P660HN

Интернет-центр для подключения по ADSL2+
с точкой доступа Wi-Fi 802.11n 300 Мбит/с
и коммутатором Ethernet

Руководство пользователя

Версия 3.70
08/2010
Редакция 1

НАСТРОЙКИ ПО УМОЛЧАНИЮ	
IP-адрес	**http://192.168.1.1**
Пароль администратора	**1234**

ZyXEL
www.zyxel.com

О данном руководстве пользователя

Для кого предназначено данное руководство

Данное руководство предназначено для тех, кто планирует производить настройку P660HN с помощью веб-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

- Инструкция по применению

  Инструкция по применению разработана с целью помочь вам изучить устройство и начать работать с ним. В ней содержится информация о настройке сети и организации доступа в Интернет.

Рекомендуется выполнять настройку P660HN 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 *zyxel.ru*.

Обратная связь с пользователями

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 *zyxel.ru*. Спасибо.

Обозначения, принятые в документе

Предупреждения и примечания

Предупреждения и примечания в данном руководстве пользователя представлены следующим образом:

Иконкой «осторожно» отмечены пункты, содержание которых предупреждает о возможном нанесении вреда пользователю или устройству.

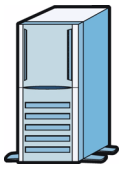
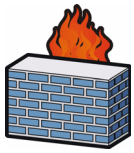
Иконкой «примечание» помечается важная информация (например, необходимость настройки других параметров или полезные подсказки), рекомендации, относящиеся к теме.

Условные обозначения

- Далее в данном Руководстве пользователя P660HN может именоваться как «Устройство P660HN», «устройство», «система» или «изделие».
- Надписи на изделии, названия экранов, имена полей и пункты меню обозначаются **жирным** шрифтом.
- Названия кнопок указаны прописными буквами в квадратных скобках, например, [ENTER] означает кнопку «ввод» или «возврат каретки» на клавиатуре.
- Указание «введите» означает, что следует набрать один или несколько символов и затем нажать кнопку [ENTER]. «Выберите» означает, что следует использовать один из предложенных вариантов.
- Правая угловая скобка (>) между названиями окон означает нажатие кнопки мыши. Например, **Maintenance > Log > Log Setting** означает, что сначала необходимо выбрать **Maintenance** в панели навигации, затем подменю **Log**, 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 приведенные ниже пиктограммы. Иконка устройства P660HN является схематичным изображением устройства.

P660HN 	Компьютер 	Ноутбук 
Сервер 	Брандмауэр 	Телефон 
Маршрутизатор 	Коммутатор 	

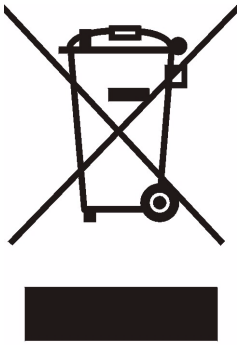
Техника безопасности

Для обеспечения безопасности необходимо прочитать данное руководство и следовать следующим правилам.

- НЕ используйте устройство в непосредственной близости от воды, например, во влажных подвалах или рядом с бассейном.
- НЕ подвергайте устройство воздействию влаги, пыли или агрессивных жидкостей.
- НЕ кладите на устройство какие-либо посторонние предметы.
- ЗАПРЕЩАЕТСЯ устанавливать, использовать и ремонтировать устройство во время грозы. Существует определенный риск поражения 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 возникновения других возможных опасностей. 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 могут ходить люди.
- 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 устройства и источника питания.
- 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 поражения 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.
- Внимание, антенна! Данное устройство соответствует требованиям сертификации ETSI и FCC при использовании с входящей в комплект антенной/антеннами. Используйте ТОЛЬКО антенну (антенны) из комплекта поставки.

Изделие пригодно для повторного использования. Утилизация должна производиться надлежащим образом.



Содержание

Оглавление

Перечень рисунков

Перечень таблиц

Часть I
Введение

1

Знакомство с устройством P660HN

В этой главе рассказывается об основных функциях и сферах применения устройства P660HN, а также о способах управления устройством P660HN.

1.1 Обзор

Интернет-центр ZyXEL P660HN – это надежное, удобное и безопасное подключение вашего дома к Интернету и IP-телевидению по выделенному каналу ADSL через существующую телефонную линию, не мешающее работе самого телефона. Он объединяет домашнюю компьютерную технику в сеть и подключает ее ко Всемирной Сети с помощью первоклассного встроенного модема ADSL2+, а безопасность от атак из Интернета и кражи информации обеспечивает встроенный межсетевой экран. Установив P660HN, вы сможете одновременно выходить в Интернет с нескольких компьютеров, обмениваться между ними фотографиями, музыкой и документами, играть в сетевые игры, совместно использовать сетевой принтер, пользоваться услугой IP-телевидиния, а также участвовать в файлообменных сетях P2P. Встроенная точка доступа Wi-Fi дает свободу перемещения по квартире подключенных к интернет-центру ноутбуков и других беспроводных устройств. По мере необходимости вы можете развивать свою домашнюю сеть с использованием различных устройств компании ZyXEL.

Необходимо использовать микропрограммное обеспечение устройства P660HN строго в соответствии с конкретной моделью устройства. См. наклейку, находящуюся на нижней панели устройства P660HN.

1.2 Способы управления устройством P660HN

Для управления устройством P660HN используются следующие средства:

- Утилита ZyXEL NetFriend. Рекомендуется для простой настройки доступа в Интернет, разработана для пользователей любого уровня подготовки. Находится на прилагаемом к модему диске, а также на сайте zyxel.ru. Информация по использованию NetFriend приведена в инструкции по применению.
- Web-конфигуратор. Рекомендуется для повседневного управления устройством P660HN с использованием рекомендуемого веб-браузера.
- Интерфейс командной строки. Управление с помощью команд главным образом используется сервисными инженерами при поиске и устранении неисправностей.
- FTP предназначен для обновления микропрограммного обеспечения и резервного копирования или восстановления конфигурации.
- SNMP. Мониторинг устройства можно выполнять через управляющую станцию SNMP. Информацию по этому вопросу см. в главе «SNMP» в данном руководстве.
- TR-069. Это сервер автоматической удаленной настройки устройств.

1.3 Полезные советы по управлению устройством P660HN

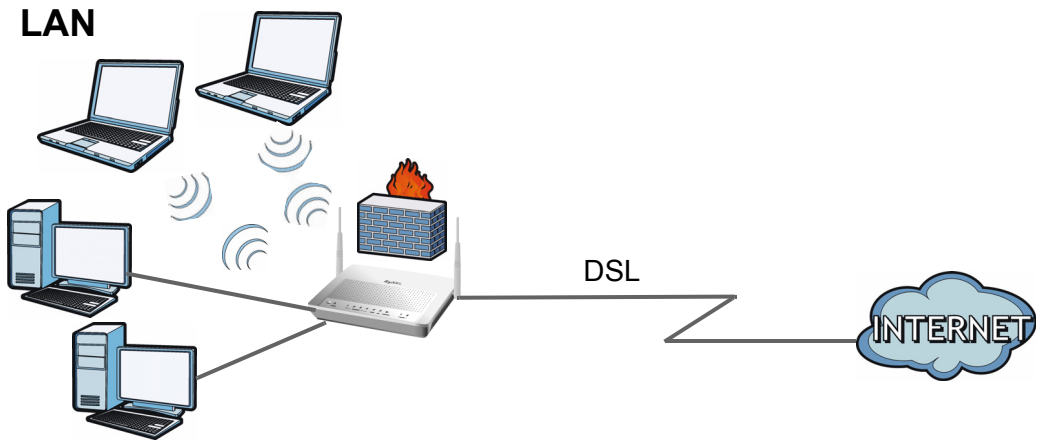
Для обеспечения безопасной и более эффективной работы устройства P660HN рекомендуется регулярное и правильное выполнение описанных далее процедур.

- 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 его 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 устройства P660HN к настройкам, установленным изготовителем по умолчанию. При наличии файла предыдущей рабочей конфигурации не нужно будет заново выполнять полную настройку устройства P660HN. Можно просто восстановить последнюю конфигурацию.

1.4 Сфера применения устройства P660HN

Ваше устройство P660HN обеспечивает совместный доступ в Интернет за счет подключения порта DSL к гнезду **DSL** или **MODEM** на сплиттере. Компьютеры могут подключаться к портам локальной сети устройства P660HN (или к беспроводной сети).

Рис. 1 Функции маршрутизатора устройства P660HN



Можно также настроить брандмауэр и контент-фильтрование на устройстве P660HN для безопасного доступа в Интернет. Когда брандмауэр включен, весь входящий трафик из Интернета 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.

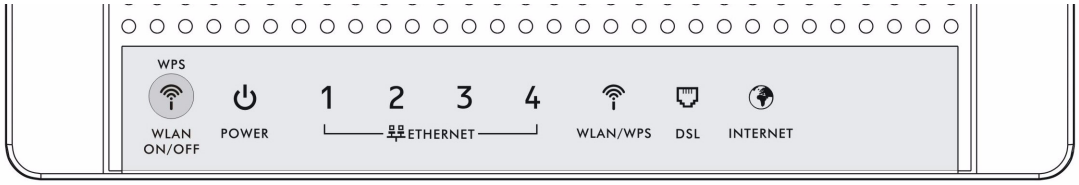
Используйте контент-фильтрование для блокировки доступа к конкретным веб-сайтам с помощью URL, содержащего указанные вами ключевые слова. Можно указать периоды времени и дни, в течение которых будет работать контент-фильтр, а также указать компьютеры, чей трафик следует фильтровать или, наоборот, не фильтровать. Например, можно блокировать доступ детей к определенным веб-сайтам.

Используйте QoS для эффективного управления трафиком вашей сети, задавая приоритет для некоторых типов трафика и/или определенных компьютеров вашей сети. Например, можно сделать так, чтобы устройство P660HN обеспечивало наивысший приоритет для голосовых вызовов по Интернету и/или ограничить полосу частот, выделенную для выгрузки важных файлов.

1.5 Светодиоды (LED)

На приведенном ниже рисунке указаны поля светодиодов.

Рис. 2 Светодиоды в верхней части устройства



Ни один из светодиодов не работает, если устройство P660HN не получает питания.

Табл. 1 Описание светодиодов

СВЕТО-ДИОД	ЦВЕТ	СОСТОЯНИЕ	ОПИСАНИЕ
ПИТАНИЕ	Зеленый	Вкл.	Устройство P660HN получает питание и готово к работе.
		Мигает	Выполняется самотестирование устройства P660HN.
	Красный	Вкл.	При самотестировании устройства P660HN была обнаружена ошибка или устройство неисправно.
		Выкл.	Устройство P660HN не получает питания.
ETHERNET 1-4	Зеленый	Вкл.	Устройство P660HN имеет Ethernet-подключение к устройству в локальной вычислительной сети (LAN).
		Мигает	Устройство P660HN передает/принимает данные из/в LAN.
		Выкл.	Устройство P660HN не имеет Ethernet-подключения к LAN.
WLAN/WPS	Зеленый	Вкл.	Беспроводная сеть активирована.
		Мигает	Устройство P660HN обменивается данными с другими беспроводными клиентами.
	Оранжевый	Мигает	Устройство P660HN устанавливает WPS-соединение.
		Выкл.	Беспроводная сеть не активирована.
DSL	Зеленый	Вкл.	Соединение DSL установлено.
		Мигает	Устройство P660HN инициализирует линию DSL.
		Выкл.	Канал DSL не работает.
INTERNET	Зеленый	Вкл.	Устройство P660HN имеет IP-подключение, но трафик отсутствует. Ваше устройство имеет IP-адрес в WAN (статический или назначенный сервером DHCP), сессия PPP была успешно выполнена (если использовалась) и DSL-подключение установлено.
		Мигает	Устройство P660HN передает или принимает IP-трафик.
	Красный	Вкл.	Устройство P660HN попыталось установить IP-подключение, но безуспешно. Возможные причины: нет отклика от сервера DHCP, нет отклика от PPPoE, сбой аутентификации PPPoE.
		Выкл.	Устройство P660HN не имеет IP-подключения.

Подключение встроенного программного обеспечения описано в Кратком руководстве пользователя.

1.6 Кнопка RESET

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

1.6.1 Использование кнопки сброса настроек

1. Убедитесь, что светодиод **POWER** горит (не мигает).
2. Для того чтобы вернуть настройки устройства к заводским настройкам по умолчанию, нажмите и удерживайте кнопку **RESET** пока не начнет мигать светодиод питания **POWER**, а затем отпустите кнопку. Когда светодиод **POWER** начинает мигать, это означает, что настройки по умолчанию восстановлены и происходит перезапуск устройства.

1.7 Кнопка WPS WLAN

Можно использовать кнопку **WPS WLAN ON/OFF** (), расположенную на верхней части устройства, для включения или выключения беспроводной локальной сети. Эту кнопку можно также использовать для активации WPS для того, чтобы быстро установить беспроводную сеть с высоким уровнем защиты.

1.7.1 Включение или выключение беспроводной локальной сети

1. Убедитесь, что светодиод **POWER** горит (не мигает).

Нажмите кнопку **WPS WLAN ON/OFF** и удерживайте ее нажатой **менее пяти** секунд. Индикатор **WLAN/WPS** изменит свое состояние с включенного на выключенное или наоборот.

По умолчанию точка доступа на устройстве выключена. Если вы планируете использовать беспроводную сеть, включите ее вышеописанным способом, либо через веб-интерфейс, либо через программу NetFriend. Во избежание несанкционированного доступа в вашу домашнюю сеть и пользования вашим доступом в Интернет, не забудьте настроить безопасность Wi-Fi.

1.7.2 Активация WPS

1. Убедитесь, что светодиод **POWER** горит (не мигает).
2. Нажмите кнопку **WPS WLAN ON/OFF** и удерживайте ее нажатой в течение **5–10 секунд**. Нажмите кнопку WPS на другом устройстве с WPS в пределах зоны доступа устройства P660HN. Индикатор **WLAN/WPS** будет мигать в то время, как устройство P660HN устанавливает WPS-соединение с беспроводным устройством.

В течение двух минут нужно активировать WPS на устройстве P660HN и на другом беспроводном устройстве. Более подробную информацию см. в Разд. 6.9.8 на с. 114.

2

Знакомство с Web-конфигуратором

2.1 Обзор

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

Чтобы воспользоваться Web-конфигуратором, необходимо включить следующие параметры:

- Инициированные модемом всплывающие окна в веб-браузере не должны блокироваться. Блокировка всплывающих окон активирована по умолчанию в Windows.
- Поддержка JavaScript (по умолчанию активирована).
- Разрешения Java (Java permissions) (по умолчанию активированы).

Если нужно узнать, разрешены ли эти функции в Internet Explorer, см. Прил. B на с. 325.

2.1.1 Доступ к Web-конфигуратору

1. Убедитесь, что ваше устройство P660HN подключено правильно (см. «Инструкцию по применению»).
2. Запустите веб-браузер.
3. Наберите 192.168.1.1 как URL.
4. На экране появится окно регистрации. Устройство P660HN имеет систему двойной регистрации. Нечитаемые символы представляют собой пароль администратора по умолчанию (1234). Если вы изменили пароль, введите свой пароль и нажмите **Login**.
5. Если вы хотите попасть в режим просмотра статуса устройства, введите пароль пользователя (по умолчанию - user) и нажмите **Login**.

Рис. 3 Экран ввода пароля

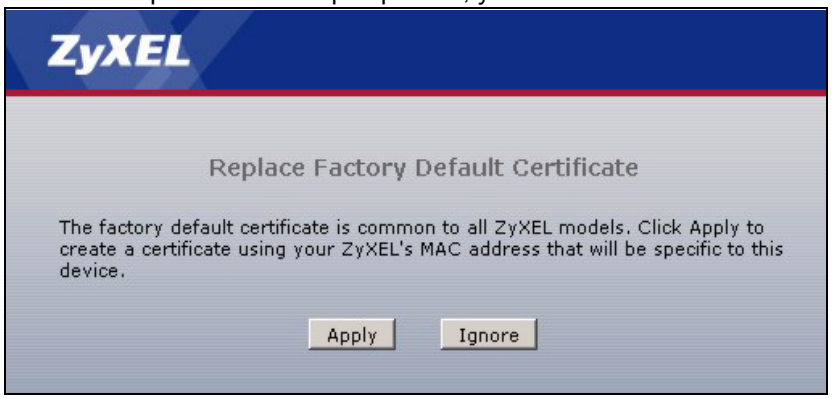
6 Этот экран отображается, если вы еще не поменяли свой пароль. Рекомендуется сменить системный пароль по умолчанию. Введите новый пароль, введите его еще раз для подтверждения и нажмите **Apply**; если вы не хотите в настоящий момент менять пароль, нажмите **Ignore** для перехода к главному меню.

Рис. 4 Экран смены пароля

7 Этот экран отображается, если вы еще не заменили сертификат, установленный изготовителем по умолчанию. Нажмите **Apply** для создания особого сертификата для устройства, использующего MAC-адрес вашего компьютера.

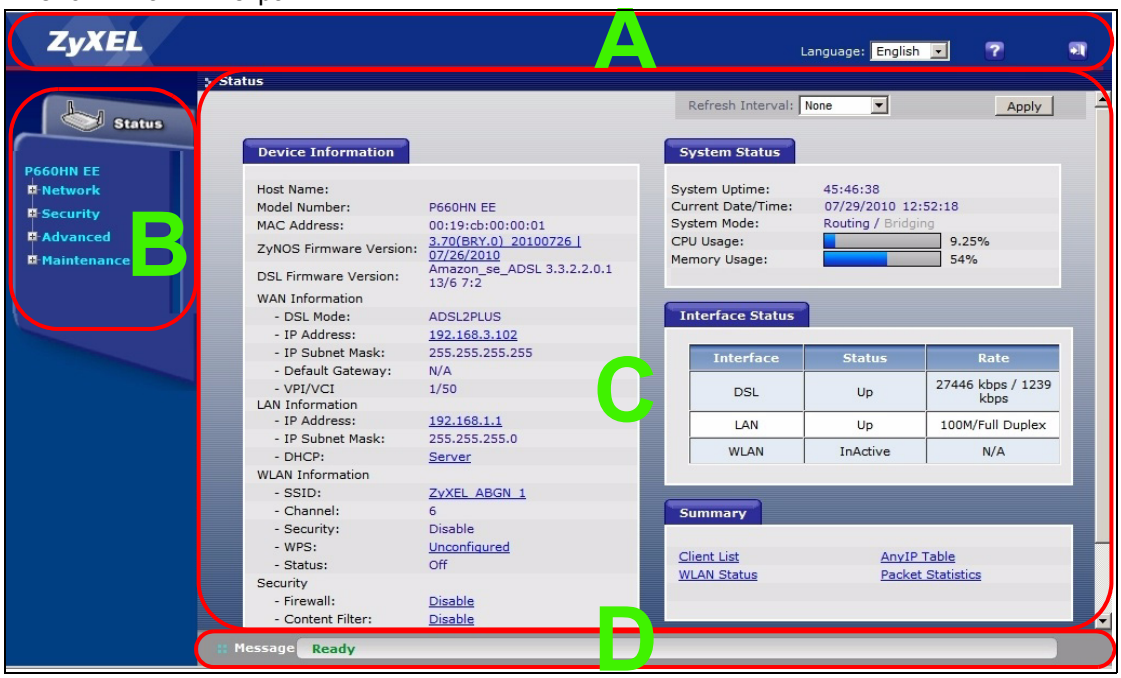
По соображениям безопасности устройство P660HN автоматически выводит вас из системы, если вы не используете Web-конфигуратор в течение пяти минут (по умолчанию). Если это произойдет, просто зарегистрируйтесь еще раз.

Рис. 5 Экран замены сертификата, установленного изготовителем по умолчанию



2.2 Главный экран Web-конфигуратора

Рис. 6 Главный экран

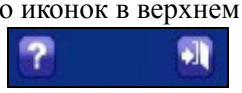


Как показано выше, главный экран разделен на следующие части:

- **A** – заголовок окна
- **B** – панель навигации
- **C** – главное окно
- **D** – строка состояния

2.2.1 Заголовок окна

Заголовок окна содержит несколько иконок в верхнем правом углу.



Эти иконки обеспечивают следующие функции.

Табл. 2 Иконка Web-конфигуратора в заголовке окна

ИКОНКА	ОПИСАНИЕ
	**Помощь**: Щелкните по этой иконке для открытия экрана помощи.
	**Выход**: Щелкните по этой иконке для выхода из Web-конфигуратора.

2.2.2 Панель навигации

Используйте позиции меню на панели навигации, чтобы открывать экраны для настройки функций устройства P660HN. В приведенных ниже таблицах показаны все позиции меню.

Табл. 3 Краткое описание панели навигации

ССЫЛКА	ЗАКЛАДКА	ФУНКЦИЯ
Status		На этом экране показано главное устройство P660HN и данные статуса в сети. Этот экран открывает доступ к статистике системы и списку клиентов.
Network		
WAN	Internet Access Setup	Этот экран позволяет установить параметры Интернет-провайдера, назначить IP-адрес устройства в глобальной сети, определить серверы DNS и настроить другие свойства.
	More Connections	На этом экране можно настроить дополнительные параметры соединений WAN.
	WAN Backup Setup	Этот экран используется для настройки резервного шлюза.
LAN	IP	Этот экран используется для настойки протокола TCP/IP в локальной сети, включения функции Any IP и других свойств.
	DHCP Setup	Этот экран используется для настройки протокола DHCP в локальной сети.
	Client List	Этот экран используется для просмотра параметров конкретного клиента DHCP и назначения специального IP-адреса индивидуальным MAC-адресам (и именам узлов).
	IP Alias	Этот экран позволяет разделить локальную сеть на подсети.

Табл. 3 Краткое описание панели навигации (продолжение)

ССЫЛКА	ЗАКЛАДКА	ФУНКЦИЯ
Wireless LAN	AP	На этом экране производится настройка параметров беспроводной локальной сети и установка параметров аутентификации/безопасности беспроводной локальной сети.
	More AP	Этот экран используется для настройки нескольких BSS в устройстве P660HN.
	WPS Station	Этот экран используется для включения WPS (настройка безопасности Wi-Fi) и для организации беспроводной сети.
	WDS	Этот экран используется для настройки связей беспроводной системы распределения с другими точками доступа.
	QoS	Этот экран используется для включения или выключения функции Quality of Service (QoS – Качество услуги).
	Scheduling	Этот экран используется для настройки даты/времени или включения/выключения беспроводной локальной сети.
NAT	General	Этот экран используется для включения функции NAT.
	Port Forwarding	Этот экран используется для того, чтобы сделать ваши локальные серверы видимыми для внешних пользователей.
	ALG	Этот экран используется для включения или выключения SIP ALG.
Security		
Firewall	General	Этот экран используется для включения/выключения брандмауэра и действий по умолчанию по распределению сетевого трафика в особых направлениях.
	Rules	Этот экран демонстрирует сводку правил брандмауэра и позволяет редактировать/добавлять правило.
	Threshold	Этот экран используется для настройки порогов, которые определяют, когда следует сбросить сеанс связи, находящийся в процессе установления соединения.
Content Filter	Keyword	Этот экран позволяет включить блокировку доступа на веб-сайты, содержащие в URL-адресе заданные ключевые слова.
	Schedule	Этот экран используется для установки расписания, по которому ваше устройство будет выполнять контент-фильтрование.
	Trusted	На этом экране можно определить группу пользователей локальной сети, для которых не будет выполняться контент-фильтрование.
Packet Filter		Этот экран используется для настройки правил фильтров для протокола и наборов общих фильтров.
Certificates	My Certificates	Этот экран используется для создания и экспорта самостоятельно подписанных сертификатов или запросов на сертификацию, а также импорта сертификатов P660HN, подписанных центром сертификации.
	Trusted CAs	Этот экран используется для сохранения на компьютере сертификатов P660HN, выданных центром сертификации.
	Trusted Remote Hosts	На этом экране производится импорт самостоятельно подписанных сертификатов.
	Directory Servers	Здесь можно создать список адресов серверов каталогов (серверов, которые содержат списки действующих и аннулированных сертификатов).

Табл. 3 Краткое описание панели навигации (продолжение)

ССЫЛКА	ЗАКЛАДКА	ФУНКЦИЯ
Advanced		
Static Route		Этот экран используется для настройки статического маршрута IP, чтобы сообщать устройству о сети, находящихся вне непосредственно подключенных удаленных узлов.
802.1Q/1P	Group Setting	Этот экран используется для активации 802.1Q/1P, указания управляющей группы VLAN, отображения групп VLAN и настройки параметров для каждой группы VLAN.
	Port Setting	Этот экран используется для настройки PVID и назначения приоритета по трафику для каждого порта.
QoS	General	Этот экран используется для включения QoS, задания приоритета для трафика и настройки управления полосой частот в глобальной сети WAN.
	Class Setup	Этот экран используется для настройки классификатора.
	Monitor	Этот экран используется для просмотра статистики каждой очереди.
Dynamic DNS		Этот экран позволяет вам использовать статический псевдоним вместо динамического IP-адреса.
Remote MGMT	WWW	На этом экране можно определить, через какие интерфейсы и с каких IP-адресов пользователям разрешается выполнять управление устройством P660HN по протоколу HTTP.
	Telnet	На этом экране можно определить, через какие интерфейсы и с каких IP-адресов пользователям разрешается выполнять управление устройством P660HN по протоколу Telnet.
	FTP	На этом экране можно определить, через какие интерфейсы и с каких IP-адресов пользователям разрешается доступ к устройству P660HN по протоколу FTP.
	SNMP	Этот экран используется для настройки параметров вашего устройства P660HN для управления простым протоколом управления сетью.
	DNS	На этом экране можно определить, через какие интерфейсы и с каких IP-адресов пользователи могут посылать запросы DNS к устройству P660HN.
	ICMP	Этот экран используется для настройки отклика вашего устройства на эхо-тестирование и зондирование тех услуг, которые вы сделали недоступными.
UPnP	General	Этот экран используется для включения или отключения UPnP.
Maintenance		
System	General	Этот экран используется для указания имени устройства, имени домена, пароля, времени простоя в режиме управления.
	Time Setting	Этот экран используется для изменения времени и даты на устройстве P660HN.
Logs	View Log	Этот экран используется для отображения журналов регистрации устройства.
	Log Settings	На этом экране можно выбрать, какие регистрационные записи или извещения должно записывать ваше устройство. Можно также указать, чтобы устройство отправляло записи журнала на вашу электронную почту.

Табл. 3 Краткое описание панели навигации (продолжение)

ССЫЛКА	ЗАКЛАДКА	ФУНКЦИЯ
Tools	Firmware	Этот экран используется для загрузки микропрограммного обеспечения в ваше устройство.
	Configuration	Этот экран используется для создания резервной копии/ восстановления файла конфигурации (настроек) или сброса настроек устройства к заводским настройкам по умолчанию.
	Restart	Этот экран позволяет выполнить перезагрузку устройства P660HN без выключения электропитания.
Diagnostic	General	Этот экран используется для проверки подключений к другим устройствам.
	DSL Line	Этот экран отображает информацию, позволяющую идентифицировать проблемы, связанные с линией DSL.

2.2.3 Главное окно

На главном окне отображается информация и поля настройки. Об этом рассказывается в оставшейся части данной документации.

Сразу же после входа в систему отображается экран **Status**. См. Гл. 3 на с. 40 с подробными сведениями об экране **Status**.

2.2.4 Строка состояния

Проверьте отметку на строке состояния после того, как нажмете **Apply** или **OK** для подтверждения обновления конфигурации.

3

Экран состояния

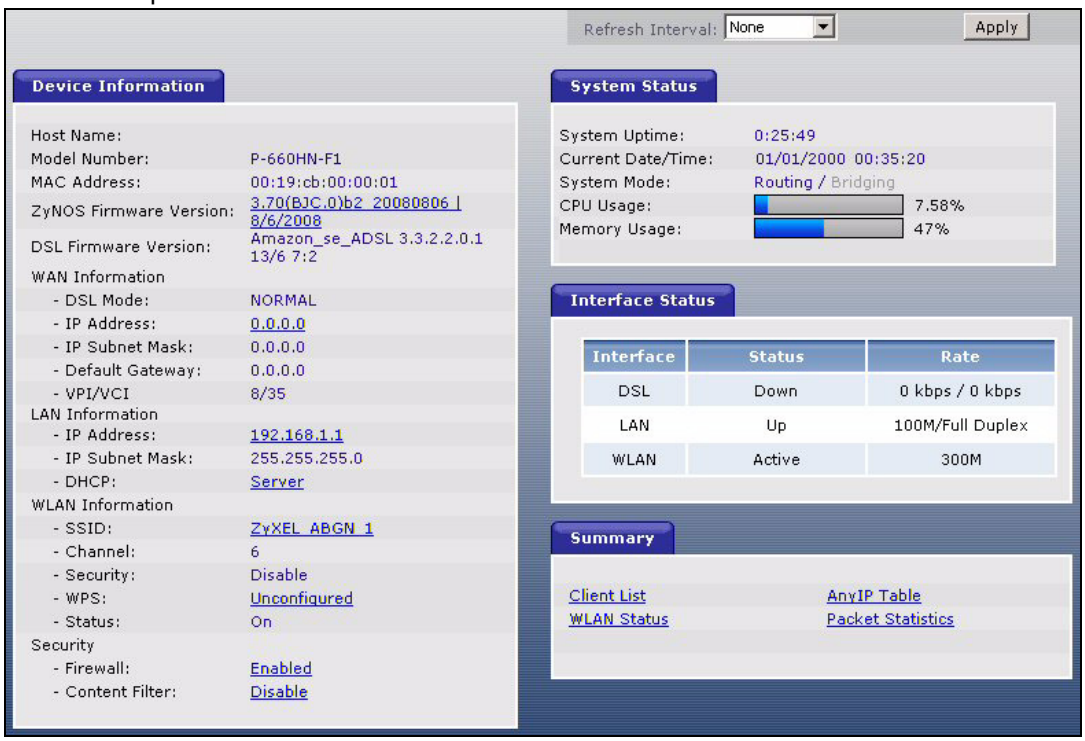
3.1 Обзор

Экран **Status** используется для просмотра текущего состояния устройства, системных ресурсов и интерфейсов (LAN и WAN). На экране **Status** можно также просмотреть подробную информацию о функции Any IP и DHCP, статистику управления пропускной способностью, а также информацию о трафике.

3.2 Экран состояния

Этот экран используется для просмотра статуса устройства P660HN. Для того, чтобы открыть этот экран, нажмите **Status**.

Рис. 7 Экран состояния



В следующей таблице даны описания полей этого экрана.

Табл. 4 Экран состояния

ПОЛЕ	ОПИСАНИЕ
Refresh Interval	Введите значение частоты обновления устройством P660HN этого экрана.
Apply	Нажмите эту кнопку для обновления экрана.
Device Information	
Host Name	В этом поле отображается системное имя устройства P660HN. Это имя используется для идентификации устройства. Изменить его можно на экране **Maintenance > System > General** в поле **System Name**.
Model Number	Наименование модели вашего устройства.
MAC Address	Уникальный MAC-адрес (Media Access Control – Управление доступом к среде) или адрес Ethernet вашего устройства P660HN.
ZyNOS Firmware Version	В этом поле отображается текущая версия микропрограммного обеспечения внутри устройства. Кроме того, здесь указывается дата создания версии микропрограммного обеспечения. Нажмите сюда для перехода к экрану, на котором можно изменить дату.
DSL Firmware Version	В этом поле отображается текущая версия кода DSL-модема устройства.
WAN Information	
DSL Mode	Здесь отображается DSL-стандарт, используемый устройством P660HN.
IP Address	В этом поле отображается текущий IP-адрес устройства P660HN в глобальной сети. Нажмите сюда для перехода к экрану, на котором можно изменить адрес.
IP Subnet Mask	В этом поле отображается текущая маска подсети в глобальной сети.
Default Gateway	Здесь отображается IP-адрес шлюза по умолчанию, если он применяется.
VPI/VCI	Идентификатор виртуального пути и идентификатор виртуального канала, настраиваемые с помощью Мастера установки или на экране **WAN**.
LAN Information	
IP Address	В этом поле отображается текущий IP-адрес устройства P660HN в локальной сети. Нажмите сюда для перехода к экрану, на котором можно изменить адрес.
IP Subnet Mask	В этом поле отображается текущая маска подсети в локальной сети.
DHCP	В этом поле отображаются службы DHCP, которые устройство P660HN предусматривает для LAN. Опциями являются: **Server** – устройство P660HN используется в качестве сервера DHCP в LAN. Оно может присваивать IP-адреса другим компьютерам в LAN. **Relay** – устройство P660HN действует в качестве фиктивного DHCP-сервера и обеспечивает передачу запросов и ответов DHCP между удаленным сервером и клиентами. **None** – устройство P660HN не обеспечивает услуги DHCP для LAN. Нажмите сюда для перехода к экрану, на котором можно изменить эту опцию.
WLAN Information	
SSID	Описательное имя, используемое для идентификации устройства P660HN в беспроводной LAN. Нажмите сюда для перехода к экрану, на котором можно изменить имя.

Табл. 4 Экран состояния (продолжение)

ПОЛЕ	ОПИСАНИЕ
Channel	Номер канала, по которому работает устройство P660HN.
Security	Здесь отображается режим безопасности, используемый устройством P660HN в беспроводной LAN.
WPS	Здесь указано, используется ли WPS. Нажмите сюда для перехода к экрану, на котором можно изменить настройку.
Status	Здесь указано, используется ли WLAN.
Security	
Firewall	Это поле показывает, включен ли брандмауэр устройства P660HN. Нажмите сюда для перехода к экрану, на котором можно изменить настройку.
Content Filter	Это поле показывает, включено ли контент-фильтрование для устройства P660HN. Нажмите сюда для перехода к экрану, на котором можно изменить настройку.
System Status	
System Uptime	Это поле показывает, сколько времени работает устройство P660HN с момента последнего запуска. Момент запуска устройства P660HN – это момент включения питания, момент перезапуска (**Maintenance > Tools > Restart**) или момент сброса настроек.
Current Date/ Time	В этом поле отображается текущая дата и время устройства P660HN. Для изменения данных нажмите **Maintenance > System > Time Setting**.
System Mode	В этом поле отображается режим работы устройства P660HN: маршрутизатор или мост.
CPU Usage	Показывает текущий процент использования вычислительной мощности устройства P660HN. Приближение этого значения к 100 % означает, что устройство P660HN работает в режиме полной нагрузки, и увеличить его производительность больше нельзя. Если некоторым приложениям недостаточно вычислительной мощности устройства, следует закрыть другие приложения (например, использование функции QoS; см. Гл. 14 на с. 215).
Memory Usage	Показывает текущий процент использования памяти устройства P660HN. Как правило, это значение не должно сильно увеличиваться. Приближение этого значения к 100 % означает, что устройство P660HN работает нестабильно, и, возможно, требуется его перезагрузить. См. Разд. 20.4 на с. 290, или выключите устройство (отключите питание) на несколько секунд.
Interface Status	
Interface	В данной колонке отображаются все типы интерфейсов вашего устройства P660HN.
Status	Это поле показывает, используется ли устройством P660HN данный интерфейс. Для интерфейса DSL в этом поле отображается **Down** (соединение отсутствует), **Up** (соединение установлено и активно), если установлена инкапсуляция Ethernet, и **Down** (соединение отсутствует), **Up** (соединение установлено и активно), **Idle** (соединение (ppp) в режиме ожидания), **Dial** (запуск процедуры вызова) и **Drop** (сброс соединения), если установлена инкапсуляция PPPoE. Для интерфейса LAN в этом поле отображается **Up**, если устройство P660HN использует этот интерфейс, и **Down**, если устройство P660HN не использует его. Для интерфейса WLAN отображается **Active**, если WLAN включен или **InActive**, если выключен.

Табл. 4 Экран состояния (продолжение)

ПОЛЕ	ОПИСАНИЕ
Rate	Для интерфейса LAN здесь отображается скорость порта и режим дуплексной передачи. Для интерфейса DSL здесь отображается скорость приема и передачи данных. Для интерфейса WLAN здесь отображается максимальная скорость передачи, если WLAN включен или **N/A**, если WLAN отключен.
Summary	
Client List	Нажмите сюда для просмотра текущей информации о клиентах DHCP. См. Разд. 5.4 на с. 77.
AnyIP Table	Нажмите сюда для просмотра списка IP-адресов и MAC-адресов компьютеров, которые находятся в подсети, отличной от подсети устройства P660HN. См. Разд. 3.3 на с. 43.
WLAN Status	Нажмите сюда для просмотра MAC-адресов беспроводных станций, подключенных к устройству P660HN. См. Разд. 3.4 на с. 43.
Packet Statistics	Нажмите сюда для просмотра состояния портов и статистики пакетов. См. Разд. 3.5 на с. 44.

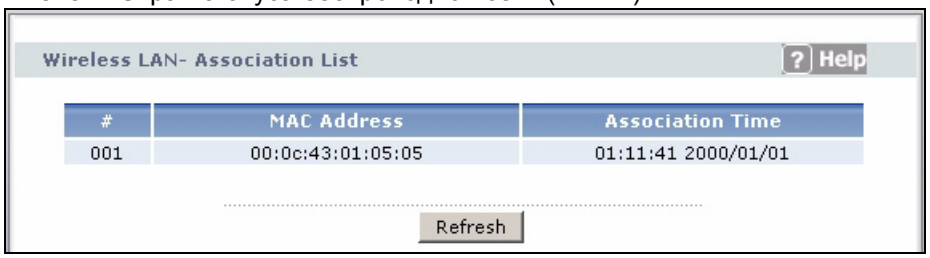
3.3 Список клиентов

Для получения более подробной информации об этом экране см. Разд. 5.4 на с. 77.

3.4 Экран статуса беспроводной сети (WLAN)

На этом экране отображается список беспроводных станций, подключенных к устройству P660HN. Для перехода к этому экрану нажмите **Status > WLAN Status**.

Рис. 8 Экран статуса беспроводной сети (WLAN)



В следующей таблице даны описания полей этого экрана.

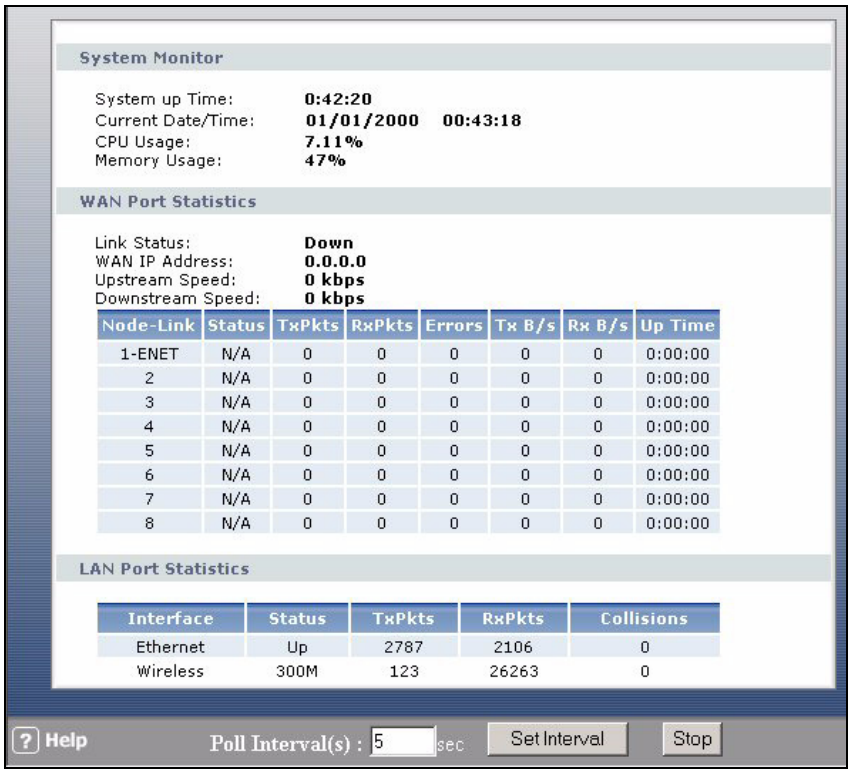
Табл. 5 WLAN Status

ПОЛЕ	ОПИСАНИЕ
#	Порядковый номер подключенного беспроводного устройства.
MAC Address	В этом поле отображается MAC-адрес (Media Access Control – Управление доступом к среде) соответствующего беспроводного устройства.
Association Time	В этом поле отображается время, в течение которого беспроводная станция подключена к устройству P660HN.
Refresh	Нажмите эту кнопку для обновления информации на экране.

3.5 Статистика пакетов

Здесь отображается информация о состоянии портов и статистика пакетов в режиме только для чтения. Также здесь отображается время работы системы и интервал опроса системы. В поле **Poll Interval(s)** можно изменять значение. Для перехода к этому экрану нажмите **Status > Packet Statistics**.

Рис. 9 Статистика пакетов



В следующей таблице даны описания полей этого экрана.

Табл. 6 Статистика пакетов

ПОЛЕ	ОПИСАНИЕ
System Monitor	
System up Time	В этом поле отображается время, истекшее с момента запуска системы.
Current Date/Time	В этом поле отображается текущая дата и время устройства P660HN.
CPU Usage	В этом поле отображается процент загрузки процессора (CPU) модема.
Memory Usage	В этом поле отображается использование памяти в процентах.
WAN Port Statistics	
Link Status	В этом поле отображается состояние подключения к глобальной сети.
WAN IP Address	IP-адрес порта WAN устройства P660HN.
Upstream Speed	В этом поле отображается скорость исходящего трафика устройства P660HN
Downstream Speed	В этом поле отображается скорость входящего трафика устройства P660HN
Node-Link	В этом поле отображается порядковый номер удаленного узла и вид соединения. Виды соединения: PPPoA, ENET, RFC 1483 и PPPoE.

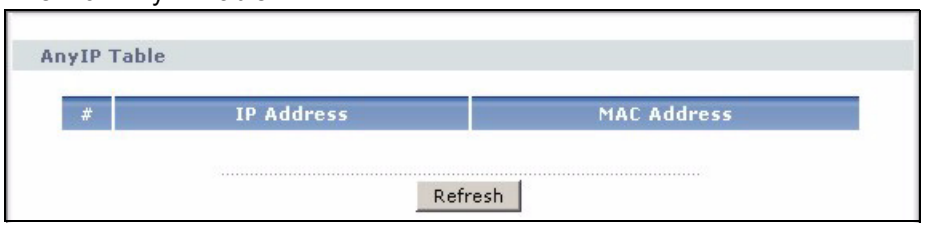
Табл. 6 Статистика пакетов (продолжение)

ПОЛЕ	ОПИСАНИЕ
Status	В этом поле отображается **Down** (соединение отсутствует), **Up** (соединение установлено и активно), если установлена инкапсуляция Ethernet и **Down** (соединение отсутствует), **Up** (соединение установлено и активно), **Idle** (соединение (ppp) в режиме ожидания), **Dial** (запуск процедуры вызова) и **Drop** (сброс соединения), если установлена инкапсуляция PPPoE.
TxPkts	В этом поле отображается количество пакетов, переданных через этот порт.
RxPkts	В этом поле отображается количество пакетов, принятых через этот порт.
Errors	В этом поле отображается количество пакетов с ошибками, принятых через этот порт.
Tx B/s	В этом поле отображается количество байтов, переданных в последнюю секунду.
Rx B/s	В этом поле отображается количество байтов, принятых в последнюю секунду.
Up Time	В этом поле отображается время, истекшее с момента установления соединения через этот порт.
LAN Port Statistics	
Interface	В этом поле отображается либо **Ethernet** (порты LAN), либо **Wireless** (порт WLAN).
Status	Для портов LAN в этом поле отображается **Down** (линия не работает) или **Up** (линия работает или включена). Для беспроводного порта WLAN здесь отображается скорость передачи, если порт WLAN включен или **N/A**, если порт WLAN отключен.
TxPkts	В этом поле отображается количество пакетов, переданных через этот интерфейс.
RxPkts	В этом поле отображается количество пакетов, принятых через этот интерфейс.
Collisions	В этом поле отображается количество конфликтов при передаче через данный интерфейс.
Poll Interval(s)	Введите интервал времени, через который браузер будет обновлять информацию о системе.
Set Interval	Нажмите эту кнопку, чтобы применить новый интервал опроса, заданный в поле **Poll Interval**.
Stop	Нажмите эту кнопку, чтобы прекратить обновление информации о системе.

3.6 Таблица Any IP

Для перехода к этому экрану нажмите **Status > AnyIP Table**. Этот экран используется для просмотра IP-адреса и MAC-адреса каждого компьютера, использующего устройство P660HN, но находящегося в подсети, отличной от подсети устройства P660HN.

Рис. 10 Any IP Table



В следующей таблице даны описания полей этого экрана.

Табл. 7 Any IP Table

ПОЛЕ	ОПИСАНИЕ
#	В этом поле содержится последовательная величина. Она не связана с каким-либо конкретным вводом.
IP Address	В этом поле отображается IP-адрес каждого компьютера, использующего устройство P660HN, но находящегося в подсети, отличной от подсети устройства P660HN.
MAC Address	В этом поле отображается MAC-адрес компьютера, использующего устройство P660HN, но находящегося в подсети, отличной от подсети устройства P660HN.
Refresh	Нажмите для обновления информации на этом экране.

Часть II
Сеть

4

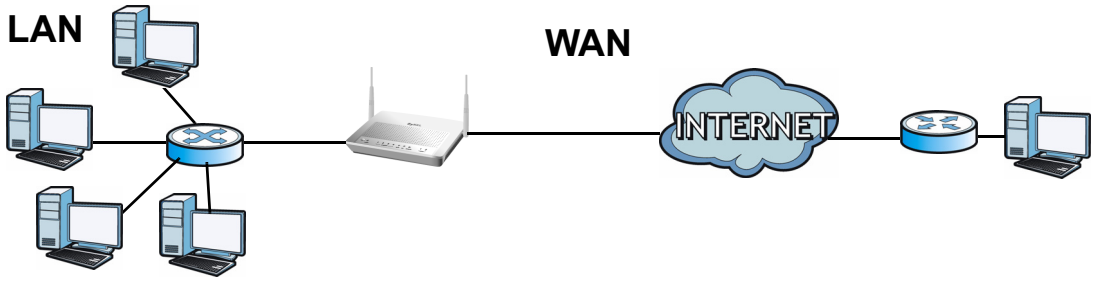
Настройка глобальной сети (WAN)

4.1 Обзор

В этой главе описывается конфигурирование настроек глобальной сети на экранах **WAN**. Эти экраны используются для настройки устройства P660HN для доступа в Интернет.

Интерфейс WAN (Wide Area Network – Глобальная вычислительная сеть) является внешним подключением к другой сети или к сети Интернет. Она подключает ваши частные сети (например LAN (локальная вычислительная сеть)), и другие сети так, что компьютер, расположенный в одном месте, может связываться с компьютерами, находящимися в других местах.

Рис. 11 LAN и WAN



4.1.1 Что можно сделать на экранах WAN

- Экран **Internet Access Setup** (Разд. 4.2 на с. 50) используется для настройки параметров WAN устройства P660HN для доступа в Интернет.
- Экран **More Connections** (Разд. 4.3 на с. 55) используется для установки дополнительных соединений для доступа в Интернет.
- Экран **WAN Backup Setup** (Разд. 4.4 на с. 62) используется для подключения резервного шлюза, который поможет перенаправить трафик к месту назначения, когда подключение к глобальной сети по умолчанию не работает.

4.1.2 Что нужно знать о глобальной сети

Метод инкапсуляции

Инкапсуляция используется для включения данных из протокола верхнего уровня в протокол нижнего уровня. Чтобы настроить подключение WAN к Интернету, необходимо применить тот же метод инкапсуляции, который используется вашим Интернет-провайдером (ISP). Если ваш Интернет-провайдер предлагает подключение к Интернету по телефонной линии с помощью PPPoE (Протокол «точка-точка» поверх Ethernet) или PPPoA (Протокол «точка-точка» через уровень 5 адаптации ATM), то он должен также дать вам имя пользователя и пароль (и наименование службы) для аутентификации пользователя.

IP-адрес WAN

IP-адрес глобальной сети WAN представляет собой IP-адрес устройства P660HN, обеспечивая доступ к нему из внешней сети. Он используется устройством P660HN для связи с другими устройствами в других сетях. Он может быть статическим (фиксированным) или динамически присваиваться Интернет-провайдером каждый раз, когда устройство P660HN пытается выйти в Интернет.

Если ваш Интернет-провайдер присваивает вам статический IP-адрес глобальной сети WAN, то он должен также присвоить вам маску подсети и IP-адрес (-адреса) сервера DNS (а также IP-адрес шлюза, если вы используете метод инкапсуляции Ethernet или ENET ENCAP).

Многоадресная рассылка

Обычно передача IP-пакетов происходит одним из двух способов – одноадресная рассылка (1 отправитель – 1 получатель) или широковещательная рассылка (1 отправитель – все компьютеры в сети). Многоадресная рассылка представляет собой третий способ передачи IP-пакетов группе хост-машин, подключенных к сети, – но не всем и не только одной.

IGMP

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. Существуют три версии IGMP. IGMP версии 2 – усовершенствованный вариант версии 1, но IGMP версии 1 по-прежнему широко используется. IGMP версии 3 поддерживает фильтрование источника, игнорирование трафика или отчет о трафике с конкретного адрес источника на конкретный узел сети.

Дополнительные сведения

Техническую вводную информацию о WAN см. в Разд. 4.5 на с. 63.

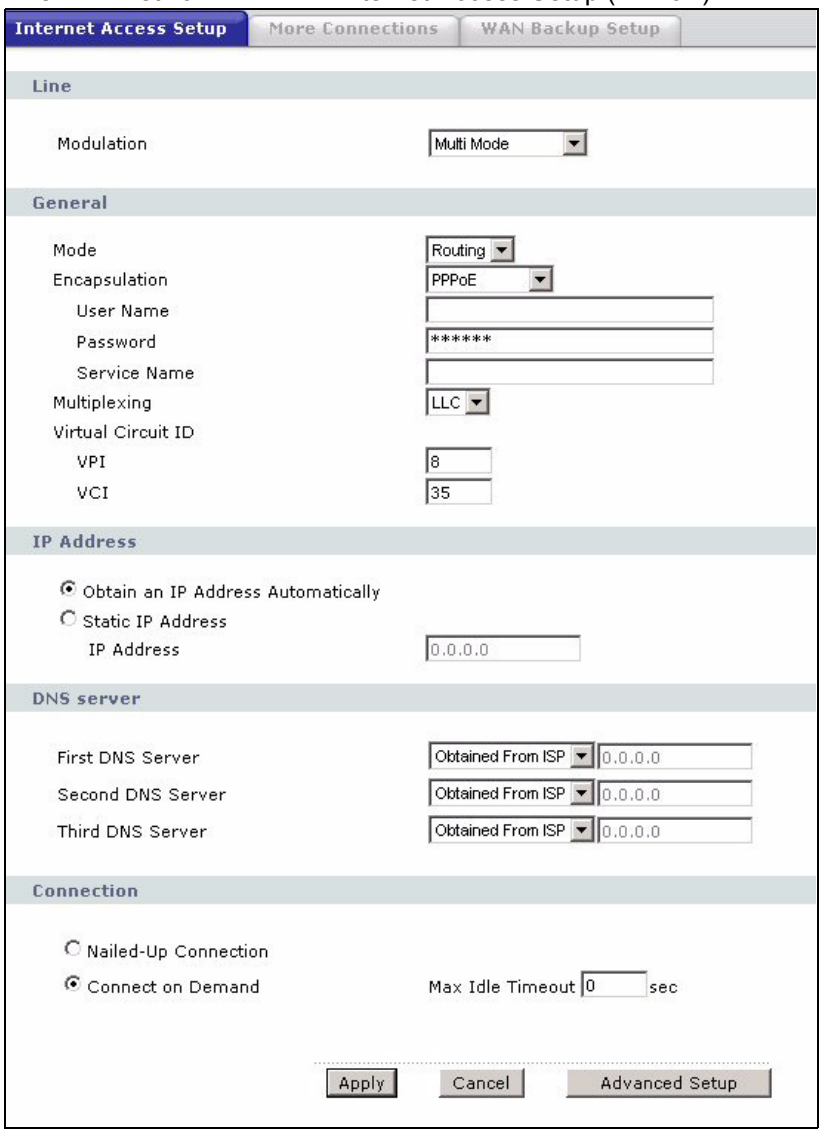
4.1.3 Перед началом

Необходимо узнать настройки доступа в Интернет, такие как инкапсуляция и IP-адрес в глобальной сети (WAN). Получите эти сведения у своего Интернет-провайдера.

