком, который не соответствует данному правилу. Включение правила управления пропускной способностью позволяет также контролировать максимальную величину пропускной способности, которая может использоваться трафиком, соответствующим данному правилу.
Rule Name (Имя правила)	В этом поле отображается имя правила.
Destination Port (Порт назначения)	Это номер порта пункта назначения. 0 означает любой порт назначения.
Priority (Приоритет)	Это приоритет для данного правила.
Bandwidth (Пропускная способность, кбит/с)	Это максимально допустимая для данного правила пропускная способность в кбит/с.

Табл. 92 Управление пропускной способностью: Настройка правил (продолжение)

ПОЛЕ	ОПИСАНИЕ
Modify (Изменить)	Щелкните по иконке редактирования для перехода к окну, где можно менять параметры правила. Для удаления существующего правила щелкните по иконке удаления.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек P660HWP.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.

15.10 DiffServ

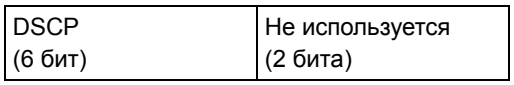
DiffServ – это модель класса обслуживания (CoS), в соответствии с которой пакеты получают специальную метку, чтобы затем подвергнуться специальной обработке (в зависимости от типов приложения и потока трафика) на каждом транзитном пункте вдоль всего маршрута со стороны совместимых с DiffServ сетевых устройств. Пакеты помечаются точками кодирования DiffServ (DSCPs), указывающими на желаемый уровень обслуживания. Это позволяет совместимым с DiffServ сетевым устройствам незамедлительно начинать обработку пакетов в зависимости от точек кодирования, не тратя время на определение пути и запоминание информации о состоянии каждого из потоков. При этом приложениям нет необходимости запрашивать определенные службы или давать расширенные отчеты о том, где проходит трафик.

15.10.1 Обработка по точкам кодирования на транзитных пунктах

DiffServ создает новое поле DS (Differentiated Services – дифференцированное обслуживание), которое должно заменить поле типа обслуживания (TOS) в IP-заголовке. 2 бита поля DS не используются, остальные 6 бит отводятся под точку кодирования DSCP, с помощью которой можно определить до 64 уровней обслуживания. Поле DS показано на следующем рисунке.

DSCP обратно совместим с битами очередности в октете ToS, который не совместим с DiffServ, т.е. сетевые устройства с поддержкой ToS не будут конфликтовать с DSCP.

Рис. 132 DiffServ: Поле дифференцированного обслуживания



Значение DSCP определяет обработку для последующего перенаправления (PHB (Per-Hop Behavior – обработка на каждом транзитном пункте)), которой подвергается каждый пакет, проходящий по сети DiffServ. По правилу маркировки разные типы трафика могут получать разные приоритеты маршрутизации. При этом ресурсы распределяются в соответствии со значениями DSCP и установленными политиками.

PHB состоит из двух типов обслуживания: EF (срочное перенаправление) и AF (гарантированное перенаправление). EF имеет повышенный приоритет. При обслуживании типа EF потери и задержки будут минимальными. Тип AF состоит из четырех подклассов, каждый из которых имеет по три уровня важности (приоритетное отбрасывание). Высокий приоритет отбрасывания означает низкую важность.

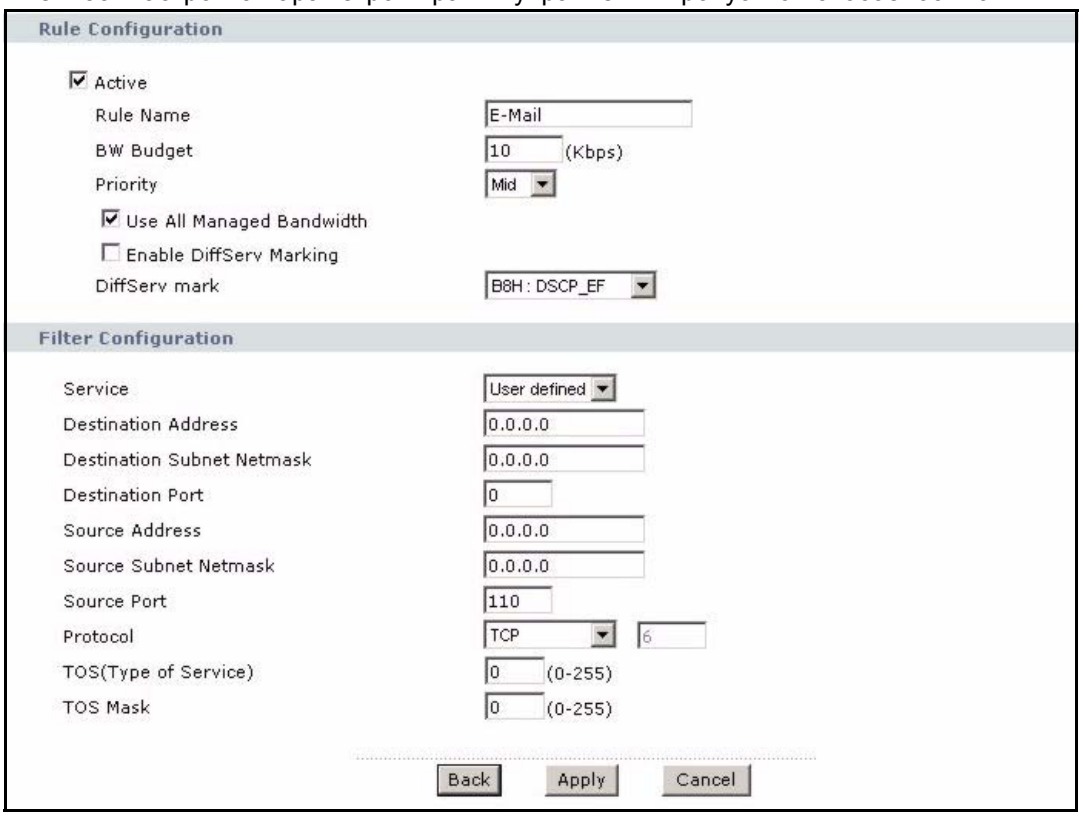
Табл. 93 Подклассы служб AF

ПРИОРИТЕТ DIFFSERV	НИЗКИЙ ПРИОРИТЕТ ОТБРАСЫВАНИЯ	СРЕДНИЙ ПРИОРИТЕТ ОТБРАСЫВАНИЯ	ВЫСОКИЙ ПРИОРИТЕТ ОТБРАСЫВАНИЯ
SUB-CLASS4	AF41	AF42	AF43
SUB-CLASS3	AF31	AF32	AF33
SUB-CLASS2	AF21	AF22	AF23
SUB-CLASS1	AF11	AF12	AF13

15.10.2 Параметры правила

Для настройки параметров правила управления пропускной способностью щелкните по иконке редактирования или выберите **User Defined (Определяется пользователем)** из выпадающего списка поля **Service (Служба)** в окне **Rule Setup (Настройка правил)**. Правила пропускной способности используются для распределения полной пропускной способности (бюджетов пропускной способности) между отдельными приложениями и/или подсетями.

Рис. 133 Настройка параметров правил управления пропускной способностью



В следующей таблице даны описания полей этого окна.

Табл. 94 Настройка параметров правил управления пропускной способностью

ПОЛЕ	ОПИСАНИЕ
Rule Configuration (Параметры правила)	
Active (Активировать)	Установите в этом поле флажок, чтобы P660HWP применял данное правило управления пропускной способностью. Включите правило управления пропускной способностью, чтобы назначить трафику, который соответствует данному правилу, приоритет над трафиком, который не соответствует данному правилу. Включение правила управления пропускной способностью позволяет также контролировать максимальную величину пропускной способности, которая может использоваться трафиком, соответствующим данному правилу.
Rule Name (Имя правила)	Используйте автоматически создаваемое имя или введите описательное имя длиной до 20 буквенно-цифровых символов, включая пробелы.
BW Budget (Бюджет пропускной способности)	Установите максимально допустимую для данного правила пропускную способность в кбит/с. Для отдельных правил рекомендуется устанавливать скорость от 20 до 20 000 кбит/с.
Priority (Приоритет)	Выберите приоритет из раскрывающегося списка. Вариантами являются: **High (Высокий)**, **Mid (Средний)** или **Low (Низкий)**.
Use All Managed Bandwidth (Использовать всю контролируемую пропускную способность)	Установите в этом поле флажок, чтобы разрешить правилу занимать неиспользуемую пропускную способность для данного интерфейса. Перераспределение пропускной способности производится в зависимости от приоритета правил. То есть, правило с более высоким приоритетом первым занимает пропускную способность. Снимите флажок, если требуется оставить доступную пропускную способность другим типам трафика или необходимо ограничить величину пропускной способности, которая может быть использована трафиком, соответствующим данному правилу.
Enable DiffServ Marking (Включить маркировку DiffServ)	Этот пункт включает маркировку DiffServ на устройстве P660HWP.
DiffServ mark (Маркировка DiffServ)	Выберите правило маркировки из раскрывающегося списка. Первые три цифры означают точку кодирования DiffServ. При занятой линии пакеты с самым низким знаком приоритета будут сбрасываться.
Filter Configuration (Параметры фильтра)	

Табл. 94 Настройка параметров правил управления пропускной способностью

ПОЛЕ	ОПИСАНИЕ
Service (Служба)	Это поле упрощает настройку класса пропускной способности, так как позволяет выбрать стандартное приложение. При установке стандартного приложения не требуется заполнять остальные поля фильтра пропускной способности (исключая включение и отключение фильтра). SIP (Протокол инициирования сеанса) представляет собой протокол, используемый в Интернет-телефонии, рассылке сообщений и прочих приложениях VoIP (Передача голоса по IP). Выберите **SIP** из раскрывающегося списка для настройки фильтра пропускной способности на трафик, использующий SIP. Протокол передачи файлов (FTP) является службой передачи файлов по сети Интернет и по сетям на основе TCP/IP. Система, в которой запущен сервер FTP, принимает команды от системы, в которой запущен клиент FTP. Данная служба позволяет пользователям посылать команды на сервер для загрузки и выгрузки файлов. Выберите **FTP** из раскрывающегося списка для настройки этого фильтра пропускной способности для трафика FTP. H.323 – стандартный протокол для телеконференций, обеспечивающий конференц-связь с обменом аудио, видео и обычными данными. Позволяет осуществлять связь в реальном времени между двумя и несколькими клиентскими компьютерами в сети с пакетным обменом, не гарантирующей качества обслуживания. Выберите **H.323** из раскрывающегося списка для настройки этого фильтра на трафик, использующий H.323 Выберите **User defined (Определяется пользователем)** из выпадающего списка, если для класса пропускной способности требуется использовать нестандартное приложение. При выборе **User defined (Определяется пользователем)** необходимо заполнить по меньшей мере одно из следующих полей (исключая поля **Subnet Mask (Маска подсети)**, которые нужно вводить, только если вы установили соответствующие IP-адреса источника и назначения).
Destination Address (Адрес назначения)	Введите IP-адрес получателя в десятичном виде с разделительными точками.
Destination Subnet Netmask (Маска подсети получателя)	Введите маску подсети получателя. Это поле будет недоступно, если не установлен **Destination Address (Адрес назначения)**. Для получения дополнительной информации о подсетях IP см. приложения.
Destination Port (Порт назначения)	Введите номер порта получателя. Информацию о распространенных службах и номерах портов см. *Табл. 95 на с. 258*. Пустое поле IP-адреса означает любой IP-адрес.
Source Address (Адрес источника)	Введите IP-адрес источника в десятичном виде с разделительными точками. Пустое поле означает любой IP-адрес источника.
Source Subnet Netmask (Маска подсети источника)	Введите маску подсети получателя. Это поле будет недоступно, если не установлен **Source Address (Адрес источника)**. Для получения дополнительной информации о подсетях IP см. приложения. Пустое поле означает любой порт источника.
Source Port (Порт источника)	Введите номер порта отправителя. Информацию о распространенных службах и номерах портов см. Табл. 95 на с. 258.
Protocol (Протокол)	Выберите протокол (**TCP** или **UDP**) или установите **User defined (Определяется пользователем)** и введите номер протокола (тип службы). 0 означает любой номер протокола.
ToS (Тип услуги)	ToS (Type of Service – Тип услуги) определяет поле DS (Differentiated Service – Дифференцированная служба) в IP-заголовке пакета. Укажите новое значение TOS для исходящего пакета (от 0 до 255). 0 означает самый низкий приоритет.

Табл. 94 Настройка параметров правил управления пропускной способностью

ПОЛЕ	ОПИСАНИЕ
TOS Mask (Маска TOS)	Маска TOS используется для сравнения указанных (или всех) битов IP-заголовка TOS со значением, указанным в данном правиле. Введите значение **TOS Mask (Маска TOS)** от 0 (низший приоритет) до 255.
Back (Назад)	Для возврата к предыдущему окну нажмите кнопку **Back (Назад)**.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек P660HWP.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.

Табл. 95 Службы и номера портов

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

15.11 Мониторинг пропускной способности

Для просмотра информации об использовании и распределении пропускной способности P660HWP щелкните **Advanced (Дополнительно) > Bandwidth MGMT (Управление пропускной способностью) > Monitor (Монитор)**. При этом откроется показанное ниже окно. Из раскрывающегося списка выберите интерфейс, для которого необходимо посмотреть использование пропускной способности по правилам. Серая часть индикатора показывает неиспользуемую пропускную способность в процентах, а оранжевый цвет показывает используемую пропускную способность. Окно обновляется с периодом в несколько секунд.

Рис. 134 Управление пропускной способностью: Монитор

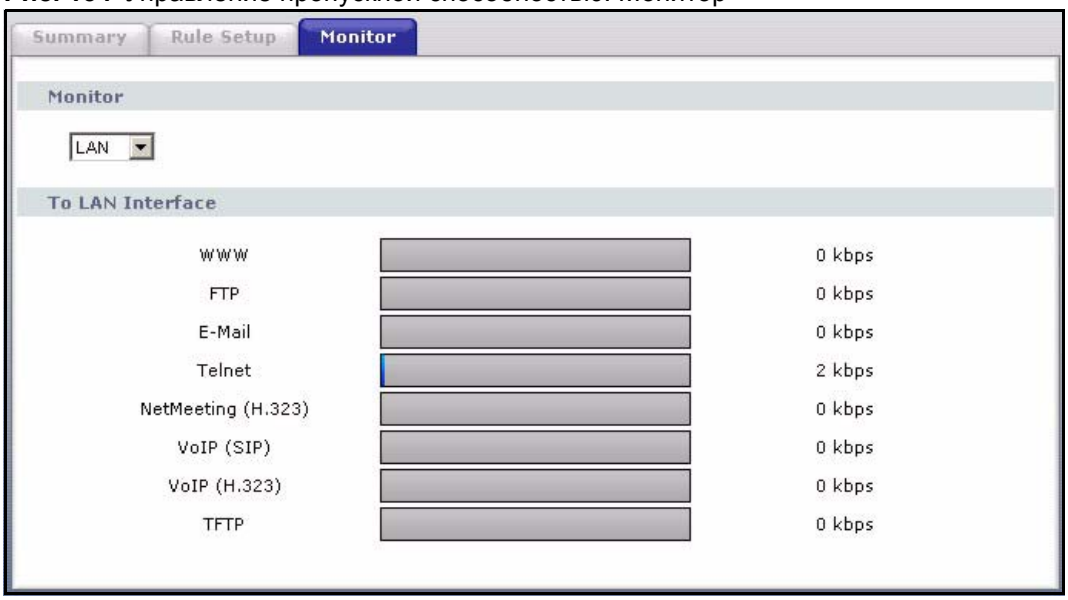


Табл. 96 Управление пропускной способностью: Монитор

ПОЛЕ	ОПИСАНИЕ
Monitor (Мониторинг)	В данном разделе можно выбрать сеть для мониторинга. Доступны следующие варианты: **LAN**, **WLAN** или **WAN**. После выбора на экране появится информация об активных службах и занимаемой ими полосе пропускания.

16

Настройка динамической системы доменных имен (DYNDNS)

В этой главе рассказывается, как выполнить настройку P660HWP для использования динамической службы доменных имен.

16.1 Динамическая система доменных имен (DYNDNS) – общая информация

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

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

16.1.1 Маски DYNDNS

Использование масок позволяет соотносить имена вида *.yourhost.dyndns.org с тем же IP-адресом, что и имя yourhost.dyndns.org. Данная функция полезна, если вы хотите иметь возможность использовать, например, адрес www.yourhost.dyndns.org и при этом предоставлять доступ к вашему узлу.

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

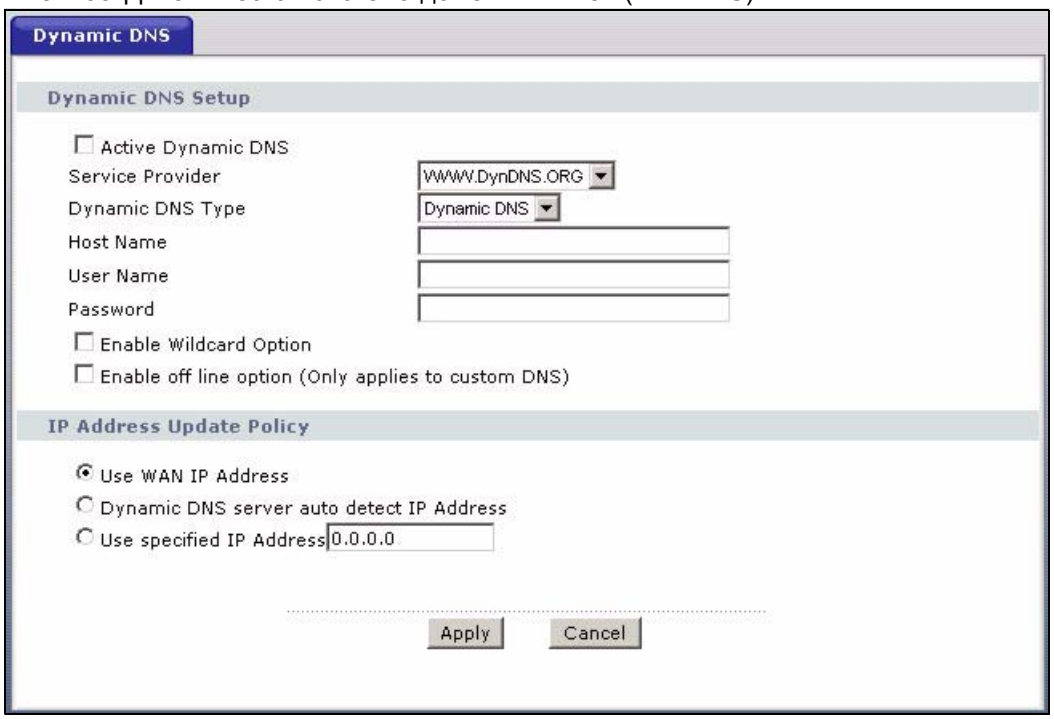
Инструкции по настройке см. Разд. 16.2 на с. 262.

16.2 Настройка динамической DNS (DYNDNS)

Для изменения настроек DDNS в P660HWP щелкните **Advanced (Дополнительно)** > **Dynamic DNS (Динамическая DNS)**. При этом откроется показанное ниже окно.

Более подробную информацию см. Разд. 16.1 на с. 261.

Рис. 135 Динамическая система доменных имен (DYNDNS)



В следующей таблице даны описания полей этого окна.

Табл. 97 Динамическая система доменных имен (DYNDNS)

ПОЛЕ	ОПИСАНИЕ
Dynamic DNS Setup (Настройка динамической системы доменных имен)	
Active Dynamic DNS (Включить динамическую DNS)	Установите этот флажок для использования динамической службы доменных имен.
Service Provider (Провайдер услуг)	В этом поле отображается имя провайдера услуг динамической DNS.
Dynamic DNS Type (Тип динамической DNS)	Выберите тип службы, предоставляемой вашим провайдером услуг динамической DNS
Host Name (Имя узла)	Введите доменное имя, назначенное интернет-центру P660HWP провайдером услуг динамической DNS. Можно ввести в это поле 2 имени, разделенных запятой («,»).
User Name (Имя пользователя)	Введите имя пользователя.
Password (Пароль)	Введите назначенный пароль.

Табл. 97 Динамическая система доменных имен (DYNDNS) (продолжение)

ПОЛЕ	ОПИСАНИЕ
Enable Wildcard Option (Включить маску)	Установите этот флажок для включения маски DYNDNS.
Enable off line option (Включить автономный режим)	Это поле доступно, только если в поле **DDNS Type (Тип DDNS)** установлено **Custom DNS (Пользовательская DNS)**. Проверьте, что провайдер услуг динамической DNS обеспечивает перенаправление трафика на указаный вами URL во время отсутствия подключения к сети.
IP Address Update Policy (Политика обновления IP-адреса)	
Use WAN IP Address (Использовать IP-адрес в глобальной сети)	Выберите эту опцию для обновления IP-адреса для имени узла(ов) на IP-адрес в глобальной сети.
Dynamic DNS server auto detect IP Address (IP-адрес автоматически обнаруженного сервера DDNS)	Выберите эту опцию, если присутствует один или несколько NAT-маршрутизаторов между P660HWP и сервером DDNS. Эта функция обеспечивает автоматическое обнаружение сервера DDNS и использование IP-адреса NAT-маршрутизатора, который имеет общедоступный IP-адрес. **Примечание: Если между устройством P660HWP и сервером DDNS присутствует прокси-сервер HTTP, сервер DDNS не сможет обнаружить соответствующий IP-адрес.**
Use WAN IP Address (Использовать IP-адрес)	Введите IP-адрес для имени узла(ов). Выберите эту опцию, если используется статический IP-адрес.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек P660HWP.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.

17

Настройка удаленного управления

В этой главе предоставлена информация для настройки удаленного управления модемом.

17.1 Удаленное управление – общая информация

При помощи удаленного управления можно определить службы/протоколы для доступа к P660HWP, интерфейс управления, а также компьютеры, с которых можно выполнять управление интернет-центром.

При установке параметров конфигурации удаленного управления, предназначенного для реализации функций управления через глобальную вычислительную сеть (WAN), необходимо также настроить правило межсетевого экрана для получения доступа.

Возможны следующие режимы удаленного управления P660HWP:

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

При выборе WAN only (Только глобальная сеть) или LAN & WAN (Локальная и глобальная сеть) необходимо также настроить правило межсетевого экрана для разрешения доступа к интернет-центру.

Для отключения удаленного управления конкретной службой выберите **Disable (Отключить)** в соответствующем поле **Access Status (Статус доступа)**.

Одновременно допускается проведение только одного сеанса удаленного управления. P660HWP автоматически завершает сеанс удаленного управления с более низким приоритетом, если запускается другой сеанс удаленного управления, имеющий более высокий приоритет. Для сеансов удаленного управления существуют следующие приоритеты:

1. Telnet
2. HTTP

17.1.1 Ограничения на удаленное управление

Удаленное управление через локальную или глобальную сеть не будет работать, если:

- Эта служба отключена в окне настройки удаленного управления.
- IP-адрес, установленный в поле **Secured Client IP (IP-адрес доверенного клиента)**, не совпадает с IP-адресом клиента. В случае несовпадения P660HWP немедленно завершает сеанс связи.
- Уже выполняется другой сеанс удаленного управления, имеющий равный или более высокий приоритет. Одновременно допускается проведение только одного сеанса удаленного управления.
- Имеется правило межсетевого экрана, блокирующее удаленное управление.

17.1.2 Удаленное управление и NAT

При включении функции NAT:

- При управлении из глобальной сети необходимо использовать IP-адрес P660HWP в глобальной сети;
- При управлении из локальной сети необходимо использовать IP-адрес P660HWP в локальной сети.

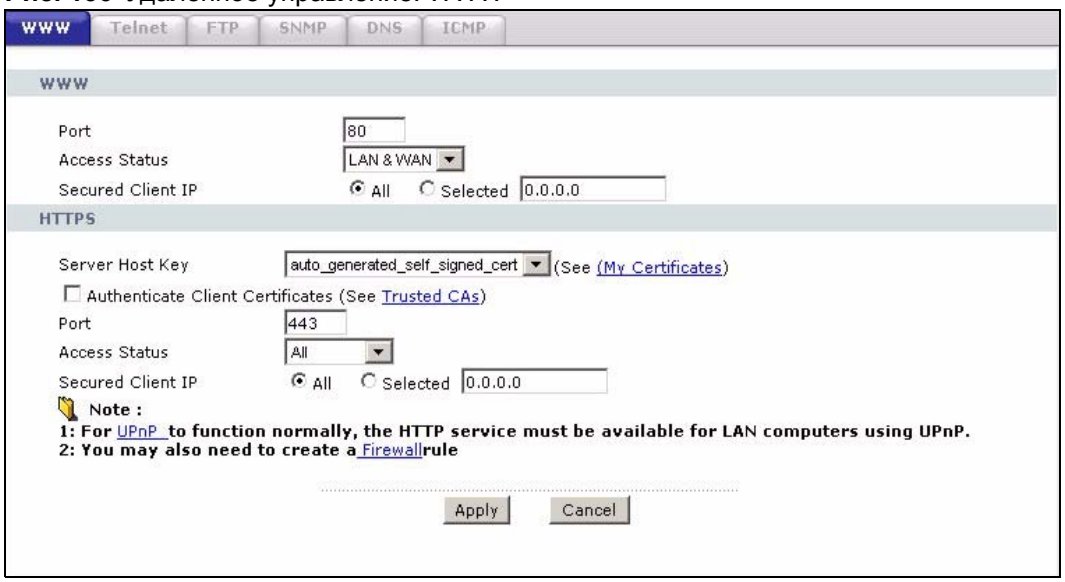
17.1.3 Время простоя системы

По умолчанию время простоя системы при выполнении сеанса управления установлено 5 минут (300 секунд). Интернет-центр P660HWP автоматически завершает сеанс управления при простое, продолжающемся более этого периода. Сеанс управления не разрывается, если в окне статистики проводится опрос системы.

17.2 WWW

Для изменения параметров подключения P660HWP к глобальной сети щелкните **Advanced (Дополнительно)** > **Remote MGMT (Удаленное управление)** для отображения окна **WWW**.

Рис. 136 Удаленное управление: WWW



В следующей таблице даны описания полей этого окна.

Табл. 98 Удаленное управление: WWW

ПОЛЕ	ОПИСАНИЕ
Port (Порт)	Если требуется, номер порта службы можно изменить, но необходимо использовать такой же номер порта при использовании этой службы для удаленного управления.
Access Status (Состояние доступа)	Выберите интерфейс(ы), через который компьютер сможет получить доступ к P660HWP при использовании этой службы.
Secured Client IP (IP-адрес защищенного клиента)	Защищенный клиент – это «доверенный» компьютер, которому разрешается подключаться к P660HWP при использовании этой службы. Выберите **All (Все)**, чтобы разрешить любому компьютеру доступ к P660HWP при использовании этой службы. Выберите **Selected (Выбранный)**, чтобы разрешить доступ к P660HWP только компьютеру с указанным IP-адресом при использовании этой службы.
HTTPS	
Server Host Key (Ключ сервера узла)	Выберите **сертификат сервера**, который устройство P660HWP будет использовать для самоидентификации. Устройство P660HWP представляет собой SSL-сервер и всегда должно идентифицировать себя для SSL-клиента (компьютера, запрашивающего HTTPS-подключение с P660HWP).
Authenticate Client Certificates (Идентифицировать сертификаты клиентов)	Выберите необязательный вариант **Authenticate Client Certificates (Идентифицировать сертификаты клиентов)**, чтобы требовать от SSL-клиентов самоидентификации для P660HWP путем отправки сертификата устройству P660HWP. Для этого SSL-клиент должен иметь подписанный центром сертификации сертификат, полученный от центра сертификации, который был загружен, как доверенный в устройство P660HWP.
Port (Порт)	Если требуется, номер порта службы можно изменить, но необходимо использовать такой же номер порта при использовании этой службы для удаленного управления.
Access Status (Состояние доступа)	Выберите интерфейс(ы), через который компьютер сможет получить доступ к P660HWP при использовании этой службы.

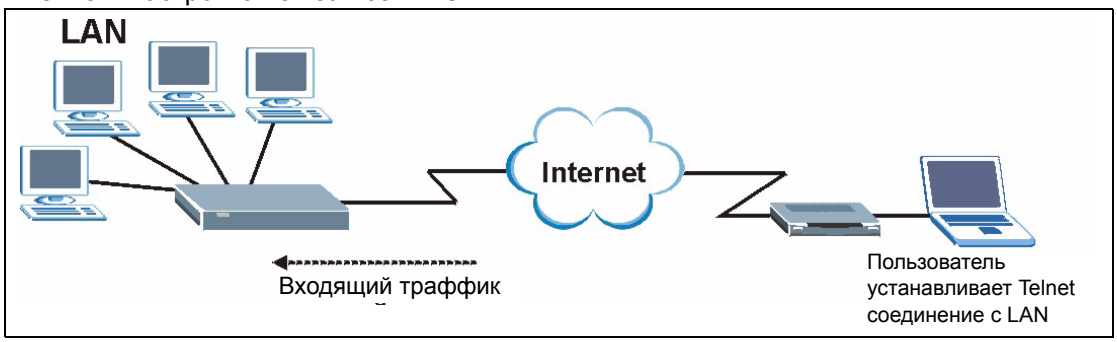
Табл. 98 Удаленное управление: WWW

ПОЛЕ	ОПИСАНИЕ
Secured Client IP (IP-адрес защищенного клиента)	Защищенный клиент – это «доверенный» компьютер, которому разрешается подключаться к P660HWP при использовании этой службы. Выберите **All (Все)**, чтобы разрешить любому компьютеру доступ к P660HWP при использовании этой службы. Выберите **Selected (Выбранный)**, чтобы разрешить доступ к P660HWP только компьютеру с указанным IP-адресом при использовании этой службы.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек P660HWP.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.

17.3 Управление с помощью Telnet

Можно настроить удаленный доступ к P660HWP через Telnet, как показано ниже. Администратор с компьютера в удаленной сети подключается к P660HWP с помощью Telnet.

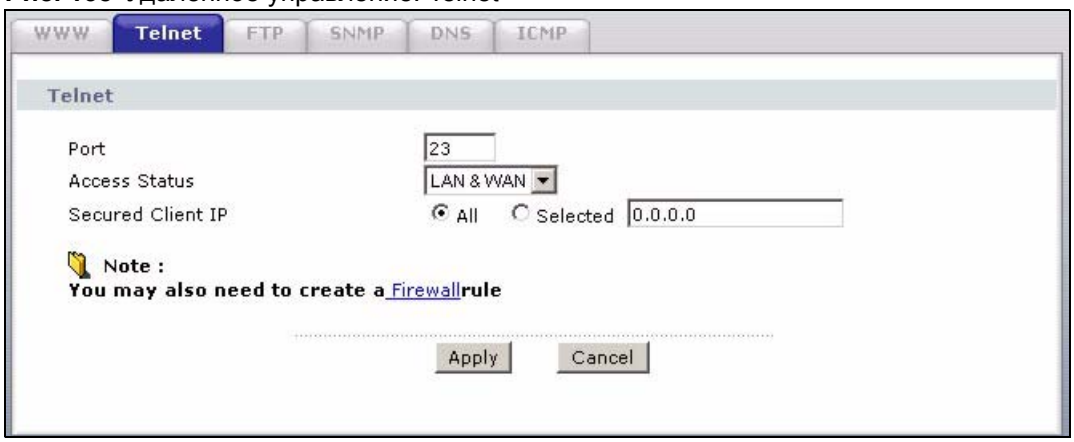
Рис. 137 Настройка Telnet в сети TCP/IP



17.4 Настройка Telnet

Щелкните **Advanced (Дополнительно)** > **Remote MGMT (Удаленное управление)** > и закладку **Telnet** для отображения окна, показанного ниже.

Рис. 138 Удаленное управление: Telnet



В следующей таблице даны описания полей этого окна.

Табл. 99 Удаленное управление: Telnet

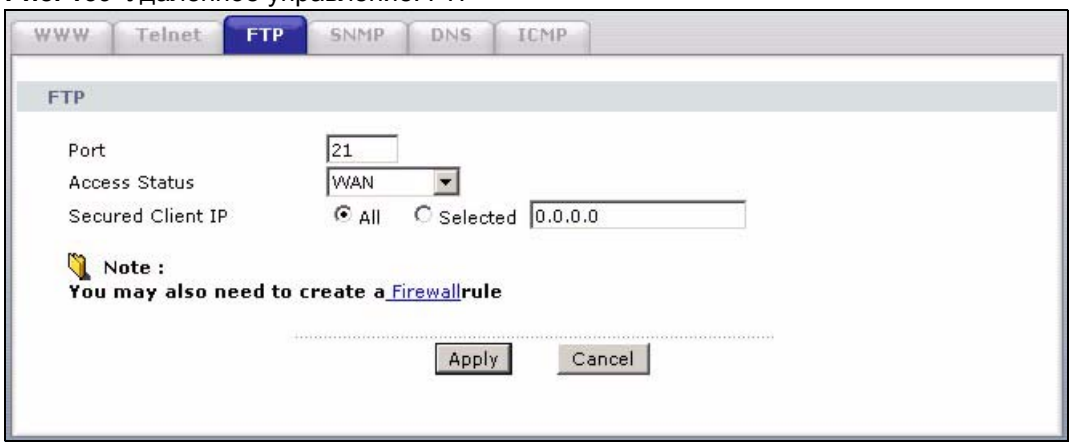
ПОЛЕ	ОПИСАНИЕ
Port (Порт)	Если требуется, номер порта службы можно изменить, но необходимо использовать такой же номер порта при использовании этой службы для удаленного управления.
Access Status (Состояние доступа)	Выберите интерфейс(ы), через который компьютер сможет получить доступ к P660HWP при использовании этой службы.
Secured Client IP (IP-адрес защищенного клиента)	Защищенный клиент – это «доверенный» компьютер, которому разрешается подключаться к P660HWP при использовании этой службы. Выберите **All (Все)**, чтобы разрешить любому компьютеру доступ к P660HWP при использовании этой службы. Выберите **Selected (Выбранный)**, чтобы разрешить доступ к P660HWP только компьютеру с указанным IP-адресом при использовании этой службы.
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить измененные настройки и выйти из этого окна.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.

17.5 Настройка FTP

С помощью FTP можно выполнять загрузку и выгрузку микропрограммы P660HWP, а также файлов конфигурации, подробнее см. главу о микропрограмме и сопровождении файлов конфигурации. Для использования данной функции на компьютере должен быть установлен FTP-клиент.

Для изменения настроек FTP в P660HWP щелкните **Advanced (Дополнительно)** > **Remote MGMT (Удаленное управление)** > и закладку **FTP**. При этом откроется показанное ниже окно.

Рис. 139 Удаленное управление: FTP



В следующей таблице даны описания полей этого окна.

Табл. 100 Удаленное управление: FTP

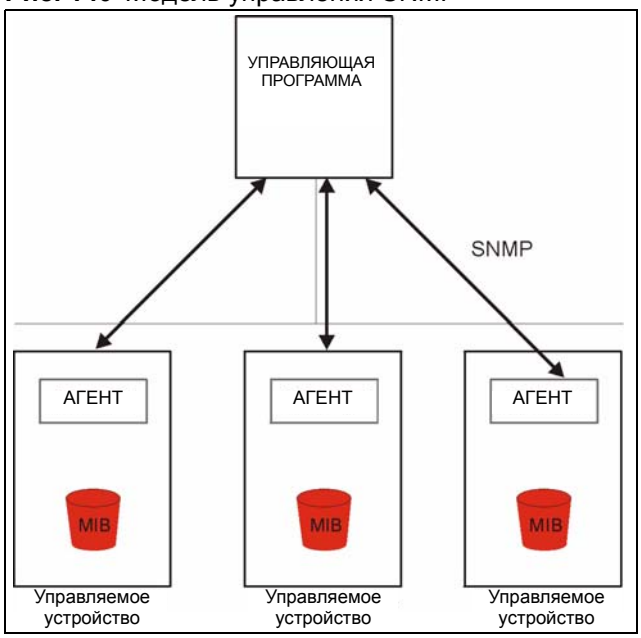
ПОЛЕ	ОПИСАНИЕ
Port (Порт)	Если требуется, номер порта службы можно изменить, но необходимо использовать такой же номер порта при использовании этой службы для удаленного управления.
Access Status (Состояние доступа)	Выберите интерфейс(ы), через который компьютер сможет получить доступ к P660HWP при использовании этой службы.
Secured Client IP (IP-адрес защищенного клиента)	Защищенный клиент – это «доверенный» компьютер, которому разрешается подключаться к P660HWP при использовании этой службы. Выберите **All (Все)**, чтобы разрешить любому компьютеру доступ к P660HWP при использовании этой службы. Выберите **Selected (Выбранный)**, чтобы разрешить доступ к P660HWP только компьютеру с указанным IP-адресом при использовании этой службы.
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить измененные настройки и выйти из этого окна.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.

17.6 Протокол SNMP

Простой протокол управления сетью (SNMP – Simple Network Management Protocol) используется для осуществления обмена управляющей информацией между сетевыми устройствами. SNMP входит в состав стека протоколов TCP/IP. Интернет-центр P660HWP поддерживает функцию агента SNMP, что позволяет выполнять управление и мониторинг P660HWP с управляющей станции по сети. P660HWP поддерживает протокол SNMP версии один (SNMPv1) и версии два (SNMPv2). На следующем рисунке показана модель управления по протоколу SNMP.

Протокол SNMP доступен только при настроенном TCP/IP.

Рис. 140 Модель управления SNMP



Сети под управлением протокола SNMP состоят из двух основных компонентов: агентов и управляющей программы.

Агент представляет собой модуль программы управления, находящийся в управляемом устройстве (P660HWP). Агент производит преобразование информации локального управления от управляемого устройства в форму, совместимую с SNMP. Управляющая программа – это консоль управления, с помощью которой сетевые администраторы осуществляют функции управления сетью. Через консоль происходит запуск приложений, предназначенных для контроля и мониторинга управляемых устройств.

Управляемые устройства содержат объектные переменные/управляемые объекты, которые определяют каждую порцию информации, собираемой об этих устройствах. В качестве примеров переменных можно назвать число полученных пакетов, статус порта узла и т. д. База управляющей информации (MIB) – это совокупность управляемых объектов. Протокол SNMP позволяет управляющей программе и агентам взаимодействовать друг с другом с целью доступа к этим объектам.

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

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

17.6.1 Поддерживаемые базы управляющей информации

P660HWP поддерживает MIB II (Management Information Base – База управляющей информации), параметры которой описываются в комментариях RFC-1213 и RFC-1215. Базы управляющей информации позволяют сетевым администраторам собирать статистические данные и контролировать состояние и производительность сети.

17.6.2 Прерывания SNMP

P660HWP посылает прерывания на управляющую станцию SNMP, когда происходит какое-либо из следующих событий:

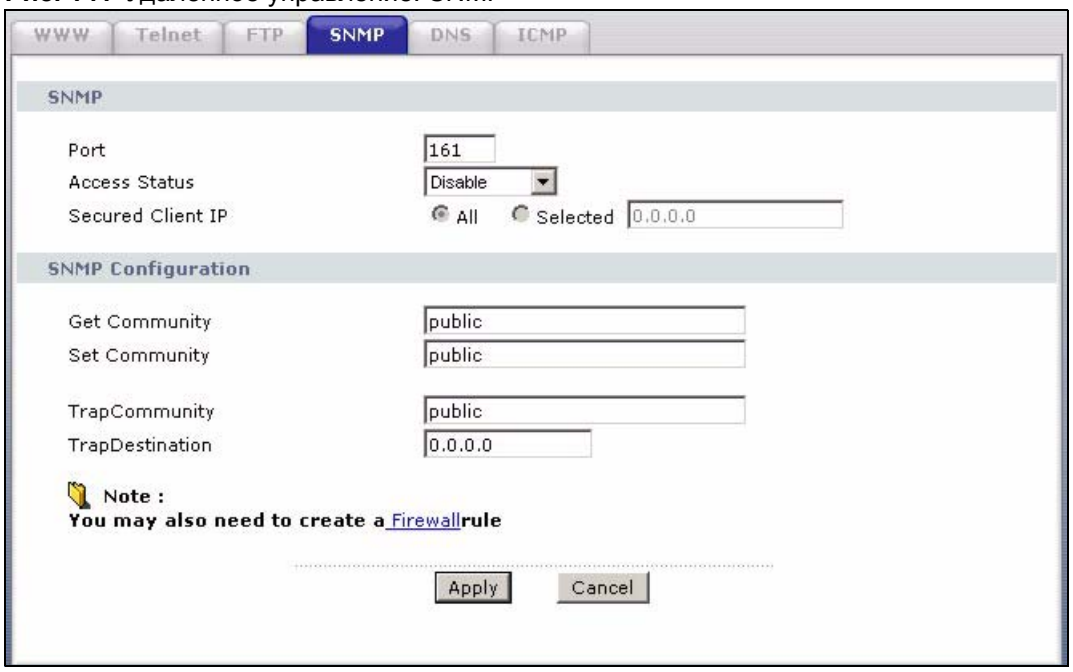
Табл. 101 Прерывания SNMP

НОМЕР ПРЕРЫВАНИЯ	ИМЯ ПРЕРЫВАНИЯ	ОПИСАНИЕ
0	coldStart (описывается в *RFC-1215*)	Прерывание посылается после загрузки (при включении питания).
1	warmStart (описывается в *RFC-1215*)	Прерывание посылается после загрузки (программная перезагрузка).
6	whyReboot (описывается в MIB ZYXEL)	Прерывание посылается с указанием кода причины перезапуска перед перезапуском, если система собирается выполнить перезапуск («горячий» запуск).
6a	Для преднамеренной перезагрузки:	Прерывание посылается с сообщением «System reboot by user!» (перезагрузка системы пользователем), когда перезагрузка производится намеренно (например, загрузка новых файлов, команда «sys reboot» и т. д.).
6b	Для неисправимой ошибки:	Прерывание посылается с кодом критической ошибки, если система перезагружается из-за возникновения критических ошибок.

17.6.3 Настройка SNMP

Для изменения настроек SNMP в P660HWP щелкните **Advanced (Дополнительно) > Remote MGMT (Удаленное управление) >** и закладку **SNMP**. При этом откроется показанное ниже окно.

Рис. 141 Удаленное управление: SNMP



В следующей таблице даны описания полей этого окна.

Табл. 102 Удаленное управление: SNMP

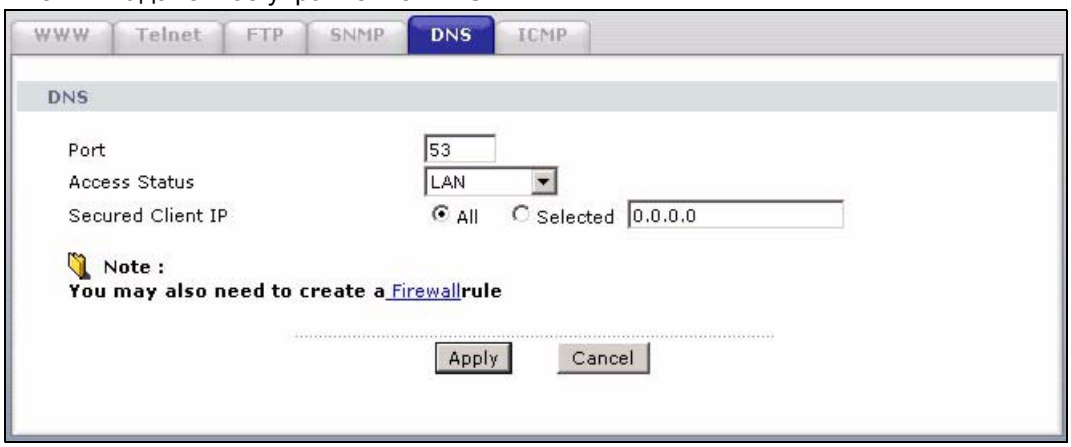
ПОЛЕ	ОПИСАНИЕ
SNMP	
Port (Порт)	Если требуется, номер порта службы можно изменить, но необходимо использовать такой же номер порта при использовании этой службы для удаленного управления.
Access Status (Состояние доступа)	Выберите интерфейс(ы), через который компьютер сможет получить доступ к P660HWP при использовании этой службы.
Secured Client IP (IP-адрес защищенного клиента)	Защищенный клиент – это «доверенный» компьютер, которому разрешается подключаться к P660HWP при использовании этой службы. Выберите **All (Все)**, чтобы разрешить любому компьютеру доступ к P660HWP при использовании этой службы. Выберите **Selected (Выбранный)**, чтобы разрешить доступ к P660HWP только компьютеру с указанным IP-адресом при использовании этой службы.
SNMP Configuration (Настройка SNMP)	
Get Community (Пароль «Get»)	Введите пароль «Get», который является паролем для входящих запросов Get и GetNext от управляющей станции. По умолчанию установлен пароль «public» и разрешаются все запросы.
Set Community (Пароль «Set»)	Введите пароль «Set», который является паролем для входящих запросов Set от управляющей станции. По умолчанию установлен пароль «public» и разрешаются все запросы.
TrapCommunity (Пароль «Trap»)	Введите пароль «Trap», передаваемый с каждым прерыванием на управляющее устройство SNMP. По умолчанию установлен пароль «public» и разрешаются все запросы.
TrapDestination (Адресат Trap)	Введите IP-адрес устройства, на которое будут посылаться прерывания SNMP.
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить измененные настройки и выйти из этого окна.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.

17.7 Настройка DNS

DNS (Система доменных имен) предназначена для отображения доменного имени на соответствующий ему IP-адрес и наоборот. Для получения дополнительной информации см. главу о локальных сетях.

Для изменения настроек DNS в P660HWP щелкните **Advanced (Дополнительно) > Remote MGMT (Удаленное управление) > DNS**. При этом откроется показанное ниже окно. Это окно используется для установки IP-адреса, с которого P660HWP будет принимать запросы DNS, а также интерфейса, через который P660HWP будет отправлять параметры DNS на эти запросы.