4.2 Экран настройки доступа в Интернет

Этот экран используется для изменения настроек WAN устройства P660HN. Нажмите **Network > WAN > Internet Access Setup**. Экран будет отличаться в зависимости от выбранного вами типа WAN и инкапсуляции.

Рис. 12 Network > WAN > Internet Access Setup (PPPoE)



В следующей таблице даны описания полей этого экрана.

Табл. 8 Network > WAN > Internet Access Setup

ПОЛЕ	ОПИСАНИЕ
Line	
Modulation	Выберите тип модуляции, поддерживаемый вашим Интернет-провайдером. Используйте **Multi Mode**, если вы не знаете точно, какой режим следует выбрать. Устройство P660HN осуществляет динамическую диагностику режима, поддерживаемого Интернет-провайдером, и выбирает для подключения наиболее совместимый режим. Другие варианты: **ADSL G.dmt**, **ADSL2**, **ADSL2+**, **ADSL2 AnnexM**, **ADSL2+ AnnexM**, **READSL2 Mode** и **ANSI T1.413**.
General	
Mode	Выберите **Routing** (по умолчанию) из выпадающего списка, если ваш Интернет-провайдер предоставляет вам только один IP-адрес, а вы хотите, чтобы несколько компьютеров использовали одну учетную запись Интернет. Выберите режим **Bridge**, если ваш Интернет-провайдер дает вам более одного IP-адреса и вы хотите присвоить подключенным компьютерам индивидуальные IP-адреса непосредственно с DHCP-сервера Интернет-провайдера. При выборе **Bridge** нельзя пользоваться брандмауэром, сервером DHCP и NAT на устройстве P660HN.
Encapsulation	Из выпадающего списка выберите метод инкапсуляции, используемый вашим Интернет-провайдером. Варианты в списке зависят от режима, установленного в поле **Mode**. Если в поле **Mode** вы установили **Bridge**, то выберите **PPPoA** или **RFC 1483**. Если в поле **Mode** вы установили **Routing**, то выберите **PPPoA**, **RFC 1483**, **ENET ENCAP** или **PPPoE**.
User Name	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 введите оба элемента имени в полном соответствии с данными от провайдера.
Password	Введите пароль для данного имени пользователя (только для инкапсуляции PPPoA и PPPoE).
Service Name	Введите имя службы PPPoE в это поле (только для PPPoE)
Multiplexing	Из выпадающего списка выберите метод мультиплексирования, используемый Интернет-провайдером. Вариантами являются **VC** или **LLC**. Это поле недоступно, если для типа WAN указано **Ethernet**.
Virtual Circuit ID	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	Допустимый диапазон для VPI – от 0 до 255. Введите назначенный вам номер VPI.
VCI	Допустимый диапазон для VCI – от 32 до 65535 (номера 0 – 31 зарезервированы для локального управления трафиком ATM). Введите назначенный вам номер VCI.
IP Address	Это поле доступно, если в поле **Mode** выбран режим **Routing**. Статический IP-адрес – это фиксированный IP-адрес, который назначает Интернет-провайдер. Динамический IP-адрес не является фиксированным. При каждом подключении к Интернету Интернет-провайдер будет назначать новый адрес. Выберите **Obtain an IP Address Automatically**, если у вас динамический IP-адрес; или выберите **Static IP Address** и введите, назначенный Интернет-провайдером IP-адрес в поле **IP Address**.

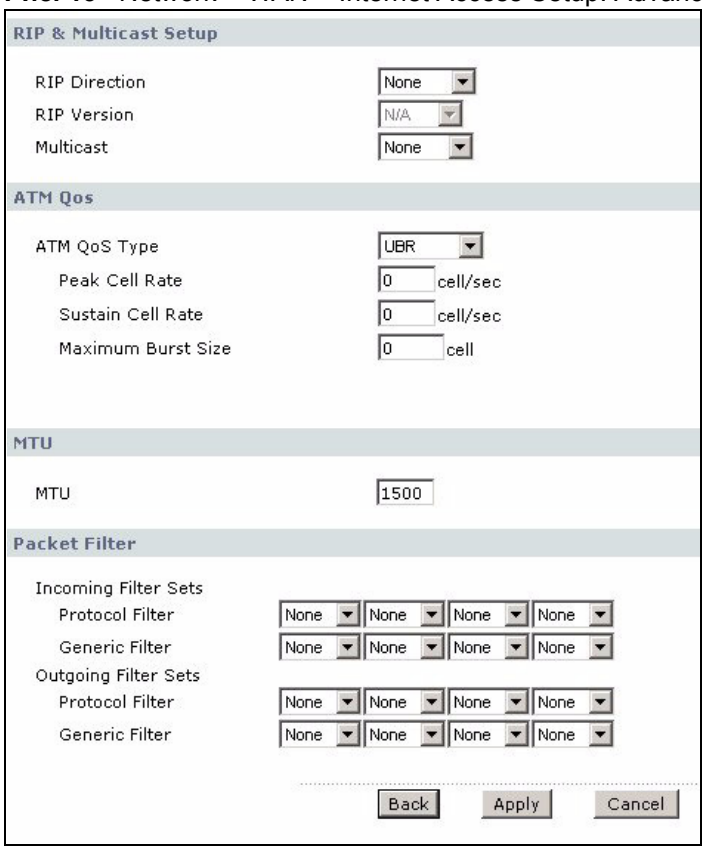
Табл. 8 Network > WAN > Internet Access Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
Subnet Mask	Это поле доступно, если выбран вариант **ENET ENCAP** в поле **Encapsulation**. Введите маску подсети в десятичном формате с разделительными точками.
Gateway IP address	Это поле доступно, если выбран вариант **ENET ENCAP** в поле **Encapsulation**. Введите IP-адрес шлюза, предоставленный Интернет-провайдером.
DNS Server	
First DNS Server Second DNS Server Third DNS Server	Выберите **Obtained From ISP**, если ваш поставщик Интернет-услуг предоставляет динамическую информацию о сервере DNS (а также IP-адрес WAN устройства P660HN), и если вы выбрали опцию **Obtain an IP Address Automatically**. Если вам известен IP-адрес сервера DNS, выберите вариант **User-Defined**. Введите IP-адрес сервера DNS в поле, расположенное справа. Если выбрать вариант **User-Defined**, но не указать IP-адрес, то при нажатии на кнопку **Apply** вариант **User-Defined** сменится на **None**. Если для второго сервера выбрать вариант **User-Defined** и указать точно такой же IP-адрес, то при нажатии на кнопку **Apply** он поменяется на **None**. Если вы не хотите настраивать серверы DNS, выберите вариант **None**. Для работы в локальной сети необходим другой сервер DHCP, в противном случае необходимо настраивать адреса DNS-серверов на компьютерах вручную. Если сервер DNS не используется, то для подключения к компьютерам необходимо будет указывать их IP-адреса.
Connection (Только для инкапсуляции PPPoA и PPPoE)	
Nailed-Up Connection	Выберите **Nailed-Up Connection**, если требуется постоянное соединение. При разрыве соединения устройство P660HN автоматически будет пытаться восстановить его.
Connect on Demand	Выберите **Connect on Demand**, если вы не хотите иметь постоянное соединение, и установите время простоя в поле **Max Idle Timeout**.
Max Idle Timeout	При выборе **Connect on Demand**, установите время простоя в поле **Max Idle Timeout**. По умолчанию установлено 0, что означает, что соединение с Интернет не будет разрываться.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.
Advanced Setup	Нажмите эту кнопку для отображения экрана **Advanced WAN Setup** и установите дополнительные настройки глобальной сети.

4.2.1 Дополнительные параметры настройки доступа в Интернет

Этот экран используется для настройки дополнительных параметров подключения устройства P660HN к WAN. Нажмите кнопку **Advanced Setup** на экране **Internet Access Setup**. При этом откроется показанный ниже экран.

Рис. 13 Network > WAN > Internet Access Setup: Advanced Setup



В следующей таблице даны описания полей этого экрана.

Табл. 9 Network > WAN > Internet Access Setup: Advanced Setup

ПОЛЕ	ОПИСАНИЕ
RIP & Multicast Setup	Этот раздел недоступен, если устройство P660HN находится в режиме межсетевого моста.
RIP Direction	RIP (Routing Information Protocol – Протокол обмена информацией о маршрутизации) позволяет маршрутизатору обмениваться информацией о маршрутизации с другими маршрутизаторами. Это поле определяет какую информацию о маршрутизации устройство P660HN передает и принимает в данной подсети. Выберите направление RIP среди вариантов **None**, **Both**, **In Only** и **Out Only**.
RIP Version	Это поле не конфигурируется, если в поле **RIP Direction** выбрано **None**. Выберите версию RIP среди вариантов **RIP-1**, **RIP-2B** и **RIP-2M**.

Табл. 9 Network > WAN > Internet Access Setup: Advanced Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
Multicast	Пакеты многоадресной рассылки передаются группе компьютеров в локальной сети LAN и являются альтернативой пакетам одноадресной рассылки (пакетам, которые передаются на один компьютер) и пакетам широковещательной рассылки (пакетам, которые рассылаются на все компьютеры). IGMP (Internet Group Multicast Protocol – Протокол многоадресной рассылки) – это протокол сетевого уровня, используемый для установления принадлежности к группе многоадресной рассылки. Устройство P660HN поддерживает **IGMP v1**, **IGMP v2** и **IGMP v3**. Выберите **None** для отключения IGMP.
ATM QoS	
ATM QoS Type	Выберите **CBR** (Continuous Bit Rate – Постоянная скорость передачи) для установки постоянной (всегда доступной) пропускной способности для трафика речи или данных. Выберите **UBR** (Unspecified Bit Rate – Неопределенная скорость передачи) для приложений, нечувствительных ко времени, таких как электронная почта. Выберите **VBR-RT** (real-time Variable Bit Rate – Переменная скорость передачи в реальном времени) для приложений с пульсирующим трафиком, который требует тщательного контроля задержки и изменений задержки. Выберите **VBR-nRT** (non real-time Variable Bit Rate – Переменная скорость передачи вне реального времени) для подключений, которые не требуют тщательного контроля задержки и изменений задержки.
Peak Cell Rate	Разделите скорость линии DSL (бит/с) на 424 (размер ячейки ATM), чтобы получить значение скорости PCR (Peak Cell Rate – Максимальная скорость передачи ячеек). Это и будет максимальная скорость, с которой отправитель может передавать ячейки. Введите в это поле значение PCR.
Sustain Cell Rate	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	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).
PPPoE Passthrough (PPPoE encapsulation only)	Это поле доступно, если вы выбрали инкапсуляцию **PPPoE**. В дополнение к встроенному в устройство P660HN клиенту PPPoE, можно включить пропускание PPPoE, позволяющее 10 узлам локальной сети с установленным клиентским программным обеспечением PPPoE подключиться к Интернет-провайдеру через устройство P660HN. 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.
MTU	
MTU	Максимальный размер единицы передаваемой информации (MTU) определяет наибольший размер пакета, допустимого для интерфейса или подключения. Введите MTU в этом поле. Для ENET ENCAP значение MTU равно 1500. Для PPPoE значение MTU равно 1492. Для PPPoA и RFC 1483 значение MTU равно 65535.

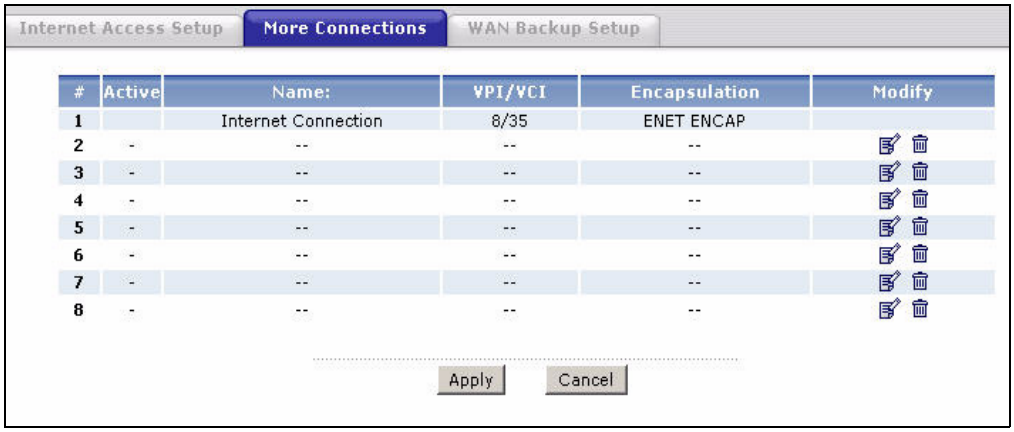
Табл. 9 Network > WAN > Internet Access Setup: Advanced Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
Packet Filter	
Incoming Filter Sets	
Protocol Filter	Выберите фильтр (фильтры) протокола для контроля входящего трафика. Можно выбрать до 4 наборов фильтров. Настроить параметры пакетных фильтров можно на экране **Packet Filter**. Более подробную информацию см. в Гл. 10 на с. 164.
Generic Filter	Выберите фильтр (фильтры) общего типа для контроля входящего трафика. Можно выбрать до 4 наборов фильтров. Настроить параметры общих фильтров можно на экране **Packet Filter**. Более подробную информацию см. в Гл. 10 на с. 164.
Outgoing Filter Sets	
Protocol Filter	Выберите фильтр (фильтры) протокола для контроля исходящего трафика. Можно выбрать до 4 наборов фильтров. Настроить параметры фильтров протоколов можно на экране **Packet Filter**. Более подробную информацию см. в Гл. 10 на с. 164.
Generic Filter	Выберите фильтр (фильтры) общего типа для контроля исходящего трафика. Можно выбрать до 4 наборов фильтров. Настроить параметры общих фильтров можно на экране **Packet Filter**. Более подробную информацию см. в Гл. 10 на с. 164.
Back	Нажмите эту кнопку для возврата к предыдущему экрану без сохранения.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

4.3 Экран дополнительных соединений

Устройство P660HN позволяет настроить более одного PVC. Для настройки дополнительных PVC нажмите **Network > WAN > More Connections**. При настройке доступа в Интернет на экране **WAN > Internet Access Setup** устанавливается основное подключение к глобальной сети.

Рис. 14 Network > WAN > More Connections



В следующей таблице даны описания полей этого экрана.

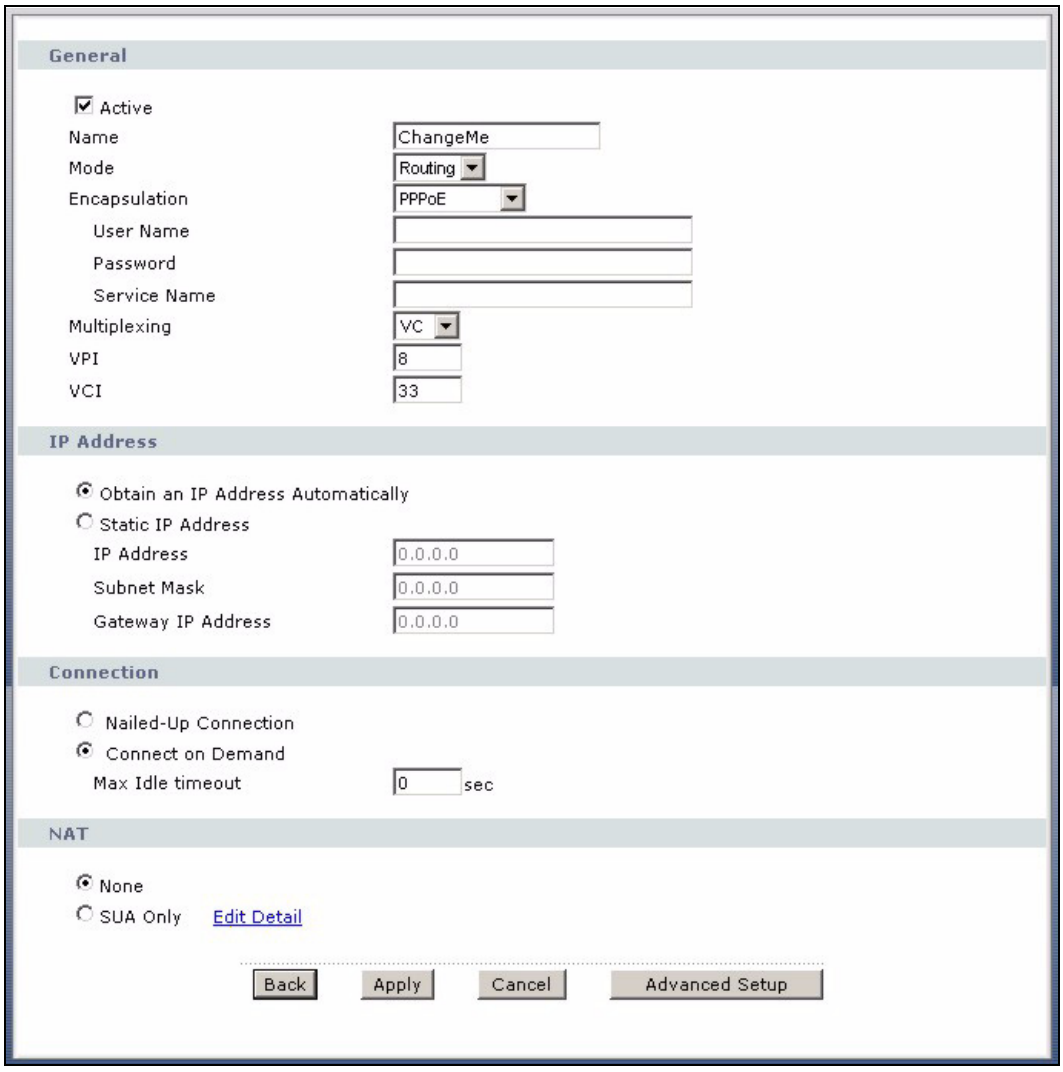
Табл. 10 Network > WAN > More Connections

ПОЛЕ	ОПИСАНИЕ
#	Этот номер соответствует порядковому номеру соединения.
Active	В этом поле указано, активно ли соединение. Чтобы отключить соединение, снимите флажок. Для включения соединения поставьте флажок.
Name	Это имя, назначенное вами Интернет-соединению.
VPI/VCI	В этом поле отображаются числа VPI (Идентификатор виртуального пути) и VCI (Идентификатор виртуального канала), указанные для этого WAN-соединения.
Encapsulation	В этом поле указывается метод инкапсуляции этого Интернет-соединения.
Modify	На этом экране отображается основное соединение (с Интернет-провайдером) в режиме только для чтения. Изменение его параметров производится на экране **WAN > Internet Access Setup**. Щелкните по иконке редактирования для изменения настроек Интернет-соединения. Щелкните по этой иконке в пустом поле конфигурации для добавления новой настройки доступа в Интернет. Щелкните по иконке удаления, чтобы удалить настройку доступа в Интернет из списка соединений.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

4.3.1 Редактирование дополнительных PVC

Этот экран используется для конфигурирования параметров соединения. Щелкните по иконке редактирования на экране **More Connections** для отображения следующего экрана.

Рис. 15 Network > WAN > More Connections: Edit



В следующей таблице даны описания полей этого экрана.

Табл. 11 Network > WAN > More Connections: Edit

ПОЛЕ	ОПИСАНИЕ
General	
Active	Чтобы включить соединение, поставьте флажок в этом поле, чтобы отключить – снимите флажок.
Name	Введите уникальное описательное имя для данного соединения длиной до 13 символов ASCII.

Табл. 11 Network > WAN > More Connections: Edit (продолжение)

ПОЛЕ	ОПИСАНИЕ
Mode	Из раскрывающегося списка выберите режим **Routing**, если ваш Интернет-провайдер разрешает подключение нескольких компьютеров по одной учетной записи. При выборе опции **Bridge** устройство P660HN будет пересылать все пакеты, которые оно не маршрутизирует, на данный удаленный узел; в противном случае, все пакеты сбрасываются.
Encapsulation	Из выпадающего списка выберите метод инкапсуляции, используемый вашим Интернет-провайдером. Варианты в списке зависят от режима, установленного в поле **Mode**. Если в поле **Mode** вы установили **Bridge**, то выберите **PPPoA** или **RFC 1483**. Если в поле **Mode** вы установили **Routing**, то выберите **PPPoA**, **RFC 1483**, **ENET ENCAP** или **PPPoE**.
User Name	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 введите оба элемента имени в полном соответствии с данными от провайдера.
Password	Введите пароль для данного имени пользователя (только для инкапсуляции PPPoA и PPPoE).
Service Name	Введите имя службы PPPoE в это поле (только для PPPoE).
Multiplexing	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	Допустимый диапазон для VPI – от 0 до 255. Введите назначенный вам номер VPI.
VCI	Допустимый диапазон для VCI – от 32 до 65535 (номера 0 – 31 зарезервированы для локального управления трафиком ATM). Введите назначенный вам номер VCI.
IP Address	Это поле доступно, если в поле **Mode** выбран режим **Routing**. Статический IP-адрес – это фиксированный IP-адрес, который назначает Интернет-провайдер. Динамический IP-адрес не является фиксированным. При каждом подключении к Интернету Интернет-провайдер будет назначать новый адрес. Если используется тип инкапсуляции кроме **RFC 1483**, выберите **Obtain an IP Address Automatically** при наличии у вас динамического IP-адреса; или выберите **Static IP Address** и введите, назначенный Интернет-провайдером IP-адрес в поле **IP Address**. Если используется **RFC 1483**, введите IP-адрес, предоставленный вашим Интернет-провайдером, в поле **IP Address**.
Subnet Mask	Это поле доступно, если выбран вариант **ENET ENCAP** в поле **Encapsulation**. Введите маску подсети в десятичном формате с разделительными точками.

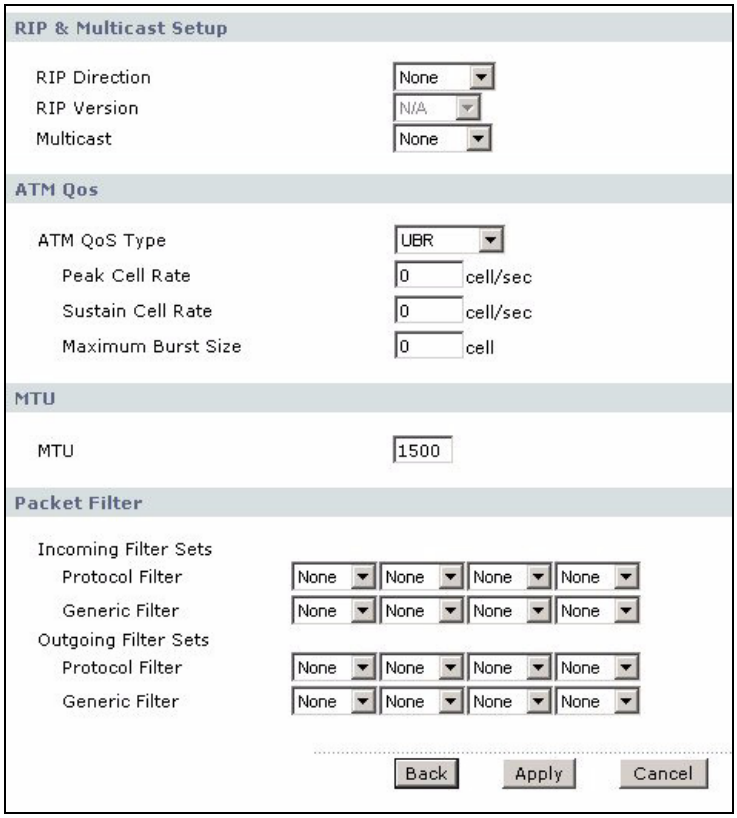
Табл. 11 Network > WAN > More Connections: Edit (продолжение)

ПОЛЕ	ОПИСАНИЕ
Gateway IP address	Это поле доступно, если выбран вариант **ENET ENCAP** в поле **Encapsulation**. Введите IP-адрес шлюза, предоставленный Интернет-провайдером.
Connection	
Nailed-Up Connection	Выберите **Nailed-Up Connection**, если требуется постоянное соединение. При разрыве соединения устройство P660HN автоматически будет пытаться восстановить его.
Connect on Demand	Выберите **Connect on Demand**, если вы не хотите иметь постоянное соединение, и установите время простоя в поле **Max Idle Timeout**.
Max Idle Timeout	При выборе **Connect on Demand,** установите время простоя в поле **Max Idle Timeout**. По умолчанию установлено 0, что означает, что соединение с Интернет не будет разрываться.
NAT	Поле **SUA Only** доступно, только если в поле **Mode** установлено значение **Routing**. Выберите **SUA Only**, если имеется только один общедоступный IP-адрес и требуется использовать NAT. Нажмите **Edit Detail** для перехода к экрану **Port Forwarding** и внесения изменений в таблицу отображения портов сервера. Чтобы отключить функцию NAT, выберите опцию **None**.
Back	Нажмите эту кнопку для возврата к предыдущему экрану без сохранения.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.
Advanced Setup	Нажмите эту кнопку для отображения экрана **More Connections Advanced Setup** и установите дополнительные настройки глобальной сети.

4.3.2 Настройка дополнительных параметров дополнительных PVC

Этот экран используется для настройки дополнительных параметров подключения устройства P660HN к WAN. Нажмите кнопку **Advanced Setup** на экране **More Connections Edit**. При этом откроется показанный ниже экран.

Рис. 16 Network > WAN > More Connections: Edit: Advanced Setup



В следующей таблице даны описания полей этого экрана.

Табл. 12 Network > WAN > More Connections: Edit: Advanced Setup

ПОЛЕ	ОПИСАНИЕ
RIP & Multicast Setup	Этот раздел недоступен, если устройство P660HN находится в режиме межсетевого моста.
RIP Direction	Выберите направление RIP среди вариантов **None**, **Both**, **In Only** и **Out Only**.
RIP Version	Выберите версию RIP среди вариантов **RIP-1**, **RIP-2B** и **RIP-2M**.
Multicast	IGMP (Internet Group Multicast Protocol – Протокол многоадресной рассылки) – это протокол сетевого уровня, используемый для установления принадлежности к группе многоадресной рассылки. Устройство P660HN поддерживает **IGMP v1**, **IGMP v2** и **IGMP v3**. Выберите **None** для отключения IGMP.

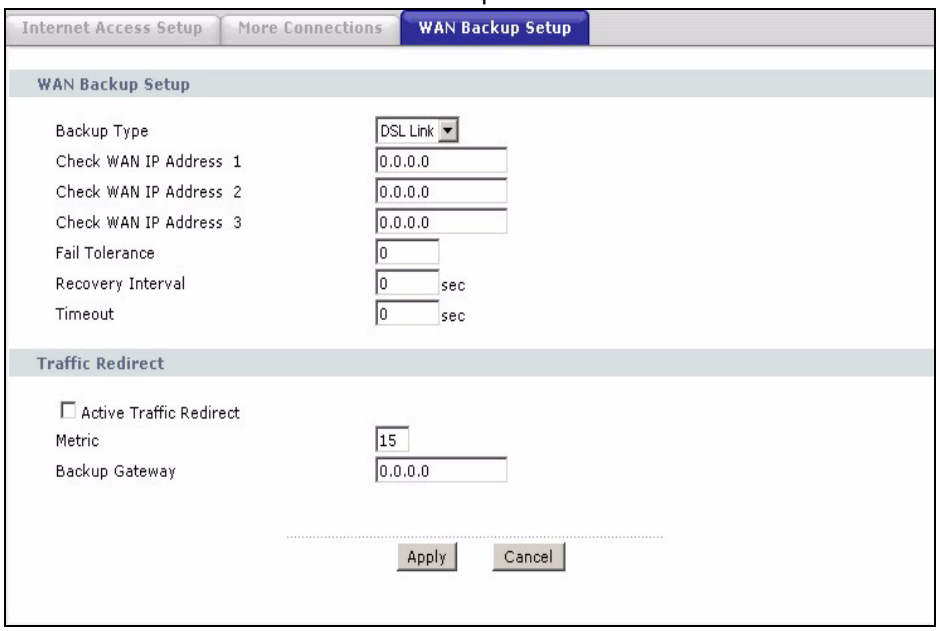
Табл. 12 Network > WAN > More Connections: Edit: Advanced Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
ATM QoS	
ATM QoS Type	Выберите **CBR** (Continuous Bit Rate – Постоянная скорость передачи) для установки постоянной (всегда доступной) пропускной способности для трафика речи или данных. Выберите **UBR** (Unspecified Bit Rate – 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	Разделите скорость линии DSL (бит/с) на 424 (размер ячейки ATM), чтобы получить значение скорости PCR (Peak Cell Rate – Максимальная скорость передачи ячеек). Это и будет максимальная скорость, с которой отправитель может передавать ячейки. Введите в это поле значение PCR.
Sustain Cell Rate	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	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).
MTU	
MTU	Максимальный размер единицы передаваемой информации (MTU) определяет наибольший размер пакета, допустимого для интерфейса или подключения. Введите MTU в этом поле. Для ENET ENCAP значение MTU равно 1500. Для PPPoE значение MTU равно 1492. Для PPPoA и RFC значение MTU равно 65535.
Packet Filter	
Incoming Filter Sets	
Protocol Filter	Выберите фильтр (фильтры) протокола для контроля входящего трафика. Можно выбрать до 4 наборов фильтров. Настроить параметры пакетных фильтров можно на экране **Packet Filter**. Более подробную информацию см. в Гл. 10 на с. 164.
Generic Filter	Выберите фильтр (фильтры) общего типа для контроля входящего трафика. Можно выбрать до 4 наборов фильтров. Настроить параметры общих фильтров можно на экране **Packet Filter**. Более подробную информацию см. в Гл. 10 на с. 164.
Outgoing Filter Sets	
Protocol Filter	Выберите фильтр (фильтры) протокола для контроля исходящего трафика. Можно выбрать до 4 наборов фильтров. Настроить параметры фильтров протоколов можно на экране **Packet Filter**. Более подробную информацию см. в Гл. 10 на с. 164.
Generic Filter	Выберите фильтр (фильтры) общего типа для контроля исходящего трафика. Можно выбрать до 4 наборов фильтров. Настроить параметры общих фильтров можно на экране **Packet Filter**. Более подробную информацию см. в Гл. 10 на с. 164.
Back	Нажмите эту кнопку для возврата к предыдущему экрану без сохранения.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

4.4 Экран настройки резервного подключения WAN

Этот экран используется для изменения настроек резервного подключения устройства P660HN. Нажмите **Network > WAN > WAN Backup Setup**.

Рис. 17 Network > WAN > WAN Backup



В следующей таблице даны описания полей этого экрана.

Табл. 13 Network > WAN > WAN Backup

ПОЛЕ	ОПИСАНИЕ
WAN Backup Setup	
Backup Type	Выберите метод, который устройство P660HN будет использовать для проверки соединения DSL. Выберите **DSL Link**, чтобы устройство P660HN проверяло, установлено ли подключение к DSLAM. Выберите **ICMP**, чтобы устройство P660HN периодически посылало эхо-пакеты на IP-адреса, установленные в полях **Check WAN IP Address**.
Check WAN IP Address1-3	Заполните это поле, чтобы устройство P660HN проверяло 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 устройство P660HN периодически посылает эхо-пакеты на заданные здесь адреса и, если ответ отсутствует, переходит на следующее резевное соединение с WAN (если установлено).
Fail Tolerance	Введите время в секундах (рекомендуется 2), в течение которого устройство P660HN будет посылать эхо-пакеты на IP-адреса, заданные в полях **Check WAN IP Address** при отсутствии ответа, прежде чем перейти на резервное соединение WAN (или другое резервное соединение WAN).

Табл. 13 Network > WAN > WAN Backup (продолжение)

ПОЛЕ	ОПИСАНИЕ
Recovery Interval	Если устройство P660HN использует соединение с более низким приоритетом (обычно резервное соединение с WAN), оно будет периодически проверять, можно ли перейти на соединение с более высоким приоритетом. Введите время в секундах (рекомендуется 30), в течение которого устройство P660HN может пребывать в режиме ожидания между проверками. Увеличьте время, если в устройстве с IP-адресом получателя обрабатывается большой объем трафика.
Timeout	Введите время в секундах (рекомендуется 3), в течение которого устройство P660HN ожидает ответ на эхо-запрос от одного из IP-адресов, установленных в поле **Check WAN IP Address**, прежде чем повторить запрос. Считается, что подключение устройства P660HN к глобальной сети отсутствует, после того как пройдет время, установленное в поле **Fail Tolerance**. Установите в этом поле большее значение, если ваша сеть очень занята или перегружена.
Traffic Redirect	При перенаправлении трафик пересылается на резервный шлюз, если устройство P660HN не может установить соединение с Интернетом.
Active Traffic Redirect	Поставьте в этом поле флажок, чтобы устройство P660HN использовало перенаправление трафика, если не удается установить нормальное подключение к глобальной сети. Примечание: При включении функции перенаправления трафика необходимо настроить хотя бы одно поле «Check WAN IP Address».
Metric	В этом поле устанавливается приоритет маршрута среди маршрутов, используемых устройством P660HN. Метрика определяет «стоимость передачи». 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, определяющее стоимость, должно лежать в интервале от «1» до «15»; значение больше «15» означает, что канал не работает. Чем меньше число, тем ниже «стоимость».
Backup Gateway	Введите IP-адрес резервного шлюза в десятичном виде с разделительными точками. Устройство P660HN автоматически пересылает трафик на данный IP-адрес при разрыве соединения устройства P660HN с Интернетом.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

4.5 Техническое руководство WAN

В этом разделе приводится некоторая вводная техническая информация по темам данной главы.

4.5.1 Инкапсуляция

Убедитесь, что используется метод инкапсуляции, предписанный вашим Интернет-провайдером. Ниже перечислены методы инкапсуляции, поддерживаемые с устройством P660HN.

4.5.1.1 Инкапсуляция ENET ENCAP

MAC 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 транспортные ячейки ATM. Для ENET ENCAP необходимо указать IP-адрес шлюза в поле **Gateway IP Address** на экране Мастера установки. Эту информацию можно получить у Интернет-провайдера.

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

Устройство P660HN поддерживает протокол PPPoE (Point-to-Point Protocol over Ethernet – Протокол «точка-точка» поверх Ethernet). PPPoE это стандарт IETF (RFC 2516), определяющий как персональный компьютер (PC) взаимодействует с широкополосным модемным соединением (DSL, кабель, беспроводной канал и т.д). Функция PPPoE применяется для коммутируемого соединения, использующего PPPoE.

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

Одно из преимуществ PPPoE заключается в возможности получения доступа к одной из многочисленных сетевых услуг – функции известной как динамической выбор услуги. Это позволяет провайдеру услуг 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 устройстве P660HN (а не на отдельных компьютерах), установка программного обеспечения PPPoE на компьютерах локальной сети не требуется, поскольку эта процедура полностью выполняется устройством P660HN. Кроме того, с NAT все компьютеры LAN будут иметь доступ.

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

PPPoA означает Протокол «точка-точка» через уровень 5 адаптации ATM (AAL5). Функции подключения PPPoA аналогичны коммутируемому подключению к Интернету. Устройство P660HN инкапсулирует сеанс связи PPP на базе RFC1483 и передает его через постоянный виртуальный канал ATM (Permanent Virtual Circuit – PVC) Интернет-провайдеру на концентратор DSLAM (Доступ мультиплексора к цифровой абонентской линии (DSL)). Для получения дополнительной информации по PPPoA см. комментарий RFC 2364. Для получения дополнительной информации по PPP см. комментарий RFC 1661.

4.5.1.4 RFC 1483

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

4.5.2 Мультиплексирование

Определить, какие протоколы используются для передачи по виртуальному каналу (VC), можно двумя способами. Убедитесь, что используется метод мультиплексирования, предписанный вашим Интернет-провайдером.

Мультиплексирование на базе VC

В этом случае, по предварительному взаимному соглашению, за каждым протоколом закрепляется конкретный виртуальный канал; например, по VC1 передается IP и т. д. Мультиплексирование на базе VC может быть основным методом в сетевом окружении, где динамическое создание большого числа виртуальных каналов ATM является более быстрым и экономичным.

Мультиплексирование на базе LLC

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

4.5.3 VPI и VCI

Убедитесь в правильности используемых номеров идентификатора виртуального пути (Virtual Path Identifier – VPI) и идентификатора виртуального канала (Virtual Channel Identifier – VCI), назначенных вам. Действительный диапазон для VPI – от 0 до 255, а для VCI – от 32 до 65535 (0 – 31 зарезервированы для локального управления трафиком ATM). Более подробно см. в Приложениях.

4.5.4 Назначение IP-адреса

Статический IP-адрес – это фиксированный IP-адрес, который назначает Интернет-провайдер. Динамический IP-адрес не является фиксированным. Интернет-провайдер каждый раз назначает новый 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.

Назначение IP с инкапсуляцией PPPoA или PPPoE

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

Назначение IP с инкапсуляцией RFC 1483

В этом случае назначение IP-адреса должно быть статическим.

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** и **Gateway IP Address** в соответствии с параметрами, предоставленными вашим Интернет-провайдером. Однако при назначении динамического IP-адреса устройство P660HN функционирует как клиент DHCP через WAN-порт и, следовательно, поля **IP Address** и **Gateway IP Address** являются недоступными (N/A), так как эти параметры для устройства P660HN назначает сервер DHCP.

4.5.5 Постоянное соединение (PPP)

Постоянное соединение – это коммутируемая линия с постоянно установленным соединением независимо от необходимости передачи трафика. Устройство P660HN выполняет при постоянном соединении два действия. Первое заключается в том, что оно отключает функцию времени простоя. Второе заключается в том, что устройство P660HN пытается восстановить соединение при включении питания, а также при разрыве соединения. Постоянное соединение может быть очень дорогостоящим по очевидным причинам.

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.

4.5.6 NAT

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

4.6 Метрика

Метрика определяет «стоимость передачи». 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, определяющее стоимость, должно лежать в интервале от «1» до «15»; значение больше «15» означает, что канал не работает. Чем меньше число, тем ниже «стоимость».

Метрика устанавливает приоритет для маршрутов трафика устройства P660HN в Интернете. Если два маршрута по умолчанию имеют одинаковую метрику, устройство P660HN использует следующие заданные приоритеты:

- Стандартный маршрут: назначается Интернет-провайдером (см. Разд. 4.2 на с. 50)
- Маршрут перенаправления трафика (см. Разд. 4.8 на с. 69)

Например, если стандартный маршрут имеет метрику «1», а маршрут перенаправления трафика имеет метрику «2», то стандартный маршрут используется как основной маршрут по умолчанию. Если по стандартному маршруту не удается подключиться к Интернету, устройство P660HN пытается использовать маршрут перенаправления трафика.

4.7 Формирование трафика

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

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 линии. Размер 1 ячейки ATM – 53 байта (424 бита), таким образом максимальная скорость передачи данных в 832 кбит/с дает максимальную скорость PCR 1962 ячеек/с. Однако эта скорость не гарантирована, потому что она зависит от скорости линии.

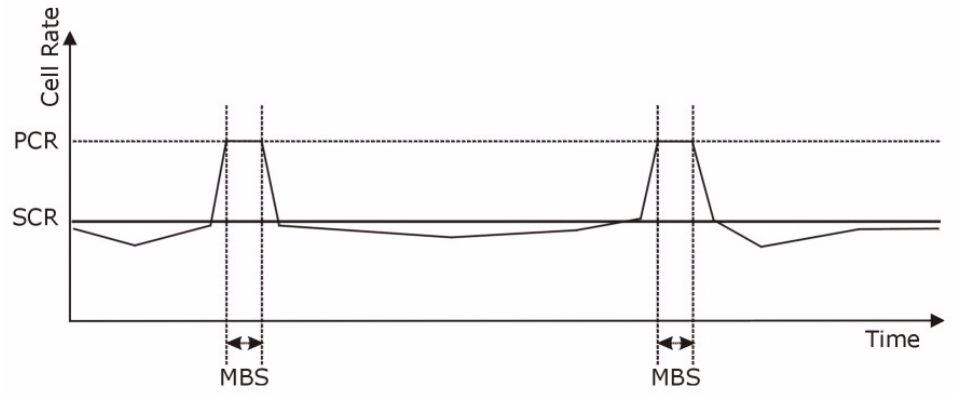
SCR (Sustained Cell Rate – Поддерживаемая скорость ячеек) – это средняя скорость ячеек каждого источника пульсирующего трафика. Она определяет максимальную среднюю скорость, с которой ячейки могут передаваться по виртуальному соединению. Поддерживаемая скорость ячеек не может быть больше, чем скорость 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 установлено по умолчанию на «0», то система будет назначать максимальное значение, определяемое скоростью передачи данных на линии.

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

Рис. 18 Пример формирования трафика



4.7.1 Классы трафика ATM

Существуют основные классы трафика ATM, определяемые в ATM Traffic Management 4.0 Specification (Спецификация ATM по управлению трафиком, версия 4.0).

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.

Переменная скорость передачи (VBR)

Тип трафика 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.

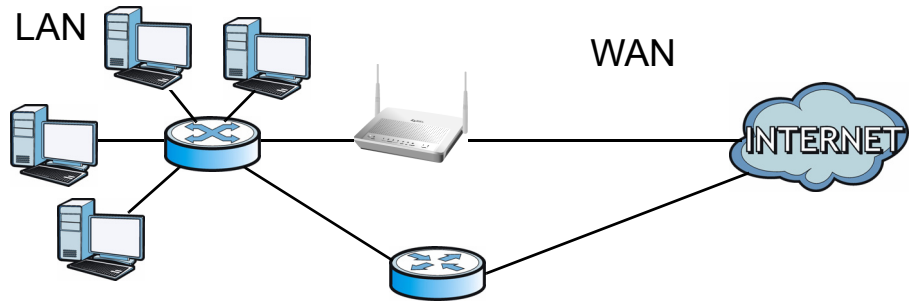
Неопределенная скорость передачи (UBR)

Тип трафика UBR ATM (Unspecified Bit Rate – Неопределенная скорость передачи) используется для пульсирующего трафика 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.

4.8 Перенаправление трафика

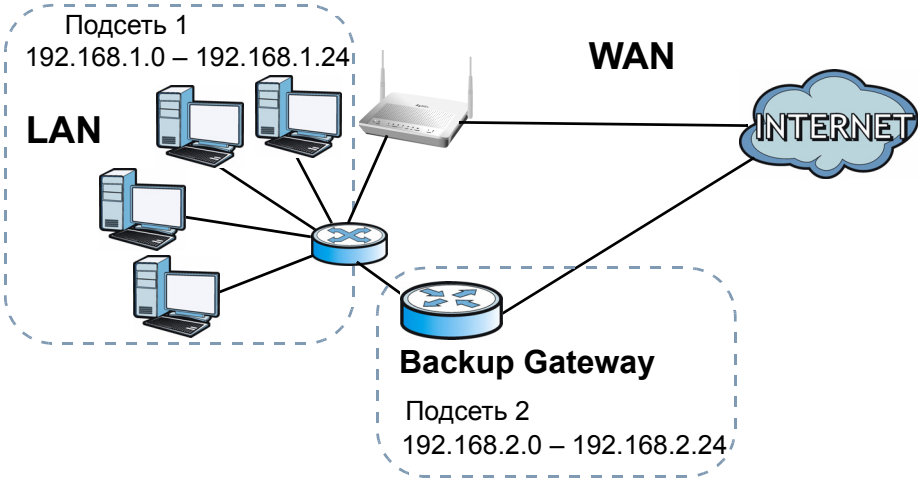
При перенаправлении трафик пересылается на резервный шлюз, если устройство P660HN не может установить соединение с Интернетом. Пример показан на следующем рисунке.

Рис. 19 Пример перенаправления трафика



Топология сети, описанная 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 устройство P660HN 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. 20 Настройка локальной сети для перенаправления трафика



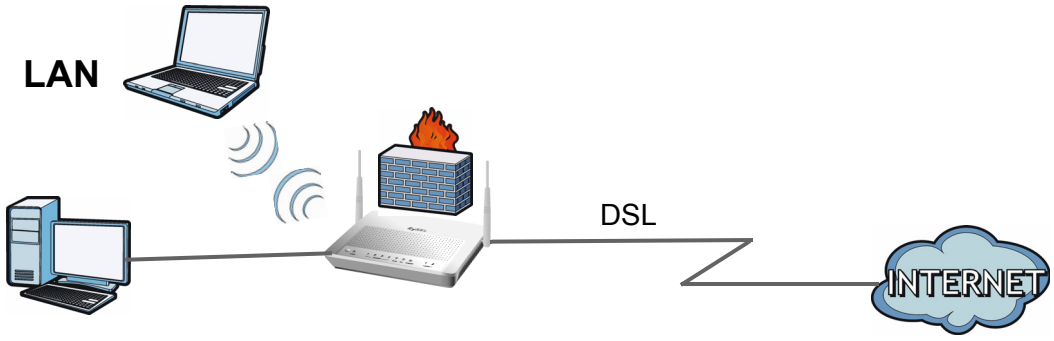
5

Настройка локальной сети (LAN)

5.1 Обзор

LAN (Local Area Network – Локальная сеть) – это коллективно используемая система связи, к которой подключено множество компьютеров. Она обычно размещается на одном участке, например, в здании или на одном этаже здания.

Экраны LAN используются для помощи в настройке сервера DHCP локальной сети и для управления IP-адресами.



5.1.1 Что можно сделать на экранах LAN

- Экран **LAN IP** (Разд. 5.2 на с. 73) используется для установки IP-адреса LAN и маски подсети вашего устройства ZyXEL. С помощью этого экрана можно также редактировать настройки устройства P660HN RIP (Протокол обмена информацией о маршрутизации), многоадресной рассылки, функции Any IP и сетевых настроек Windows.
- Экран **DHCP Setup** (Разд. 5.3 на с. 76) используется для настройки параметров DHCP устройства ZyXEL.
- На экране **Client List** (Разд. 5.4 на с. 77) можно назначать IP-адреса отдельным компьютерам локальной сети на основе их MAC-адресов.
- Экран **IP Alias** (Разд. 5.5 на с. 79) используется для изменения настроек псевдонима IP устройства P660HN.

5.1.2 Что нужно знать о локальной сети

IP-адрес

IP-адрес определяет конкретное устройство в сети. Каждому сетевому устройству (включая компьютеры, серверы, маршрутизаторы, принтеры и т. д.) для обмена информацией по сети требуется IP-адрес. Такие сетевые устройства также называют узлами.

Маска подсети

Маска подсети определяет максимальное количество узлов в сети. Также маски подсети используются для разделения сети на несколько подсетей.

DHCP

При включении сервер DHCP (протокол динамической конфигурации узла) присваивает подключенным в локальную сеть устройствам IP-адрес, маску подсети, DNS и другую информацию о маршрутизации.

RIP

RIP (Routing Information Protocol – Протокол обмена информацией о маршрутизации) позволяет маршрутизатору обмениваться информацией о маршрутизации с другими маршрутизаторами.

Многоадресная рассылка

Обычно передача IP-пакетов происходит одним из двух способов – одноадресная рассылка (1 отправитель – 1 получатель) или широковещательная рассылка (1 отправитель – все компьютеры в сети). При многоадресной рассылке IP-пакеты пересылаются конкретной группе компьютеров в сети, то есть, не одному компьютеру, но и не всем.

IGMP

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. Существуют три версии IGMP. IGMP версии 2 – усовершенствованный вариант версии 1, но IGMP версии 1 по-прежнему широко используется. IGMP версии 3 поддерживает фильтрование источника, игнорирование трафика или отчет о трафике с конкретного адрес источника на конкретный узел сети.

DNS

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

Дополнительные сведения

Техническую вводную информацию о LAN см. в Разд. 5.6 на с. 81.

5.1.3 Перед началом

Для добавления сетевых устройств в список клиентов DHCP необходимо знать их MAC-адреса (Управление доступом к среде).

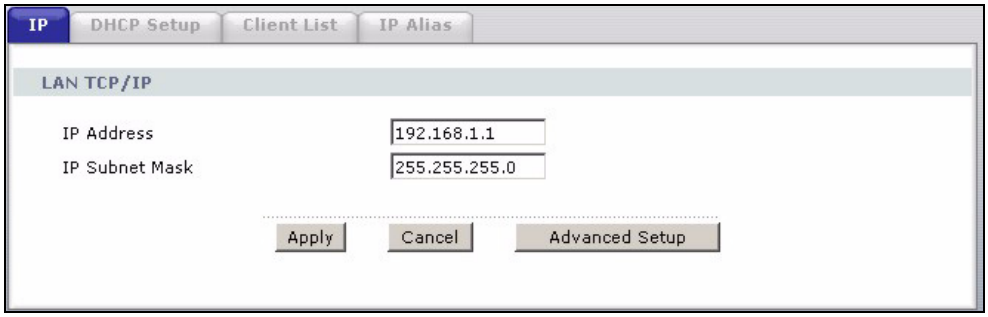
5.2 Экран LAN IP

Этот экран используется для настройки IP-адреса и маски подсети локальной вычислительной сети устройства P660HN. Нажмите **Network > LAN**, чтобы открыть экран **IP**.

Выполните приведенные ниже операции для настройки параметров LAN.

1. Введите IP-адрес в поле **IP Address**. IP-адрес указывается в десятичном виде с разделительными точками. Он станет IP-адресом вашего устройства P660HN.
2. Введите маску IP-подсети в поле **IP Subnet Mask**. Если особо не оговаривается, то лучше всего оставить, как есть: конфигуратор автоматически рассчитает маску подсети на базе введенного вами IP-адреса.
3. Нажмите **Apply** для сохранения изменений.

Рис. 21 Network > LAN > IP



В следующей таблице даны описания полей этого экрана.

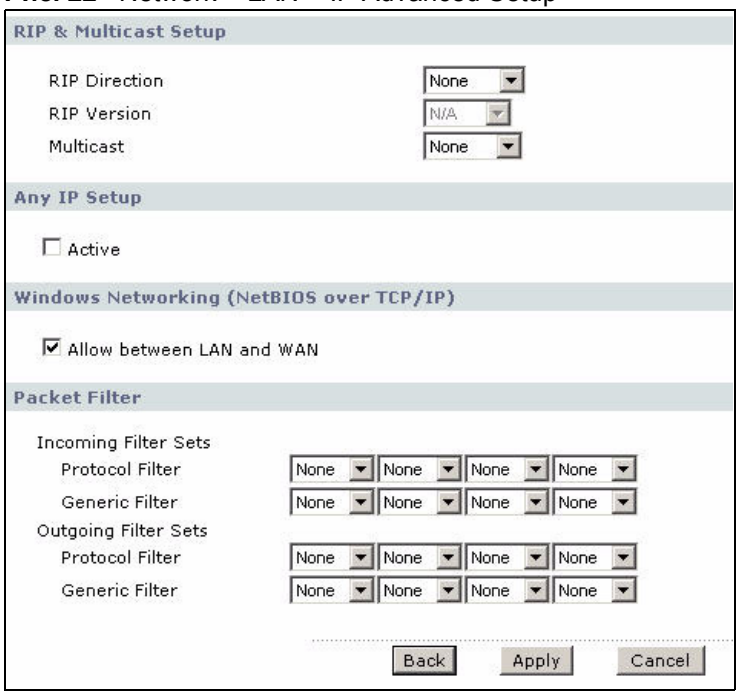
Табл. 14 Network > LAN > IP

ПОЛЕ	ОПИСАНИЕ
IP-адрес	Введите IP-адрес LAN, который вы хотите присвоить устройству P660HN в десятичном виде с разделительными точками, например, 192.168.1.1 (установленный изготовителем по умолчанию).
Маска IP подсети	Введите маску подсети вашей сети в десятичном виде с разделительными точками, например, 255.255.255.0 (установлена изготовителем по умолчанию). Ваше устройство P660HN автоматически подсчитает маску подсети на основании введенного вами IP-адреса, поэтому не следует вносить изменения в это поле, если для этого нет особых указаний.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.
Advanced Setup	Нажмите эту кнопку для отображения экрана **Advanced LAN Setup** и установите дополнительные настройки локальной сети.

5.2.1 Экран дополнительных настроек IP локальной сети

Этот экран используется для редактирования параметров устройства P660HN RIP, многоадресной рассылки, функции Any IP и сетевых настроек Windows. Нажмите **Advanced Setup** на экране **LAN IP**. При этом откроется показанный ниже экран.

Рис. 22 Network > LAN > IP Advanced Setup



В следующей таблице даны описания полей этого экрана.

Табл. 15 Network > LAN > IP Advanced Setup

ПОЛЕ	ОПИСАНИЕ
RIP & Multicast Setup	
RIP Direction	Выберите направление RIP среди вариантов **None**, **Both**, **In Only** и **Out Only**.
RIP Version	Выберите версию RIP среди вариантов **RIP-1**, **RIP-2B** и **RIP-2M**.
Multicast	IGMP (Internet Group Multicast Protocol – Протокол многоадресной рассылки) – это протокол сетевого уровня, используемый для установления принадлежности к группе многоадресной рассылки. Устройство P660HN поддерживает **IGMP v1**, **IGMP v2** и **IGMP v3**. Выберите **None** для отключения IGMP.

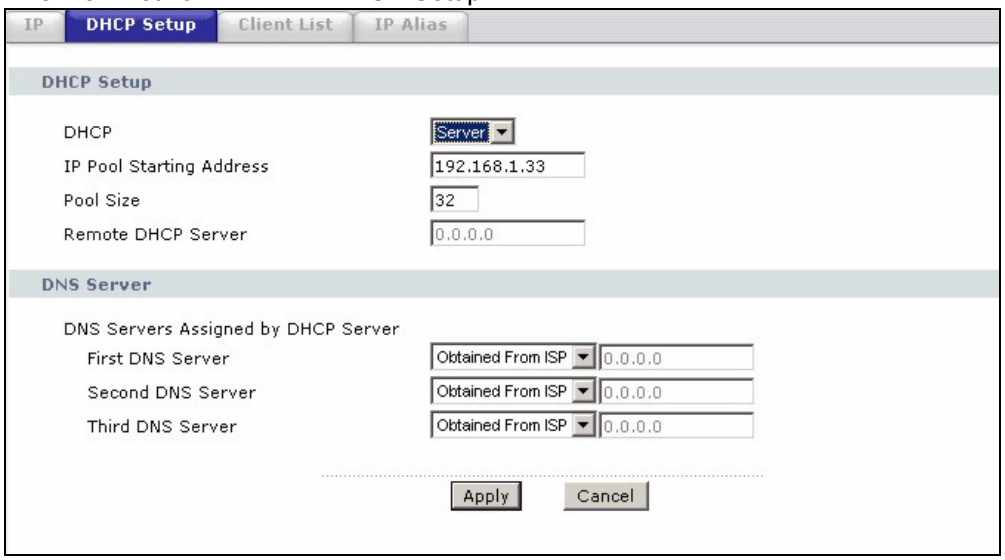
Табл. 15 Network > LAN > IP Advanced Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
Any IP Setup	Поставьте флажок в поле **Active** для включения функции Any IP. Функция Any IP позволяет компьютеру получить доступ в Интернет через устройство P660HN без изменения сетевых настроек (таких как IP-адрес и маска подсети), даже если IP-адреса компьютера и устройства P660HN находятся в разных подсетях. При отключении функции Any IP только компьютеры с динамическими или статическими IP-адресами, принадлежащими той же подсети, что и IP-адрес устройства P660HN в локальной сети, смогут подключиться к устройству P660HN или получить доступ в Интернет через устройство P660HN. Примечание: Чтобы использовать функцию Any IP на устройстве P660HN, необходимо включить функцию NAT/SUA на экране **NAT**.
Windows Networking (NetBIOS over 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	Поставьте в этом поле флажок, чтобы разрешить передачу пакетов NetBIOS из локальной сети в глобальную сеть и наоборот. Если в брандмауэре установлена политика по умолчанию, которая блокирует трафик из глобальной сети в локальную сеть, необходимо включить правило брандмауэра, 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.
Packet Filter	
Incoming Filter Sets	
Protocol Filter	Выберите фильтр (фильтры) протокола для контроля входящего трафика. Можно выбрать до 4 наборов фильтров. Настроить параметры пакетных фильтров можно на экране **Packet Filter**. Более подробную информацию см. в Гл. 10 на с. 164.
Generic Filter	Выберите фильтр (фильтры) общего типа для контроля входящего трафика. Можно выбрать до 4 наборов фильтров. Настроить параметры общих фильтров можно на экране **Packet Filter**. Более подробную информацию см. в Гл. 10 на с. 164.
Outgoing Filter Sets	
Protocol Filter	Выберите фильтр (фильтры) протокола для контроля исходящего трафика. Можно выбрать до 4 наборов фильтров. Настроить параметры фильтров протоколов можно на экране **Packet Filter**. Более подробную информацию см. в Гл. 10 на с. 164.
Generic Filter	Выберите фильтр (фильтры) общего типа для контроля исходящего трафика. Можно выбрать до 4 наборов фильтров. Настроить параметры общих фильтров можно на экране **Packet Filter**. Более подробную информацию см. в Гл. 10 на с. 164.
Back	Нажмите эту кнопку для возврата к предыдущему экрану без сохранения.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

5.3 Экран настройки DHCP

На этом экране устанавливаются параметры сервера DNS, которые устройство P660HN посылает клиентам DHCP в локальной сети. Нажмите **Network > DHCP Setup** для отображения следующего экрана.

Рис. 23 Network > LAN > DHCP Setup



В следующей таблице даны описания полей этого экрана.

Табл. 16 Network > LAN > DHCP Setup

ПОЛЕ	ОПИСАНИЕ
DHCP Setup	
DHCP	Если в данном поле установлено значение **Server**, то устройство P660HN 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**, функция сервера DHCP отключена. Если установлено значение **Relay**, то устройство P660HN 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**. Если функция DHCP включена, необходимо установить следующие параметры:
IP Pool Starting Address	В этом поле вводится первый адрес из непрерывного диапазона IP-адресов.
Pool Size	В этом поле задается размер пула непрерывных IP-адресов.
Remote DHCP Server	Если в поле **DHCP** выбрано значение **Relay**, следует ввести IP-адрес фактического удаленного сервера DHCP.
DNS Server	
DNS Servers Assigned by DHCP Server	Устройство P660HN пересылает IP-адрес сервера DNS (Domain Name System – Система доменных имен) клиентам DHCP.

Табл. 16 Network > LAN > DHCP Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
First DNS Server Second DNS Server Third DNS Server	Выберите вариант **Obtained From ISP** если ваш поставщик Интернет-услуг предоставляет динамическую информацию о сервере DNS (а также IP-адрес WAN устройства P660HN). Если вам известен IP-адрес сервера DNS, выберите вариант **User-Defined**. Введите IP-адрес сервера DNS в поле, расположенное справа. Если выбрать вариант **User-Defined**, но не указать IP-адрес (0.0.0.0), то при нажатии на кнопку **Apply** вариант **User-Defined** сменится на **None**. Если для второго сервера выбрать вариант **User-Defined** и указать точно такой же IP-адрес, то при нажатии на кнопку **Apply** он поменяется на **None**. Выберите **DNS Relay**, чтобы устройство P660HN работало в качестве прокси-сервера DNS, только если Интернет-провайдер использует серверные расширения DNS IPCP. IP-адрес устройства P660HN в локальной сети отображается в поле справа (только для чтения). В этом случае устройство P660HN сообщает клиентам DHCP в локальной сети, что роль сервера DNS выполняет устройство P660HN. Когда компьютер в локальной сети посылает запрос DNS на устройство P660HN, то устройство P660HN пересылает этот запрос на истинный сервер DNS, определенный с помощью IPCP, и ретранслирует ответ компьютеру, пославшему запрос. Значение **DNS Relay** можно выбрать только для одного из трех серверов; при выборе **DNS Relay** для второго или третьего сервера DNS, значение изменяется на **None** после нажатия кнопки **Apply**. Если вы не хотите настраивать серверы DNS, выберите вариант `None`. Для работы в локальной сети необходим другой сервер DHCP, в противном случае необходимо настраивать адреса DNS-серверов на компьютерах вручную. Если сервер DNS не используется, то для подключения к компьютерам необходимо будет указывать их IP-адреса.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

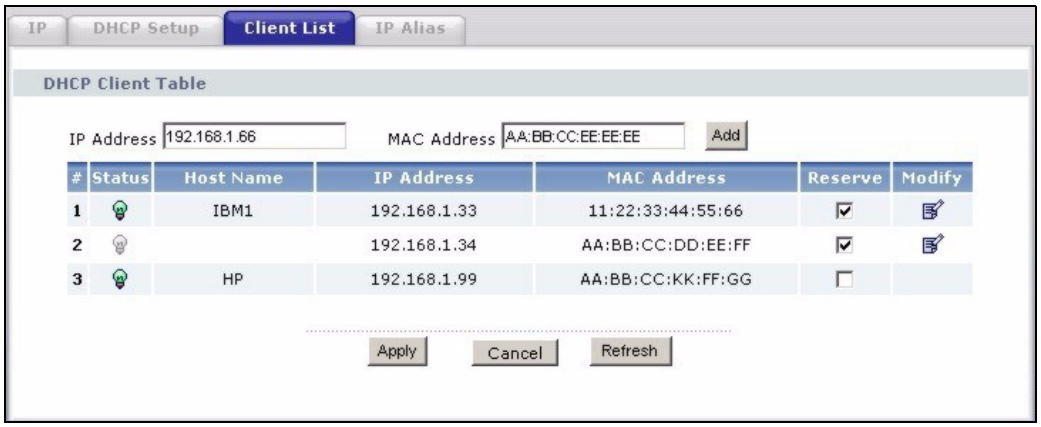
5.4 Экран списка клиентов

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.

Этот экран используется для изменения статических настроек DHCP на устройстве P660HN. Нажмите **Network > LAN > Client List**, чтобы открыть следующий экран.

Рис. 24 Network > LAN > Client List



В следующей таблице даны описания полей этого экрана.

Табл. 17 Network > LAN > Client List

ПОЛЕ	ОПИСАНИЕ
IP Address	Введите IP-адрес, который вы хотите назначить компьютеру в локальной сети, а также его MAC-адрес в соседнее поле.
MAC Address	Введите MAC-адрес компьютера локальной сети.
Add	Нажмите эту кнопку для добавления статической записи DHCP.
#	Порядковый номер записи в таблице статических IP-адресов (строки).
Status	В этом поле отображается, подключен ли данный клиент к устройству P660HN.
Host Name	В этом поле отображается имя компьютера.
IP Address	В этом поле отображается IP-адрес компьютера с номером, указанным выше.
MAC Address	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	Поставьте флажок в поле заголовка для автоматической установки всех флажков для каждой записи, чтобы устройство P660HN всегда назначало выбранный(е) IP-адрес(а) компьютерам с соответствующим(и) MAC-адресом(ами) (и именем узла). В данной таблице можно выбрать до 10 записей.
Modify	Щелкните по иконке для изменения IP-адреса.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.
Refresh	Нажмите эту кнопку для перезагрузки таблицы DHCP.

5.5 Экран псевдонима IP

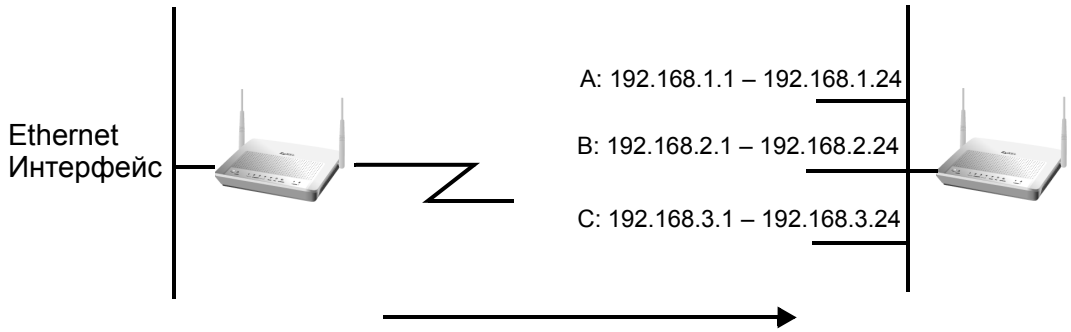
Псевдоним IP позволяет разделить физическую сеть на несколько логических сетей с помощью одного интерфейса Ethernet. Устройство P660HN поддерживает три логических интерфейса локальной сети через один физический интерфейс Ethernet, причем устройство P660HN является шлюзом для каждой локальной сети.

Если используется псевдоним IP, можно также настроить правила брандмауэра 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.

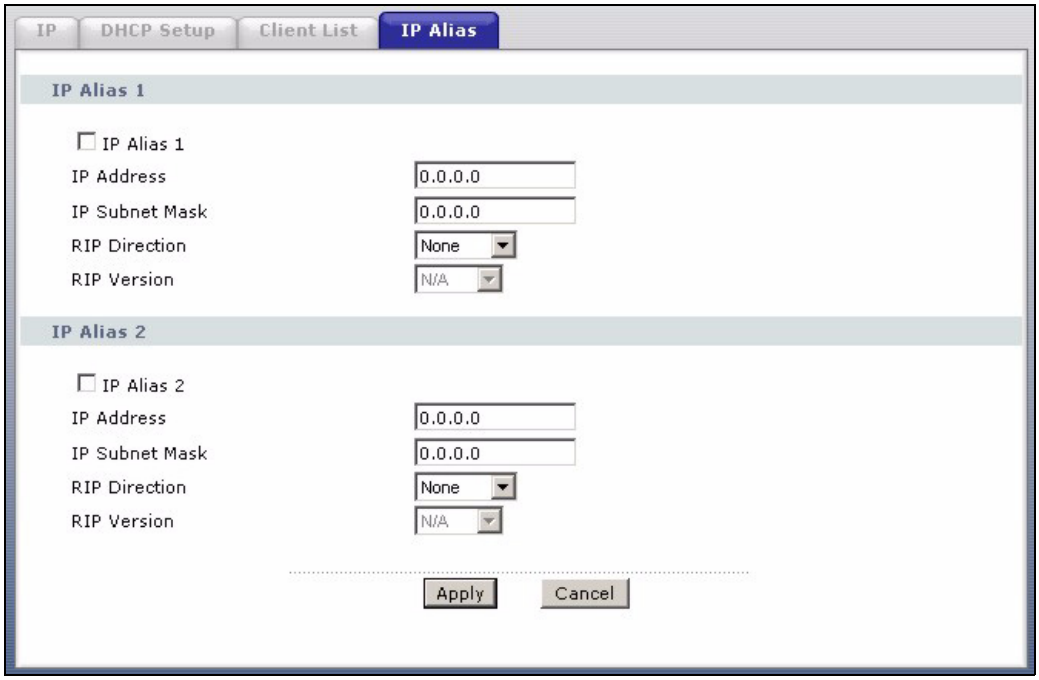
Рис. 25 Физическая сеть и ее разделение на логические сети



5.5.1 Настройка экрана псевдонима IP локальной сети

Этот экран используется для изменения настроек псевдонима IP устройства P660HN. Нажмите **Network** > **LAN** > **IP Alias**, чтобы открыть следующий экран.

Рис. 26 Network > LAN > IP Alias



В следующей таблице даны описания полей этого экрана.

Табл. 18 Network > LAN > IP Alias

ПОЛЕ	ОПИСАНИЕ
IP Alias 1, 2	Поставьте флажок для настройки другой локальной сети в устройстве P660HN.
IP Address	Введите IP-адрес устройства P660HN в десятичном виде с разделительными точками. Или щелкните правой кнопкой мыши для копирования и/или вставки IP-адреса.
IP Subnet Mask	Устройство P660HN вычисляет маску подсети автоматически на основании назначенного IP-адреса. Пока не реализована структура подсетей, следует использовать маску подсети, вычисленную устройством P660HN.
RIP Direction	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** производится управление передачей и приемом пакетов RIP. Выберите направление RIP среди вариантов **Both/In Only/Out Only/None**. Если установлено **Both** или **Out Only**, устройство P660HN будет периодически выполнять широко-вещательную рассылку своей таблицы маршрутизации. Если установлено **Both** или **In Only**, устройство будет объединять свои данные и полученные данные RIP. Если установлено **None**, устройство не посылает пакеты RIP и игнорирует поступающие пакеты RIP.

Табл. 18 Network > LAN > IP Alias (продолжение)

ПОЛЕ	ОПИСАНИЕ
RIP Version	Параметр **RIP Version** управляет форматом и методом широковещательной рассылки пакетов RIP, которые рассылает устройство P660HN (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 передачу данных маршрутизации в формате RIP-2; отличие заключается в том, что **RIP-2B** использует широковещательную рассылку, 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**, а для версии – **RIP-1**.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

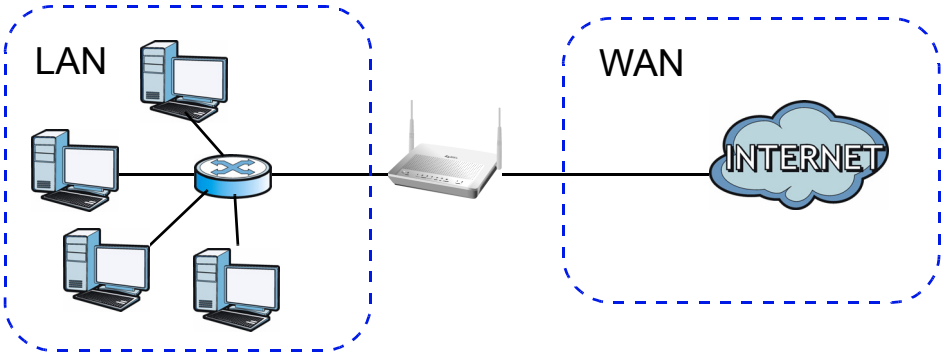
5.6 Техническое руководство LAN

В этом разделе приводится некоторая вводная техническая информация по темам данной главы.

5.6.1 Локальные, глобальные сети и устройство ZyXEL

Фактическое физическое соединение определяет, являются ли порты устройства P660HN портами локальной или глобальной сети. Существуют две отдельные IP-сети: одна внутренняя локальная сеть, другая внешняя глобальная сеть, как показано ниже.

Рис. 27 Локальные и глобальные IP-адреса



5.6.2 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 устройство P660HN как сервер DHCP или отключить эту функцию. При работе в режиме сервера устройство P660HN предоставляет клиентам конфигурацию TCP/IP. Если вы отключаете сервер DHCP, то необходимо иметь в LAN другой сервер DHCP, в противном случае необходимо конфигурировать компьютеры вручную.

Настройка пула IP-адресов

В устройстве P660HN установлен диапазон IP-адресов клиентов DHCP (диапазон DHCP). См. характеристики устройства в приложениях. Не присваивайте компьютерам локальной сети статических IP-адресов из диапазона DHCP.

5.6.3 Адреса сервера DNS

Служба DNS (Domain Name System – Система имен доменов) выполняет преобразование доменного имени в соответствующий 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. Адреса сервера DNS, которые задаются при настройке DHCP, передаются клиентским машинам вместе с назначенным IP-адресом и маской подсети.

Существует два способа распространения адресов серверов DNS Интернет-провайдером.

- 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 Server** на экране **DHCP Setup**.
- Некоторые Интернет-провайдеры предпочитают передавать адреса серверов DNS после подключения с помощью DNS-расширения протокола PPP IPCP (Протокол управления IP). Если Интернет-провайдер не предоставляет адрес серверов DNS в явной форме, значит, они передаются в процессе согласования IPCP. Устройство P660HN поддерживает расширения IPCP сервера DNS посредством функции прокси-сервера DNS.

  Если в полях **DNS Server** на экране **DHCP Setup** установлено значение **DNS Relay**, устройство P660HN сообщает клиентам DHCP, что он сам является сервером DNS. Когда компьютер посылает запрос DNS на устройство P660HN, то устройство P660HN действует как прокси-сервер DNS и пересылает запрос на истинный сервер DNS, определенный с помощью IPCP, а затем ретранслирует ответ назад компьютеру.

  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 на экране **DHCP Setup**.

5.6.4 Настройка TCP/IP локальной сети

Устройство P660HN имеет функцию встроенного сервера DHCP, которая позволяет назначать IP-адреса и серверы DNS компьютерам, поддерживающим клиента DHCP.

IP-адрес и маска подсети

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

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 устройство P660HN функцию трансляции сетевых адресов (NAT). Агентство по назначению имен и уникальных параметров протоколов Интернет (IANA) специально зарезервировало блок адресов для частного использования. Если не предписано иное, не следует использовать адреса за пределами этого диапазона. Если, например, выбрать в качестве сетевого адреса 192.168.1.0, то получится 254 индивидуальных адреса от 192.168.1.1 до 192.168.1.254 (числа ноль и 255 зарезервированы). Другими словами, в этом случае первые три числа задают номер сети, а остальные определяют конкретный компьютер в этой сети.

Выбрав номер сети, выберите для устройства P660HN 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. Устройство P660HN автоматически рассчитывает маску подсети для заданного IP-адреса. Нельзя изменять маску подсети, вычисленную устройством P660HN, без прямых указаний к этому.

IP-адреса для частных сетей

Каждый компьютер в сети Интернет должен иметь уникальный адрес. Если сеть изолирована от Интернет, например, только внутри двух сетей филиала, можно без проблем назначать любые IP-адреса хост-машинам. 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 рекомендуется назначать произвольные IP-адреса; необходимо следовать приведенным выше указаниям. Для получения более подробной информации по назначению адресов см. RFC 1597, «Address Allocation for Private Internets» и RFC 1466, «Guidelines for Management of IP Address Space».

5.6.5 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** производится управление передачей и приемом пакетов RIP. Если установлено:

- **Both –** устройство P660HN осуществляет периодическую широковещательную рассылку своей маршрутной таблицы и полученных данных RIP.
- **In Only –** устройство P660HN не посылает пакеты RIP, но принимает все входящие пакеты RIP.
- **Out Only –** устройство P660HN посылает пакеты RIP, но не принимает входящие пакеты RIP.
- **None –** устройство P660HN не посылает пакеты RIP и игнорирует все входящие пакеты RIP.

Поле **Version** управляет форматом и методом широковещательной рассылки пакетов RIP, которые рассылает устройство P660HN (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 передачу данных маршрутизации в формате RIP-2; отличие заключается в том, что RIP-2B использует широковещательную рассылку, а RIP-2M – многоадресную рассылку.

5.6.6 Многоадресная рассылка

Обычно передача IP-пакетов происходит одним из двух способов – одноадресная рассылка (1 отправитель – 1 получатель) или широковещательная рассылка (1 отправитель – все компьютеры в 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. IGMP версии 3 поддерживает фильтрование источника, игнорирование трафика или отчет о трафике с конкретного адрес источника на конкретный узел сети. Для получения более подробной информации о взаимодействии между IGMP версии 2 и версии 1 см. разделы 4 и 5 RFC 2236. IP-адрес класса D используется для идентификации групп хост-машин и может находиться 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 IP хост-машины (включая шлюзы). Для участия в IGMP хост-машина должна принадлежать к группе 224.0.0.1. Адрес 224.0.0.2 назначается группе маршрутизаторов, участвующих в многоадресной рассылке.

Устройство P660HN поддерживает IGMP версии 1 (**IGMP-v1**), IGMP версии 2 (**IGMP-v2**) и IGMP версии 3 (**IGMP-v3**). При запуске устройства P660HN запрашивает все непосредственно подключенные сети о принадлежности к группе. После получения информации устройство P660HN периодически обновляет ее. В устройстве P660HN многоадресную рассылку IP можно включить/отключить на интерфейсах LAN и/или WAN с помощью Web-конфигуратора (**LAN**;**WAN**). Для отключения многоадресной рассылки для этих интерфейсов выберите **None**.

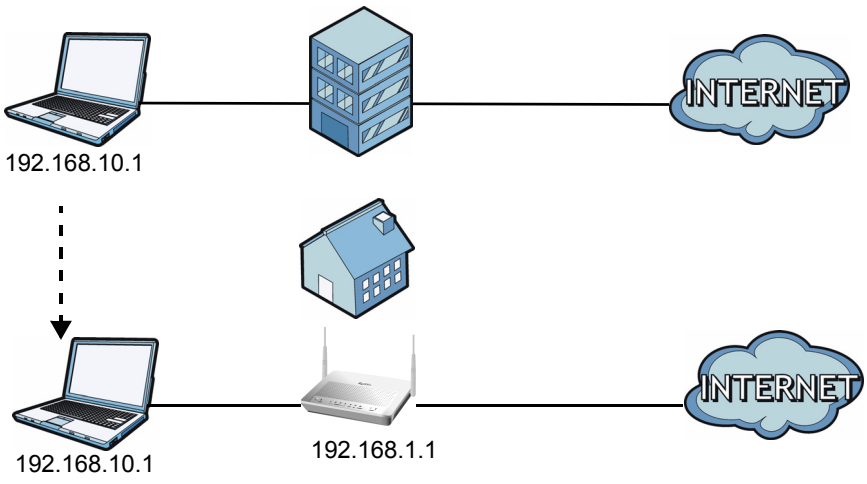
5.6.7 Функция Any IP

Чтобы предоставить компьютеру доступ в Интернет через устройство P660HN, необходимо, чтобы IP-адреса и маски подсети компьютера и устройство P660HN находились в одной и той же подсети. В случае, если компьютеру необходимо использовать статический IP-адрес, принадлежащий другой сети, вам необходимо устанавливать сетевые настройки компьютера вручную каждый раз, когда нужно получить доступ в Интернет через устройство P660HN.

Если в устройстве P660HN 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 устройства P660HN находятся в разных подсетях. Независимо от того, динамический или статический IP-адрес назначен компьютеру, вы можете просто подключить компьютер к устройству P660HN для получения доступа в Интернет.

На следующем рисунке представлен сценарий, где компьютеру назначен статический частный IP-адрес в корпоративной сети. При установке устройства P660HN в жилом доме можно получить доступ в Интернет без изменения сетевых настроек компьютера, даже если IP-адреса компьютера и устройства P660HN находятся в разных подсетях.

Рис. 28 Пример Any IP



Функция Any IP не применяется к компьютерам с динамическим или статическим IP-адресом, принадлежащим к той же подсети, что и IP-адрес устройства P660HN.

Для использования в устройстве P660HN функции Any IP необходимо включить NAT/SUA.

Как работает функция Any 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 (устройства P660HN) определяет следующий транзитный пункт, который необходимо использовать для пересылки данных конкретному адресату.

Когда компьютер пытается в первый раз получить доступ в Интернет через устройство P660HN, 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 устройство P660HN) 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. Устройство P660HN 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 устройство P660HN.
5. При получении пакетов от компьютера устройство P660HN 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 устройству P660HN и в Интернет, как будто он находится в той же подсети, что и устройство P660HN.

6

Беспроводная локальная сеть (WLAN)

6.1 Обзор

В этой главе описывается установка и оптимальная настройка беспроводной сети, включая следующее:

- Включение или выключение беспроводного соединения.
- Задание имени сети, беспроводного канала и параметров безопасности.
- Использование настройки безопасности WiFi (WPS) для конфигурирования вашей беспроводной сети.
- Организация нескольких беспроводных сетей.
- Настройка функции QoS для оптимизации работы вашей сети.
- Использование фильтра MAC-адресов (Media Access Control – Управление доступом к среде) для ограничения доступа к беспроводной сети.
- Установка беспроводной системы распределения (WDS).
- Выполнение других беспроводных заданий, относящихся к работе сети.

6.1.1 Что можно сделать на экранах LAN

Данный раздел описывает экраны устройства P660HN **Network > Wireless LAN**. Эти экраны используются для настройки беспроводного соединения устройства P660HN.

- Экран **AP** (см. Разд. 6.2 на с. 90) используется для включения или выключения беспроводного соединения, настройки безопасности беспроводной сети, конфигурирования фильтра MAC-адресов, и выполнения других основных настроек.
- Экран **More AP** (см. Разд. 6.3 на с. 100) используется для установки на вашем устройстве P660HN нескольких беспроводных сетей.
- Экран **WPS** (см. Разд. 6.4 на с. 102) используется для включения и выключения WPS, генерирования безопасного PIN (Personal Identification Number – персональный идентификационный номер) и просмотра информации о статусе WPS устройства P660HN.
- Экран **WPS Station** (см. Разд. 6.5 на с. 103) используется для установки WPS путем нажатия кнопки или использования PIN.
- Экран **WDS** (см. Разд. 6.6 на с. 103) используется для настройки беспроводной системы распределения (WDS), в которой устройство P660HN функционирует в качестве моста к другим точкам доступа ZyXEL.

- Экран **QoS** (см. Разд. 6.7 на с. 105) используется для включения и выключения Качества услуги (QoS).
- Экран **Scheduling** (см. Разд. 6.8 на с. 106) используется для конфигурирования даты/времени включения или выключения беспроводной LAN.

Для установки беспроводного соединения вам необязательно использовать все эти экраны. Например, вам может понадобиться настроить только имя сети, беспроводной радиоканал и параметры безопасности на экране **AP**.

6.1.2 Что нужно знать о беспроводной связи

Основная информация о беспроводной связи

«Беспроводная связь» фактически является радиосвязью. Беспроводные сетевые устройства обмениваются информацией друг с другом аналогично тому, как переносные рации отправляют и получают информацию с помощью воздушных радиоканалов. Беспроводное сетевое устройство подобно радио, которое позволяет вашему компьютеру обмениваться информацией с такими же радио, подключенными к другим компьютерам. Как и переносные рации, большинство устройств, подключенных к беспроводным сетям, работают в радиочастотных диапазонах, открытых для общего доступа и не требующих лицензии для использования. Однако беспроводные сети отличаются от традиционной радиосвязи тем, что имеют большое количество доступных стандартов беспроводных сетей с различными методами шифрования данных.

На территории вашей страны могут действовать ограничения на эксплуатацию беспроводного оборудования Wi-Fi. Ограничения могут касаться используемых частот и мощности передаваемого сигнала, а также требовать обязательной регистрации беспроводного оборудования в органах регулирования.
Перед началом эксплуатации беспроводного оборудования Wi-Fi убедитесь, что выбранные вами режимы его использования не противоречат требованиям закона и правилам, действующим в вашей стране.

Идентификатор SSID

У каждой сети должно быть имя, называемое «SSID» (Service Set IDentifier – Идентификатор набора служб). «Набор служб» – это сеть, таким образом, «идентификатор набора служб» – это имя сети. Он помогает идентифицировать вашу беспроводную сеть в случае пересечения зон покрытия нескольких беспроводных сетей.

Фильтр MAC-адресов

Каждое устройство Ethernet имеет уникальный MAC-адрес (Media Access Control – Управление доступом к среде). MAC-адрес состоит из двенадцати шестнадцатеричных символов (0–9, A–F) и обычно представлен в следующем формате: «0A:A0:00:BB:CC:DD».

Фильтр MAC-адресов контролирует доступ к беспроводной сети. MAC-адрес каждого беспроводного клиента можно использовать для разрешения или запрета доступа к беспроводной сети.

Дополнительные сведения

См. Разд. 6.9 на с. 106 для поиска дополнительной технической информации о беспроводных сетях.

6.1.3 Перед началом работы

Перед началом использования этих экранов, задайте себе следующие вопросы. См. Разд. 6.1.2 на с. 88, если какие-либо из встретившихся терминов будут вам незнакомы.

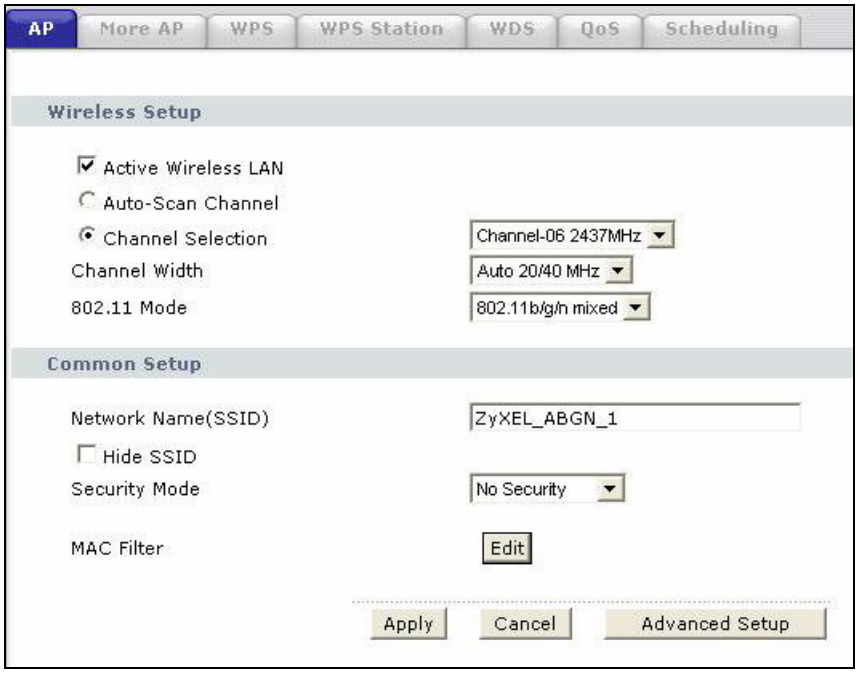
- Какие стандарты беспроводной связи поддерживаются другими беспроводными устройствами в вашей сети (IEEE 802.11g, например)? Какой стандарт наиболее подходит для использования?
- Какие функции безопасности используются другими беспроводными устройствами в вашей сети (WPA-PSK, например)? Какова наиболее сильная функция безопасности, поддерживаемая всеми устройствами в вашей сети?
- Поддерживают ли другие беспроводные устройства в вашей сети функцию WPS (Защищенная настройка Wi-Fi)? Если да, то безопасную сеть можно установить очень легко.

  Даже если некоторые ваши устройства поддерживают WPS, а некоторые не поддерживают, вы можете использовать WPS для настройки вашей сети, а затем добавить не поддерживающие WPS устройства вручную, хотя это несколько более сложно.
- Хотите ли вы настроить дополнительные функции и какие? При настройке дополнительных функций, таких как QoS, убедитесь, что вы точно знаете, что нужно делать. Если вам не нужны дополнительные функции, оставьте настройки как есть.

6.2 Экран AP

Этот экран используется для настройки параметров беспроводной сети устройства P660HN Нажмите **Network > Wireless LAN**, чтобы открыть экран **AP**.

Рис. 29 Network > Wireless LAN > AP



В следующей таблице даны описания полей этого экрана.

Табл. 19 Network > Wireless LAN > AP

ПОЛЕ	ОПИСАНИЕ
Wireless Setup	
Active Wireless LAN	Поставьте в этом поле флажок, чтобы включить беспроводную локальную сеть.
Auto-Scan Channel	Выберите эту опцию для устройства P660HN, чтобы автоматически выбрать канал с наименьшим уровнем помех. Снимите флажок в этом окне, если вы хотите выбрать канал вручную с помощью поля **Channel Section**.
Channel Selection	Настройте рабочую частоту / канал в зависимости от вашего региона. Выберите канал из раскрывающегося списка.
Channel Width	Укажите, канал какой ширины должно использовать устройство P660HN: 20 или 40 МГц. Стандартный канал на 20 МГц обеспечивает скорость передачи до 150 Мбит/с, а канал на 40 МГц использует два стандартных канала и обеспечивает скорость до 300 Мбит/с. Поскольку не все устройства поддерживают канал 40 МГц, выберите **Auto 20/40MHz**, чтобы устройство P660HN могло автоматически выбрать полосу частот канала.

Табл. 19 Network > Wireless LAN > AP (продолжение)

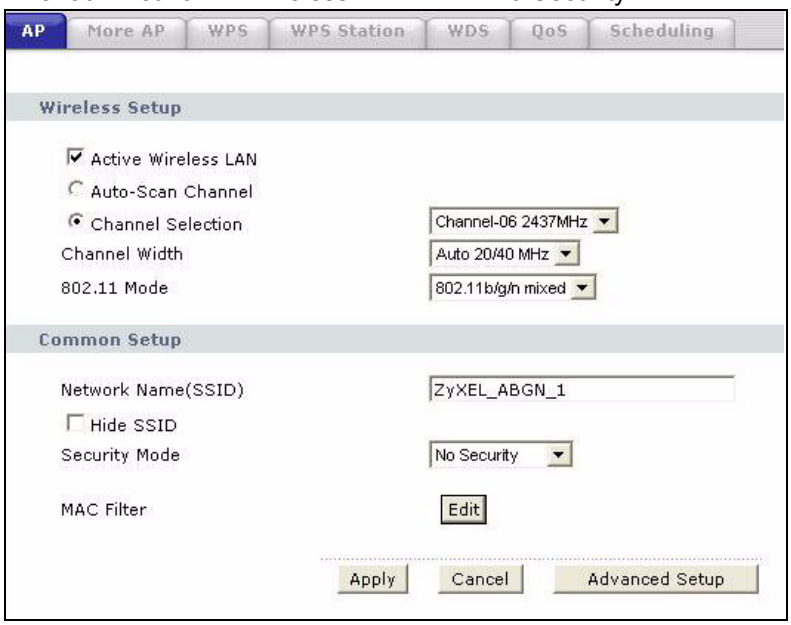
ПОЛЕ	ОПИСАНИЕ
802.11 Mode	Выберите **802.11b**, чтобы разрешить подключение к устройству P660HN только тем беспроводным устройствам, которые совместимы со стандартом IEEE 802.11b. Выберите **802.11g Only**, чтобы разрешить подключение к устройству P660HN только тем беспроводным устройствам, которые совместимы со стандартом IEEE 802.11g. Выберите **802.11n Only**, чтобы разрешить подключение к устройству P660HN только тем беспроводным устройствам, которые совместимы со стандартом IEEE 802.11g. Выберите **802.11g/n mixed**, чтобы разрешить подключение к устройству P660HN беспроводным устройствам, совместимым как со стандартом IEEE 802.11g, так и с IEEE 802.11n. При этом скорость передачи устройства P660HN может снизиться. Выберите **802.11b/g mixed**, чтобы разрешить подключение к устройству P660HN беспроводным устройствам, совместимым как со стандартом IEEE 802.11b, так и с IEEE 802.11g. При этом скорость передачи устройства P660HN может снизиться. Выберите **802.11b/g/n mixed**, чтобы разрешить подключение к P660HN беспроводным устройствам, совместимым как со стандартами IEEE 802.11b, IEEE 802.11g так и с IEEE802.11n. При этом скорость передачи устройства P660HN может снизиться.
Common Setup	
Network Name (SSID)	SSID (Service Set IDentity – Идентификатор набора служб) устанавливает набор служб для беспроводного устройства. Беспроводные устройства, подключенные к одной точке доступа (AP) должны иметь одинаковый SSID. Введите описательное имя для беспроводной локальной сети (не более 32 семиразрядных печатных символов ASCII). Примечание: Если вы настраиваете устройство P660HN с компьютера, подключенного через беспроводную локальную сеть, и при этом изменяете в устройстве P660HN идентификатор SSID или параметры WEP, то при нажатии на кнопку **Apply** беспроводное соединение будет потеряно. В этом случае необходимо изменить беспроводные настройки компьютера для соответствия новым настройкам устройства P660HN.
Hide 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.
Security Mode	Более подробную информацию об этом поле см. в следующих разделах.
MAC Filter	Здесь показано, разрешен или запрещен устройствам с перечисленными в списке MAC-адресами доступ к устройству P660HN с помощью данного SSID.
Edit	Нажмите эту кнопку для перехода к экрану **MAC Filter** для настройки параметров фильтра MAC-адресов.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.
Advanced Setup	Нажмите эту кнопку для отображения экрана **Wireless Advanced Setup** и установите дополнительные настройки беспроводной локальной сети.

6.2.1 Отключение защиты сети

На экране **Network > Wireless LAN > AP** выберите **No Security** из списка **Security Mode**, чтобы разрешить беспроводным устройствам обмениваться информацией с устройством P660HN без шифрования данных или аутентификации.

Если функция обеспечения беспроводной безопасности в устройстве P660HN отключена, ваша сеть будет доступна для любого беспроводного сетевого устройства, которое находится в зоне охвата сети.

Рис. 30 Network > Wireless LAN > AP: No Security



В следующей таблице даны описания полей этого экрана.

Табл. 20 Network > Wireless LAN > AP: Отключение защиты сети

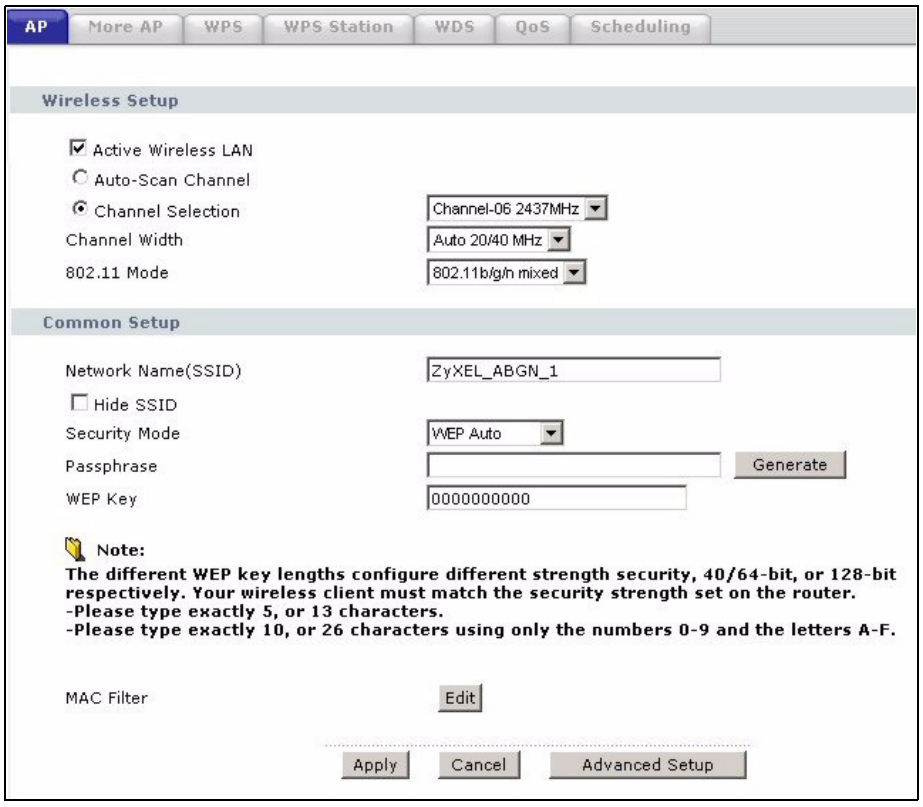
ПОЛЕ	ОПИСАНИЕ
Security Mode	Выберите **No Security** из выпадающего списка.

6.2.2 WEP-шифрование

Этот экран используется для включения и настройки WEP-шифрования. Нажмите **Network > Wireless LAN**, чтобы открыть экран **AP**. Выберите **WEP Auto** из списка **Security Mode**.

WEP-шифрование небезопасно! Этот шифр может быть взломан злоумышленником с помощью широко доступного программного обеспечения. Мы настоятельно рекомендуем вам использовать более эффективный механизм защиты. Используйте самую надежную систему безопасности, которую поддерживают все беспроводные устройства вашей сети. Например, используйте WPA-PSK или WPA2-PSK, если все ваши беспроводные устройства их поддерживают; используйте WPA или WPA2, если ваши беспроводные устройства их поддерживают, и у вас есть сервер RADIUS. Если ваши беспроводные устройства не поддерживают механизмов защиты более надежных, чем WEP, используйте самый высокий доступный уровень шифрования.

Рис. 31 Network > Wireless LAN > AP: WEP Auto



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

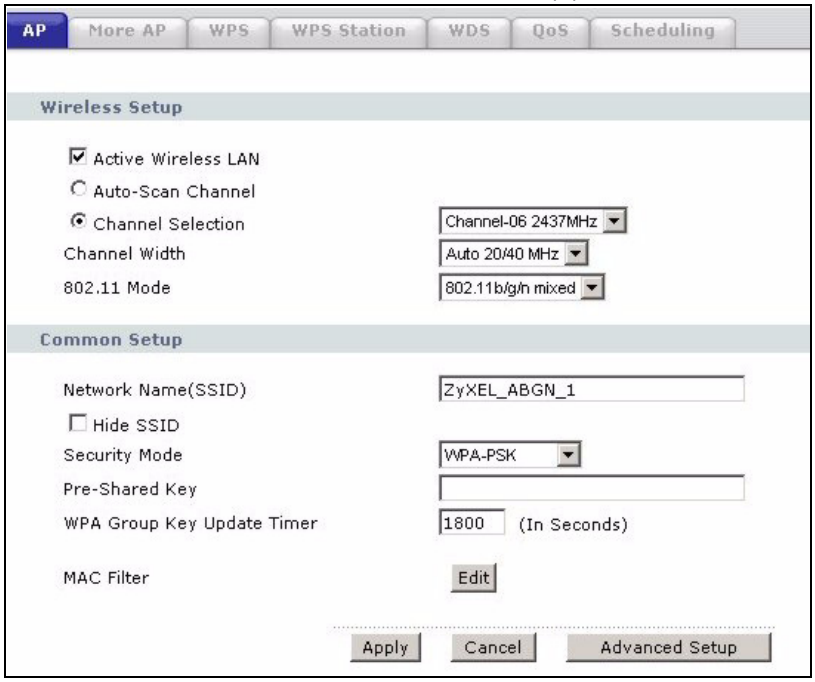
Табл. 21 Network > Wireless LAN > AP: WEP Auto

ПОЛЕ	ОПИСАНИЕ
Security Mode	Из раскрывающегося списка выберите **WEP Auto**.
Passphrase	Введите идентификационную фразу (до 32 знаков) и нажмите **Generate**. Устройство P660HN автоматически сгенерирует ключ WEP.
WEP Key	Ключ WEP используется для шифрования данных. Для обеспечения передачи данных необходимо, чтобы устройство P660HN и все беспроводные станции использовали одинаковый ключ WEP. Если требуется вручную установить ключ WEP, введите любые 5 или 13 символов (формат ASCII) или 10 или 26 шестнадцатеричных символов (0–9, A–F) для генерирования ключа WEP длиной 64 бита или 128 бит соответственно.

6.2.3 WPA(2)-PSK

Этот экран используется для включения и настройки аутентификации WPA(2)-PSK. Нажмите **Network > Wireless LAN**, чтобы открыть экран **AP**. Выберите **WPA-PSK**, **WPA2-PSK** или **WPAPSKMixed** в списке **Security Mode**.

Рис. 32 Network > Wireless LAN > AP: WPA(2)-PSK



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

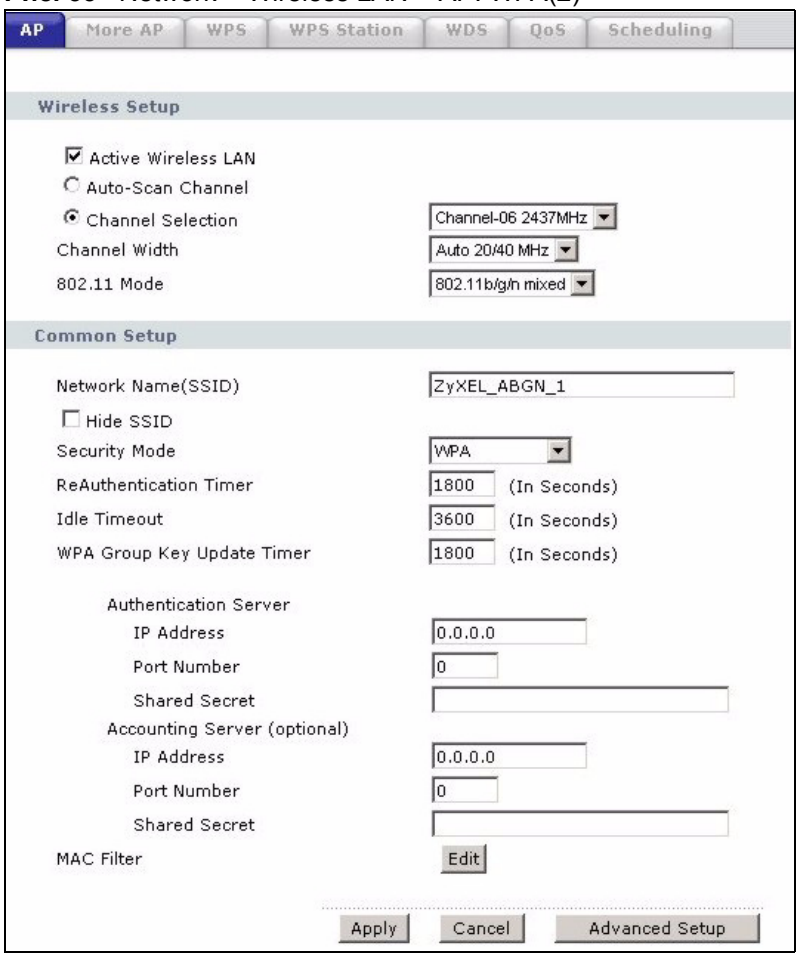
Табл. 22 Network > Wireless LAN > AP: WPA(2)-PSK

ПОЛЕ	ОПИСАНИЕ
Security Mode	Из выпадающего списка выберите **WPA-PSK** или **WPA2-PSK** или **WPAPSK Mixed**. Выберите **WPAPSK Mixed**, чтобы устройство P660HN одновременно поддерживало WPA-PSK и WPA2-PSK.
Pre-Shared Key	Механизмы шифрования, используемые для **WPA(2)** и **WPA(2)-PSK** являются одинаковыми. Разница между ними состоит в том, что **WPA(2)-PSK** использует единственный предварительно согласованный ключ (пароль) для аутентификации всех пользователей, не предполагая наличие индивидуального пароля у каждого пользователя. Введите предварительно согласованный ключ от 8 до 63 символов ASCII с учетом регистра (включая пробелы и знаки).
WPA Group Key Update Timer	**WPA Group Key Update Timer** – это интервал времени, через который точка доступа (если используется управление ключами **WPA(2)-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. Настройка **WPA Group Key Update Timer** также поддерживается в режиме **WPA(2)-PSK**. По умолчанию в устройстве P660HN устанавливается значение в **1800** секунд (30 минут).

6.2.4 Аутентификация WPA(2)

Этот экран используется для включения и настройки аутентификации WPA или WPA2. Нажмите ссылку **Wireless LAN** под **Network**, чтобы открыть экран **AP**. Выберите **WPA**, **WPA2** или **WPAMixed** в списке **Security Mode**.