Рис. 142 Удаленное управление: DNS



В следующей таблице даны описания полей этого окна.

Табл. 103 Удаленное управление: DNS

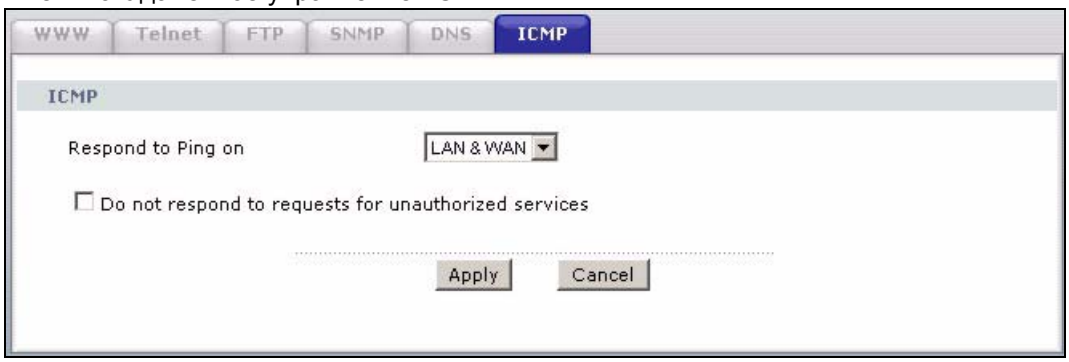
ПОЛЕ	ОПИСАНИЕ
Port (Порт)	Номер порта службы DNS – 53.
Access Status (Состояние доступа)	Выберите интерфейс(ы), через который компьютер сможет посылать P660HWP запросы DNS.
Secured Client IP (IP-адрес защищенного клиента)	Защищенный клиент – это «доверенный» компьютер, которому разрешается посылать P660HWP запросы DNS. Выберите **All (Все)**, чтобы разрешить любому компьютеру посылать P660HWP запросы DNS. Выберите **Selected (Выбранный)**, чтобы разрешить P660HWP посылать запросы DNS только компьютеру с указанным IP-адресом.
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить измененные настройки и выйти из этого окна.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.

17.8 Настройка ICMP

Для изменения настроек безопасности в P660HWP щелкните **Advanced (Дополнительно) > Remote MGMT (Удаленное управление) > ICMP**. При этом откроется показанное ниже окно.

Если внешний пользователь попытается прозондировать неподдерживаемый порт P660HWP, ему будет автоматически отправлен ответный пакет ICMP. Это позволяет внешнему пользователю узнать о существовании интернет-центра P660HWP. Также P660HWP поддерживает блокирование эхо-тестирования без отправки ответного пакета ICMP. Это позволяет скрыть существование P660HWP от посторонних лиц при попытке эхо-тестирования неподдерживаемого порта.

Рис. 143 Удаленное управление: ICMP



В следующей таблице даны описания полей этого окна.

Табл. 104 Удаленное управление: ICMP

ПОЛЕ	ОПИСАНИЕ
ICMP	Протокол управляющих сообщений в сети Интернет (Internet Control Message Protocol) является протоколом управляющих сообщений и сообщений об ошибках между основным узлом и шлюзом в Интернет. ICMP использует дейтаграммы протокола Интернета (IP), но сообщения обрабатываются программным обеспечением TCP/IP, и невидимы для пользователей приложений.
Respond to PING on (Отвечать на PING-запросы)	Интернет-центр P660HWP не отвечает на входящие запросы эхо-тестирования, если в поле **Disable (Отключить)** установлен флажок. Выберите **LAN** для ответа на входящие Ping-запросы из локальной сети.Выберите **WAN** для ответа на входящие Ping-запросы по глобальной сети. В противном случае выберите **LAN & WAN** для ответа на Ping-запросы как по локальной, так и глобальной сети.
Do not respond to requests for unauthorized services (Не отвечать на запросы для запрещенных служб).	Установите флажок, чтобы предотвратить обнаружение хакерами интернет-центра P660HWP посредством эхо-тестирования неиспользуемых портов. Если флажок установлен, P660HWP не будет отвечать на запросы на неиспользуемые порты. Таким образом, неиспользуемые порты и интернет-центр P660HWP остаются невидимыми. По умолчанию флажок снят и P660HWP посылает пакет ICMP «Port Unreachable» (Порт недоступен) в ответ на зондирование неиспользуемых портов UDP, а в ответ на зондирование неиспользуемых портов TCP – пакет «TCP Reset» (Сброс TCP). Следует отметить, что прежде чем зондирующие пакеты достигнут механизма блокирования эхо-тестирования, они сначала должны пройти через межсетевой экран P660HWP. Следовательно, если механизм межсетевого экрана блокирует зондирующий пакет, реакция P660HWP производится на основе политики межсетевого экрана: в ответ на заблокированный пакет TCP посылается пакет «сброс TCP», на заблокированный пакет UDP – пакет ICMP «порт недоступен», или пакеты просто сбрасываются без отправки ответных пакетов.
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить измененные настройки и выйти из этого окна.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.

17.9 TR-069

TR-069 – это стандарт форума DSL, который определяет способы управления оборудованием, расположенным на территории клиента (CPE: Customer Premise Equipment), например, устройством P660HWP, через глобальную сеть с помощью сервера автоматической настройки (ACS: Auto Configuration Server), например ZyXEL CNM. Стандарт TR-069 описывает передачу RPC (Remote Procedure Call – вызовов удаленных процедур) между ACS и устройством клиента. RPC передаются в формате XML (Extensible Markup Language – расширяемый язык разметки) через HTTP- или HTTPS-подключение.

Администратор может использовать доступ CNM для удаленной настройки устройства ZyXEL, изменения параметров, выполнения обновления микропрограммы, а также мониторинга и диагностики устройства ZyXEL. Для этого необходимо включить управление устройством через CNM и установить IP-адрес или доменное имя CNM, а также имя пользователя и пароль.

Для настройки управления P660HWP через CNM выполните процедуру, представленную далее. Информацию о структуре команд и запуске CLI (Command Line Interface – Интерфейс командной строки) в P660HWP см. в приложении об интерпретаторе команд.

В этом примере «a.b.c.d» – это IP-адрес CNM. Этот адрес необходимо изменить, чтобы установить фактический IP-адрес или доменное имя управляющего сервера. Подробное описание команд см. Табл. 105 на с. 276.

Рис. 144 Включение 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
```

В следующей таблице представлено описание команд TR-069.

Табл. 105 Команды TR-069

КОРНЕВОЙ КЛАСС	КОМАНДА ИЛИ ПОДКАТАЛОГ	КОМАНДА	ОПИСАНИЕ
wan	tr069		Все команды TR-069 должны начинаться с «wan tr069».
		load	Запуск настройки TR-069 в P660HWP.

Табл. 105 Команды TR-069

КОРНЕВОЙ КЛАСС	КОМАНДА ИЛИ ПОДКАТАЛОГ	КОМАНДА	ОПИСАНИЕ
		`active [0:no/ 1:yes]`	Включить/отключить TR-069.
		`acsUrl <URL>`	Установка IP-адреса или доменного имени сервера CNM.
		`username [maxlength:15]`	Имя пользователя, используемое для аутентификации устройства при подключении к CNM. Это имя пользователя устанавливается на сервере и должно быть предоставлено администратором CNM.
		`password [maxlength:15]`	Пароль, используемый для аутентификации устройства при подключении к CNM. Этот пароль устанавливается на сервере и должен быть предоставлен администратором CNM.
		`periodicEnable [0:Disable/ 1:Enable]`	Включение и отключение периодической отправки информации на CNM. Рекомендуется установить значение `1` для этого параметра, чтобы P660HWP посылал информацию на CNM.
		`informInterval [sec]`	Время в секундах, через которое устройство ДОЛЖНО производить попытку подключения к CNM для отправки информации и проверки обновлений конфигурации. Введите значение от 30 до 2147483647.
		`save`	Сохранение настроек TR-069 в P660HWP.

18

Универсальная функция Plug and Play (UPnP)

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

18.1 Описание универсальной функции Plug and Play

Универсальная функция Plug and Play (UPnP) – это распространенный открытый сетевой стандарт, использующий TCP/IP для обеспечения взаимодействия между устройствами в одноранговой сети. Устройство UPnP может динамически присоединяться к сети, получать IP-адрес, сообщать о своих функциях и собирать информацию о других устройствах сети. Также устройство может беспрепятственно и автоматически покидать сеть, если оно больше не используется.

Инструкции по настройке см. Разд. 18.2.1 на с. 280.

18.1.1 Как узнать, используется ли UPnP?

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

18.1.2 NAT Traversal

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

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

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

Для получения более подробной информации о NAT см. главу по трансляции сетевых адресов.

18.1.3 Предупреждения по использованию UPnP

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

Когда устройство UPnP подключается к сети, оно объявляет о своем присутствии с помощью многоадресной рассылки сообщения. По причине безопасности P660HWP разрешает многоадресную рассылку сообщений только по локальной сети.

Все устройства с включенной функцией UPnP могут свободно взаимодействовать друг с другом без дополнительной настройки. Отключите функцию UPnP, если вы не собираетесь ее использовать.

Чтобы функция UPnP работала, необходимо включить службу IIS (Internet Information Services – информационные службы Интернет) на Web-сервере Windows.

18.2 UPnP и ZyXEL

Корпорация ZyXEL получила сертификат от организации Universal Plug and Play Forum UPnP™ Implementers Corp. (UIC). Реализация UPnP ZyXEL поддерживает функцию IGD 1.0 (Internet Gateway Device – шлюзовое устройство подключения к Интернету).

Примеры установки и использования UPnP см. в следующих разделах.

18.2.1 Настройка UPnP

Щелкните **Advanced (Дополнительно) > UPnP** для отображения окна, как показанного ниже.

Более подробную информацию см. Разд. 18.1 на с. 279.

Рис. 145 Настройка UPnP

В следующей таблице даны описания полей этого окна.

Табл. 106 Настройка UPnP

ПОЛЕ	ОПИСАНИЕ
Active the Universal Plug and Play (UPnP) Feature (Включить функцию UPnP)	Установите флажок для включения UPnP. Помните, что любой может с помощью приложения UPnP открыть окно регистрации Web-конфигуратора без ввода IP-адреса интернет-центра P660HWP (хотя для доступа к Web-конфигуратору необходимо ввести пароль).
Allow users to make configuration changes through UPnP (Разрешить пользователям вносить изменения в конфигурацию через UPnP)	Установите здесь флажок, чтобы разрешить приложениям с включенной функцией UPnP автоматически выполнять настройку P660HWP для того, чтобы они могли взаимодействовать через P660HWP. Например, с помощью обхода NAT приложения UPnP автоматически резервируют порт переадресации NAT, чтобы взаимодействовать с другим устройством UPnP. Это устраняет необходимость ручной настройки переадресации портов для приложений UPnP.
Allow UPnP to pass through Firewall (Разрешить прохождение UPnP через межсетевой экран)	Установите здесь флажок, если нужно разрешить прохождение трафика от приложений, использующих UPnP, через межсетевой экран. Снимите флажок, если межсетевой экран должен блокировать все пакеты приложений на базе UPnP (например, пакеты MSN).
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек P660HWP.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)** для возврата к предыдущим сохраненным настройкам.

18.3 Пример установки UPnP в Windows

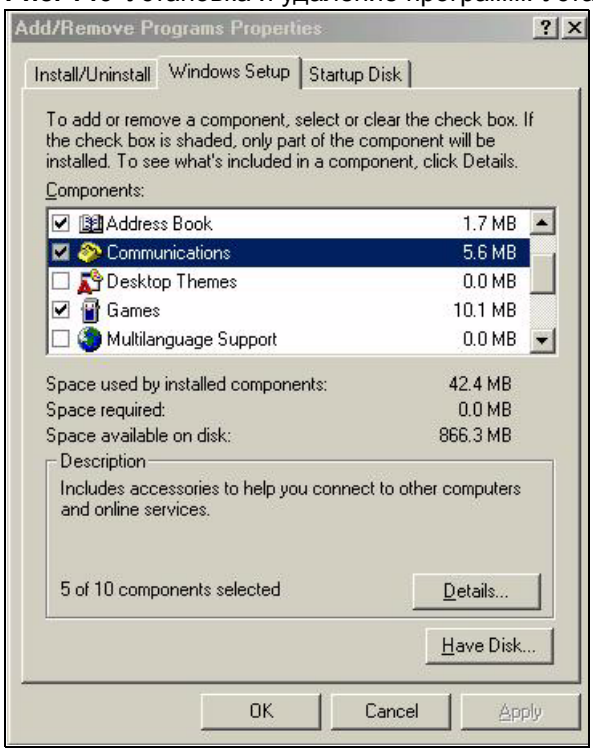
В данном разделе описывается установка UPnP в Windows Me и Windows XP.

18.3.1 Установка UPnP в Windows Me

Выполните следующие действия для установки UPnP в Windows Me.

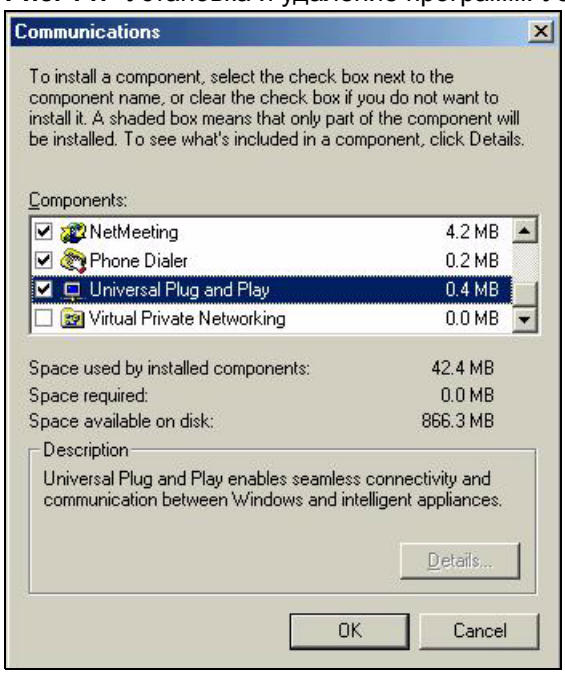
1. Нажмите **Start (Пуск)** и выберите пункт **Control Panel (Панель управления)**. Дважды щелкните **Add/Remove Programs (Установка и удаление программ)**.
2. Выберите закладку **Windows Setup (Установка Windows)** и выберите **Communication (Связь)** в поле **Components (Компоненты)**. Нажмите **Details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

Рис. 146 Установка и удаление программ: Установка Windows: Связь



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

Рис. 147 Установка и удаление программ: Установка Windows: Связь: Компоненты



4 Нажмите **OK** для возврата в окно **Add/Remove Programs Properties (Свойства: Установка и удаление программ)** и нажмите **Next (Далее)**.

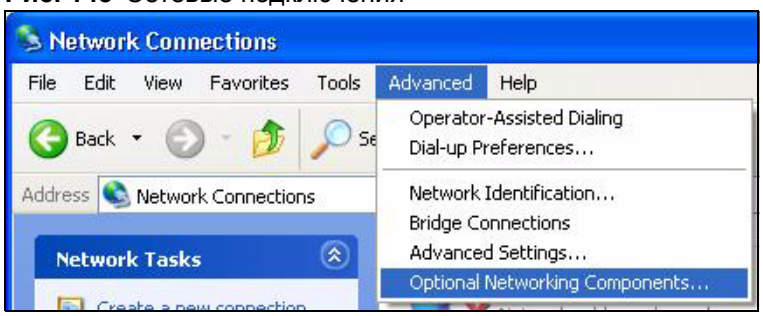
5 При появлении запроса перезагрузите компьютер.

18.3.2 Установка UPnP в Windows XP

Выполните следующие действия для установки UPnP в Windows XP.

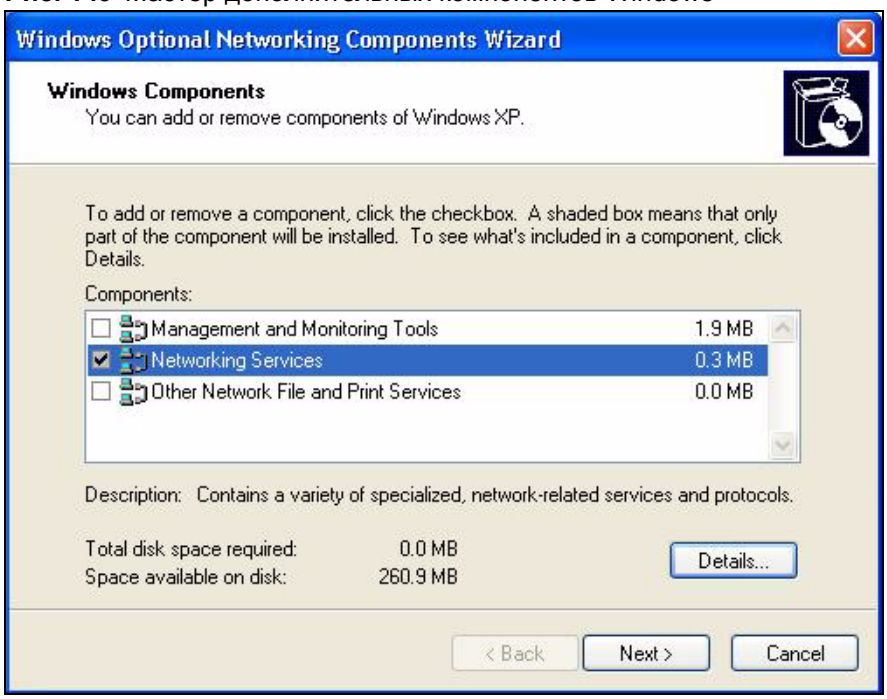
1. Нажмите **Start (Пуск)** и выберите пункт **Control Panel (Панель управления)**.
2. Дважды щелкните значок **Network Connections (Сетевые подключения)**.
3. В окне **Network Connections (Сетевые подключения)** выберите **Advanced (Дополнительно)** в главном меню и выберите **Optional Networking Components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

Рис. 148 Сетевые подключения



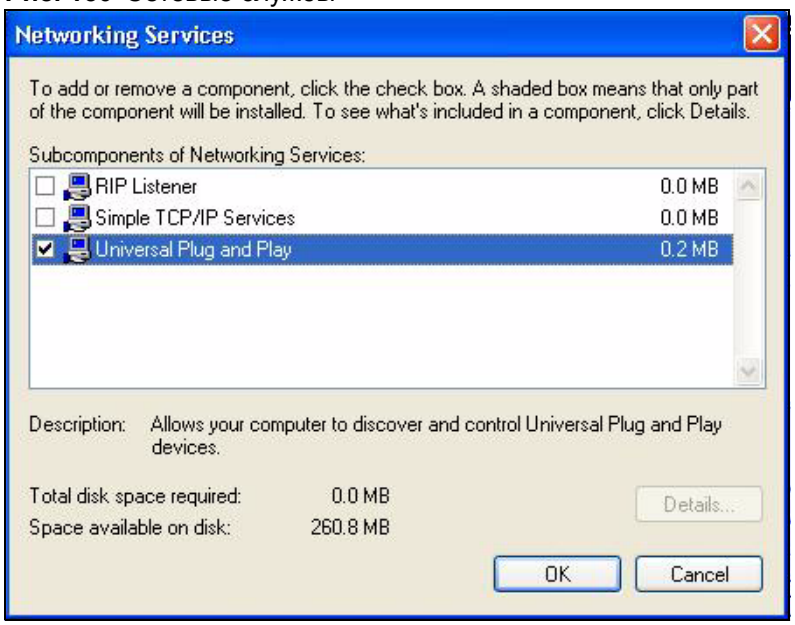
4. Появится окно **Windows Optional Networking Components Wizard (Мастер установки дополнительных сетевых компонентов Windows)**. Выберите **Networking Services (Сетевые службы)** в поле **Components (Компоненты)** и нажмите **Details (Состав)**.

Рис. 149 Мастер дополнительных компонентов Windows



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

Рис. 150 Сетевые службы



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

18.4 Пример использования UPnP в Windows XP

В этом разделе описывается использование функции UPnP в Windows XP. Функция UPnP уже должна быть установлена в Windows XP и включена в интернет-центре P660HWP.

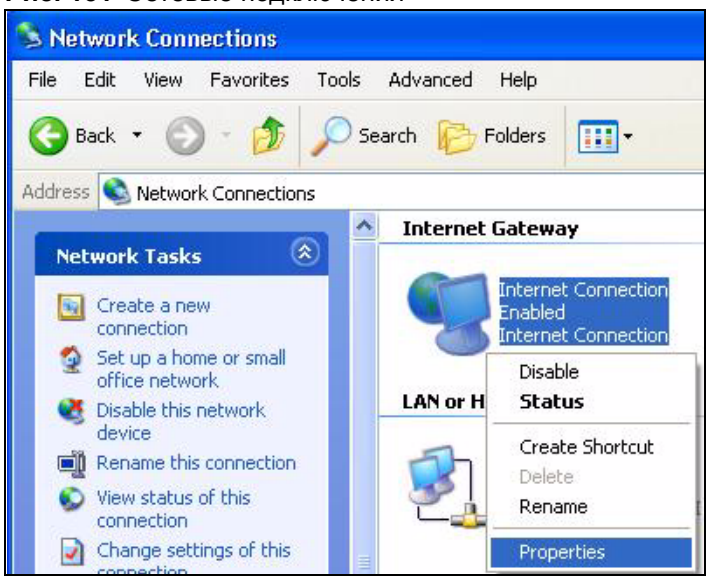
Убедитесь, что компьютер подключен к порту LAN интернет-центра P660HWP. Включите компьютер и P660HWP.

18.4.1 Автоматическое обнаружение сетевого устройства UPnP

1 Нажмите **Start (Пуск)** и выберите пункт **Control Panel (Панель управления)**. Дважды щелкните значок **Network Connections (Сетевые подключения)**. В разделе **Internet Gateway (Шлюз Интернет)** появится значок.

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

Рис. 151 Сетевые подключения



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

Рис. 152 Свойства подключения к Интернет

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

Рис. 153 Свойства подключения к Интернет: Дополнительные настройки

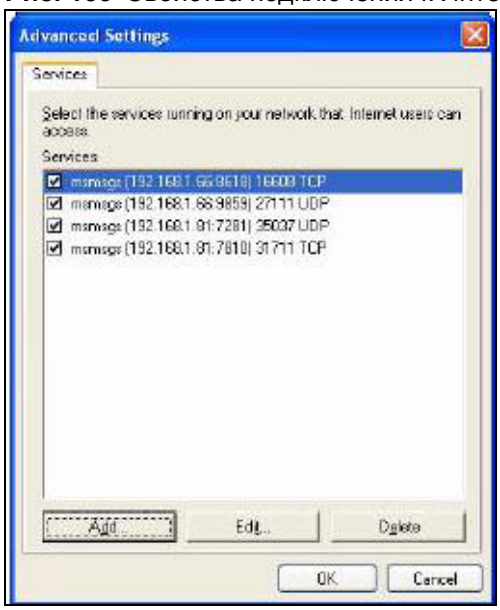
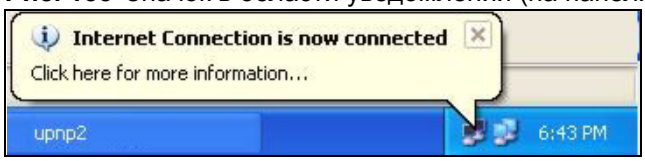


Рис. 154 Свойства подключения к Интернет: Дополнительные настройки: Добавить

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

5 Выберите **Show icon in notification area when connected (При подключении вывести значок в области уведомлений)** и нажмите **OK**. На панели задач появится значок.

Рис. 155 Значок в области уведомлений (на панели задач)



6 Дважды щелкните значок для отображения текущего состояния подключения к Интернету.

Рис. 156 Состояние подключения к Интернет

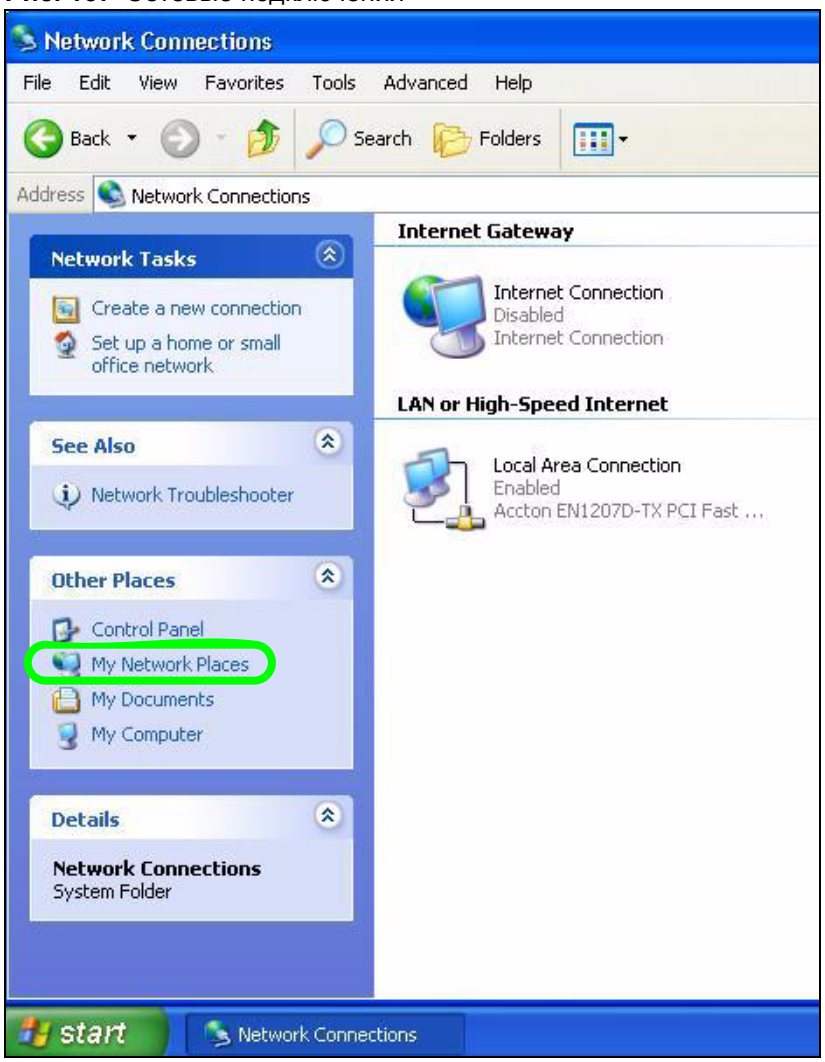
18.4.2 Простой доступ к Web-конфигуратору

С помощью UPnP вы можете получить доступ к программе настройки P660HWP на основе Web технологии без предварительного выяснения IP-адреса P660HWP. Это может оказаться полезным, если вы не знаете IP-адрес P660HWP.

Выполните следующие действия для доступа к Web-конфигуратору.

1 Нажмите **Start (Пуск)**, **Control Panel (Панель управления)**.
2 Дважды щелкните значок **Network Connections (Сетевые подключения)**.
3 Выберите **My Network Places (Сетевое окружение)** в разделе **Other Places (Другие места)**.

Рис. 157 Сетевые подключения



4 В разделе **Local Network (Локальная сеть)** для каждого UPnP-совместимого устройства отображается значок с описанием.

5 Щелкните правой кнопкой мыши на иконке P660HWP и выберите **Invoke (Запустить)**. Появится окно регистрации Web-конфигуратора.

Рис. 158 Сетевые подключения: Сетевое окружение

6 Щелкните правой кнопкой мыши на иконке P660HWP и выберите **Properties (Свойства)**. Появится окно свойств с основной информацией об устройстве P660HWP.

Рис. 159 Пример – Сетевые подключения: Сетевое окружение: Свойства

Часть VI
Обслуживание, поиск и устранение неисправностей

19

Система

Это окно используется для установки времени и даты в интернет-центре P660HWP.

19.1 Настройка общих параметров

19.1.1 Настройка общих параметров и ввод системного имени

Окно **General Setup (Общие параметры)** содержит административную и общесистемную информацию. **Системное имя** используется для идентификации. Однако, поскольку некоторые Интернет-провайдеры проверяют это имя, следует вводить имя вашего компьютера.

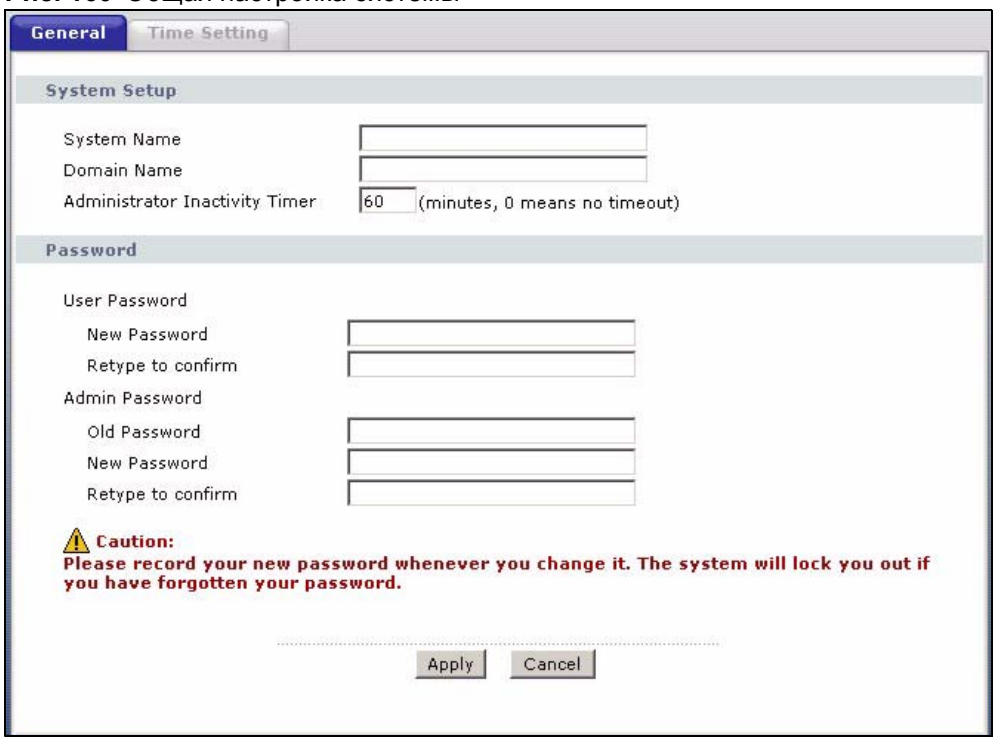
- В Windows 95/98 нажмите кнопку **Start (Пуск), Settings (Настройка), Control Panel (Панель управления), Network (Сеть и удаленный доступ к сети)**. Щелкните по закладке **Identification (Идентификация)**, запишите имя, установленное в поле **Computer Name (Имя компьютера)**, и введите его в качестве системного имени.
- В Windows 2000 щелкните **Start (Пуск), Settings (Настройка), Control Panel (Панель управления)** и дважды щелкните **System (Система)**. Выберите закладку **Network Identification (Сетевая идентификация)**, а затем щелкните по кнопке **Properties (Свойства)**. Запишите имя, установленное в поле **Computer name (Имя компьютера)**, и введите его в качестве системного имени.
- В Windows XP нажмите кнопку **Start (Пуск), My Computer (Мой компьютер), View system information (Просмотр сведений о системе)**, а затем выберите закладку **Computer Name (Имя компьютера)**. Запишите имя, установленное в поле **Full Computer Name (Полное имя компьютера)**, и введите его в качестве системного имени P660HWP.

19.1.2 Настройка общих параметров

Запись **Domain Name (Доменное имя)** передается клиентам DHCP в локальной сети. Если вы оставите это поле незаполненным, будет использоваться имя домена, полученное протоколом DHCP от Интернет-провайдера. В отличие от имени узла (системное имя), которое вы должны вводить на каждом отдельном компьютере, доменное имя может назначаться интернет-центром P660HWP с помощью DHCP.

Щелкните **Maintenance (Сопровождение) > System (Система)** для отображения окна **General (Общие параметры)**.

Рис. 160 Общая настройка системы



В следующей таблице даны описания полей этого окна.

Табл. 107 Общая настройка системы

ПОЛЕ	ОПИСАНИЕ
General Setup (Настройка общих параметров)	
System Name (Системное имя)	Введите имя системы, которое будет использоваться для идентификации. В это поле рекомендуется ввести имя вашего компьютера (Computer name). Имя может включать до 30 алфавитно-цифровых символов. Использование пробелов не допускается, но допускается использование тире «-» и символа подчеркивания «_».
Domain Name (Доменное имя)	Введите в это поле доменное имя (если оно известно). Если это поле оставлено пустым, Интернет-провайдер может назначить доменное имя с помощью DHCP. Введенное доменное имя обладает более высоким приоритетом, чем доменное имя, назначенное Интернет-провайдером.
Administrator Inactivity Timer (Таймер простоя сеанса администрирования)	Введите время простоя в минутах, по истечении которого сеанс управления будет завершен. Значение по умолчанию 5 минут. Чтобы подключиться после завершения сеанса, необходимо снова зарегистрироваться и ввести пароль. Очень долгое время простоя увеличивает риск нарушения безопасности сети. Значение 0 означает, что сеанс управления не разрывается, независимо от времени простоя (не рекомендуется).
Password (Пароль)	
User Password (Пароль пользователя)	При регистрации с паролем пользователя можно выполнять только просмотр статуса P660HWP. По умолчанию установлен пароль пользователя **user**.

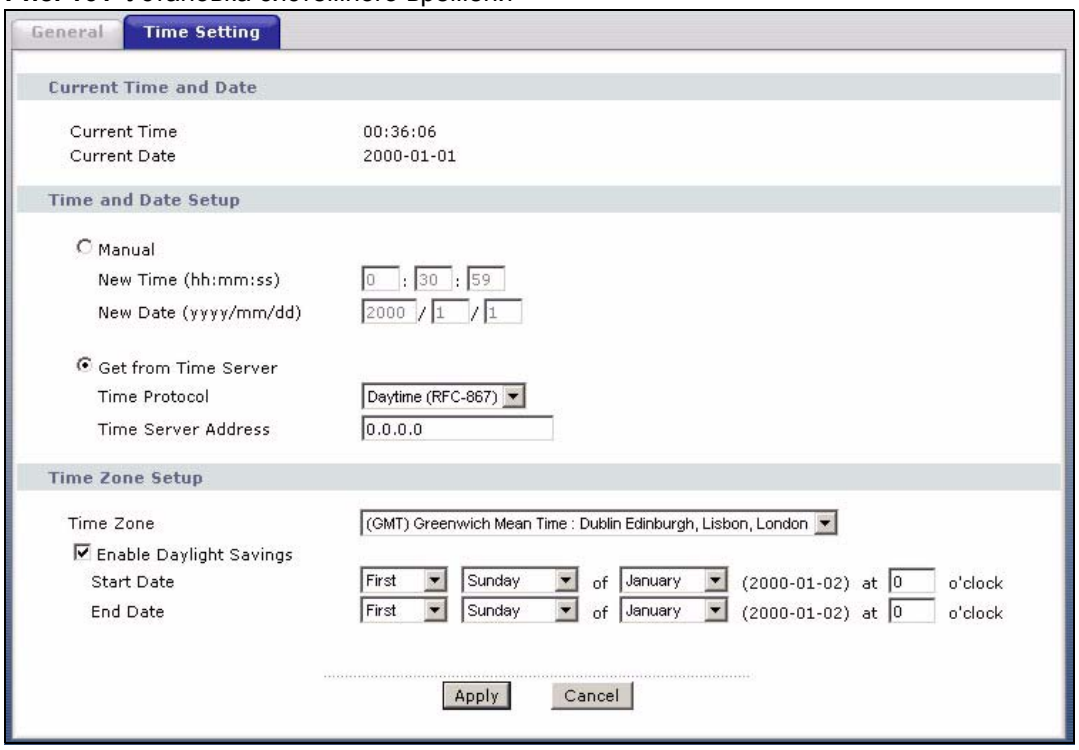
Табл. 107 Общая настройка системы

ПОЛЕ	ОПИСАНИЕ
New Password (Новый пароль)	Введите новый системный пароль длиной до 30 символов. При вводе пароля вводимые символы заменяются на экране на символ *. После изменения пароля для доступа к P660HWP необходимо использовать новый пароль.
Retype to Confirm (Повторный ввод для подтверждения)	Введите новый пароль еще раз для подтверждения.
Admin Password (Пароль администратора)	При регистрации с паролем администратора, кроме выполнения настроек с помощью Мастера, также можно выполнять настройку расширенных возможностей P660HWP.
Old Password (Старый пароль)	Введите пароль администратора по умолчанию (**1234**) или существующий пароль, который используется для доступа к системе при настройке расширенных возможностей.
New Password (Новый пароль)	Введите новый системный пароль длиной до 30 символов. При вводе пароля вводимые символы заменяются на экране на символ *. После изменения пароля для доступа к P660HWP необходимо использовать новый пароль.
Retype to Confirm (Повторный ввод для подтверждения)	Введите новый пароль еще раз для подтверждения.
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек P660HWP.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.

19.2 Установка времени

Для изменения даты и времени в P660HWP щелкните **Maintenance (Сопровождение) > System (Система) > Time Setting (Установка времени)**. При этом откроется показанное ниже окно. Это окно используется для установки времени в интернет-центре P660HWP в соответствии с вашим часовым поясом.

Рис. 161 Установка системного времени



В следующей таблице даны описания полей этого окна.

Табл. 108 Установка системного времени

ПОЛЕ	ОПИСАНИЕ
Current Time and Date (Текущее время и дата)	
Current Time (Текущее время)	В этом поле отображается время в устройстве P660HWP. При каждой загрузке этой страницы интернет-центр P660HWP синхронизирует время с сервером времени.
Current Date (Текущая дата)	В этом поле отображается дата в интернет-центре P660HWP. При каждой загрузке этой страницы интернет-центр P660HWP синхронизирует дату с сервером времени.
Time and Date Setup (Установка времени и даты)	
Manual (Вручную)	Выберите эту опцию для установки времени и даты вручную. При одновременной установке новых параметров даты и времени, часового пояса и перехода на летнее время, новые дата и время имеют приоритет, и параметры «Time Zone» (Часовой пояс) и «Daylight Saving» (Переход на летнее время) не влияют на них.
New Time (Новое время) (hh:mm:ss) (чч:мм:сс)	В этом поле отображается время, последний раз обновленное с помощью сервера времени или последний раз установленное вручную. При выборе в разделе **Time and Date Setup (Установка времени и даты)** режима **Manual (Ручной)** введите в это поле новое время и щелкните по кнопке **Apply (Применить)**.

Табл. 108 Установка системного времени (продолжение)

ПОЛЕ	ОПИСАНИЕ
New Date (Новая дата) (yyyy/mm/dd) (гггг/мм/дд)	В этом поле отображается дата, последний раз обновленная с помощью сервера времени или последний раз установленная вручную. При выборе в разделе **Time and Date Setup (Установка времени и даты)** режима **Manual (Ручной)**, введите в это поле новую дату и нажмите кнопку **Apply (Применить)**.
Get from Time Server (Получить от сервера времени)	Выберите эту опцию, чтобы P660HWP синхронизировал время и дату с сервером, указанным в поле ниже.
Time Protocol (Протокол времени)	Выберите сервисный протокол, который используется сервером времени. Не все серверы времени поддерживают любые протоколы, поэтому следует проконсультироваться с Интернет-провайдером/сетевым администратором, или попытаться определить работающий протокол методом проб и ошибок. Основные различия между ними заключаются в формате представления времени. Формат **Daytime (RFC 867)** содержит день/месяц/год/часовой пояс сервера. Формат **Time (RFC 868)** представляет собой 4-байтовое целое число, означающее общее количество секунд, истекшее с 00:00:00, 01.01.1970. По умолчанию формат **NTP (RFC 1305)** аналогичен формату **Time (RFC 868)**.
Time Server Address (Адрес сервера времени)	Введите IP-адрес или URL сервера времени длиной до 20 символов латинского алавита. Если вы не обладаете этой информацией, следует обратиться к Интернет-провайдеру/сетевому администратору.
Time Zone Setup (Установка часового пояса)	
Time Zone (Часовой пояс)	Выберите часовой пояс вашего местонахождения. Это поле устанавливает разницу между вашим часовым поясом и временем по Гринвичу (Greenwich Mean Time – GMT).
Enable Daylight Savings (Включить переход на летнее время)	Летнее время – это период с поздней весны до ранней осени, когда во многих странах стрелки часов переводятся на час вперед, чтобы добавить час светлого времени суток. Установите флажок, если вы используете переход на летнее время.
Start Date (Дата начала)	Введите месяц и день, когда начинается летнее время, если выбран вариант **Enable Daylight Savings** (Включить переход на летнее время). В поле **o'clock (час.)** используется 24 часовой формат. Далее приводится два примера: В большинстве частей Соединенных Штатов переход на летнее время начинается в первое воскресенье апреля. В каждой временной зоне Соединенных Штатов переход осуществляется в 2 часа ночи по местному времени. Таким образом, в Соединенных Штатах необходимо установить **First (Первое), Sunday (Воскресенье), April (Апрель)** и 2 в поле **o'clock (час.)**. В странах Европейского Союза переход на летнее время начинается в последнее воскресенье марта. Во всех временных зонах Европейского Союза переход осуществляется в одно время – в 1 час ночи по Гринвичскому меридиану или универсальному скоординированному времени. Таким образом, в странах Европейского союза необходимо установить **Last (Последнее)**, **Sunday (Воскресенье)**, **March (Март)**. Время, которое нужно ввести в поле **o'clock (час.)** зависит от вашей временной зоны. Например, в Германии необходимо установить 2, так как временная зона Германии находится на 1 час впереди зоны GMT или UTC (GMT+1).

Табл. 108 Установка системного времени (продолжение)

ПОЛЕ	ОПИСАНИЕ
End Date (Конечная дата)	Введите месяц и день, когда заканчивается летнее время, если выбран вариант **Enable Daylight Saving (Включить переход на летнее время)**. В поле **o'clock (час.)** используется 24 часовой формат. Далее приводится два примера: В Соединенных Штатах летнее время заканчивается в последнее воскресенье октября. В каждой временной зоне Соединенных Штатов переход осуществляется в 2 часа ночи по местному времени. Таким образом, в Соединенных Штатах необходимо установить **Last (Последнее)**, **Sunday (Воскресенье)**, **October (Октябрь)** и 2 в поле **o'clock (час.)**. В странах Европейского Союза летнее время заканчивается в последнее воскресенье октября. Во всех временных зонах Европейского Союза обратный переход осуществляется в одно время – в 1 час ночи по Гринвичскому меридиану или универсальному скоординированному времени. Таким образом, в странах Европейского Союза необходимо установить **Last (Последнее)**, **Sunday (Воскресенье)**, **October (Октябрь)**. Время, которое нужно ввести в поле **o'clock (час.)** зависит от вашей временной зоны. Например, в Германии необходимо установить 2, так как временная зона Германии находится на 1 час впереди зоны GMT или UTC (GMT+1).
Apply (Применить)	Нажмите кнопку **Apply (Применить)** для сохранения настроек P660HWP.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)**, чтобы заново начать настройку в этом окне.

20

Регистрационные журналы

В этой главе описывается настройка общих параметров регистрационных журналов, а также порядок просмотра журналов интернет-центра P660HWP. Примеры журнальных сообщений приведены в Приложении.

20.1 Регистрационные журналы – общие сведения

Web-конфигуратор P660HWP позволяет выбрать категории событий и/или предупреждений, которые интернет-центр P660HWP должен регистрировать, а затем заносить в журналы или отправлять администратору в виде сообщений электронной почты или на сервер системных журналов.

20.1.1 Предупреждения и журнальные записи

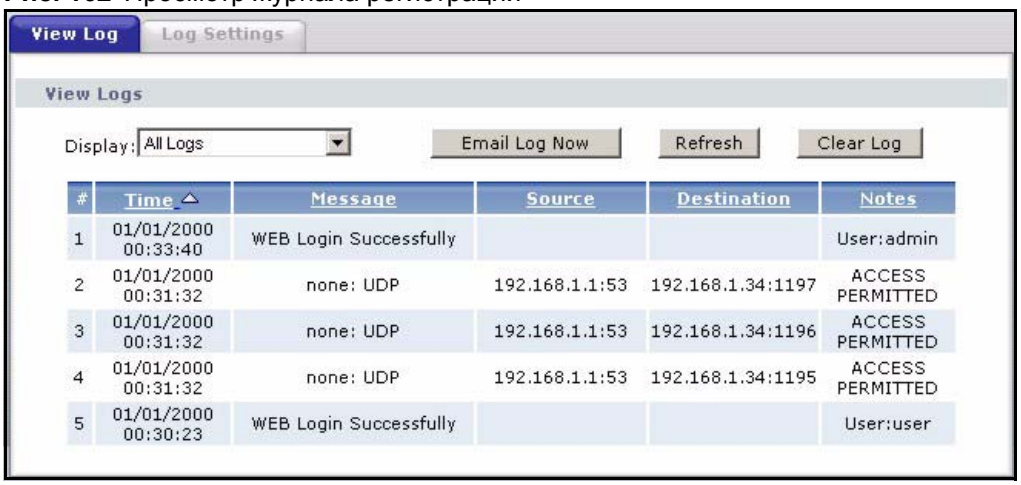
Предупреждение – это тип журнальной записи, требующий серьезного внимания. К предупреждениям относятся сообщения о системных ошибках, атаках (управление доступом) и попытках доступа к заблокированным сайтам. Некоторые категории, такие как **System Errors (Системные ошибки)** состоят как из журнальных записей, так и предупреждений. Вы можете различить их по цвету в окне **View Log (Просмотр журнала)**. Предупреждения отображаются красным цветом, а обычные журнальные записи – черным.

20.2 Просмотр регистрационных журналов

Щелкните **Maintenance (Сопровождение) > Logs (Регистрационные журналы)** для отображения окна **View Log (Просмотр журнала)**. В окне **View Log (Просмотр журнала)** можно посмотреть журнальные записи по категориям, выбранным в окне **Log Settings (Настройки журналов)** (см. Разд. 20.3 на с. 301).

Записи, выделенные красным цветом, означают предупреждения. Если журнал заполнен, самые старые журнальные записи стираются по мере добавления новых. Щелкните по заголовку столбца для сортировки записей. Треугольник показывает возрастающий или убывающий порядок сортировки.

Рис. 162 Просмотр журнала регистрации



В следующей таблице даны описания полей этого окна.

Табл. 109 Просмотр журнала регистрации

ПОЛЕ	ОПИСАНИЕ
Display (Отобразить)	Категории, выбранные Вами в окне **Log Settings (Настройки журналов)** отобразятся в раскрывающемся списке. Выберите категорию журналов для просмотра или установите **All Logs (Все журналы)** для просмотра журналов всех категорий, выбранных в окне **Log Settings (Настройки журналов)**.
Email Log Now (Отправить журнал по электронной почте)	Щелкните **Email Log Now (Отправить журнал по электронной почте)** для отправки журнала по адресу электронной почты, указанному в окне **Log Settings (Настройки журналов)**. Для этого сначала нужно заполнить поля **E-mail Log Settings (Настройки журналов для отправки по электронной почте)** в окне **Log Settings (Настройки журналов)**.
Refresh (Обновить)	Нажмите **Refresh (Обновить)** для обновления экрана регистрационных записей.
Clear Log (Удалить записи)	Нажмите **Clear Log (Удалить записи)** для удаления всех регистрационных записей из журнала.
#	В этом поле отображается номер журнала.
Time (Время)	В этом поле отображается время, когда была зарегистрирована запись.
Message (Сообщение)	В этом поле приводится причина внесения записи в журнал.
Source (Источник)	В этом поле указываются IP-адрес источника и номер порта входящего пакета.
Destination (Адрес назначения)	В этом поле указываются IP-адрес получателя и номер порта входящего пакета.
Notes (Примечания)	В этом поле выводится дополнительная информация о регистрационной записи.

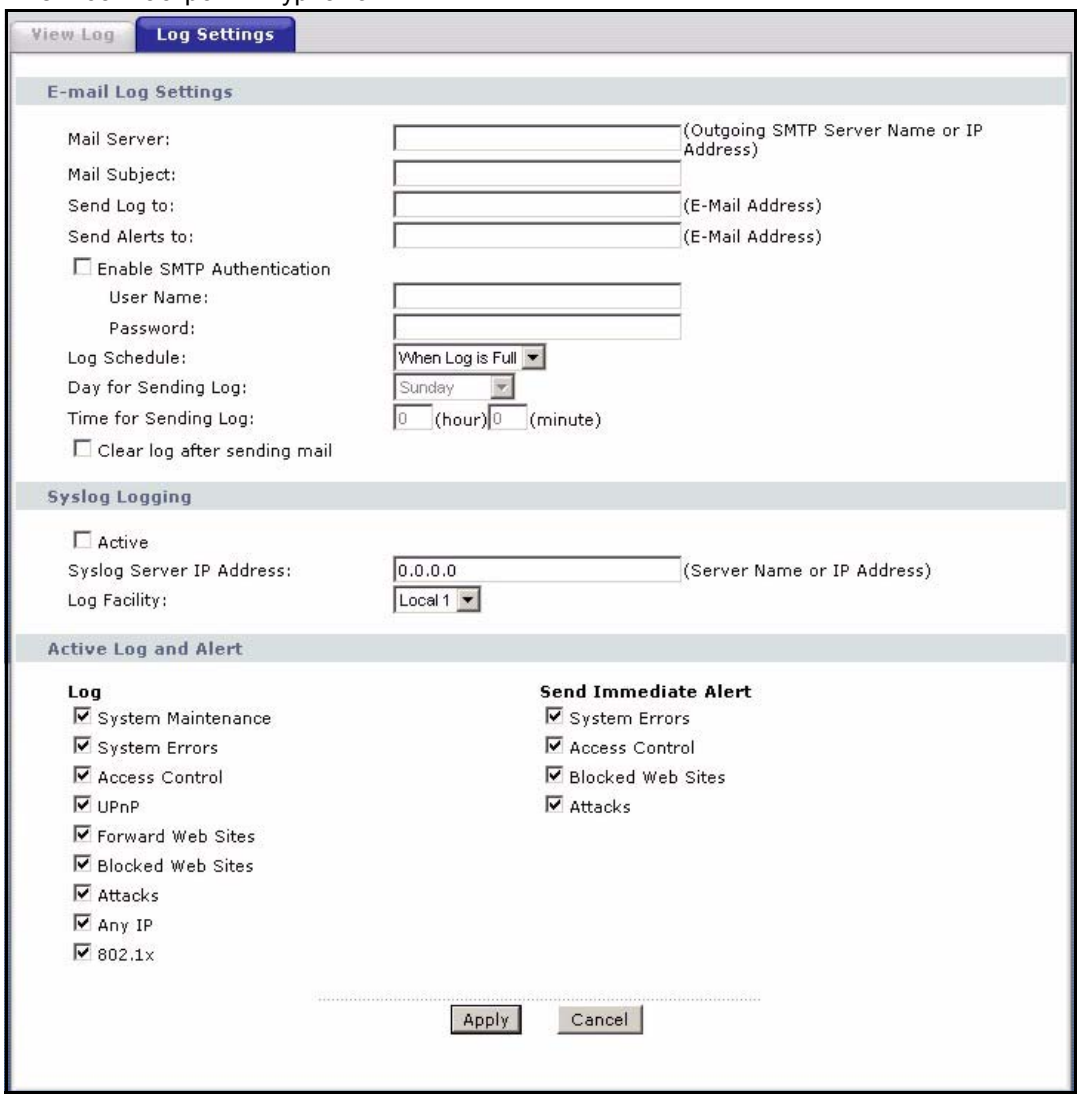
20.3 Настройка параметров журнала

В окне **Log Settings (Настройки журналов)** можно установить следующие параметры: куда P660HWP должен отправлять журналы; расписание, когда P660HWP должен отправлять журналы и запись каких журналов и/или срочных предупреждений P660HWP должен производить. Более подробную информацию см. Разд. 20.1 на с. 299.

Для изменения настроек журналов P660HWP щелкните **Maintenance (Сопровождение) > Logs (Регистрационные журналы) > Log Settings (Настройки журналов)**. При этом откроется показанное ниже окно.

Предупреждения отправляются адресату непосредственно в момент их появления. Журнальные записи отправляются по мере заполнения журнала. Выбор большого количества категорий предупреждений и/или журнальных записей (особенно это касается **Управления доступом**) может привести к тому, что будет рассылаться большое количество сообщений электронной почты.

Рис. 163 Настройки журналов



В следующей таблице даны описания полей этого окна.

Табл. 110 Настройки журналов

ПОЛЕ	ОПИСАНИЕ
E-mail Log Settings (Настройки журналов для отправки по электронной почте)	
Mail Server (Почтовый сервер)	Введите имя сервера или IP-адрес почтового сервера для указанных ниже адресов электронной почты. Если не заполнять это поле, журнал и предупреждающие сообщения не будут высылаться по электронной почте.
Mail Subject (Тема сообщения)	Введите заголовок для помещения в строку «subject» (тема) сообщения электронной почты, отправляемого P660HWP. Это поле присутствует не во всех моделях ZyXEL.
Send log to (Адресаты журнальных записей)	Интернет-центр P660HWP отправляет регистрационные журналы по адресам электронной почты, указанным в этом поле. Если это поле оставить пустым, P660HWP не отправляет журналы по электронной почте.
Send alerts to (Адресаты предупреждений)	Предупреждения – это сообщения в реальном времени, посылаемые сразу после того, как произошло событие, такое как атака DoS, системная ошибка или попытка доступа в запрещенную зону сети. Введите адрес электронной почты, куда будут отправляться предупреждающие сообщения. К предупреждающим сообщениям относятся сообщения о системных ошибках, атаках и попыткам доступа к заблокированным web-сайтам. Если это поле оставить пустым, предупреждающие сообщения не будут отправляться по электронной почте.
Enable SMTP Authentication (Включить аутентификацию SMTP)	Simple Mail Transfer Protocol (Простой протокол электронной почты) – стандартный протокол обмена сообщениями для сети Интернет. SMTP обеспечивает пересылку сообщений с одного почтового сервера на другой.
User Name (Имя пользователя)	Введите регистрационное имя, предоставленное Интернет-провайдером.
Password (Пароль)	Введите пароль для данного имени пользователя.
Log Schedule (План журнальной регистрации)	В этом раскрывающемся меню выбирается частота рассылки журнальных записей по электронной почте: • Daily (Ежедневно) • Weekly (Еженедельно) • Hourly (Каждый час) • When Log is Full (По заполнении журнала) • None (Нет). При выборе опции **Weekly (Еженедельно)** или **Daily (Ежедневно)** необходимо указать время дня для рассылки e-mail сообщений. При выборе опции **Weekly (Еженедельно)** также необходимо указать день недели для рассылки сообщений. При выборе опции **When Log is Full (По заполнении журнала)** сообщение посылается только при условии, что журнал заполнен. При выборе **None (Никогда)** сообщения не отправляются.
Day for Sending Log (День рассылки журнальных записей)	Из раскрывающегося списка выберите день недели, в который должны отправляться записи.
Time for Sending Log (Время рассылки журнальных записей)	Введите время отправки журнальных записей в 24-часовом формате (например, 23:00 для 11 часов вечера).

Табл. 110 Настройки журналов

ПОЛЕ	ОПИСАНИЕ
Clear log after sending mail (Очищать журнал после отправки почтовых сообщений)	Установите здесь флажок для удаления всех записей после их отправки интернет-центром P660HWP по электронной почте.
Syslog Logging (Системный журнал)	P660HWP отправляет журнал на внешний сервер системного журнала.
Active (Активировать)	Для активации системного журнала нажмите кнопку **Active (Активировать)**.
Syslog Server IP Address (IP-адрес сервера системных журналов)	Введите имя сервера или IP-адрес сервера системных журналов, который будет регистрировать выбранные категории сообщений.
Log Facility (Размещение журнала)	Из выпадающего списка выберите место, где будут храниться журнальные записи. Эта функция дает возможность регистрировать сообщения в различных файлах на сервере системных журналов. Для получения дополнительной информации см. руководство по серверу системных журналов.
Active Log and Alert (Включить журналы и предупреждения)	
Log (Регистрационный журнал)	Выберите категории журнальных записей, которые необходимо регистрировать.
Send Immediate Alert (Отправить предупреждение немедленно)	Выберите категории журналов, для которых P660HWP будет отправлять предупреждения по электронной почте немедленно.
Apply (Применить)	Нажмите кнопку **Apply (Применить)**, чтобы сохранить измененные настройки и выйти из этого окна.
Cancel (Отменить)	Нажмите кнопку **Cancel (Отменить)** для возврата к предыдущим сохраненным настройкам.

20.3.1 Пример журнала, отправляемого по электронной почте

Сообщение «End of Log» (Конец журнала) появляется каждый раз, когда отправляется полностью заполненный журнал. Ниже приводится пример журнала, посланного по электронной почте.

- Разрешено редактировать заглавие объекта.
- Ввод даты в формате «день-месяц-год».
- Ввод даты в формате «месяц-день-год». Ввод времени в формате «часы-минуты-секунды».
- Сообщение «`End of Log`» означает, что отправлен весь журнал.

Рис. 164 Пример журнала, высылаемого по электронной почте

```
Subject:
        Firewall Alert From xxxxx
   Date:
        Fri, 07 Apr 2000 10:05:42
   From:
        user@zyxel.com
     To:
        user@zyxel.com
  1|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |default policy  |forward
   | 09:54:03 |UDP     src port:00520 dest port:00520  |<1,00>          |
  2|Apr  7 00 |From:192.168.1.131   To:192.168.1.255   |default policy  |forward
   | 09:54:17 |UDP     src port:00520 dest port:00520  |<1,00>          |
  3|Apr  7 00 |From:192.168.1.6     To:10.10.10.10     |match           |forward
   | 09:54:19 |UDP     src port:03516 dest port:00053  |<1,01>          |
……..{snip}……..
……..{snip}……..
126|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |match           |forward
   | 10:05:00 |UDP     src port:00520 dest port:00520  |<1,02>          |
127|Apr  7 00 |From:192.168.1.131   To:192.168.1.255   |match           |forward
   | 10:05:17 |UDP     src port:00520 dest port:00520  |<1,02>          |
128|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |match           |forward
   | 10:05:30 |UDP     src port:00520 dest port:00520  |<1,02>          |
End of Firewall Log
```

20.4 Описание сообщений журнала

В данном разделе приводится описание примеров сообщений в регистрационном журнале.

Табл. 111 Журнальные сообщения, связанные с обслуживанием системы

СООБЩЕНИЕ	ОПИСАНИЕ
Time calibration is successful	Маршрутизатор синхронизировал свое время на базе информации, полученной от сервера времени.
Time calibration failed	При синхронизации времени маршрутизатора с сервером времени произошел сбой.
WAN interface gets IP:%s	Порту WAN назначен новый IP-адрес от сервера DHCP, PPPoE, PPTP или удаленного сервера.
DHCP client IP expired	Время аренды IP-адреса клиента DHCP истекло.
DHCP server assigns%s	Сервер DHCP назначил клиенту IP-адрес.
Successful WEB login	Успешный вход в систему через интерфейс Web-конфигуратора.
WEB login failed	Произошел сбой при входе в систему через интерфейс Web-конфигуратора.
Successful TELNET login	Успешный вход в систему по telnet.
TELNET login failed	Произошел сбой при входе в систему по telnet.
Successful FTP login	Успешный вход в систему по ftp.
FTP login failed	Произошел сбой при регистрации сеанса ftp.

Табл. 111 Журнальные сообщения, связанные с обслуживанием системы

СООБЩЕНИЕ	ОПИСАНИЕ
NAT Session Table is Full!	Достигнуто максимальное число записей в таблице NAT и таблица заполнена.
Starting Connectivity Monitor	Запуск Диспетчера соединений.
Time initialized by Daytime Server	Маршрутизатор получил время и дату от сервера даты и времени.
Time initialized by Time server	Маршрутизатор получил время и дату от сервера времени.
Time initialized by NTP server	Маршрутизатор получил время и дату от сервера NTP.
Connect to Daytime server fail	Произошел сбой при подключении маршрутизатора к серверу даты и времени.
Connect to Time server fail	Произошел сбой при подключении маршрутизатора к серверу времени.
Connect to NTP server fail	Произошел сбой при подключении маршрутизатора к серверу NTP.
Too large ICMP packet has been dropped	Маршрутизатор сбросил пакет ICMP, размер которого превышал допустимый.
Configuration Change: PC = 0x%x, Task ID = 0x%x	Маршрутизатор сохраняет изменения конфигурации.
Successful SSH login	Успешный вход в систему через сервер SSH.
SSH login failed	Произошел сбой при входе в систему через сервер SSH маршрутизатора.
Successful HTTPS login	Успешный вход в систему через интерфейс Web-конфигуратора по протоколу HTTPS.
HTTPS login failed	Произошел сбой при входе в систему через интерфейс Web-конфигуратора по протоколу HTTPS.

Табл. 112 Журнальные сообщения о системных ошибках

СООБЩЕНИЕ	ОПИСАНИЕ
%s exceeds the max. number of session per host!	Попытка создания сеанса NAT привела к превышению максимального количества записей в таблице сеансов NAT, допустимого для одного узла.
setNetBIOSFilter: calloc error	Произошел сбой при выделении памяти маршрутизатора для параметров фильтра NetBIOS.
readNetBIOSFilter: calloc error	Произошел сбой при выделении памяти маршрутизатора для параметров фильтра NetBIOS.
WAN connection is down.	Подключение к глобальной сети не работает. Доступ в сеть через этот порт невозможен.

Табл. 113 Журнальные сообщения, связанные с управлением доступом

СООБЩЕНИЕ	ОПИСАНИЕ
`Firewall default policy: [TCP | UDP | IGMP | ESP | GRE | OSPF] <Packet Direction>`	Попытка доступа через протокол TCP/UDP/IGMP/ ESP/GRE/OSPF, подпадающая под действие политики межсетевого экрана, заданной по умолчанию, и заблокированная либо переадресованная согласно установкам этой политики.
`Firewall rule [NOT] match:[TCP | UDP | IGMP | ESP | GRE | OSPF] <Packet Direction>, <rule:%d>`	Попытка доступа через протокол TCP/UDP/IGMP/ ESP/GRE/OSPF, подпадающая (или не подпадающая) под действие заданного правила межсетевого экрана (обозначается номером) и заблокированная или переадресованная согласно этому правилу.
`Triangle route packet forwarded: [TCP | UDP | IGMP | ESP | GRE | OSPF]`	Межсетевой экран разрешил проход сеанса с треугольным маршрутом.
`Packet without a NAT table entry blocked: [TCP | UDP | IGMP | ESP | GRE | OSPF]`	Маршрутизатор заблокировал пакет, для которого нет соответствующей записи в таблице NAT.
`Router sent blocked web site message: TCP`	Маршрутизатор отправил сообщение, уведомляющее пользователя о блокировке доступа к запрошенному Web-сайту.

Табл. 114 Журнальные сообщения о сбросе сеансов TCP

СООБЩЕНИЕ	ОПИСАНИЕ
`Under SYN flood attack, sent TCP RST`	Маршрутизатор отправил пакет сброса сеансов TCP при обнаружении синхронной атаки на узел (подсчет незавершенных сеансов TCP ведется по целевому хосту).
`Exceed TCP MAX incomplete, sent TCP RST`	Маршрутизатор отправил пакет сброса сеансов TCP, когда количество незавершенных подключений через TCP превысило заданное пользователем пороговое значение (подсчет открытых сеансов TCP ведется по целевому узлу). Примечание: информацию о значении порога **TCP Maximum Incomplete (Максимум неполных TCP)** см. в описании окна **Firewall Attack Alerts (Предупреждения об атаках на межсетевой экран)**.
`Peer TCP state out of order, sent TCP RST`	Маршрутизатор отправил пакет сброса сеансов TCP, когда состояние TCP соединения было неисправно. Примечание: межсетевой экран проверяет состояние TCP по RFC793 Рис. 6.
`Firewall session time out, sent TCP RST`	Маршрутизатор отправил пакет сброса TCP по истечении времени простоя динамического сеанса связи через межсетевой экран. Время простоя сеансов связи по умолчанию: Время простоя сеанса ICMP: 3 минуты Время простоя сеанса UDP: 3 минуты Время ожидания соединения TCP (трехстороннее согласование установления связи): 270 секунд Время ожидания FIN-пакета TCP: 2 MSL (значение «Maximum Segment Lifetime» (Максимальная продолжительность сегмента), установленное в заголовке TCP). Время простоя установленного соединения TCP:150 минут Время ожидания сброса TCP соединения: 10 секунд

Табл. 114 Журнальные сообщения о сбросе сеансов TCP

СООБЩЕНИЕ	ОПИСАНИЕ
`Exceed MAX incomplete, sent TCP RST`	Маршрутизатор отправил пакет сброса сеансов TCP, когда количество незавершенных подключений (через TCP и UDP) превысило заданное пользователем пороговое значение. (открытыми считаются все соединения TCP и UDP через межсетевой экран). Примечание: когда количество открытых соединений (TCP + UDP) > «Maximum Incomplete High» (Максимальный порог), маршрутизатор отправляет пакеты TCP RST для соединений TCP и разрывает соединения (динамические сеансы через межсетевой экран) до тех пор, пока число открытых соединений не будет < «Maximum Incomplete Low» (Минимальный порог).
`Access block, sent TCP RST`	Маршрутизатор отправляет пакет TCP RST и создает эту запись в журнале, если включен механизм сброса TCP межсетевого экрана (с помощью команды интерепретатора «sys firewall tcprst»).

Табл. 115 Журнальные сообщения о фильтре пакетов

СООБЩЕНИЕ	ОПИСАНИЕ
`[TCP | UDP | ICMP | IGMP | Generic] packet filter matched (set:%d, rule:%d)`	Произведена попытка доступа, соответствующая настроенному правилу фильтра (указывается номер набора и номер правила), и выполнена блокировка или пересылка пакета в соответствии с правилом.

Табл. 116 Журнальные сообщения ICMP (Протокол межсетевых управляющих сообщений)

СООБЩЕНИЕ	ОПИСАНИЕ
`Firewall default policy: ICMP <Packet Direction>, <type:%d>, <code:%d>`	Доступ через протокол межсетевых управляющих сообщений (ICMP), подпадающий под действие политики по умолчанию и заблокированный или переадресованный согласно настройкам пользователя. Подробное описание типов и кодов приведено в Табл. 127 на с. 316.
`Firewall rule [NOT] match: ICMP <Packet Direction>, <rule:%d>, <type:%d>, <code:%d>`	Доступ через ICMP, подпадающий (либо не подпадающий) под действие правила для межсетевых экранов (идентифицированное своим номером) и блокированный или переадресованный в соответствии с правилом. Подробное описание типов и кодов приведено в Табл. 127 на с. 316.
`Triangle route packet forwarded: ICMP`	Межсетевой экран разрешил проход сеанса с треугольным маршрутом.
`Packet without a NAT table entry blocked: ICMP`	Маршрутизатор заблокировал пакет, для которого нет соответствующей записи в таблице NAT.
`Unsupported/out-of-order ICMP: ICMP`	Межсетевой экран не поддерживает такие пакеты ICMP либо произошел сбой в пакетах ICMP.
`Router reply ICMP packet: ICMP`	Маршрутизатор послал ответный пакет ICMP отправителю.

Табл. 117 Журнальные сообщения CDR (Журнал регистрации вызовов)

СООБЩЕНИЕ	ОПИСАНИЕ
`board%d line%d channel%d, call%d, %s C01 Outgoing Call dev=%x ch=%x %s`	Маршрутизатор получил запрос на установление соединения для выполнения вызова. «call» – номер вызова. «dev» – тип устройства (3 – коммутируемое соединение, 6 – PPPoE, 10 – PPTP). «channel» или «ch» – идентификатор канала вызова. Например, «board 0 line 0 channel 0, call 3, C01 Outgoing Call dev=6 ch=0» означает, что маршрутизатор выполнял вызов сервера PPPoE 3 раза.
`board%d line%d channel%d, call%d, %s C02 OutCall Connected%d%s`	Установлено PPPoE, PPTP или коммутируемое соединение.
`board%d line%d channel%d, call%d, %s C02 Call Terminated`	Прервано PPPoE, PPTP или коммутируемое соединение.

Табл. 118 Журнальные сообщения PPP (Протокол «точка-точка»)

СООБЩЕНИЕ	ОПИСАНИЕ
`ppp:LCP Starting`	Запущена стадия протокола управления каналом связи для PPP соединения.
`ppp:LCP Opening`	Открывается стадия протокола управления каналом связи для PPP соединения.
`ppp:CHAP Opening`	Открывается стадия протокола аутентификации по методу «Challenge Handshake Authentication» (Вызов-рукопожатие) для PPP соединения.
`ppp:IPCP Starting`	Начинается стадия протокола управления протоколом Интернет (Internet Protocol Control Protocol) для PPP соединения.
`ppp:IPCP Opening`	Открывается стадия протокола управления протоколом Интернет (Internet Protocol Control Protocol) для PPP соединения.
`ppp:LCP Closing`	Закрывается стадия протокола управления каналом связи (Link Control Protocol) для PPP соединения.
`ppp:IPCP Closing`	Закрывается стадия протокола управления протоколом Интернет (Internet Protocol Control Protocol) для PPP соединения.

Табл. 119 Журнальные сообщения UPnP

СООБЩЕНИЕ	ОПИСАНИЕ
`UPnP pass through Firewall`	Пакеты UPnP могут проходить через межсетевой экран.

Табл. 120 Журнальные сообщения о фильтрации контента

СООБЩЕНИЕ	ОПИСАНИЕ
`%s: Keyword blocking`	На запрошенной веб-странице имеется заданное пользователем ключевое слово.
`%s: Not in trusted web list`	Данный web-сайт находится на домене, не гарантирующем высокой степени защиты, и маршрутизатор блокирует весь трафик, оставляя доступ только к сайтам, размещенным на надежных доменах.
`%s: Forbidden Web site`	Данный web-сайт входит в список запрещенных.
`%s: Contains ActiveX`	Данный web-сайт содержит элементы ActiveX.
`%s: Contains Java applet`	Данный web-сайт содержит апплеты языка Java.
`%s: Contains cookie`	Данный web-сайт содержит файлы cookie.
`%s: Proxy mode detected`	Маршрутизатор обнаружил режим прокси в данном пакете.
`%s`	Сервер фильтрации содержания ответил, что данный web-сайт входит в список заблокированных, но не указал категорию блокировки.
`%s:%s`	Сервер фильтрации содержания ответил, что данный web-сайт входит в список заблокированных, и указал категорию блокировки.
`%s(cache hit)`	Система обнаружила, что данный web-сайт входит в список заблокированных из локального кэша, но не указала категорию блокировки.
`%s:%s(cache hit)`	Система обнаружила, что данный web-сайт входит в список заблокированных из локального кэша, и известна категория блокировки.
`%s: Trusted Web site`	Данный web-сайт находится на доверенном домене с высокой степенью защиты.
`%s`	Если фильтр содержания отключен согласно расписанию или Вы не установили флажок «Block Matched Web Site» (Блокируемый сайт), то система переадресует содержание.
`Waiting content filter server timeout`	Сервер фильтрации внешнего содержания не ответил в течение заданного времени ожидания.
`DNS resolving failed`	Интернет-центр P660HWP не может получить IP-адрес сервера фильтрации внешнего контента с помощью запроса DNS.
`Creating socket failed`	Интернет-центр P660HWP не может создать запрос из-за сбоя при создании канала TCP/IP, порт:номер порта.
`Connecting to content filter server fail`	Сбой при подключении к серверу фильтрации внешнего содержания.
`License key is invalid`	Недействительный лицензионный ключ внешнего сервера фильтрации содержания.

Табл. 121 Журнальные сообщения об атаках

СООБЩЕНИЕ	ОПИСАНИЕ
`attack [TCP | UDP | IGMP | ESP | GRE | OSPF]`	Межсетевой экран обнаружил атаку TCP/UDP/IGMP/ESP/GRE/OSPF.
`attack ICMP (type:%d, code:%d)`	Межсетевой экран обнаружил атаку ICMP. Подробное описание типов и кодов приведено в Табл. 127 на с. 316.
`land [TCP | UDP | IGMP | ESP | GRE | OSPF]`	Межсетевой экран обнаружил атаку по TCP/UDP/IGMP/ESP/GRE/OSPF на каталог локальной сети (LAND).
`land ICMP (type:%d, code:%d)`	Межсетевой экран обнаружил атаку ICMP на каталог локальной сети (LAND). Подробное описание типов и кодов приведено в Табл. 127 на с. 316.
`ip spoofing - WAN [TCP | UDP | IGMP | ESP | GRE | OSPF]`	Межсетевой экран обнаружил атаку с подменой IP-адреса на порт WAN.
`ip spoofing - WAN ICMP (type:%d, code:%d)`	Межсетевой экран обнаружил атаку с подменой IP-адреса ICMP на порт WAN. Подробное описание типов и кодов приведено в Табл. 127 на с. 316.
`icmp echo: ICMP (type:%d, code:%d)`	Межсетевой экран обнаружил атаку с использованием отклика ICMP. Подробное описание типов и кодов приведено в Табл. 127 на с. 316.
`syn flood TCP`	Межсетевой экран обнаружил синхронную атаку TCP.
`ports scan TCP`	Межсетевой экран обнаружил атаку TCP со сканированием портов.
`teardrop TCP`	Межсетевой экран обнаружил Teardrop-атаку TCP.
`teardrop UDP`	Межсетевой экран обнаружил Teardrop-атаку UDP.
`teardrop ICMP (type:%d, code:%d)`	Межсетевой экран обнаружил Teardrop-атаку ICMP. Подробное описание типов и кодов приведено в Табл. 127 на с. 316.
`illegal command TCP`	Межсетевой экран обнаружил атаку TCP с недопустимой командой.
`NetBIOS TCP`	Межсетевой экран обнаружил атаку TCP NetBIOS.
`ip spoofing - no routing entry [TCP | UDP | IGMP | ESP | GRE | OSPF]`	Межсетевой экран классифицировал пакет без записи о маршрутизации от источника как атаку с подменой IP-адреса.
`ip spoofing - no routing entry ICMP (type:%d, code:%d)`	Межсетевой экран классифицировал пакет ICMP без указания источника как атаку с подстановкой IP (IP spoofing).
`vulnerability ICMP (type:%d, code:%d)`	Межсетевой экран обнаружил атаку ICMP на уязвимость. Подробное описание типов и кодов приведено в Табл. 127 на с. 316.
`traceroute ICMP (type:%d, code:%d)`	Межсетевой экран обнаружил атаку ICMP с отслеживанием маршрута. Подробное описание типов и кодов приведено в Табл. 127 на с. 316.

Табл. 122 Журнальные сообщения IPSec

СООБЩЕНИЕ	ОПИСАНИЕ
Discard REPLAY packet	Маршрутизатор получил и отклонил пакет с некорректным порядковым номером.
Inbound packet authentication failed	Маршрутизатор получил пакет, который был изменен. Пакет мог быть изменен или умышленно испорчен третьей стороной.
Receive IPSec packet, but no corresponding tunnel exists	Маршрутизатор удалил входящий пакет, для которого протокол последовательного периферийного интерфейса (SPI) не смог найти соответствующего безопасного соединения в фазе 2 (Phase 2 SA).
Rule <%d> idle time out, disconnect	Маршрутизатор разорвал соединение, имевшее исходящий и не имевшее входящего трафика в течение определенного периода времени. Для установки периода времени можно использовать команду «ipsec timer chk_conn». Значение по умолчанию составляет 2 минуты.
WAN IP changed to <IP>	Маршрутизатор разорвал все соединения с MyIP = 0.0.0.0 при изменении IP-адреса в глобальной сети (WAN).

Табл. 123 Журнальные сообщения протокола обмена ключами (IKE)

СООБЩЕНИЕ	ОПИСАНИЕ
Active connection allowed exceeded	Сбой при обмене ключами для установки нового соединения из-за достижения предельного количества одновременных безопасных подключений в фазе 2 (Phase 2 SA).
Start Phase 2: Quick Mode	Запущен быстрый режим 2-й фазы.
Verifying Remote ID failed:	Соединение разорвано во время 2-й фазы обмена ключами (IKE) из-за несовпадения локальных/удаленных адресов маршрутизатора и клиентского устройства.
Verifying Local ID failed:	Соединение разорвано во время 2-й фазы обмена ключами (IKE) из-за несовпадения локальных/удаленных адресов маршрутизатора и клиентского устройства.
IKE Packet Retransmit	Маршрутизатор выполнил повторную передачу пакета, т.к. не был получен ответ от клиентского устройства.
Failed to send IKE Packet	Передача пакетов обмена ключами (IKE) маршрутизатором была прервана из-за ошибки Ethernet.
Too many errors! Deleting SA	Безопасное соединение (SA) было сброшено из-за слишком большого количества ошибок.
Phase 1 IKE SA process done	Завершена 1-я фаза обмена ключами (IKE) при установке безопасного соединения.
Duplicate requests with the same cookie	Маршрутизатор получил несколько запросов от одного клиентского устройства, но продолжает обрабатывать первый пакет IKE от данного устройства.
IKE Negotiation is in process	Маршрутизатор уже начал согласование по установке соединения с другой стороной, но процесс обмена ключами (IKE) не завершен.
No proposal chosen	Не совпадают параметры фазы 1 или фазы 2. Проверьте все протоколы/настройки. Пример: если одно устройство конфигурируется под 3DES, а другое – под DES, то установить соединение будет невозможно.

Табл. 123 Журнальные сообщения протокола обмена ключами (IKE) (продолжение)

СООБЩЕНИЕ	ОПИСАНИЕ
Local / remote IPs of incoming request conflict with rule <%d>	Задан адрес безопасного шлюза 0.0.0.0, и маршрутизатор использовал «локальный адрес» клиентского устройства в качестве «удаленного адреса» маршрутизатора. Такие параметры конфликтуют со статическим правилом #d; таким образом, установить соединение невозможно.
Cannot resolve Secure Gateway Addr for rule <%d>	Маршрутизатор не смог выделить IP-адрес из имени домена, который использовался в качестве адреса безопасного шлюза.
Peer ID: <peer id> <My remote type> -<My local type>	Отображаемый ID не совпадает на разных концах соединения.
vs. My Remote <My remote> - <My remote>	Отображаемый ID не совпадает на разных концах соединения.
vs. My Local <My local>-<My local>	Отображаемый ID не совпадает на разных концах соединения.
Send <packet>	Отправлен пакет.
Recv <packet>	Протокол обмена ключами использует пакет ISAKMP для передачи данных. В каждом пакете ISAKMP содержится много различных типов полезной информации. Все они отображаются в журнале. Список всех типов полезной информации в пакетах ISAKMP приведен в RFC2408 – ISAKMP.
Recv <Main or Aggressive> Mode request from <IP>	Маршрутизатор получил с указанного адреса клиентского устройства запрос на начало согласования по обмену ключами.
Send <Main or Aggressive> Mode request to <IP>	Маршрутизатор начал процесс согласования с клиентским устройством.
Invalid IP <Peer local> / <Peer local>	Недействительный локальный IP-адрес клиентского устройства.
Remote IP <Remote IP> / <Remote IP> conflicts	Задан адрес безопасного шлюза 0.0.0.0, и маршрутизатор использовал «локальный адрес» клиентского устройства в качестве «удаленного адреса» маршрутизатора. Такие параметры конфликтуют со статическим правилом #d; таким образом, установить соединение невозможно.
Phase 1 ID type mismatch	Тип клиентского идентификатора (Peer ID Type) данного маршрутизатора отличается от типа локального идентификатора (Local ID Type) маршрутизатора IPSec, обслуживающего клиентское устройство.
Phase 1 ID content mismatch	Содержание клиентского идентификатора (Peer ID Content) данного маршрутизатора отличается от содержания локального идентификатора (Local ID Content) маршрутизатора IPSec, обслуживающего клиентское устройство.
No known phase 1 ID type found	При попытке подключения маршрутизатор не смог найти известного идентификатора 1-й фазы.
ID type mismatch. Local / Peer: <Local ID type/Peer ID type>	Не совпадают типы идентификаторов 1-й фазы.
ID content mismatch	Не совпадает содержание идентификаторов 1-й фазы.
Configured Peer ID Content: <Configured Peer ID Content>	Не совпадает содержание идентификаторов 1-й фазы и отображается настроенное содержание идентификатора клиентского устройства (Peer ID Content).
Incoming ID Content: <Incoming Peer ID Content>	Не совпадает содержание идентификаторов 1-й фазы и отображается содержание идентификатора входящих пакетов.

Табл. 123 Журнальные сообщения протокола обмена ключами (IKE) (продолжение)

СООБЩЕНИЕ	ОПИСАНИЕ
Unsupported local ID Type: <%d>	Данный тип идентификатора 1-й фазы не поддерживается маршрутизатором.
Build Phase 1 ID	Маршрутизатор начал построение идентификатора 1-й фазы.
Adjust TCP MSS to%d	Маршрутизатор автоматически изменил максимальный размер сегментов TCP после создания туннельного соединения.
Rule <%d> input idle time out, disconnect	Туннельное соединение в рамках имеющегося правила было разорвано из-за отсутствия входящего трафика в течение времени простоя.
XAUTH succeed! Username: <Username>	Для аутентификации имеющегося имени пользователя маршрутизатор использовал расширенную аутентификацию.
XAUTH fail! Username: <Username>	Маршрутизатор не смог использовать расширенную аутентификацию для аутентификации имеющегося имени пользователя.
Rule[%d] Phase 1 negotiation mode mismatch	Режим согласования 1-й фазы обмена ключами (IKE), заданный в правиле маршрутизатора, не совпадает с таковым у клиентского устройства.
Rule [%d] Phase 1 encryption algorithm mismatch	Алгоритм шифрования 1-й фазы обмена ключами (IKE), заданный в правиле маршрутизатора, не совпадает с таковым у клиентского устройства.
Rule [%d] Phase 1 authentication algorithm mismatch	Алгоритм аутентификации 1-й фазы обмена ключами (IKE), заданный в правиле маршрутизатора, не совпадает с алгоритмом клиентского устройства.
Rule [%d] Phase 1 authentication method mismatch	Метод аутентификации 1-й фазы обмена ключами (IKE), заданный в правиле маршрутизатора, не совпадает с таковым у клиентского устройства.
Rule [%d] Phase 1 key group mismatch	Группа ключей 1-й фазы обмена ключами (IKE), заданная в правиле маршрутизатора, не совпадает с таковой у клиентского устройства.
Rule [%d] Phase 2 protocol mismatch	Протокол 2-й фазы обмена ключами (IKE), заданный в правиле маршрутизатора, не совпадает с таковым у клиентского устройства.
Rule [%d] Phase 2 encryption algorithm mismatch	Алгоритм шифрования 2-й фазы обмена ключами (IKE), заданный в правиле маршрутизатора, не совпадает с таковым у клиентского устройства.
Rule [%d] Phase 2 authentication algorithm mismatch	Алгоритм аутентификации 2-й фазы обмена ключами (IKE), заданный в правиле маршрутизатора, не совпадает с алгоритмом клиентского устройства.
Rule [%d] Phase 2 encapsulation mismatch	Инкапсуляция 2-й фазы обмена ключами (IKE), заданная в правиле маршрутизатора, не совпадает с таковой у клиентского устройства.
Rule [%d]> Phase 2 pfs mismatch	Настройки абсолютной секретности пересылки (pfs) 2-й фазы обмена ключами (IKE), заданные в правиле маршрутизатора, не совпадают с таковыми у клиентского устройства.
Rule [%d] Phase 1 ID mismatch	Идентификатор 1-й фазы обмена ключами (IKE), заданный в правиле маршрутизатора, не совпадает с таковым у клиентского устройства.
Rule [%d] Phase 1 hash mismatch	Хэш 1-й фазы обмена ключами (IKE), заданный в правиле маршрутизатора, не совпадает с таковым у клиентского устройства.

Табл. 123 Журнальные сообщения протокола обмена ключами (IKE) (продолжение)

СООБЩЕНИЕ	ОПИСАНИЕ
`Rule [%d] Phase 1 preshared key mismatch`	Общий ключ 1-й фазы обмена ключами (IKE), заданный в правиле маршрутизатора, не совпадает с таковым у клиентского устройства.
`Rule [%d] Tunnel built successfully`	Успешно установлено заданное в правиле туннельное соединение IPSec.
`Rule [%d] Peer's public key not found`	Не найден заданный в правиле открытый ключ клиентского устройства в рамках 1-й фазы обмена ключами (IKE).
`Rule [%d] Verify peer's signature failed`	Не удалось проверить заданную в правиле подпись клиентского устройства в рамках 1-й фазы обмена ключами (IKE).
`Rule [%d] Sending IKE request`	Протокол обмена ключами (IKE) отправил IKE-запрос для имеющегося правила.
`Rule [%d] Receiving IKE request`	Протокол обмена ключами (IKE) получил IKE-запрос для имеющегося правила.
`Swap rule to rule [%d]`	Маршрутизатор переключился на использование имеющегося правила.
`Rule [%d] Phase 1 key length mismatch`	Длина ключа 1-й фазы обмена ключами (с алгоритмом шифрования AES), заданная в правиле маршрутизатора, не совпадает с таковой у клиентского устройства.
`Rule [%d] phase 1 mismatch`	1-я фаза обмена ключами (IKE), заданная в правиле маршрутизатора, не соответствует таковой у клиентского устройства.
`Rule [%d] phase 2 mismatch`	2-я фаза обмена ключами (IKE), заданная в правиле маршрутизатора, не соответствует таковой у клиентского устройства.
`Rule [%d] Phase 2 key length mismatch`	Длина ключей 2-й фазы обмена ключами (с алгоритмом шифрования AES), заданная в правиле маршрутизатора, не совпадает с таковой у клиентского устройства.

Табл. 124 Журнальные сообщения PKI (инфраструктуры сертификации открытых ключей)

СООБЩЕНИЕ	ОПИСАНИЕ
`Enrollment successful`	Успешно выполнена регистрация сертификата SCEP в режиме реального времени. Поле «Destination» (Адрес назначения) содержит IP-адрес и порт сервера центра сертификации.
`Enrollment failed`	Не удалось выполнить регистрацию сертификата SCEP в режиме реального времени. Поле «Destination» (Адрес назначения) содержит IP-адрес и порт сервера центра сертификации.
`Failed to resolve <SCEP CA server url>`	Не удалось выполнить регистрацию сертификата SCEP в режиме реального времени из-за невозможности определения адреса сервера бюро сертификации.
`Enrollment successful`	Успешно выполнена регистрация сертификата CMP в режиме реального времени. Поле «Destination» (Адрес назначения) содержит IP-адрес и порт сервера центра сертификации.
`Enrollment failed`	Не удалось выполнить регистрацию сертификата CMP в режиме реального времени. Поле «Destination» (Адрес назначения) содержит IP-адрес и порт сервера центра сертификации.
`Failed to resolve <CMP CA server url>`	Не удалось выполнить регистрацию сертификата CMP в режиме реального времени из-за невозможности определения IP-адреса сервера бюро сертификации.

Табл. 124 Журнальные сообщения PKI (инфраструктуры сертификации открытых ключей)

СООБЩЕНИЕ	ОПИСАНИЕ
`Rcvd ca cert: <subject name>`	Маршрутизатор получил сертификат центра сертификации с указанием темы от сервера LDAP (облегченный протокол службы каталогов), IP-адрес и порт которого указаны в поле «Source» (Отправитель).
`Rcvd user cert: <subject name>`	Маршрутизатор получил сертификат пользователя с указанием темы от сервера LDAP (облегченный протокол службы каталогов), IP-адрес и порт которого указаны в поле «Source» (Отправитель).
`Rcvd CRL <size>: <issuer name>`	Маршрутизатор получил список аннулирования сертификатов (CRL) с указанием темы от сервера LDAP (облегченный протокол службы каталогов), IP-адрес и порт которого указаны в поле «Source» (Отправитель).
`Rcvd ARL <size>: <issuer name>`	Маршрутизатор получил список аннулирования полномочий (ARL) с указанием темы от сервера LDAP (облегченный протокол службы каталогов), IP-адрес и порт которого указаны в поле «Source» (Отправитель).
`Failed to decode the received ca cert`	Маршрутизатор получил недействительный сертификат центра сертификации от сервера LDAP, IP-адрес и порт которого указаны в поле «Source» (Отправитель).
`Failed to decode the received user cert`	Маршрутизатор получил недействительный сертификат пользователя от сервера LDAP, IP-адрес и порт которого указаны в поле «Source» (Отправитель).
`Failed to decode the received CRL`	Маршрутизатор получил недействительный список аннулирования сертификатов (CRL) от сервера LDAP, IP-адрес и порт которого указаны в поле «Source» (Отправитель).
`Failed to decode the received ARL`	Маршрутизатор получил недействительный список аннулирования полномочий (ARL) от сервера LDAP, IP-адрес и порт которого указаны в поле «Source» (Отправитель).
`Rcvd data <size> too large! Max size allowed: <max size>`	Маршрутизатор получил слишком большой объем данных справочника (с указанием размера) от сервера LDAP, IP-адрес и порт которого указаны в поле «Source» (Отправитель). Также указывается максимальный размер данных справочника, которые может пропустить маршрутизатор.
`Cert trusted: <subject name>`	Маршрутизатор сверил путь сертификата с указанной темой.
`Due to <reason codes>, cert not trusted: <subject name>`	В силу перечисленных причин сертификат с указанной темой не прошел сверку пути. Зарегистрированные коды отражают лишь примерные причины ненадежности сертификату. Соответствующие описания кодов приведены в Табл. 125 на с. 315.

Табл. 125 Коды причин непрохождения сверки путей сертификатов

КОД	ОПИСАНИЕ
1	Несоответствие алгоритмов в сертификате и критериях поиска.
2	Несоответствие при использовании ключей в сертификате и критериях поиска.
3	Сертификат был недействителен в данном интервале времени.
4	(Не используется)
5	Сертификат недействителен.
6	Подлинность подписи сертификата не была корректно проверена.
7	Сертификат входит в список аннулирования сертификатов (CRL).
8	Сертификат не был добавлен в кэш.

Табл. 125 Коды причин непрохождения сверки путей сертификатов (продолжение)

КОД	ОПИСАНИЕ
9	Не удалось декодировать сертификат.
10	Сертификат (нигде) не найден.
11	Замыкание цепи сертификатов (не найден доверенный корень).
12	Сертификат содержит критическое расширение, которое не было обработано.
13	Непроверенный издатель сертификата (отсутствуют сведения о центре сертификации).
14	(Не используется)
15	Слишком старый список аннулирования сертификатов (CRL).
16	Недействительный CRL.
17	Подлинность подписи CRL не была корректно проверена.
18	CRL (нигде) не найден.
19	CRL не был добавлен в кэш.
20	Не удалось декодировать CRL.
21	CRL будет действителен только в будущем.
22	CRL содержит дублируемые серийные номера.
23	Временной интервал не является непрерывным.
24	Нет сведений о времени.
25	Из-за истечения времени ожидания не удалось проверить подлинность методом баз данных.
26	Не удалось проверить подлинность методом баз данных.
27	Путь не проверен.
28	Достигнута максимальная длина пути.

Табл. 126 Настройка списка управления доступом (ACL)

НАПРАВЛЕНИЕ ПАКЕТОВ	НАПРАВЛЕНИЕ	ОПИСАНИЕ
(L to W)	LAN to WAN (лок. сеть – глоб. сеть)	Список управления доступом (ACL) для пакетов, пересылаемых из локальной сети (LAN) в глобальную (WAN).
(W to L)	WAN to LAN (глоб. сеть – лок. сеть)	Список управления доступом (ACL) для пакетов, пересылаемых из глобальной сети (WAN) в локальную (LAN).
(L to L)	LAN to LAN/P660HWP (локальная сеть – локальная сеть/ устройство ZyXEL)	Список управления доступом (ACL) для пакетов, пересылаемых из одной локальной сети (LAN) в другую локальную сеть (LAN) или в P660HWP.
(W to W)	WAN to WAN/P660HWP (глобальная сеть – глобальная сеть/ устройство)	Список управления доступом (ACL) для пакетов, пересылаемых из одной глобальной сети в другую или в P660HWP.

Табл. 127 Записи ICMP

ТИП	КОД	ОПИСАНИЕ
0		Эхо-ответ
	0	Сообщение с эхо-ответом
3		Адресат недоступен

Табл. 127 Записи ICMP

ТИП	КОД	ОПИСАНИЕ
	0	Сеть недоступна
	1	Узел недоступен
	2	Протокол недоступен
	3	Порт недоступен
	4	Пакет, который требует фрагментации, отброшен, так как имеет параметр DF (Don't Fragment – Не фрагментировать)
	5	Ошибка в маршруте источника
4		Источник произвел сброс
	0	Шлюз может сбросить дейтаграммы Интернет, если он не имеет буферной памяти, достаточной для организации очереди дейтаграмм, чтобы передать их в следующую сеть по маршруту к сети получателя.
5		Перенаправление
	0	Перенаправление дейтаграмм для сети
	1	Перенаправление дейтаграмм для узла
	2	Перенаправление дейтаграмм для типа услуги (ToS) и сети
	3	Перенаправление дейтаграмм для типа услуги (ToS) и узла
8		Эхо
	0	Эхо-сообщение
11		Время истекло
	0	Время жизни пакета истекло в пути
	1	Время на повторную сборку фрагментов истекло
12		Неверный параметр
	0	Указатель показывает на ошибку
13		Временная метка
	0	Сообщение с запросом временной метки
14		Ответ с временной меткой
	0	Ответное сообщение с временной меткой
15		Запрос параметров
	0	Сообщение с запросом параметров
16		Ответ на запрос параметров
	0	Сообщение с ответом на запрос параметров

Табл. 128 Сообщения системного журнала

СООБЩЕНИЕ	ОПИСАНИЕ
<Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="<msg>" note="<note>" devID="<mac address last three numbers>" cat="<category>	Это сообщение посылается системой («RAS» отображается в качестве системного имени, если оно не было присвоено), когда маршрутизатор создает запись в системном журнале. Эта функция устанавливается на странице: ГЛАВНОЕ МЕНЮ Web-конфигуратора->ЖУРНАЛЫ РЕГИСТРАЦИИ->Настройки журналов. Серьезность ошибки – это класс записи в системном журнале. Описание сообщений и записей определяются различными схемами записей в этом приложении. «devID» – это последние три символа MAC-адреса порта LAN маршрутизатора. «cat» – то же, что категория в журналах маршрутизатора.

В следующей таблице приводятся типы полезной информации в сообщениях протокола ISAKMP (см. RFC-2408) и их обозначения в журнале. Более подробную информацию по каждому типу см. в RFC.

Табл. 129 Типы данных сообщений RFC-2408 ISAKMP

ОБОЗНАЧЕНИЕ В ЖУРНАЛЕ	ТИП ПОЛЕЗНОЙ ИНФОРМАЦИИ
SA	Безопасное соединение
PROP	Предложение
TRANS	Преобразование
KE	Обмен ключами
ID	Идентификация
CER	Сертификат
CER_REQ	Запрос сертификата
HASH	Хеш
SIG	Подпись
NONCE	Сл. число
NOTFY	Уведомление
DEL	Удаление
VID	Идентификационный номер поставщика

21

Программные средства

В этой главе рассказывается о загрузке новой микропрограммы, управлении конфигурацией и перезагрузке интернет-центра P660HWP.

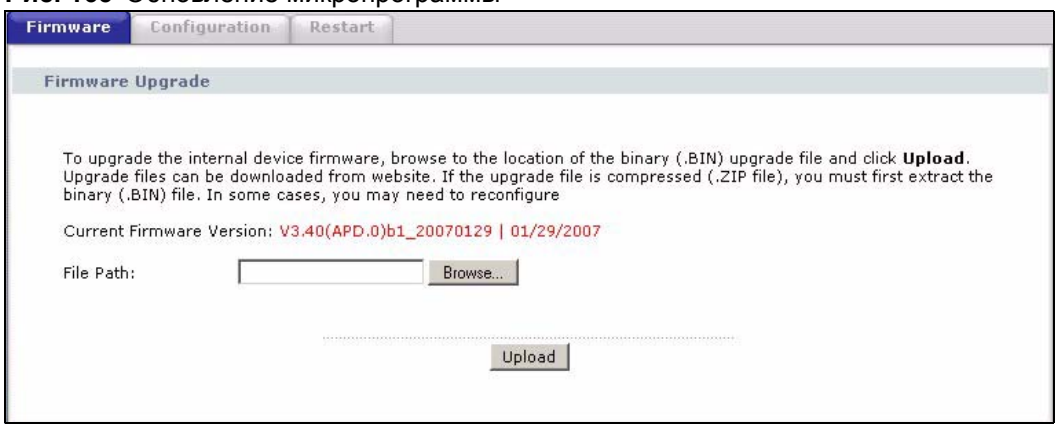
21.1 Обновление микропрограммы

Найдите программное обеспечение на сайте www.zyxel.ru в файле, в названии которого обычно используется название модели с расширением .bin, например, «P660HWP.bin». Для загрузки используется протокол HTTP (Hypertext Transfer Protocol – Протокол передачи гипертекста), загрузка может занять до 2-х минут времени. После успешной загрузки микропрограммы система перезапускается.

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

Щелкните **Maintenance (Сопровождение) > Tools (Программные средства)** для отображения окна **Firmware (Микропрограмма)**. Следуйте указаниям в этом окне для загрузки микропрограммы в интернет-центр P660HWP.

Рис. 165 Обновление микропрограммы



В следующей таблице даны описания полей этого окна.

Табл. 130 Обновление микропрограммы

ПОЛЕ	ОПИСАНИЕ
Current Firmware Version (Текущая версия микропрограммы)	Здесь отображается текущая версия и дата создания микропрограммы.
File Path (Путь к файлу)	Введите путь к файлу, который требуется загрузить, или нажмите кнопку **Browse... (Обзор)**, чтобы выполнить поиск файла.
Browse... (Обзор...)	Нажмите кнопку **Browse... (Обзор)**, для поиска файла с расширением .bin, который требуется загрузить. Не забудьте распаковать сжатые файлы (.ZIP), прежде чем загружать их.
Upload (Загрузить)	Нажмите кнопку **Upload (Загрузить)** для запуска процесса загрузки. Процесс загрузки может занять до 2 минут.

НЕЛЬЗЯ выключать питание P660HWP во время загрузки микропрограммы!

После появления окна **Firmware Upload in Progress (Выполняется загрузка микропрограммы)** подождите 2 минуты, прежде чем снова входить в программу P660HWP.

Рис. 166 Выполняется загрузка микропрограммы

P660HWP автоматически перезапускается, что вызывает временное отключение устройства от сети. В некоторых операционных системах на Рабочем столе может появиться следующая иконка.

Рис. 167 Временное отключение сети

По истечении 2 минут снова зарегистрируйтесь и проверьте версию новой микропрограммы в окне **System Status (Состояние системы)**.

Если загрузку не удалось завершить успешно, появляется следующее окно. Нажмите кнопку **Return (Возврат)** для возврата к окну **Firmware (Микропрограмма)**.

Рис. 168 Сообщение об ошибке

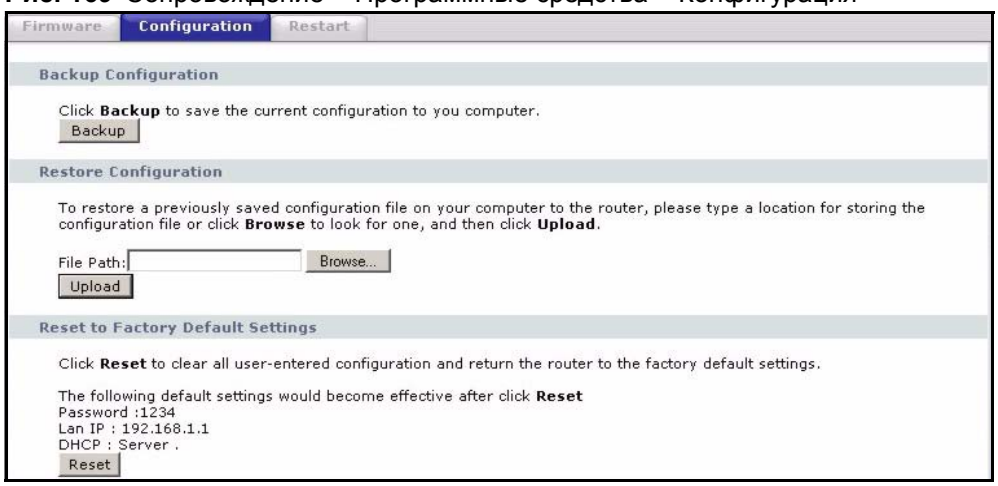
21.2 Окно конфигурации

Из этого окна можно управлять настройками вашего устройства.

21.2.1 Резервное сохранение конфигурации

Щелкните **Maintenance (Сопровождение) > Tools (Программные средства) > Configuration (Конфигурация)**. В этом окне отображается информация о заводских настройках по умолчанию, резервном сохранении и восстановлении конфигурации.

Рис. 169 Сопровождение > Программные средства > Конфигурация



Резервное сохранение конфигурации позволяет сохранить текущую конфигурацию P660HWP в файле на компьютере. Если настройка P660HWP выполнена, и устройство работает нормально, то перед внесением каких-либо изменений настоятельно рекомендуется создать резервную копию файла конфигурации. Файл с резервной копией конфигурации пригодится в случае, если Вам придется вернуться к предыдущим настройкам.

Табл. 131 Сопровождение > Программные средства > Конфигурация

ПОЛЕ	ОПИСАНИЕ
Backup Configuration (Резервное сохранение конфигурации)	
Backup (Резервное копирование)	Для сохранения текущей конфигурации на компьютере щелкните **Backup (Резервное копирование)**.
Restore Configuration (Восстановление конфигурации)	
Upload (Загрузить)	Восстановление конфигурации маршрутизатора путем загрузки предварительно сохраненного на компьютере файла конфигурации.
Reset to Factory Default Settings (Восстановление заводских настроек по умолчанию)	
Reset (Сброс)	Сброс всех пользовательских настроек и восстановление в маршрутизаторе заводских установок.

21.2.2 Восстановление конфигурации

Функция восстановления конфигурации позволяет загрузить с компьютера в P660HWP новый или предварительно сохраненный файл конфигурации.

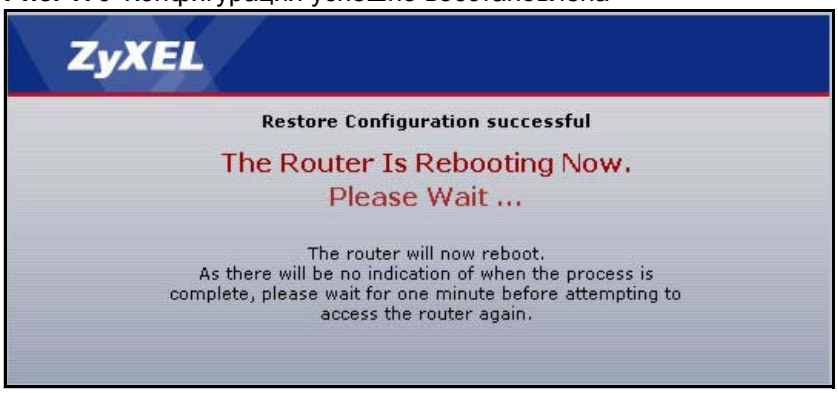
Табл. 132 Сопровождение: Восстановление конфигурации

ПОЛЕ	ОПИСАНИЕ
File Path (Путь к файлу)	Введите путь к файлу, который требуется загрузить, или нажмите кнопку **Browse... (Обзор)**, чтобы указать местонахождение файла.
Browse... (Обзор...)	Нажмите эту кнопку, чтобы найти файл для загрузки. Не забудьте распаковать сжатые файлы (.ZIP), прежде чем загружать их.
Upload (Загрузить)	Нажмите кнопку **Upload (Загрузить)** для запуска процесса загрузки.

НЕЛЬЗЯ выключать питание P660HWP во время загрузки файла конфигурации!

После появления окна **Restore Configuration successful (Конфигурация успешно восстановлена)**, необходимо подождать одну минуту, прежде чем снова регистрироваться в P660HWP.

Рис. 170 Конфигурация успешно восстановлена



P660HWP автоматически перезапускается, что вызывает временное отключение устройства от сети. В некоторых операционных системах на Рабочем столе может появиться следующая иконка.

Рис. 171 Временное отключение сети

При загрузке файла конфигурации по умолчанию необходимо изменить IP-адрес компьютера, чтобы он находился в той же подсети, что и IP-адрес P660HWP по умолчанию (192.168.1.1). Подробнее об установке IP-адреса компьютера см. в соответствующем приложении.

Если загрузку не удалось завершить успешно, появляется следующее окно. Нажмите кнопку **Return (Возврат)** для возврата к окну **Configuration (Конфигурация)**.

Рис. 172 Ошибка восстановления конфигурации

21.2.3 Восстановление заводских настроек по умолчанию

При нажатии кнопки **RESET (Сброс)** в этом разделе сбрасываются все измененные пользователем параметры, и настройки P660HWP возвращаются к заводским настройкам по умолчанию.

Возвращение настроек P660HWP к заводским настройкам по умолчанию также можно выполнить, нажав кнопку **RESET (Сброс)** на задней панели устройства. Дополнительную информацию о кнопке **RESET (Сброс)** см. в главе описания Web-конфигуратора.

21.3 Перезапуск

Это окно позволяет выполнить перезагрузку P660HWP без выключения электропитания.

Щелкните **Maintenance (Сопровождение) > Tools (Программные средства) > Restart (Перезапуск)**. Щелкните по кнопке **Restart (Перезапуск)** P660HWP для перезагрузки. Эта операция не влияет на конфигурацию P660HWP.

Рис. 173 Окно перезапуска

22

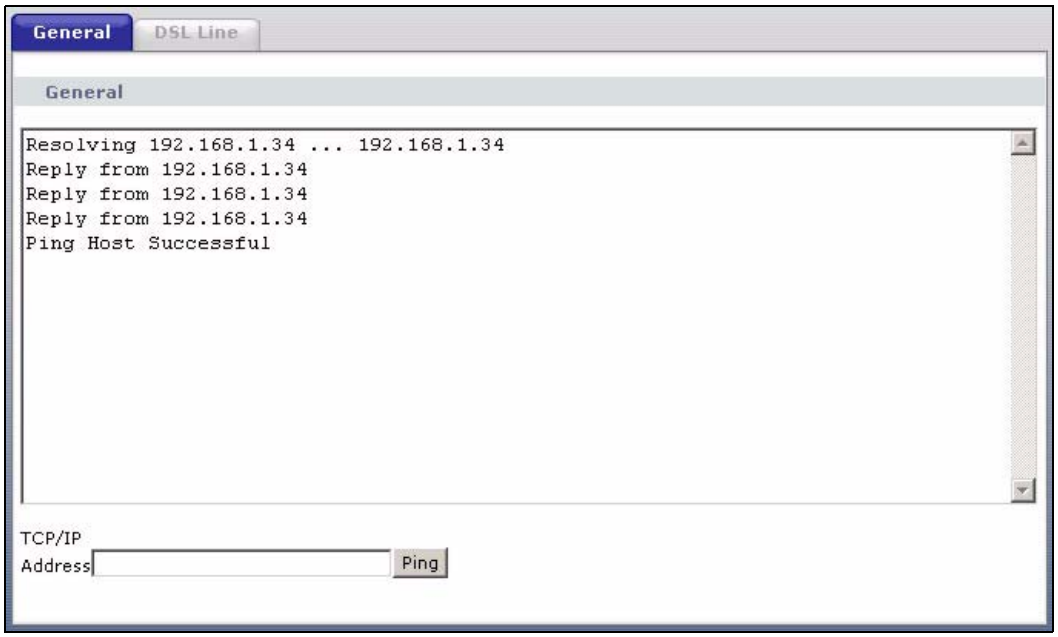
Диагностика

Информация в этих окнах представлена в режиме только для чтения и предназначена, чтобы помочь определить неисправность P660HWP.

22.1 Общая диагностика

Щелкните **Maintenance (Сопровождение) > Diagnostic (Диагностика)** для отображения окна, показанного ниже.

Рис. 174 Диагностика: Общая информация



В следующей таблице даны описания полей этого окна.

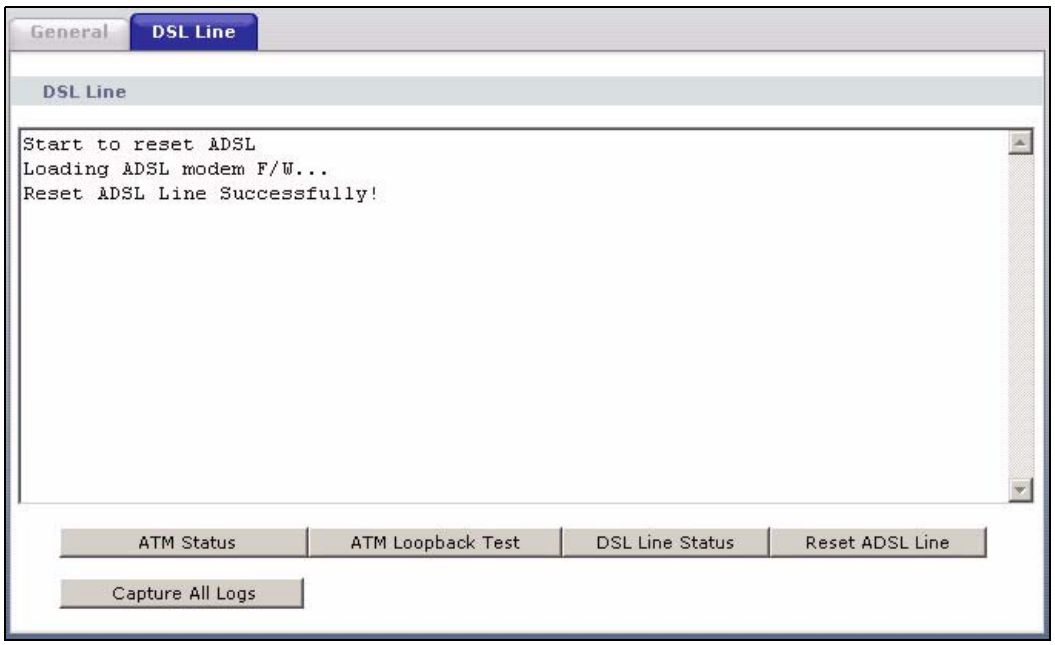
Табл. 133 Диагностика: Общая информация

ПОЛЕ	ОПИСАНИЕ
TCP/IP Address (Адрес TCP/IP)	Введите IP-адрес компьютера, который необходимо протестировать с помощью команды «ping», чтобы проверить соединение.
Ping (Эхо-тестирование)	Нажмите эту кнопку для тестирования устройства с введенным IP-адресом с помощью команды «ping».

22.2 Диагностика линии DSL

Щелкните **Maintenance (Сопровождение) > Diagnostic (Диагностика) > DSL Line (Линия DSL)** для отображения окна, показанного ниже.

Рис. 175 Диагностика: Линия DSL



В следующей таблице даны описания полей этого окна.

Табл. 134 Диагностика: Линия DSL

ПОЛЕ	ОПИСАНИЕ
ATM Status (Состояние ATM)	Нажмите на эту кнопку для отображения состояния ATM.
ATM Loopback Test (Кольцевой тест ATM)	Нажмите на эту кнопку для запуска кольцевого тестирования ATM. Прежде чем начать выполнение теста, убедитесь, что вы настроили хотя бы один канал PVC с соответствующими VPI/VCI. P660HWP посылает пакет OAM F5 на коммутатор DSLAM/ATM, после чего он возвращается обратно в P660HWP. Кольцевое тестирование ATM используется для поиска и устранения неисправностей в сети ATM.
DSL Line Status (Статус линии DSL)	Щелкните по этой кнопке для просмотра линейных рабочих величин и линейного побитового распределения порта DSL.
Reset ADSL Line (Сброс ADSL линии)	Нажмите эту кнопку, чтобы заново инициализировать ADSL линию. Тогда в большом текстовом поле сверху будет отображаться прохождение и результаты этой операции, например: "Start to reset ADSL Loading ADSL modem F/W... Reset ADSL Line Successfully!"
Capture All Logs (Показать все регистрационные записи)	Щелкните по этой кнопке для отображения всех регистрационных записей, сгенерированных линией DSL.

23

Поиск и устранение неисправностей

В этой главе рассказывается об устранении возмозможных неисправностей, которые могут появиться при работе с интернет-центром. Возможные неисправности можно разделить на следующие категории:

- Питание, подключение оборудования и светодиоды
- Доступ и регистрация в P660HWP
- Доступ в Интернет
- Проблемы использования технологии Powerline

23.1 Питание, подключение оборудования и светодиоды

? Адаптер P660HWP не включается. Ни один из светодиодов не включается.

1. Убедитесь, что P660HWP включен.
2. Убедитесь, что используется адаптер или кабель питания из комплекта поставки P660HWP.
3. Убедитесь, что адаптер или кабель питания подключен к P660HWP и к соответствующему источнику питания. Убедитесь, что источник питания включен.
4. Выключите и снова включите P660HWP.
5. Если неисправность не устраняется, свяжитесь с поставщиком оборудования.

? Один из светодиодов работает неправильно.

1. Убедитесь, что вы знаете, как светодиод должен работь в нормальном режиме. См. Разд. 1.4 на с. 38.
2. Проверьте подключение оборудования. См. Краткое руководство.
3. Убедитесь, что кабели не повреждены. Для замены поврежденных кабелей свяжитесь с поставщиком оборудования.
4. Выключите и снова включите P660HWP.

5 Если неисправность не устраняется, свяжитесь с поставщиком оборудования.

23.2 Доступ и регистрация в P660HWP

Потеряна информация об IP-адресе P660HWP.

1 IP-адрес, установленный изготовителем по умолчанию – 192.168.1.1.
2 Если IP-адрес был изменен и затем информация об этом утеряна, можно посмотреть IP-адрес P660HWP, установленный для шлюза по умолчанию на компьютере. Чтобы выполнить это на компьютере под управлением Windows, нажмите кнопку **Start (Пуск) > Run (Выполнить)**, введите команду **cmd** и затем **ipconfig**. IP-адрес **Default Gateway (Шлюз по умолчанию)** может являться IP-адресом интернет-центра P660HWP (это зависит от конкретной сети). Введите этот IP-адрес в Интернет браузере.
3 Если это не поможет, выполните сброс параметров устройства к заводским настройкам по умолчанию. См. Разд. 2.3 на с. 46.

Утерян пароль.

1 По умолчанию установлен пароль пользователя **user**. Пароль администратора по умолчанию – **1234**.
2 Если это не поможет, выполните сброс параметров устройства к заводским настройкам по умолчанию. См. Разд. 2.3 на с. 46.

Не отображается окно Web-конфигуратора Login (Регистрация) или отсутствует доступ в систему.

1 Убедитесь, что используется правильный IP-адрес.
   - IP-адрес, установленный изготовителем по умолчанию – 192.168.1.1.
   - Если IP-адрес был изменен (Разд. 6.2.1 на с. 105), используйте новый IP-адрес.
   - Если IP-адрес был изменен и затем утерян, см. рекомендации по поиску и устранению неисправностей в разделе Потеряна информация об IP-адресе P660HWP.
2 Проверьте подключение оборудования и удостоверьтесь, что светодиоды работают в нормальном режиме. См. Краткое руководство.
3 Убедитесь, что в Интернет-браузере включена поддержка всплывающих окон, а также JavaScripts и Java. См. Прил. H на с. 411.

4 Если функция «Any IP» (Любой IP) (Разд. 6.2.4 на с. 108) отключена, проверьте, что компьютер находится в той же подсети, что и P660HWP (пропустите этот шаг, если известно, что между компьютером и P660HWP имеются маршрутизаторы.)
   - Если в вашей сети есть сервер DHCP, убедитесь, что ваш компьютер использует динамический IP-адрес. См. Разд. 6.2.1 на с. 105. По умолчанию устройство P660HWP выполняет функцию DHCP-сервера.
   - Если в вашей сети нет другого сервера DHCP, убедитесь, что IP-адреса компьютеров входят в ту же подсеть, что и P660HWP. См. Разд. 6.2.1 на с. 105.
5 Выполните сброс устройства к заводским настройкам по умолчанию и попробуйте получить доступ к P660HWP с IP-адресом по умолчанию. См. Разд. 2.3 на с. 46.
6 Если неисправность не устраняется, обратитесь к сетевому администратору или поставщику оборудования, или выполните дополнительные рекомендации.

Дополнительные советы

- Попробуйте получить доступ к P660HWP с использованием другой службы, например, Telnet. Если доступ к P660HWP существует, проверьте параметры удаленного управления и правила межсетевого экрана, чтобы выяснить причину, по которой P660HWP не отвечает по HTTP.
- Если ваш компьютер не подключен к порту **WAN** или подключен по беспроводной связи, используйте компьютер, подключенный к порту **LAN/ETHERNET**.

Окно Login (Вход в систему) отображается, но невозможно выполнить вход в систему P660HWP.

1 Проверьте, что имя пользователя и пароль введены правильно. По умолчанию установлен пароль **1234**. Символы в это поле вводятся с учетом регистра, поэтому убедитесь, что клавиша [Caps Lock] выключена.
2 Нельзя получить доступ к Web-конфигуратору, если другой пользователь подключился к P660HWP через Telnet. Подключитесь к P660HWP позднее или попросите зарегистрированного пользователя выполнить выход из системы.
3 Выключите и снова включите P660HWP.
4 Если это не поможет, выполните сброс параметров устройства к заводским настройкам по умолчанию. См. Разд. 2.3 на с. 46.

Невозможно подключиться к P660HWP через Telnet.