Рис. 33 Network > Wireless LAN > AP: WPA(2)



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

Табл. 23 Network > Wireless LAN > AP: WPA(2)

ПОЛЕ	ОПИСАНИЕ
Security Mode	Из выпадающего списка выберите **WPA**, **WPA2** или **WPAMixed**. Выберите **WPAMixed**, чтобы устройство P660HN одновременно поддерживало WPA и WPA2.
Reauthentication Timer	Установите интервал времени, через который беспроводные станции должны периодически передавать имя пользователя и пароль для того, чтобы оставаться в сети. Введите период времени в диапазоне от 10 до 9999 секунд. Временной интервал по умолчанию – 1800 секунд (30 минут). Примечание: Если аутентификация беспроводного устройства производится с помощью сервера RADIUS, приоритет имеет таймер повторной аутентификации на сервере RADIUS.

Табл. 23 Network > Wireless LAN > AP: WPA(2) (продолжение)

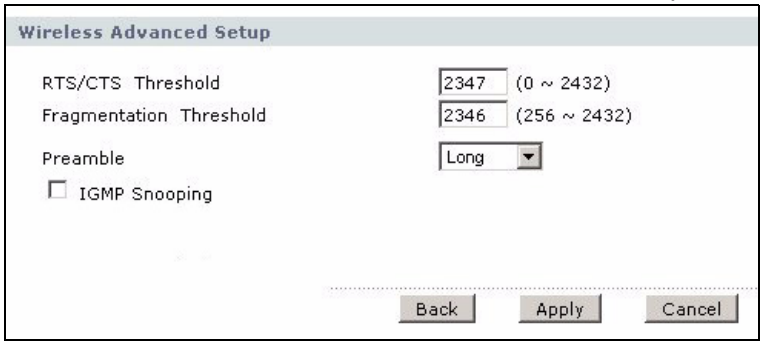
ПОЛЕ	ОПИСАНИЕ
Idle Timeout	По истечении периода простоя устройство P660HN автоматически отключает беспроводное устройство от проводной сети. Для подключения к проводной сети беспроводное устройство должно снова отправить имя пользователя и пароль. По умолчанию устанавливается значение в 3600 секунд (или 1 час).
WPA Group Key Update Timer	**WPA Group Key Update Timer** – это интервал времени, через который точка доступа (если используется управление ключами **WPA(2)-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. Настройка **WPA Group Key Update Timer** также поддерживается в режиме **WPA(2)-PSK**. По умолчанию в устройстве P660HN устанавливается значение в **1800** секунд (30 минут).
Authentication Server	
IP Address	Введите в этом поле IP-адрес внешнего сервера аутентификации в десятичном виде с разделительными точками.
Port Number	Введите номер порта сервера внешней аутентификации. Не изменяйте это значение, если на то нет специальных указаний и информации от сетевого администратора.
Shared Secret	Введите пароль (до 31 буквенно-цифрового символа) для создания ключа, совместно используемого внешним сервером аутентификации и устройством P660HN. Внешний сервер аутентификации и устройство P660HN должны использовать одинаковый ключ. Этот ключ не передается по сети.
Accounting Server (optional)	
IP Address	Введите в этом поле IP-адрес внешнего сервера учета в десятичном виде с разделительными точками.
Port Number	Введите номер порта внешнего сервера учета. Не изменяйте это значение, если на то нет специальных указаний и информации от сетевого администратора.
Shared Secret	Введите пароль (до 31 буквенно-цифрового символа) для создания ключа, совместно используемого внешним сервером учета и устройством P660HN. Внешний сервер учета и устройство P660HN должны использовать одинаковый ключ. Этот ключ не передается по сети.

6.2.5 Дополнительные настройки беспроводной локальной сети

Этот экран используется для настройки дополнительных параметров беспроводной сети. Нажмите кнопку **Advanced Setup** на экране **AP**. При этом откроется показанный ниже экран.

Подробные определения терминов, встречающихся на этом экране, см. в Разд. 6.9.2 на с. 108.

Рис. 34 Network > Wireless LAN > AP: Advanced Setup



В следующей таблице даны описания полей этого экрана.

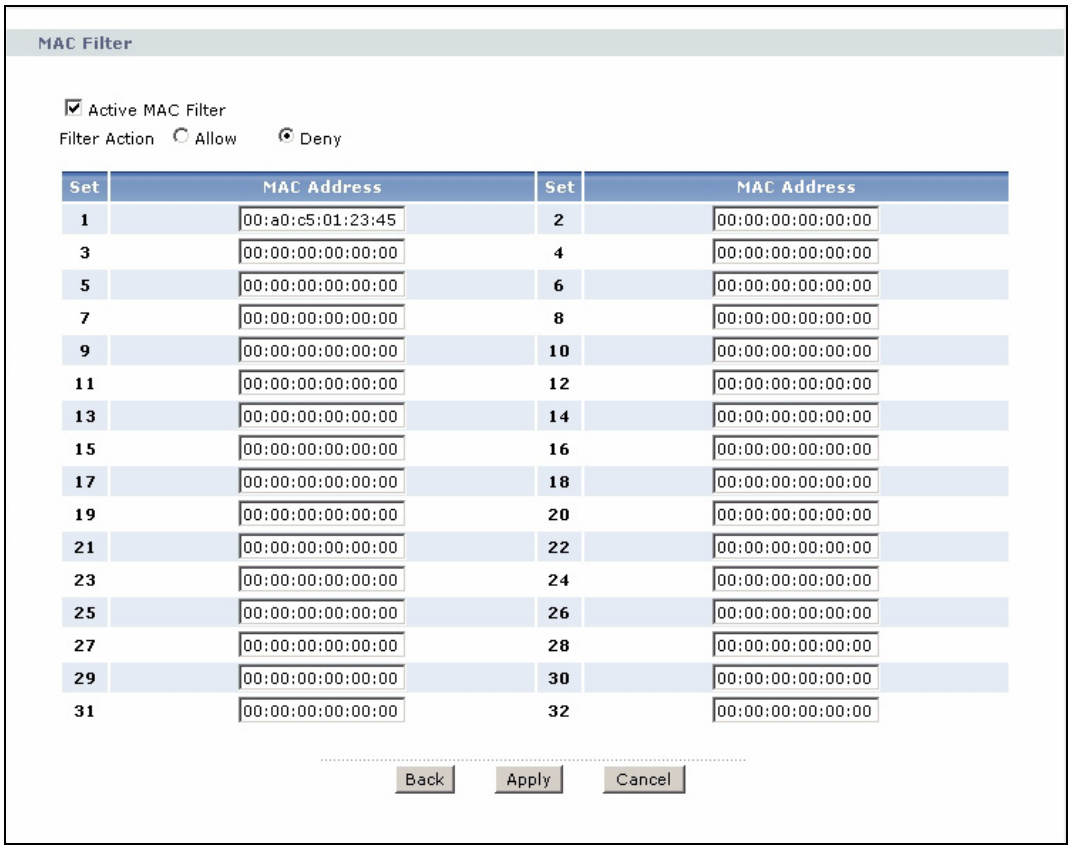
Табл. 24 Network > Wireless LAN > AP: Advanced Setup

ПОЛЕ	ОПИСАНИЕ
RTS/CTS Threshold	Введите значение от 0 до 2432.
Fragmentation Threshold	Это максимальный размер фрагмента данных для передачи. Введите значение от 256 до 2432.
Preamble	Выберите тип заголовка из раскрывающегося списка. Опциями являются: **Long**, **Short** или **Dynamic**. По умолчанию установлено **Long**. Более подробно см. в приложениях.
IGMP Snooping	Этот пункт включает управление многоадресной рассылкой по протоколу IGMP на устройстве P660HN.
Back	Нажмите эту кнопку для возврата к предыдущему экрану без сохранения.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

6.2.6 Фильтр MAC-адресов

Этот экран используется для изменения настроек фильтра MAC-адресов на устройстве P660HN. Нажмите кнопку **Edit** на экране **AP**. При этом откроется показанный ниже экран.

Рис. 35 Network > Wireless LAN > AP: MAC Address Filter



В следующей таблице даны описания полей этого экрана.

Табл. 25 Network > Wireless LAN > AP: MAC Address Filter

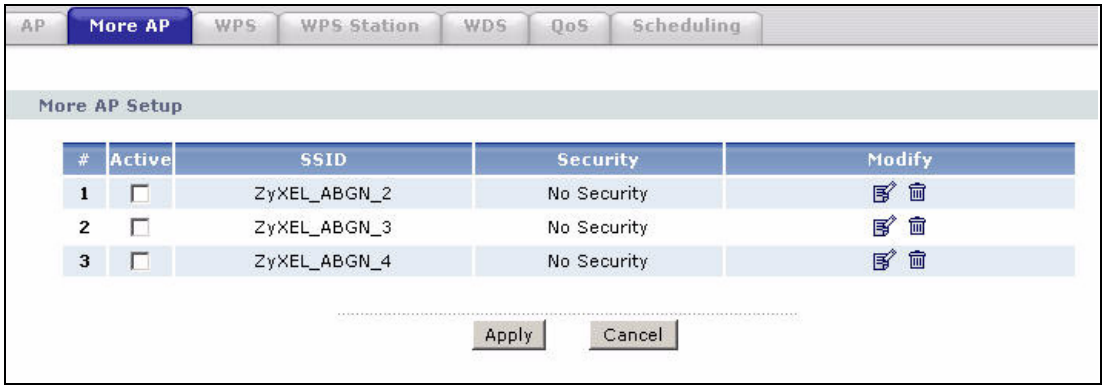
ПОЛЕ	ОПИСАНИЕ
Active MAC Filter	Поставьте в этом поле флажок, чтобы включить фильтрование MAC-адресов.
Filter Action	Определите способ фильтрования для списка MAC-адресов в таблице **MAC Address**. Выберите **Deny** для блокирования доступа к устройству P660HN. MAC-адресам, не указанным в списке, доступ к устройству P660HN будет разрешен. Выберите **Allow** для разрешения доступа к устройству P660HN. MAC-адресам, не указанным в списке, будет отказано в доступе к устройству P660HN.
Set	Это порядковый номер MAC-адреса.
MAC Address	Введите в адресные поля MAC-адреса беспроводных устройств, которым разрешен или запрещен доступ к устройству P660HN. MAC-адреса необходимо вводить в специальном формате MAC-адресов, т. е., шесть пар шестнадцатеричных символов, например, 12:34:56:78:9a:bc.
Back	Нажмите эту кнопку для возврата к предыдущему экрану без сохранения.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

6.3 Экран More AP

Этот экран позволяет включать и настраивать несколько базовых наборов служб (BSS) на устройстве P660HN.

Нажмите **Network > Wireless LAN** > **More AP**. Появится следующий экран.

Рис. 36 Network > Wireless LAN > More AP



В следующей таблице даны описания полей этого экрана.

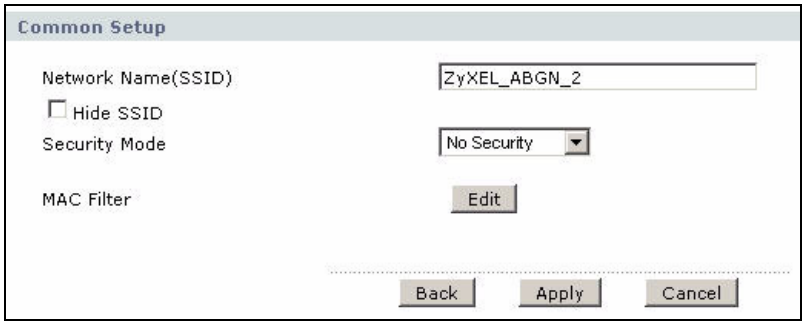
Табл. 26 Network > Wireless LAN > More AP

ПОЛЕ	ОПИСАНИЕ
#	Это порядковый номер каждого профиля SSID.
Active	Поставьте флажок для включения профиля SSID.
SSID	Профиль SSID – это набор параметров, относящихся к одному из BSS устройства P660HN. SSID (Service Set IDentifier – Идентификатор набора служб) устанавливает набор служб для беспроводного устройства. В этом поле отображается имя беспроводного профиля в сети. При поиске беспроводным клиентом точки доступа для подключения это имя транслируется и отображается на утилите беспроводного клиента.
Security	В этом поле отображается режим безопасности профиля SSID.
Modify	Для конфигурирования профиля SSID щелкните по иконке **Edit**. Для удаления профиля SSID щелкните по иконке **Remove**.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

6.3.1 Редактирование More AP

Этот экран используется для редактирования профиля SSID. Щелкните по иконке **Edit** рядом с полями SSID на экране **More AP**. Появится следующий экран.

Рис. 37 Network > Wireless LAN > More AP: Edit



В следующей таблице даны описания полей этого экрана.

Табл. 27 Network > Wireless LAN > More AP: Edit

ПОЛЕ	ОПИСАНИЕ
Network Name (SSID)	SSID (Service Set IDentity – Идентификатор набора служб) устанавливает набор служб для беспроводного устройства. Введите описательное имя для беспроводной локальной сети (не более 32 семиразрядных печатных символов ASCII). Примечание: Если вы настраиваете устройство P660HN с компьютера, подключенного через беспроводную локальную сеть, и при этом изменяете в устройстве P660HN идентификатор SSID или параметры безопасности, то при нажатии на кнопку **Apply** беспроводное соединение будет потеряно. В этом случае необходимо изменить беспроводные настройки компьютера для соответствия новым настройкам устройства P660HN.
Hide 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.
Security Mode	См. Разд. 6.2 на с. 90 для получения дополнительной информации об этом поле.
MAC Filter	Здесь показано, разрешен или запрещен устройствам с перечисленными в списке MAC-адресами доступ к устройству P660HN с помощью данного SSID.
Edit	Нажмите эту кнопку для перехода к экрану **MAC Filter** для настройки параметров фильтра MAC-адресов. Более подробную информацию см. в Разд. 6.2.6 на с. 99.
Back	Нажмите эту кнопку для возврата к предыдущему экрану без сохранения.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

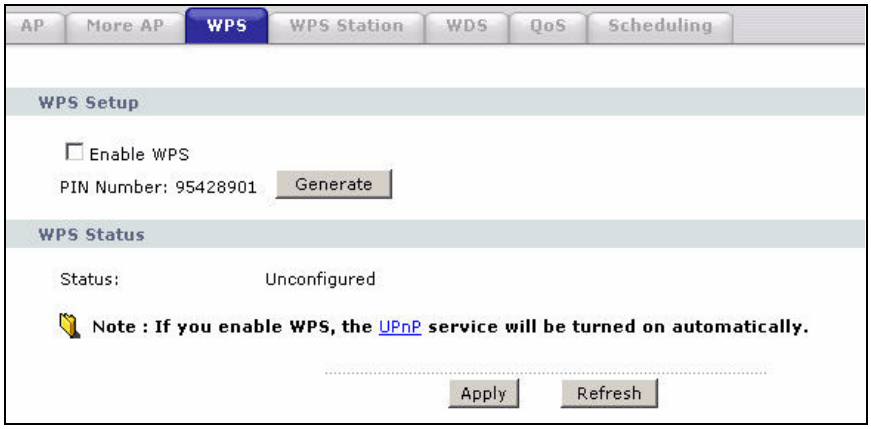
6.4 Экран WPS

Этот экран используется для настройки безопасности WiFi (WPS) на устройстве P660HN.

WPS позволяет быстро настроить беспроводную сеть, обеспечивая надежную защиту без ручной установки параметров защиты. Каждое подключение WPS устанавливается между двумя устройствами. Оба устройства должны поддерживать WPS.

Нажмите **Network > Wireless LAN > WPS**. Появится следующий экран.

Рис. 38 Network > Wireless LAN > WPS



В следующей таблице даны описания полей этого экрана.

Табл. 28 Network > Wireless LAN > WPS

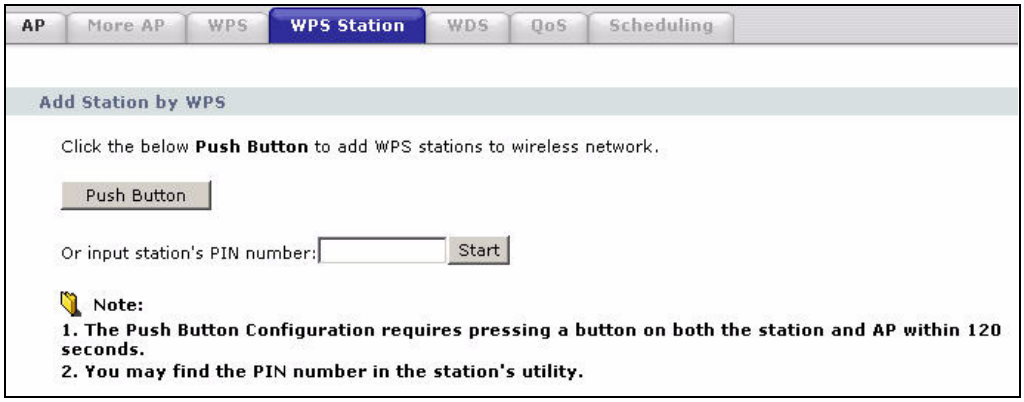
ПОЛЕ	ОПИСАНИЕ
WPS Setup	
Enable WPS	Поставьте флажок, чтобы включить функцию WPS в устройстве P660HN.
PIN Number	Здесь указан PIN (персональный идентификационный номер) устройства P660HN. Введите этот PIN в утилите конфигурации устройства, к которому вы хотите подключиться, используя WPS. Ввод PIN необязателен, если вы используете метод настройки WPS кнопкой.
Generate	Нажмите для создания устройством P660HN нового PIN.
WPS Status	Здесь отображается опция **Configured**, когда устройство P660HN подключается к беспроводной сети с помощью WPS или если выбрана опция **Enable WPS** и изменены настройки беспроводной сети или настройки безопасности беспроводной сети. На экране отображаются также текущие настройки беспроводной сети и настройки безопасности беспроводной сети. Здесь отображается опция **Unconfigured**, если отключена WPS и отсутствуют изменения параметров беспроводной сети и безопасности беспроводной сети в устройстве P660HN или если вы нажимаете **Release_Configuration** для удаления настроек беспроводной сети или безопасности беспроводной сети.
Release_ Configuration	Эта кнопка доступна только в том случае, если для состояния WPS отображается **Configured.** Нажмите эту кнопку для удаления всех измененных настроек беспроводной сети и настроек безопасности беспроводной сети для подключений WPS в устройстве P660HN.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Refresh	Нажмите эту кнопку для восстановления ранее заданных настроек.

6.5 Экран WPS Station

Этот экран используется для настройки беспроводной сети WPS с помощью PBC (Push Button Configuration – Настройка кнопкой) или настройки PIN-кодом.

Нажмите **Network > Wireless LAN > WPS Station**. Появится следующий экран.

Рис. 39 Network > Wireless LAN > WPS Station



В следующей таблице даны описания полей этого экрана.

Табл. 29 Network > Wireless LAN > WPS Station

ПОЛЕ	ОПИСАНИЕ
Push Button	Нажмите для добавления другого беспроводного устройства с функцией WPS (в пределах беспроводного диапазона устройства P660HN) к вашей беспроводной сети. Эта кнопка может фактически находиться на внешней стороне устройства, или же это кнопка меню, подобная кнопке **Push Button** на этом экране. Примечание: В течение двух минут после нажатия этой кнопки необходимо также нажать кнопку WPS другого беспроводного устройства.
Or input station's PIN number	Введите PIN-код устройства, с которым нужно установить WPS-соединение, и нажмите **Start** для аутентификации и добавления этого устройства к вашей беспроводной сети. PIN-код расположен на внешней части устройства или его можно посмотреть в настройках устройства. Примечание: Также необходимо активировать WPS на этом устройстве в течение двух минут, чтобы оно предоставило свой PIN-код устройству P660HN.

6.6 Экран WDS

Точка доступа (AP), использующая WDS (Wireless Distribution System – беспроводная система распределения) может функционировать как беспроводной сетевой мост, позволяя установить беспроводное соединение между двумя сегментами проводной сети. Экран **WDS** используется для настройки устройства P660HN, чтобы установить беспроводное соединение между двумя или несколькими точками доступа при включенной WDS.

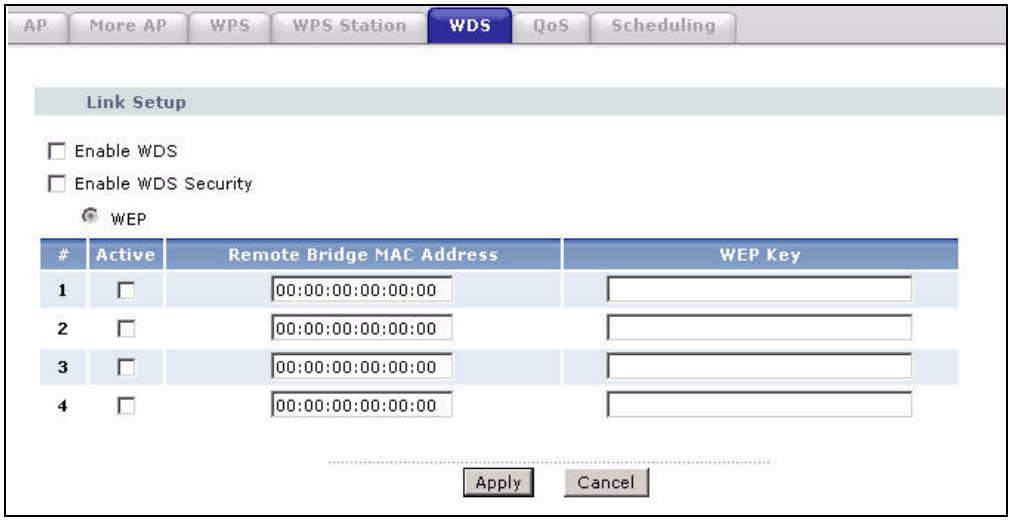
Этот экран используется для установки WDS-соединений между устройством P660HN и другими беспроводными точками доступа. Необходимо знать MAC-адрес клиентского устройства. Если настройки безопасности клиентов совпадают, то выполняется соединение между устройствами.

Безопасность WDS не зависит от настроек безопасности между устройством ZyXEL и любыми беспроводными клиентами.

На момент написания руководства WDS совместима только с другими точками доступа ZyXEL. Не все модели поддерживают соединения WDS. См. руководства к другим точкам доступа.

Нажмите **Network > Wireless LAN > WDS**. Появится следующий экран.

Рис. 40 Network > Wireless LAN > WDS



В следующей таблице даны описания полей этого экрана.

Табл. 30 Network > Wireless LAN > WDS

ПОЛЕ	ОПИСАНИЕ
Enable WDS	Поставьте флажок, чтобы включить функцию WDS в устройстве P660HN.
Enable WDS Security	Выберите эту опцию и тип ключа, используемого для шифрования данных, передаваемых между точками доступа. Все беспроводные точки доступа (включая устройство P660HN) для передачи данных должны использовать один и тот же предварительно согласованный ключ. При отмене выбора этой опции данные, передаваемые между точками доступа, не будут зашифрованы. Любой посторонний сможет их прочитать.
WEP	Поставьте флажок для выбора WEP-шифрования.
#	Это порядковый номер конкретного WDS-соединения.

Табл. 30 Network > Wireless LAN > WDS (продолжение)

ПОЛЕ	ОПИСАНИЕ
Active	Выберите для активации соединения между устройством ZyXEL и клиентским устройством, к которому относится эта запись. Если флажок не установлен, соединение отсутствует.
Remote Bridge MAC Address	Введите MAC-адрес клиентского устройства в специальном формате MAC-адресов (шесть пар шестнадцатеричных символов, например, 12:34:56:78:9a:bc).
WEP Key	Введите любые 5 или 13 символов (формат ASCII) или 10 или 26 шестнадцатеричных символов (0–9, A–F) для установки ключа WEP длиной 64 бита или 128 бит соответственно.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

6.7 Экран QoS

Для улучшения качества передачи речи и видеоприложений по беспроводной сети существует возможность включить QoS (Quality of Service – Качество и класс предоставляемых услуг передачи данных) в беспроводной среде передачи. С QoS голосовым сигналам и видеосигналам назначается высокий приоритет, что позволяет приложениям выполняться более равномерно. Также, назначается низкий приоритет для передачи больших файлов, так как это не снижает качество других приложений.

Нажмите **Network > Wireless LAN > QoS**. Появится следующий экран.

Рис. 41 Network > Wireless LAN > QoS

В следующей таблице даны описания полей этого экрана.

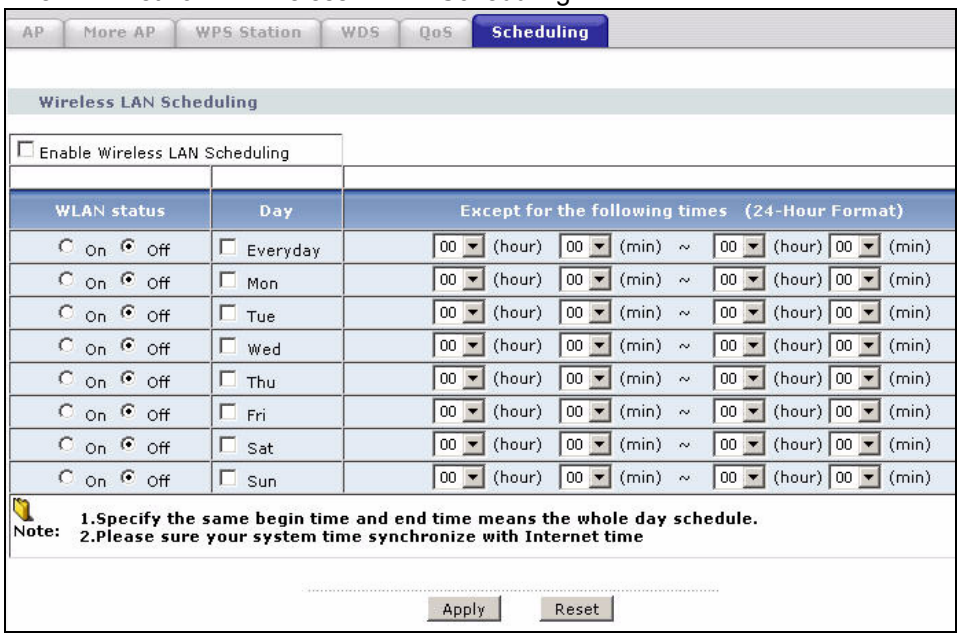
Табл. 31 Network > Wireless LAN > QoS

ПОЛЕ	ОПИСАНИЕ
Enable WMM QoS	Поставьте флажок, чтобы включить функцию WMM QoS в устройстве P660HN. Устройство P660HN назначает приоритет пакетам на основе информации о IEEE 802.1Q или DSCP в их заголовках. Если в заголовке пакета нет информации о WMM, ему назначается стандартный приоритет.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

6.8 Экран расписания

Экран расписания беспроводной LAN используется для конфигурирования дат включения и выключения этой беспроводной сети. Нажмите **Network > Wireless LAN > Scheduling**. Появится следующий экран.

Рис. 42 Network > Wireless LAN > Scheduling



В следующей таблице даны описания полей этого экрана.

Табл. 32 Network > Wireless LAN > QoS

ПОЛЕ	ОПИСАНИЕ
Enable Wireless LAN Scheduling	Установите флажок для активации расписания беспроводной LAN на устройстве P660HN.
WLAN Status	Выберите **On** или **Off** для включения или выключения беспроводной LAN.
Day	Отметьте день (дни), когда необходимо включить или выключить беспроводную LAN.
Except for the following times	Укажите период времени, к которому расписание применяться не будет. Например, вы установили выключение беспроводной LAN ежедневно, а также установили исключение с 12:00 до 1:30. В таком случае беспроводная LAN будет доступна ежедневно только с 12:00 до 1:30.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Reset	Нажмите эту кнопку для восстановления ранее заданных настроек.

6.9 Техническое руководство по беспроводной локальной сети

В этом разделе подробно описываются беспроводные локальные сети. Более подробно см. в приложениях.

6.9.1 Обзор беспроводных сетей

Беспроводные сети состоят из беспроводных клиентских устройств, точек доступа и мостов.

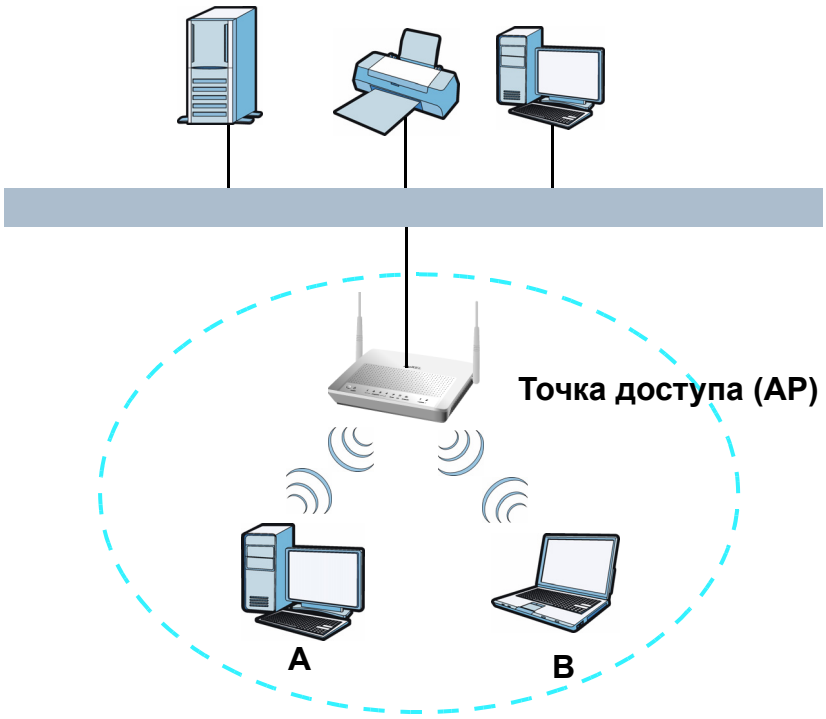
- Беспроводное клиентское устройство представляет собой радиостанцию, подключенную к компьютеру пользователя.
- Точка доступа – это радиостанция с проводным подключением к сети, которая может связываться с большим количеством беспроводных клиентов и предоставлять им доступ в сеть.
- Мост является радиостанцией, обеспечивающей связь между точками доступа и беспроводными клиентами, увеличивая сетевой диапазон.

Как правило, беспроводная сеть работает одним из двух способов.

- Сеть типа «infrastructure» (с точкой доступа) имеет одну или несколько точек доступа и одно или несколько беспроводных клиентских устройств. Беспроводные клиентские устройства подключаются к точкам доступа.
- Сеть типа «ad-hoc» (компьютер-компьютер) не имеет точек доступа. Для обмена информацией беспроводные клиенты подключаются друг к другу.

На следующем рисунке представлен пример беспроводной сети.

Рис. 43 Пример беспроводной сети с точкой доступа



Беспроводная сеть обозначена синим кругом. В этой беспроводной сети устройства **A** и **B** используют точку доступа (**AP**) для подключения к другим устройствам (таким как принтер) или для выхода в Интернет. Устройство P660HN является точкой доступа.

В любой беспроводной сети действуют следующие основные правила:

- Все устройства внутри одной и той же сети должны использовать одинаковые идентификаторы SSID.

  SSID является именем беспроводной сети. Это идентификатор набора служб (Service Set IDentifier).
- Если зоны покрытия двух беспроводных сетей перекрываются, необходимо, чтобы сети работали на разных каналах.

  Подобно радиостанциям или телевизионным каналам, беспроводные сети используют для приема и передачи информации определенные каналы или частоты.
- Все 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.

Радио каналы

Существуют определенные частоты диапазона радиочастот, предназначенные для нелицензируемого гражданского использования. В целях создания беспроводных сетей эти частоты разделены на большое количество каналов. Таким образом, в одном месте может существовать несколько сетей, не влияющих друг на друга. При создании своей сети вам необходимо выбрать канал для использования.

Величина радиочастотных диапазонов доступных для нелицензируемого использования в разных странах различается, следовательно различно и количество доступных каналов.

6.9.2 Дополнительные термины, используемые при беспроводной передаче

В следующей таблице описаны некоторые термины и аббревиатуры, используемые в Web-конфигураторе устройства P660HN.

Табл. 33 Дополнительные термины, используемые при беспроводной передаче

ТЕРМИН	ОПИСАНИЕ
Порог RTS/CTS	В беспроводной сети с большой зоной охвата беспроводные устройства иногда не «знают» о существовании друг друга. При этом могут возникать случаи, когда устройства начинают одновременно передавать информацию на точку доступа, что приводит к конфликтам и передаваемые данные теряются. Если величина порога установлена меньше, чем значение по умолчанию, беспроводные устройства периодически должны получать разрешение на передачу данных в устройство P660HN. Чем меньше значение, тем более часто устройства должны получать разрешение. Если это значение больше, чем величина порога фрагментации (см. ниже), то беспроводные устройства никогда не получат разрешение на передачу данных в устройство P660HN.
Заголовок	Заголовок влияет на синхронизацию в беспроводной сети. Существует два режима заголовков: использование длинных и коротких заголовков. Если устройство использует режим заголовка, отличный от используемого устройством P660HN, оно не сможет установить связь с устройством P660HN.
Аутентификация	Это процедура проверки, которая определяет, может ли беспроводное устройство использовать данную беспроводную сеть.

Табл. 33 Дополнительные термины, используемые при беспроводной передаче (продолжение)

ТЕРМИН	ОПИСАНИЕ
Порог фрагментации	Низкий порог фрагментации рекомендуется устанавливать в перегруженных сетях, в то время как высокий порог обеспечивает увеличение производительности в сетях с небольшой загрузкой.
IGMP	Как правило, IP-пакеты передаются одним из двух способов – одноадресная рассылка (1 отправитель – 1 получатель) или широковещательная рассылка (1 отправитель – все абоненты сети). Многоадресная рассылка доставляет IP-пакеты только группе узлов в сети. IGMP (Internet Group Management Protocol – Протокол управления группами сети Интернет) – это протокол сетевого уровня, используемый для установления принадлежности к группе многоадресной рассылки – он не предназначен для передачи пользовательских данных.
Управление многоадресной рассылкой по протоколу IGMP	Устройство P660HN может только пассивно отслеживать пакеты IGMP, передаваемые между IP маршрутизаторами/коммутаторами и узлами, участвующими в многоадресной рассылке, для сбора информации о членстве в группах многоадресной рассылки. Он проверяет проходящие пакеты IGMP, извлекает данные групповой регистрации, и конфигурирует многоадресную рассылку соответственно полученной информации. Управление многоадресной рассылкой по протоколу IGMP позволяет устройству P660HN получить информацию о группах многоадресной рассылки без необходимости настраивать их вручную.

6.9.3 Обзор защиты беспроводной сети

В сущности радиосигнал можно легко перехватить. В случае беспроводных сетей для обмена данными это означает, что любой пользователь, находящийся в радиусе действия беспроводной сети, не обеспеченной защитой, может не только прочитать информацию, передаваемую по радиоволнам, но также и подключиться к сети. Неавторизованный пользователь, имеющий доступ к сети, может украсть информацию или внедрить вирусы (вредоносные программные средства) с целью дискредитирования информации в сети. По этой причине было разработано большое количество систем безопасности, чтобы только авторизованные пользователи могли пользоваться данной беспроводной сетью или получать информацию, передаваемую по сети.

Эти стандарты безопасности осуществляют защиту по следующим параметрам. Во-первых, они обеспечивают аутентификацию. Это значит, что только пользователи, предоставляющие правильные регистрационные параметры (имя пользователя и пароль или «ключевую фразу»), могут получить доступ в сеть. Во-вторых, они обеспечивают шифрование. Это означает, что информация передается по воздушным радиоволнам в зашифрованном виде. Расшифровать ее могут только пользователи, имеющие кодовый ключ, который выдается только пользователям, прошедшим процедуру аутентификации.

Эти стандарты безопасности отличаются по степени эффективности. Некоторые могут быть взломаны, как, например, старый протокол WEP (Wired Equivalent Protocol). Использование WEP лучше, чем полное отсутствие защиты, но это средство не остановит настойчивого злоумышленника. Другие стандарты безопасности сами по себе безопасны, но также могут быть взломаны, если используются неправильно. Например, стандарт безопасности WPA-PSK имеет высокий уровень защиты при использовании длинного ключа, который злоумышленнику будет трудно расшифровать

с помощью специального ПО, – например, строку длиной в двадцать символов, состоящую из произвольно выбранных букв и цифр, – но низкий уровень защиты при использовании короткого ключа, который можно легко расшифровать, – например, любое слово из словаря, состоящее из трех букв.

Злоумышленник может нанести большой вред сети, поэтому стандарты безопасности должны использоваться не только пользователями, имеющими в сети конфиденциальную информацию. Каждый пользователь беспроводной сети должен убедиться в том, что использует эффективные средства защиты.

Хорошим примером создания эффективных ключей безопасности и паролей является использование информации, известной только вам, и которую вы сами легко запомните, и ввод ее в таком виде, что она будет казаться случайной и не будет включать целые слова. Например, у вашей матери есть автомобиль Dodge Challenger 1970, а ее любимый фильм – «Исчезающая точка» (Vanishing Point) (который, как вы знаете, вышел на экраны в 1971 году). Вы могли бы использовать фразу «70dodchal71vanpoi» в качестве ключа безопасности.

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

6.9.3.1 Идентификатор SSID

В стандартном режиме устройство P660HN работает как радиомаяк, регулярно рассылая в эфир идентификатор SSID. Можно скрыть SSID, и в этом случае устройство P660HN не будет транслировать SSID. Также можно изменить заданный по умолчанию SSID на трудноугадываемый идентификатор.

Однако этот метод защиты 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.

6.9.3.2 Фильтр MAC-адресов

Любое беспроводное сетевое устройство имеет уникальный идентификационный номер, именуемый физическим или MAC-адресом.[1] MAC-адрес обычно записывается с помощью двенадцати шестнадцатеричных символов[2]; например, 00A0C5000002 или 00:A0:C5:00:00:02. Информацию об определении MAC-адреса устройства в беспроводной сети см. в руководстве пользователя для конкретного устройства или в другой документации.

С помощью установки фильтра MAC-адресов в устройстве P660HN можно определить устройства, которым разрешено или не разрешено подключаться к беспроводной сети. Если устройству разрешено подключаться к беспроводной сети, оно должно обладать надлежащими сведениями (SSID, канал и способ защиты). Если устройству не разрешено подключаться к беспроводной сети, то не имеет значения, обладает ли оно этой информацией.

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.

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

6.9.3.3 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. Для прохождения аутентификации все устройства в беспроводной сети должны поддерживать стандарт IEEE 802.1x.

В беспроводных сетях имена пользователей и пароли для каждого пользователя обычно хранятся на сервере RADIUS. Этот сервер чаще используется в организациях, чем дома. Если у вас нет сервера RADIUS, вы не сможете устанавливать имена и пароли для пользователей.

Несанкционированные беспроводные 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.

6.9.3.4 Шифрование

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

Виды шифрования выбираются в зависимости от типа аутентификации. (Дополнительную информацию см. в Разд. 6.9.3.3 на с. 111.)

Табл. 34 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 наиболее сложное шифрование, которое поддерживает каждое устройство в беспроводной сети. Предположим, ваше устройство P660HN подключено к беспроводной сети, и у вас нет сервера RADIUS. Следовательно, аутентификация отсутствует. Предположим, что в беспроводной сети находится два устройства. 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 других типов шифрования лучше, чем полное отсутствие шифрования, но для несанкционированных устройств существует возможность достаточно быстро вычислить исходные данные для подключения.

При выборе **WPA2** или **WPA2-PSK** в устройстве P660HN можно также установить параметр **WPA compatible** с целью реализации поддержки WPA. В таком случае, если некоторые устройства поддерживают WPA, а некоторые WPA2, необходимо установить **WPA2-PSK** or **WPA2** (в зависимости от типа регистрации в беспроводной сети, а также установить **WPA compatible** в устройстве P660HN.

В большинстве типов шифрования для защиты информации в беспроводной сети используется ключ. Чем длиннее ключ, тем сложнее шифрование. Все устройства в одной беспроводной сети должны использовать один и тот же ключ.

6.9.4 Проблемы с сигналом

Беспроводные сети являются радиосетями, а значит могут появиться такие проблемы, как ограничение сигнала из-за большого расстояния, помехи и поглощение сигнала.

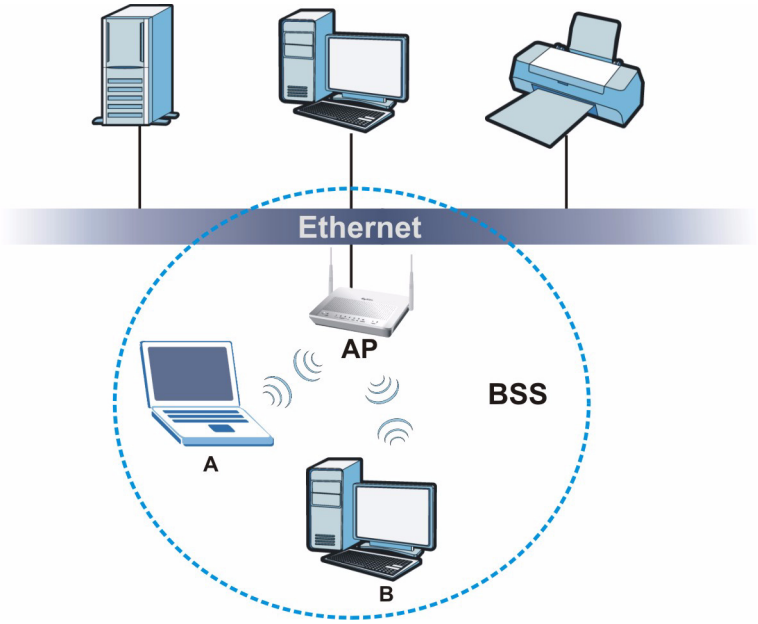
Проблемы с расстоянием возникают в том случае, если две радиостанции находятся очень далеко друг от друга. Проблемы с помехами возникают, когда другие радиоволны вмешиваются в сигнал данных. Помехи могут появиться из-за других радиопередач, например, при военном сообщении или управлении воздушным движением, а также из-за устройств, которые являются случайными источниками излучения, таких как электродвигатели и микроволновые печи. Проблемы с поглощением возникают, когда между двумя радиостанциями находятся физические объекты (например, толстые стены), которые глушат сигнал.

6.9.5 BSS

Базовый набор служб (BSS) существует тогда, когда весь трафик между беспроводными устройствами или между беспроводным устройством и клиентом проводной сети идет через одну точку доступа (AP).

Intra-BSS трафик – это трафик между беспроводными устройствами в пределах одного базового набора служб. При отключении блокировки Intra-BSS трафика беспроводные устройства A и B могут получать доступ к проводной сети и обмениваться информацией между собой. При включении блокировки Intra-BSS трафика беспроводные устройства A и B все равно могут получить доступ к проводной сети, однако не могут обмениваться информацией.

Рис. 44 Базовый набор служб



6.9.6 MBSSID

Как правило, вам необходимо использовать разные точки доступа (AP) для настройки разных базовых наборов служб (BSS). Покупка дополнительных точек доступа требует дополнительных затрат, а также может возникнуть проблема помех в каналах. Функция устройства P660HN MBSSID (Multiple Basic Service Set IDentifier – Идентификатор нескольких наборов служб) позволяет использовать одну точку доступа для обеспечения нескольких BSS одновременно. В этом случае вы можете назначить различные приоритеты QoS и/или режимы безопасности разным SSID.

Беспроводные устройства могут использовать разные BSSID для связи с одной и той же точкой доступа.

6.9.6.1 Примечания по функции Multiple BSS

- Максимальное количество BSS, которые могут работать с одной точкой доступа, – восемь.
- Для разных BSS нужно использовать разные ключи. Если у двух беспроводных устройств разные BSSID (они находятся в разных BSS), но у них одинаковые ключи, они могут слышать друг друга (но не обмениваться данными друг с другом).
- MBSSID не должен заменять защиту по стандарту 802.1x, но использоваться вместе с ней.

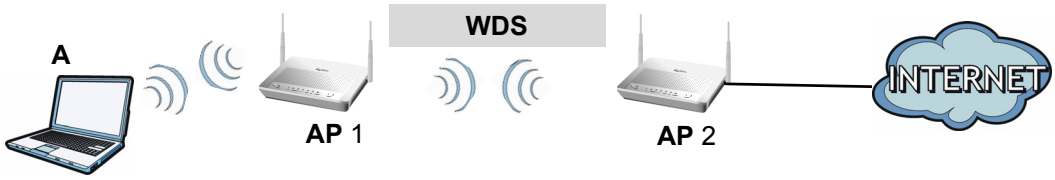
6.9.7 Беспроводная система распределения (WDS)

Устройство P660HN может работать в качестве беспроводного сетевого моста и устанавливать соединения WDS с другими точками доступа. Для того, чтобы установить соединение с точкой доступа, нужно знать ее MAC-адрес. Если настройки безопасности клиентов совпадают, то выполняется соединение между устройствами.

На момент написания руководства безопасность WDS совместима только с другими точками доступа ZyXEL. Подробную информацию см. в документации к точке доступа другого производителя.

На следующем рисунке показано, как работает соединение WDS между точками доступа. Ноутбук **A** является беспроводным клиентским устройством, соединяющимся с точкой доступа **AP 1**. На **AP 1** нет проводного Интернет-соединения, но она может установить WDS-соединение с точкой доступа **AP 2**, что и происходит. Когда **AP 1** устанавливает WDS-соединение с **AP 2**, ноутбук получает доступ к Интернет через **AP 2**.

Рис. 45 Пример WDS-соединения



6.9.8 Настройка безопасности Wi-Fi (WPS)

Ваше устройство P660HN поддерживает настройку безопасности WiFi (WPS), которая представляет собой простой способ защиты беспроводной сети. WPS является технической характеристикой промышленного стандарта, определяемого WiFi Alliance.

WPS позволяет быстро настроить беспроводную сеть, обеспечивая надежную защиту без ручной установки параметров защиты. Каждое подключение WPS устанавливается между двумя устройствами. Оба устройства должны поддерживать WPS (для надежности проверяйте документацию для каждого устройства).

В зависимости от устройств, которые есть у вас, вы можете либо нажать кнопку (на самом устройстве или на утилите конфигурации), либо ввести PIN-код (уникальный персональный идентификационный номер, позволяющий одному устройству определять другое) на каждом из устройств. При активации WPS на устройстве у него есть две минуты, чтобы найти другое устройство, в котором тоже активирована WPS. Затем происходит подключение обоих устройств, и автоматически формируется защищенная сеть.

6.9.8.1 Настройка кнопкой

Настройка кнопкой (PBC) WPS инициализируется при нажатии кнопки на каждом устройстве с WPS и позволяет устройствам соединяться автоматически. Нет необходимости вводить какую-либо информацию.

Не у каждого устройства с WPS есть фактическая кнопка WPS. У некоторых устройств есть кнопка WPS PBC в утилите настройки, вместо или в дополнение к фактической кнопке.

Выполните следующие действия для установки WPS с помощью кнопки.

1. Убедитесь в том, что оба устройства, на которых вы проводите установку, находятся в пределах беспроводного диапазона.
2. Найдите кнопку WPS на каждом из устройств. Если на устройстве нет такой кнопки, зайдите в утилиту настройки и найдите кнопку (как это сделать, см. в Руководстве пользователя устройства – для устройства P660HN см. Разд. 6.5 на с. 103).
3. Нажмите кнопку на одном из устройств (неважно, на каком). Для устройства P660HN: нужно удерживать кнопку WPS нажатой более трех секунд.
4. В течение двух минут нажмите кнопку на втором устройстве. Регистратор отправляет по безопасному соединению регистрируемому устройству имя сети (SSID) и ключ безопасности.

Если вы хотите убедиться, что WPS работает, проверьте список подключенных беспроводных клиентов в утилите настройки точки доступа. Если вы видите нужное клиентское устройство в списке, значит WPS установлено успешно.

6.9.8.2 Настройка PIN-кодом

Каждое устройство с WPS обладает собственным PIN-кодом (Personal Identification Number – персональный идентификационный номер). Он может быть статическим (его нельзя изменить) или динамическим (на некоторых устройствах можно сгенерировать новый PIN, нажав на кнопку в конфигурационном интерфейсе).

Используйте метод настройки PIN-кодом, вместо метода настройки кнопкой (PBC), чтобы убедиться, что соединение устанавливается между указанными вами устройствами, а не только между первыми двумя устройствами, которые активировали WPS в беспроводном диапазоне друг друга. Однако для использования метода настройки PIN-кодом необходимо зайти в конфигурационный интерфейс обоих устройств.

При использовании метода настройки PIN-кодом, необходимо ввести PIN-код одного из устройств (как правило, беспроводного клиента) во второе устройство (как правило, точку доступа или беспроводной маршрутизатор). Затем, когда WPS активируется на первом устройстве, оно предоставляет свой PIN-код второму устройству. Если PIN-код совпадает, одно из устройств отправляет второму информацию о сети и настройки безопасности, позволяя этому устройству присоединиться к сети.

Выполните следующие действия для того, чтобы установить WPS-соединение, используя метод настройки PIN-кодом, между точкой доступа или беспроводным маршрутизатором (называемым здесь точкой доступа (AP)) и клиентским устройством.

1. Убедитесь в том, что на обоих устройствах активирована функция WPS.
2. Войдите в раздел WPS в конфигурационном интерфейсе точки доступа. Как это сделать, описано в Руководстве пользователя устройства.
3. Найдите PIN-код клиентского устройства с WPS; он написан на устройстве, или отображен в разделе WPS конфигурационного интерфейса клиентского устройства (как найти WPS PIN-код, см. в Руководстве пользователя – для устройства P660HN см. Разд. 6.4 на с. 102).
4. Введите PIN-код клиентского устройства в конфигурационный интерфейс точки доступа.

Если в конфигурационном интерфейсе клиентского устройства есть область для ввода PIN-кода другого устройства, можно либо ввести PIN-код клиентского устройства в интерфейс точки доступа, либо – PIN-код точки доступа в интерфейс клиентского устройства – на ваш выбор.

5 Запустите WPS на обоих устройствах в течение двух минут.

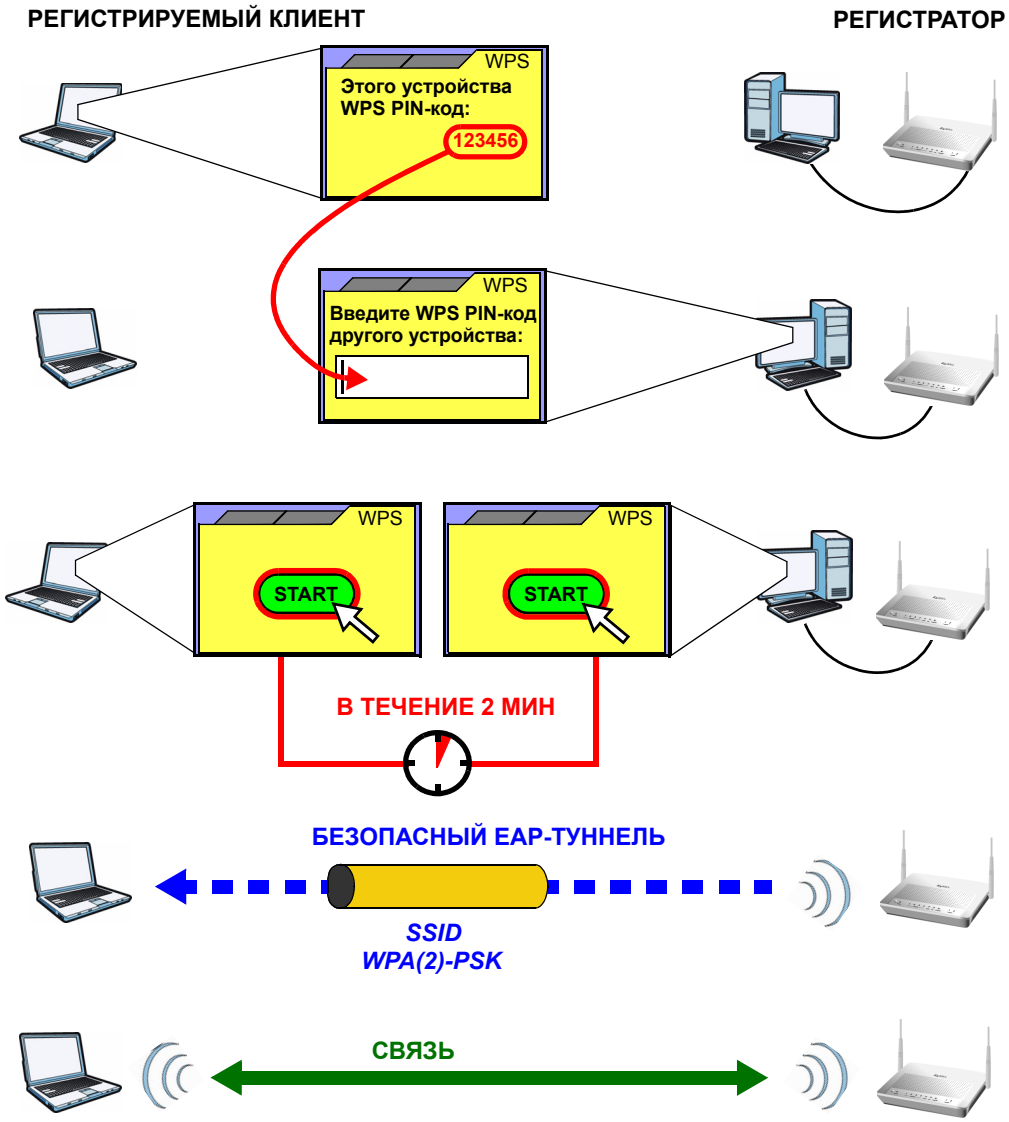
Для активации WPS, используйте утилиту настройки, а не кнопку на самом устройстве.

6 На компьютере, подключенном к беспроводному клиенту, попытайтесь подключиться к Интернету. Если осуществить подключение удалось, WPS было установлено успешно.

Если подключиться невозможно, проверьте список подключенных беспроводных клиентов в утилите настройки точки доступа. Если вы видите нужное клиентское устройство в списке, значит WPS установлено успешно.

На следующем рисунке показано подключение беспроводного клиента с функцией WPS (установленной на ноутбуке) к точке доступа с функцией WPS с помощью метода настройки PIN-кодом.

Рис. 46 Пример процесса WPS: Способ защиты PIN-кодом

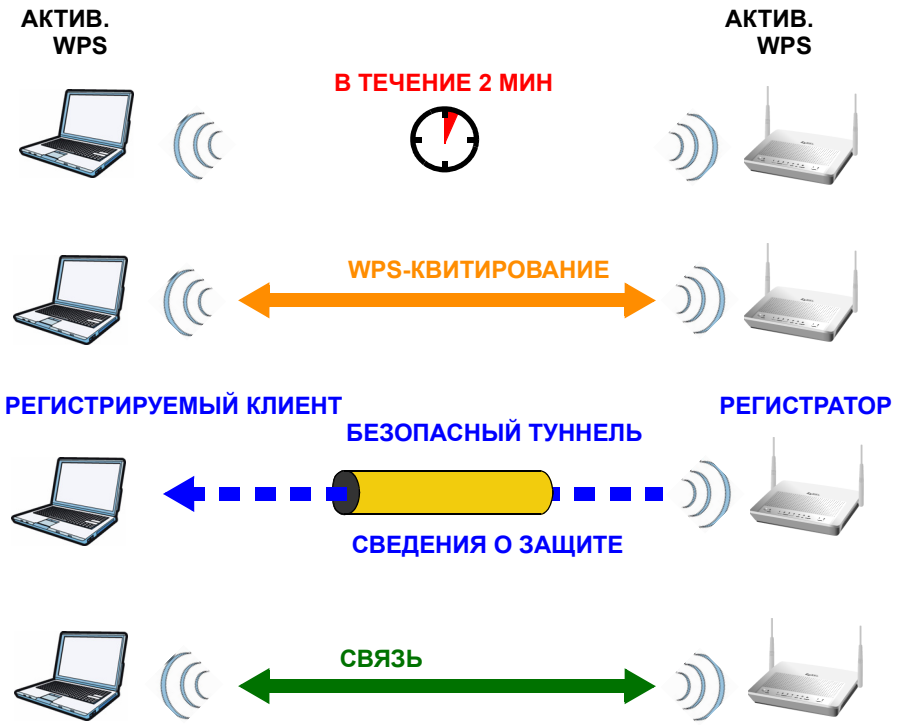


6.9.8.3 Как работает WPS

При подключении друг к другу двух устройств с функцией WPS, каждое устройство должно принять на себя специфическую роль. Одно устройство действует в качестве регистратора (устройство, поставляющее сетевые настройки и настройки безопасности), а другое устройство действует, как регистрируемое (устройство, получающее сетевые настройки и настройки безопасности). Регистратор создает безопасный EAP-туннель (Extensible Authentication Protocol – Расширенный протокол аутентификации) и отправляет имя сети (SSID) и предварительно согласованный ключ WPA-PSK или WPA2-PSK регистрируемому устройству. Использование WPA-PSK или WPA2-PSK зависит от стандартов, поддерживаемых устройствами. Если регистратор уже является частью сети, он отправляет существующую информацию. Если нет, то он произвольно генерирует SSID и WPA(2)-PSK.

На следующем рисунке показано подключение клиентского устройства с функцией WPS (установленной на ноутбуке) к точке доступа с функцией WPS.

Рис. 47 Как работает WPS



Роли регистратора и регистрируемого устройства актуальны только во время процесса установки WPS (две минуты). В следующий раз при использовании WPS, другое устройство может выполнять роль регистратора (при необходимости).

Процесс установления соединения WPS называется «квитирование», он подобен рукопожатию – только два устройства участвуют в каждой из транзакций WPS. Для добавления других устройств необходимо повторить процедуру с одним из существующих сетевых устройств и новым устройством.

Помните, что точка доступа (AP) не всегда является регистратором, а беспроводной клиент – регистрируемым устройством. Все точки доступа с WPS, а также некоторые беспроводные клиенты с WPS могут быть регистратором.

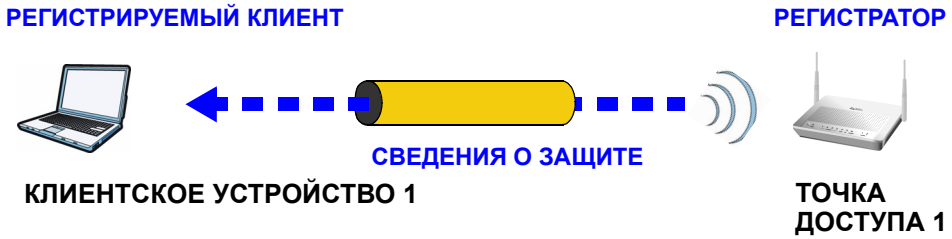
По умолчанию, устройство WPS «не сконфигурировано» (unconfigured). Это значит, что оно не является частью существующей сети и может работать в качестве регистратора и регистрируемого (если оно поддерживает обе функции). Если устройство-регистратор не сконфигурировано, настройки безопасности, которые оно отправляет регистрируемому устройству, генерируются случайным образом. Как только устройство с WPS подключается к другому устройству, использующему WPS, оно становится «сконфигурированным» (configured). Сконфигурированный беспроводной клиент может работать в качестве регистрируемого или регистратора в последующих WPS-соединениях, но сконфигурированная точка доступа не может быть регистрируемым устройством. Во всех последующих WPS-соединениях, в которые она вовлечена, она будет регистратором. Для того, чтобы точка доступа работала, как регистрируемое устройство, нужно сбросить параметры устройства к заводским настройкам по умолчанию.

6.9.8.4 Пример настройки сети WPS

В этом разделе показано, как проходит распределение настроек безопасности, на примере настроенного WPS-соединения.

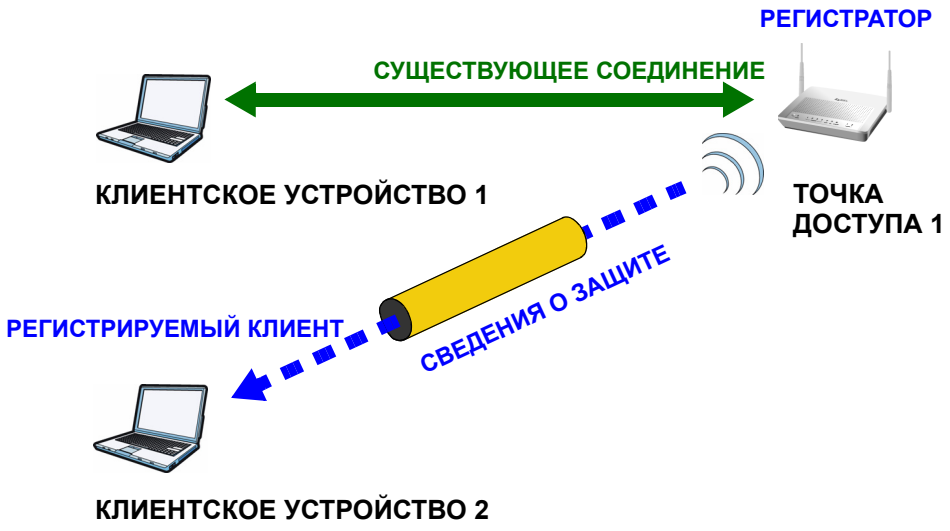
На следующем рисунке представлен пример сети. Шаг **1**: **точка доступа 1** и **клиентское устройство 1** не сконфигурированы. Когда на обоих устройствах активируется WPS, они выполняют квитирование. В данном примере **точка доступа 1** является регистратором, а **клиентское устройство 1** – регистрируемым. Регистратор случайным образом генерирует настройки безопасности для установки сети, так как это устройство не сконфигурировано и не имеет существующих настроек.

Рис. 48 WPS: Пример сети, шаг 1



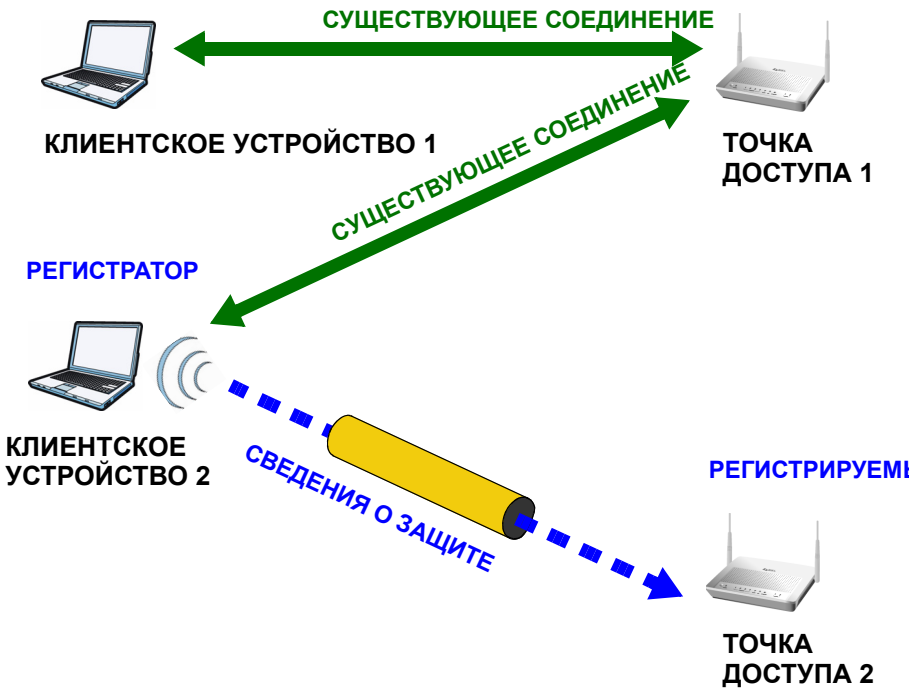
Шаг **2**: вы добавляете в сеть другое беспроводное клиентское устройство. Вы знаете, что **клиентское устройство 1** поддерживает режим регистратора, но лучше использовать **точку доступа 1** для WPS-квитирования с новым клиентским устройством, так как для использования сети в любом случае нужно подключиться к точке доступа. В данном случае **точка доступа 1** должна быть регистратором, так как она сконфигурирована (уже обладает настройками безопасности для установки сети). **Точка доступа 1** поставляет существующие настройки безопасности **клиентскому устройству 2**.

Рис. 49 WPS: Пример сети, шаг 2



Шаг 3: вы добавляете другую точку доступа (**точка доступа 2**) в вашу сеть. **Точка доступа 2** находится вне зоны доступа **точки доступа 1**, следовательно, **точку доступа 1** нельзя использовать для WPS-квитирования с новой точкой доступа. Однако, вы знаете, что **клиентское устройство 2** поддерживает функцию регистратора, таким образом, его можно использовать для WPS-квитирования.

Рис. 50 WPS: Пример сети, шаг 3



6.9.8.5 Ограничения WPS

WPS имеет ограничения, о которых вам нужно знать.

- WPS работает только в сетях «с точкой доступа» (Infrastructure) (где данными обмениваются точка доступа и беспроводной клиент). Эта функция не работает в сетях «компьютер-компьютер» (Ad-Hoc) (где точка доступа отсутствует).
- При использовании WPS эта функция работает только между двумя устройствами. Нельзя одновременно зарегистрировать несколько устройств; устройства регистрируются одно после другого.

  Например, если у вас два регистрируемых устройства и регистратор, необходимо сначала установить первое регистрируемое устройство (например, нажав кнопку WPS на регистраторе и первом регистрируемом устройстве), затем, убедившись в успешном выполнении регистрации, установить второе устройство таким же образом.
- WPS работает только с устройствами, поддерживающими WPS. Однако, в уже настроенную с помощью WPS сеть, все же можно добавить устройства без WPS.

WPS работает, атоматически передавая предварительно согласованный ключ WPA-PSK или WPA2-PSK от устройства-регистратора к регистрируемому устройству. Использование ключа WPA-PSK или WPA2-PSK зависит от устройства. Чтобы узнать, какой ключ используется системой, нужно войти в конфигурационный интерфейс регистратора (если устройство поддерживает эту функцию). Затем, вы можете ввести ключ в интерфейс устройства без WPS и присоединиться к сети (устройство без WPS также должно поддерживать WPA-PSK или WPA2-PSK).

- При использовании метода PBC есть короткий период (с момента нажатия кнопки на одном устройстве до момента ее нажатия на другом), когда любое устройство с WPS может подключиться к сети. Это происходит потому, что регистратор не способен определить «правильное» регистрируемое устройство и не различает ваше устройство и неавторизованное устройство. Вследствие этого существует опасность получения хакером доступа к сети.

  Проверить наличие неавторизованных устройств легко. WPS работает одновременно только между двумя устройствами, таким образом, если другое устройство подключилось к сети, то ваше устройство не сможет зарегистрироваться и получить доступ к сети. Если это произошло, откройте конфигурационный интерфейс точки доступа и проверьте список подключенных клиентов (обычно отображаются MAC-адреса). Неважно, является ли точка доступа регистратором WPS, регистрируемым устройством, или она вообще не была вовлечена в WPS-квитирование; неавторизованное устройство все равно должно подключаться к точке доступа для получения доступа к сети. Проверьте MAC-адреса ваших беспроводных клиентских устройств (как правило, они напечатаны на табличке на нижней части устройства). Если в списке присутствует незнакомый MAC-адрес, его можно удалить или перезапустить точку доступа.

7

Трансляция сетевых адресов (NAT)

7.1 Обзор

В этой главе рассказывается, как настроить функцию NAT в устройстве P660HN. NAT (Network Address Translation – Трансляция сетевых адресов, RFC 1631) – это преобразование IP-адреса узла в пакете, напр., адрес источника исходящего пакета, используемого в одной сети, в другой IP-адрес, известный в другой сети.

7.1.1 Что можно сделать на экранах NAT

- Экран **NAT General Setup** (Разд. 7.2 на с. 123) используется для настройки параметров установки NAT.
- Экран **Port Forwarding** (Разд. 7.3 на с. 125) используется для пересылки на сервер(ы) вашей локальной сети входных запросов на услугу.
- Экран **Address Mapping** (Разд. 7.4 на с. 128) используется для изменения параметров отображения адреса устройства P660HN.
- Экран **SIP ALG** (Разд. 7.5 на с. 131) используется для включения и выключения функции SIP (VoIP) ALG на устройстве P660HN.

7.1.2 Что нужно знать о NAT

Внутренний/Внешний

Определение «Внутренний/внешний» означает расположение узла относительно устройства P660HN, например, компьютеры ваших абонентов являются внутренними узлами, тогда как веб-серверы Интернета являются внешними узлами.

Глобальный/локальный

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.

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 назначения (внутренний глобальный адрес) обратно во внутренний локальный адрес перед пересылкой исходному внутреннему узлу.

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.

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, устройство P660HN 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. 42 на с. 135.

- Выберите **SUA Only**, если устройство P660HN имеет только один общедоступный IP-адрес в глобальной сети.
- Выберите **Full Feature**, если устройство P660HN имеет несколько общедоступных IP-адресов в глобальной сети.

Дополнительные сведения

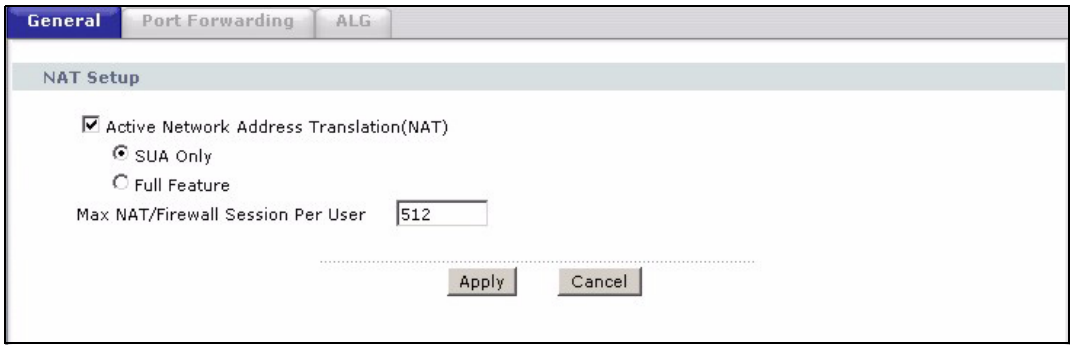
Техническую вводную информацию о NAT см. в Разд. 7.6 на с. 132.

7.2 Экран настройки общих параметров NAT

Этот экран используется для включения функции NAT. Нажмите **Network** > **NAT** для отображения следующего экрана.

Чтобы разрешить прохождение трафика из глобальной сети через устройство P660HN, необходимо в дополнение к SUA/NAT создать правило брандмауэра.

Рис. 51 Network > NAT > General



В следующей таблице даны описания полей этого экрана.

Табл. 35 Network > NAT > General

ПОЛЕ	ОПИСАНИЕ
Active Network Address Translation (NAT)	Поставьте флажок в этом поле, чтобы включить NAT.
SUA Only	Выберите эту опцию, если устройство P660HN имеет только один общедоступный IP-адрес в глобальной сети.
Full Feature	Выберите эту опцию, если устройство P660HN имеет несколько общедоступных IP-адресов в глобальной сети.
Max NAT/Firewall Session Per User	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 брандмауэра. Это поле предназначено для ограничения количества сеансов NAT/брандмауэр, которые клиентские компьютеры могут устанавливать через устройство P660HN. Если в вашей сети небольшое число клиентов использует равноправные соединения, это число можно увеличить, чтобы не снижать качество обслуживания из-за ограничения доступных каждому клиенту сеансов NAT. Если в вашей сети большое число клиентов использует равноправные соединения, это число следует уменьшить, чтобы не допустить ситуации, когда один клиент занимает все доступные сеансы NAT.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

7.3 Экран переадресации портов

Экран переадресации портов доступен, только если установлен режим **SUA Only** на экране **NAT > General**.

Этот экран используется для переадресации входных запросов на услугу, поступающих на сервер(ы) вашей локальной сети.

Можно ввести либо номер одного порта, либо диапазон номеров портов, подлежащих пересылке, и локальный IP-адрес требуемого сервера. Номер порта идентифицирует службу; например, услуга Web – 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.

Чаще всего используют номера портов и службы, приведенные в Прил. E на с. 354. Дополнительную информацию по номерам портов см. в RFC 1700.

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.

IP-адрес сервера по умолчанию

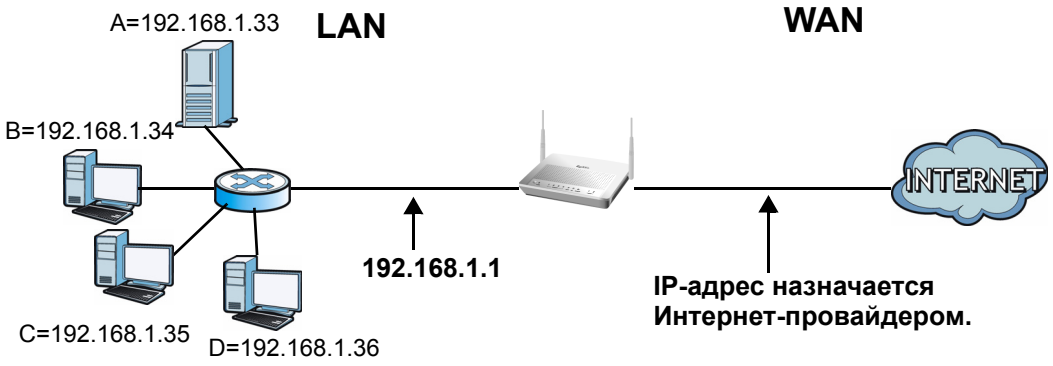
Кроме серверов для конкретных служб, NAT поддерживает IP-адрес сервера по умолчанию. Сервер по умолчанию принимает пакеты от портов, которые не указаны на данном экране (т. е. все пакеты, не попадающие под созданные вами правила, будут перенаправляться на сервер по умолчанию).

Если **серверу по умолчанию** не назначен IP-адрес, устройство P660HN сбрасывает все пакеты, принятые для портов, которые не указаны здесь или в настройках удаленного управления.

Пример настройки серверов, расположенных за преобразованием 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. 52 Пример: несколько серверов расположены за NAT

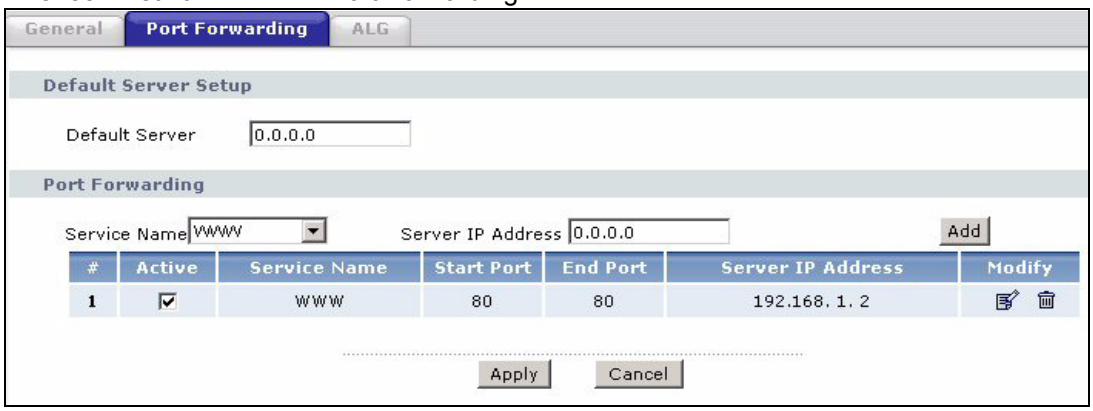


7.3.1 Конфигурирование экрана переадресации портов

Нажмите **Network > NAT > Port Forwarding**, чтобы открылся следующий экран.

Информацию по номерам портов, обычно используемых для конкретных служб см. в Прил. E на с. 354.

Рис. 53 Network > NAT > Port Forwarding



В следующей таблице даны описания полей этого экрана.

Табл. 36 Network > NAT > Port Forwarding

ПОЛЕ	ОПИСАНИЕ
Default Server Setup	
Default Server	Кроме серверов определенных видов служб NAT поддерживает сервер по умолчанию. Сервер по умолчанию принимает пакеты от портов, которые не указаны на данном экране. Если **серверу по умолчанию** не назначен IP-адрес, устройство P660HN сбрасывает все пакеты, принятые для портов, которые не указаны здесь или в настройках удаленного управления.

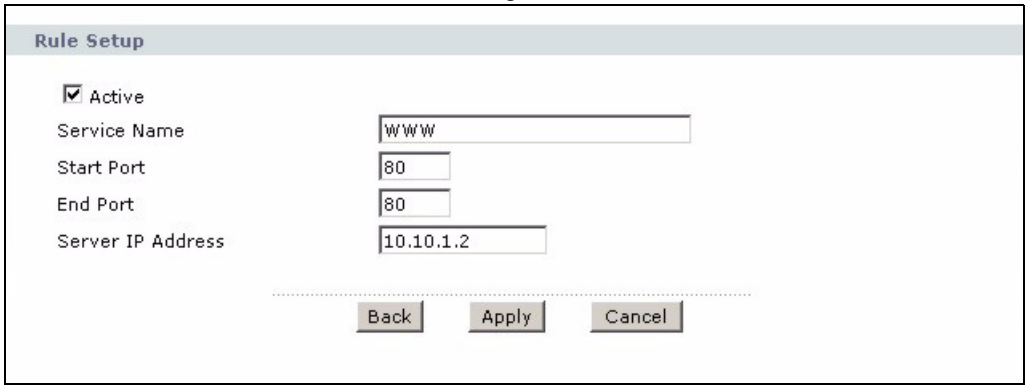
Табл. 36 Network > NAT > Port Forwarding (продолжение)

ПОЛЕ	ОПИСАНИЕ
Port Forwarding	
Service Name	Выберите службу из выпадающего списка.
Server IP Address	Введите IP-адрес сервера для данной службы.
Add	Нажмите эту кнопку, чтобы добавить в таблицу новое правило.
#	Это порядковый номер правила (только для чтения).
Active	Показывает, включено ли правило. Чтобы отключить данное правило, снимите флажок. Для включения соединения поставьте флажок.
Service Name	Здесь отображается имя службы.
Start Port	Номер первого порта, определяющего службу.
End Port	Номер последнего порта, определяющего службу.
Server IP Address	IP-адрес сервера.
Modify	Щелкните по иконке редактирования для перехода к экрану, 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	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

7.3.2 Экран редактирования правил переадресации портов

Этот экран используется для редактирования правила переадресации портов. Щелкните по иконке редактирования для соответствующего правила на экране **Port Forwarding** для отображения следующего экрана.

Рис. 54 Network > NAT > Port Forwarding: Edit



В следующей таблице даны описания полей этого экрана.

Табл. 37 Network > NAT > Port Forwarding: Edit

ПОЛЕ	ОПИСАНИЕ
Active	Поставьте флажок для включения правила.
Service Name	Введите имя для описания правила переадресации портов.
Start Port	Введите в это поле номер порта. Для переадресации трафика только одного порта введите его номер еще раз в поле **End Port**. Для переадресации трафика серии портов введите в это поле номер первого порта, а в поле **End Port** – номер последнего порта.
End Port	Введите в это поле номер порта. Для переадресации трафика только одного порта, введите его номер в поле **Start Port**, а затем введите этот же номер еще раз в это поле. Для переадресации трафика серии портов введите номер последнего порта серии портов, начинающейся с номера порта, установленного в поле **Start Port**.
Server IP Address	Введите в это поле внутренний IP-адрес сервера.
Back	Нажмите эту кнопку для возврата к предыдущему экрану без сохранения.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

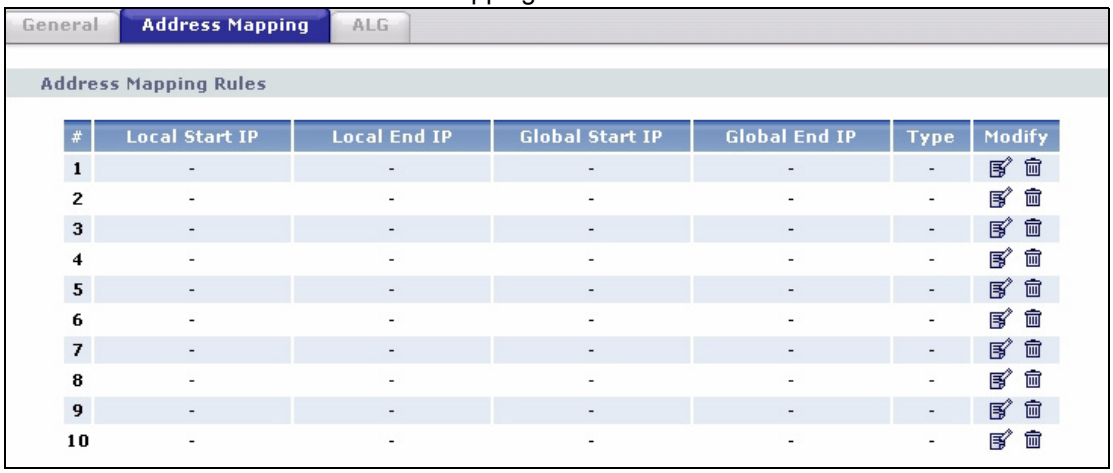
7.4 Экран отображения адресов

Экран **Address Mapping** доступен, только если установлен режим **Full Feature** на экране **NAT > General**.

Порядок следования правилам имеет большое значение, так как устройство P660HN применяет правила в установленном порядке. Когда текущий пакет соответствует какому-либо правилу устройства, устройство P660HN 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, если в текущем наборе уже имеются правила с 1 по 6 и теперь создается правило под номером 9, на сводном экране набора правил новое правило будет иметь номер 7, а 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 устройстве P660HN параметров отображения адресов, нажмите **Network > NAT > Address Mapping**, чтобы открыть следующий экран.

Рис. 55 Network > NAT > Address Mapping



В следующей таблице даны описания полей этого экрана.

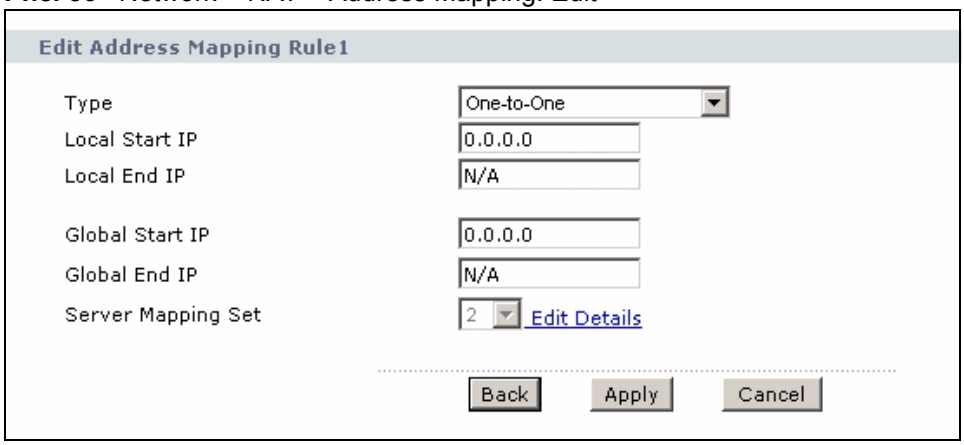
Табл. 38 Network > NAT > Address Mapping

ПОЛЕ	ОПИСАНИЕ
#	Это порядковый номер правила.
Local Start IP	Начальный внутренний локальный IP-адрес (начальный ILA). Локальные IP-адреса недоступны (**N/A**) для типа отображения портов **Server**.
Local End IP	Это конечный внутренний локальный IP-адрес (конечный ILA). Если правило предназначено для всех локальных IP-адресов, то в поле **Local Start IP** отображается 0.0.0.0, а в поле **Local End IP** отображается 255.255.255.255. В этом поле отображается **N/A** для типов отображения **One-to-One** и **Server**.
Global Start IP	Начальный внутренний глобальный IP-адрес (начальный IGA). Если вы используете динамический IP-адрес, назначаемый Интернет-провайдером, введите в это поле 0.0.0.0. В этом случае используются только отображения **Many-to-One** и **Server**.
Global End IP	Конечный внутренний глобальный IP-адрес (конечный IGA). В этом поле отображается **N/A** для типов отображения **One-to-One**, **Many-to-One** и **Server**.
Type	**1-1**: В режиме один-к-одному один локальный IP-адрес преобразуется в один глобальный IP-адрес. Следует отметить, что в данном режиме отображения NAT номера портов не изменяются. **M-1**: В режиме много-к-одному несколько локальных IP-адресов преобразуется в 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 много-ко-многим с перегрузкой несколько локальных IP-адресов преобразуется в несколько коллективных глобальных IP-адресов. **MM No** (No Overload): В режиме много-ко-многим без перегрузки каждый локальный IP-адрес преобразуется в уникальный глобальный IP-адрес. **Server**: Этот режим позволяет установить внутренний сервер различных служб после преобразования NAT для доступа внешних пользователей.
Modify	Щелкните по иконке редактирования для перехода к экрану, 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.

7.4.1 Экран редактирования правила отображения адресов

Этот экран используется для редактирования правила отображения адресов. Щелкните по иконке редактирования для соответствующего правила на экране **Address Mapping** для отображения следующего экрана.

Рис. 56 Network > NAT > Address Mapping: Edit



В следующей таблице даны описания полей этого экрана.

Табл. 39 Network > NAT > Address Mapping: Edit

ПОЛЕ	ОПИСАНИЕ
Type	Выберите тип отображения портов из следующих вариантов. **One-to-One**: В режиме один-к-одному один локальный IP-адрес преобразуется в один глобальный IP-адрес. Следует отметить, что в данном режиме отображения NAT номера портов не изменяются. **Many-to-One**: В режиме много-к-одному несколько локальных IP-адресов преобразуется в 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**: В режиме много-ко-многим с перегрузкой несколько локальных IP-адресов преобразуется в несколько коллективных глобальных IP-адресов. **Many-to-Many No Overload**: В режиме много-ко-многим без перегрузки каждый локальный IP-адрес преобразуется в уникальный глобальный IP-адрес. **Server**: Этот режим позволяет установить внутренний сервер различных служб после преобразования NAT для доступа внешних пользователей.
Local Start IP	Начальный локальный IP-адрес (начальный ILA). Локальные IP-адреса недоступны (**N/A**) для типа отображения портов **Server**.
Local End IP	Конечный локальный IP-адрес (конечный ILA). Если правило предназначено для всех локальных IP-адресов, то в поле **Local Start IP** введите 0.0.0.0, а в поле **Local End IP** введите 255.255.255.255. В этом поле отображается **N/A** для типов отображения **One-to-One** и **Server**.
Global Start IP	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 (конечный IGA). В этом поле отображается **N/A** для типов отображения **One-to-One**, **Many-to-One** и **Server**.
Server Mapping Set	Это поле доступно, только если в поле **Type** установлено значение **Server**. Выберите число из выпадающего списка, чтобы установить набор переадресации портов.

Табл. 39 Network > NAT > Address Mapping: Edit (продолжение)

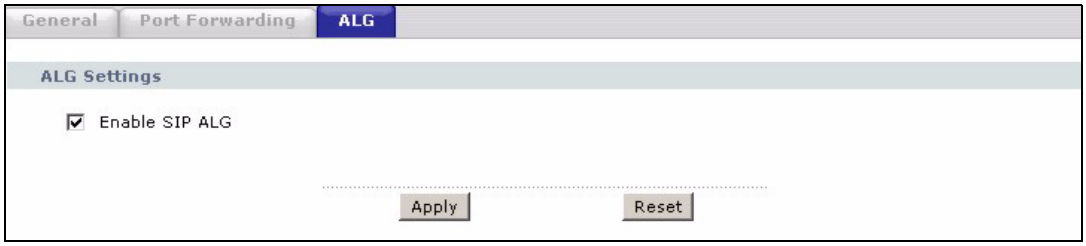
ПОЛЕ	ОПИСАНИЕ
Edit Details	Щелкните по этой ссылке для перехода к экрану **Port Forwarding** для внесения изменений в набор переадресации портов, установленный в поле **Server Mapping Set**.
Back	Нажмите эту кнопку для возврата к предыдущему экрану без сохранения.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

7.5 Экран SIP ALG

Некоторые NAT маршрутизаторы могут включать функцию SIP ALG (Session Initialization Protocol Application Layer Gateway – Встроенный программный шлюз для приложений, использующих протокол SIP). SIP ALG позволяет вызовам SIP проходить через NAT с помощью анализа и преобразования IP-адресов, содержащихся в потоке данных. Когда устройство P660HN регистрируется в сервере SIP, шлюз SIP ALG производит преобразование частного IP-адреса устройства P660HN внутри потока данных SIP в общедоступный IP-адрес. При этом не требуется использовать STUN или исходящий прокси-сервер, если устройство P660HN находится за шлюзом SIP ALG.

Этот экран используется для включения и выключения функции SIP (VoIP) ALG устройства P660HN. Для перехода к этому экрану нажмите **Network > NAT > ALG**.

Рис. 57 Network > NAT > ALG



В следующей таблице даны описания полей этого экрана.

Табл. 40 Network > NAT > ALG

ПОЛЕ	ОПИСАНИЕ
Enable SIP ALG	Установите флажок для корректной работы SIP (VoIP) с правилами переадресации портов и правилами отображения адресов.
Apply	Нажмите эту кнопку для сохранения своих изменений
Reset	Нажмите эту кнопку для восстановления ранее заданных настроек.

7.6 Техническое руководство NAT

В этой главе содержится дополнительная информация о NAT.

7.6.1 Определения NAT

Определение «Внутренний/внешний» означает расположение узла относительно устройства P660HN, например, компьютеры ваших абонентов являются внутренними узлами, тогда как веб-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. 41 Определения NAT

ПАРАМЕТР	ОПИСАНИЕ
Inside	Означает узел в локальной сети LAN.
Outside	Означает узел в глобальной сети WAN.
Local	Относится к адресу в пакете (источника или адресата), когда пакет перемещается в локальной сети.
Global	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.

7.6.2 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.

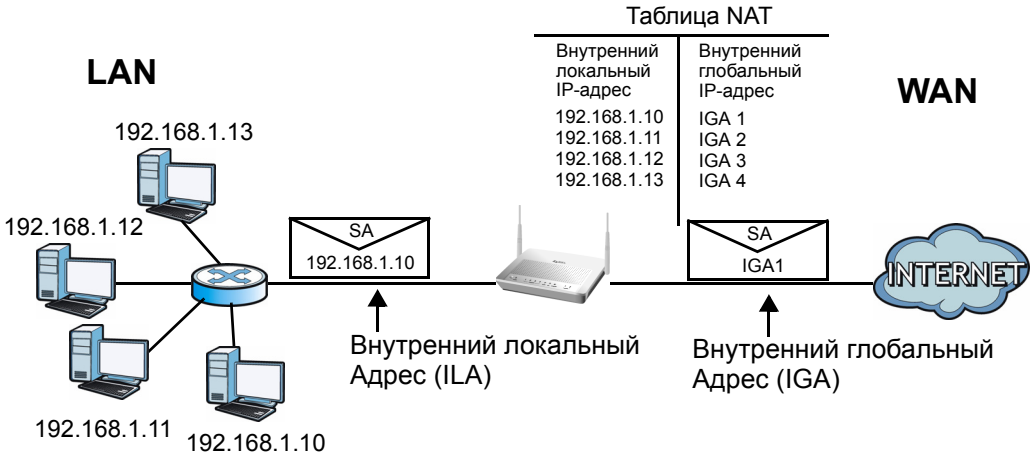
Глобальные IP-адреса внутренних узлов могут быть статическими, или могут динамически назначаться Интернет-провайдером. Кроме того, вы можете определить серверы, например, веб-сервер и сервер Telnet, находящиеся в вашей локальной сети, и сделать их доступными для внешних пользователей. Если вы не определили серверы (с отображением «много-к-одному» и «много-ко-многим с перегрузкой» – см. Табл. 42 на с. 135), NAT предлагает дополнительное преимущество защиты сети с помощью

брандмауэра. Если серверы не установлены, устройство P660HN отфильтровывает все входящие запросы, таким образом блокируя зондирование вашей сети злоумышленниками. Дополнительные сведения о трансляции IP-адресов см. в *RFC 1631*, «*Трансляция сетевых IP-адресов (NAT)*».

7.6.3 Как работает NAT

Каждый пакет содержит два адреса – адрес источника и адрес назначения. Для исходящих пакетов, внутренний локальный адрес (ILA) является адресом источника в локальной сети, а внутренний глобальный адрес (IGA) – адресом источника в глобальной сети. Для входящих пакетов ILA – это адрес назначения в локальной сети, а IGA – адрес назначения в глобальной сети. NAT 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. Устройство P660HN отслеживает оригинальные адреса и номера портов, и, таким образом, во входящих ответных пакетах восстанавливаются исходные значения. На рисунке ниже это представлено в графическом виде.

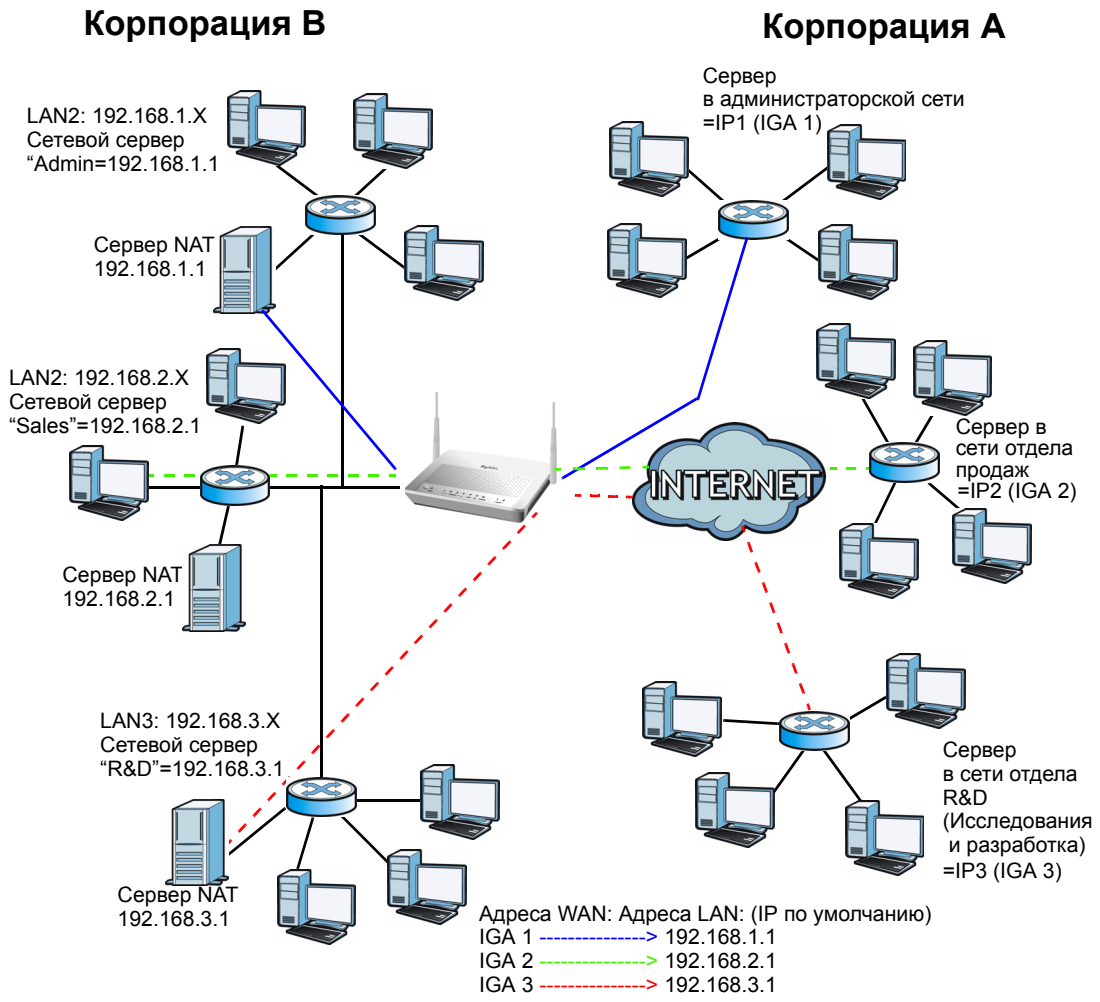
Рис. 58 Как работает NAT



7.6.4 Применение NAT

На следующем рисунке приведен вариант применения NAT, где три внутренних локальных сети (логические локальные сети, образованные с помощью псевдонимов IP), расположенные за устройством P660HN, взаимодействуют с тремя различными глобальными сетями.

Рис. 59 Применение NAT с использованием псевдонимов IP



7.6.5 Типы отображения NAT

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

- **One to One**: В режиме один-к-одному устройство P660HN отображает один локальный IP-адрес на один глобальный IP-адрес.
- **Many to One**: В режиме много-к-одному устройство P660HN отображает несколько локальных IP-адресов на 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** в современных маршрутизаторах).

- **Many to Many Overload**: В режиме много-ко-многим с перегрузкой устройство P660HN отображает множество локальных IP-адресов в несколько совместно используемых глобальных IP-адресов.
- **Many-to-Many No Overload**: В режиме много-ко-многим без перегрузки устройство P660HN отображает каждый локальный IP-адрес в уникальный глобальный IP-адрес.
- **Server**: Этот режим позволяет установить внутренний сервер различных служб после преобразования NAT для доступа внешних пользователей.

Номера портов НЕ изменяются при использовании типов отображения NAT **One-to-One** и **Many-to-Many No Overload**.

В следующей таблице приведена сводная информация о типах NAT.

Табл. 42 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

Часть III
Безопасность

8

Брандмауэр (Firewall)

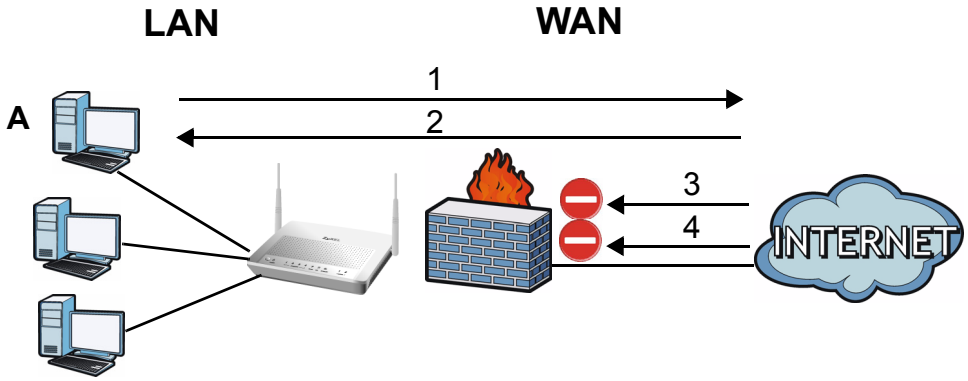
8.1 Обзор

В этой главе рассказывается, как включить и настроить брандмауэр устройства P660HN. Эти экраны используются для включения и настройки брандмауэра, защищающего устройство P660HN и сеть от атак хакеров в Интернете и управляющего доступом к устройству. По умолчанию, брандмауэр обладает следующими свойствами:

- обеспечивает трафик из компьютеров сети LAN во все остальные сети;
- блокирует попадание в локальную сеть LAN трафика, порождаемого в других сетях;

На рисунке показаны основные действия брандмауэра, задаваемые по умолчанию. Пользователь **A** может инициировать сессию IM (Instant Messaging – Мгновенный обмен сообщениями) из локальной сети LAN в глобальную сеть WAN (**1**). Обратный трафик для данной сессии также разрешен (**2**). Однако, другой трафик, инициируемый со стороны WAN, блокируется (**3** и **4**).

Рис. 60 Работа брандмауэра по умолчанию



8.1.1 Что можно сделать на экране брандмауэра

- Экран **General** (Разд. 8.2 на с. 142) используется для включения брандмауэра и треугольного маршрута на устройстве P660HN и установки действия по умолчанию, которое выполняется для пакетов, не соответствующих ни одному из правил брандмауэра.
- Экран **Rules** (Разд. 8.3 на с. 144) используется для просмотра настроенных правил брандмауэра, а также для добавления, редактирования или удаления правил брандмауэра.
- Экран **Threshold** (Разд. 8.4 на с. 150) используется для настройки порогов, использующихся устройством P660HN для определения того, когда следует сбросить сеанс связи, находящийся в процессе установления соединения (полуоткрытые сеансы связи).

8.1.2 Что нужно знать о брандмауэре

DoS

Атаки типа «Отказ в обслуживании» (DoS) нацелены на устройства и сети, подключенные к Интернету. Их цель не украсть информацию, а отключить устройство или сеть с тем, чтобы пользователи не могли больше иметь доступ к сетевым ресурсам.

Предотвращение зондирования

Если внешний пользователь попытается прозондировать неподдерживаемый порт устройства P660HN, ему будет автоматически отправлен ответный пакет ICMP. Это позволяет внешнему пользователю узнать о существовании устройства P660HN. Также устройство P660HN поддерживает блокирование зондирования без отправки ответного пакета ICMP. Это позволяет скрыть существование устройства P660HN от посторонних лиц при попытке зондирования неподдерживаемого порта.

Протокол управляющих сообщений в сети Интернет (ICMP)

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 Интернет-протокола (IP), но сообщения обрабатываются программным обеспечением TCP/IP, и напрямую видимы пользователю приложений.

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

Для атак типа DoS устройство P660HN применяет пороги, которые определяют, когда следует сбросить сеанс связи, находящийся в процессе установления соединения. Эти пороги универсально применяются для всех сеансов связи. Можно использовать значения порога, установленные по умолчанию, или изменить их до значений, более подходящих к требованиям безопасности.

Дополнительные сведения

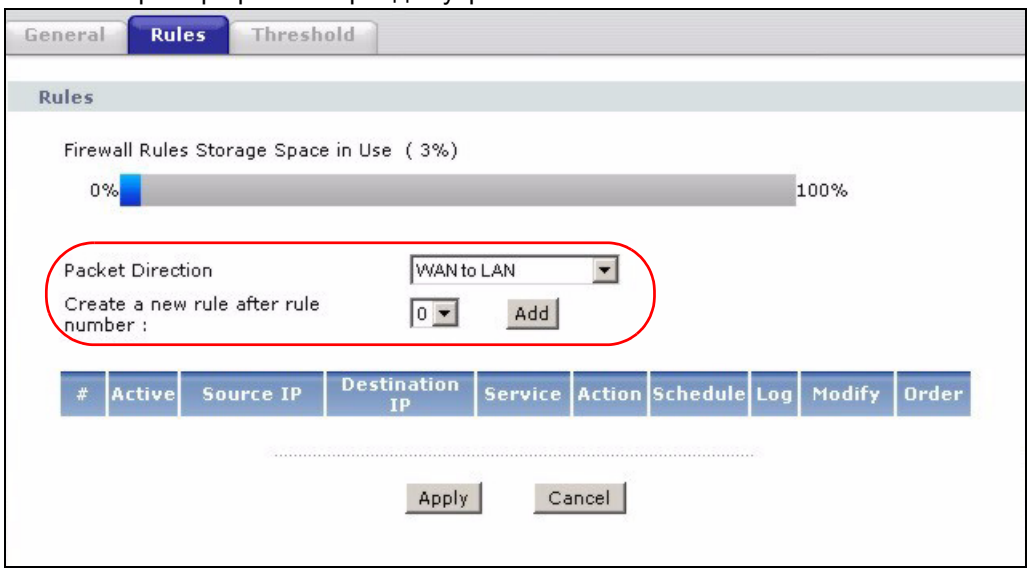
- Пример настройки брандмауэра см. в Разд. 8.1.3 на с. 139.
- Техническую вводную информацию о брандмауэре см. в Разд. 8.5 на с. 153.