См. рекомендации по поиску и устранению неисправностей в разделе Не отображается окно Web-конфигуратора Login (Регистрация) или отсутствует доступ в систему. Рекомендации по настройке браузера сюда не относятся.

Невозможно выполнить загрузку/скачивание файла конфигурации с помощью FTP. / Не удается загрузить новую версию микропрограммы с помощью FTP.

См. рекомендации по поиску и устранению неисправностей в разделе Не отображается окно Web-конфигуратора Login (Регистрация) или отсутствует доступ в систему. Рекомендации по настройке браузера сюда не относятся.

23.3 Доступ в Интернет

Невозможно получить доступ в Интернет.

1. Проверьте подключение оборудования и удостоверьтесь, что светодиоды работают в нормальном режиме. См. Краткое руководство и Разд. 1.4 на с. 38.
2. Если информацию об Интернет-подключении вы получаете от своего провайдера, убедитесь, что вы указали ее в окне **Network (Сеть)** > **WAN (Глобальная сеть)** > **Internet Connection (Подключение к Интернету)**. Символы в эти поля вводятся с учетом регистра, поэтому убедитесь, что клавиша [Caps Lock] выключена.
3. Если вы пытаетесь подключиться к сети Интернет по беспроводной связи, убедитесь, что клиентские настройки беспроводного клиента совпадают с настройками в точке доступа.
4. Отключите все кабели от устройства и еще раз выполните инструкции Краткого руководства.
5. Если неисправность не устраняется, обратитесь к интернет-провайдеру.

Не удается воспользоваться функцией передачи голоса через Интернет (VoIP) с помощью устройства P660HWP.

1. Проверьте подключение. Убедитесь, что нужные светодиоды работают в нормальном режиме (см. Разд. 1.4 на с. 38).
2. Убедитесь в правильности настройки учетной записи VoIP.
3. При использовании трансляции сетевых адресов (NAT) убедитесь, что включена функция **Enable SIP ALG (Включить SIP ALG)** в окне **NAT** > **General (Общие)**. См. Разд. 9.2 на с. 156.
4. Убедитесь, что на вашем устройстве VoIP отключена функция STUN.
5. При использовании новой учетной записи VoIP обратитесь к своему провайдеру Интернет-телефонии (ITSP) с просьбой подтвердить ее активацию.

Невозможно получить доступ в Интернет. Доступ в Интернет настроен через P660HWP, но подключение к Интернету больше не работает.

1. Проверьте подключение оборудования и удостоверьтесь, что светодиоды работают в нормальном режиме. См. Краткое руководство и Разд. 1.4 на с. 38.
2. Перезагрузите P660HWP.
3. Выключите и снова включите P660HWP.
4. Если неисправность не устраняется, обратитесь к интернет-провайдеру.

Подключение к Интернету работает медленно или нестабильно.

1. Возможно, что локальная сеть перегружена. Посмотрите на светодиоды и проверьте их работу согласно Разд. 1.4 на с. 38. Если интернет-центр P660HWP посылает и передает большие объемы информации, закройте программы, которые используют Интернет, особенно равноправные приложения.
2. Перезагрузите P660HWP.
3. Выключите и снова включите P660HWP.
4. Если неисправность не устраняется, обратитесь к сетевому администратору или поставщику оборудования, или выполните дополнительные рекомендации.

Дополнительные советы

- Проверьте настройки управления полосой пропускания. Если управление отключено, попробуйте его включить. Если включено, попробуйте изменить распределение.

23.4 Проблемы использования технологии Powerline

Не удается включить Powerline-устройство.

1. Проверьте источник питания. Питание Powerline-адаптеры получают из домашней электросети и не могут работать при отсутствии в ней напряжения.
2. Убедитесь, что для подключения к электрической розетке P660HWP используется шнур питания, входящий в комплект с P660HWP. Обычные штепсельные вилки для этого не подходят.
3. Вытащите штепсельную вилку устройства P660HWP из розетки. Включите в эту розетку другое рабочее электрическое устройство. Тем самым вы проверите наличие напряжения в ней.
4. Попробуйте подключить другой адаптер HomePlug AV к смежной розетке к P660HWP и проверьте, загорится ли светодиод **LINK**. Тем самым вы проверите, может ли устройство P660HWP обнаружить другие Powerline-адаптеры в вашей электрической цепи.

Не удается подключиться к Powerline-сети.

1. Убедитесь, что все устройства подключены к одной электрической линии.
2. Убедитесь, что сеть не разделена ваттметром. Сигналы Powerline не могут пройти через него.
3. Убедитесь, что все используемые Powerline-адаптеры соответствуют стандарту HomePlug AV. Устройство P660HWP HE распознает более ранние версии Powerline-адаптеров стандарта HomePlug, например, HomePlug 1.0 или 1.0.1 (однако они могут работать в одной сети независимо друг от друга.)
4. Убедитесь, что на всех Powerline-адаптерах установлен одинаковый сетевой пароль.

Слабый сигнал в Powerline-сети.

1. Не подключайте устройства через сетевые фильтры, т.к. они могут снижать Powerline-сигнал.
2. Не подключайте Powerline-устройства рядом с приборами большой мощности, например, холодильниками или кондиционерами.
3. Во избежание интерференции сигналов, не включайте рядом с Powerline-устройствами приборы для отпугивания насекомых.
4. Избегайте использования старой, низкокачественной или слишком длинной проводки, т.к. это может повлиять на качество Powerline-сигнала.

Часть VII
Приложения и алфавитный указатель

A

Характеристики и крепление на стену

Характеристики устройства

В следующей таблице представлены характеристики оборудования и программного обеспечения P660HWP.

Табл. 135 Технические характеристики оборудования

Размеры (Ш × Г × В)	250 x 170 x 36 мм
Питание	Вход: 100-240 В, 50-60 Гц Выход: 12В, 1А
Встроенный коммутатор	Четыре порта Ethernet MDI/MDI-X 10/100 Мбит/с RJ-45 с автоматическим выбором скорости
Рабочая температура	0ºC ~ 40ºC
Температура хранения	-20ºC ~ 60ºC
Рабочая влажность	20% ~ 85%
Влажность при хранении	10% ~ 90%
Расстояние между центрами отверстий на задней панели устройства (для настенного монтажа).	215,5 мм
Размер саморезов для настенного крепления	Саморез M4
Антенна	Устройство P660HWP оборудовано съемной антенной мощностью 3 дБ.

Табл. 136 Характеристики программного обеспечения

ФУНКЦИЯ	ОПИСАНИЕ
IP-адрес по умолчанию	192.168.1.1
Маска подсети по умолчанию	255.255.255.0 (24 бита)
Стандартный пароль администратора (Admin Password)	1234
Стандартный пароль пользователя (User Password)	user
Диапазон DHCP	От 192.168.1.33 до 192.168.1.64

Табл. 136 Характеристики программного обеспечения

ФУНКЦИЯ	ОПИСАНИЕ
Управление устройством	Веб-конфигуратор упрощает настройку широкого спектра функций устройства P660HWP.
Обновление микропрограммы	Загрузите новую версию микропрограммы (если есть) с Web-сайта ZyXEL в интернет-центр P660HWP с помощью Web-конфигуратора, по FTP или TFTP. **Примечание: Необходимо загружать микропрограмму строго в соответствии с конкретной моделью устройства.**
Резервное сохранение и восстановление конфигурации	Сделайте копию конфигурации P660HWP. Эту копию можно загрузить в P660HWP позже, если потребуется вернуться к предыдущей конфигурации.
Трансляция сетевых адресов (NAT)	Каждый компьютер в сети должен иметь уникальный IP-адрес. Используйте функцию NAT для преобразования общедоступного IP-адреса(ов) в несколько частных IP-адресов для компьютеров вашей сети.
Переадресация портов	Если в сети есть сервер (например, Web-сервер или сервер электронной почты), с помощью этой функции можно разрешить доступ к нему пользователям из Интернета.
DHCP (Протокол динамической настройки узла)	С помощью этой функции интернет-центр P660HWP назначает IP-адреса, шлюз IP по умолчанию и серверы DNS компьютерам локальной сети.
Поддержка динамических DNS	Поддержка динамической DNS (Domain Name System – Система доменных имен) позволяет использовать фиксированный URL, например, www.zyxel.com с динамическим IP-адресом. Для использования этой услуги необходимо зарегистрироваться у провайдера услуг динамической DNS.
Поддержка стандарта HomePlug AV	Стандарт HomePlug AV определяет взаимодействие сетевых устройств по стандартной электрической сети. Он поддерживает скорость передачи данных до 200 Мбит/с. Данные при этом шифруются по алгоритму 128-битного канального шифрования AES. Устройства с поддержкой стандарта HomePlug AV могут работать одновременно с устройствами, работающими по стандарту HomePlug 1.0, однако между собой они не совместимы. Радиус действия сети стандарта HomePlug AV составляет 300 м. Стандарт совместим со всеми ОС
Многоадресная рассылка IP	Многоадресная рассылка IP используется для отправки трафика определенной группе компьютеров. Интернет-центр P660HWP поддерживает версии 1 и 2 протокола IGMP (Internet Group Management Protocol – протокол управления группами в сети Интернет), который используется для присоединения к группам многоадресной рассылки (см. RFC 2236).
Псевдоним IP	Псевдоним IP позволяет разделить физическую сеть на логические подсети на одном интерфейсе Ethernet, при этом P660HWP действует как шлюз для каждой подсети.
Время и дата	Можно синхронизировать текущее время и дату с внешним сервером времени при включении питания P660HWP. Время также можно установить вручную. Дата и время используются в регистрационных журналах.
Протоколирование и трассировка	Для диагностики неисправностей можно использовать пакетную трассировку и журналы. Устройство P660HWP позволяет отправлять журналы на внешний сервер хранения системных журналов.

Табл. 136 Характеристики программного обеспечения

ФУНКЦИЯ	ОПИСАНИЕ
PPPoE	PPPoE имитирует коммутируемое соединение для доступа в Интернет.
Инкапсуляция PPTP	PPTP (Point-to-Point Tunneling Protocol – Протокол туннелирования «точка-точка») обеспечивает безопасную передачу данных по VPN (Virtual Private Network – Виртуальная частная сеть). Интернет-центр P660HWP поддерживает одно соединение PPTP одновременно.
Универсальная функция «Plug and Play» (UPnP)	Устройство UPnP может динамически присоединяться к сети, получать IP-адрес, сообщать о своих функциях и собирать информацию о других устройствах сети.
Межсетевой экран	Чтобы обезопасить доступ в Интернет, на устройстве P660HWP можно включить межсетевой экран. По умолчанию, когда межсетевой экран включен, весь входящий трафик из Интернет к локальной сети блокируется, если он не инициирован из этой локальной сети. Это значит, что внешнее зондирование вашей сети блокируется, но при этом Вы можете безопасно просматривать Интернет-сайты и загружать файлы.
Контент-фильтр	Устройство P660HWP блокирует или разрешает просмотр указанных веб-сайтов с URL, содержащими определенные ключевые слова. Можно указать периоды времени, в течение которых будет работать контент-фильтр. Кроме того, можно указать компьютеры, чей трафик следует фильтровать или, наоборот, не фильтровать. Помимо этого можно подписаться на фильтрацию по категориям, которая позволяет устройству P660HWP проверять веб-сайты по внешней базе данных.
Управление пропускной способностью	Для определенных типов трафика и определенных компьютеров вашей сети можно зарезервировать полосу пропускания и задать им приоритет для повышения эффективности управления трафиком.
Удаленное управление	Удаленное управление позволяет с помощью выбранной службы (например, HTTP или FTP) с компьютера в сети (LAN или WAN) подключиться к P660HWP.
Совместимость с протоколом TR-069	TR-069 – это протокол, позволяющий управлять P660HWP через управляющий сервер, например, через систему централизованного управления Vantage CNM ZyXEL. С помощью управляющего сервера можно безопасно выполнять управление интернет-центром и производить изменения в конфигурации устройства.
Any IP (Любой IP)	Функция «Any IP» (Любой IP) позволяет компьютерам из разных подсетей подключаться к устройству P660HWP (а затем к другим компьютерам). Это происходит без изменения параметров сети (например, IP-адреса и маски подсети) на компьютере.
Перенаправление трафика (Traffic Redirect)	Функция перенаправления трафика автоматически направляет трафик WAN к резервному шлюзу LAN, если P660HWP не может установить соединение с Интернетом, выполняя, таким образом, функции дополнительного резервирования в случае невозможности подключения к WAN обычным образом.
Услуга «три в одном» (голос + данные + видео)	Устройство P660HWP поддерживает одновременную передачу данных, голоса и видео через сеть Интернет.
Политика маршрутизации IP (IPPR)	Как правило, маршрутизация производится только на основе адреса получателя, поэтому маршрутизатор выбирает самый короткий путь для пересылки пакета. Политика маршрутизации IP (IP Policy Routing – IPPR) обеспечивает механизм замены схемы маршрутизации по умолчанию и позволяет изменить алгоритм прохождения пакетов на основе политики, определяемой сетевым администратором.

Табл. 137 Характеристики программного обеспечения беспроводной связи

ФУНКЦИЯ	ОПИСАНИЕ
Беспроводная локальная сеть (Wireless LAN)	Устройство P660HWP полностью совместимо со стандартами IEEE 802.11b и IEEE 802.11g и может поддерживать клиентов обоих типов в одной сети.
WEP-шифрование	При использовании WEP (Wired Equivalent Privacy – протокол шифрования беспроводной связи) пакеты данных шифруются перед отправкой по сети.
Защищенный доступ Wi-Fi (WPA)	Стандарт WPA2, как часть стандарта IEEE 802.11, обеспечивает идентификацию пользователей и шифрование данных.
WPA2	WPA2 – это расширение стандарта WPA, позволяющее выполнять усовершенствованное шифрование данных, идентификацию пользователей и управление ключами.
WPA2-PSK	WPA(2)-PSK: WPA-PSK и WPA2-PSK позволяют выполнять более совершенное шифрование по стандартам WPA и WPA2 без использования сервера RADIUS (службы дистанционной аутентификации пользователей по коммутируемым линиям). Вместо этого в WPA(2)-PSK для идентификации устройств в беспроводной сети используются общие ключи (PSK).
Управление выходной мощностью	Позволяет изменять уровень мощности устройства P660HWP. К примеру, это может быть полезно при близком расположении точек доступа.
Фильтрация MAC-адресов беспроводной ЛВС	Фильтрует подключения по списку разрешенных и запрещенных MAC-адресов.

Далее приводится не полный список стандартов, поддерживаемых устройством P660HWP.

Табл. 138 Стандарты, поддерживаемые устройством

СТАНДАРТ	ОПИСАНИЕ
RFC 867	Протокол Daytime
RFC 868	Протокол Time
RFC 1058	RIP-1 (Routing Information Protocol – Протокол обмена информацией о маршрутизации)
RFC 1112	IGMP v1 (Internet Group Management Protocol – Межсетевой протокол управления группами)
RFC 1157	SNMPv1 (Simple Network Management Protocol – Простой протокол управления сетью) версии 1
RFC 1305	Протокол сетевого времени (NTP версии 3)
RFC 1332	Управляющий протокол для IP (IPCP)
RFC 1334	Протокол аутентификации по паролю (PAP)
RFC 1441	SNMPv2 (Simple Network Management Protocol – Простой протокол управления сетью) версии 2
RFC 1483	Многопротокольная инкапсуляция поверх адаптации ATM, уровень 5
RFC 1631	Трансляция сетевых IP-адресов (NAT)
RFC 1661	Протокол «точка-точка» (PPP)
RFC 1723	RIP-2 (Routing Information Protocol – Протокол обмена информацией о маршрутизации)
RFC 1994	Протокол аутентификации с предварительным согласованием вызова (CHAP)
RFC 2236	SNMPv2 (Simple Network Management Protocol – Простой протокол управления сетью версии 2)
RFC 2364	Протокол «точка-точка» поверх уровня адаптации AAL, уровень 5 (PPP через ATM через ADSL)

Табл. 138 Стандарты, поддерживаемые устройством (продолжение)

СТАНДАРТ	ОПИСАНИЕ
RFC 2408	Протокол интернет-безопасности и протокол управления ключами (ISAKMP)
RFC 2516	Метод передачи от точки к точке через сеть Интернет (PPPoE)
RFC 2684	Многопротокольная инкапсуляция поверх адаптации ATM, уровень 5
RFC 2766	Протокол трансляции сетевых адресов (NAT)
RFC 2865	Сервис удалённой аутентификации звонящего
IEEE 802.11	Известный как Wi-Fi, он определяет набор стандартов беспроводной локальной или глобальной связи, определенный рабочей группой 11 комитета стандартизации IEEE LAN/MAN (IEEE 802).
IEEE 802.11b	Использует диапазон частот 2,4 гигагерц (ГГц)
IEEE 802.11g	Использует диапазон частот 2,4 гигагерц (ГГц)
IEEE 802.11g+	Режимы Turbo и Super G
IEEE 802.11d	Стандарты локальных сетей и сетей уровня города: мосты протокола управления доступом к среде передачи (MAC)
IEEE 802.11e QoS	Стандарт беспроводной локальной связи IEEE 802.11 e для качества обслуживания
IEEE 802.11i	WPA2
IEEE 802.1x	Контроль доступа в сеть через порты
ANSI T1.413, изд. 2	Стандарт асимметричной цифровой абонентской линии (ADSL).
G dmt(G.992.1)	Трансиверы стандарта асимметричной цифровой абонентской линии (ADSL) G.992.1
ITU G.992.1 (G.DMT)	Стандарт международного союза по электросвязи для ADSL с использованием цифровой многоканальной тональной модуляции.
ITU G.992.3 (G.dmt.bis)	Стандарт международного союза по электросвязи (также называемый ADSL 2), разрешающий более высокие скорости передачи данных, чем ADSL.
ITU G.992.5 (ADSL 2+)	Стандарт международного союза по электросвязи (также называемый ADSL 2+), обеспечивающий вдвое количество входящих битов.
Microsoft PPTP	MS PPTP (протокол туннелирования между узлами в версии от Microsoft)
MBM v2	Управление пропускной способностью среды передачи версии 2
RFC 2383	ST2+ через спецификацию протокола ATM – версии UNI 3.1
TR-069	Стандарт форума DSL TR-069 для управления оборудованием глобальной связи, расположенным на территории клиента.
1.363.5	Совместимый с уровнем AAL5 подуровень сегментации и сборки (SAR)

Инструкции по настенному монтажу

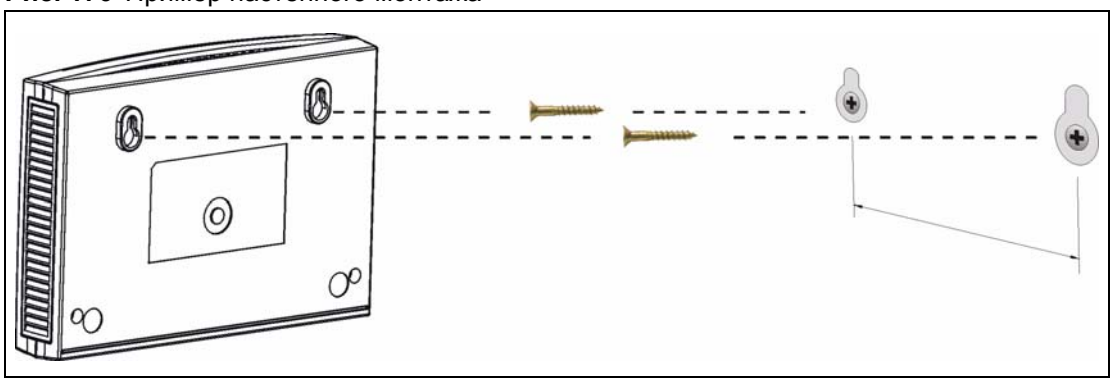
Для установки адаптера P660HWP на стене выполните следующие действия.

Размер используемых саморезов и расстояние между центрами см. в таблице технических характеристик аппаратного обеспечения.

1. Найдите на стене свободное место, расположенное на достаточной высоте.
2. Просверлите два отверстия под саморезы.

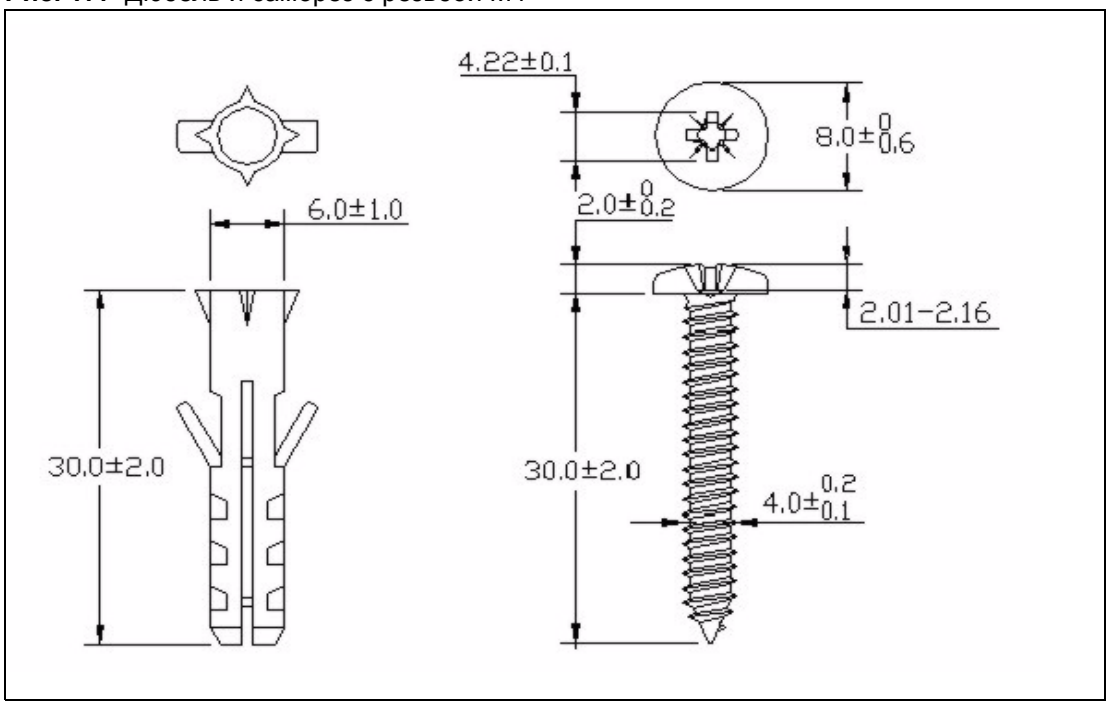
3 При сверлении не повредите проходящие внутри стены трубы и скрытую проводку.
4 Саморезы закручивайте в стену не полностью, Оставьте небольшой зазор (около 5 мм) между головками саморезов и стеной.
5 Убедитесь, что саморезы надежно закреплены в стене. Они должны выдерживать вес устройства P660HWP и соединительных проводов.
6 Совместите отверстия на задней панели устройства P660HWP с саморезами в стене. Повесьте адаптер P660HWP на саморезы.

Рис. 176 Пример настенного монтажа



Далее указаны размеры самореза M4 и дюбеля (используются для настенного монтажа). Все размеры даны в миллиметрах (мм).

Рис. 177 Дюбель и саморез с резьбой M4



B

Беспроводные локальные сети

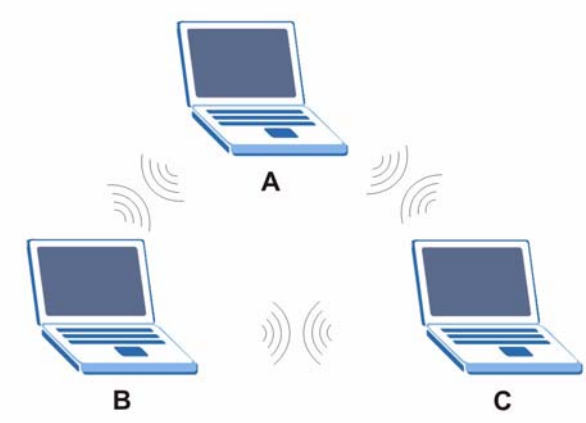
Топологии беспроводных локальных сетей

В этом разделе описаны временные (Ad-hoc) и фиксированные топологические схемы беспроводных локальных сетей.

Конфигурация временной (Ad-hoc) беспроводной локальной сети

Простейшей конфигурацией беспроводной локальной вычислительной сети (WLAN) является независимая сеть Ad-hoc, объединяющая группу компьютеров, оснащенных беспроводными адаптерами (A, B, C). Когда два или более беспроводных адаптеров попадают в зону действия друг друга, они могут образовать независимую сеть, обычно называемую «временной сетью» (Ad-hoc network) или «независимым базовым набором служб» (Independent Basic Service Set, IBSS). На приведенной диаграмме показан пример, где несколько ноутбуков используют беспроводные адаптеры для образования временной (Ad-hoc) беспроводной локальной сети.

Рис. 178 Одноранговая связь во временной (Ad-hoc) беспроводной сети

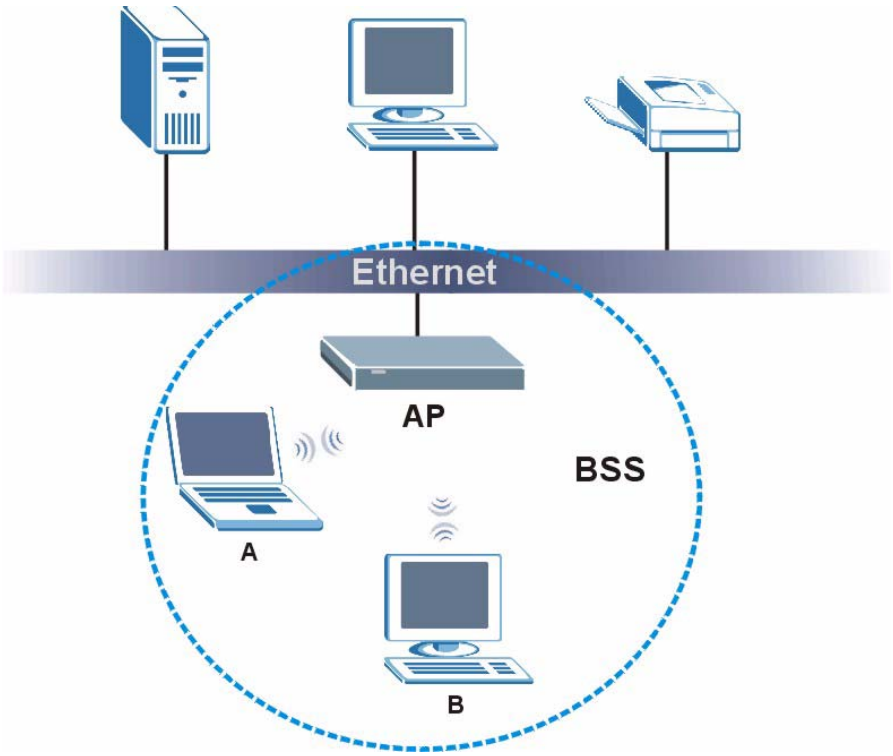


BSS

BSS (Basic Service Set – Базовый набор служб) используется, если весь трафик между беспроводными устройствами или между беспроводным устройством и клиентом проводной сети передается через одну точку доступа.

Трафик Intra-BSS – это трафик между беспроводными клиентами в пределах одного базового набора служб. При активации Intra-BSS трафика беспроводные клиенты **A** и **B** могут получить доступ к проводной сети и обмениваться информацией между собой. При отключении трафика Intra-BSS беспроводные клиенты **A** и **B** все равно могут получить доступ к проводной сети, однако не могут обмениваться информацией между собой.

Рис. 179 Базовый набор служб



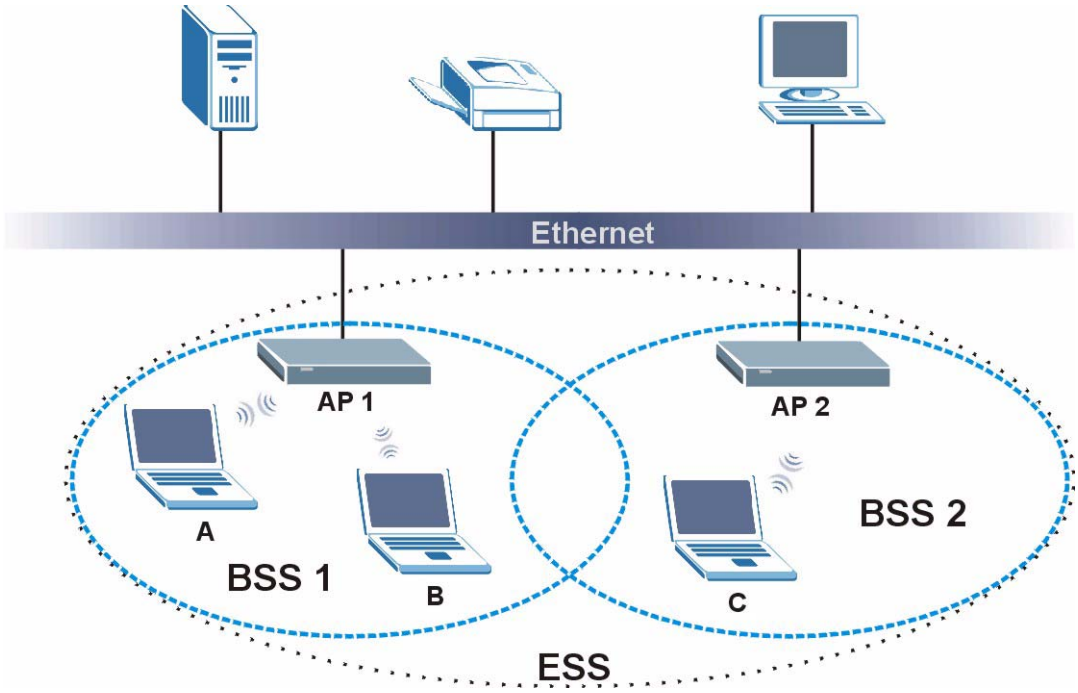
ESS

Расширенный набор служб (ESS) состоит из нескольких перекрывающихся базовых наборов служб (BSS), каждый из которых имеет точку доступа, а точки доступа связаны проводной сетью. Это проводное соединение точек доступа называется системой распределения (Distribution System, DS).

Этот тип беспроводной топологической организации локальной сети называется фиксированной беспроводной локальной сетью (Infrastructure WLAN). Точки доступа не только обеспечивают связь с проводной сетью, но и служат связующим звеном для трафика беспроводной локальной сети в непосредственном окружении.

Каждый ESS идентифицируется уникальным идентификатором (ESSID). Все точки доступа и связанные с ними беспроводные клиенты в одном наборе ESS должны иметь одинаковый идентификатор ESSID.

Рис. 180 Фиксированная беспроводная сеть



Канал

Канал представляет собой радиочастоту(ы), используемую(ые) беспроводными устройствами IEEE 802.11b/g. Доступность каналов зависит от географического положения. В некоторых регионах каналов может быть несколько, поэтому для снижения уровня помех следует использовать канал, отличающийся от канала ближайшей точки доступа. Помехи появляются при перекрывании радиосигналов от разных точек доступа, при этом ухудшается качество сигнала.

Однако смежные каналы частично перекрываются. Во избежание помех из-за перекрывания, канал точки доступа (AP) должен отстоять по крайней мере на пять каналов от частот, которые используют смежные точки доступа. Например, если в регионе действуют 11 каналов и смежная точка доступа использует канал 1, то Вам необходимо выбрать канал 6 или 11.

RTS/CTS (Запрос на передачу/Подтверждение готовности к приему)

«Скрытый» узел – это ситуация, когда два устройства находятся в рабочей зоне одной и той же точки доступа, но вне рабочих зон друг друга. Следующий рисунок иллюстрирует ситуацию «скрытого» узла. Оба устройства (STA) находятся в рабочей зоне точки доступа (AP) или беспроводного шлюза, но вне рабочих зон друг друга, поэтому они не могут «слышать» друг друга, т. е. они не знают, используется ли в данный момент канал. Поэтому они считаются скрытыми друг от друга.

Рис. 181 RTS/CTS

Когда устройство **A** посылает данные в точку доступа, оно может не знать, что устройство **B** уже использует этот канал. Если эти два устройства послали данные одновременно, может произойти конфликт, при котором обе партии данных достигают AP одновременно, результатом чего является потеря сообщений от обоих устройств.

RTS/CTS предназначен для предотвращения конфликтов из-за невидимых узлов. **RTS/CTS** определяет максимальный размер кадра данных, который можно отправить до квитирования (отправки запроса на передачу (RTS) и последующего получения подтверждения готовности к приему (CTS)).

Если кадр данных превышает значение **RTS/CTS**, установленное в диапазоне от 0 до 2432 байт, устройство, которое хочет передать этот кадр, должно вначале послать сообщение RTS (Request To Send – Запрос на передачу) точке доступа (AP) для получения разрешения на пересылку. Затем AP отвечает сообщением CTS (Clear to Send – Готовность к приему) всем другим устройствам в рабочей зоне, извещая их о необходимости задержки передачи данных. Для устройства, отправлявщего запрос, это сообщение одновременно подтверждает временные рамки, отведенные на передачу данных.

Кадры, меньше указанных в **RTS/CTS**, устройства могут посылать непосредственно в AP без квитирования (отправки запроса на передачу (RTS) и последующего получения подтверждения готовности к приему (CTS)).

Настройка **RTS/CTS** необходима только в случае, если существует вероятность наличия «скрытых» узлов в сети, а расходы на повторную отправку больших фрагментов оказываются больше, чем дополнительные сетевые издержки в связи с запросом разрешения на сеанс связи RTS (Request To Send – Запрос на передачу)/CTS(Clear to Send – Готовность к приему).

Если значение **RTS/CTS** превышает значение **порога фрагментации** (см. далее), квитирование RTS (Request To Send – Запрос на передачу)/CTS (Clear to Send – Готовность к приему) не будет иметь места, так как кадры данных будут фрагментированы до того, как достигнут размера **RTS/CTS**.

Включение порога RTS влечет за собой лишние сетевые издержки, которые зачастую негативно сказываются на пропускной способности, а не меняют ситуацию к лучшему.

Порог фрагментации

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

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

Если значение **порога фрагментации** меньше установленного значения **RTS/CTS** (см. ранее), квитирование RTS/CTS не будет иметь места, так как кадры данных будут фрагментированы до того как достигнут размера **RTS/CTS**.

Тип заголовка

Заголовок используется для уведомления о приходе данных к получателю. Параметры **Short (Короткий заголовок)** и **Long (Длинный заголовок)** относятся к длине поля синхронизации пакета.

Использование коротких заголовков увеличивает эффективность, так как меньшее время, затраченное на отправку заголовка, дает больше времени на отправку данных. Все IEEE 802.11b/g-совместимые беспроводные адаптеры поддерживают длинные заголовки, но не все поддерживают короткие.

Выберите **Long (Длинный заголовок)**, если неизвестно, какой режим заголовков поддерживают беспроводные адаптеры, а также для обеспечения более надежной связи в загруженных беспроводных сетях.

Выберите **Short (Короткий заголовок)**, если Вы уверены, что этот режим заголовков поддерживается беспроводными адаптерами, а также для обеспечения большей пропускной способности.

Выберите **Dynamic (Динамический)**, чтобы точка доступа автоматически использовала короткий заголовок, если он поддерживается всеми беспроводными адаптерами в сети. В другом случае точка доступа будет использовать длинный заголовок.

Точка доступа и беспроводные устройства ДОЛЖНЫ использовать один и тот же режим заголовков.

Беспроводные локальные сети стандарта IEEE 802.11g

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

Табл. 139 IEEE 802.11g

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

Защита беспроводной сети – общая информация

Безопасность беспроводных соединений имеет важное значение для безопасности всей сети. Необходимо обеспечивать защиту связи между беспроводными клиентами, точками доступа и проводной сетью.

Методы защиты беспроводной сети, предлагаемые интернет-центром P660HWP, включают шифрование данных, аутентификацию беспроводных клиентов, ограничение доступа по MAC-адресам устройств и скрытие беспроводной сети от обнаружения P660HWP.

На приведенном ниже рисунке показана сравнительная эффективность методов защиты беспроводных сетей, доступных в P660HWP.

Табл. 140 Уровни безопасности беспроводной сети

УРОВНИ БЕЗОПАСНОСТИ	ТИП ЗАЩИТЫ
Самый низкий уровень защиты	Уникальный идентификатор SSID (по умолчанию)
	Уникальный идентификатор SSID с включенной функцией «Скрыть SSID»
	Фильтрация MAC-адресов
	WEP-шифрование
	Расширенный протокол идентификации IEEE802.1x и аутентификация с использованием сервера RADIUS
	Защищенный доступ Wi-Fi (WPA)
Самый высокий уровень защиты	WPA2

Необходимо включить одинаковые параметры безопасности в интернет-центре P660HWP и на всех беспроводных клиентах, которые будут подключены к интернет-центру.

IEEE 802.1x

В июне 2001 года был создан стандарт IEEE 802.1x, расширивший возможности стандарта IEEE 802.11, а именно поддерживающий расширенную аутентификацию и имеющий дополнительные функции учета и контроля. Он поддерживается Windows XP и рядом сетевых устройств. Вот некоторые из преимуществ IEEE 802.1x:

- Идентификация на уровне пользователей, обеспечивающая возможность роуминга.
- Поддержка системы RADIUS (Аутентификация удаленных пользователей по коммутируемым каналам связи, RFC 2138, 2139) для централизованного управления пользовательскими профилями и учетом на сетевом сервере RADIUS.
- Поддержка EAP (Расширяемого протокола аутентификации, RFC 2486), позволяющая использовать дополнительные методы аутентификации, не меняя настроек точки доступа и беспроводных клиентов.

RADIUS

Система RADIUS основывается на модели «клиент-сервер», поддерживающей аутентификацию, авторизацию и учет. Клиент – это точка доступа, а сервер – это сервер RADIUS. Сервер RADIUS выполняет следующие задачи:

- Аутентификация

  Устанавливает подлинность пользователей.
- Авторизация

  Определяет сетевые службы, доступные для аутентифицированных пользователей после подключения к сети.
- Учет

  Отслеживает активность сети клиента.

RADIUS использует простой обмен пакетами, в котором точка доступа выступает в качестве ретранслятора сообщений между беспроводным устройством и сетевым сервером RADIUS.

Типы сообщений RADIUS

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

- Access-Request (Доступ-Запрос)

  Посылается точкой доступа при запросе аутентификации.
- Access-Reject (Доступ-Отказ)

Посылается сервером RADIUS при отказе в доступе.

- Access-Accept (Доступ-Разрешение)
  Посылается сервером RADIUS при разрешении доступа.
- Access-Challenge (Доступ-Приглашение)
  Посылается сервером RADIUS при запросе дополнительной информации для получения доступа. Точка доступа получает от пользователя надлежащий ответ, а затем посылает еще одно сообщение «Access-Request».

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

- Accounting-Request (Учет-Запрос)
  Посылается точкой доступа при запросе учета.
- Accounting-Response (Учет-Ответ)
  Посылается сервером RADIUS и указывает, что учет начался или закончился.

Для обеспечения сетевой безопасности точка доступа и сервер RADIUS используют общий секретный ключ, который является паролем, известным им обоим. Этот ключ не передается по сети. Помимо общего секретного ключа, обмен информацией о пароле также кодируется для защиты сети от несанкционированного доступа.

Методы аутентификации EAP

В этом разделе рассматривается несколько распространенных типов аутентификации: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP и LEAP. Ваше беспроводное устройство может не поддерживать некоторые методы аутентификации.

Протокол EAP (Расширенный протокол аутентификации) выполняется на верхнем уровне транспортного алгоритма IEEE 802.1x, что обеспечивает поддержку многочисленных типов аутентификации пользователей. Используя протокол EAP для взаимодействия с EAP-совместимым сервером RADIUS, точка доступа помогает беспроводному устройству и серверу RADIUS выполнить аутентификацию.

Непосредственно используемый тип аутентификации зависит от сервера RADIUS и от промежуточной точки (точек) доступа с поддержкой стандарта IEEE 802.1x. .

Для аутентификации типа EAP-TLS сначала необходимо установить проводное подключение к сети и получить сертификат(ы) от центра сертификации (CA). Сертификат (также называемый цифровым идентификатором) может быть использован для аутентификации пользователей. Центр сертификации выдает сертификаты и гарантирует подлинность персональных данных каждого обладателя сертификата.

EAP-MD5 (Алгоритм представления сообщения в краткой форме 5)

Аутентификация по методу MD5 – это простейший способ односторонней аутентификации. Сервер аутентификации посылает запрос беспроводному клиенту. Беспроводной клиент подтверждает знание пароля, для чего он шифрует его и отправляет серверу в качестве ответа на запрос. Пароль не отправляется в виде обычного текста.

Однако метод MD5 имеет слабые стороны. Дело в том, что поскольку серверу аутентификации пароль нужен в виде обычного текста, его необходимо где-то сохранять. Следовательно, доступ к файлу с паролями может получить не только сервер аутентификации. Кроме того, сервер аутентификации можно сымитировать, т. е. выдать себя за него (поскольку метод MD5 не выполняет двусторонней аутентификации). И, наконец, метод MD5 не поддерживает шифрование данных с помощью динамического сеансового ключа. Чтобы зашифровать данные, необходимо настроить ключи шифрования WEP.

EAP-TLS (Безопасность на транспортном уровне)

При использовании метода EAP-TLS серверу и беспроводным клиентам необходимы цифровые удостоверения для взаимной аутентификации. Сервер предоставляет клиентскому устройству свое удостоверение. После идентификации сервера клиентское устройство отправляет серверу свое удостоверение. До создания защищенного туннеля обмен удостоверениями производится в открытую. Это делает пользователя уязвимым для пассивных атак. Цифровое удостоверение – это электронная ID-карта, идентифицирующая отправителя. Однако для использования метода EAP-TLS необходимо иметь дело с Центром сертификации (CA), которое занимается обработкой удостоверений, что повлечет за собой административные издержки.

EAP-TTLS (Защита туннелированного транспортного уровня)

Метод EAP-TTLS представляет собой расширенную версию метода EAP-TLS. Для установления безопасного соединения удостоверения используются для аутентификации только со стороны сервера. Аутентификация клиента производится путем отправки имени пользователя и пароля через безопасное соединение, таким образом обеспечивается защита клиента. Метод EAP-TTLS поддерживает методы аутентификации клиента EAP и традиционные методы аутентификации, такие как PAP, CHAP, MS-CHAP и MS-CHAP v2.

PEAP (Защищенный EAP)

Как и в методе EAP-TTLS, для создания безопасного соединения здесь используется аутентификация удостоверений на стороне сервера, затем для аутентификации клиентов используются обычные методы проверки имени пользователя и пароля через созданное безопасное соединение. Таким образом защищаются персональные данные клиентов. Однако метод PEAP поддерживает лишь методы аутенификации клиента EAP, такие как EAP-MD5, EAP-MSCHAPv2 и EAP-GTC. Метод EAP-GTC реализует только корпорация Cisco.

LEAP (Упрощенный расширяемый протокол аутентификации)

LEAP (Упрощенный расширяемый протокол аутентификации) представляет собой протокол стандарта IEEE 802.1x, реализованный корпорацией Cisco.

Динамический обмен ключами WEP

Точка доступа копирует уникальный ключ, генерируемый сервером RADIUS. Этот ключ действителен до тех пор, пока беспроводное соединение не будет разорвано, не будет превышен лимит времени простоя, либо пока не истечет время простоя при повторной аутентификации. При каждой повторной аутентификации генерируется новый ключ WEP.

Если включить эту функцию, то настраивать ключ шифрования по умолчанию в окне **Wireless (Беспроводная сеть)** не обязательно. Вы можете создавать и сохранять ключи в этом окне, но они не будут использоваться при включенном режиме динамического шифрования WEP.

EAP-MD5 нельзя использовать для динамического обмена ключами WEP

Для дополнительной безопасности методы аутентификации на основе цифровых удостоверений (EAP-TLS, EAP-TTLS и PEAP) используют динамические ключи для шифрования данных. Они часто используются в корпоративной среде, однако для применения в обычной среде более практичным оказывается традиционная пара «имя пользователя+пароль». В приведенной ниже таблице сравниваются функции различных методов аутентификации.

Табл. 141 Сравнительный анализ методов аутентификации EAP

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Двусторонняя аутентификация	Нет	Да	Да	Да	Да
Удостоверение – Клиент	Нет	Да	По выбору	По выбору	Нет
Удостоверение – Сервер	Нет	Да	Да	Да	Нет
Динамический обмен ключами	Нет	Да	Да	Да	Да
Целостность мандата	Нет	Сильная	Сильная	Сильная	Средняя
Сложность применения	Низкая	Высокая	Средняя	Средняя	Средняя
Защита персональных данных клиентского устройства	Нет	Нет	Да	Да	Нет

WPA и WPA2

Wi-Fi Protected Access (WPA – Защищенный доступ Wi-Fi) представляет собой элемент из набора средств безопасности стандарта IEEE 802.11i. WPA2 (IEEE 802.11i) представляет собой безопасный стандарт беспроводной связи, обеспечивающий более защищенные по сравнению с WPA методы шифрования, аутентификации и управления ключами.

Основные отличия WPA и WPA2 от WEP заключаются в использовании аутентификации пользователей и более совершенном шифровании данных.

Если точка доступа и компьютеры беспроводных клиентов поддерживают WPA2 и имеется внешний сервер RADIUS, то следует использовать WPA2 для более совершенного шифрования данных. Если внешний сервер RADIUS отсутствует, следует использовать WPA2-PSK (общий ключ WPA2), который требует ввода только одного (одинакового) пароля для каждой точки доступа, беспроводного шлюза и компьютера беспроводного клиента. Если пароли совпадают, клиенту будет предоставлен доступ в беспроводную локальную сеть.

Если точка доступа или компьютеры беспроводных клиентов не поддерживают WPA2, следует использовать WPA или WPA-PSK, в зависимости от наличия внешнего сервера RADIUS.

Используйте WEP только в том случае, если точка доступа и/или беспроводные клиенты не поддерживают WPA или WPA2. WEP является менее надежным по сравнению с WPA или WPA2.

Шифрование

В WPA и WPA2 шифрование данных улучшено за счет использования протокола целостности временного ключа (TKIP), проверки целостности сообщения (MIC) и стандарта IEEE 802.1x. В WPA и WPA2 используется расширенный стандарт шифрования (AES) в режиме счетчика и протокол сцепления блоков шифртекста с кодом аутентификации сообщения (CCMP), что обеспечивает более совершенное шифрование по сравнению с TKIP.

В протоколе TKIP используются 128-битные ключи, динамически генерируемые и распределяемые сервером аутентификации. AES (Расширенный стандарт шифрования) представляет собой блочный шифр, использующий 256-битный математический алгоритм Rijndael. Оба метода включают функцию внесения ключа в каждый пакет данных, проверку целостности сообщения (MIC), называемую Michael, расширенный вектор инициализации (IV) с правилами установления последовательности соединения и механизм перекодирования.

WPA и WPA2 регулярно меняют и чередуют ключи шифрования, так чтобы один и тот же ключ шифрования никогда не использовался дважды.

Сервер RADIUS выдает парный главный ключ (PMK) точке доступа, которая затем создает систему управления и иерархии ключей с использованием парного ключа для динамического генерирования уникальных ключей шифрования данных для шифрования каждого пакета, передаваемого беспроводным методом между точкой доступа и беспроводными клиентами. Все это происходит автоматически в фоновом режиме.

Проверка целостности пакетов (MIC) предназначена для предотвращения перехвата, изменения и повторной отправки пакетов данных злоумышленниками. MIC имеет строгую математическую функцию, где принимающая и отправляющая стороны вычисляют каждая свой MIC, которые затем сравниваются. Если они не совпадают, то предполагается, что данные испорчены, и пакет удаляется.

При помощи генерирования уникальных ключей шифрования данных для каждого пакета данных и создания алгоритма проверки на целостность (MIC) методы TKIP и AES гораздо больше осложняют дешифрование данных в сети Wi-Fi по сравнению с WEP, затрудняя злоумышленнику проникновение в сеть.

Механизмы шифрования, используемые для WPA(2) и WPA(2)-PSK, одинаковы. Разница между WPA(2) и WPA-PSK состоит в том, что WPA-PSK использует единственный предварительно согласованный ключ (пароль) для аутентификации всех пользователей, в то время как WPA предполагает наличие индивидуального пароля у каждого пользователя. Использование обычного пароля делает механизм WPA(2)-PSK восприимчивым к атакам «грубой силы» с подбором пароля, однако по сравнению с WEP этот механизм является более прогрессивным, поскольку для получения парного главного ключа, который используется для генерирования уникальных временных ключей шифрования, применяется постоянный буквенно-цифровой пароль. Это позволяет предотвратить использование одинаковых ключей шифрования всеми беспроводными устройствами с общим доступом (что является уязвимым местом WEP)

Аутентификация пользователя

В WPA и WPA2 применяется стандарт IEEE 802.1x и протокол EAP (Extensible Authentication Protocol – Расширенный протокол аутентификации) для аутентификации беспроводных клиентов с использованием внешней базы данных RADIUS. WPA2 позволяет уменьшить количество сообщений об обмене ключами с шести до четырех (4-этапный протокол передачи данных CCMP) и сократить время, необходимое для подключения к сети. Другим отличием WPA2 от WPA является процесс аутентификации, который включает в себя кэширование ключей и предварительную аутентификацию. Эти две функции являются факультативными и могут не поддерживаться некоторыми беспроводными устройствами.

Кэширование ключей позволяет компьютеру беспроводного клиента сохранять парный главный ключ, который он получает после успешного прохождения аутентификации в точке доступа. Компьютер беспроводного клиента использует этот ключ при попытке подключения к той же точке доступа для того, чтобы не проходить процедуру аутентификации снова.

Предварительная аутентификация включает быстрый роуминг, что позволяет компьютеру беспроводного клиента (уже подключенному к точке доступа) провести аутентификацию стандарта IEEE 802.1x другой точкой доступа, прежде чем подключиться к ней.

Вспомогательное программное обеспечение для беспроводных клиентов WPA

Вспомогательное ПО беспроводного клиента – это программа, работающая в операционной системе и дающая беспроводному клиенту инструкции по использованию WPA. На момент написания данного руководства самыми распространенными программами являются: вставка WPA для Windows XP и клиент Odyssey компании Funk.

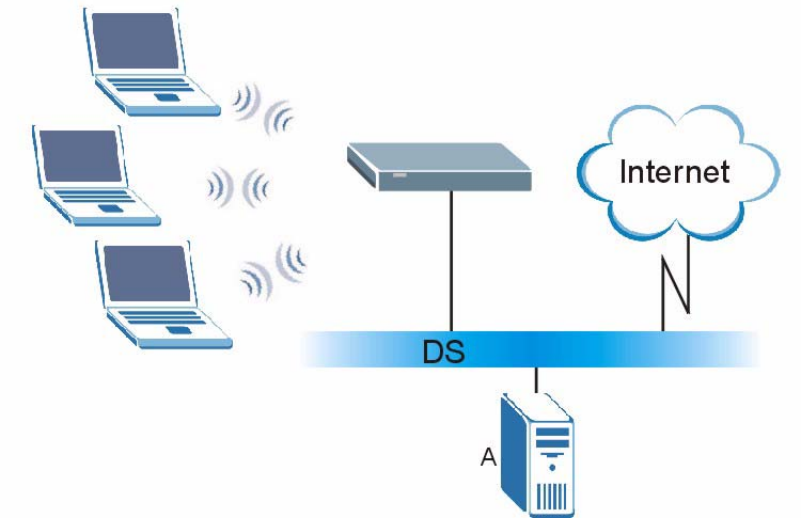
Обновление для Windows XP представляет собой бесплатную подпрограмму, которая добавляет функцию WPA к встроенному беспроводному клиенту Windows XP с функцией «Zero Configuration» (Автоматическая настройка). Однако, для ее использования необходимо работать в Windows XP.

Пример применения WPA(2)-PSK с сервером RADIUS

Потребуются IP-адрес, номер порта (по умолчанию 1812) и общий секретный ключ сервера RADIUS. Далее приводится пример подключения по WPA(2) с использованием внешнего сервера RADIUS. «A» – это сервер RADIUS. «DS» – это система распределения.

1. Точка доступа посылает запрос серверу RADIUS на аутентификацию беспроводного клиента.
2. Сервер RADIUS проводит идентификацию пользователя по своей базе данных и соответственно предоставляет или запрещает доступ в сеть.
3. Сервер RADIUS выдает парный главный ключ (PMK) точке доступа, которая затем создает иерархию и систему управления ключами с использованием парного ключа для дальнейшего динамического генерирования уникальных ключей шифрования данных. Эти уникальные ключи используются для шифрования всех пакетов данных, передаваемых беспроводным методом между точкой доступа и беспроводными клиентами.

Рис. 182 Пример применения WPA(2)-PSK с сервером RADIUS

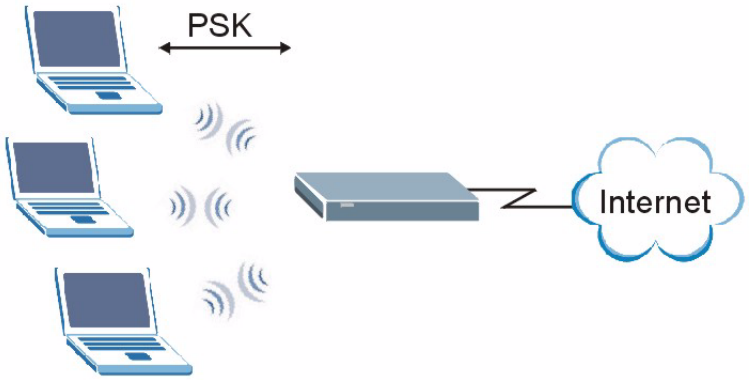


Пример применения WPA(2)-PSK

WPA(2)-PSK применяется следующим образом.

1. Сначала вводятся идентичные пароли для точки доступа и всех беспроводных устройств. Общий ключ (PSK) может содержать от 8 до 63 латинских символов или 64 шестнадцатеричных символа (включая пробелы и служебные символы).
2. Точка доступа проверяет пароль каждого беспроводного клиента и, если пароль совпадает, разрешает подключает к сети.
3. Точка доступа и беспроводные клиенты используют общий ключ для генерации общего парного главного ключа (PMK).
4. Точка доступа и беспроводные клиенты используют протокол TKIP или стандарт AES для шифрования данных, передаваемых друг другу.

Рис. 183 Аутентификация WPA(2)-PSK



Обзор параметров безопасности

В этой таблице приведены прочие параметры безопасности, которые нужно настроить для каждого метода аутентификации/протокола управления ключами. Фильтры MAC-адресов не зависят от настройки этих характеристик безопасности.

Табл. 142 Сравнительная таблица беспроводной безопасности

МЕТОД АУТЕНТИФИКАЦИИ/ ПРОТОКОЛ УПРАВЛЕНИЯ КЛЮЧАМИ	МЕТОД ШИФРОВАНИЯ	РУЧНОЙ ВВОД КЛЮЧА	IEEE 802.1X
Открытый	Нет	Нет	Отключен
			Включен с динамическим ключом WEP
Открытый	WEP	Нет	Включен с динамическим ключом WEP
		Да	Включен с динамическим ключом WEP
		Да	Отключен
Общий	WEP	Нет	Включен с динамическим ключом WEP
		Да	Включен с динамическим ключом WEP
		Да	Отключен
WPA	TKIP/AES	Нет	Включен
WPA-PSK	TKIP/AES	Да	Отключен
WPA2	TKIP/AES	Нет	Включен
WPA2-PSK	TKIP/AES	Да	Отключен

Антенна – общее описание

Антенна передает радиосигналы в эфир. Передатчик беспроводного устройства посылает радичастоты на антенну, которая передает их через эфир. Антенна работает и на прием, принимая радиосигналы из эфира.

Правильное направление антенны увеличивает радиус покрытия беспроводной локальной сети.

Характеристики антенны

Частота

Для эффективной связи в беспроводной локальной сети необходима антенна, способная работать на частоте 2,4 ГГц (стандарт IEEE 802.11b) или 5 ГГц (стандарт IEEE 802.11a).

Диаграмма направленности

Диаграмма направленности помогает визуально представить область покрытия антенны.

Усиление антенного сигнала

Усиление антенного сигнала, измеряемое в дБ (в децибелах), означает увеличение зоны покрытия в рамках ширины диаграммы направленности антенны. Более мощное усиление увеличивает дальность сигнала, что обеспечивает лучшую связь.

При внутреннем использовании каждый дБ усиления сигнала увеличивает зону покрытия примерно на 2,5%. При внешнеем использовании (без препятствий) каждый дБ усиления сигнала увеличивает зону покрытия, примерно, на 5%. Реальные результаты, в зависимости от сетевого окружения, могут отличаться от указанных.

Иногда усиление антенного сигнала указывается в дБ относительно изотропной антенны (dBi), показывая, насколько антенна усиливает мощность сигнала по сравнению с изотропной антенной. Изотропной антенной называется такая идеальная антенна, которая посылает радиосигналы одинаково во всех направлениях. Таким образом, указанная выше единица измерения представляет собой реальное усиление антенны.

Типы антенн для беспроводных локальных сетей

В беспроводных локальных сетях используются два типа антенн.

- Всенаправленные антенны. Они посылают радиосигналы во всех направлениях в горизонтальной плоскости. Зона охвата имеет тороидальную форму (в форме бублика), что позволяет эффективно использовать эти антенны внутри помещений. При использовании нескольких точек доступа возможно перекрытие зон охвата.

- Направленные антенны. Они концентрируют радиосигнал в виде луча (подобно пучку света, испускаемому фонарем). Угол луча определяет ширину зоны обслуживания. Обычно угол составляет от 20 (строгонаправленные) до 120 градусов (слабонаправленные). Направленные антенны хорошо подходят для использования в коридорах и для создания внешних подключений типа «точка-точка».

Размещение антенн

Антенны должны монтироваться, главным образом, как можно выше и дальше от препятствий. При подключениях типа «точка-точка» антенны следует располагать на одной высоте и направлять точно друг на друга.

Всенаправленные антенны устанавливаются на столах, стойках и т.д. При этом антенна должна смотреть вверх. Направленные антенны крепятся на стенах или потолках. При этом антенна должна смотреть вниз. В схемах с одной точкой доступа всенаправленную антенну следует размещать как можно ближе к центру планируемой области покрытия.

Направленные антенны следует направлять в сторону желаемой области покрытия.

C

Внутренний генератор таблицы системных параметров (SPTGEN)

В этом приложении рассказывается о встроенной функции SPTGEN. Все меню в данном приложении являются примерами для демонстрации использования SPTGEN. Вид фактических меню для конкретного изделия может отличаться.

Внутренний SPTGEN – общая информация

Внутренний SPTGEN (System Parameter Table Generator – Генератор таблицы системных параметров) представляет собой текстовый файл конфигурации, с помощью которого можно быстро выполнить настройку нескольких устройств P660HWP. Внутренний SPTGEN позволяет настраивать, сохранять и загружать множество меню одновременно при помощи одного текстового файла конфигурации, что исключает необходимость перемещения по различным окнам SMT и их последовательной настройки для каждого устройства P660HWP. Файл SPTGEN можно получить с помощью FTP. Затем этот файл можно отредактировать в текстовом редакторе и с помощью FTP загрузить в то же или другое устройство. Подробнее см. в следующих разделах.

Формат текстового файла конфигурации

Все текстовые файлы внутреннего генератора таблицы системных параметров имеют схожий формат, а именно:

```
<field identification number = field name = parameter values allowed =
input>,
```

где `<input>` (ввод)- это вводимые данные, отвечающие `<parameter values allowed>` (допустимым значениям параметра).

На рисунке ниже приводится пример текстового файла внутреннего генератора таблицы системных параметров.

Рис. 184 Формат текстового файла конфигурации: Описание столбцов

```
/ Меню 1 – Настройка общих параметров
10000000 = Configured              <0(No)| 1(Yes)>      = 1
10000001 = System Name             <Str>                = Your Device
10000002 = Location                <Str>                =
10000003 = Contact Person's Name   <Str>                =
10000004 = Route IP                <0(No)| 1(Yes)>      = 1
10000005 = Route IPX               <0(No)| 1(Yes)>      = 0
10000006 = Bridge                  <0(No)| 1(Yes)>      = 0
```

НЕ редактируйте и не удаляйте никакие поля, за исключением параметров в столбце Input (Ввод).

В этом приложении рассказывается о встроенной функции SPTGEN. Все меню в данном приложении являются примерами для демонстрации использования SPTGEN. Вид фактических меню для конкретного изделия может отличаться.

Изменение файла внутреннего генератора таблицы системных параметров – что необходимо запомнить

Каждому вводимому параметру должны предшествовать один знак равенства «=» и один пробел.

Некоторые параметры зависят от других. Например, если отключить поле **Configured (Настроено)** в меню 1 (см. Рис. 184 на с. 358), то необходимо отключить все поля в данном меню.

Если в столбец **Input (Ввод)**, введен неверный параметр, P660HWP не сохранит конфигурацию, и в командной строке будет отображаться **Field Identification Number (Идентификационный номер поля)**. На Рис. 185 на с. 358 приведен пример сообщения в командной строке P660HWP, если в столбце **Input (Ввод) идентификационного номера поля** 1000000 введено значение, отличающееся от 0 и 1 (см. Рис. 184 на с. 358).

Рис. 185 Пример командной строки при вводе неверного параметра

```
field value is not legal error:-1
ROM-t is not saved, error Line ID:10000000
reboot to get the original configuration
Bootbase Version: V2.02 | 2/22/2001 13:33:11
RAM: Size = 8192 Kbytes
FLASH: Intel 8M *2
```

Если параметр(ы) введен(ы) *правильно*, в командной строке P660HWP отображается следующая информация.

Рис. 186 Пример командной строки при правильном вводе параметра

```
Please wait for the system to write SPT text file(ROM-t)...
Bootbase Version: V2.02 | 2/22/2001 13:33:11
RAM: Size = 8192 Kbytes
FLASH: Intel 8M *2
```

Пример скачивания файла внутреннего генератора таблицы системных параметров по протоколу FTP

1. Запустите приложение FTP.
2. Введите «bin». Команда «bin» переключает режим передачи на бинарный.
3. Получите файл «rom-t» (get "rom-t"). Команда «get» выполняет передачу файлов из интернет-центра P660HWP на ваш компьютер. Имя файла «rom-t» является именем файла конфигурации в интернет-центре P660HWP.
4. Внесите изменения в файл «rom-t» при помощи текстового редактора (не используйте текстовый процессор Word). Для того чтобы отредактировать файл, необходимо выйти из экранной формы FTP.

Рис. 187 Пример скачивания файла внутреннего генератора таблицы системных параметров по протоколу FTP

```
c:\ftp 192.168.1.1
220 PPP FTP version 1.0 ready at Sat Jan 1 03:22:12 2000
User (192.168.1.1:(none)):
331 Enter PASS command
Password:
230 Logged in
ftp>bin
200 Type I OK
ftp> get rom-t
ftp>bye
c:\edit rom-t
(edit the rom-t text file by a text editor and save it)
```

При сохранении файла «rom-t» на компьютере его можно переименовать, но при загрузке из компьютера в P660HWP этот файл должен иметь имя «rom-t».

Пример загрузки внутреннего генератора таблицы системных параметров по протоколу FTP

1. Запустите приложение FTP.
2. Введите «bin». Команда «bin» переключает режим передачи на бинарный.

3 Загрузите файл «rom-t» из компьютера в P660HWP с помощью команды «put».

4 Закройте приложение FTP.

Рис. 188 Пример загрузки внутреннего генератора таблицы системных параметров по протоколу FTP