8.1.3 Пример настройки правила брандмауэра

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

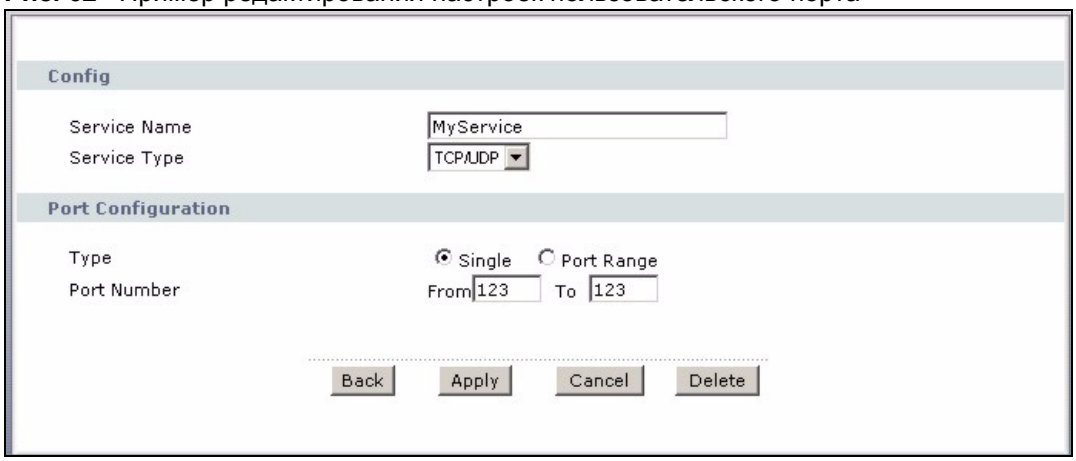
1. Нажмите **Security > Firewall** > **Rules**.
2. Выберите **WAN to LAN** в поле **Packet Direction**.

Рис. 61 Пример правила брандмауэра: Rules



3. На экране **Rule** 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 **Add** для отображения экрана настройки правил брандмауэра.
5. На экране **Edit Rule** щелкните по ссылке **Edit Customized Services** для отображения экрана **Customized Service**.
6. Выберите порядковый номер правила, при этом откроется экран **Customized Services Config**, введите указанные ниже параметры и нажмите **Apply**.

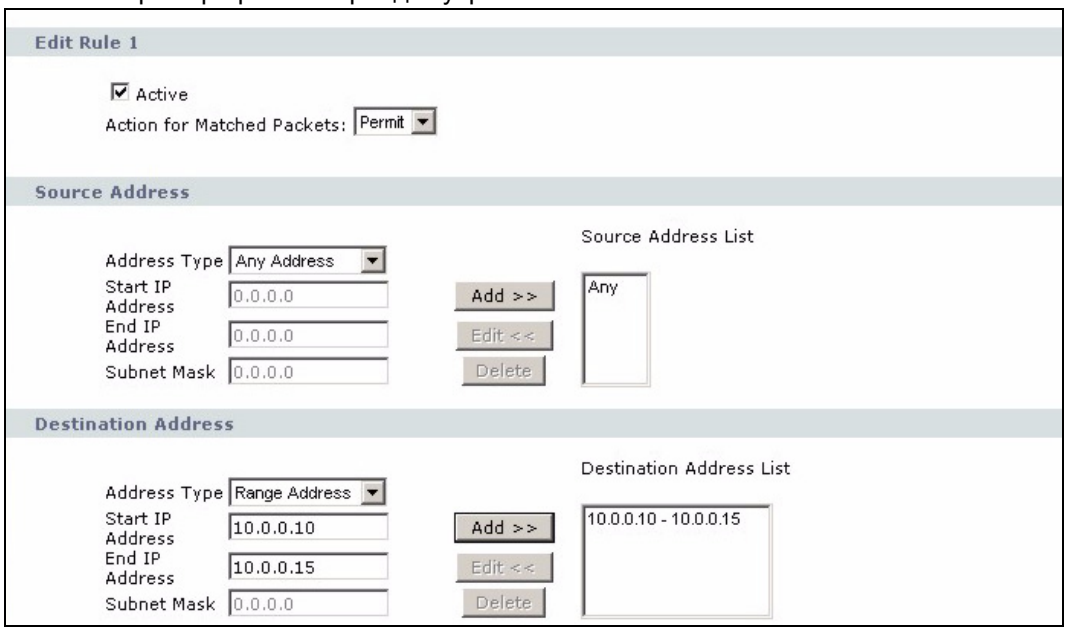
Рис. 62 Пример редактирования настроек пользовательского порта



7. Выберите **Any** в окне **Destination Address List**, а затем нажмите **Delete**.

8 Выполните настройки на экране адреса получателя, как показано ниже и нажмите кнопку **Add**.

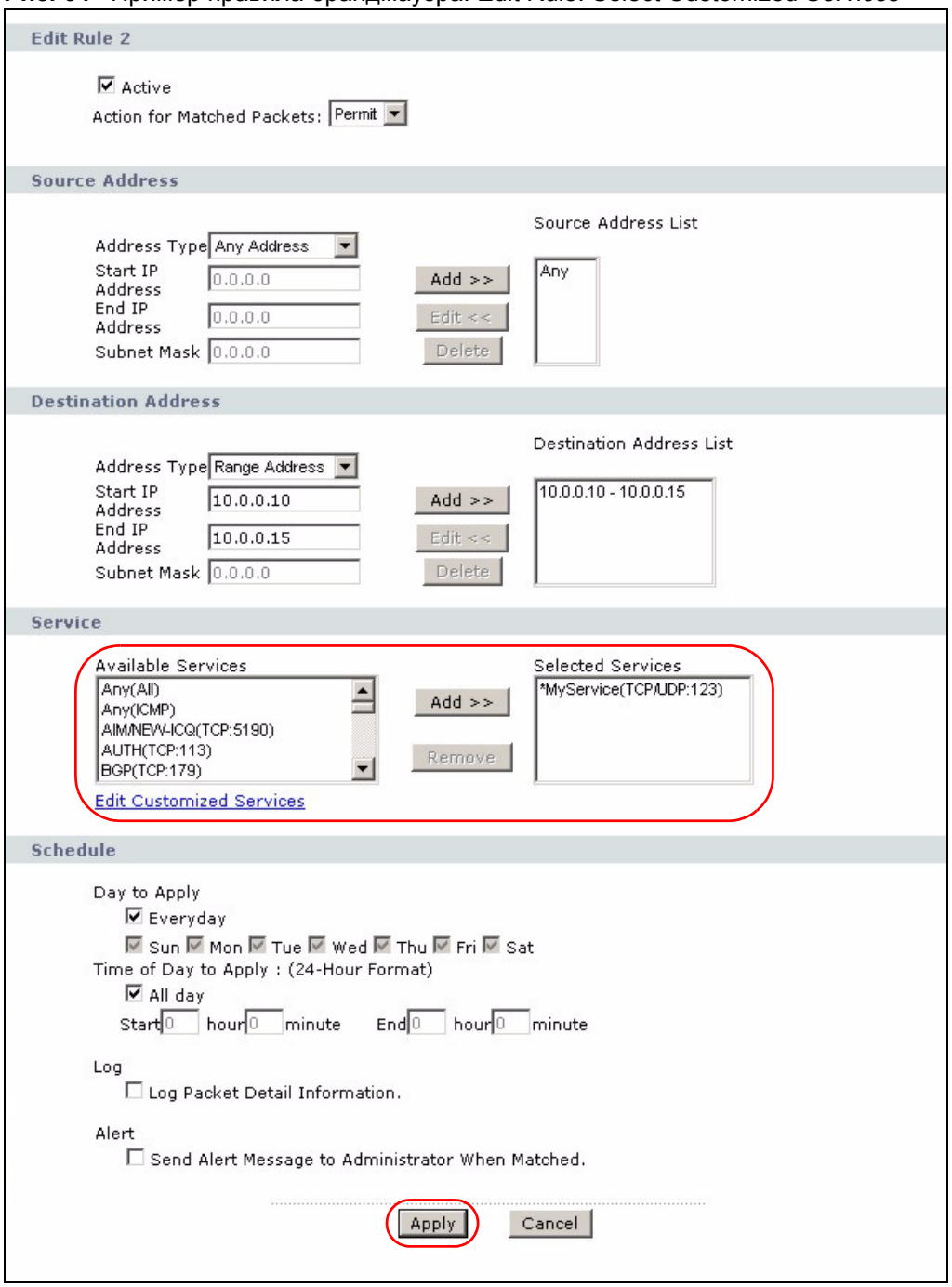
Рис. 63 Пример правила брандмауэра: Edit Rule: Destination Address



9 С помощью кнопок **Add >>** и **Remove** между полями со списками **Available Services** и **Selected Services** установите параметры, как показано ниже. По окончании нажмите **Apply**.

В списках **Services** и **Rules** пользовательские службы отмечены символом «*» перед именем.

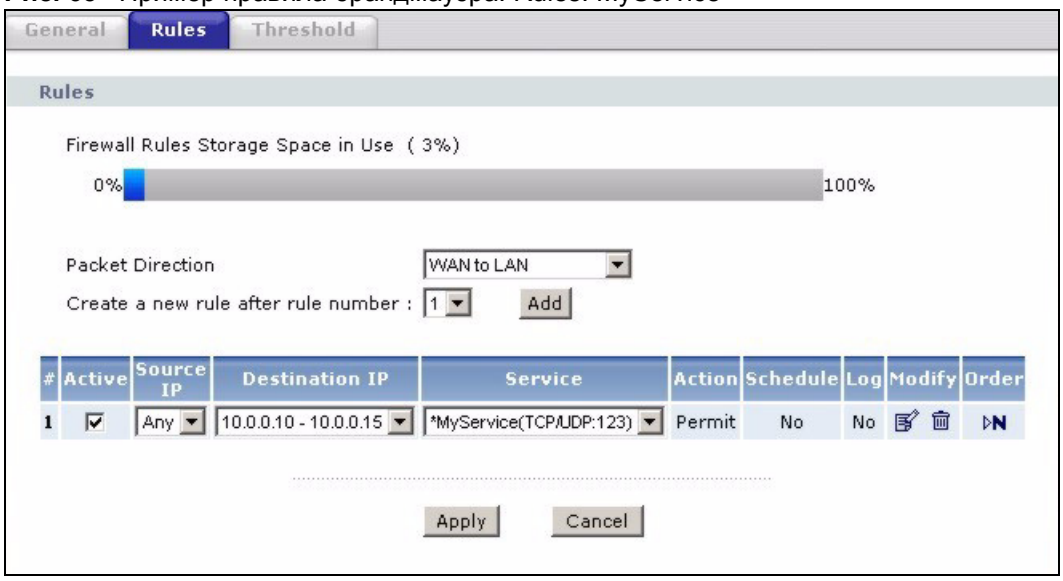
Рис. 64 Пример правила брандмауэра: Edit Rule: Select Customized Services



По завершении настройки правила брандмауэра для Интернета, экран **Rules** должен 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.

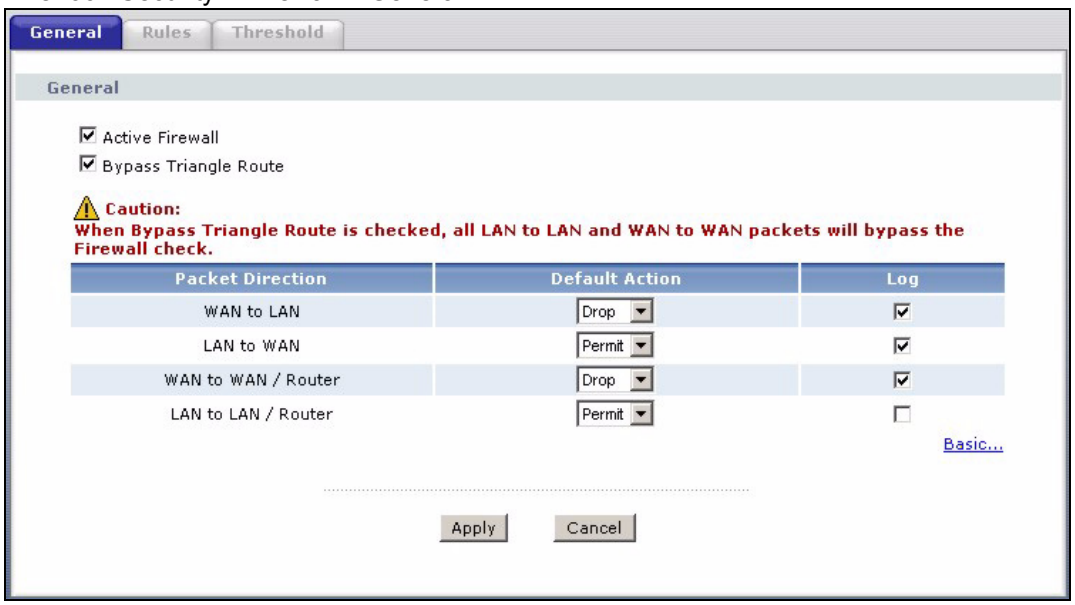
Рис. 65 Пример правила брандмауэра: Rules: MyService



8.2 Экран общей настройки брандмауэра

Этот экран используется для настройки параметров брандмауэра. Нажмите **Security** > **Firewall** для отображения следующего экрана.

Рис. 66 Security > Firewall > General



В следующей таблице даны описания полей этого экрана.

Табл. 43 Security > Firewall > General

ПОЛЕ	ОПИСАНИЕ
Active Firewall	Поставьте флажок для включения брандмауэра. Если брандмауэр включен, устройство P660HN осуществляет управление доступом и защиту от атак типа DoS.
Bypass Triangle Route	Если в локальной сети имеется шлюз с IP-адресом, входящим в ту же подсеть, что и устройство P660HN, то обратный трафик может и не проходить через устройство P660HN. Такой маршрут называется асимметричным или «треугольным». В результате устройство P660HN сбрасывает соединение, так как для этого соединения отсутствует подтверждение. Установите этот флажок, чтобы настроить устройство P660HN на работу с асимметричными маршрутами (чтобы он не разрывал подключение). Примечание: Использование несимметричных маршрутов может привести к передаче трафика из глобальной сети прямо к компьютеру локальной сети без прохождения через устройство P660HN. Лучше воспользоваться псевдонимом IP, чтобы поместить устройство P660HN и резервный шлюз в разные подсети. Пример см. в Разд. 8.5.4.1 на с. 156.
Packet Direction	Это направление движения пакетов (**LAN to LAN / Router**, **LAN to WAN**, **WAN to WAN / Router**, **WAN to LAN**). Правила брандмауэра группируются по направлениям движения пакетов, к которым они применяются. Например, направление **LAN to LAN / Router** означает, что пакеты передаются от компьютера/подсети в локальной сети к другому компьютеру/подсети, подключенному к интерфейсу LAN устройства P660HN или к самому устройству P660HN.
Default Action	Из выпадающего списка выберите действие по умолчанию, которое брандмауэр выполняет для пакетов, которые перемещаются в выбранном направлении и не соответствуют ни одному из правил брандмауэра. Выберите **Drop** для сброса пакетов без предупреждения и без отправки пакета сброса TCP или сообщения ICMP отправителю о недоступности адресата. Выберите **Reject** чтобы не принимать пакеты и отправить пакет сброса TCP (для пакетов TCP) или сообщение ICMP отправителю о недоступности адресата (для пакетов UDP). Выберите **Permit**, чтобы разрешить прохождение пакетов.
Log	Установите флажок для ведения журнала регистрации (когда производится выбранное выше действие) для пакетов, которые перемещаются в выбранном направлении и не соответствуют ни одному из правил брандмауэра.
Expand...	Нажмите эту кнопку для отображения дополнительных параметров.
Basic...	Нажмите эту кнопку, чтобы дополнительные параметры не отображались.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

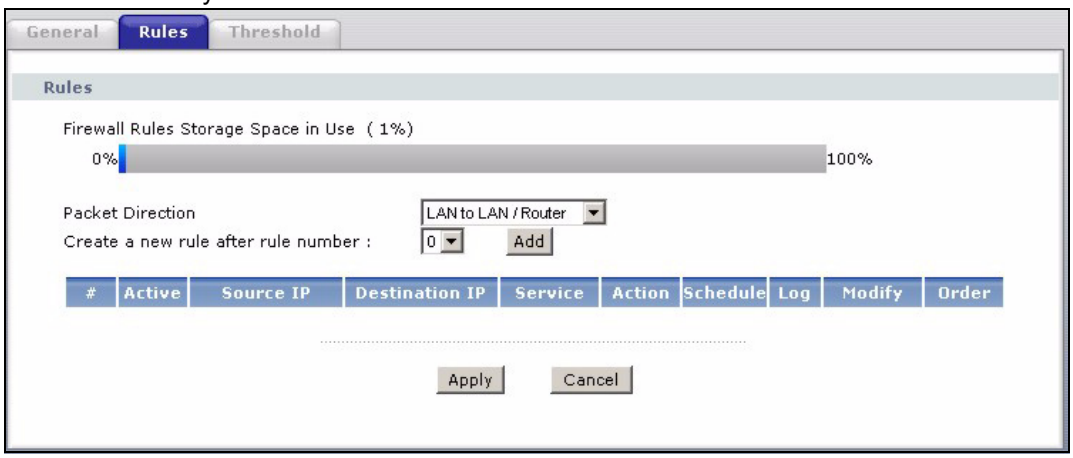
8.3 Экран правил брандмауэра

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

Более подробную информацию см. в Разд. 8.5 на с. 153.

Нажмите **Security > Firewall > Rules** для отображения следующего окна. На этом экране отображается список установленных правил брандмауэра. Следует обратить внимание на тот порядок, в котором они перечислены.

Рис. 67 Security > Firewall > Rules



В следующей таблице даны описания полей этого экрана.

Табл. 44 Security > Firewall > Rules

ПОЛЕ	ОПИСАНИЕ
Firewall Rules Storage Space in Use	Этот информационный индикатор показывает, какая часть памяти устройства P660HN, предназначенная для записи правил брандмауэра, находится в использовании. Если занято 80 % памяти или менее, индикатор будет зеленого цвета. Если занято свыше 80 % памяти, индикатор будет красного цвета.
Packet Direction	Для выбора направления передачи пакетов, для которых необходимо сконфигурировать правила брандмауэра, используйте выпадающий список.
Create a new rule after rule number	Выберите порядковый номер и нажмите **Add**, чтобы добавить новое правило брандмауэра 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.
	В указанных ниже полях (доступных только для чтения) отображается созданный вами свод правил, который предназначен к применению в отношении передачи пакетов данных в указанном направлении. Установленные правила брандмауэра (в таблице ниже) имеют приоритет над общими настройками брандмауэра, установленными на экране **General**.
#	Номер правила брандмауэра. Порядок расположения правил имеет большое значение, так как правила выполняются по очереди.
Active	В этом поле отображается состояние брандмауэра: включен или отключен. Поставьте флажок в это поле для включения данного правила. Чтобы отключить данное правило, снимите флажок.

Табл. 44 Security > Firewall > Rules (продолжение)

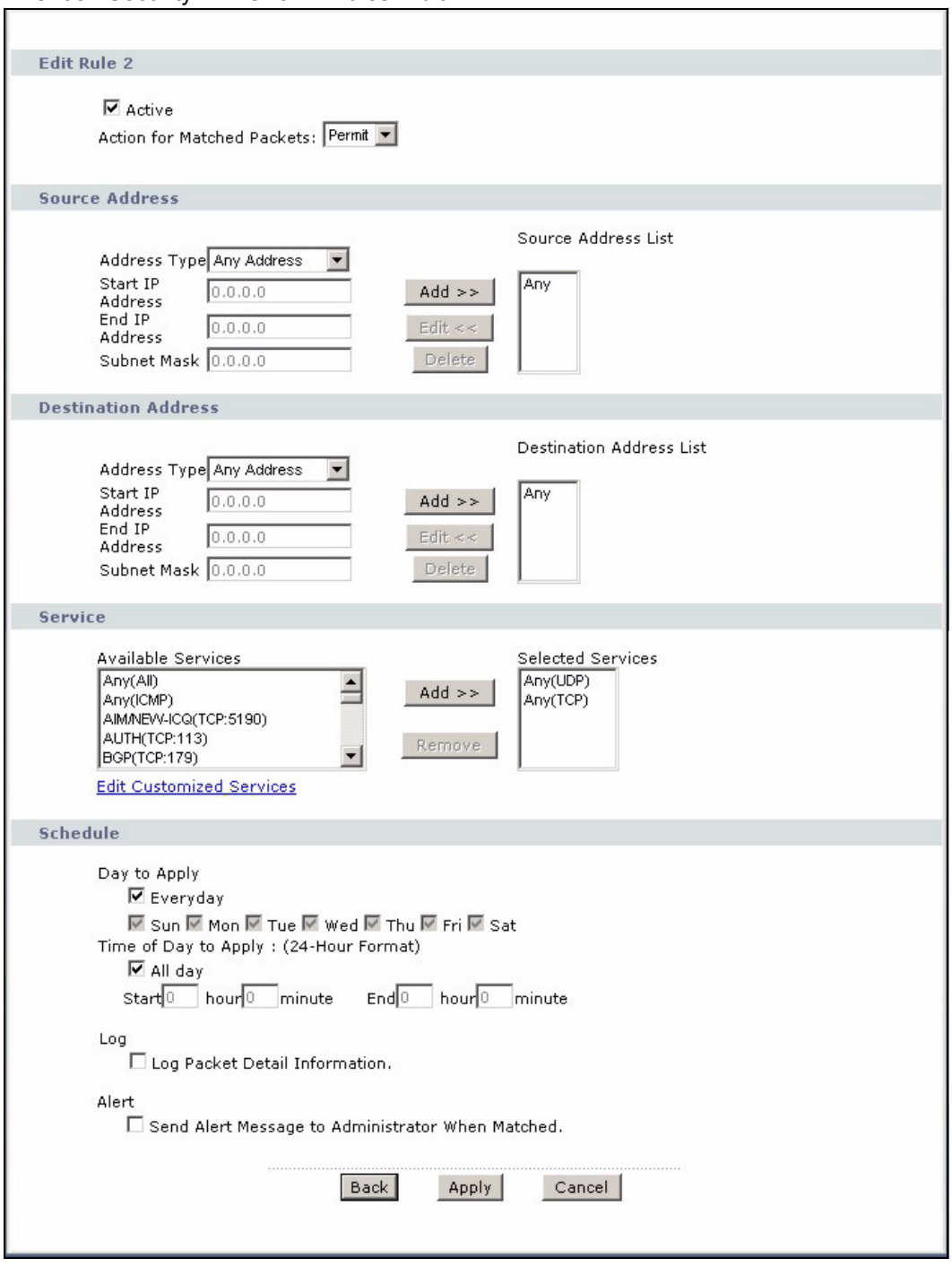
ПОЛЕ	ОПИСАНИЕ
Source IP	Поле с выпадающим списком показывает адреса или диапазон адресов источников, к которым применяются правила брандмауэра. Заметьте, что отсутствие адреса источника или назначения эквивалентно выбору **Any**.
Destination IP	Поле с выпадающим списком показывает адреса или диапазон адресов назначения, к которым применяются правила брандмауэра. Заметьте, что отсутствие адреса источника или назначения эквивалентно выбору **Any**.
Service	Поле с выпадающим списком содержит службы, к которым применяется правило брандмауэра. Более подробную информацию см. в Прил. E на с. 354.
Action	В этом поле отображается одно из следующих значений: **Drop** – брандмауэр сбрасывает пакеты без предупреждения, **Reject** – брандмауэр сбрасывает пакеты и отправляет пакет сброса TCP или сообщение ICMP отправителю о недоступности адресата, **Permit** – брандмауэр разрешает прохождение пакетов.
Schedule	Это поле показывает, определено или нет расписание: **Yes** или **No**.
Log	Это поле показывает, создается ли запись в журнале регистрации, при соответствии пакетов данному правилу: **Yes** или **No**.
Modify	Щелкните по иконке редактирования для перехода к экрану, где можно менять параметры правила. Для удаления существующего правила брандмауэра щелкните по иконке удаления. Появляется окно с запросом на подтверждение операции удаления правила брандмауэра. Следует помнить, что при удалении одного правила все последующие сдвигаются на позицию вверх.
Order	Щелкните по иконке перемещения для отображения поля **Move the rule to**. В поле **Move the rule to** введите число и нажмите кнопку **Move**, чтобы переместить правило на позицию с указанным номером. Порядок расположения правил имеет большое значение, так как правила выполняются в порядке своих номеров.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

8.3.1 Настройка правил брандмауэра

Более подробную информацию см. в Разд. 8.1.2 на с. 138.

Этот экран используется для конфигурирования правил брандмауэра. На экране **Rules** выберите порядковый номер и нажмите **Add** или щелкните по иконке **Edit** для отображения этого экрана. В таблице представлена информация по заполнению полей этого экрана.

Рис. 68 Security > Firewall > Rules: Edit



В следующей таблице даны описания полей этого экрана.

Табл. 45 Security > Firewall > Rules: Edit

ПОЛЕ	ОПИСАНИЕ
Edit Rule	
Active	Выберите эту опцию, чтобы задействовать данное правило брандмауэра.
Action for Matched Packet	Используйте выпадающий список для выбора: сбросить (**Drop**), отказать и отправить сообщение ICMP отправителю о недоступности адресата (**Reject**) или разрешить (**Permit**) прохождение пакетов, соответствующих этому правилу.
Source/Destination Address	
Address Type	Вы хотите, чтобы правило применялось к пакетам с индивидуальным (единичным) IP-адресом, диапазону IP-адресов (напр., от 192.168.1.10 до 192.169.1.50), подсети или любому IP-адресу? Выберите свойство из выпадающего списка этого поля, который включает: **Single Address**, **Range Address**, **Subnet Address** и **Any Address**.
Start IP Address	Введите одиночный IP-адрес или начальный IP-адрес в группе.
End IP Address	Введите конечный IP-адрес группы.
Subnet Mask	Если нужно, введите маску подсети.
Add >>	Нажмите кнопку **Add >>**, чтобы добавить новый адрес в поле **Source** или **Destination Address**. Добавлять можно группы адресов, диапазоны адресов, и/или подсети.
Edit <<	Чтобы изменить существующий адрес источника или назначения, выделите его в соответствующем поле и нажмите **Edit<<**.
Delete	Выделите существующий адрес источника или получателя в поле **Source** или **Destination Address** и нажмите кнопку **Delete**, чтобы удалить его.
Services	
Available/ Selected Services	Более подробную информацию об имеющихся службах см. в Прил. E на с. 354. Выделите одну из служб в списке **Available Services** слева, затем нажмите **Add >>**, чтобы добавить ее в список **Selected Services** справа. Для удаления службы, выделите ее в поле **Selected Services** справа, затем нажмите **Remove**.
Edit Customized Service	Щелкните по ссылке **Edit Customized Services**, чтобы открыть экран, позволяющий настроить новую службу, отсутствующую в стандартном списке служб.
Schedule	
Day to Apply	Выберите, должно ли правило применяться каждый день (Everyday) или в определенные дни недели.
Time of Day to Apply (24-Hour Format)	Выберите **All Day** или введите время начала и окончания применения правила в часах и минутах.
Log	
Log Packet Detail Information	Это поле определяет, создается или нет запись в журнале регистрации для пакетов, соответствующих данному правилу. Перейдите на страницу **Log Settings** и выберите категорию **Access Control**, чтобы включить ведение журналов регистрации устройства P660HN.
Alert	
Send Alert Message to Administrator When Matched	Поставьте флажок, чтобы устройство P660HN генерировало извещение, если происходит событие, соответствующее условиям данного правила.

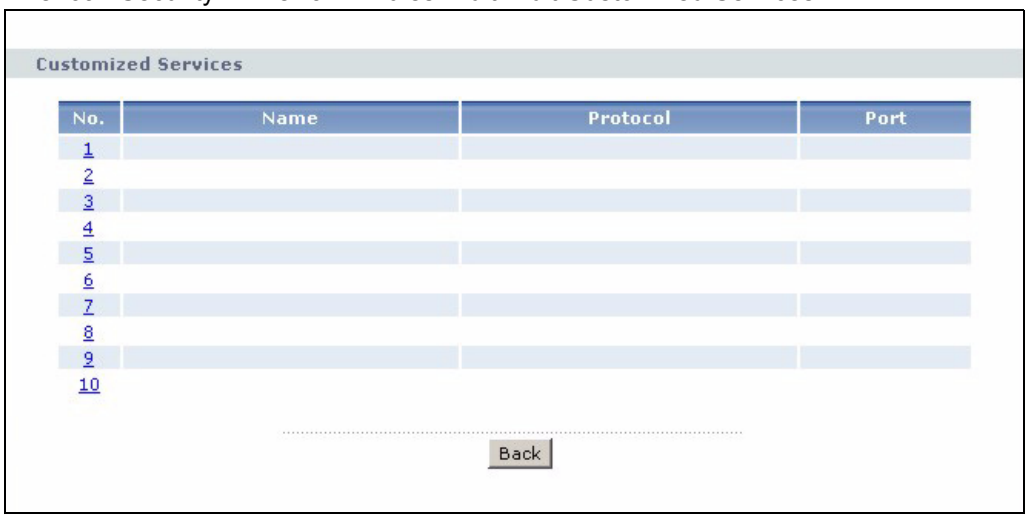
Табл. 45 Security > Firewall > Rules: Edit (продолжение)

ПОЛЕ	ОПИСАНИЕ
Back	Нажмите эту кнопку для возврата к предыдущему экрану без сохранения.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

8.3.2 Пользовательские службы

В брандмауэре устройства P660HN можно настроить пользовательские службы и соответствующие им номера портов. Посетите Web-сайт IANA (Агентство по назначению имен и уникальных параметров протоколов Интернет), на котором представлен полный перечень номеров портов и услуг. Примеры представлены в Прил. E на с. 354. Щелкните по ссылке **Edit Customized Services** в окне редактирования правил брандмауэра, чтобы установить для пользовательской службы номер порта. При этом откроется следующий экран.

Рис. 69 Security > Firewall > Rules: Edit: Edit Customized Services



В следующей таблице даны описания полей этого экрана.

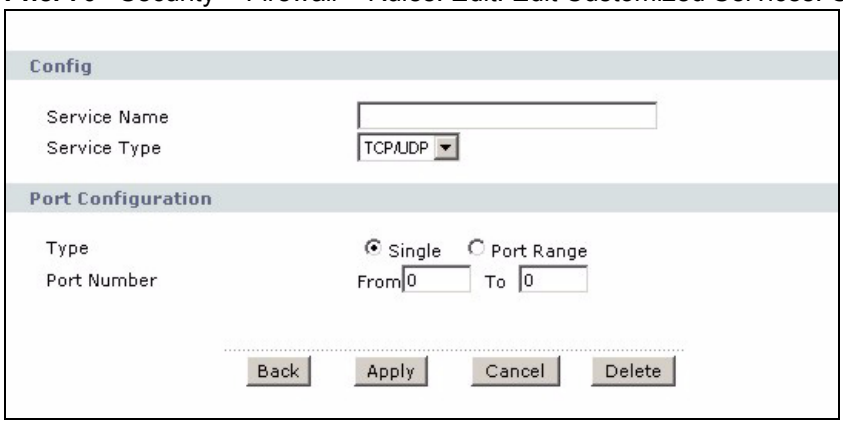
Табл. 46 Security > Firewall > Rules: Edit: Edit Customized Services

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

8.3.3 Настройка пользовательских служб

Данный экран используется для добавления пользовательских правил и редактирования существующих правил. Выберите номер правила на экране **Firewall Customized Services** для отображения следующего экрана.

Рис. 70 Security > Firewall > Rules: Edit: Edit Customized Services: Config



В следующей таблице даны описания полей этого экрана.

Табл. 47 Security > Firewall > Rules: Edit: Edit Customized Services: Config

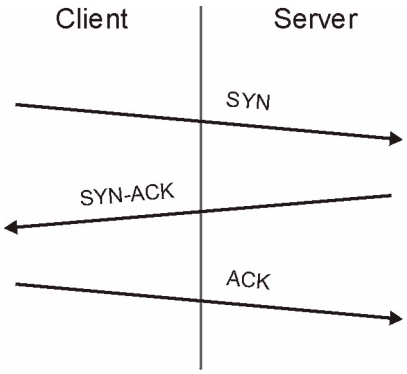
ПОЛЕ	ОПИСАНИЕ
Config	
Service Name	Введите уникальное имя для пользовательского порта.
Service Type	Выберите порт IP (**TCP**, **UDP** или **TCP/UDP**), который определяет пользовательский порт.
Port Configuration	
Type	Нажмите **Single** для установления только одного порта или **Range** для установления диапазона портов, которые определяют пользовательскую услугу.
Port Number	Введите единичный номер порта или диапазон номеров порта, которые определяют пользовательскую услугу.
Back	Нажмите эту кнопку для возврата к предыдущему экрану без сохранения.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.
Delete	Нажмите эту кнопку для удаления текущего правила.

8.4 Экран настройки порога брандмауэра

Для атак типа DoS устройство P660HN использует пороги для определения того, когда следует сбросить сеанс связи, находящийся в процессе установления соединения (полуоткрытые сеансы связи). Эти пороги универсально применяются для всех сеансов связи.

Для TCP, «полуоткрытый» означает, что сеанс связи не достиг установленного состояния – трехстороннее квитирование TCP еще не завершено. При нормальных обстоятельствах, приложение, которое инициирует сеанс связи посылает пакет SYN (синхронизация) на принимающий сервер. Приемник отправляет назад пакет ACK (уведомление) и свой собственный SYN, а затем инициатор отвечает ACK (уведомление). После этого квитирования устанавливается соединение.

Рис. 71 Трехстороннее квитирование



Для UDP, «полуоткрытый» означает, что брандмауэр не обнаружил обратного трафика. Слишком большое количество полуоткрытых сеансов связи (в виде частоты поступлений) может означать наличие атаки DOS.

8.4.1 Значения порога

Если все работает надлежащим образом, возможно, нет необходимости изменять настройки порогов. Значения, установленные по умолчанию, хорошо подходят для небольших офисов. Эти параметры нужно настроить в случае, если вы думаете, что устройство P660HN испытывало атаки DoS, не зафиксированные в журналах, или журналы показывают, что устройство P660HN классифицирует стандартный трафик, как атаки DoS. Факторы, влияющие на опции для значений порога, следующие:

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

Если сеть медленнее, чем средние значения любого из этих факторов (особенно, если имеются сервера, которые медленно работают или обрабатывают много задач и часто заняты), тогда величины порогов необходимо уменьшить.

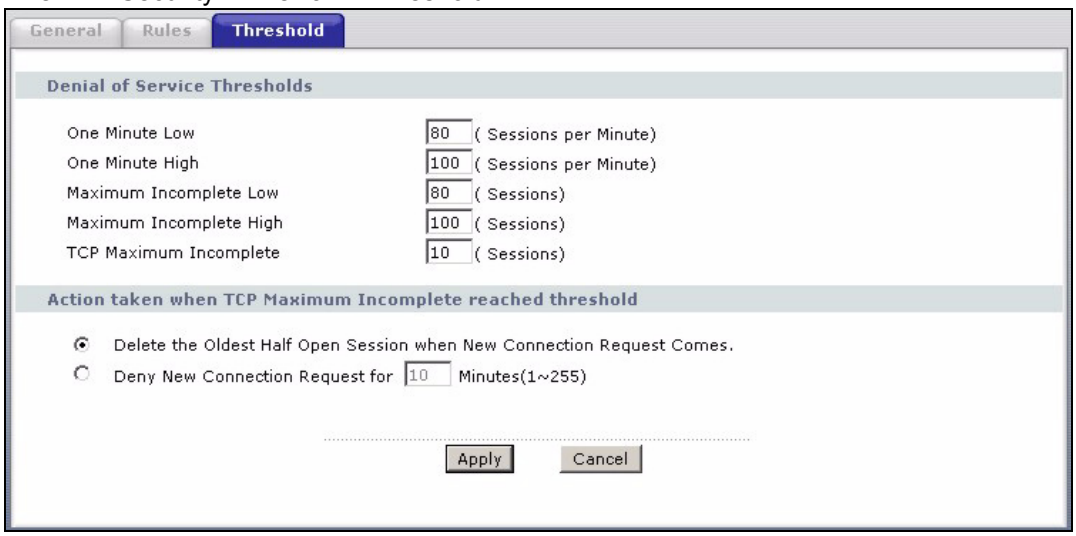
- Если вы часто используете приложения P2P (например, обмен файлами с помощью eMule или BitTorrent), рекомендуется увеличить величины порогов, так как в течение небольшого периода времени устанавливается большое количество сеансов, и устройство P660HN может классифицировать их как атаки DoS.

8.4.2 Настройка порогов брандмауэра

Устройство P660HN также посылает извещения, каждый раз, когда превышается значение **TCP Maximum Incomplete**. Общие значения, определенные для допустимого порога и интервала простоя, применимы ко всем TCP соединениям.

Нажмите **Firewall** > **Threshold**, чтобы открыть следующий экран.

Рис. 72 Security > Firewall > Threshold



В следующей таблице даны описания полей этого экрана.

Табл. 48 Security > Firewall > Threshold

ПОЛЕ	ОПИСАНИЕ
Denial of Service Thresholds	Устройство P660HN измеряет общее количество существующих полуоткрытых сеансов и интенсивность попыток установления сеансов. Полуоткрытые сеансы связи TCP и UDP подсчитываются по общему числу и интенсивности. Измерения производятся раз в минуту.
One Minute Low	В этом поле отображается интенсивность новых полуоткрытых сеансов связи в минуту, обуславливающая брандмауэр прекратить удаление полуоткрытых сеансов связи. Устройство P660HN удаляет полуоткрытые сеансы до тех пор, пока значение интенсивности новых попыток установления соединения не станет меньше, чем это число.

Табл. 48 Security > Firewall > Threshold (продолжение)

ПОЛЕ	ОПИСАНИЕ
One Minute High	В этом поле отображается интенсивность новых полуоткрытых сеансов связи в минуту, обуславливающая брандмауэр начать удаление полуоткрытых сеансов связи. Когда интенсивность новых попыток установления соединения превышает это число, устройство P660HN начинает удалять полуоткрытые сеансы связи для выполнения новых запросов на установление соединения. Например, если вы установите в поле «One Minute High» значение 100, устройство P660HN начнет удалять полуоткрытые соединения, как только в течение последней минуты будет зафиксировано более 100 попыток установки соединения. Оно прекратит удалять полуоткрытые соединения, когда в течение последней минуты будет зафиксировано попыток менее числа, установленного в поле «One Minute Low».
Maximum Incomplete Low	Количество существующих полуоткрытых соединений при котором брандмауэр прекращает удалять полуоткрытые соединения. Устройство P660HN удаляет полуоткрытые сеансы до тех пор, пока количество существующих полуоткрытых соединений не станет меньше, чем это число.
Maximum Incomplete High	Количество существующих полуоткрытых соединений, при котором брандмауэр начинает удалять полуоткрытые соединения. Когда количество существующих полуоткрытых сеансов связи превышает это число, устройство P660HN начинает удалять полуоткрытые сеансы связи для выполнения новых запросов на установление соединений. Нельзя устанавливать значение **Maximum Incomplete High** ниже текущего значения **Maximum Incomplete Low**. Например, если в поле «Maximum Incomplete High» установлено значение 100, то устройство P660HN начнет удалять полуоткрытые соединения, как только количество существующих полуоткрытых соединений превысит 100. Оно прекратит удалять полуоткрытые соединения, если количество текущих полуоткрытых сеансов станет меньше числа, установленного в поле «Maximum Incomplete Low».
TCP Maximum Incomplete	Необычно высокое число полуоткрытых сеансов связи с одинаковым адресом целевого узла может указывать на то, что против узла осуществляется атака DoS. Укажите количество существующих полуоткрытых соединений через TCP с одним и тем же IP-адресом получателя, при котором брандмауэр 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. Устройство P660HN посылает извещения, каждый раз, когда превышается значение **TCP Maximum Incomplete**.
Action taken when TCP Maximum Incomplete reached threshold	Выберите действие, которое устройство P660HN должно выполнить при достижении максимального количества полуоткрытых TCP-соединений. Устройство P660HN можно настроить на выполнение следующих действий. Удалить самое старое полуоткрытое соединение при получении запроса на новое соединение или Не принимать запросы на новое соединение в течение указанного количества минут (между 1 и 255).
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

8.5 Техническая информация о брандмауэре

В этом разделе приводится некоторая вводная техническая информация по темам данной главы.

8.5.1 Обзор правил брандмауэра

Правила, установленные пользователем, имеют более высокий приоритет по отношению к настройкам по умолчанию устройства P660HN и замещают их. Устройство P660HN проверяет IP-адрес источника, IP-адрес назначения, а также тип протокола IP сетевого трафика на соответствие правилам брандмауэра (в указанном вами порядке). Если трафик соответствует правилу, устройство P660HN выполняет действие, заданное правилом.

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

- Соединение одной локальной сети с другой (LAN–LAN) или с маршрутизатором
- Соединение локальной сети с глобальной сетью (LAN–WAN)
- Соединение глобальной сети с локальной сетью (WAN–LAN)
- Соединение одной глобальной сети с другой (WAN–WAN) или с маршрутизатором

Локальная сеть включает в себя как порты LAN, так и беспроводную сеть.

По умолчанию выполняемая устройством P660HN инспекция пакетов с учетом состояния разрешает прохождение пакетов в следующих направлениях:

- Соединение одной локальной сети с другой (LAN–LAN) или с маршрутизатором

  В этих правилах указывается, какие компьютеры в локальной сети могут управлять устройством P660HN (удаленное управление) обмениваться данными с сетями и подсетями, подключенными к порту локальной сети (IP alias).

Можно также настроить параметры удаленного управления так, чтобы только конкретный компьютер мог управлять устройством P660HN.

- Соединение локальной сети с глобальной сетью (LAN–WAN)

  В этих правилах указывается, какие компьютеры локальной сети имеют доступ к каким компьютерам или услугам в глобальной сети.

По умолчанию выполняемая устройством P660HN инспекция пакетов с учетом состояния отбрасывает пакеты, передаваемые в следующих направлениях:

- Соединение глобальной сети с локальной сетью (WAN–LAN)

  В этих правилах указывается, какие компьютеры глобальной сети имеют доступ к каким компьютерам или услугам в локальной сети.

Необходимо также задать правило переадресации порта NAT (полный набор правил отображения адресов NAT), чтобы предоставить компьютерам глобальной сети доступ к устройствам локальной сети.

- Соединение одной глобальной сети с другой (WAN–WAN) или с маршрутизатором
  По умолчанию устройство P660HN предотвращает управление устройством P660HN компьютерами глобальной сети или использование устройства P660HN в качестве шлюза для связи с другими компьютерами в глобальной сети. Одно из этих правил можно настроить таким образом, чтобы компьютер в глобальной сети мог управлять устройством P660HN.

Нужно также настроить параметры удаленного управления так, чтобы только компьютер в глобальной сети мог управлять устройством P660HN.

Можно определить дополнительные правила и установить или модифицировать существующие, но соблюдайте крайнюю осторожность в выполнении этого.

Например, можно создать правила для:

- Блокирования определенных типов трафика, как, например, IRC (Internet Relay Chat – Трансляция чатов в Интернет) из локальной сети в Интернет.
- Разрешения определенных типов трафика, как, например, синхронизация базы данных Lotus Notes из конкретных узлов в Интернет для конкретных узлов в локальной сети.
- Разрешения доступа к веб-серверу всем, кроме ваших конкурентов.
- Ограничения использования определенных протоколов, таких как, например, Telnet (теледоступ) санкционированным пользователям в 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 устройства P660HN и замещают их.

8.5.2 Методы усиления безопасности при помощи брандмауэра

1. Измените пароль по умолчанию при помощи Web-конфигуратора.
2. Подумайте о допуске к устройству до его подключения в сеть.
3. Ограничьте круг лиц, имеющих право доступа к маршрутизатору.
4. Не включайте никаких локальных служб (типа telnet или FTP), если вы их не используете. Любые включенные службы могут представлять потенциальный риск для безопасности. Некоторые хакеры могут найти оригинальные способы злоупотребления включенными службами для доступа к брандмауэру или сети.
5. Для включенных локальных служб должна применяться защита от злоупотребления. Установите защиту, сконфигурировав службы для связи только с одним конкретным клиентским устройством, и сконфигурировав правила для блокирования пакетов этих служб в конкретных интерфейсах.
6. Установите защиту от ложного IP-адреса, убедившись, что брандмауэр активен.
7. Само устройство брандмауэра должно находиться в недоступном (закрытом) помещении.

8.5.3 Информация о безопасности

Неправильная настройка брандмауэра может привести к блокированию допустимого доступа или к увеличению риска нарушения безопасности устройства P660HN и вашей защищенной сети. Будьте предельно внимательны при создании или удалении правил брандмауэра и перед конфигурированием правил протестируйте их.

Перед созданием правила необходимо рассмотреть те последствия, которые оно будет иметь для безопасности сети:

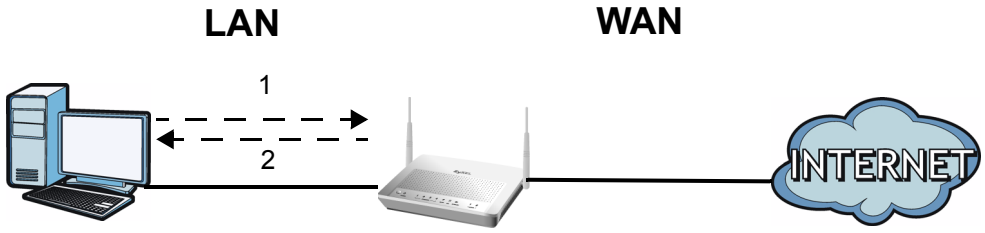
1. Блокирует ли это правило доступ пользователей LAN к важным ресурсам в Интернете? Например, если IRC блокируется, существуют ли пользователи, которым требуется эта услуга?
2. Возможно ли модифицировать правило так, чтобы оно было более конкретным? Например, если IRC блокировано для всех пользователей,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

Если ответы на эти вопросы известны, то добавление правил сведется к простому внесению данных в нужные поля на экранах Web-конфигуратора.

8.5.4 Треугольный маршрут

Если брандмауэр включен, устройство P660HN выступает в качестве безопасного шлюза между локальной сетью и Интернетом. При идеальной сетевой топологии весь входящий и исходящий сетевой трафик проходит через устройство P660HN, чтобы обеспечить защиту локальной сети от возможных атак.

Рис. 73 Образец настройки брандмауэра



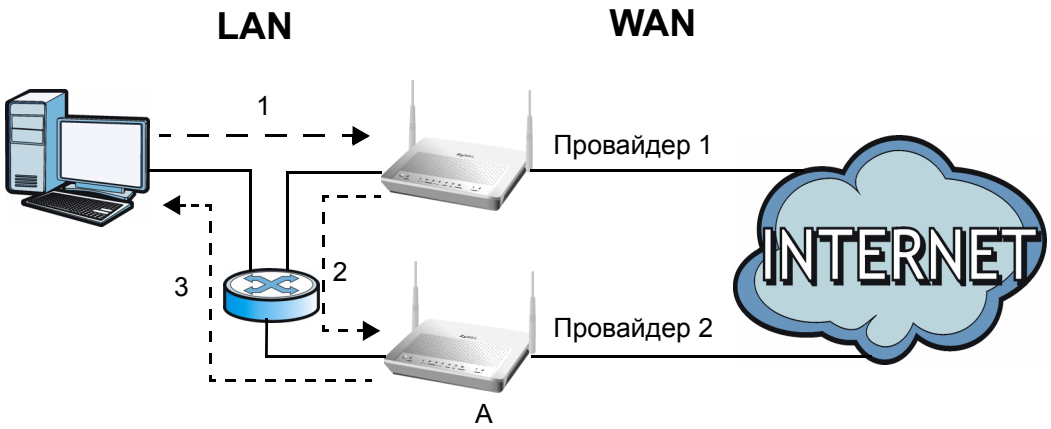
8.5.4.1 Проблема «треугольного маршрута»

Маршрут трафика – это путь для отправки или приема пакетов данных между двумя устройствами Ethernet. Возможно, у вас более одного соединения с Интернет (через одного или более Интернет-провайдеров). Если альтернативный шлюз находится в локальной сети (а его IP-адрес принадлежит той же подсети, что и LAN IP-адрес устройства P660HN), может возникнуть проблема «треугольного» маршрута (также называемого асимметричным). Проблему «треугольного маршрута» можно представить следующим образом.

1. Компьютер локальной сети инициирует соединение, посылая пакет SYN принимающему серверу в глобальной сети.
2. Устройство P660HN изменяет маршрут пакета SYN через шлюз **A** локальной сети в глобальную сеть.
3. Ответ из глобальной сети приходит прямо на компьютер локальной сети, минуя устройство P660HN.

В результате устройство P660HN сбрасывает соединение, так как для этого соединения отсутствует подтверждение.

Рис. 74 Проблема «треугольного маршрута»



8.5.4.2 Решение проблемы «треугольного маршрута»

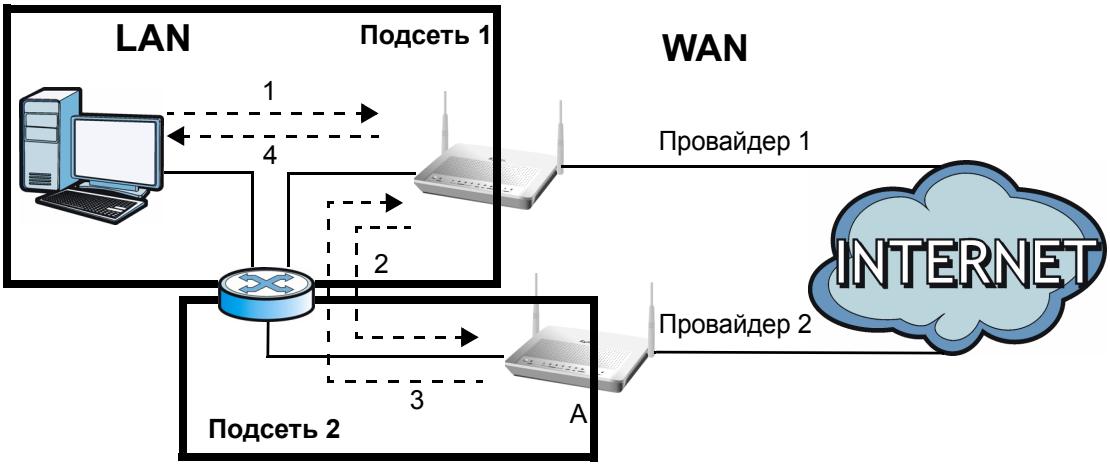
Если устройство P660HN настроено на использование сеансов треугольных маршрутов, трафик из WAN может напрямую поступать на компьютер LAN без прохождения через устройство P660HN и его брандмауэр.

Другое решение – это использование псевдонима IP (IP alias). Псевдоним IP позволяет разделить локальную сеть на несколько логических сегментов с использованием одного интерфейса Ethernet. Устройство P660HN поддерживает три логических интерфейса локальной сети, при этом устройство P660HN является шлюзом для каждой логической сети.

При этом одни и те же кабели и порты используются несколькими локальными сетями. При расположении локальной сети и шлюза «**A**» в разных подсетях весь сетевой трафик, возвращающийся в локальную сеть, должен проходить через устройство P660HN. Это можно представить с помощью следующего сценария.

1. Компьютер локальной сети инициирует соединение, посылая пакет SYN принимающему серверу в глобальной сети.
2. Устройство P660HN изменяет маршрут пакета и отправляет его на шлюз **A**, который находится в подсети 2.
3. Ответ из глобальной сети приходит на устройство P660HN.
4. Затем устройство P660HN перенаправляет его на компьютер, который находится в подсети 1.