```
c:\ftp 192.168.1.1
220 PPP FTP version 1.0 ready at Sat Jan 1 03:22:12 2000
User (192.168.1.1:(none)):
331 Enter PASS command
Password:
230 Logged in
ftp>bin
200 Type I OK
ftp> put rom-t
ftp>bye
```

Пример меню SPTGEN

В этом разделе описываются меню внутреннего генератора таблицы системных параметров.

Табл. 143 Сокращения, использованные в экранных формах внутреннего генератора таблицы системных параметров

СОКРАЩЕНИЕ	ЗНАЧЕНИЕ
FIN	Идентификационный номер поля
FN	Имя поля
PVA	Допустимые значения параметров
INPUT	Пример вводимых значений
*	Применяется к интернет-центру P660HWP.

Табл. 144 Меню 1 – Настройка общих параметров

/ Меню 1 – Настройка общих параметров			
FIN	FN	PVA	INPUT
10000000 =	Configured (Установлено)	<0(Нет) | 1(Да)>	= 0
10000001 =	System Name (Системное имя)	<строка>	= Your Device
10000002 =	Location (Местонахождение)	<строка>	=
10000003 =	Contact Person's Name (Имя контактного лица)	<строка>	=
10000004 =	Route IP (Маршрутизация IP)	<0(Нет) | 1(Да)>	= 1
10000006 =	Bridge (Мост)	<0(Нет) | 1(Да)>	= 0

Табл. 145 Меню 3

/ Меню 3.1 Общая настройка Ethernet			
FIN	FN	PVA	INPUT
30100001 =	Input Protocol filters Set 1 (Набор входных фильтров протоколов 1)		= 2
30100002 =	Input Protocol filters Set 2 (Набор входных фильтров протоколов 2)		= 256
30100003 =	Input Protocol filters Set 3 (Набор входных фильтров протоколов 3)		= 256
30100004 =	Input Protocol filters Set 4 (Набор входных фильтров протоколов 4)		= 256
30100005 =	Input device filters Set 1 (Набор входных фильтров устройства 1)		= 256
30100006 =	Input device filters Set 2 (Набор входных фильтров устройства 2)		= 256
30100007 =	Input device filters Set 3 (Набор входных фильтров устройства 3)		= 256
30100008 =	Input device filters Set 4 (Набор входных фильтров устройства 4)		= 256
30100009 =	Output protocol filters Set 1 (Набор выходных фильтров протоколов 1)		= 256
30100010 =	Output protocol filters Set 2 (Набор выходных фильтров протоколов 2)		= 256
30100011 =	Output protocol filters Set 3 (Набор выходных фильтров протоколов 3)		= 256
30100012 =	Output protocol filters Set 4 (Набор выходных фильтров протоколов 4)		= 256
30100013 =	Output device filters Set 1 (Набор выходных фильтров устройства 1)		= 256
30100014 =	Output device filters Set 2 (Набор выходных фильтров устройства 2)		= 256
30100015 =	Output device filters Set 3 (Набор выходных фильтров устройства 3)		= 256
30100016 =	Output device filters Set 4 (Набор выходных фильтров устройства 4)		= 256
/ Меню 3.2 Настройка TCP/IP и DHCP для Ethernet			
FIN	FN	PVA	INPUT
30200001 =	DHCP	<0(нет) | 1(сервер) | 2(ретранслятор)>	= 0
30200002 =	Client IP Pool Starting Address (Начальный IP-адрес клиентского диапазона)		= 192.168.1.33
30200003 =	Size of Client IP Pool (Размер клиентского IP-диапазона)		= 32

Табл. 145 Меню 3

30200004 =	Primary DNS Server (Основной сервер DNS)		= 0.0.0.0
30200005 =	Secondary DNS Server (Дополнительный сервер DNS)		= 0.0.0.0
30200006 =	Remote DHCP Server (Удаленный сервер DHCP)		= 0.0.0.0
30200008 =	IP Address (IP-адрес)		= 172.21.2.200
30200009 =	IP Subnet Mask (Маска IP подсети)		= 16
30200010 =	RIP Direction (Направление RIP)	<0(нет) | 1(оба) | 2(только вход) | 3(только выход)>	= 0
30200011 =	Version (версия)	<0(Rip-1) | 1(Rip-2B) |2(Rip-2M)>	= 0
30200012 =	Multicast (Многоадресная рассылка)	<0(IGMP-v2) | 1(IGMP-v1) | 2(нет)>	= 2
30200013 =	IP Policies Set 1 (Набор политик IP 1) (1~12)		= 256
30200014 =	IP Policies Set 2 (Набор политик IP 2) (1~12)		= 256
30200015 =	IP Policies Set 3 (Набор политик IP 3) (1~12)		= 256
30200016 =	IP Policies Set 4 (Набор политик IP 4) (1~12)		= 256
/ Меню 3.2.1 Настройка псевдонима IP			
FIN	FN	PVA	INPUT
30201001 =	IP Alias 1 (Псевдоним IP 1)	<0(Нет) | 1(Да)>	= 0
30201002 =	IP Address (IP-адрес)		= 0.0.0.0
30201003 =	IP Subnet Mask (Маска IP подсети)		= 0
30201004 =	RIP Direction (Направление RIP)	<0(нет) | 1(оба) | 2(только вход) | 3(только выход)>	= 0
30201005 =	Version (версия)	<0(Rip-1) | 1(Rip-2B) |2(Rip-2M)>	= 0
30201006 =	IP Alias #1 Incoming protocol filters Set 1 (Псевдоним IP #1 Набор фильтров входных протоколов 1)		= 256
30201007 =	IP Alias #1 Incoming protocol filters Set 2 (Псевдоним IP #1 Набор фильтров входных протоколов 2)		= 256

Табл. 145 Меню 3

30201008 =	IP Alias #1 Incoming protocol filters Set 3 (Псевдоним IP #1 Набор фильтров входных протоколов 3)		= 256
30201009 =	IP Alias #1 Incoming protocol filters Set 4 (Псевдоним IP #1 Набор фильтров входных протоколов 4)		= 256
30201010 =	IP Alias #1 Outgoing protocol filters Set 1 (Псевдоним IP #1 Набор фильтров выходных протоколов 1)		= 256
30201011 =	IP Alias #1 Outgoing protocol filters Set 2 (Псевдоним IP #1 Набор фильтров выходных протоколов 2)		= 256
30201012 =	IP Alias #1 Outgoing protocol filters Set 3 (Псевдоним IP #1 Набор фильтров выходных протоколов 3)		= 256
30201013 =	IP Alias #1 Outgoing protocol filters Set 4 (Псевдоним IP #1 Набор фильтров выходных протоколов 4)		= 256
30201014 =	IP Alias 2 <0(No) | 1(Yes)> (Псевдоним IP 2 <0(Нет) | 1(Да)>)		= 0
30201015 =	IP Address (IP-адрес)		= 0.0.0.0
30201016 =	IP Subnet Mask (Маска IP подсети)		= 0
30201017 =	RIP Direction (Направление RIP)	<0(нет) | 1(оба) | 2(только вход) | 3(только выход)>	= 0
30201018 =	Version (версия)	<0(Rip-1) | 1(Rip-2B) |2(Rip-2M)>	= 0
30201019 =	IP Alias #2 Incoming protocol filters Set 1 (Псевдоним IP #2 Набор фильтров входных протоколов 1)		= 256
30201020 =	IP Alias #2 Incoming protocol filters Set 2 (Псевдоним IP #2 Набор фильтров входных протоколов 2)		= 256
30201021 =	IP Alias #2 Incoming protocol filters Set 3 (Псевдоним IP #2 Набор фильтров входных протоколов 3)		= 256
30201022 =	IP Alias #2 Incoming protocol filters Set 4 (Псевдоним IP #2 Набор фильтров входных протоколов 4)		= 256
30201023 =	IP Alias #2 Outgoing protocol filters Set 1 (Псевдоним IP #2 Набор фильтров выходных протоколов 1)		= 256
30201024 =	IP Alias #2 Outgoing protocol filters Set 2 (Псевдоним IP #2 Набор фильтров выходных протоколов 2)		= 256

Табл. 145 Меню 3

30201025 =	IP Alias #2 Outgoing protocol filters Set 3 (Псевдоним IP #2 Набор фильтров выходных протоколов 3)		= 256
30201026 =	IP Alias #2 Outgoing protocol filters Set 4 (Псевдоним IP #2 Набор фильтров выходных протоколов 4)		= 256

Табл. 146 Меню 4 – Настройка доступа в Интернет

/ Меню 4 Настройка доступа в Интернет			
FIN	FN	PVA	INPUT
40000000 =	Configured (Установлено)	<0(Нет) | 1(Да)>	= 1
40000001 =	ISP (Интернет-провайдер)	<0(Нет) | 1(Да)>	= 1
40000002 =	Active (Активировать)	<0(Нет) | 1(Да)>	= 1
40000003 =	ISP's Name (Имя Интернет-провайдера)		= ChangeMe
40000004 =	Encapsulation (Инкапсуляция)	<2(PPPOE) | 3(RFC 1483)| 4(PPPoA)| 5(ENET ENCAP)>	= 2
40000005 =	Multiplexing (Мультиплексирование)	<1(на основе LLC) | 2(на основе VC)	= 1
40000006 =	VPI # (Номер VPI)		= 0
40000007 =	VCI # (Номер VCI)		= 35
40000008 =	Service Name (Имя услуги)	<строка>	= любое
40000009 =	My Login (Регистрационное имя)	<строка>	= test@pqa
40000010 =	My Password (Пароль)	<строка>	= 1234
40000011 =	Single User Account (Режим одной учетной записи)	<0(Нет) | 1(Да)>	= 1
40000012 =	IP Address Assignment (Назначение IP-адреса)	<0(статический)| 1(динамический)>	= 1
40000013 =	IP Address (IP-адрес)		= 0.0.0.0
40000014 =	Remote IP address (Удаленный IP-адрес)		= 0.0.0.0
40000015 =	Remote IP subnet mask (Удаленная маска IP подсети)		= 0
40000016 =	ISP incoming protocol filter set 1 (Набор фильтров входного протокола интернет-провайдера 1)		= 6
40000017 =	ISP incoming protocol filter set 2 (Набор фильтров входного протокола интернет-провайдера 2)		= 256
40000018 =	ISP incoming protocol filter set 3 (Набор фильтров входного протокола интернет-провайдера 3)		= 256

Табл. 146 Меню 4 – Настройка доступа в Интернет (продолжение)

40000019 =	ISP incoming protocol filter set 4 (Набор фильтров входного протокола интернет-провайдера 4)		= 256
40000020 =	ISP outgoing protocol filter set 1 (Набор фильтров выходного протокола интернет-провайдера 1)		= 256
40000021 =	ISP outgoing protocol filter set 2 (Набор фильтров выходного протокола интернет-провайдера 2)		= 256
40000022 =	ISP outgoing protocol filter set 3 (Набор фильтров выходного протокола интернет-провайдера 3)		= 256
40000023 =	ISP outgoing protocol filter set 4 (Набор фильтров выходного протокола интернет-провайдера 4)		= 256
40000024 =	ISP PPPoE idle timeout (Время простоя PPP поверх Ethernet Интернет-провайдера)		= 0
40000025 =	Route IP (Маршрутизация IP)	<0(Нет) | 1(Да)>	= 1
40000026 =	Bridge (Мост)	<0(Нет) | 1(Да)>	= 0
40000027 =	ATM QoS Type (Тип качества услуг ATM)	<0(CBR) | (1 (UBR)>	= 1
40000028 =	Peak Cell Rate (Пиковая скорость ячеек) (PCR)		= 0
40000029 =	Sustain Cell Rate (Поддерживаемая скорость ячеек) (SCR)		= 0
40000030 =	Maximum Burst Size(MBS) (Максимальный размер пакета)		= 0
40000031 =	RIP Direction (Направление RIP)	<0(нет) | 1(оба) | 2(только вход) | 3(только выход)>	= 0
40000032 =	RIP Version (Версия RIP)	<0(Rip-1) | 1(Rip-2B) |2(Rip-2M)>	= 0
40000033 =	Nailed-up Connection (Постоянное соединение)	<0(Нет) | 1(Да)>	= 0

Табл. 147 Меню 12

/ Меню 12.1.1 Настройка статического маршрута IP			
FIN	FN	PVA	INPUT
120101001 =	IP Static Route set #1, Name (Набор статических маршрутов IP#1, Имя)	<строка>	=
120101002 =	IP Static Route set #1, Active (Набор статических маршрутов IP#1, Активен)	<0(Нет) | 1(Да)>	= 0

Табл. 147 Меню 12 (продолжение)

120101003 =	IP Static Route set #1, Destination IP address (Набор статических маршрутов IP #1, IP-адрес назначения)		= 0.0.0.0
120101004 =	IP Static Route set #1, Destination IP subnetmask (Набор статических маршрутов IP #1, маска IP подсети получателя)		= 0
120101005 =	IP Static Route set #1, Gateway (Набор статических маршрутов IP #1, шлюз)		= 0.0.0.0
120101006 =	IP Static Route set #1, Metric (Набор статических маршрутов IP #1, метрика)		= 0
120101007 =	IP Static Route set #1, Private (Набор статических маршрутов IP #1, частный)	<0(Нет) | 1(Да)>	= 0
/ Меню 12.1.2 Настройка статического маршрута IP			
FIN	FN	PVA	INPUT
120108001 =	IP Static Route set #8, Name (Набор статических маршрутов IP#8, Имя)	<строка>	=
120108002 =	IP Static Route set #8, Active (Набор статических маршрутов IP#8, Активен)	<0(Нет) | 1(Да)>	= 0
120108003 =	IP Static Route set #8, Destination IP address (Набор статических маршрутов IP #8, IP-адрес назначения)		= 0.0.0.0
120108004 =	IP Static Route set #8, Destination IP subnetmask (Набор статических маршрутов IP #8, маска IP подсети получателя)		= 0
120108005 =	IP Static Route set #8, Gateway (Набор статических маршрутов IP #8, шлюз)		= 0.0.0.0
120108006 =	IP Static Route set #8, Metric (Набор статических маршрутов IP #8, метрика)		= 0
120108007 =	IP Static Route set #8, Private (Набор статических маршрутов IP #8, частный)	<0(Нет) | 1(Да)>	= 0

Табл. 148 Меню 15. Настройка сервера SUA

/ Меню 15 Настройка сервера SUA			
FIN	FN	PVA	INPUT
150000001 =	SUA Server IP address for default port (IP-адрес сервера SUA для порта по умолчанию)		= 0.0.0.0

Табл. 148 Меню 15. Настройка сервера SUA (продолжение)

150000002 =	SUA Server #2 Active (Сервер SUA #2, активный)	<0(Нет) | 1(Да)>	= 0
150000003 =	SUA Server #2 Protocol (Сервер SUA #2, протокол)	<0(All)|6(TCP)|17(UDP)>	= 0
150000004 =	SUA Server #2 Port Start (Сервер SUA #2, начальный порт)		= 0
150000005 =	SUA Server #2 Port End (Сервер SUA #2, конечный порт)		= 0
150000006 =	SUA Server #2 Local IP address (Локальный IP-адрес сервера SUA #2)		= 0.0.0.0
150000007 =	SUA Server #3 Active (Сервер SUA #3, активный)	<0(Нет) | 1(Да)>	= 0
150000008 =	SUA Server #3 Protocol (Сервер SUA #3, протокол)	<0(All)|6(TCP)|17(UDP)>	= 0
150000009 =	SUA Server #3 Port Start (Сервер SUA #3, начальный порт)		= 0
150000010 =	SUA Server #3 Port End (Сервер SUA #3, конечный порт)		= 0
150000011 =	SUA Server #3 Local IP address (Локальный IP-адрес сервера SUA #3)		= 0.0.0.0
150000012 =	SUA Server #4 Active (Сервер SUA #4, активный)	<0(Нет) | 1(Да)>	= 0
150000013 =	SUA Server #4 Protocol (Сервер SUA #4, протокол)	<0(All)|6(TCP)|17(UDP)>	= 0
150000014 =	SUA Server #4 Port Start (Сервер SUA #4, начальный порт)		= 0
150000015 =	SUA Server #4 Port End (Сервер SUA #4, конечный порт)		= 0
150000016 =	SUA Server #4 Local IP address (Локальный IP-адрес сервера SUA #4)		= 0.0.0.0
150000017 =	SUA Server #5 Active (Сервер SUA #5, активный)	<0(Нет) | 1(Да)>	= 0
150000018 =	SUA Server #5 Protocol (Сервер SUA #5, протокол)	<0(All)|6(TCP)|17(UDP)>	= 0
150000019 =	SUA Server #5 Port Start (Сервер SUA #5, начальный порт)		= 0
150000020 =	SUA Server #5 Port End (Сервер SUA #5, конечный порт)		= 0
150000021 =	SUA Server #5 Local IP address (Локальный IP-адрес сервера SUA #5)		= 0.0.0.0
150000022 =	SUA Server #6 Active (Сервер SUA #6, активный)	<0(Нет) | 1(Да)> = 0	= 0
150000023 =	SUA Server #6 Protocol (Сервер SUA #6, протокол)	<0(All)|6(TCP)|17(UDP)>	= 0

Табл. 148 Меню 15. Настройка сервера SUA (продолжение)

150000024 =	SUA Server #6 Port Start (Сервер SUA #6, начальный порт)		= 0
150000025 =	SUA Server #6 Port End (Сервер SUA #6, конечный порт)		= 0
150000026 =	SUA Server #6 Local IP address (Локальный IP-адрес сервера SUA #6)		= 0.0.0.0
150000027 =	SUA Server #7 Active (Сервер SUA #7, активный)	<0(Нет) | 1(Да)>	= 0
150000028 =	SUA Server #7 Protocol (Сервер SUA #7, протокол)	<0(All)|6(TCP)|17(UDP)>	= 0.0.0.0
150000029 =	SUA Server #7 Port Start (Сервер SUA #7, начальный порт)		= 0
150000030 =	SUA Server #7 Port End (Сервер SUA #7, конечный порт)		= 0
150000031 =	SUA Server #7 Local IP address (Локальный IP-адрес сервера SUA #7)		= 0.0.0.0
150000032 =	SUA Server #8 Active (Сервер SUA #8, активный)	<0(Нет) | 1(Да)>	= 0
150000033 =	SUA Server #8 Protocol (Сервер SUA #8, протокол)	<0(All)|6(TCP)|17(UDP)>	= 0
150000034 =	SUA Server #8 Port Start (Сервер SUA #8, начальный порт)		= 0
150000035 =	SUA Server #8 Port End (Сервер SUA #8, конечный порт)		= 0
150000036 =	SUA Server #8 Local IP address (Локальный IP-адрес сервера SUA #8)		= 0.0.0.0
150000037 =	SUA Server #9 Active (Сервер SUA #9, активный)	<0(Нет) | 1(Да)>	= 0
150000038 =	SUA Server #9 Protocol (Сервер SUA #9, протокол)	<0(All)|6(TCP)|17(UDP)>	= 0
150000039 =	SUA Server #9 Port Start (Сервер SUA #9, начальный порт)		= 0
150000040 =	SUA Server #9 Port End (Сервер SUA #9, конечный порт)		= 0
150000041 =	SUA Server #9 Local IP address (Локальный IP-адрес сервера SUA #9)		= 0.0.0.0
150000042 =	SUA Server #10 Active (Сервер SUA #10, активный)	<0(Нет) | 1(Да)>	= 0
150000043 =	SUA Server #10 Protocol (Сервер SUA #5, протокол)	<0(All)|6(TCP)|17(UDP)>	= 0
150000044 =	SUA Server #10 Port Start (Сервер SUA #10, начальный порт)		= 0
150000045 =	SUA Server #10 Port End (Сервер SUA #10, конечный порт)		= 0

Табл. 148 Меню 15. Настройка сервера SUA (продолжение)

150000046 =	SUA Server #10 Local IP address (Локальный IP-адрес сервера SUA #10)		= 0.0.0.0
150000047 =	SUA Server #11 Active (Сервер SUA #11, активный)	<0(Нет) | 1(Да)>	= 0
150000048 =	SUA Server #11 Protocol (Сервер SUA #11, протокол)	<0(All)|6(TCP)|17(UDP)>	= 0
150000049 =	SUA Server #11 Port Start (Сервер SUA #11, начальный порт)		= 0
150000050 =	SUA Server #11 Port End (Сервер SUA #11, конечный порт)		= 0
150000051 =	SUA Server #11 Local IP address (Локальный IP-адрес сервера SUA #11)		= 0.0.0.0
150000052 =	SUA Server #12 Active (Сервер SUA #12, активный)	<0(Нет) | 1(Да)>	= 0
150000053 =	SUA Server #12 Protocol (Сервер SUA #12, протокол)	<0(All)|6(TCP)|17(UDP)>	= 0
150000054 =	SUA Server #12 Port Start (Сервер SUA #12, начальный порт)		= 0
150000055 =	SUA Server #12 Port End (Сервер SUA #12, конечный порт)		= 0
150000056 =	SUA Server #12 Local IP address (Локальный IP-адрес сервера SUA #12)		= 0.0.0.0

Табл. 149 Меню 21.1. Набор фильтров #1

/ Меню 21 Набор фильтров #1			
FIN	FN	PVA	INPUT
210100001 =	Filter Set 1, Name (Набор фильтров 1, Имя)	<строка>	=
/ Меню 21.1.1.1 набор #1, правило #1			
FIN	FN	PVA	INPUT
210101001 =	IP Filter Set 1,Rule 1 Type (Фильтр IP, набор 1, правило 1, тип)	<2(TCP/IP)>	= 2
210101002 =	IP Filter Set 1,Rule 1 Active (Фильтр IP, набор 1, правило 1, активный)	<0(Нет) | 1(Да)>	= 1
210101003 =	IP Filter Set 1,Rule 1 Protocol (Набор фильтров IP 1, правило 1, протокол)		= 6
210101004 =	IP Filter Set 1,Rule 1 Dest IP address (Набор фильтров IP 1, правило 1, IP-адрес получателя)		= 0.0.0.0
210101005 =	IP Filter Set 1,Rule 1 Dest Subnet Mask (Набор фильтров IP 1, правило 1, маска подсети получателя)		= 0

Табл. 149 Меню 21.1. Набор фильтров #1 (продолжение)

210101006 =	IP Filter Set 1,Rule 1 Dest Port (Набор фильтров IP 1, правило 1, порт получателя)		= 137
210101007 =	IP Filter Set 1,Rule 1 Dest Port Comp (Набор фильтров IP 1, правило 1, сравнение порта получателя)	<0(нет)|1(равно)| 2(не равно)| 3(меньше| 4(больше)>	= 1
210101008 =	IP Filter Set 1,Rule 1 Src IP address (Набор фильтров IP, набор 1, правило 1, IP-адрес источника)		= 0.0.0.0
210101009 =	IP Filter Set 1,Rule 1 Src Subnet Mask (Набор фильтров IP 1, правило 1, маска подсети отправителя)		= 0
210101010 =	IP Filter Set 1,Rule 1 Src Port (Набор фильтров IP 1, правило 1, порт отправителя)		= 0
210101011 =	IP Filter Set 1,Rule 1 Src Port Comp (Набор фильтров IP 1, правило 1, сравнение порта отправителя)	<0(нет)|1(равно)| 2(не равно)| 3(меньше| 4(больше)>	= 0
210101013 =	IP Filter Set 1,Rule 1 Act Match (Набор фильтров IP 1, правило 1, действие при соответствии)	<1(проверить след.) | 2(переслать) | 3(сбросить)>	= 3
210101014 =	IP Filter Set 1,Rule 1 Act Not Match (Набор фильтров IP 1, правило 1, действие при несоответствии)	<1(проверить след.) | 2(переслать) | 3(сбросить)>	= 1
/ Меню 21.1.1.2 набор #1, правило #2			
FIN	FN	PVA	INPUT
210102001 =	IP Filter Set 1,Rule 2 Type (Фильтр IP, набор 1, правило 2, тип)	<2(TCP/IP)>	= 2
210102002 =	IP Filter Set 1,Rule 2 Active (Фильтр IP, набор 1, правило 2, активный)	<0(Нет) | 1(Да)>	= 1
210102003 =	IP Filter Set 1,Rule 2 Protocol (Набор фильтров IP 1, правило 2, протокол)		= 6
210102004 =	IP Filter Set 1,Rule 2 Dest IP address (Набор фильтров IP 1, правило 2, IP-адрес получателя)		= 0.0.0.0
210102005 =	IP Filter Set 1,Rule 2 Dest Subnet Mask (Набор фильтров IP 1, правило 2, маска подсети получателя)		= 0
210102006 =	IP Filter Set 1,Rule 2 Dest Port (Набор фильтров IP 1, правило 2, порт получателя)		= 138
210102007 =	IP Filter Set 1,Rule 2 Dest Port Comp (Набор фильтров IP 1, правило 2, сравнение порта получателя)	<0(нет)|1(равно)| 2(не равно)| 3(меньше| 4(больше)>	= 1

Табл. 149 Меню 21.1. Набор фильтров #1 (продолжение)

210102008 =	IP Filter Set 1,Rule 2 Src IP address (Набор фильтров IP, набор 1, правило 2, IP-адрес источника)		= 0.0.0.0
210102009 =	IP Filter Set 1,Rule 2 Src Subnet Mask (Набор фильтров IP 1, правило 2, маска подсети отправителя)		= 0
210102010 =	IP Filter Set 1,Rule 2 Src Port (Набор фильтров IP 1, правило 2, порт отправителя)		= 0
210102011 =	IP Filter Set 1,Rule 2 Src Port Comp (Набор фильтров IP 1, правило 2, сравнение порта отправителя)	<0(нет)|1(равно)| 2(не равно)| 3(меньше| 4(больше)>	= 0
210102013 =	IP Filter Set 1,Rule 2 Act Match (Набор фильтров IP 1, правило 2, действие при соответствии)	<1(проверить след.) | 2(переслать) | 3(сбросить)>	= 3
210102014 =	IP Filter Set 1,Rule 2 Act Not Match (Набор фильтров IP 1, правило 2, действие при несоответствии)	<1(проверить след.) | 2(переслать) | 3(сбросить)>	= 1

Табл. 150 Меню 21.1. Набор фильтров #2

/ Меню 21.1 Набор фильтров #2,			
FIN	FN	PVA	INPUT
210200001 =	Filter Set 2, Nam (Набор фильтров 2, название)	<строка>	= NetBIOS_WAN
/ Меню 21.1.2.1 Набор фильтров #2, правило #1			
FIN	FN	PVA	INPUT
210201001 =	IP Filter Set 2,Rule 1 Type (Фильтр IP, набор 2, правило 1, тип)	<0(нет) | 2(TCP/ IP)>	= 2
210201002 =	IP Filter Set 2,Rule 1 Active (Фильтр IP, набор 2, правило 1, активный)	<0(Нет) | 1(Да)>	= 1
210201003 =	IP Filter Set 2,Rule 1 Protocol (Набор фильтров IP 2, правило 1, протокол)		= 6
210201004 =	IP Filter Set 2,Rule 1 Dest IP address (Набор фильтров IP 2, правило 1, IP-адрес получателя)		= 0.0.0.0
210201005 =	IP Filter Set 2,Rule 1 Dest Subnet Mask (Набор фильтров IP 2, правило 1, маска подсети получателя)		= 0
210201006 =	IP Filter Set 2,Rule 1 Dest Port (Набор фильтров IP 2, правило 1, порт получателя)		= 137

Табл. 150 Меню 21.1. Набор фильтров #2 (продолжение)

210201007 =	IP Filter Set 2,Rule 1 Dest Port Comp (Набор фильтров IP 2, правило 1, сравнение порта получателя)	<0(нет)|1(равно)|2 (не равно)| 3(меньше| 4(больше)>	= 1
210201008 =	IP Filter Set 2,Rule 1 Src IP address (Набор фильтров IP, набор 2, правило 1, IP-адрес источника)		=0.0.0.0
210201009 =	IP Filter Set 2,Rule 1 Src Subnet Mask (Набор фильтров IP 2, правило 1, маска подсети отправителя)		= 0
210201010 =	IP Filter Set 2,Rule 1 Src Port (Набор фильтров IP 2, правило 2, порт отправителя)		= 0
210201011 =	IP Filter Set 2,Rule 1 Src Port Comp (Набор фильтров IP 2, правило 1, сравнение порта отправителя)	<0(нет)|1(равно)|2 (не равно)| 3(меньше| 4(больше)>	= 0
210201013 =	IP Filter Set 2,Rule 1 Act Match (Набор фильтров IP 2, правило 1, действие при соответствии)	<1(проверить след.) | 2(переслать) | 3(сбросить)>	= 3
210201014 =	IP Filter Set 2,Rule 1 Act Not Match (Набор фильтров IP 2, правило 1, действие при несоответствии)	<1(проверить след.) | 2(переслать) | 3(сбросить)>	= 1
/ Меню 21.1.2.2 Набор фильтров #2, правило #2			
FIN	FN	PVA	INPUT
210202001 =	IP Filter Set 2,Rule 2 Type (Фильтр IP, набор 2, правило 2, тип)	<0(нет) | 2(TCP/ IP)>	= 2
210202002 =	IP Filter Set 2,Rule 2 Active (Фильтр IP, набор 2, правило 2, активный)	<0(Нет) | 1(Да)>	= 1
210202003 =	IP Filter Set 2,Rule 2 Protocol (Набор фильтров IP 2, правило 2, протокол)		= 6
210202004 =	IP Filter Set 2,Rule 2 Dest IP address (Набор фильтров IP 2, правило 2, IP-адрес получателя)		=0.0.0.0
210202005 =	IP Filter Set 2,Rule 2 Dest Subnet Mask (Набор фильтров IP 2, правило 2, маска подсети получателя)		= 0
210202006 =	IP Filter Set 2,Rule 2 Dest Port (Набор фильтров IP 2, правило 2, порт получателя)		=138
210202007 =	IP Filter Set 2,Rule 2 Dest Port Comp (Набор фильтров IP 2, правило 2, сравнение порта получателя)	<0(нет)|1(равно)|2 (не равно)| 3(меньше| 4(больше)>	= 1

Табл. 150 Меню 21.1. Набор фильтров #2 (продолжение)

210202008 =	IP Filter Set 2,Rule 2 Src IP address (Набор фильтров IP, набор 2, правило 2, IP-адрес источника)		= 0.0.0.0
210202009 =	IP Filter Set 2,Rule 2 Src Subnet Mask (Набор фильтров IP 2, правило 2, маска подсети отправителя)		= 0
210202010 =	IP Filter Set 2,Rule 2 Src Port (Набор фильтров IP 2, правило 2, порт отправителя)		= 0
210202011 =	IP Filter Set 2,Rule 2 Src Port Comp (Набор фильтров IP 2, правило 2, сравнение порта отправителя)	<0(нет)|1(равно)|2 (не равно)| 3(меньше| 4(больше)>	= 0
210202013 =	IP Filter Set 2,Rule 2 Act Match (Набор фильтров IP 2, правило 2, действие при соответствии)	<1(проверить след.) | 2(переслать) | 3(сбросить)>	= 3
210202014 =	IP Filter Set 2,Rule 2 Act Not Match (Набор фильтров IP 2, правило 2, действие при несоответствии)	<1(проверить след.) | 2(переслать) | 3(сбросить)>	= 1

Табл. 151 Меню 23. Системные меню

*/ Меню 23.1 Установка системного пароля			
FIN	FN	PVA	INPUT
230000000 =	System Password (Системный пароль)		= 1234
*/ Меню 23.2 Защитные функции системы: сервер RADIUS			
FIN	FN	PVA	INPUT
230200001 =	Authentication Server Configured (Сервер аутентификации настроен)	<0(Нет) | 1(Да)>	= 1
230200002 =	Authentication Server Active (Сервер аутентификации, активный)	<0(Нет) | 1(Да)>	= 1
230200003 =	Authentication Server IP Address (Сервер аутентификации, IP-адрес)		= 192.168.1.32
230200004 =	Authentication Server Port (Сервер аутентификации, порт)		= 1822
230200005 =	Authentication Server Shared Secret (Сервер аутентификации, общий секретный ключ)		= 1111111111111111 1111111111111111
230200006 =	Accounting Server Configured (Сервер учета настроен)	<0(Нет) | 1(Да)>	= 1
230200007 =	Accounting Server Active (Сервер учета активен)	<0(Нет) | 1(Да)>	= 1

Табл. 151 Меню 23. Системные меню (продолжение)

230200008 =	Accounting Server IP Address (IP-адрес сервера учета)		= 192.168.1.44
230200009 =	Accounting Server Port (Порт сервера учета)		= 1823
230200010 =	Accounting Server Shared Secret (Сервер учета, общий секретный ключ)		= 1234
*/ Меню 23.4 Защитные функции системы: IEEE802.1x			
FIN	FN	PVA	INPUT
230400001 =	Wireless Port Control (Управление беспроводным портом)	<0(требуется аутентификация) | 1(доступ запрещен) | 2(аутентификация не требуется)>	= 2
230400002 =	ReAuthentication Timer (in Seconds) (Таймер повторной аутентификации, сек.)		= 555
230400003 =	Idle Timeout (in second) (Макс. время простоя, сек.)		= 999
230400004 =	Authentication Databases (Базы данных аутентификации)	<0(только БД лок. польз.) | 1(только RADIUS) | 2(лок., RADIUS) | 3(RADIUS, лок.)>	= 1
230400005 =	Key Management Protocol (Протокол управления ключами)	<0(8021x) |1(WPA) |2(WPAPSK)>	= 0
230400006 =	Dynamic WEP Key Exchange (Динамический обмен ключами WEP)	<0(ОТКЛЮЧ.) | 1(64-разрядное шифрование WEP) | 2(128-разрядное шифрование WEP)>	= 0
230400007 =	PSK (Предварительно согласованный ключ) =		=
230400008 =	WPA Mixed Mode (Смешанный режим WPA)	<0(Отключ.) | 1(Включ.)>	= 0
230400009 =	Data Privacy for Broadcast/ Multicast packets (Конфиденциальность данных для пакетов широковещательной/ многоадресной рассылки)	<0(TKIP) |1(WEP)>	= 0
230400010 =	WPA Broadcast/Multicast Key Update Timer (Широковещательная рассылка WPA/Интервал обновления ключа многоадресной рассылки)		= 0

Табл. 152 Меню 24.11 – Контроль удаленного управления

/ Меню 24.11 Контроль удаленного управления			
FIN	FN	PVA	INPUT
241100001 =	TELNET Server Port (Порт сервера TELNET)		= 23
241100002 =	TELNET Server Access (Доступ к серверу TELNET)	<0(LAN+WAN) | 1(недоступен) | 2(LAN) | 3(WAN)>	= 0
241100003 =	TELNET Server Secured IP address (Защищенный IP-адрес сервера TELNET)		= 0.0.0.0
241100004 =	FTP Server Port (Порт сервера FTP)		= 21
241100005 =	FTP Server Access (Доступ к серверу FTP)	<0(LAN+WAN) | 1(недоступен) | 2(LAN) | 3(WAN)>	= 0
241100006 =	FTP Server Secured IP address (Защищенный IP-адрес сервера FTP)		= 0.0.0.0
241100007 =	WEB Server Port (Порт Web-сервера)		= 80
241100008 =	WEB Server Access (Доступ к Web-серверу)	<0(LAN+WAN) | 1(недоступен) | 2(LAN) | 3(WAN)>	= 0
241100009 =	WEB Server Secured IP address (Безопасный IP-адрес WEB-сервера)		= 0.0.0.0

Примеры команд

Далее приводятся экранные формы внутреннего генератора таблицы системных параметров в соответствии с командами интерпретатора команд интернет-центра P660HWP.

Табл. 153 Примеры команд

FIN	FN	PVA	INPUT
/ci command (for annex A): wan adsl opencmd			
FIN	FN	PVA	INPUT
990000001 =	ADSL OPMD	<0(glite)|1(t1.413)|2(gdmt)|3(multimode)>	= 3
/ci command (for annex B): wan adsl opencmd			
FIN	FN	PVA	INPUT
990000001 =	ADSL OPMD	<0(etsi)|1(normal)|2(gdmt)|3(multimode)>	= 3

D

Настройка IP-адреса компьютера

На всех компьютерах должны быть установлены сетевые платы Ethernet 10 или 100 Мбит/с и протоколы TCP/IP.

Операционные системы Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 и выше, а также все версии систем UNIX/LINUX уже содержат программные компоненты, необходимые для инсталляции и использования стека протоколов TCP/IP на вашем компьютере. При использовании ОС Windows 3.1 необходимо приобрести пакет прикладных программ TCP/IP от стороннего производителя.

На компьютерах с операционными системами Windows NT/2000/XP, Macintosh OS 7 (или более поздними) компоненты TCP/IP должны быть уже установлены.

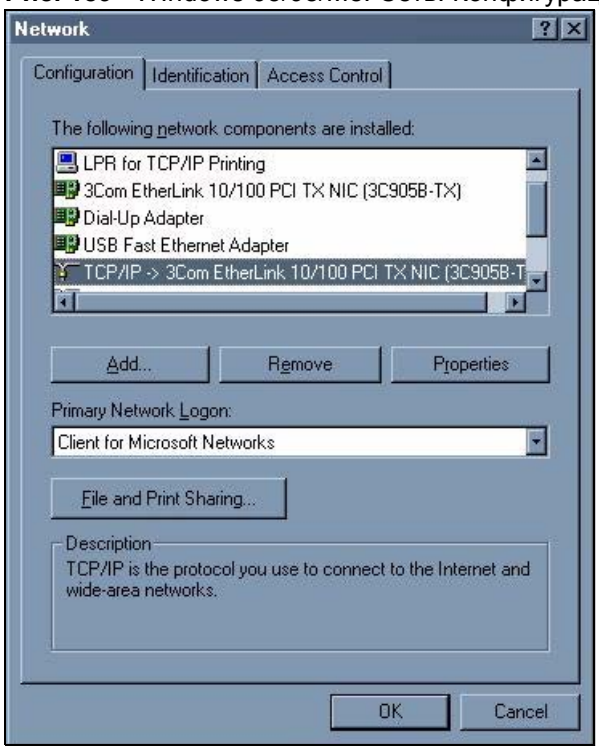
После установки компонентов TCP/IP, настройте параметры TCP/IP для соединения с сетью.

Если вы назначаете IP-адреса вручную, вместо использования динамических адресов, убедитесь, что ваши компьютеры имеют IP-адреса, относящиеся к той же подсети, что и порт LAN P660HWP.

Windows 95/98/Me

Нажмите **Start (Пуск)**, **Settings (Настройка)**, **Control Panel (Панель управления)** и дважды щелкните по значку **Network (Сеть)**, чтобы открыть окно **Network (Сеть)**.

Рис. 189 WIndows 95/98/Me: Сеть: Конфигурация



Установка компонентов

В окне **Network (Сеть)** на закладке **Configuration (Конфигурация)** отображается список установленных компонентов. Вам потребуется сетевая карта, протокол TCP/IP и клиент для сетей Microsoft.

Если необходимо установить сетевую карту:

1. В окне **Network (Сеть)** нажмите **Add (Добавить)**.
2. Выберите **Adapter (Сетевая плата)** и нажмите **Add (Добавить)**.
3. Выберите производителя и модель вашей сетевой карты и нажмите **OK**.

Если необходимо установить протокол TCP/IP:

1. В окне **Network (Сеть)** нажмите **Add (Добавить)**.
2. Выберите **Protocol (Протокол)** и нажмите **Add (Добавить)**.
3. Выберите **Microsoft** из списка **manufacturers (производители)**.
4. Выберите **TCP/IP** из списка сетевых протоколов и нажмите кнопку **OK**.

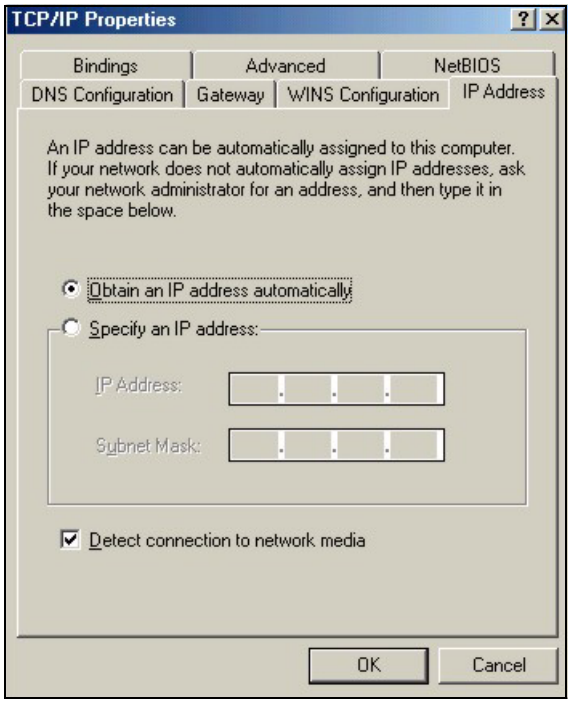
Если необходимо установить Клиента для сетей Microsoft:

1. Нажмите кнопку **Add (Добавить)**.
2. Выберите **Client (Клиент)** и нажмите **Add (Добавить)**.
3. Выберите **Microsoft** из списка производителей.
4. Выберите **Client for Microsoft Networks (Клиент для сетей Microsoft)** из списка сетевых клиентов и нажмите **OK**.
5. Перезагрузите компьютер, чтобы произведенные изменения вступили в силу.

Настройка

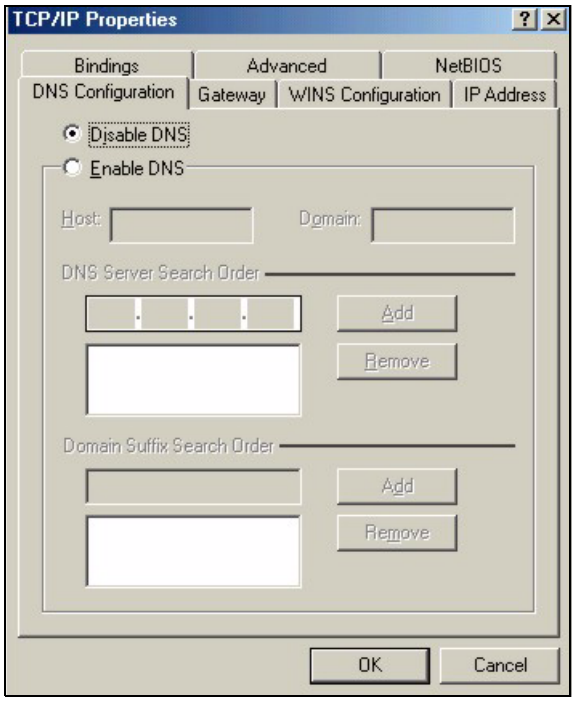
1. В окне **Network (Сеть)** выберите закладку **Configuration (Конфигурация)**, выберите пункт TCP/IP для вашего сетевого адаптера и нажмите **Properties (Свойства)**
2. Выберите закладку **IP-адрес**.
   - Если вы используете динамический IP-адрес, выберите вариант **Obtain an IP address automatically (Получить IP-адрес автоматически)**.
   - Если вы используете статический IP-адрес, выберите вариант **Specify an IP address (Указать IP-адрес явным образом)** и заполните поля **IP address (IP-адрес)** и **Subnet Mask (Маска подсети)**.

Рис. 190 Windows 95/98/Me: Свойства: TCP/IP: IP-адрес



3. Выберите закладку **DNS Configuration (Конфигурация DNS)**.
   - Если вы не знаете параметры DNS, выберите **Disable DNS (Отключить DNS)**.
   - Если вам известны параметры DNS, выберите **Enable DNS (Включить DNS)** и заполните поля, расположенные ниже (возможно, потребуется заполнять не все поля).

Рис. 191 Windows 95/98/Me: Свойства: TCP/IP: Конфигурация DNS



4 Выберите закладку **Gateway (Шлюз)**.
   - Если вы не знаете IP-адрес шлюза, удалите все установленные ранее шлюзы.
   - Если у вас есть IP-адрес шлюза, введите его в поле **New gateway (Новый шлюз)** и нажмите кнопку **Add (Добавить)**.
5 Нажмите **OK**, чтобы сохранить сделанные изменения и закрыть окно **TCP/IP Properties (Свойства: TCP/IP)**.
6 Нажмите кнопку **OK**, чтобы закрыть окно **Network (Сеть)**. При появлении запроса вставьте в дисковод компакт диск Windows.
7 Включите P660HWP и перезагрузите компьютер при появлении запроса.

Проверка настроек

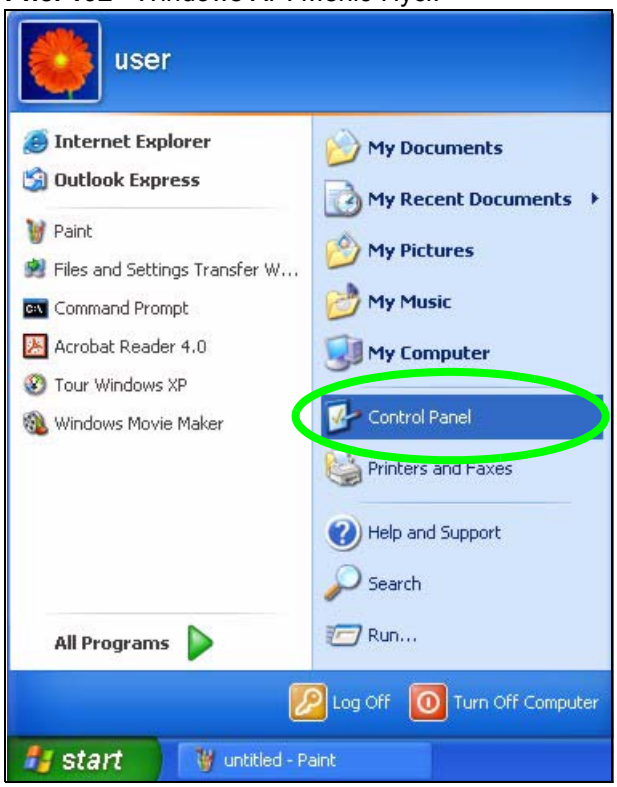
1 Нажмите **Start (Пуск)**, а затем **Run (Выполнить)**.
2 В окне **Run (Выполнить)** введите команду "winipcfg", а затем нажмите **OK** для отображения окна **IP Configuration (Конфигурация IP)**.
3 Выберите свою сетевую карту. При этом должны отображаться IP-адрес и маска подсети вашего компьютера, а также шлюз по умолчанию.

Windows 2000/NT/XP

В следующих примерах используется тема графического интерфейса Windows XP по умолчанию.

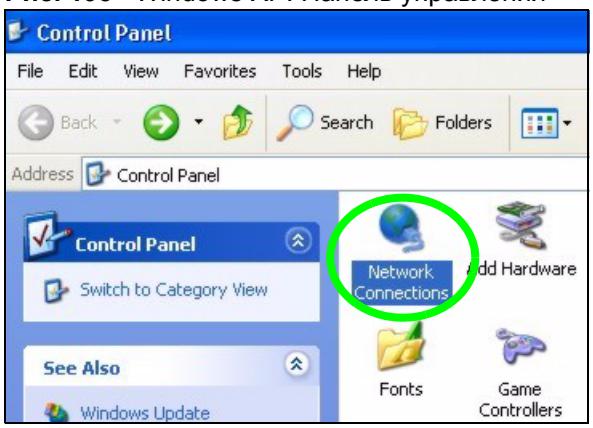
1 Нажмите **start (пуск)** (**Start (Пуск)** в Windows 2000/NT), **Settings (Настройка)**, **Control Panel (Панель управления)**.

Рис. 192 Windows XP: Меню Пуск



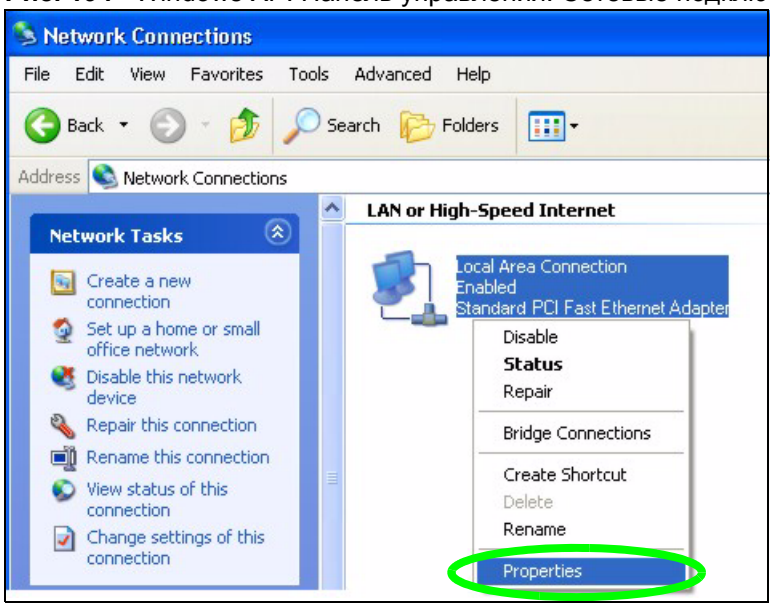
2 На **Панели управления** дважды щелкните **Network Connections (Сетевые подключения)** (**Network and Dial-up Connections (Сеть и удаленный доступ к сети)** в Windows 2000/NT).

Рис. 193 Windows XP: Панель управления



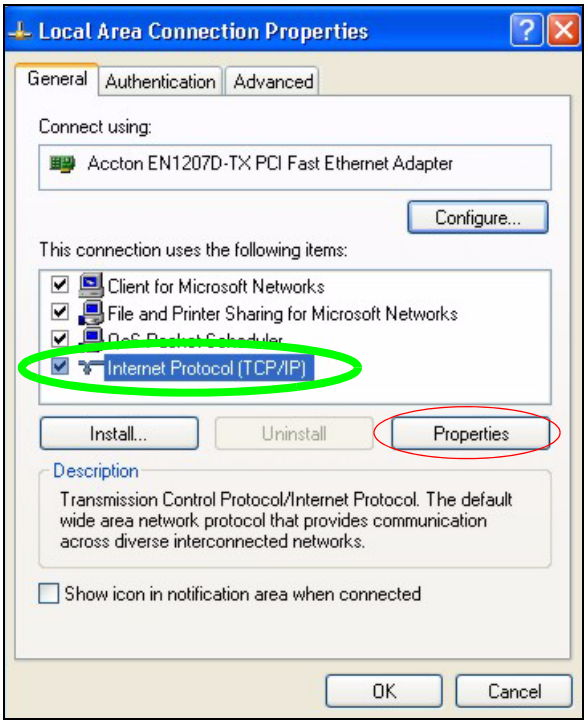
3 Щелкните правой кнопкой мыши **Local Area Connection (Подключение по локальной сети)** и выберите **Properties (Свойства)**.

Рис. 194 Windows XP: Панель управления: Сетевые подключения: Свойства



4 На вкладке **General (Общие)** в WinXP выберите **Internet Protocol (TCP/IP)** (Протокол Интернета (TCP/IP)) и нажмите **Properties (Свойства)**.

Рис. 195 Windows XP: Подключение по локальной сети: Свойства

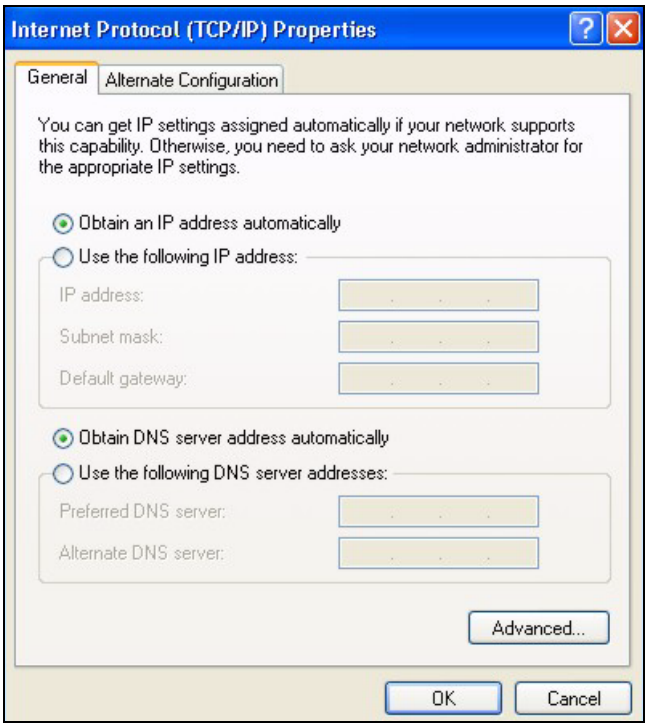


5 Появится окно **Internet Protocol TCP/IP Properties (Свойства: Протокол Интернета (TCP/IP))** (закладка **General (Общие)** в Windows XP).

- Если вы используете динамический IP-адрес, выберите **Obtain an IP address automatically (Получить IP-адрес автоматически)**.

- Если вы имеете статический IP-адрес, выберите **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. 196 Windows XP: Свойства: Протокол Интернета (TCP/IP)



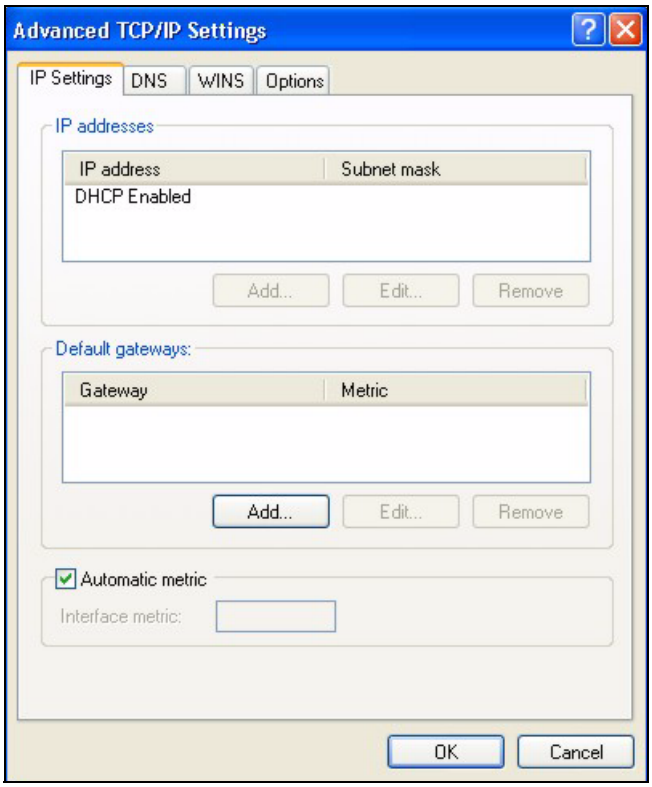
6 Если Вы не знаете IP-адрес шлюза, удалите все предварительно настроенные шлюзы на закладке **IP Settings (Параметры IP)** и нажмите **OK**.

Для настройки дополнительных IP-адресов выполните следующие действия:

- На закладке **IP Settings (Параметры IP)** в поле для IP-адресов нажмите **Add (Добавить)**.
- В окне **Адрес TCP/IP** введите IP-адрес в поле **IP-адрес** и маску подсети в поле **Маска подсети**, затем нажмите кнопку **Добавить**.
- Повторите описанные выше действия для каждого IP-адреса, который необходимо добавить.
- Настройте дополнительные основные шлюзы на закладке **IP Settings (Параметры IP)**, щелкнув по кнопке **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)**. Для ручной настройки метрики по умолчанию (количества транзитных пунктов при передаче), снимите флажок **Automatic metric (Автоматическая метрика)** и введите значение в поле **Metric (Метрика)**.
- Нажмите кнопку **Add (Добавить)**.
- Повторите предыдущие три действия для всех шлюзов, которые необходимо добавить.

- Нажмите **OK** после завершения настройки.

Рис. 197 Windows XP: Дополнительные свойства TCP/IP

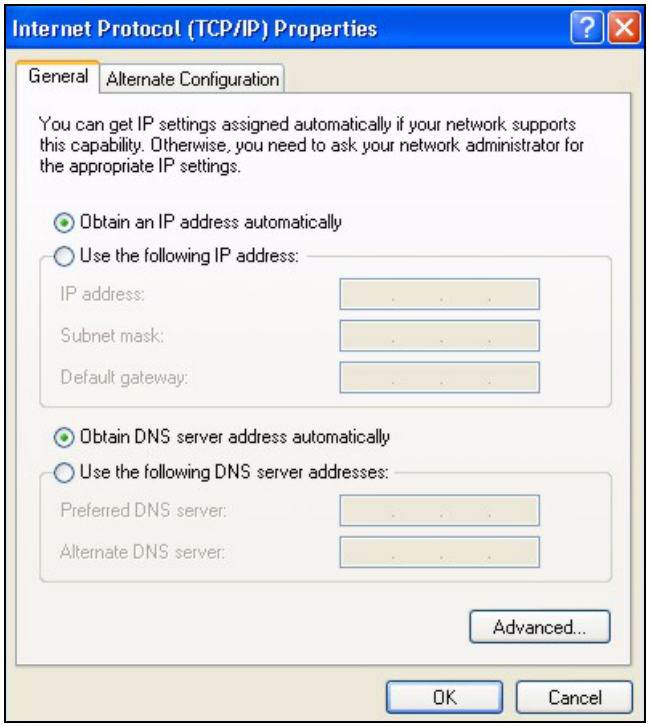


7 В окне **Internet Protocol TCP/IP Properties (Свойства: Протокол Интернета (TCP/IP))** на закладке **General (Общие)** в Windows XP:

- Выберите **Obtain DNS server automatically (Получить адрес DNS-сервера автоматически)**, если вы не знаете IP-адрес(а) сервера(ов) DNS.
- Если вы знаете IP-адрес(а) сервера(ов) DNS, выберите **Use the following DNS server addresses (Использовать следующие адреса серверов DNS)**, и введите адреса в поля **Preferred DNS server (Предпочитаемый DNS-сервер)** и **Alternate DNS server (Альтернативный DNS-сервер)**.

  Если серверы DNS были настроены ранее, нажмите **Advanced (Дополнительно)** и затем закладку **DNS** для определения порядка их использования.

Рис. 198 Windows XP: Свойства: Протокол Интернета (TCP/IP)



8 Нажмите **OK**, чтобы закрыть окно **Internet Protocol (TCP/IP) Properties (Свойства: Протокол Интернета (TCP/IP))**.

9 Нажмите **Close (Закрыть)**, (**OK** в Windows 2000\NT) чтобы закрыть окно **Local Area Connection Properties (Подключение по локальной сети – свойства)**.

10 Закройте окно **Network Connections (Сетевые подключения)** (**Network and Dial-up Connections (Сеть и удаленный доступ к сети)** в Windows 2000/NT).

11 Включите P660HWP и перезагрузите компьютер при появлении запроса.

Проверка настроек

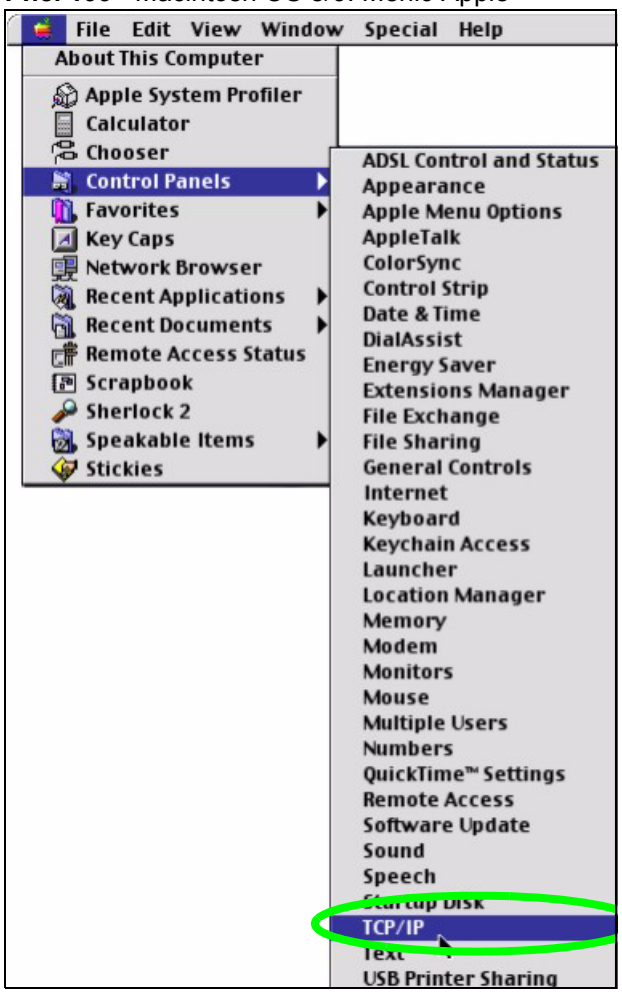
1 Нажмите **Start (Пуск)**, **All Programs (Все программы)**, **Accessories (Стандартные)**, **Command Prompt (Командная строка)**.

2 В окне **Command Prompt (Командная строка)** введите команду «ipconfig» и нажмите клавишу [ENTER]. Также можно открыть окно **Network Connections (Сетевые подключения)**, щелкнуть правой кнопкой мыши на сетевом подключении, выбрать **Status (Состояние)** и затем щелкнуть закладку **Support (Поддержка)**.

Macintosh OS 8/9

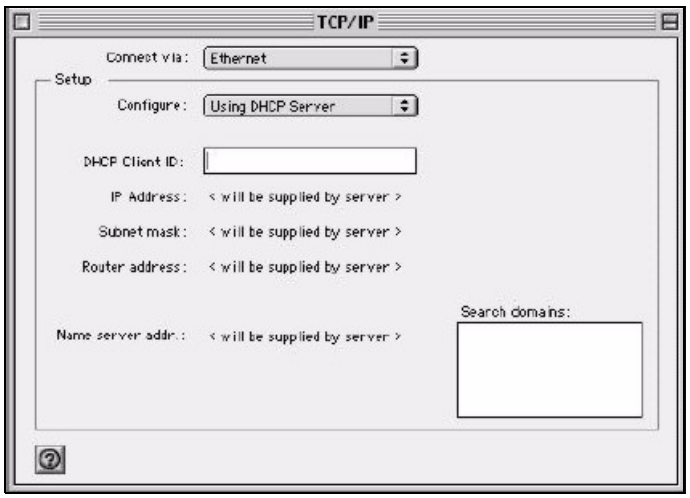
1 Нажмите кнопку меню **Apple**, выберите **Control Panel (Панель управления)**, а затем дважды щелкните **TCP/IP**, чтобы открыть **TCP/IP Control Panel (Панель управления TCP/IP)**.

Рис. 199 Macintosh OS 8/9: Меню Apple



2 Выберите **Ethernet built-in (Встроенный сетевой контроллер)** из списка **Connect via (Подключение через...)**.

Рис. 200 Macintosh OS 8/9: TCP/IP



3 Для настройки динамических параметров выберите **Using DHCP (Использовать сервер DHCP)** в списке **Configure: (Настроить)**.

4 Для настройки статических параметров выполните следующие действия:
   - В разделе **Configure (Настроить)**, выберите **Manually (Настроить вручную)**.
   - Введите IP-адрес в окне **IP Address (IP-адрес)**.
   - Введите маску подсети в окне **Subnet mask (Маска подсети)**.
   - Введите IP-адрес P660HWP в окне **Router address (Адрес маршрутизатора)**.
5 Закройте окно **TCP/IP Control Panel (Панель управления TCP/IP)**.
6 При появлении запроса нажмите **Save (Сохранить)** для сохранения изменений в конфигурации.
7 Включите P660HWP и перезагрузите компьютер при появлении запроса.

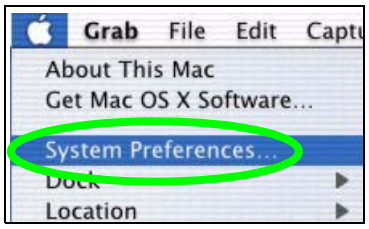
Проверка настроек

Проверьте свойства TCP/IP в окне **TCP/IP Control Panel (Панель управления TCP/IP)**.

Macintosh OS X

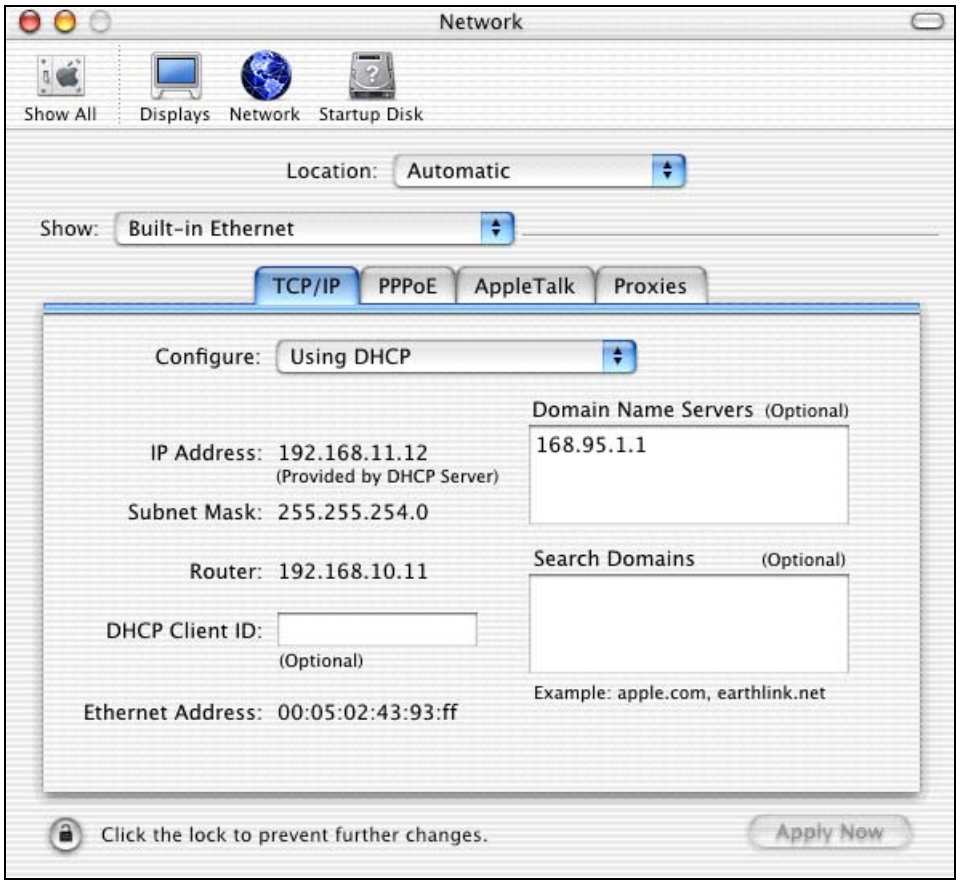
1 Нажмите кнопку меню **Apple** и затем **System Preferences (Настройки системы)**, чтобы открыть окно **System Preferences (Настройки системы)**.

Рис. 201 Macintosh OS X: Меню Apple



2 Щелкните **Network (Сеть)** на панели значков.
   - Выберите **Automatic (Автоматически)** в списке **Location (Местонахождение)**.
   - Выберите **Built-in Ethernet (Встроенный сетевой контроллер)** из списка **Show (Показать)**.
   - Выберите закладку **TCP/IP**.
3 Для динамической настройки параметров выберите **Using DHCP (Использовать DHCP)** в списке **Configure (Настроить)**.

Рис. 202 Macintosh OS X: Сеть



4 Для настройки статических параметров выполните следующие действия:
   - В разделе **Configure (Настроить)**, выберите **Manually (Настроить вручную)**.
   - Введите IP-адрес в окне **IP Address (IP-адрес)**.
   - Введите маску подсети в окне **Subnet mask (Маска подсети)**.
   - Введите IP-адрес P660HWP в окне **Router address (Адрес маршрутизатора)**.
5 Нажмите **Apply Now (Применить)** и закройте окно.
6 Включите P660HWP и перезагрузите компьютер при появлении запроса.

Проверка настроек

Проверьте свойства TCP/IP в окне **Network (Сеть)**.

Linux

В этом разделе описана настройка TCP/IP Вашего компьютера в Red Hat Linux 9.0. Порядок настройки, диалоговые окна и размещение файлов могут различаться в зависимости от версии Linux.

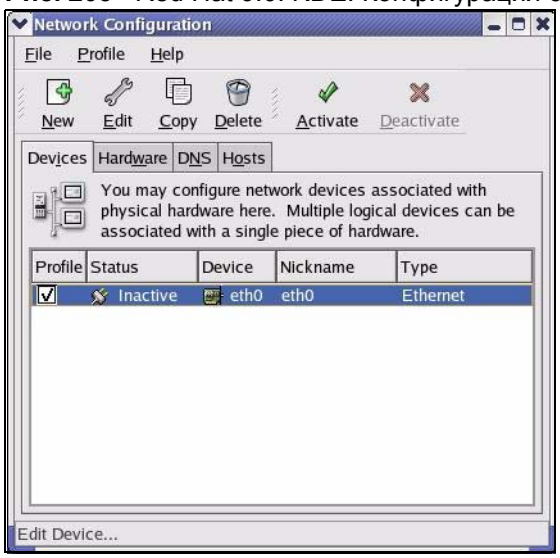
Вы должны быть зарегистрированы в системе в качестве корневого администратора.

Использование графического интерфейса KDE

Для настройки IP-адреса Вашего компьютера с помощью KDE проделайте следующее.

1 Нажмите кнопку Red Hat (в нижнем левом углу экрана), выберите **System Setting (Настройка системы)** и **Network (Сеть)**.

Рис. 203 Red Hat 9.0: KDE: Конфигурация сети: Устройства



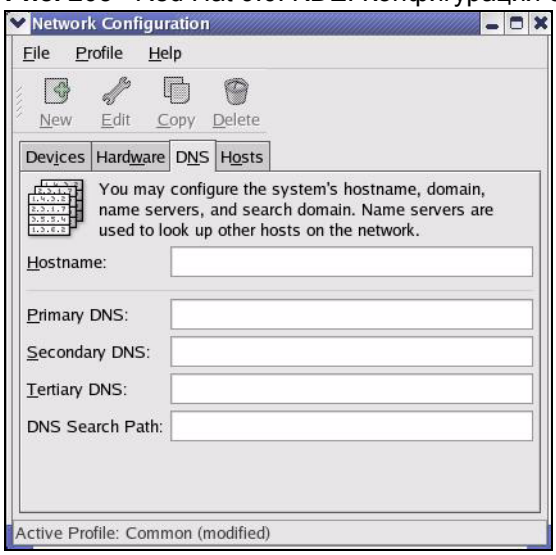
2 Дважды щелкните по профилю сетевой карты, которую Вы хотите настроить. При этом откроется окно **Ethernet Device – General (Устройство Ethernet – Общие)**.

Рис. 204 Red Hat 9.0: KDE: Устройство Ethernet: Общие

- Если у Вас динамический IP-адрес, нажмите **Automatically obtain IP address settings with (Автоматическое получение IP-адреса через...)** и из предложенного списка выберите **DHCP**.
- Если у Вас статический IP-адрес, нажмите **Statically set IP Addresses (Статическое присвоение IP-адреса)** и заполните поля **IP address (IP-адрес)**, **Subnet mask (Маска подсети)** и **Default gateway (Шлюз по умолчанию)**.

3. Нажмите **OK** для сохранения изменений и закройте окно **Ethernet Device General (Устройство Ethernet – Общие)**.
4. Если Вы знаете IP-адрес(а) сервера(ов) DNS, выберите вкладку **DNS** в окне **Network Configuration (Конфигурация сети)**. Введите данные серверов DNS в имеющиеся поля.

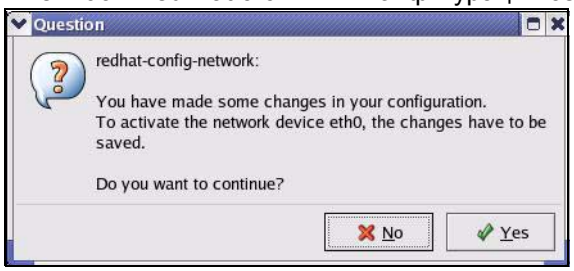
Рис. 205 Red Hat 9.0: KDE: Конфигурация сети: DNS



5. Выберите закладку **Devices (Устройства)**.

6 Нажмите кнопку **Activate (Активировать)** для вступления изменений в силу. Появится следующее окно. Нажмите **Yes (Да)**, чтобы сохранить изменения во всех окнах.

Рис. 206 Red Hat 9.0: KDE: Конфигурация сети: Активировать



7 По завершении перезагрузки сетевой карты убедитесь, что **Status (Состояние)** = **Active (Активен)** в окне **Network Configuration (Конфигурация сети)**.

Использование файлов конфигурации

Для редактирования файлов сетевой конфигурации и настройки IP-адреса Вашего компьютера выполните следующие действия:

1 Предположим, что Ваш компьютер оборудован только одной сетевой картой. Найдите файл конфигурации «`ifconfig-eth0`» (где «`eth0`» – имя карты Ethernet). Откройте его с помощью любого текстового редактора.

- Если у Вас динамический IP-адрес, то введите **«dhcp»** в поле «`BOOTPROTO=`». Пример показан на следующем рисунке.

Рис. 207 Red Hat 9.0: Настройка динамического IP-адреса в файле «ifconfig-eth0»

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- Если у Вас статический IP-адрес, то введите **`static`** в поле «`BOOTPROTO=`». Введите «`IPADDR=`», затем IP-адрес (в десятичном виде с разделительными точками), «`NETMASK=`» и затем маску подсети. В приведенном ниже примере показан статический IP-адрес = 192.168.1.10 и маска подсети = 255.255.255.0.

Рис. 208 Red Hat 9.0: Настройка 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 Вы знаете IP-адрес(а) Вашего сервера DNS, то введите информацию о сервере DNS в файл «`resolv.conf`» в каталоге «`/etc`». В следующем примере показан ввод двух IP-адресов сервера DNS.

Рис. 209 Red Hat 9.0: Установка параметров DNS в файле «resolv.conf»