Рис. 75 Псевдоним IP



9

Контент-фильтрование

9.1 Обзор

Контент-фильтрование дает возможность блокировать веб-сайты по определенным ключевым словам в URL.

Пример настройки контент-фильтрования см. в Разд. 9.1.4 на с. 159.

9.1.1 Что можно сделать на экране контент-фильтрования

- Экран **Keyword** (Разд. 9.2 на с. 160) используется для блокирования веб-сайтов по определенным ключевым словам в URL.
- Экран **Schedule** (Разд. 9.3 на с. 162) используется для указания дней и времени активации блокирования по ключевым словам.
- Экран **Trusted** (Разд. 9.4 на с. 163) используется для исключения компьютеров и других устройств в вашей локальной сети из фильтра блокирования по ключевым словам.

9.1.2 Что нужно знать о контент-фильтровании

URL

URL (Унифицированный указатель информационного ресурса) идентифицирует и помогает определить местонахождение ресурсов в сети. В Интернете URL представляет собой веб-адрес, который вы набираете в адресной строке вашего Интернет-браузера, например http://www.zyxel.com.

9.1.3 Перед началом

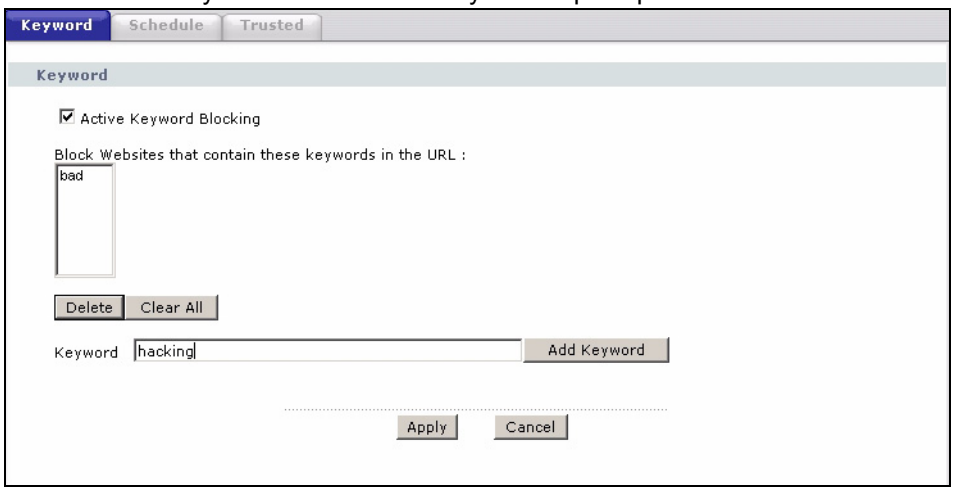
Для использования экрана **Trusted**, вам необходима информация об IP-адресах устройств вашей сети. Более подробную информацию см. в разделе **LAN** (Разд. 9.4 на с. 163).

9.1.4 Пример контент-фильтрования

В следующем примере показано, какие шаги нужно предпринять родителю (Бобу) для того, чтобы установить контент-фильтрование в домашней сети для ограничения доступа детям на определенные веб-сайты. В данном примере все URL, содержащие слово «bad» (плохой), блокируются.

1. Нажмите **Security > Content Filter**, чтобы открыть следующий экран.
2. Выберите **Active Keyword Blocking**.
3. В поле **Keyword** напечатайте ключевые слова, по которым будут блокироваться сайты.
4. Нажмите **Add Keyword** для ввода каждого ключевого слова.
5. Нажмите **Apply**.

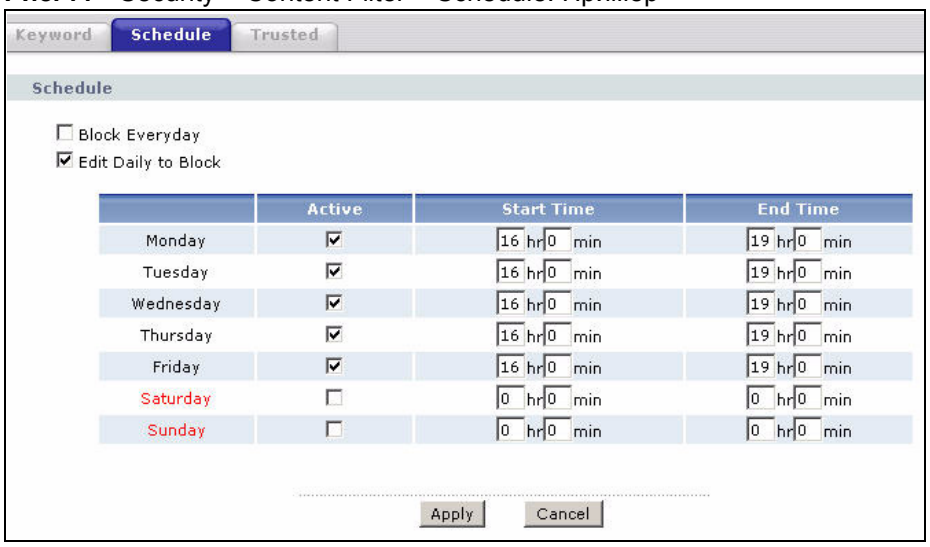
Рис. 76 Security > Content Filter > Keyword: Пример



Сын Боба приезжает домой из школы в четыре часа дня, а его родители приезжают позже – около семи часов вечера. Таким образом, блокирование по ключевым словам включается в этот период времени по будням, но не включается по выходным, когда родители дома.

1. Нажмите **Security > Content Filter > Schedule** для отображения следующего экрана.
2. Нажмите **Edit Daily to Block** и выберите все рабочие дни.
3. В полях под **Start Time** и **End Time** напечатайте время, когда следует начать и закончить блокирование (в данном примере: 16.00 – 19.00).
4. Нажмите **Apply**.

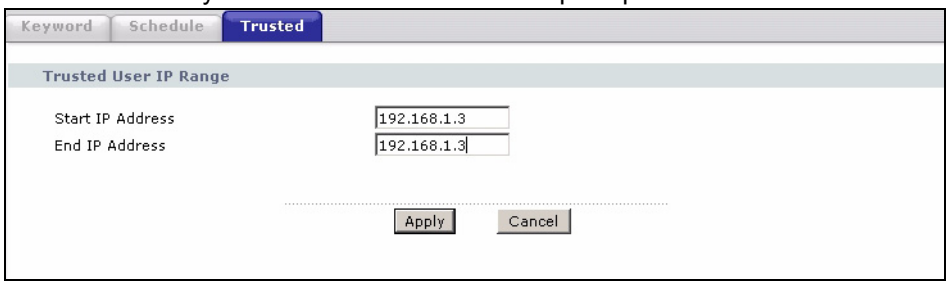
Рис. 77 Security > Content Filter > Schedule: Пример



Дети имеют доступ к семейному компьютеру в зале, в кабинете же компьютер используется только родителями. Таким образом, блокирование по ключевым словам нужно включить только на семейном компьютере, а на компьютере в кабинете – исключить эту функцию. Домашняя сеть Боба – на домене «192.168.1.xxx». Боб присвоил своему домашнему компьютеру статический IP-адрес 192.168.1.2, а компьютеру в кабинете – статический IP-адрес 192.168.1.3. Для того чтобы исключить компьютер в кабинете из блокирования по ключевым словам, необходимо выполнить следующее.

1. Нажмите **Security > Content Filter** > **Trusted** для отображения следующего экрана.
2. В полях **Start IP Address** и **End IP Address** напечатайте 192.168.1.3.
3. Нажмите **Apply**.

Рис. 78 Security > Content Filter > Trusted: Пример



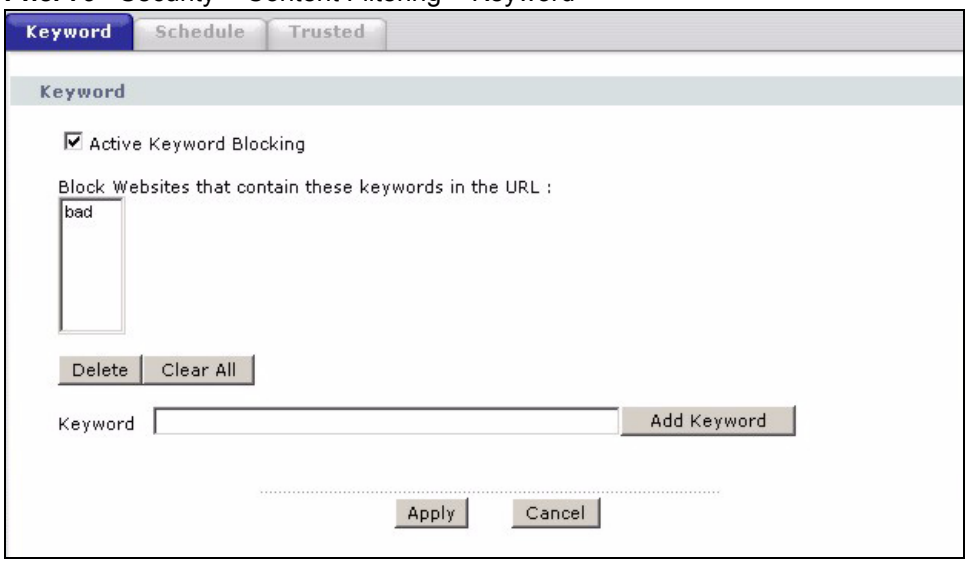
Эта процедура завершает блокирование по ключевым словам на домашнем компьютере.

9.2 Экран ключевых слов

Этот экран используется для блокирования сайтов, содержащих определенные слова в URL. Например, если вы включите эту функцию со словом «bad», устройство P660HN будет блокировать все сайты, содержащие это слово, включая URL http://www.website.com/bad.html.

Для того чтобы устройство P660HN блокировало веб-сайты, содержащие ключевые слова в URL, нажмите **Security > Content Filter**. При этом откроется показанный ниже экран.

Рис. 79 Security > Content Filtering > Keyword



В следующей таблице даны описания полей этого экрана.

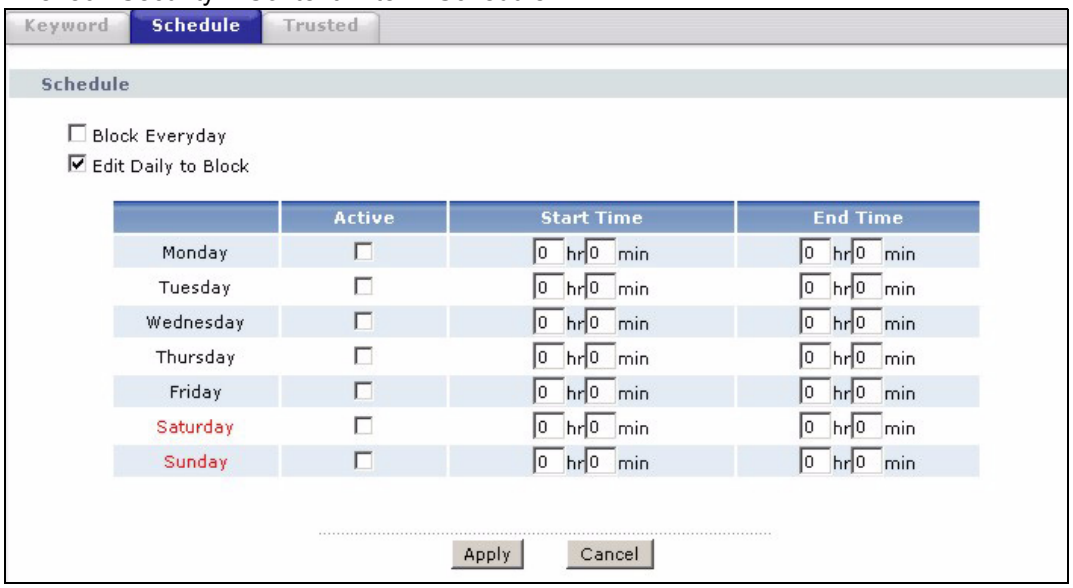
Табл. 49 Security > Content Filtering > Keyword

ПОЛЕ	ОПИСАНИЕ
Active Keyword Blocking	Поставьте галочку в поле для включения этой функции.
Block Websites that contain these keywords in the URL:	Это поле содержит список всех установленных ключевых слов, по которым устройство P660HN будет производить блокирование сайтов.
Delete	Выделите ключевое слово в прямоугольнике и нажмите кнопку для его удаления.
Clear All	Нажмите эту кнопку для удаления всех ключевых слов из этого списка.
Keyword	Введите в это поле ключевое слово. Допускается использование любых символов (до 127 символов). Специальные символы не разрешаются.
Add Keyword	Нажмите эту кнопку после ввода ключевого слова. Повторите эту процедуру для добавления других ключевых слов. Допускается до 64 ключевых слов. При попытке доступа к веб-странице, содержащей ключевое слово, вы получите сообщение, в котором говорится, что контент-фильтр блокирует этот запрос.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

9.3 Экран расписания

На этом экране устанавливается расписание, по которому P660HN выполняет фильтрование содержания. Нажмите **Security > Content Filter** > **Schedule**. При этом откроется показанный ниже экран.

Рис. 80 Security > Content Filter > Schedule



В следующей таблице даны описания полей этого экрана.

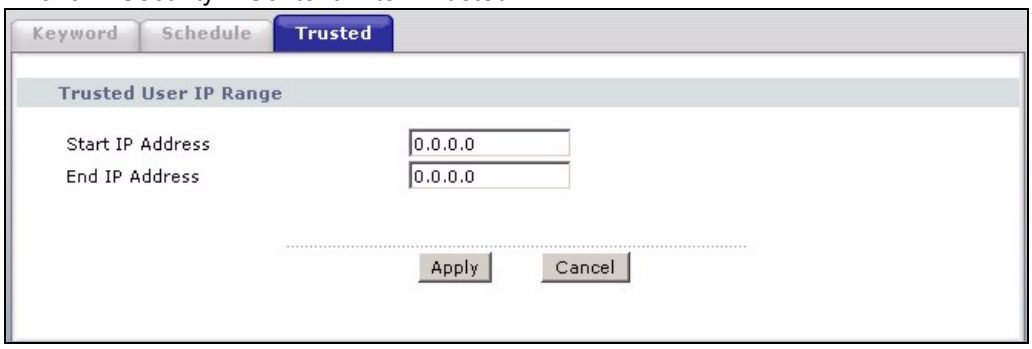
Табл. 50 Security > Content Filter: Schedule

ПОЛЕ	ОПИСАНИЕ
Schedule	Выберите **Block Everyday**, чтобы фильтрование контента выполнялось каждый день. В противном случае, выберите **Edit Daily to Block** и выберите дни недели (или каждый день), а также время дня, когда необходимо выполнять фильтрование контента.
Active	Установите флажок, чтобы выполнять фильтрование контента в выбранный день.
Start Time	Введите время, когда необходимо начать выполнение фильтрования контента в формате «часы–минуты».
End Time	Введите время, когда необходимо прекратить выполнение фильтрования контента в формате «часы–минуты».
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

9.4 Экран Trusted

На этом экране можно определить группу пользователей локальной сети, для которых устройство P660HN не будет выполнять фильтрование содержания. Нажмите **Security > Content Filter** > **Trusted**. При этом откроется показанный ниже экран.

Рис. 81 Security > Content Filter: Trusted



В следующей таблице даны описания полей этого экрана.

Табл. 51 Security > Content Filter: Trusted

ПОЛЕ	ОПИСАНИЕ
Start IP Address	Введите IP-адрес компьютера (или начальный IP-адрес конкретного диапазона компьютеров) в локальной сети, который вы хотите исключить из контент-фильтрования.
End IP Address	Введите конечный IP-адрес конкретного диапазона пользователей в локальной сети, которых вы хотите исключить из контент-фильтрования. Оставьте это поле не заполненным, если вы хотите исключить отдельный компьютер.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

10

Фильтр пакетов

10.1 Обзор

Устройство P660HN использует фильтры для того чтобы определить, разрешить ли прохождение определенного трафика. В данной главе описываются порядок создания и установки фильтров.

10.1.1 Что можно сделать на экране фильтра пакетов

Экран **Packet Filter** (Разд. 10.2 на с. 165) используется для отображения наборов фильтров и настройки правил для фильтров протоколов и общих фильтров.

10.1.2 Что нужно знать о фильтре пакетов

Фильтры

Устройство P660HN использует фильтры для того чтобы определить, необходимо ли разрешение пересылки пакета данных. Фильтры подразделяются на общие фильтры и фильтры протоколов. Правила фильтра общего типа применяются к необработанным данным, передаваемым из/в LAN и WAN. Правила фильтра протоколов применяются к IP-пакетам.

Структура фильтра

Набор фильтров состоит из одного или нескольких правил фильтров. Устройство P660HN позволяет задать настройку до двенадцати фильтрующих наборов по шесть правил для каждого набора. Итого в системе используется 72 правила фильтрования. В одном наборе нельзя объединять правила общих фильтров и правила фильтров протоколов. На каждом порту можно устанавливать до четырех наборов фильтров, предназначенных для блокирования пакетов множества разных типов. Каждый набор фильтров может содержать 6 правил, поэтому на каждый отдельный порт можно установить до 24 активных правил.

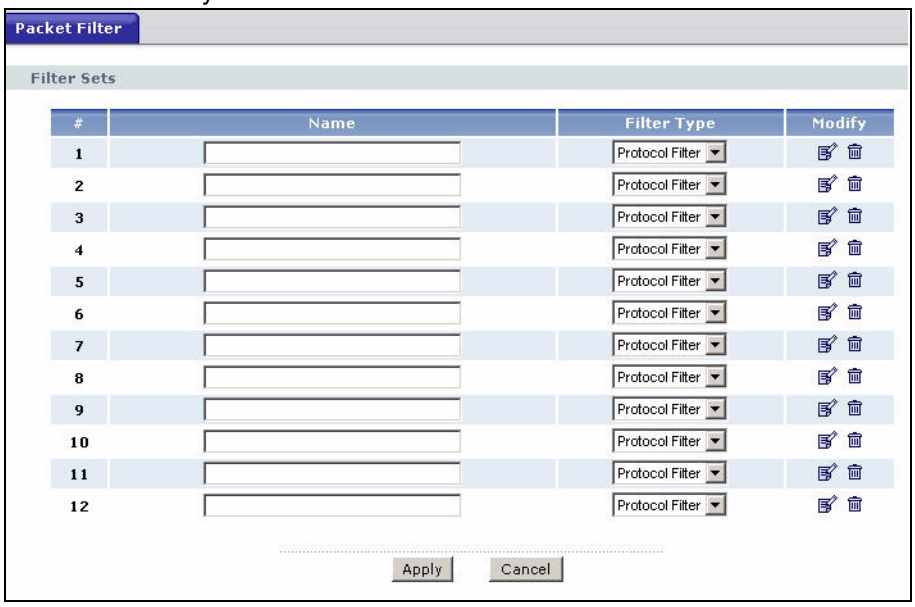
Дополнительные сведения

Техническую вводную информацию о фильтрах пакетов см. в Разд. 10.3 на с. 171.

10.2 Экран фильтров пакетов

Этот экран используется для установки пакета фильтров на устройстве P660HN. Нажмите **Security > Packet Filter** для отображения следующего экрана.

Рис. 82 Security > Packet Filter



В следующей таблице даны описания полей этого экрана.

Табл. 52 Security > Packet Filter

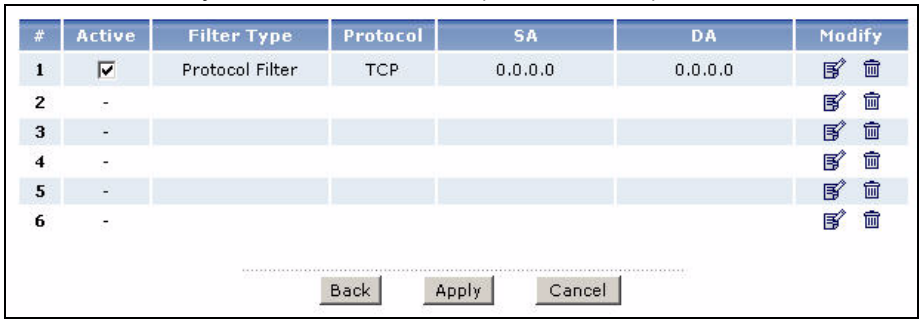
ПОЛЕ	ОПИСАНИЕ
#	В этом поле отображается порядковый номер фильтра.
Name	Введите имя набора фильтров. Текст может состоять не более, чем из 16 букв, цифр и любых печатаемых символов, расположенных на стандартной англоязычной клавиатуре.
Filter Type	Выберите **Protocol Filter** или **Generic Filter** для вашего набора фильтров. Правила фильтра протоколов применяются к IP-пакетам, а правила общих фильтров служат для фильтрования не IP-пакетов.
Modify	Нажмите кнопку **Edit** для конфигурирования набора фильтров. Нажмите кнопку **Remove** для удаления набора фильтров.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

10.2.1 Редактирование фильтров протоколов

Этот экран используется для отображения набора фильтров протокола на устройстве P660HN. Правила протоколов позволяют установить правило в полях протокола IP и в протоколах более высокого уровня, например, в заголовках UDP и TCP.

На экране **Packet Filter** выберите **Protocol Filter** в поле **Filter Type**. Затем нажмите кнопку **Edit** в поле **Modify** для отображения следующего экрана.

Рис. 83 Security > Packet Filter > Edit (Protocol Filter)



В следующей таблице даны описания полей этого экрана.

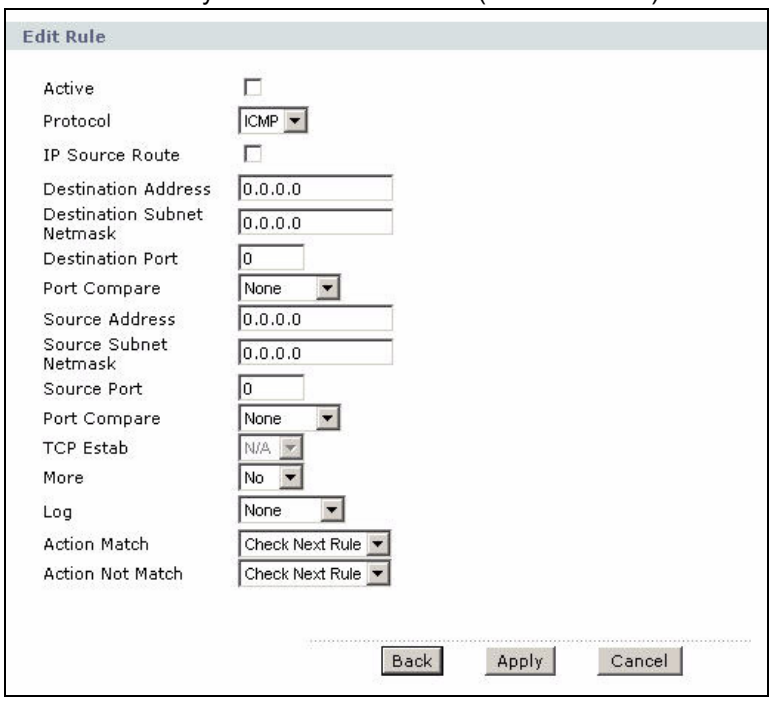
Табл. 53 Security > Packet Filter > Edit (Protocol Filter)

ПОЛЕ	ОПИСАНИЕ
#	Это порядковый номер правила в наборе фильтров.
Active	Установите флажок для включения правила фильтра; снимите флажок – для выключения.
Filter Type	В этом поле отображается тип фильтра – фильтр протокола или общий фильтр.
Protocol	В этом поле отображается протокол верхнего уровня.
SA	В этом поле отображается IP-адрес источника.
DA	В этом поле отображается IP-адрес назначения.
Modify	Для конфигурирования правила фильтра щелкните по иконке **Edit**. Для удаления правила фильтра щелкните по иконке **Remove**.
Back	Нажмите эту кнопку для возврата к предыдущему экрану без сохранения.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

10.2.2 Конфигурирование правил фильтров протоколов

Этот экран используется для конфигурирования правил фильтров протоколов. На экране **Edit (Protocol Filter)** щелкните по иконке **Edit** для отображения следующего экрана.

Рис. 84 Security > Packet Filter > Edit (Protocol Filter) > Edit Rule



В следующей таблице даны описания полей этого экрана.

Табл. 54 Security > Packet Filter > Edit (Protocol Filter) > Edit Rule

ПОЛЕ	ОПИСАНИЕ
Active	Установите флажок для включения правила фильтра.
Protocol	Выберите **ICMP**, **TCP** или **UDP** для протокола верхнего уровня.
IP Source Route	Установите флажок для применения правила фильтра к пакетам с опцией исходной IP-маршрутизации. Однако большинство IP-пакетов не имеют маршрута источника.
Destination Address	Введите IP-адрес назначения для пакета, который вы хотите отфильтровать. Если в это поле вводится значение 0.0.0.0., то оно игнорируется.
Destination Subnet Netmask	Введите маску IP-подсети для IP-адреса назначения.
Destination Port	Введите порт назначения для пакетов, которые вы хотите отфильтровать. Значение поля должно находиться в диапазоне от 0 до 65535. Это поле игнорируется, если вы указываете 0.
Port Compare	Выберите способ сравнения портов назначения, указанных в пакетах и в поле **Destination Port**. Опциями являются **None**, **Equal**, **Not Equal**, **Less** и **Greater**.
Source Address	Введите IP-адрес источника для пакета, который вы хотите отфильтровать. Если в это поле вводится значение 0.0.0.0., то оно игнорируется.
Source Subnet Netmask	Введите маску IP-подсети для IP-адреса источника.

Табл. 54 Security > Packet Filter > Edit (Protocol Filter) > Edit Rule (продолжение)

ПОЛЕ	ОПИСАНИЕ
Source Port	Введите исходный порт для пакетов, которые вы хотите отфильтровать. Значение поля должно находиться в диапазоне от 0 до 65535. Это поле игнорируется, если вы указываете 0.
Port Compare	Выберите способ сравнения портов источника, указанных в пакетах и в поле **Source Port**. Опциями являются **None**, **Equal**, **Not Equal**, **Less** и **Greater**.
TCP Estab	Данное поле доступно только в случае выбора **TCP** в поле **Protocol**. Выберите **Yes** для того, чтобы правило распространялось на пакеты, которые предназначены для установки TCP соединения. При выборе **No** это поле будет недоступно.
More	Выберите **Yes** для того, чтобы пакет, соответствующий параметрам фильтра, был передан следующему правилу фильтра прежде, чем будет выполнено действие. Выберите **No** для обработки пакета в соответствии с полями, где назначены действия.
Log	Выберите функцию журнальной регистрации из предложенных: **None** – пакеты не регистрируются в журнальном файле. **Match** – в журнале регистрируются только те пакеты, которые соответствуют параметрам правила. **Not Match** – в журнале регистрируются только те пакеты, которые не соответствуют параметрам правила. **Both** – все пакеты регистрируются в журнальном файле.
Action Match	Выберите действие, выполняемое при соответствии пакета правилу. Опциями являются **Check Next Rule**, **Forward** и **Drop**.
Action Not Match	Выберите действие, выполняемое при несоответствии пакета правилу. Опциями являются **Check Next Rule**, **Forward** и **Drop**.
Back	Нажмите эту кнопку для возврата к предыдущему экрану без сохранения.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

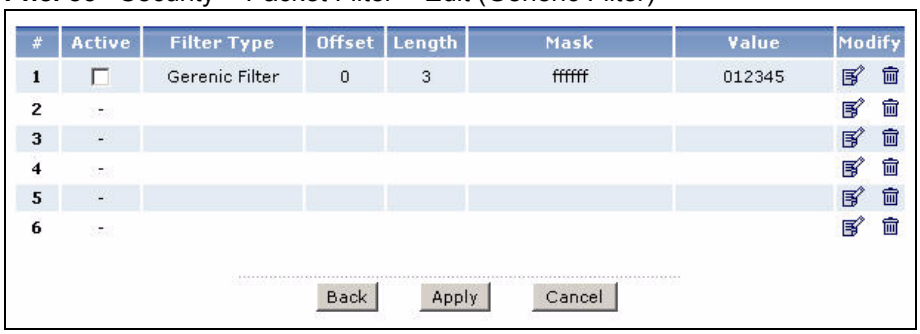
10.2.3 Редактирование общих фильтров

Этот экран используется для отображения набора общих фильтров на устройстве P660HN. Общие правила предназначены для того, чтобы дать возможность пользователю фильтровать пакеты, не относящиеся к IP. Обычно для фильтрования IP-пакетов значительно проще использовать непосредственно правила IP.

При общих правилах устройство P660HN обрабатывает пакет не как пакет IP или IPX, а как битовый поток. Вы указываете часть пакета, которую надлежит проверить по полям **Offset** (от 0) и **Length**, и то и другое в байтах. Устройство P660HN использует Маску (Mask) (поразрядное выполнение операции «И») для блока данных до того, как проводит сравнение полученного результата со Значением (Value) и определяет соответствие. Значения полей **Mask** и **Value** указываются в шестнадцатеричной форме. Следует иметь в виду, что для обозначения байта используются две шестнадцатеричные цифры. Поэтому, если длина равна 4 байтам, то значение в каждом поле будет состоять из 8 цифр, например, FFFFFFFF.

На экране **Packet Filter** выберите **Generic Filter** в поле **Filter Type**. Затем нажмите кнопку **Edit** в поле **Modify** для отображения следующего экрана.

Рис. 85 Security > Packet Filter > Edit (Generic Filter)



В следующей таблице даны описания полей этого экрана.

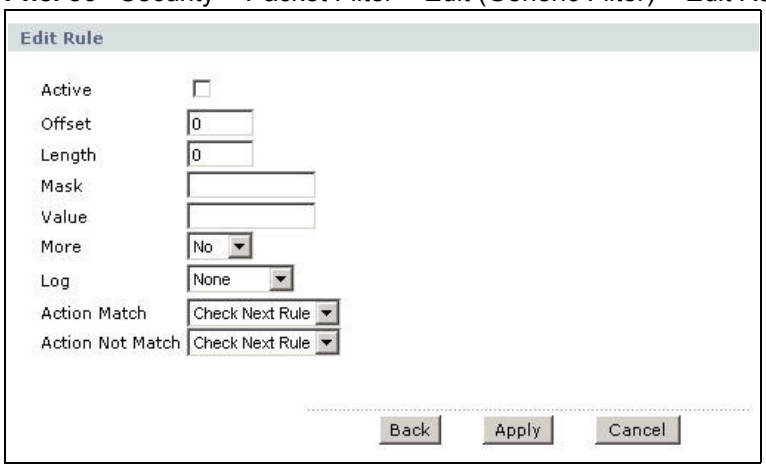
Табл. 55 Security > Packet Filter > Edit (Generic Filter)

ПОЛЕ	ОПИСАНИЕ
#	Это порядковый номер правила в наборе фильтров.
Active	Установите флажок для включения правила фильтра; снимите флажок – для выключения.
Filter Type	В этом поле отображается тип фильтра – фильтр протокола или общий фильтр.
Offset	В этом поле отображается значение смещения.
Length	В этом поле отображается значение длины.
Mask	В этом поле отображается маска.
Value	В этом поле отображается значение.
Modify	Для конфигурирования правила фильтра щелкните по иконке **Edit**. Для удаления правила фильтра щелкните по иконке **Remove**.
Back	Нажмите эту кнопку для возврата к предыдущему экрану без сохранения.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

10.2.4 Конфигурирование общих правил пакетов

Этот экран используется для конфигурирования правил общих фильтров. На экране **Edit (Generic Filter)** нажмите кнопку **Edit** в поле **Modify** для отображения следующего экрана.

Рис. 86 Security > Packet Filter > Edit (Generic Filter) > Edit Rule



В следующей таблице даны описания полей этого экрана.

Табл. 56 Security > Packet Filter > Edit (Generic Filter) > Edit Rule

ПОЛЕ	ОПИСАНИЕ
Active	Установите флажок для включения правила фильтра.
Offset	Наберите с клавиатуры начальный байт блока данных в пакете, который требуется сравнить. Значения в этом поле устанавливаются в диапазоне от 0 до 255.
Length	Наберите с клавиатуры счетчик байтов блока данных в пакете, который требуется сравнить. Значения в этом поле устанавливаются в диапазоне от 0 до 8.
Mask	Введите с клавиатуры маску (в шестнадцатеричной форме), используемую для блока данных до выполнения операции сравнения.
Value	Введите с клавиатуры значение (в шестнадцатеричной форме), используемое для сравнения с блоком данных.
More	Выберите **Yes** для того, чтобы пакет, соответствующий параметрам фильтра, был передан следующему правилу фильтра прежде, чем будет выполнено действие. Выберите **No** для обработки пакета в соответствии с полями, где назначены действия.
Log	Выберите функцию журнальной регистрации из предложенных: **None** – пакеты не регистрируются в журнальном файле. **Match** – в журнале регистрируются только те пакеты, которые соответствуют параметрам правила. **Not Match** – в журнале регистрируются только те пакеты, которые не соответствуют параметрам правила. **Both** – все пакеты регистрируются в журнальном файле.
Action Match	Выберите действие, выполняемое при соответствии пакета правилу. Опциями являются **Check Next Rule**, **Forward** и **Drop**.
Action Not Match	Выберите действие, выполняемое при несоответствии пакета правилу. Опциями являются **Check Next Rule**, **Forward** и **Drop**.

Табл. 56 Security > Packet Filter > Edit (Generic Filter) > Edit Rule (продолжение)

ПОЛЕ	ОПИСАНИЕ
Back	Нажмите эту кнопку для возврата к предыдущему экрану без сохранения.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

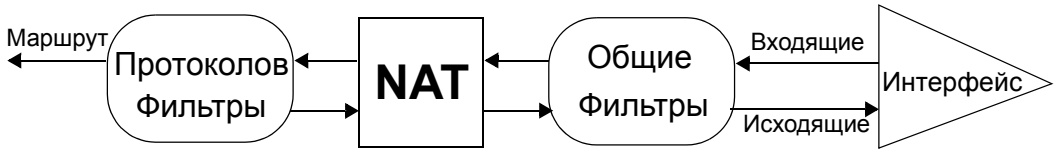
10.3 Техническое руководство по фильтрам пакетов

В этом разделе приводится некоторая вводная техническая информация по темам данной главы.

10.3.1 Типы фильтров и трансляция сетевых адресов (NAT)

Существуют два класса правил фильтров: правила общих фильтров и правила фильтров протоколов. Правила фильтра общего типа применяются к необработанным данным, передаваемым из/в LAN и WAN. Правила фильтра протоколов применяются к IP-пакетам. Когда функция NAT (Трансляция сетевых адресов) включена, то при каждом подключении IP-адрес и номер порта меняются, поэтому невозможно установить точный адрес и порт проводного соединения. Поэтому устройство P660HN устанавливает фильтры протоколов на «родных» IP-адресах и номерах портов для исходящих пакетов до NAT, а для входящих пакетов – после NAT. С другой стороны, общие фильтры применяются по отношению к исходным пакетам, которые появляются в проводном соединении. Эти фильтры устанавливаются в точке, где устройство P660HN получает или отправляет пакеты данных; это интерфейс. В качестве интерфейса может выступать порт Ethernet или любой другой порт, относящийся к аппаратному обеспечению. На следующей диаграмме это представлено в графическом виде.

Рис. 87 Наборы фильтров протоколов и общих фильтров



10.3.2 Брандмауэр и фильтры

Ниже представлено сравнение функций фильтрования и брандмауэра в устройстве P660HN.

Фильтрование пакетов

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

Когда использовать фильтрование

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

Брандмауэр

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

Когда использовать брандмауэр

1. Для предотвращения атак типа DoS и предотвращения взламывания сети хакерами.
2. Диапазон отправителя и IP-адресов назначения, а также номера портов, могут быть определены в одном правиле брандмауэра, делая брандмауэр лучшей альтернативой, когда необходимы сложные правила.
3. Для выборочного блокирования/разрешения входящего или исходящего трафика между внутренним узлом/сетями и внешним узлом/сетями. Помните, что фильтры не могут различать по IP-адресу трафик, исходящий из внутреннего или внешнего узла.
4. Брандмауэр работает лучше, чем фильтрование, если необходимо проверить много правил.
5. Используйте брандмауэр, если необходимы текущие сообщения электронной почты о системе или необходимы извещения о произошедшей атаке.
6. Брандмауэр может блокировать конкретный трафик URL, который может встретиться в будущем. URL может сохраняться в базе данных ACL (Access Control List – Список контроля доступа).

11

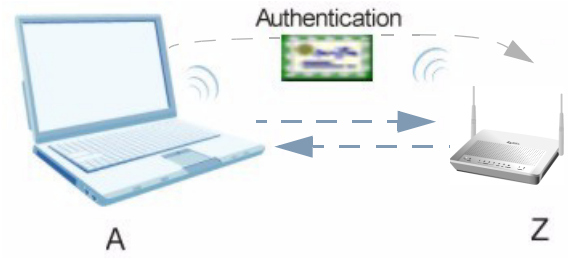
Сертификаты

11.1 Обзор

В этой главе описывается, как устройство P660HN может использовать сертификаты для аутентификации беспроводных клиентов. Здесь представлена вводная информация о сертификатах открытого ключа и рассказывается об их использовании.

Каждый сертификат содержит идентификатор владельца и открытый ключ. Сертификаты обеспечивают обмен открытыми ключами для проведения аутентификации.

Рис. 88 Сертификаты: пример



На рисунке ниже показано, как устройство P660HN (Z) проверяет идентификационные данные ноутбука (A) с помощью сертификата перед тем, как предоставить ему доступ к сети.

11.1.1 Что можно сделать на экране сертификатов

- Экран **My Certificates** (Разд. 11.2 на с. 175) используется для создания и экспорта самостоятельно подписанных сертификатов или запросов на сертификацию, а также импорта сертификатов устройства P660HN, подписанных центром сертификации.
- Экран **Trusted CAs** (Разд. 11.3 на с. 184) используется для сохранения сертификатов, выданных центром сертификации в устройстве P660HN.
- Экран **Trusted Remote Hosts** (Разд. 11.4 на с. 190) используется для импорта самостоятельно подписанных сертификатов.
- Экран **Directory Servers** (Разд. 11.5 на с. 196) используется для создания списка адресов серверов каталогов, которые содержат списки действующих и аннулированных сертификатов).

11.1.2 Что нужно знать о сертификатах

Центр сертификации

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. Устройство P660HN может генерировать запросы на сертификацию, содержащие идентифицирующую информацию и открытые ключи, а затем отправлять эти запросы в центр сертификации.

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.
- PEM (Base-64) в зашифрованном формате X.509: В формате электронной почты с усовершенствованной защитой (Privacy Enhanced Mail) используются буквы нижнего и верхнего регистров, а также числа 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 устройство P660HN позволяет выполнять импорт файла PKS#7, который содержит один сертификат.
- PEM (Base-64) в зашифрованном формате PKCS#7: В формате электронной почты с усовершенствованной защитой (PEM) используются 64 символа ASCII для преобразования бинарного сертификата PKCS#7 в печатную форму.

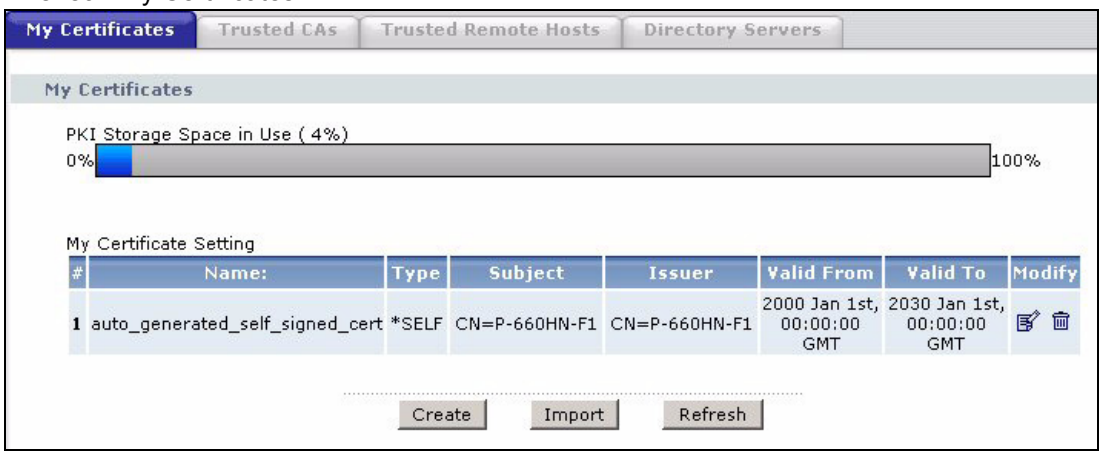
Дополнительные сведения

Техническую вводную информацию о сертификатах см. в Разд. 11.6 на с. 198.

11.2 Экран My Certificates

Окно содержит сводный список сертификатов устройства P660HN и запросов на сертификацию. Сертификаты отображаются черным шрифтом, а запросы на сертификацию – серым. Нажмите **Security > Certificates > My Certificates**, чтобы открыть экран **My Certificates**.

Рис. 89 My Certificates



В следующей таблице даны описания полей этого экрана.

Табл. 57 My Certificates

ПОЛЕ	ОПИСАНИЕ
PKI Storage Space in Use	Этот индикатор показывает находящуюся в использовании память устройства P660HN в процентах для хранения инфраструктуры открытого ключа. Индикатор меняет свой цвет с зеленого на красный, когда память используется полностью. Когда индикатор становится красным, необходимо удалить просроченные или ненужные сертификаты перед добавлением новых сертификатов.
My Certificate Setting	
#	В этом поле отображается порядковый номер сертификата. Сертификаты отображаются в алфавитном порядке.
Name	В этом поле отображается описательное имя сертификата. Рекомендуется давать каждому сертификату уникальное имя.
Type	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. Экран **My Certificate Import** используется для импорта сертификатов и замены запросов. **SELF** обозначает самостоятельно подписанный сертификат. ***SELF** обозначает самостоятельно подписанный сертификат по умолчанию, который используется устройством P660HN для подписи сертификатов, импортированных из доверенных удаленных узлов. **CERT** обозначает сертификат, выданный центром сертификации.
Subject	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.

Табл. 57 My Certificates (продолжение)

ПОЛЕ	ОПИСАНИЕ
Issuer	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**.
Valid From	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	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	Щелкните по иконке **Edit**, чтобы открыть экран, содержащий полную информацию о сертификате. Для удаления сертификата щелкните по иконке **Remove**. 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** 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 **Edit** в строке другого самостоятельно подписанного сертификата (если требуется создать самостоятельно подписанный сертификат, см. описание кнопки **Create**). 3. Установите флажок в поле **Default self-signed certificate which signs the imported remote host certificates**. 4. Нажмите **Apply** для сохранения изменений и возврата к экрану **My Certificates**. 5. Сертификат, который первоначально отображался как ***SELF**, сейчас отображается как **SELF** и его можно удалить. Следует помнить, что при удалении сертификата все последующие сдвигаются на позицию вверх.
Create	Нажмите эту кнопку для перехода к экрану, в котором устройство P660HN генерирует сертификат или запрос на сертификацию.
Import	Нажмите эту кнопку для отображения экрана, где можно перенести сертификат, полученный из центра сертификации, с вашего компьютера в устройство P660HN.
Refresh	Нажмите эту кнопку для обновления информации о текущем статусе сертификатов.

11.2.1 Импорт сертификатов

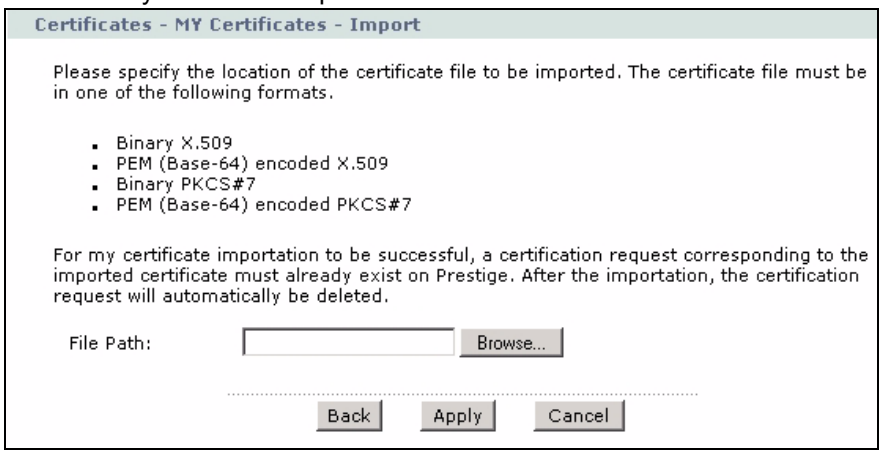
Следуйте указаниям на этом экране для сохранения существующего сертификата в устройстве P660HN. Нажмите **Security > Certificates > My Certificates**, а затем **Import**, чтобы открыть экран **My Certificate Import**.

Импорт сертификата можно выполнить, только если он соответствует запросу на сертификацию, который был сгенерирован устройством P660HN.

Импортированный сертификат замещает соответствующий запрос на экране **My Certificates**.

Перед импортом необходимо удалить все пробелы в имени файла сертификата.

Рис. 90 My Certificate Import



В следующей таблице даны описания полей этого экрана.

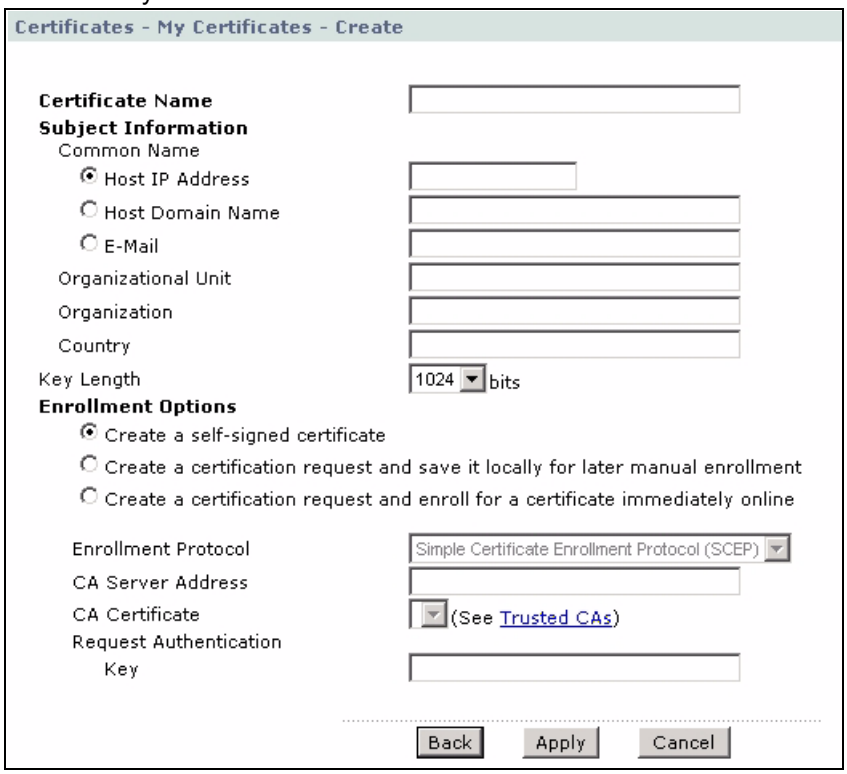
Табл. 58 My Certificate Import

ПОЛЕ	ОПИСАНИЕ
File Path	Введите в это поле путь к файлу, который требуется загрузить, или нажмите **Browse** для его поиска.
Browse	Нажмите эту кнопку для поиска файла сертификата, который требуется загрузить.
Back	Нажмите эту кнопку для возврата к предыдущему экрану без сохранения.
Apply	Нажмите эту кнопку для сохранения сертификата в устройстве P660HN.
Cancel	Нажмите эту кнопку для сброса ваших настроек.

11.2.2 Создание сертификатов

На этом экране устройство P660HN может создать самостоятельно подписанный сертификат, зарегистрировать сертификат от центра сертификации или сгенерировать запрос на сертификацию. Нажмите **Security** > **Certificates** > **My Certificates** > **Create**, чтобы открыть экран **My Certificate Create**.

Рис. 91 My Certificate Create



В следующей таблице даны описания полей этого экрана.

Табл. 59 My Certificate Create

ПОЛЕ	ОПИСАНИЕ
Certificate Name	Введите до 31 символа ASCII (пробелы исключаются) для описания сертификата.
Subject Information	В эти поля заполняется информация, идентифицирующая владельца сертификата. Не обязательно заполнять все поля, но поле **Common Name** 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	Установите переключатель, чтобы идентифицировать владельца сертификата по IP-адресу, доменному имени или адресу электронной почты. Введите IP-адрес (в десятичном формате с разделительными точками), доменное имя или адрес электронной почты в соответствующее поле. Доменное имя и адрес электронной почты могут содержать до 31 символа ASCII. Доменное имя и адрес электронной почты служат только для идентификации и могут быть любыми.

Табл. 59 My Certificate Create (продолжение)

ПОЛЕ	ОПИСАНИЕ
Organizational Unit	Введите до 127 символов для описания организационной единицы или отдела, к которому относится владелец сертификата. Допускается вводить любые символы, включая пробелы, однако устройство P660HN отбрасывает пробелы в конце строки.
Organization	Введите до 127 символов для описания компании или группы, к которому относится владелец сертификата. Допускается вводить любые символы, включая пробелы, однако устройство P660HN отбрасывает пробелы в конце строки.
Country	Введите до 127 символов для описания страны, где находится владелец сертификата. Допускается вводить любые символы, включая пробелы, однако устройство P660HN отбрасывает пробелы в конце строки.
Key Length	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	Здесь определяется способ создания сертификата.
Create a self-signed certificate	Выберите **Create a self-signed certificate**, чтобы устройство P660HN выступало в качестве центра сертификации (CA) и генерировало сертификаты. В этом случае не требуется делать запрос в центр сертификации на получение сертификата.
Create a certification request and save it locally for later manual enrollment	Выберите **Create a certification request and save it locally for later manual enrollment**, чтобы устройство P660HN генерировало и сохраняло запросы на сертификаты. Просмотр и копирование запросов на сертификат, а также их отправка в центр сертификации производится на экране **My Certificate Details**. Скопируйте запрос на сертификат на экране **My Certificate Details** (см. Разд. 11.2.3 на с. 181) и затем отправьте его в центр сертификации.
Create a certification request and enroll for a certificate immediately online	Выберите **Create a certification request and enroll for a certificate immediately online**, чтобы устройство P660HN сгенерировало запрос на сертификат и отправило этот запрос в центр сертификации. Заранее необходимо выполнить импорт сертификата центра сертификации на экране **Trusted CAs**. 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** и **Key**, если эта информация требуется центру сертификации.
Enrollment Protocol	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.
CA Server Address	Введите IP-адрес или URL сервера центра сертификации.

Табл. 59 My Certificate Create (продолжение)

ПОЛЕ	ОПИСАНИЕ
CA Certificate	Из выпадающего списка поля **CA Certificate** выберите сертификат центра сертификации. Заранее необходимо выполнить импорт сертификата центра сертификации на экране **Trusted CAs**. Нажмите **Trusted CAs** для перехода к экрану **Trusted CAs**, где можно выполнять просмотр и управление списком сертификатов устройства P660HN от доверенных центров сертификации.
Request Authentication	При выборе поля **Create a certification request and enroll for a certificate immediately online** центр сертификации может запросить данные о регистрационном номере и ключе для проведения идентификации во время получения вашего запроса на сертификат. Заполните поля **Reference Number** и **Key**, если ваш центр сертификации применяет протокол регистрации CMP. Если ваш центр сертификации применяет протокол регистрации SCEP, заполните только поле **Key**.
Key	Введите ключ, предоставленный центром сертификации.
Back	Нажмите эту кнопку для возврата к предыдущему экрану без сохранения.
Apply	Нажмите эту кнопку для сохранения сертификата в устройстве P660HN.
Cancel	Нажмите эту кнопку для сброса ваших настроек.