```
nameserver 172.23.5.1
nameserver 172.23.5.2
```

3 После того как Вы отредактируете и сохраните файлы конфигурации, необходимо перезагрузить сетевую карту. Введите «`./network restart`» в каталоге «`/etc/rc.d/init.d`». Пример показан на следующем рисунке.

Рис. 210 Red Hat 9.0: Перезапуск карты Ethernet

```
[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, введите «`ifconfig`» в окне терминала.

Рис. 211 Red Hat 9.0: Проверка свойств протокола 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]#
```

E

Организация подсетей IP

В этом приложении представлена информация об IP-адресах, классах IP-адресов и масках подсети.

Описание IP-адресов

IP-адрес состоит их четырех байтов, записанных в десятичном формате с разделительными точками, например: 192.168.1.1. Байт – это 8-значное двоичное число. Следовательно, каждый байт имеет диапазон возможных значений от 00000000 до 11111111 в двоичном формате, или от 0 до 256 в десятичном.

IP-адрес состоит из двух частей: номера сети и идентификатора узла. Номер сети используется маршрутизаторами при отправке пакетов в соответствующую сеть, а идентификатор узла определяет конкретное устройство в этой сети.

Классы IP-адресов и узлы

Класс IP-адреса определяет максимальное количество узлов в сети.

- В адресах класса A первый байт является номером сети, а оставшиеся три байта являются идентификатором узла.
- В адресах класса B первые два байта являются номером сети, а оставшиеся два байта являются идентификатором узла.
- В адресах класса C первые три байта составляют номер сети, а последний байт является идентификатором узла.

В следующей таблице показано расположение номера сети и идентификатора узла в IP-адресе для классов A, B и C.

Табл. 154 Классы IP-адресов

IP-АДРЕС	БАЙТ 1	БАЙТ 2	БАЙТ 3	БАЙТ 4
Класс A	**Номер сети**	Идентификатор узла	Идентификатор узла	Идентификатор узла
Класс B	**Номер сети**	**Номер сети**	Идентификатор узла	Идентификатор узла
Класс C	**Номер сети**	**Номер сети**	**Номер сети**	Идентификатор узла

IP-адрес, в котором идентификатор узла состоит только из нулей, является IP-адресом сети. IP-адрес, в котором идентификатор узла состоит только из единиц, является широковещательным адресом этой сети. Следовательно, общее число узлов, допустимых в сети, рассчитывается следующим образом:

- В сети класса C (1 байт для идентификатора узла: 8 битов) может находиться $2^8 – 2 = 254$ узла.
- В сети класса B (2 байта для идентификатора узла: 16 битов) может находиться $2^{16} – 2 = 65534$ узла.

В сети класса A (3 байта для идентификатора узла: 24 бита) может находиться $2^{24} – 2$, или примерно 16 миллионов узлов.

Классы IP-адресов и номер сети

Значение первого байта IP-адреса определяет класс адреса.

- Адреса класса A содержат **0** в крайнем левом бите.
- Адреса класса B содержат **1** в крайнем левом бите и **0** в следующем бите.
- Адреса класса C начинаются с **1 1 0** в трех крайних левых битах.
- Адреса класса D начинаются с **1 1 1 0**. Адреса класса D применяются для многоадресной рассылки, которая используется для отправки информации группе компьютеров.
- Еще существуют адреса класса E. Они зарезервированы для будущего использования.

В следующей таблице приведены диапазоны допустимых значений битов первого байта адреса для каждого класса. Диапазоны определяют количество подсетей, допустимых в данной сети.

Табл. 155 Допустимые диапазоны IP-адресов для каждого класса

КЛАСС	ДОПУСТИМЫЙ ДИАПАЗОН ЗНАЧЕНИЙ ПЕРВОГО БАЙТА (В ДВОИЧНОЙ ЗАПИСИ)	ДОПУСТИМЫЙ ДИАПАЗОН ЗНАЧЕНИЙ ПЕРВОГО БАЙТА (В ДЕСЯТИЧНОЙ ЗАПИСИ)
Класс A	от **0**0000000 до **0**1111111	от 0 до 127
Класс B	от **10**000000 до **10**111111	от 128 до 191
Класс C	от **110**00000 до **110**11111	от 192 до 223
Класс D	от **1110**0000 до **1110**1111	от 224 до 239
Класс E (зарезер-вированы)	от **1111**0000 до **1111**1111	от 240 до 255

Маска подсети

С помощью маски подсети можно определить, какие биты являются частью номера сети, а какие – частью идентификатора узла (используя операцию логического «И»).

Маска подсети состоит из 32 битов. Если бит маски подсети имеет значение «1», это значит, что соответствующий бит IP-адреса является частью номера сети. Если бит маски подсети имеет значение «0», это значит, что соответствующий бит IP-адреса является частью идентификатора узла.

Маски подсети записываются в десятичном виде с разделительными точками, так же, как и IP-адреса. «Естественные» маски для классов IP-адресов A, B и C приведены ниже.

Табл. 156 «Естественные» маски

КЛАСС	ЕСТЕСТВЕННАЯ МАСКА
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Организация подсетей

При организации подсетей распределение IP-адресов по классам игнорируется. Например, адрес класса C не обязательно должен иметь номер сети из 24 бит и идентификатор узла из 8 бит. При организации подсетей некоторые биты идентификатора узла можно использовать в качестве битов номера сети.

По договоренности маска подсети всегда состоит из непрерывной последовательности единиц в начале маски (слева), за которой следует непрерывная последовательность нулей общей длиной в 32 бита.

Поскольку маска всегда состоит из непрерывной последовательности сначала единиц и затем непрерывной последовательности нулей общей длиной 32 бита, можно просто указывать количество единиц вместо того, чтобы определять значение каждого байта. Это обычно обозначается посредством записи после адреса символа «/» и количества бит с единицами.

Например, запись 192.1.1.0 /25 равносильна 192.1.1.0 с маской 255.255.255.128.

В следующей таблице приведены все возможные маски подсети для адресов класса C, записанные в двух вариантах.

Табл. 157 Альтернативные варианты записи маски подсети

МАСКА ПОДСЕТИ	МАСКА ПОДСЕТИ ПРИ ЗАПИСИ КОЛИЧЕСТВА ЕДИНИЦ	ЗНАЧЕНИЯ БИТОВ ПОСЛЕДНЕГО БАЙТА
255.255.255.0	/24	0000 0000
255.255.255.128	/25	1000 0000
255.255.255.192	/26	1100 0000
255.255.255.224	/27	1110 0000
255.255.255.240	/28	1111 0000
255.255.255.248	/29	1111 1000
255.255.255.252	/30	1111 1100

Первая маска – это естественная маска класса C. Обычно, если маска подсети не указана, то считается, что используется естественная маска.

Пример: Две подсети

В качестве примера рассмотрим адрес класса «C» 192.168.1.0 с маской подсети 255.255.255.0.

Табл. 158 Пример организации 2-х подсетей

IP/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ИДЕНТИФИКАТОР УЗЛА
IP-адрес	192.168.1.	0
IP-адрес (в двоичной форме)	11000000.10101000.00000001.	00000000
маска подсети	255.255.255.	0
Маска подсети (в двоичной форме)	11111111.11111111.11111111.	00000000

Первые три байта адреса образуют номер сети (класс «C»).

Для организации двух сетей нужно разделить сеть 192.168.1.0 на две отдельные логические подсети с помощью преобразования одного бита из идентификатора узла в IP-адресе в бит номера сети. «Заимствованный» бит идентификатора узла может принимать значения 0 или 1, давая, таким образом, две подсети; 192.168.1.0 с маской 255.255.255.128 и 192.168.1.128 с маской 255.255.255.128.

В следующих таблицах выделенным шрифтом обозначены значения битов последнего байта, «заимствованные» из идентификатора узла для образования дополнительных битов номера сети. Количество «заимствованных» битов идентификатора узла определяет число подсетей, которые вы можете создать. Оставшееся (после «заимствования») количество битов идентификатора узла определяет максимально возможное количество узлов в каждой подсети.

Табл. 159 Подсеть 1

IP/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ЗНАЧЕНИЯ БИТОВ ПОСЛЕДНЕГО БАЙТА
IP-адрес	192.168.1.	0
IP-адрес (в двоичной форме)	11000000.10101000.00000001.	**0**0000000
маска подсети	255.255.255.	128
Маска подсети (в двоичной форме)	11111111.11111111.11111111.	**1**0000000
Адрес подсети: 192.168.1.0	Минимальный идентификатор узла: 192.168.1.1	
Адрес широковещательной рассылки: 192.168.1.127	Максимальный идентификатор узла: 192.168.1.126	

Табл. 160 Подсеть 2

IP/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ЗНАЧЕНИЯ БИТОВ ПОСЛЕДНЕГО БАЙТА
IP-адрес	192.168.1.	128
IP-адрес (в двоичной форме)	11000000.10101000.00000001.	**1**0000000
маска подсети	255.255.255.	128
Маска подсети (в двоичной форме)	11111111.11111111.11111111.	**1**0000000
Адрес подсети: 192.168.1.128	Минимальный идентификатор узла: 192.168.1.129	
Адрес широковещательной рассылки: 192.168.1.255	Максимальный идентификатор узла: 192.168.1.254	

Идентификаторы узлов, состоящие только из нулей, представляют собственно подсеть, а идентификаторы узлов, состоящие только из единиц, являются адресами широковещательной рассылки для каждой подсети, поэтому реальное количество доступных узлов для каждой подсети для данного примера равно $2^7 – 2$, т. е. 126 узлов в каждой подсети.

192.168.1.0 с маской 255.255.255.128 это сама сеть, а 192.168.1.127 с маской 255.255.255.128 является адресом направленной широковещательной рассылки первой подсети. Следовательно, самый младший IP-адрес, который может быть назначен действительному узлу для первой подсети – 192.168.1.1, а старший – 192.168.1.126. Аналогично диапазон адресов для узлов второй подсети – от 192.168.1.129 до 192.168.1.254.

Пример: четыре подсети

В примере выше демонстрируется использование 25-битной маски подсети для разделения адресного пространства класса «C» на две подсети. Аналогично для разделения адреса класса C на четыре подсети, потребуется «заимствовать» два бита из идентификатора узла для получения четырех возможных комбинаций: 00, 01, 10 и 11. Маска подсети имеет 26 бит (11111111.11111111.11111111.**11**000000) или 255.255.255.192. Каждая подсеть имеет 6 битов для идентификатора узла, при этом получается $2^6 – 2 = 62$ узла в каждой подсети (все нули обозначают саму подсеть, все единицы являются широковещательным адресом этой подсети).

Табл. 161 Подсеть 2

IP/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ЗНАЧЕНИЯ БИТОВ ПОСЛЕДНЕГО БАЙТА
IP-адрес	192.168.1.	64
IP-адрес (в двоичной форме)	11000000.10101000.00000001.	**01**000000
Маска подсети (в двоичной форме)	11111111.11111111.11111111.	**11**000000

Табл. 161 Подсеть 2 (продолжение)

IP/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ЗНАЧЕНИЯ БИТОВ ПОСЛЕДНЕГО БАЙТА
Адрес подсети: 192.168.1.64	Минимальный идентификатор узла: 192.168.1.65	
Адрес широковещательной рассылки: 192.168.1.127	Максимальный идентификатор узла: 192.168.1.126	

Табл. 162 Подсеть 3

IP/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ЗНАЧЕНИЯ БИТОВ ПОСЛЕДНЕГО БАЙТА
IP-адрес	192.168.1.	128
IP-адрес (в двоичной форме)	11000000.10101000.00000001.	**10**000000
Маска подсети (в двоичной форме)	11111111.11111111.11111111.	**11**000000
Адрес подсети: 192.168.1.128	Минимальный идентификатор узла: 192.168.1.129	
Адрес широковещательной рассылки: 192.168.1.191	Максимальный идентификатор узла: 192.168.1.190	

Табл. 163 Подсеть 4

IP/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ЗНАЧЕНИЯ БИТОВ ПОСЛЕДНЕГО БАЙТА
IP-адрес	192.168.1.	192
IP-адрес (в двоичной форме)	11000000.10101000.00000001.	**11**000000
Маска подсети (в двоичной форме)	11111111.11111111.11111111.	**11**000000
Адрес подсети: 192.168.1.192	Минимальный идентификатор узла: 192.168.1.193	
Адрес широковещательной рассылки: 192.168.1.255	Максимальный идентификатор узла: 192.168.1.254	

Табл. 164 Подсеть 1

IP/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ЗНАЧЕНИЯ БИТОВ ПОСЛЕДНЕГО БАЙТА
IP-адрес	192.168.1.	0
IP-адрес (в двоичной форме)	11000000.10101000.00000001.	**00**000000
Маска подсети (в двоичной форме)	11111111.11111111.11111111.	**11**000000
Адрес подсети: 192.168.1.0	Минимальный идентификатор узла: 192.168.1.1	
Адрес широковещательной рассылки: 192.168.1.63	Максимальный идентификатор узла: 192.168.1.62	

Пример: восемь подсетей

Аналогично используется 27-битная маска для создания 8 подсетей (000, 001, 010, 011, 100, 101, 110 и 111).

В следующей таблице приведены значения битов последнего байта адреса класса C для каждой подсети.

Табл. 165 Восемь подсетей

ПОДСЕТЬ	АДРЕС ПОДСЕТИ	ПЕРВЫЙ АДРЕС	ПОСЛЕДНИЙ АДРЕС	ШИРОКОВЕЩА-ТЕЛЬНЫЙ 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

В следующей таблице приведены сводные данные по организации подсетей класса «C».

Табл. 166 Организация подсетей класса «C»

КОЛИЧЕСТВО «ЗАИМСТВОВАННЫХ» БИТОВ УЗЛА	МАСКА ПОДСЕТИ	КОЛИЧЕСТВО ПОДСЕТЕЙ	КОЛИЧЕСТВО УЗЛОВ В КАЖДОЙ ПОДСЕТИ
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

Организация подсетей в сетях класса A и класса B.

Для адресов класса «A» и класса «B» маска подсети также определяет, какие биты являются частью номера сети, а какие – частью идентификатора узла.

Адрес класса B имеет два байта идентификаторов узлов для организации подсетей, а адрес класса A – три байта идентификаторов узлов (см. Табл. 154 на с. 393) для организации подсетей.

В следующей таблице приведены сводные данные по организации подсетей класса «B».

Табл. 167 Организация подсетей класса B

КОЛИЧЕСТВО «ЗАИМСТВОВАННЫХ» БИТОВ УЗЛА	МАСКА ПОДСЕТИ	КОЛИЧЕСТВО ПОДСЕТЕЙ	КОЛИЧЕСТВО УЗЛОВ В КАЖДОЙ ПОДСЕТИ
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

F

Интерпретатор команд

Ниже приводятся инструкции по работе с интерпретатором команд. Доступ к CLI (Command Line Interface - интерфейс командной строки) P660HWP можно получить с помощью Telnet. Более подробная информация по этим командам находится на компакт-диске, входящем в комплект поставки, а также на web-сайте www.zyxel.ru.

Использование не описанных в документации команд или неправильная настройка могут повредить устройство или полностью вывести его из строя.

Подключение к CLI

Чтобы подключиться к устройству P660HWP с помощью Telnet, выполните следующие действия:

1. Подключите компьютер к порту **ETHERNET** интернет-центра P660HWP.
2. Проверьте, что IP-адрес компьютера и IP-адрес P660HWP находятся в одной подсети. В Windows щелкните **Start (Пуск)** (обычно в левом нижнем углу), **Run (Выполнить)**, а затем ведите команду `telnet 192.168.1.1` (IP-адрес P660HWP по умолчанию) и щелкните **OK**.
3. На экране появится окно регистрации. Введите пароль администратора по умолчанию «1234».

Синтаксис команд

- Ключевые слова команд выделены шрифтом `courier new`.
- Ключевые слова команды необходимо вводить в точности так, как показано, без использования сокращений.
- Обязательные поля команды заключаются в угловые скобки <>.
- Необязательные поля команды заключаются в квадратные скобки `[]`.
- Символ `|` означает "или".

  Например:

  sys filter netbios config <type> <on|off>

  означает, что необходимо указать тип фильтра NetBIOS и включить либо отключить его.

Использование команд

Для отображения списка доступных команд введите `help` или `?` в командной строке. Команду всегда следует вводить полностью. Для завершения сеанса CLI введите `exit`.

Команды регистрационного журнала

В этом разделе представлено несколько примеров использования команд регистрационного журнала. Отображаемая информация для конкретной модели может отличаться от приведенной, но основные функции являются аналогичными.

Перейдите к интерфейсу интерпретатора команд.

Настройка регистрационного журнала интернет-центра P660HWP

1. Команда «sys logs load» используется для загрузки буфера настроек журнальной регистрации, позволяющего установить категории журнала, которые должен записывать P660HWP.
2. Для просмотра списка категорий регистрационных записей используйте команду «sys logs category».

Рис. 212 Пример отображения категорий регистрационных записей

```
Copyright (c) 1994 - 2006 ZyXEL Communications Corp.
ras>?
Valid commands are:
sys             exit            ether           aux
ip              ipsec           bridge          bm
certificates    cnm             8021x           radius
ras>
```

3. Для отображения параметров, имеющихся для данной категории, используется команда «sys logs category», после которой указывается категория журнальной записи.

Рис. 213 Пример отображения параметров регистрационных записей

```
ras> sys logs category access
Usage: [0:none/1:log/2:alert/3:both] [0:don't show debug type/1:show debug
type]
```

4. Для определения записей, подлежащих регистрации в журнале, используется команда «sys logs category», после которой указывается категория журнальной записи и параметр.

Если записи данной категории не должны регистрироваться, введите 0, если должны регистрироваться только записи данной категории, введите 1, если должны регистрироваться только предупреждения данной категории, введите 2, если же должны регистрироваться и записи, и предупреждения данной категории, введите 3. Не все параметры доступны для каждой категории.

5 Для сохранения настроек интернет-центра P660HWP (это необходимо выполнить, чтобы велась запись журналов) используется команда «sys logs save».

Отображение журнальных записей

- Команда «sys logs display» используется для отображения всех записей журнала интернет-центра P660HWP.
- Для отображения настроек всех категорий журналов модема используйте команду «sys logs category display».
- Для отображения записей отдельной категории журнала интернет-центра P660HWP используется команда «sys logs display [log category]».
- Для удаления всех записей журнала интернет-центра P660HWP используется команда «sys logs clear».

Пример команды управления журналом

В этом примере показано, как настроить интернет-центр P660HWP для регистрации сообщений и предупреждений о входе в систему и затем выполнить 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)
 1|06/08/2004 05:58:20 |172.21.3.56           |239.255.255.250       |ACCESS
BLOCK
    Firewall default policy: IGMP (W to W)
 2|06/08/2004 05:58:20 |172.21.0.2            |239.255.255.254       |ACCESS
BLOCK
    Firewall default policy: IGMP (W to W)
 3|06/08/2004 05:58:20 |172.21.3.191          |224.0.1.22            |ACCESS
BLOCK
    Firewall default policy: IGMP (W to W)
 4|06/08/2004 05:58:20 |172.21.0.254          |224.0.0.1             |ACCESS
BLOCK
    Firewall default policy: IGMP (W to W)
 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)
```

G

Команды управления межсетевым экраном

Ниже дается описание команд управления межсетевым экраном.

Табл. 168 Команды управления межсетевым экраном

ФУНКЦИЯ	КОМАНДА	ОПИСАНИЕ
Настройка межсетевого экрана		
	`config edit firewall active <yes | no>`	Включить/выключить межсетевой экран.
	`config retrieve firewall`	Вернуться к ранее сохраненным настройкам межсетевого экрана.
	`config save firewall`	Сохранить текущие настройки межсетевого экрана.
Вывод информации		
	`config display firewall`	Показать настройки межсетевого экрана: электронная почта, атаки, наборы правил.
	`config display firewall set <set #>`	Эта команда отображает текущую конфигурацию набора, включая время простоя, имя, разрешения по умолчанию и т.д. Если не указано число (#) после «set», то отображается информация обо всех наборах/правилах.
	`config display firewall set <set #> rule <rule #>`	Показать текущие данные по одному из правил в наборе.
	`config display firewall attack`	Показать настройки ответов на атаки.
	`config display firewall e-mail`	Показать настройки электронной почты.
	`config display firewall?`	Показать все имеющиеся подкоманды межсетевого экрана.

Табл. 168 Команды управления межсетевым экраном (продолжение)

ФУНКЦИЯ	КОМАНДА	ОПИСАНИЕ
Изменение		
E-Mail	`config edit firewall e-mail mail-server <ip address of mail server>`	Указать IP-адрес, на который отсылаются электронные сообщения.
	`config edit firewall e-mail return-addr <e-mail address>`	Указать адрес электронной почты, с которого будут отсылаться сообщения межсетевого экрана.
	`config edit firewall e-mail email-to <e-mail address>`	Указать адрес электронной почты, на который будут отсылаться сообщения межсетевого экрана.
	`config edit firewall e-mail policy <full | hourly | daily | weekly>`	Указать частоту рассылки журнала сообщений межсетевого экрана по электронной почте.
	`config edit firewall e-mail day <sunday | monday | tuesday | wednesday | thursday | friday | saturday>`	Эта команда устанавливает день для отправки текущего регистрационного журнала межсетевого экрана по электронной почте, если настройки P660HWP установлены на отправку по дням недели.
	`config edit firewall e-mail hour <0-23>`	Эта команда устанавливает часы для отправки текущего регистрационного журнала межсетевого экрана по электронной почте, если настройки P660HWP установлены на отправку по часам, ежедневно или по дням недели.
	`config edit firewall e-mail minute <0-59>`	Эта команда устанавливает минуты для отправки текущего регистрационного журнала межсетевого экрана по электронной почте, если настройки P660HWP установлены на отправку по часам, ежедневно или по дням недели.
Атака	`config edit firewall attack send-alert <yes | no>`	Включить или отключить немедленное уведомление об атаках DOS по e-mail.
	`config edit firewall attack block <yes | no>`	Установить «yes» (да) для блокирования нового трафика после превышения порога «tcp-max-incomplete». Установить «no» (нет) для удаления самых старых полуоткрытых сессий в случае, если трафик превышает допустимый порог «tcp-max-incomplete».

Табл. 168 Команды управления межсетевым экраном (продолжение)

ФУНКЦИЯ	КОМАНДА	ОПИСАНИЕ
	config edit firewall attack block-minute <0-255>	Установить время в минутах, по истечении которого блокируются новые сессии при превышении допустимого порога tcp-max-incomplete. Данная команда действительна только если в поле «block» (блокировать) установлено «yes» (да).
	config edit firewall attack minute-high <0-255>	Устанавливает максимально допустимое количество новых полуоткрытых сеансов связи в минуту, при котором P660HWP начинает удалять старые полуоткрытые сеансы, пока их число не достигнет минимального значения (minute-low threshold).
	config edit firewall attack minute-low <0-255>	Устанавливает допустимое количество полуоткрытых сеансов связи, при котором P660HWP прекращает удаление полуоткрытых сессий.
	config edit firewall attack max-incomplete-high <0-255>	Устанавливает максимально допустимое количество полуоткрытых сеансов связи, при котором P660HWP начинает удалять старые полуоткрытые сеансы, пока их число не достигнет минимального значения (max incomplete low).
	config edit firewall attack max-incomplete-low <0-255>	Устанавливает порог, при котором P660HWP прекращает удаление полуоткрытых сеансов связи.
	config edit firewall attack tcp-max-incomplete <0-255>	Устанавливает максимально допустимое количество полуоткрытых сеансов TCP с одним адресом назначения, при котором P660HWP начинает сбрасывать полуоткрытые сеансы с этим адресом назначения.
Наборы	config edit firewall set <set #> name <desired name>	Указать идентификационное имя конкретного набора.
	Config edit firewall set <set #> default-permit <forward | block>	Сбрасывать или разрешать пакет, не удовлетворяющий правилам в наборе.
	Config edit firewall set <set #> icmp-timeout <seconds>	Установить время ожидания ответа ICMP во время сессии ICMP.

Табл. 168 Команды управления межсетевым экраном (продолжение)

ФУНКЦИЯ	КОМАНДА	ОПИСАНИЕ
	`Config edit firewall set <set #> udp-idle-timeout <seconds>`	Устанавливает время простоя соединения UDP, по истечении которого P660HWP завершает это соединение.
	`Config edit firewall set <set #> connection-timeout <seconds>`	Устанавливает время ожидания на установление сеанса связи TCP, прежде чем P660HWP сбросит подключение.
	`Config edit firewall set <set #> fin-wait-timeout <seconds>`	Устанавливает время, в течение которого соединение TCP остается открытым, после того как межсетевой экран P660HWP обнаружит FIN-пакет (что означает конец сеанса TCP).
	`Config edit firewall set <set #> tcp-idle-timeout <seconds>`	Устанавливает время, в течение которого неактивное соединение TCP остается открытым, прежде чем P660HWP завершит это соединение.
	`Config edit firewall set <set #> log <yes | no>`	Включает или выключает ведение записей в регистрационном журнале для пакетов, удовлетворяющих набору правил межсетевого экрана P660HWP, установленному по умолчанию.
Правила	`Config edit firewall set <set #> rule <rule #> permit <forward | block>`	Сбрасывать или разрешать пакеты, соответствующие данному правилу.
	`Config edit firewall set <set #> rule <rule #> active <yes | no>`	Включить или отключить данное правило.
	`Config edit firewall set <set #> rule <rule #> protocol <integer protocol value >`	Указать номер спецификации протокола в данном правиле для ICMP.
	`Config edit firewall set <set #> rule <rule #> log <none | match | not-match | both>`	Устанавливает режим P660HWP для регистрации трафика: при соответствии правилу, несоответствии, и в том и другом случае или не регистрировать.
	`Config edit firewall set <set #> rule <rule #> alert <yes | no>`	Включает или выключает отправку предупреждений по электронной почте, если P660HWP обнаруживает атаку DOS или нарушение конкретного правила.

Табл. 168 Команды управления межсетевым экраном (продолжение)

ФУНКЦИЯ	КОМАНДА	ОПИСАНИЕ
	config edit firewall set <set #> rule <rule #> srcaddr-single <ip address>	Устанавливает правило, по которому P660HWP будет проверять трафик с указанным адресом источника.
	config edit firewall set <set #> rule <rule #> srcaddr-subnet <ip address> <subnet mask>	Устанавливает правило, по которому P660HWP будет проверять трафик от указанной подсети (указывается IP-адрес и маска подсети).
	config edit firewall set <set #> rule <rule #> srcaddr-range <start ip address> <end ip address>	Устанавливает правило, по которому P660HWP будет проверять трафик от указанного диапазона адресов.
	config edit firewall set <set #> rule <rule #> destaddr-single <ip address>	Устанавливает правило, по которому P660HWP будет проверять трафик с указанным адресом назначения.
	config edit firewall set <set #> rule <rule #> destaddr-subnet <ip address> <subnet mask>	Устанавливает правило, по которому P660HWP будет проверять трафик с указанным адресом подсети назначения (указывается IP-адрес и маска подсети).
	config edit firewall set <set #> rule <rule #> destaddr-range <start ip address> <end ip address>	Устанавливает правило, по которому P660HWP будет проверять трафик с адресом назначения из данного диапазона адресов.
	config edit firewall set <set #> rule <rule #> TCP destport-single <port #>	Устанавливает правило, по которому P660HWP будет проверять трафик TCP с указанным адресом назначения. Эту команду можно повторить с различными (неповторяющимися) номерами портов.
	config edit firewall set <set #> rule <rule #> TCP destport-range <start port #> <end port #>	Устанавливает правило, по которому P660HWP будет проверять трафик TCP с портом назначения из указанного диапазона портов.
	config edit firewall set <set #> rule <rule #> UDP destport-single <port #>	Устанавливает правило, по которому P660HWP будет проверять трафик UDP с указанным адресом назначения. Эту команду можно повторить с различными (неповторяющимися) номерами портов.

Табл. 168 Команды управления межсетевым экраном (продолжение)

ФУНКЦИЯ	КОМАНДА	ОПИСАНИЕ
	`config edit firewall set <set #> rule <rule #> UDP destport-range <start port #> <end port #>`	Устанавливает правило, по которому P660HWP будет проверять трафик UDP с портом назначения из указанного диапазона портов.
Удаление		
	`config delete firewall e-mail`	Удалить все настройки предупреждений, отсылаемых по электронной почте.
	`config delete firewall attack`	Вернуться к настройкам ответов на атаки по умолчанию.
	`config delete firewall set <set #>`	Удалить указанный набор из конфигурации межсетевого экрана.
	`config delete firewall set <set #> rule<rule #>`	Удалить указанное правило из конфигурации межсетевого экрана.

H

Всплывающие окна, сценарии и разрешения Java

Чтобы воспользоваться web-конфигуратором, необходимо включить следующие параметры:

- Всплывающие окна в Интернет-браузере.
- Поддержка JavaScript (по умолчанию активирована).
- Разрешения Java (Java permissions) (активированы по умолчанию).

В настоящем руководстве использованы снимки окон Internet Explorer 6.0. Окна в других версиях Internet Explorer могут отличаться.

Блокирование всплывающих окон в Internet Explorer

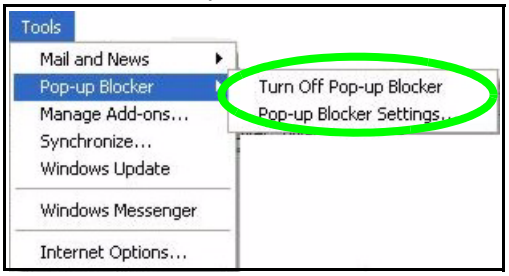
Чтобы зарегистрироваться на Вашем устройстве, Вам возможно придется отключить блокирование всплывающих окон.

Либо отключите блокирование всплывающих окон (в Windows XP SP 2 оно по умолчанию включено), либо разрешите его и создайте исключение для IP-адреса Вашего устройства.

Отключение блокирования всплывающих окон

1 Откройте Internet Explorer, выберите **Tools (Сервис)**, **Pop-up Blocker** (Блокирование всплывающих окон) и затем **Turn Off Pop-up Blocker** (Выключить блокирование всплывающих окон).

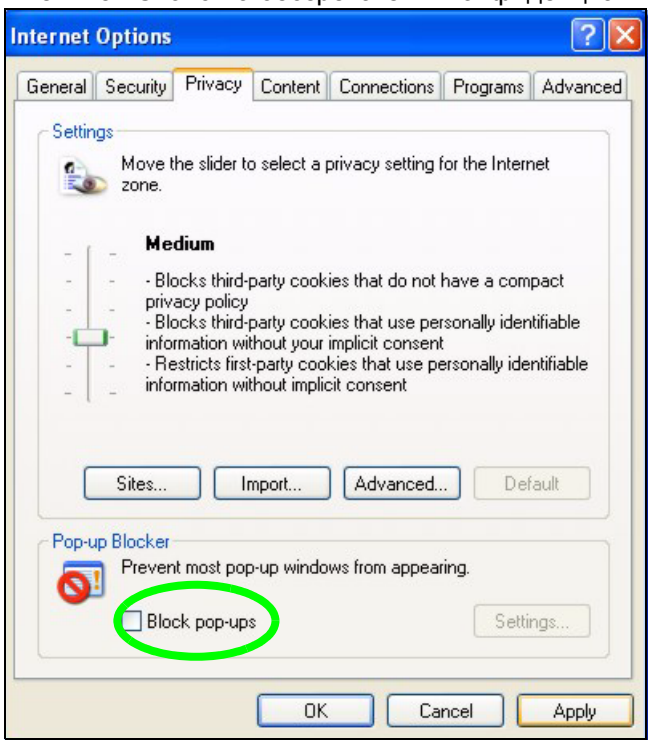
Рис. 214 Блокирование всплывающих окон



Вы также можете проверить, отключено ли блокирование всплывающих окон в разделе **Pop-up Blocker (Блокирование всплывающих окон)** на вкладке **Privacy (Конфиденциальность).**

1. Откройте Internet Explorer, выберите пункт **Tools (Сервис)**, **Internet Options (Свойства обозревателя)**, **Privacy (Конфиденциальность)**.
2. Уберите галочку из окошка **Block pop-ups (Блокировать всплывающие окна)** в разделе **Pop-up Blocker (Блокирование всплывающих окон)** в нижней части окна. Это отключит блокирование всплывающих окон.

Рис. 215 Свойства обозревателя: Конфиденциальность



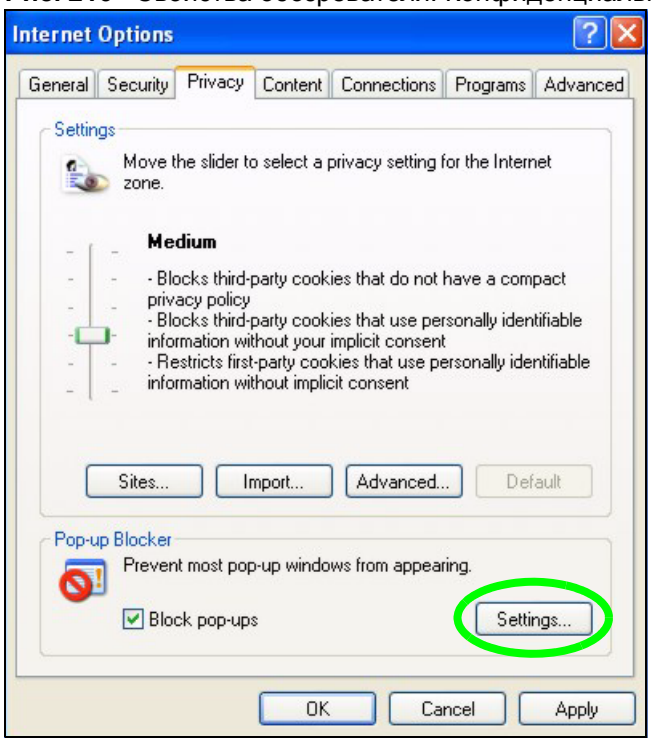
3. Нажмите кнопку **Apply (Применить)** для сохранения настроек.

Включение блокировки всплывающих окон с исключениями

Если же Вы хотите, чтобы всплывающие окна были разрешены лишь на Вашем устройстве, то можно сделать следующее.

1. Откройте Internet Explorer, выберите пункт **Tools (Сервис)**, **Internet Options (Свойства обозревателя)**, **Privacy (Конфиденциальность)**.
2. Выберите пункт **Settings… (Параметры...)** – откроется окно **Pop-up Blocker Settings (Параметры блокирования всплывающих окон)**.

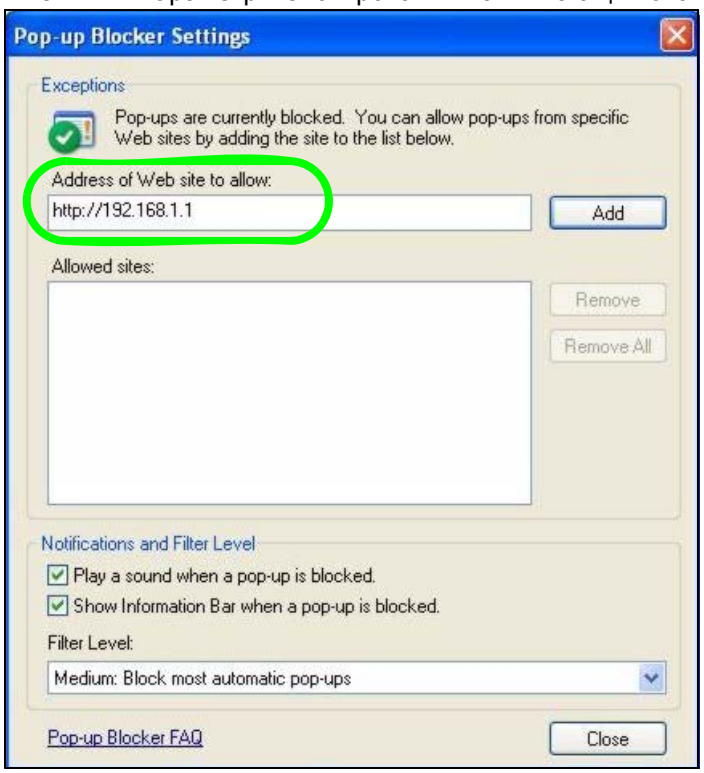
Рис. 216 Свойства обозревателя: Конфиденциальность



3 Введите IP-адрес Вашего устройства (web-сайт, который Вы не хотите блокировать) с префиксом «http://». Например, введите http://192.168.167.1

4 Нажмите кнопку **«Add» (Добавить)** для переноса IP-адреса в список **«Allowed sites» (Разрешенные веб-узлы)**.

Рис. 217 Параметры блокирования всплывающих окон



5 Для возврата на закладку **Privacy (Конфиденциальность)** нажмите кнопку **Close (Закрыть)**.

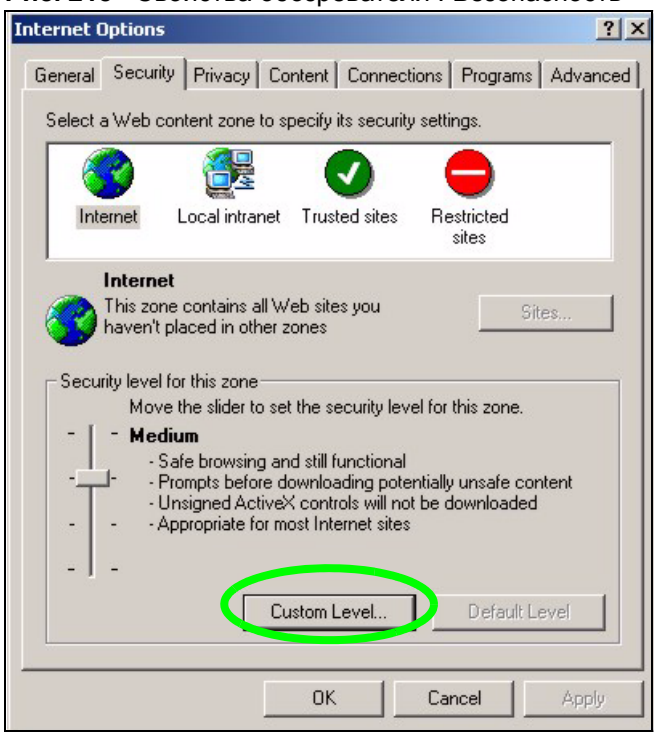
6 Нажмите кнопку **Apply (Применить)** для сохранения настроек.

Сценарии Java (JavaScripts)

Если страницы web-конфигуратора отображаются в Internet Explorer некорректно, проверьте, разрешено ли использование сценариев Java.

1 Откройте Internet Explorer, выберите пункт **Tools (Сервис)**, **Internet Options (Свойства обозревателя)** и перейдите на закладку **Security (Безопасность)**.

Рис. 218 Свойства обозревателя : Безопасность



2 Нажмите кнопку **Custom Level... (Другой...)**.

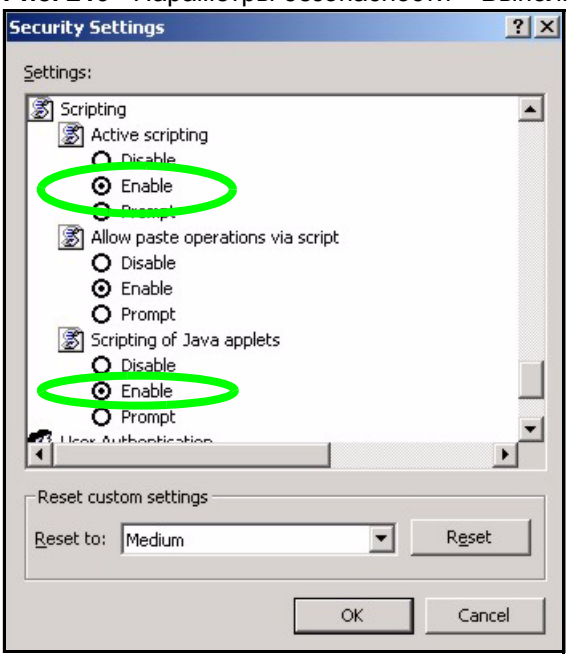
3 Пролистайте до раздела **Scripting (Сценарии)**.

4 В разделе **Active scripting (Активные сценарии)** должно быть установлено **Enable (Разрешить)** (значение по умолчанию).

5 В разделе **Scripting of Java applets (Выполнять сценарии приложений Java)** также должно быть установлено **Enable (Разрешить)** (значение по умолчанию).

6 Нажмите **OK**, чтобы закрыть окно.

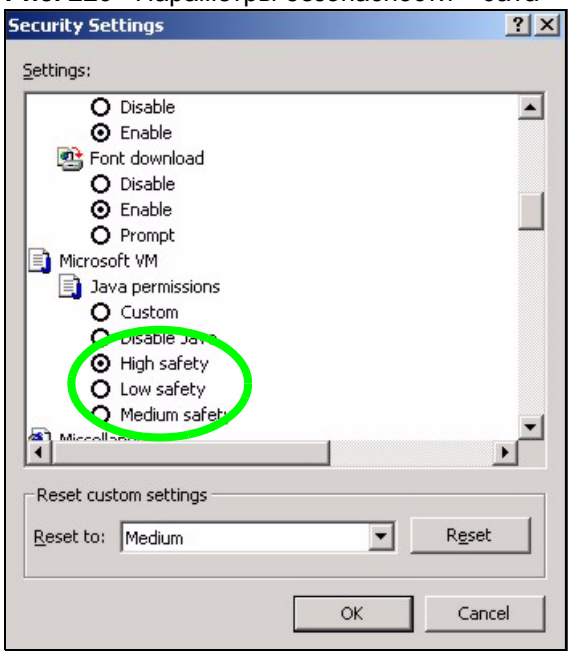
Рис. 219 Параметры безопасности – Выполнение сценариев приложений Java



Разрешения Java

1. Откройте Internet Explorer, выберите **Tools (Сервис)**, **Internet Options (Свойства обозревателя)**, **Security (Безопасность)**.
2. Нажмите кнопку **Custom Level... (Другой...)**.
3. Спуститесь вниз к разделу **Microsoft VM**.
4. Для **Java permissions (Разрешения Java)** должен быть выбран уровень безопасности.
5. Нажмите **OK**, чтобы закрыть окно.

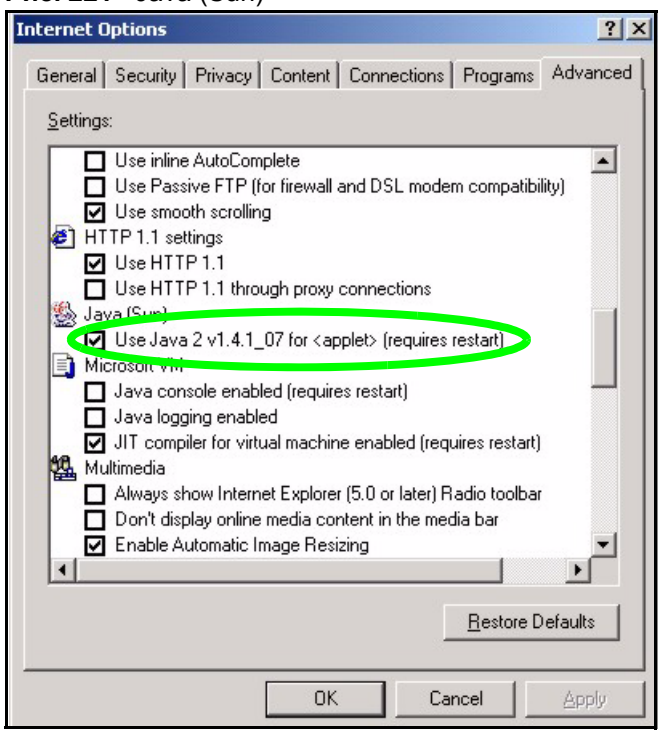
Рис. 220 Параметры безопасности – Java



JAVA (Sun)

1. Откройте Internet Explorer, выберите **Tools (Сервис)**, **Internet Options (Свойства обозревателя)** и затем закладку **Advanced (Дополнительно)**.
2. Убедитесь, в разделе **Java (Sun)** установлено **Use Java 2 for <applet> (Использовать Java 2 для приложения)**.
3. Нажмите **OK**, чтобы закрыть окно.

Рис. 221 Java (Sun)



I

Команды фильтра NetBIOS

Ниже приводится описание команд пакетного фильтра NetBIOS.

Введение

Пакеты NetBIOS (Network Basic Input/Output System – Сетевая базовая система ввода-вывода) – широковещательные пакеты TCP или UDP, позволяющие устанавливать соединение и обмен данными между компьютером и локальной сетью.

Для некоторых служб с автоматическим набором номера, например PPPoE или PPTP, пакеты NetBIOS инициируют нежелательные вызовы.

Вы можете настроить фильтры NetBIOS, чтобы:

- Разрешить/запретить отправку пакетов NetBIOS из локальной сети (LAN) в глобальную (WAN) и наоборот.
- Разрешить/запретить отправку пакетов NetBIOS через VPN-подключения.
- Разрешить/запретить отправку пакетов NetBIOS для инициирования звонков.

Вывод настроек фильтра NetBIOS

Синтаксис: `sys filter netbios disp`

Эта команда выводит список текущих режимов фильтра NetBIOS P660HWP в режиме только для чтения.

Пример команды вывода на экран настроек фильтра NetBIOS

```
=========== NetBIOS Filter Status ===========
          Between LAN and WAN: Block
          IPSec Packets: Forward
          Trigger Dial: Disabled
```

Ниже перечислены типы фильтров и их установки по умолчанию.

Табл. 169 Настройки фильтров NetBIOS по умолчанию

ИМЯ	ОПИСАНИЕ	ПРИМЕР
Between LAN and WAN (Из LAN в WAN)	Это поле показывает, будут ли пересылаться или блокироваться пакеты NetBIOS, исходящие из локальной сети в глобальную.	Block (Блокировать)
IPSec Packets (Пакеты IPSec)	Это поле показывает, будут ли пересылаться или блокироваться пакеты NetBIOS по VPN-соединениям.	Forward (Пересылать)
Trigger dial (Инициировать вызов)	Это поле показывает, разрешено ли пакетам NetBIOS инициировать вызовы. «Disabled» (Отключено) означает, что пакеты NetBIOS не могут инициировать вызовы.	Disabled (Отключено)

Настройка фильтров NetBIOS

```
Syntax:sys filter netbios config <type> <on|off>
```

где

`<type>` = Указывает номер фильтра NetBIOS (от 0 до 3), который необходимо настроить.

0 = из LAN в WAN

3 = проход пакета IPSec

4 = инициирование вызова

`<on|off>` = Чтобы включить фильтр и блокировать пакеты NetBIOS, следует установить параметр «on» для фильтров 0 и 1. Установка параметра «off» отключает фильтр и разрешает пересылку пакетов NetBIOS.

Чтобы блокировать пересылку пакетов по соединениям VPN, следует установить параметр «on» для фильтра 3. Установка параметра «off» разрешает пересылку пакетов NetBIOS по соединениям VPN.

Чтобы разрешить пакетам NetBIOS инициировать вызовы, следует установить параметр «on» для фильтра 4. Установка параметра «off» не позволяет пакетам NetBIOS инициировать вызовы.

Примеры команд:

`sys filter netbios config 0 on` Эта команда блокирует пакеты NetBIOS «LAN–WAN» и «WAN–LAN».

`sys filter netbios config 3 on` Эта команда блокирует пакеты IPSec NetBIOS.

`sys filter netbios config 4 off` Эта команда запрещает командам NetBIOS инициировать вызовы.

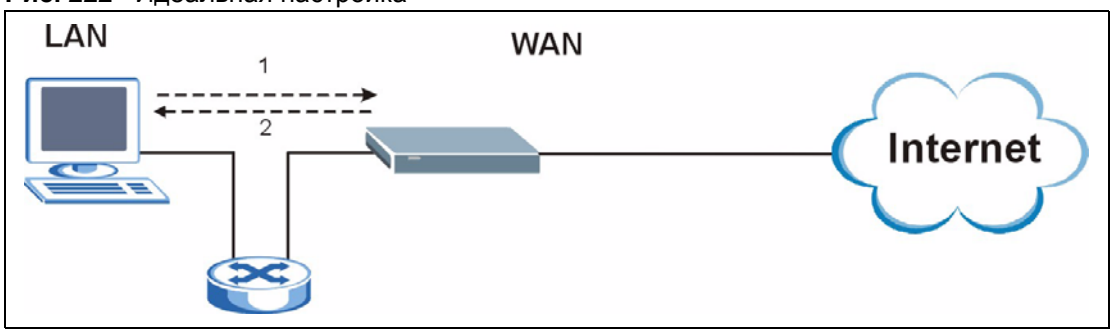
J

Треугольный маршрут

Идеальная настройка

Если межсетевой экран включен, P660HWP выступает в качестве безопасного шлюза между локальной сетью и Интернетом. При идеальной сетевой топологии весь входящий и исходящий сетевой трафик проходит через P660HWP, чтобы обеспечить защиту локальной сети от возможных атак.

Рис. 222 Идеальная настройка



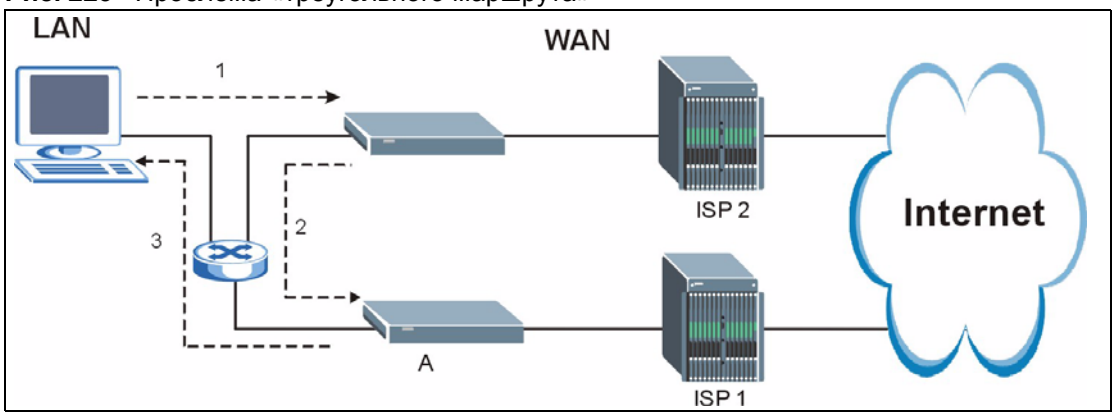
Проблема «треугольного маршрута»

Маршрут трафика – это путь для отправки или приема пакетов данных между двумя устройствами Ethernet. Некоторые компании используют несколько маршрутов к одному или нескольким Интернет-провайдерам. Если альтернативный шлюз находится в локальной сети (и IP-адрес находится в той же подсети), то может возникнуть проблема «треугольного маршрута». Проблему «треугольного маршрута» можно представить следующим образом.

1. Компьютер локальной сети инициирует соединение, посылая пакет SYN принимающему серверу в глобальной сети.
2. Интернет-центр P660HWP изменяет маршрут пакета SYN через шлюз **A** локальной сети в глобальную сеть.
3. Ответ из глобальной сети приходит прямо на компьютер локальной сети, минуя P660HWP.

В результате P660HWP сбрасывает соединение, так как для этого соединения отсутствует подтверждение.

Рис. 223 Проблема «треугольного маршрута»



Решение проблемы «треугольного маршрута»

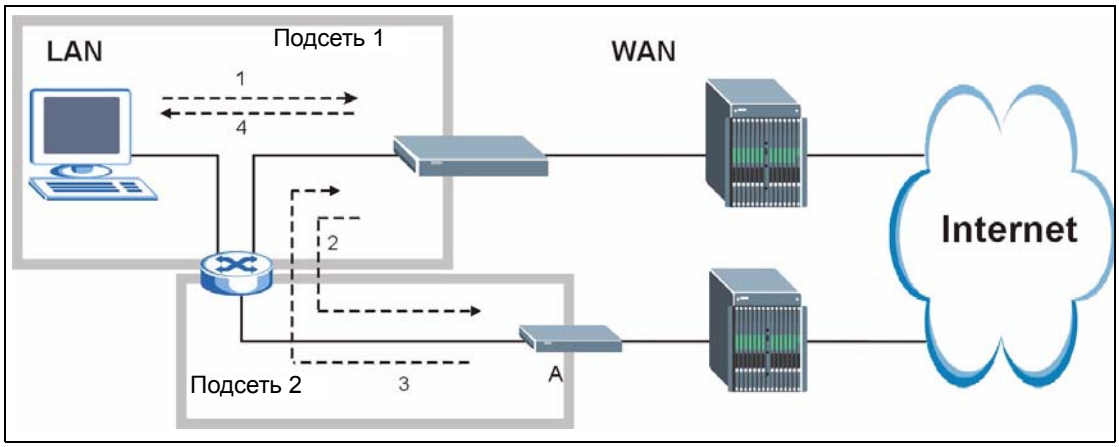
В этом разделе представлено два варианта решения проблемы «треугольного маршрута».

Использование псевдонимов IP

Псевдоним IP позволяет разделить локальную сеть на несколько логических сегментов с использованием одного интерфейса Ethernet. Интернет-центр P660HWP поддерживает три логических интерфейса локальной сети, при этом P660HWP является шлюзом для каждой логической сети. При расположении локальной сети и шлюза **«B»** в разных подсетях весь сетевой трафик, возвращающийся в локальную сеть, должен проходить через P660HWP. Это можно представить с помощью следующего сценария.

1. Компьютер локальной сети инициирует соединение, посылая пакет SYN принимающему серверу в глобальной сети.
2. Интернет-центр P660HWP изменяет маршрут пакета и отправляет его на шлюз **A**, который находится в подсети 2.
3. Ответ из глобальной сети приходит через P660HWP к компьютеру, который находится в локальной сети в подсети 1.

Рис. 224 Псевдоним IP



E K

Правовая информация

Авторское право

Непризнание иска

Корпорация ZyXEL не принимает на себя ни в какой форме ответственность за применение или использование любого изделия или программного обеспечения, описанного в данном руководстве пользователя. Корпорация ZyXEL также не предоставляет никаких лицензий на свои патентные права, а также на патентные права третьих сторон. Кроме того, корпорация ZyXEL сохраняет за собой право вносить изменения в любые описываемые в данном документе изделия без дополнительного уведомления. Информация в этом руководстве также может быть изменена без специального уведомления.

Торговая марка

ZyNOS (ZyXEL Network Operating System — Сетевая операционная система ZyXEL) является зарегистрированной торговой маркой ZyXEL Communications, Inc. Торговые марки, упомянутые в данном издании, используются только в целях идентификации и являются собственностью своих законных владельцев.

Ограниченная гарантия корпорации ZyXEL

Корпорация ZyXEL гарантирует легальному конечному пользователю (покупателю), что данное изделие не имеет и в течение периода до двух лет со дня покупки не будет иметь дефектов, связанных с использованными материалами и производственным браком. В течение гарантийного периода и по подтверждении покупки, если изделие имеет признаки неисправности, связанные с производственным браком и/или использованными материалами, корпорация ZyXEL будет, по своему выбору, ремонтировать или заменять дефектные изделия или комплектующие без оплаты деталей или стоимости работы, а также всего того, что окажется необходимым для

восстановления надлежащего режима работы изделия или комплектующих. Любая замена может включать как новые, так и восстановленные функционально эквивалентные изделия аналогичной или более высокой стоимости; выбор в данном случае остается за корпорацией ZyXEL. Данные гарантийные обязательства не распространяются на случаи, когда изделие было вскрыто, модифицировано, использовано не по назначению, повреждено в результате форс-мажорных обстоятельств или неправильных условий эксплуатации.

Примечание

Покупатель, согласно данным гарантийным обязательствам, может рассчитывать только на ремонт или замену. Данные гарантийные обязательства заменяют собой все прочие гарантийные обязательства, явные или неявные, включая любые неявные гарантийные обязательства в отношении годности для продажи или решения конкретных целей и задач. Корпорация ZyXEL не несет никакой ответственности перед покупателем за косвенные убытки любого олда.

Для получения обслуживания по данным гарантийным обязательствам следует связаться с Сервисным центром ZyXEL; информация о номере разрешения на возврат (RMA) содержится в Гарантийном талоне на данное оборудование. Изделия должны быть возвращены с предварительно оплаченным почтовым сбором. Рекомендуется застраховать каждое устройство на период пересылки. Изделия, возвращенные без документов, подтверждающих факт покупки или с просроченной гарантией, будут отремонтированы или заменены (по усмотрению корпорации ZyXEL), и клиенту будет выставлен счет на оплату работ и деталей. Все отремонтированные или замененные изделия будут отправлены корпорацией ZyXEL по соответствующему обратному адресу с оплаченным почтовым сбором. Данные гарантийные обязательства предоставляют определенные законом права, а также дополнительные права, которые могут быть различными в разных странах.

Регистрация

Зарегистрируйте ваше изделие в режиме он-лайн для получения по электронной почте сообщений об обновлениях микропрограммного обеспечения и информации об изделиях на сайте www.zyxel.com (глобальный), или на сайте www.zyxel.ru (для России).

L

Сервисная служба

При обращении в Сервисную службу будьте готовы предоставить следующую информацию:

Обязательные сведения

- Модель изделия и серийный номер.
- Гарантийные обязательства.
- Дата приобретения устройства.
- Краткое описание неисправности, а также действий, предпринятых по ее устранению.

Вместо «+» наберите код международной телефонной связи.

Головной офис корпорации (По всему миру)

- E-mail службы поддержки: support@zyxel.com.tw
- E-mail отдела продаж: sales@zyxel.com.tw
- Телефон: +886-3-578-3942
- Факс: +886-3-578-2439
- Web-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

Великобритания

- E-mail службы поддержки: support@zyxel.co.uk
- E-mail отдела продаж: sales@zyxel.co.uk
- Телефон: +44-1344-303044, 08707-555779 (только Великобритания)
- Факс: +44-1344-303034
- Web-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)

Венгрия

- E-mail службы поддержки: support@zyxel.hu
- E-mail отдела продаж: info@zyxel.hu
- Телефон: +36-1-3361649
- Факс: +36-1-3259100
- Web-сайт: www.zyxel.hu
- Обычная почта: ZyXEL Hungary, 48, Zoldlomb Str., H-1025, Budapest, Hungary

Германия

- E-mail службы поддержки: support@zyxel.de
- E-mail отдела продаж: sales@zyxel.de
- Телефон: +49-2405-6909-69
- Факс: +49-2405-6909-99
- Web-сайт: www.zyxel.de
- Обычная почта: ZyXEL Deutschland GmbH., Adenauerstr. 20/A2 D-52146, Wuerselen, Germany

Дания

- E-mail службы поддержки: support@zyxel.dk
- E-mail отдела продаж: sales@zyxel.dk
- Телефон: +45-39-55-07-00
- Факс: +45-39-55-07-07
- Web-сайт: www.zyxel.dk
- Обычная почта: ZyXEL Communications A/S, Columbusvej, 2860 Soeborg, Denmark

Индия

- E-mail службы поддержки: support@zyxel.in
- E-mail отдела продаж: sales@zyxel.in
- Телефон: с +91-11-30888144 по +91-11-30888153
- Факс: +91-11-30888149, +91-11-26810715
- Web-сайт: http://www.zyxel.in
- Обычная почта: Индия - ZyXEL Technology India Pvt Ltd., II-Floor, F2/9 Okhla Phase-1, New Delhi 110020, India

Испания

- E-mail службы поддержки: support@zyxel.es
- E-mail отдела продаж: sales@zyxel.es
- Телефон: +34-902-195-420
- Факс: +34-913-005-345
- Web-сайт: www.zyxel.es
- Обычная почта: ZyXEL Communications, Arte, 21 5ª planta, 28033 Madrid, Spain

Казахстан

- Служба поддержки: http://zyxel.kz/support
- E-mail отдела продаж: sales@zyxel.kz
- Телефон: +7-7272-590-698
- Факс: +7-7272-590-689
- Web-сайт: www.zyxel.kz
- Обычная почта: ZyXEL Kazakhstan, 43, Dostyk ave.,Office 414, Dostyk Business Centre, 050010, Almaty, Republic of Kazakhstan

Коста-Рика

- E-mail службы поддержки: soporte@zyxel.co.cr
- E-mail отдела продаж: sales@zyxel.co.cr
- Телефон: +506-2017878
- Факс: +506-2015098
- Web-сайт: www.zyxel.co.cr
- FTP-сервер: ftp.zyxel.co.cr
- Обычная почта: ZyXEL Costa Rica, Plaza Roble Escazú, Etapa El Patio, Tercer Piso, San José, Costa Rica

Малайзия

- E-mail службы поддержки: support@zyxel.com.my
- E-mail отдела продаж: sales@zyxel.com.my
- Телефон: +603-8076-9933
- Факс: +603-8076-9833
- Web-сайт: http://www.zyxel.com.my
- Обычная почта: ZyXEL Malaysia Sdn Bhd., 1-02 & 1-03, Jalan Kenari 17F, Bandar Puchong Jaya, 47100 Puchong, Selangor Darul Ehsan, Malaysia

Норвегия

- E-mail службы поддержки: support@zyxel.no
- E-mail отдела продаж: sales@zyxel.no
- Телефон: +47-22-80-61-80
- Факс: +47-22-80-61-81
- Web-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
- Web -сайт: www.pl.zyxel.com
- Обычная почта: ZyXEL Communications, ul. Okrzei 1A, 03-715 Warszawa, Poland

Россия

- Служба поддержки: http://zyxel.ru/support
- E-mail отдела продаж: sales@zyxel.ru
- Телефон: +7-095-542-89-29
- Факс: +7-095-542-89-25
- Web -сайт: www.zyxel.ru
- Обычная почта: Россия, 117279, г. Москва, ул. Островитянова, 37а

Северная Америка

- E-mail службы поддержки: support@zyxel.com
- E-mail отдела продаж: sales@zyxel.com
- Телефон: +1-800-255-4101, +1-714-632-0882
- Факс: +1-714-632-0858
- Web-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.

Сингапур

- E-mail службы поддержки: support@zyxel.com.sg
- E-mail отдела продаж: sales@zyxel.com.sg
- Телефон: +65-6899-6678
- Факс: +65-6899-8887
- Web-сайт: http://www.zyxel.com.sg
- Обычная почта: ZyXEL Singapore Pte Ltd., No. 2 International Business Park, The Strategy #03-28, Singapore 609930

Таиланд

- E-mail службы поддержки: support@zyxel.co.th
- E-mail отдела продаж: sales@zyxel.co.th
- Телефон: +662-831-5315
- Факс: +662-831-5395
- Web-сайт: http://www.zyxel.co.th
- Обычная почта: ZyXEL Thailand Co., Ltd., 1/1 Moo 2, Ratchaphruk Road, Bangrak-Noi, Muang, Nonthaburi 11000, Thailand.

Украина

- E-mail службы поддержки: support@ua.zyxel.com
- E-mail отдела продаж: sales@ua.zyxel.com
- Телефон: +380-44-247-69-78
- Факс: +380-44-494-49-32
- Web-сайт: www.ua.zyxel.com
- Обычная почта: ZyXEL Ukraine, 13, Pimonenko Str., Kiev 04050, Ukraine

Финляндия

- E-mail службы поддержки: support@zyxel.fi
- E-mail отдела продаж: sales@zyxel.fi
- Телефон: +358-9-4780-8411
- Факс: +358-9-4780-8448
- Web-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
- Web-сайт: www.zyxel.fr
- Обычная почта: ZyXEL France, 1 rue des Vergers, Bat. 1 / C, 69760 Limonest, France

Чешская Республика

- E-Mail: info@cz.zyxel.com
- Телефон: +420-241-091-350
- Факс: +420-241-091-359
- Web-сайт: www.zyxel.cz
- Обычная почта: ZyXEL Communications, Czech s.r.o., Modranská 621, 143 01 Praha 4 - Modrany, Ceská Republika

Швеция

- E-mail службы поддержки: support@zyxel.se
- E-mail отдела продаж: sales@zyxel.se
- Телефон: +46-31-744-7700
- Факс: +46-31-744-7701
- Web-сайт: www.zyxel.se
- Обычная почта: ZyXEL Communications A/S, Sjöporten 4, 41764 Göteborg, Sweden

Япония

- E-mail службы поддержки: support@zyxel.co.jp
- E-mail отдела продаж: sales@zyxel.co.jp
- Телефон: +81-3-6847-3700
- Факс: +81-3-6847-3705
- Web-сайт: www.zyxel.co.jp
- Обычная почта: ZyXEL Japan, 3F, Office T&U, 1-10-10 Higashi-Gotanda, Shinagawa-ku, Tokyo 141-0022, Japan

Алфавитный указатель

L

M

N

P

R

S

T

U

V

W

A

Б

В

Г

Д

З

И

К

Л

М

Н

О

П

Р

C

T

У

Ф

Х

Ц

Ч

Ш

Э