После нажатия **Apply** на экране **My Certificate Create** появляется экран с сообщением о том, что устройство P660HN генерирует самостоятельно подписанный сертификат или запрос на сертификат.

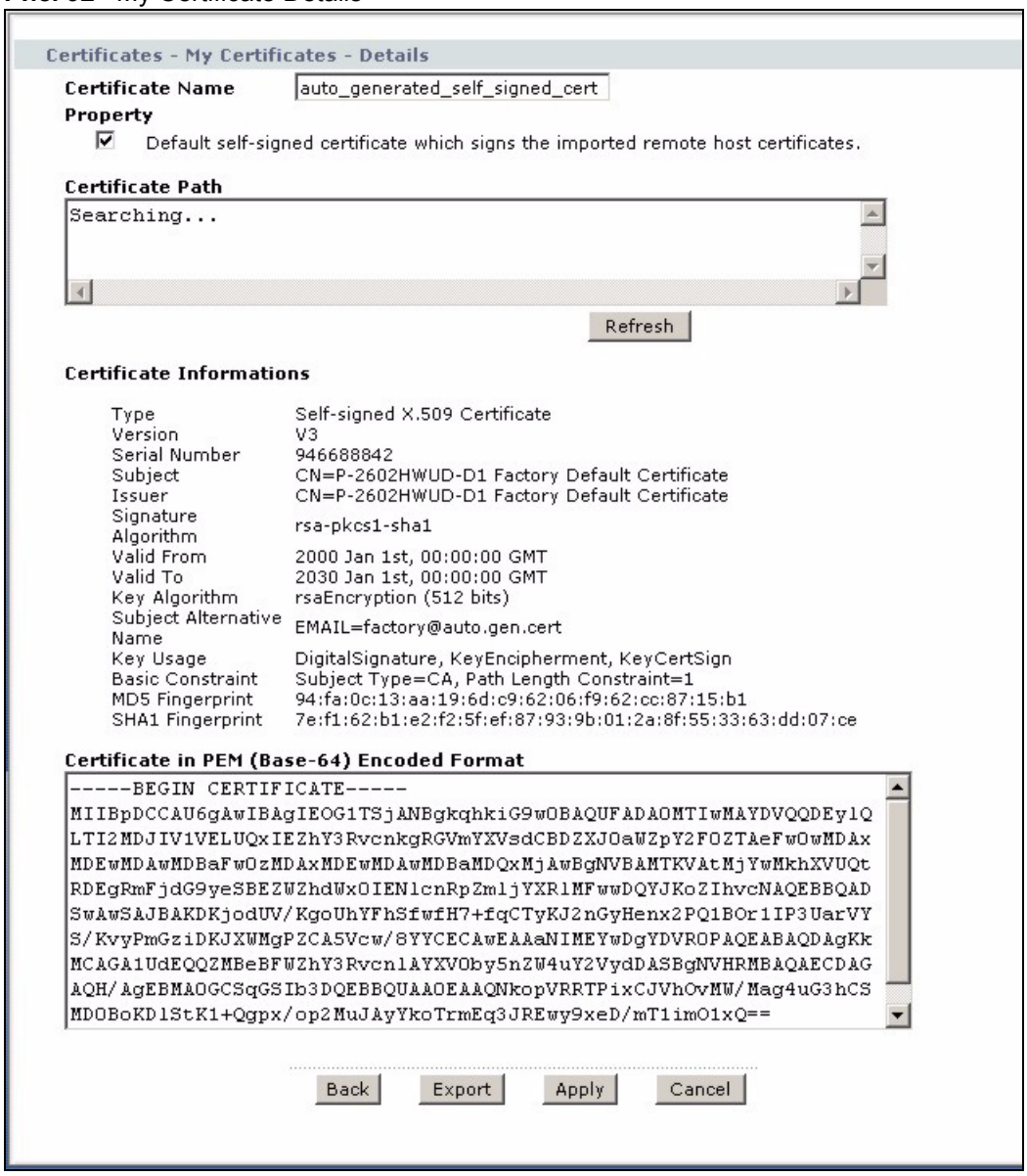
После того как устройство P660HN успешно зарегистрирует сертификат или сгенерирует запрос или самостоятельно подписанный сертификат, появляется экран с кнопкой **Return**, при нажатии на которую происходит возврат к экрану **My Certificates**.

Если на экране **My Certificate Create** производилась регистрация сертификата, и устройство P660HN не смогло ее выполнить успешно, появляется экран с кнопкой **Return**, при нажатии на которую происходит возврат к экрану **My Certificate Create**. Нажмите кнопку **Return** и проверьте настройки на экране **My Certificate Create**. Убедитесь, что параметры центра сертификации установлены правильно и подключение к Интернету работает нормально, чтобы устройство P660HN зарегистрировало сертификат в режиме онлайн.

11.2.3 Экран сведений о сертификате

На этом экране можно просмотреть подробную информацию о данном сертификате или изменить его имя. Если выбран самостоятельно подписанный сертификат, то можно использовать его для подписи устройством P660HN сертификатов доверенных удаленных узлов, которые импортируются в устройство P660HN. Нажмите **Security** > **Certificates** > **My Certificates**, чтобы открыть экран **My Certificates** (см. Рис. 89 на с. 175). Щелкните по иконке редактирования для перехода к экрану **My Certificate Details**.

Рис. 92 My Certificate Details



В следующей таблице даны описания полей этого экрана.

Табл. 60 My Certificate Details

ПОЛЕ	ОПИСАНИЕ
Certificate Name	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 Default self-signed certificate which signs the imported remote host certificates.	Установите в этом поле флажок, чтобы устройство P660HN использовало этот сертификат для подписи сертификатов от доверенных удаленных узлов, которые импортируются в устройство P660HN. Это поле доступно только при использовании самостоятельно подписанных сертификатов. Если здесь флажок уже установлен, то на этом экране его снять нельзя, флажок необходимо установить на экране с параметрами другого самостоятельно подписанного сертификата. Тогда флажок автоматически будет снят на экране с параметрами сертификата, который ранее был установлен для подписи импортированных сертификатов от доверенных удаленных узлов.
Certification Path	Нажмите **Refresh** 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, устройство P660HN считает такой сертификат непроверенным, и в этом поле появляется сообщение «Not trusted» (Не подтвержден).
Refresh	Нажмите эту кнопку для отображения пути к сертификату.
Certificate Information	В следующих полях отображается подробная информация о сертификате в режиме только для чтения.
Type	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	В этом поле отображается номер версии X.509.
Serial Number	В этом поле отображается идентификационный номер сертификата, выданного центром сертификации или сгенерированного устройством P660HN.
Subject	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	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 Name**.
Signature Algorithm	В этом поле отображается тип алгоритма, использованного для подписи сертификата. В устройстве P660HN 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).

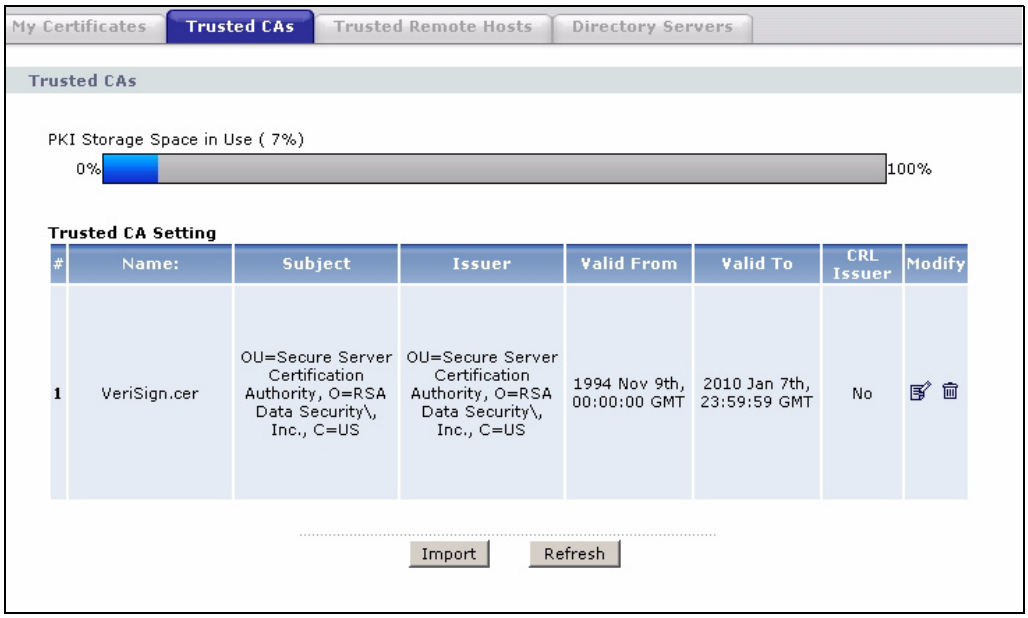
Табл. 60 My Certificate Details (продолжение)

ПОЛЕ	ОПИСАНИЕ
Valid From	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	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	В этом поле отображается тип алгоритма, который используется для генерирования пар ключей сертификатов (в устройстве P660HN используется шифрование RSA), и длина ключа в битах (в примере 1024 бит).
Subject Alternative Name	В этом поле отображается IP-адрес (IP), доменное имя (DNS) или адрес электронной почты (EMAIL) владельца сертификата.
Key Usage	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	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	Это профиль сообщения сертификата, который устройство P660HN вычислило с использованием алгоритма MD5.
SHA1 Fingerprint	Это профиль сообщения сертификата, который устройство P660HN вычислило с использованием алгоритма SHA1.
Certificate in PEM (Base-64) Encoded Format	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	Нажмите эту кнопку для возврата к предыдущему экрану без сохранения.
Export	Нажмите эту кнопку, а затем – кнопку **Save** на экране **File Download**. Откроется экран **Save As**. Выберите местонахождение файла и нажмите **Save**.
Apply	Нажмите эту кнопку для сохранения своих изменений. Изменить можно только имя, исключение составляет самостоятельно подписанный сертификат, который можно установить как сертификат по умолчанию для подписи импортированных сертификатов доверенных удаленных узлов.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

11.3 Экран доверенных центров сертификации

На этом экране отображается сводный список сертификатов от центров сертификации, которые установлены в устройстве P660HN как доверенные. Любой действительный сертификат из этого списка, подписанный центром сертификации, устройство P660HN принимает как надежный, поэтому импорт сертификата, подписанного одним из этих центров сертификации, выполнять не требуется. Нажмите **Security > Certificates > Trusted CAs**, чтобы открыть экран **Trusted CAs**.

Рис. 93 Trusted CAs



В следующей таблице даны описания полей этого экрана.

Табл. 61 Trusted CAs

ПОЛЕ	ОПИСАНИЕ
PKI Storage Space in Use	Этот индикатор показывает находящуюся в использовании память устройства P660HN в процентах для хранения инфраструктуры открытого ключа. Индикатор меняет свой цвет с зеленого на красный, когда память используется полностью. Когда индикатор становится красным, необходимо удалить просроченные или ненужные сертификаты перед добавлением новых сертификатов.
#	В этом поле отображается порядковый номер сертификата. Сертификаты отображаются в алфавитном порядке.
Name	В этом поле отображается описательное имя сертификата.
Subject	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	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**.

Табл. 61 Trusted CAs (продолжение)

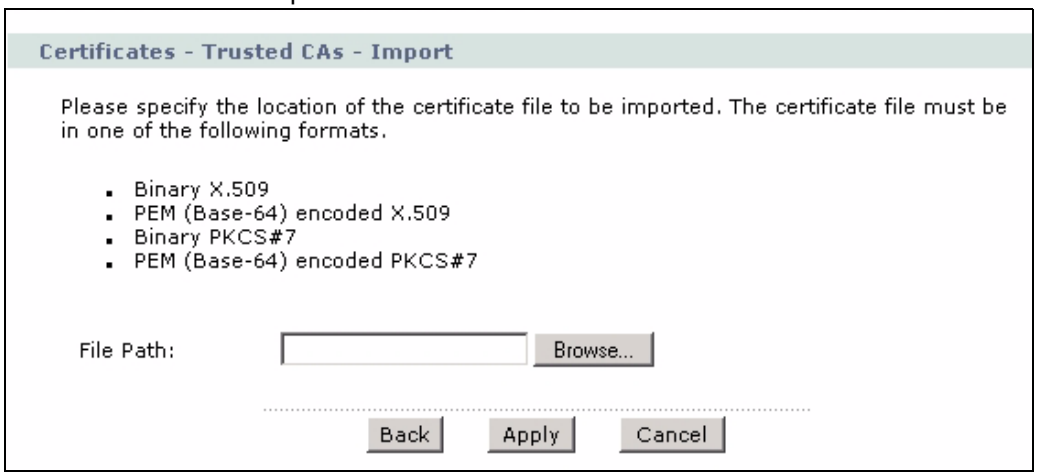
ПОЛЕ	ОПИСАНИЕ
Valid From	В этом поле отображается дата, начиная с которой применяется сертификат. Если сертификат еще не может применяться, то текст в этом поле отображается красным шрифтом и содержит сообщение «Not Yet Valid!» (Еще не действителен!).
Valid To	В этом поле отображается дата, после которой 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	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)** на экране с параметрами сертификата установлен флажок, чтобы устройство P660HN проверяло списки CRL, прежде чем принимать какой-либо сертификат от этого центра сертификации как надежный. В противном случае в этом поле отображается «No» (Нет).
Modify	Щелкните по иконке **Edit**, чтобы открыть экран, содержащий полную информацию о сертификате. Для удаления сертификата щелкните по иконке **Remove**. Появляется окно с запросом на подтверждение операции удаления сертификатов. Следует помнить, что при удалении сертификата все последующие сдвигаются на позицию вверх.
Import	Нажмите эту кнопку, для отображения экрана, где можно перенести сертификат от центра сертификации, который рассматривается как надежный, с вашего компьютера в устройство P660HN.
Refresh	Нажмите эту кнопку для обновления информации о текущем статусе сертификатов.

11.3.1 Импорт доверенного центра сертификации

Следуйте указаниям на этом экране для сохранения сертификата доверенного центра сертификации в устройстве P660HN. Нажмите **Security** > **Certificates** > **Trusted CAs** для отображения экрана **Trusted CAs**, затем нажмите **Import**, чтобы открыть экран **Trusted CA Import**.

Перед импортом необходимо удалить все пробелы в имени файла сертификата.

Рис. 94 Trusted CA Import



В следующей таблице даны описания полей этого экрана.

Табл. 62 Trusted CA Import

ПОЛЕ	ОПИСАНИЕ
File Path	Введите в это поле путь к файлу, который требуется загрузить, или нажмите **Browse** для его поиска.
Browse	Нажмите эту кнопку для поиска файла сертификата, который требуется загрузить.
Back	Нажмите эту кнопку для возврата к предыдущему экрану без сохранения.
Apply	Нажмите эту кнопку для сохранения сертификата в устройстве P660HN.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

11.3.2 Сведения о доверенном центре сертификации

На этом экране отображается подробная информация о сертификате центра сертификации. Здесь также можно изменить имя сертификата и указать, будет ли устройство P660HN проверять список аннулированных сертификатов этого центра, прежде чем принимать какой-либо сертификат от этого центра сертификации как надежный. Нажмите **Security** > **Certificates** > **Trusted CAs**, чтобы открыть экран **Trusted CAs**. Щелкните по иконке дополнительной информации для перехода к экрану **Trusted CA Details**.

Рис. 95 Trusted CA Details

В следующей таблице даны описания полей этого экрана.

Табл. 63 Trusted CA Details

ПОЛЕ	ОПИСАНИЕ
Certificate Name	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 Issues certificate revocation lists (CRLs)	Установите в этом поле флажок, чтобы устройство P660HN проверяло входящие сертификаты, изданные этим центром сертификации, по списку CRL (Certificate Revocation List – Список аннулированных сертификатов). Снимите флажок в этом поле, чтобы устройство P660HN не выполняло проверку входящих сертификатов, изданных этим центром сертификации, по списку CRL (Certificate Revocation List – Список аннулированных сертификатов).

Табл. 63 Trusted CA Details (продолжение)

ПОЛЕ	ОПИСАНИЕ
Certificate Path	Нажмите кнопку **Refresh** 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, устройство P660HN считает сертификат последнего объекта непроверенным, и в этом поле появляется сообщение «Not trusted» (Не подтвержден).
Refresh	Нажмите эту кнопку для отображения пути к сертификату.
Certificate Information	В следующих полях отображается подробная информация о сертификате в режиме только для чтения.
Type	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	В этом поле отображается номер версии X.509.
Serial Number	В этом поле отображается идентификационный номер сертификата, выданного центром сертификации.
Subject	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	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 та же информация, что и в поле **Subject Name**.
Signature Algorithm	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	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	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	В этом поле отображается тип алгоритма, который используется для генерирования пар ключей сертификатов (в устройстве P660HN используется шифрование RSA), и длина ключа в битах (в примере 1024 бит).
Subject Alternative Name	В этом поле отображается IP-адрес (IP), доменное имя (DNS) или адрес электронной почты (EMAIL) владельца сертификата.

Табл. 63 Trusted CA Details (продолжение)

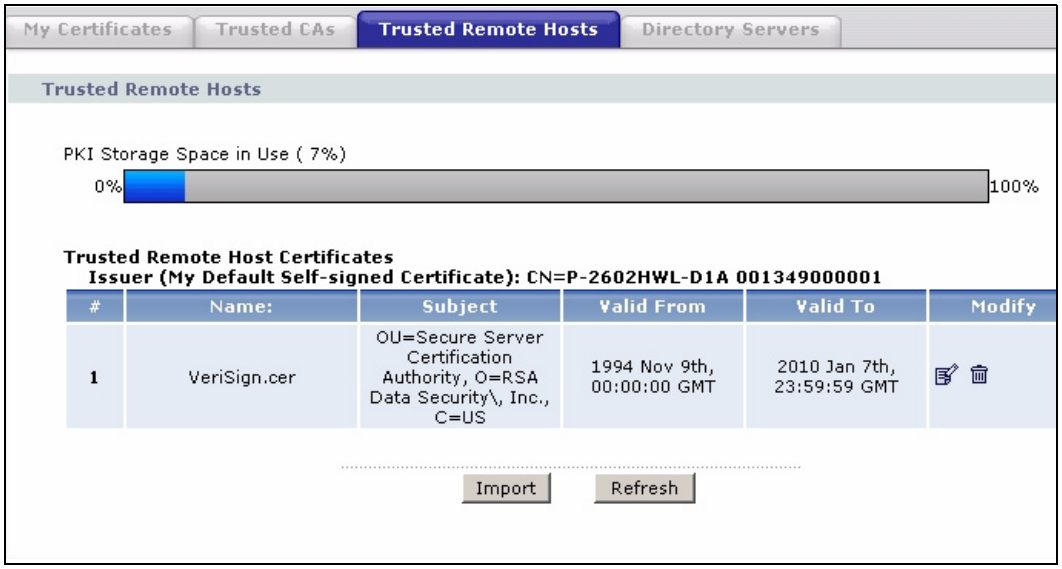
ПОЛЕ	ОПИСАНИЕ
Key Usage	В этом поле отображаются функции, для которых применяется ключ сертификата. Например, «DigitalSignature» (Цифровая подпись) означает, что ключ может использоваться для подписи сертификатов, а «KeyEncipherment» (Шифрование с использованием ключа) означает, что ключ может использоваться для шифрования текста.
Basic Constraint	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	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	Это профиль сообщения сертификата, который устройство P660HN вычислило с использованием алгоритма MD5. По этому значению через центр сертификации можно проверить, действительно ли это выданный им сертификат (например, по телефону).
SHA1 Fingerprint	Это профиль сообщения сертификата, который устройство P660HN вычислило 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	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	Нажмите эту кнопку для возврата к предыдущему экрану без сохранения.
Export	Нажмите эту кнопку, а затем – кнопку **Save** на экране **File Download**. Откроется экран **Save As**. Выберите местонахождение файла и нажмите **Save**.
Apply	Нажмите эту кнопку для сохранения своих изменений. Можно изменить только имя сертификата и/или указать, будет ли устройство P660HN проверять список CRL, издаваемый этим центром сертификации, прежде чем принимать сертификат от этого центра сертификации как надежный.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

11.4 Экраны доверенных удаленных узлов

На этом экране отображается список сертификатов узлов сети, которым вы доверяете, но не подписанных ни одним из центров сертификации, перечисленных на экране **Trusted CAs**. Нажмите **Security > Certificates > Trusted Remote Hosts** для отображения экрана **Trusted Remote Hosts**.

Любой действительный сертификат, подписанный доверенным центром сертификации, устройство P660HN автоматически принимает как надежный, поэтому добавлять сертификат, подписанный центром сертификации, из списка на экране **Trusted CAs** не требуется.

Рис. 96 Trusted Remote Hosts



В следующей таблице даны описания полей этого экрана.

Табл. 64 Trusted Remote Hosts

ПОЛЕ	ОПИСАНИЕ
PKI Storage Space in Use	Этот индикатор показывает находящуюся в использовании память устройства P660HN в процентах для хранения инфраструктуры открытого ключа. Индикатор меняет свой цвет с зеленого на красный, когда память используется полностью. Когда индикатор становится красным, необходимо удалить просроченные или ненужные сертификаты перед добавлением новых сертификатов.
Issuer (My Default Self-signed Certificate)	В этом поле отображается идентифицирующая информация о самостоятельно подписанном сертификате по умолчанию, установленном в устройстве P660HN, и использующемся устройством P660HN для подписи сертификатов доверенных удаленных узлов.
#	В этом поле отображается порядковый номер сертификата. Сертификаты отображаются в алфавитном порядке.
Name	В этом поле отображается описательное имя сертификата.
Subject	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.

Табл. 64 Trusted Remote Hosts (продолжение)

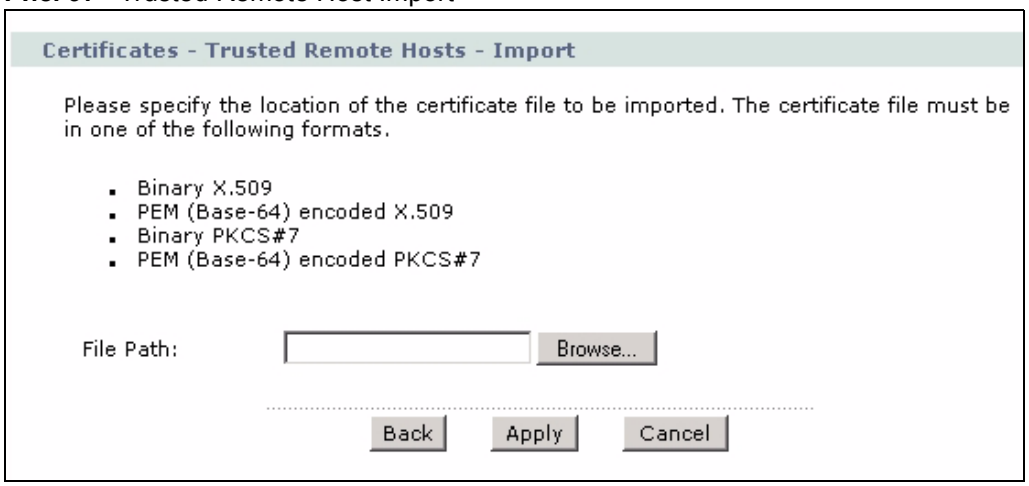
ПОЛЕ	ОПИСАНИЕ
Valid From	В этом поле отображается дата, начиная с которой применяется сертификат. Если сертификат еще не может применяться, то текст в этом поле отображается красным шрифтом и содержит сообщение «Not Yet Valid!» (Еще не действителен!).
Valid To	В этом поле отображается дата, после которой 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	Щелкните по иконке **Edit**, чтобы открыть экран, содержащий полную информацию о сертификате. Для удаления сертификата щелкните по иконке **Remove**. Появляется окно с запросом на подтверждение операции удаления сертификата. Следует помнить, что при удалении сертификата все последующие сдвигаются на позицию вверх.
Import	Нажмите эту кнопку для отображения экрана, где можно перенести сертификат удаленного узла, который рассматривается как надежный, с вашего компьютера на устройство P660HN.
Refresh	Нажмите эту кнопку для обновления информации о текущем статусе сертификатов.

11.4.1 Импорт доверенных удаленных узлов

Нажмите **Security** > **Certificates** > **Trusted Remote Hosts** для отображения экрана **Trusted Remote Hosts** и затем нажмите **Import**, чтобы открыть экран **Trusted Remote Host Import**. Следуйте указаниям на этом экране для сохранения сертификата доверенного узла в устройстве P660HN.

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

Рис. 97 Trusted Remote Host Import



В следующей таблице даны описания полей этого экрана.

Табл. 65 Trusted Remote Host Import

ПОЛЕ	ОПИСАНИЕ
File Path	Введите в это поле путь к файлу, который требуется загрузить, или нажмите **Browse** для его поиска.
Browse	Нажмите эту кнопку для поиска файла сертификата, который требуется загрузить.
Back	Нажмите эту кнопку для возврата к предыдущему экрану без сохранения.
Apply	Нажмите эту кнопку для сохранения сертификата в устройстве P660HN.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

11.4.2 Сведения о сертификате доверенного удаленного узла

На этом экране можно просмотреть подробную информацию о сертификате доверенного удаленного узла и/или изменить имя сертификата. Нажмите **Security** > **Certificates** > **Trusted Remote Hosts** для отображения экрана **Trusted Remote Hosts**. Щелкните по иконке дополнительной информации для перехода к экрану **Trusted Remote Host Details**.

Рис. 98 Trusted Remote Host Details

В следующей таблице даны описания полей этого экрана.

Табл. 66 Trusted Remote Host Details

ПОЛЕ	ОПИСАНИЕ
Certificate Name	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	Нажмите кнопку **Refresh** 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 устройством P660HN для подписи сертификатов удаленных узлов.
Refresh	Нажмите эту кнопку для отображения пути к сертификату.
Certificate Path	В следующих полях отображается подробная информация о сертификате в режиме только для чтения.
Type	В этом поле отображается общая информация о сертификате. Для сертификатов доверенных удаленных узлов в этом поле всегда отображается «CA-signed». Центром сертификации является устройство P660HN, которое подписало 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	В этом поле отображается номер версии X.509.
Serial Number	В этом поле отображается идентификационный номер сертификата, выданного устройством, которое создало сертификат.
Subject	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	В этом поле отображается идентифицирующая информация о самостоятельно подписанном сертификате по умолчанию, установленном в устройстве P660HN, и использующемся устройством P660HN для подписи сертификатов доверенных удаленных узлов.
Signature Algorithm	В этом поле отображается тип алгоритма, с помощью которого устройство P660HN подписало сертификат, например, rsa-pkcs1-sha1 (алгоритм шифрования с использованием открытого-секретного ключа RSA и алгоритм с использованием хэш-функции SHA1).
Valid From	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	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	В этом поле отображается тип алгоритма, который используется для генерирования пар ключей сертификатов (в устройстве P660HN используется шифрование RSA), и длина ключа в битах (в примере 1024 бит).
Subject Alternative Name	В этом поле отображается IP-адрес (IP), доменное имя (DNS) или адрес электронной почты (EMAIL) владельца сертификата.

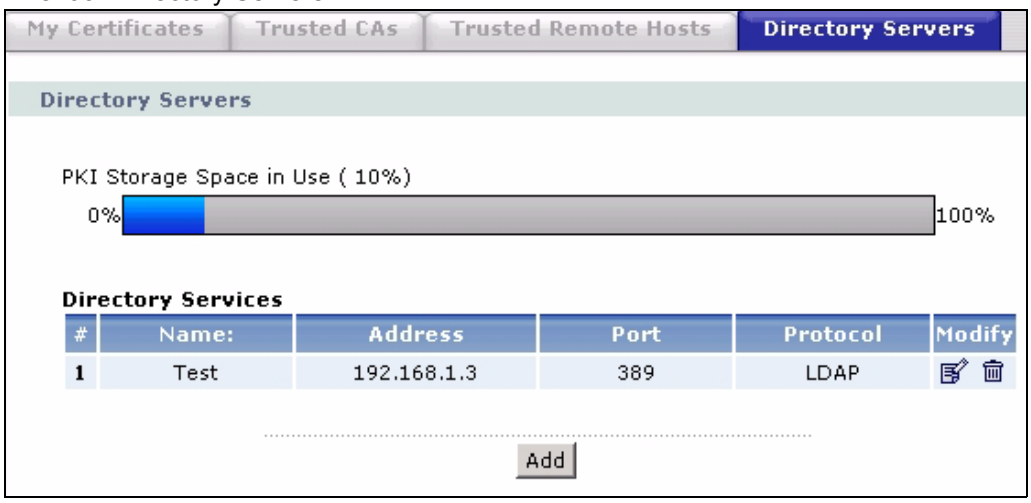
Табл. 66 Trusted Remote Host Details (продолжение)

ПОЛЕ	ОПИСАНИЕ
Key Usage	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	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.
SHA1 Fingerprint	Это профиль сообщения сертификата, который устройство P660HN вычислило с использованием алгоритма MD5. Это значение нельзя использовать для проверки правильности сертификата удаленного узла, так как устройство P660HN уже подписало сертификат, и поэтому это значение будет отличаться от значения в этом же поле на удаленном компьютере.Для проверки сертификата удаленного узла см. Разд. 11.6.3 на с. 200.
SHA1 Fingerprint	Это профиль сообщения сертификата, который устройство P660HN вычислило с использованием алгоритма SHA1. Это значение нельзя использовать для проверки правильности сертификата удаленного узла, так как устройство P660HN уже подписало сертификат, и поэтому это значение будет отличаться от значения в этом же поле на удаленном компьютере.Для проверки сертификата удаленного узла см. Разд. 11.6.3 на с. 200.
Certificate in PEM (Base-64) Encoded Format	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	Нажмите эту кнопку для возврата к предыдущему экрану без сохранения.
Export	Нажмите эту кнопку, а затем – кнопку **Save** на экране **File Download**. Откроется экран **Save As**. Выберите местонахождение файла и нажмите **Save**.
Apply	Нажмите эту кнопку для сохранения своих изменений. Изменить можно только имя сертификата.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

11.5 Экраны серверов каталогов

На этом экране отображается сводный список серверов каталогов (которые содержат списки действительных и аннулированных сертификатов), сохраненный в устройстве P660HN. Если требуется, чтобы устройство P660HN проверяло входящие сертификаты по списку аннулированных сертификатов, выдавшего сертификат центра сертификации, то сначала устройство P660HN проверяет список серверов в поле **CRL Distribution Points** входящего сертификата. Если в сертификате сервер не указан или указанный сервер недоступен, устройство P660HN проверяет серверы, перечисленные в этом поле. Нажмите **Security** > **Certificates** > **Directory Servers** для отображения экрана **Directory Servers**.

Рис. 99 Directory Servers



В следующей таблице даны описания полей этого экрана.

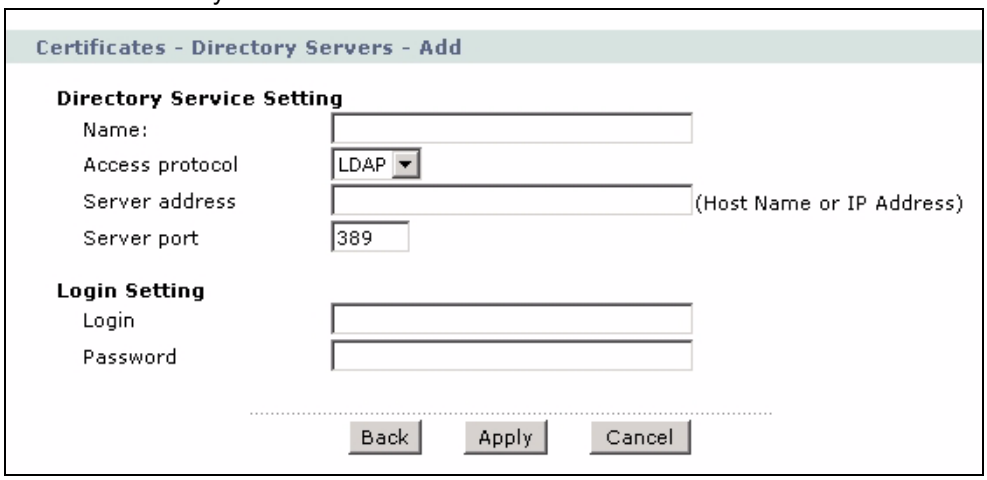
Табл. 67 Directory Servers

ПОЛЕ	ОПИСАНИЕ
PKI Storage Space in Use	Этот индикатор показывает находящуюся в использовании память устройства P660HN в процентах для хранения инфраструктуры открытого ключа. Индикатор меняет свой цвет с зеленого на красный, когда память используется полностью. Когда индикатор становится красным, необходимо удалить просроченные или ненужные сертификаты перед добавлением новых сертификатов.
#	В этом поле отображается порядковый номер сервера каталогов. Серверы отображаются в алфавитном порядке.
Name	В этом поле отображается описательное имя сервера каталогов.
Address	В этом поле отображается IP-адрес или доменное имя сервера каталогов.
Port	В этом поле отображается номер порта, который используется сервером каталогов.
Protocol	В этом поле отображается протокол, который используется сервером каталогов.
Modify	Щелкните по иконке **Edit**, для отображения экрана, где можно изменить параметры сервера каталогов. Щелкните по иконке **Remove** 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	Нажмите эту кнопку для отображения экрана, в котором можно изменить параметры сервера каталогов, чтобы обеспечить к нему доступ устройству P660HN.

11.5.1 Добавление и удаление сервера каталогов

Этот экран служит для настройки параметров сервера каталогов для обеспечения доступа к этому серверу устройству P660HN. Нажмите **Security** > **Certificates** > **Directory Servers** для отображения экрана **Directory Servers**. Нажмите кнопку **Add** (или щелкните по иконке дополнительной информации) для отображения экрана **Directory Server Add**.

Рис. 100 Directory Server Add and Edit



В следующей таблице даны описания полей этого экрана.

Табл. 68 Directory Server Add and Edit

ПОЛЕ	ОПИСАНИЕ
Directory Service Setting	
Name	Введите до 31 символа ASCII (пробелы исключаются) для описания сервера каталогов.
Access Protocol	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	Введите IP-адрес (в десятичном виде с разделительными точками) или доменное имя сервера каталогов.
Server Port	В этом поле отображается номер порта сервера по умолчанию, используемый протоколом, который установлен в поле **Access Protocol**. 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	
Login	Чтобы получить доступ к серверу каталогов, устройству P660HN необходимо пройти аутентификацию. Введите регистрационное имя (до 31 символа ASCII) с объекта, управляющего сервером каталогов (обычно центр сертификации).
Password	Введите пароль (до 31 символа ASCII) с объекта, управляющего сервером каталогов (обычно центр сертификации).
Back	Нажмите эту кнопку, чтобы вернуться к экрану **Directory Servers**.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

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

11.6 Техническая информация о сертификатах

В этом разделе приводится вводная техническая информация по темам данной главы.

11.6.1 Сертификаты – общее описание

Устройство P660HN для аутентификации пользователей может 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.

В устройстве P660HN сертификаты на основе шифрования с использованием открытого ключа применяются для аутентификации пользователей, которые пытаются установить соединение, но не для шифрования данных, передаваемых после установления соединения. 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. Устройство P660HN считает сертификат ненадежным, если срок действия этого сертификата 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). Устройство P660HN 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).

Преимущества сертификатов

Сертификаты имеют следующие преимущества.

- Устройство P660HN 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.

Самостоятельно подписанные сертификаты

Устройство P660HN может выступать в качестве центра сертификации и подписывать свои сертификаты.

11.6.2 Секретные-открытые сертификаты

При использовании аутентификации по открытому ключу каждый узел имеет два ключа. Первый ключ является открытым и может быть доступен всем. Второй ключ является секретным и должен храниться в тайне.

Эти ключи работают как аналоги собственноручной подписи (действительно, о сертификатах зачастую упоминают, как о «цифровых подписях»). Только вы можете воспроизвести свою подпись именно так, как она должна выглядеть. Когда людям известно, как выглядит ваша подпись, они могут понять, был ли документ подписан вами или кем-либо другим. По тому же принципу ваш секретный ключ воспроизводит вашу цифровую подпись, а ваш открытый ключ позволяет другим людям понять, были ли данные подписаны вами или же кем-либо другим. Этот процесс происходит следующим образом.

1. Тим хочет отправить Дженни сообщение. Он хочет быть уверен в том, что сообщение придет именно от него, и его содержимое не сможет изменить какой-либо другой пользователь. Тим создает пару: один открытый ключ и один секретный ключ.
2. Тим хранит у себя секретный ключ и предоставляет открытый ключ в общий доступ. Это значит, что любой пользователь, который получит сообщение от Тима, сможет прочитать его и удостовериться, что оно пришло именно от Тима.
3. Тим подписывает сообщение с помощью секретного ключа и отправляет сообщение Дженни.
4. Дженни получает сообщение и использует открытый ключ Тима для его проверки. Дженни знает, что сообщение пришло от Тима, и, хотя другие пользователи могли прочитать это сообщение, никто не мог изменить его (так как невозможно повторно подписать сообщение, используя секретный ключ Тима).
5. Кроме того, Дженни использует свой секретный ключ для того, чтобы подписать сообщение, а Тим использует открытый ключ Дженни для проверки сообщения.

11.6.3 Проверка сертификата доверенного удаленного узла

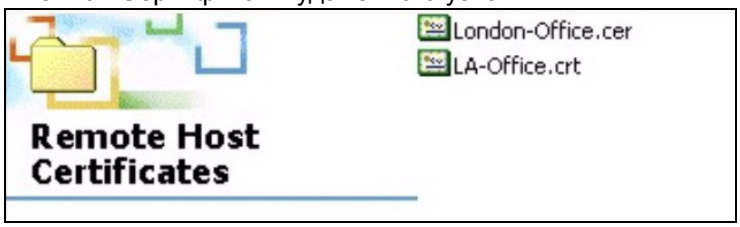
Сертификаты, выданные центрами сертификации, имеют подпись этих центров, предназначенную для проверки. Самостоятельно подписанные сертификаты имеют подпись самого узла. Следовательно, необходимо соблюдать большую осторожность при принятии решения об импорте (а также доверии) самостоятельно подписанного сертификата удаленного узла.

Сигнатуры сертификата доверенного удаленного узла

Сигнатуры сертификатов – это профили сообщений, рассчитанные с использованием алгоритма MD5 или SHA1. Для проверки правильности сертификата удаленного узла с помощью сигнатуры сертификата используется следующая процедура.

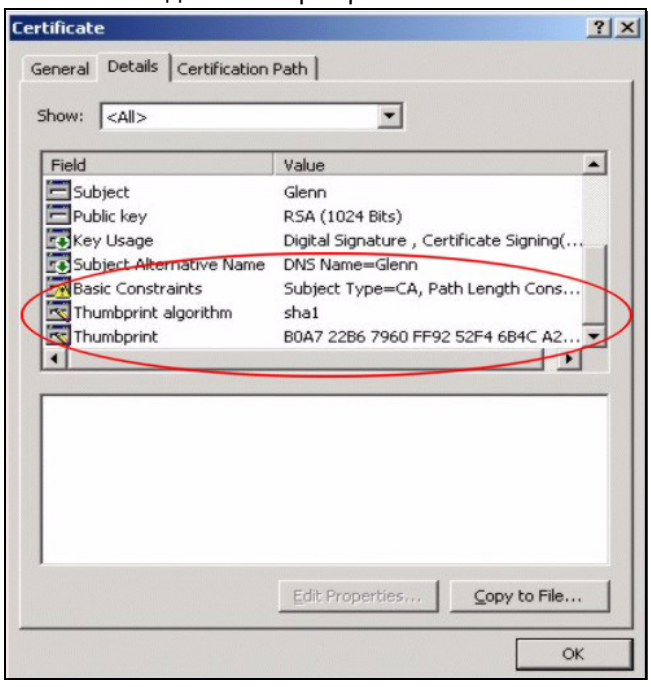
1. Откройте на компьютере папку с сохраненным сертификатом удаленного узла.
2. Убедитесь, что файл сертификата имеет расширение «.cer» или «.crt».

Рис. 101 Сертификаты удаленного узла



3. Дважды щелкните по иконке сертификата, чтобы открыть окно **Certificate**. Щелкните по закладке **Details** и прокрутите окно вниз, чтобы отображались поля **Thumbprint Algorithm** и **Thumbprint**.

Рис. 102 Сведения о сертификате



4. Проверьте, например по телефону, что в полях **Thumbprint Algorithm** и **Thumbprint** на удаленном компьютере содержится такая же информация.

Часть IV
Дополнительные настройки

12

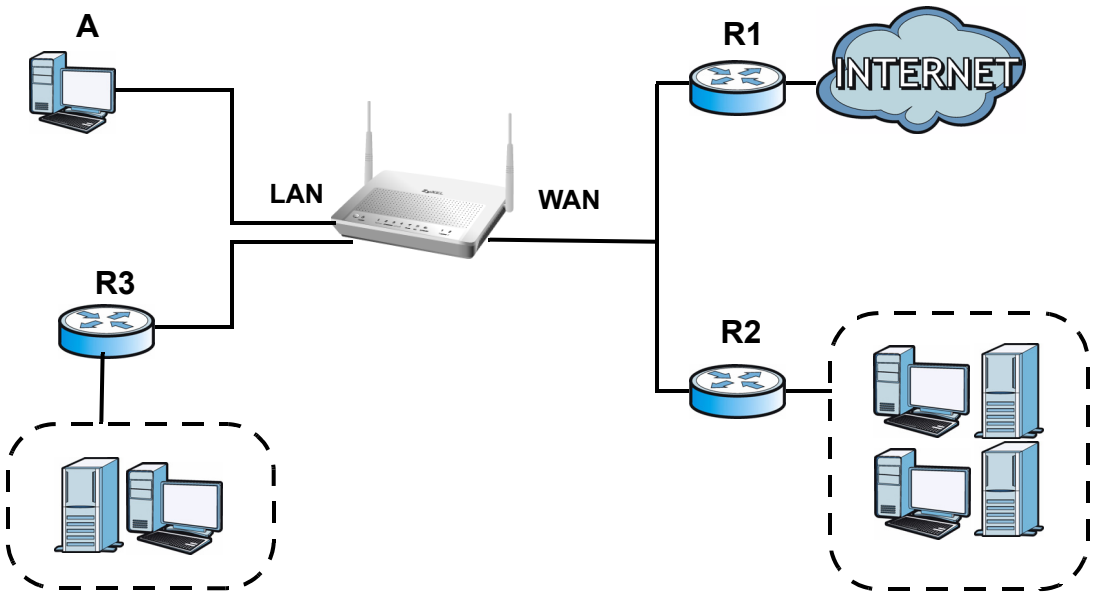
Статический маршрут

12.1 Обзор

Устройство P660HN обычно использует заданный по умолчанию шлюз для маршрутизации исходящего трафика от компьютеров, находящихся в локальной сети, в Интернет. Чтобы маршрутизатор устройства P660HN мог передавать данные на устройства, недоступные через заданный по умолчанию шлюз, используют статические маршруты.

Например, на следующем рисунке показан компьютер (**A**), подключенный к сетевому интерфейсу маршрутизатора устройства P660HN. Маршрутизатор устройства P660HN направляет большую часть трафика от компьютера **A** в Интернет через основной шлюз устройства P660HN, заданный по умолчанию (**R1**). Создается один статический маршрут для подключения к службам, предоставляемым Интернет-провайдером за маршрутизатором **R2**. Другой статический маршрут задается для связи с изолированной сетью, находящейся за маршрутизатором **R3,** подключенным к локальной вычислительной сети.

Рис. 103 Пример топологии статической маршрутизации



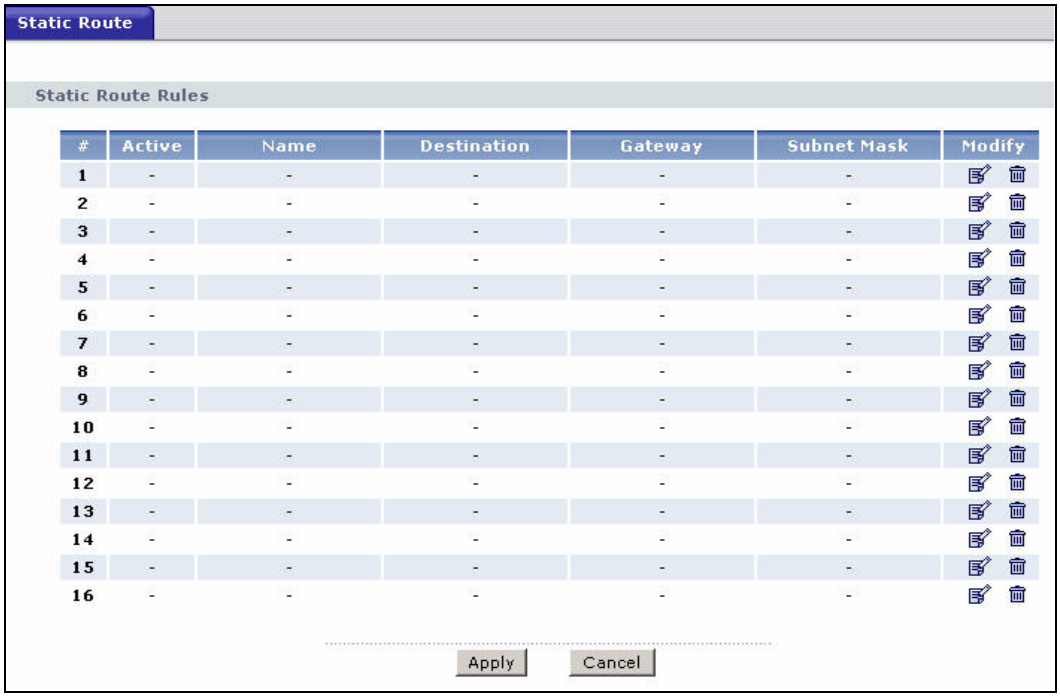
12.1.1 Что можно сделать на экранах статического маршрута

Экран **Static Route** (Разд. 12.2 на с. 203) используется для просмотра и настройки статических маршрутов IP в устройстве P660HN.

12.2 Экран статических маршрутов

Этот экран используется для просмотра правил статической маршрутизации. Нажмите **Advanced > Static Route** для отображения окна **Static Route**.

Рис. 104 Advanced > Static Route



В следующей таблице даны описания полей этого экрана.

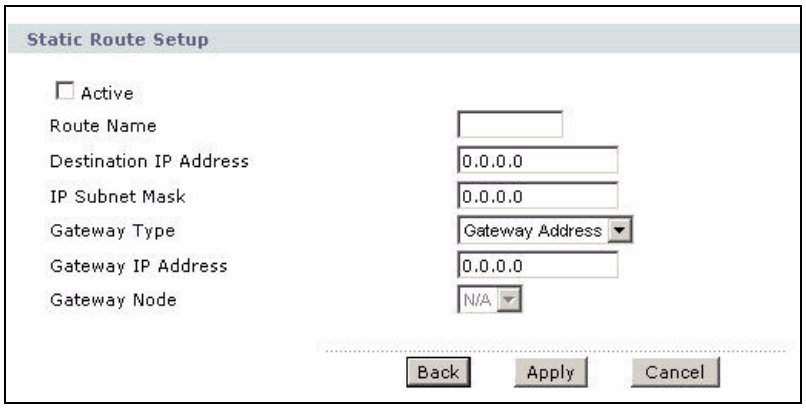
Табл. 69 Advanced > Static Route

ПОЛЕ	ОПИСАНИЕ
#	Номер конкретного маршрута.
Active	Показывает, включено ли правило. Чтобы отключить данное правило, снимите флажок. Для включения соединения поставьте флажок.
Name	Описательное имя данного маршрута.
Destination	Данный параметр определяет IP-адрес сети конечного адресата. Маршрутизация всегда основывается на сетевом номере.
Gateway	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	Данный параметр определяет маску подсети конечного назначения для IP-сети.
Modify	Щелкните по иконке редактирования для перехода к экрану, где можно изменить параметры статического маршрута устройства P660HN. Щелкните по иконке удаления для удаления статического маршрута устройства P660HN. Появится окно с запросом на подтверждение операции удаления маршрута.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

12.2.1 Изменение статического маршрута

Этот экран используется для настройки параметров статического маршрута. Выберите номер статического маршрута и нажмите **Edit**. При этом откроется показанный ниже экран.

Рис. 105 Advanced > Static Route: Edit



В следующей таблице даны описания полей этого экрана.

Табл. 70 Advanced > Static Route: Edit

ПОЛЕ	ОПИСАНИЕ
Active	Это поле служит для включения/отключения данного статического маршрута.
Route Name	Введите имя статического маршрута IP. Текст может состоять не более, чем из 9 букв, цифр и любых печатаемых символов, расположенных на стандартной англоязычной клавиатуре. Чтобы удалить данный статический маршрут, оставьте это поле пустым.
Destination IP Address	Данный параметр определяет IP-адрес сети конечного адресата. Маршрутизация всегда основывается на сетевом номере. Если нужно определить маршрут к отдельной хост-машине, следует использовать маску подсети 255.255.255.255 в поле маски подсети. Это нужно, чтобы сетевой номер был такой же, как и идентификационный номер (ID) хост-машины.
IP Subnet Mask	Введите маску подсети IP.
Gateway Type	Для настройки статического маршрута используйте **Gateway Address** (IP) или **Gateway Node** (PVC).
Gateway IP Address	Это поле доступно, если выбран параметр **Gateway Address** в **Gateway Type**. 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.
Gateway Node	Это поле доступно, если выбран параметр **Gateway Node** в **Gateway Type**. Для настройки статического маршрута выберите удаленный узел, т. е. номер PVC. Удаленный узел представляет собой точку подключения вне локальной вычислительной сети. Одним из примеров удаленного узла является подключение к вашему Интернет-провайдеру. Более подробные сведения о настройке удаленного узла см. в Разд. 4.3 на с. 55.
Back	Нажмите эту кнопку для возврата к предыдущему экрану без сохранения.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

13

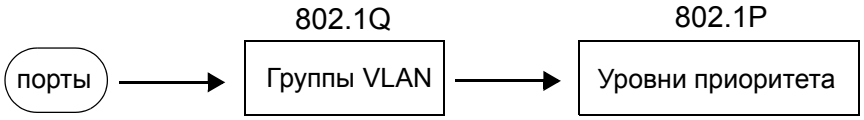
802.1Q/1P

13.1 Обзор

В этой главе описывается настройка параметров 802.1Q/1P.

Виртуальная локальная сеть (VLAN) позволяет разделить физическую сеть на несколько логических сетей. Группа VLAN может рассматриваться как индивидуальное устройство. У каждой группы могут быть свои правила, куда и как направлять трафик. Вы можете назначить любой порт устройства P660HN группе VLAN и настроить параметры для этой группы. Вы также можете установить уровень приоритета для трафика, проходящего через эти порты.

Рис. 106 802.1Q/1P



13.1.1 Что можно сделать на экране 802.1Q/1P

- Экран **Group Setting** (Разд. 13.2 на с. 211) используется для активации 802.1Q/1P, указания управляющей группы VLAN, отображения групп VLAN и настройки параметров для каждой группы VLAN.
- Экран **Port Setting** (Разд. 13.3 на с. 214) используется для настройки PVID и назначения приоритета по трафику для каждого порта.

13.1.2 Что нужно знать о 802.1Q/1P

Приоритет IEEE 802.1P

Стандарт IEEE 802.1P указывает поле с уровнем приоритета пользователя и устанавливает восемь различных типов трафика, образуемых с помощью вставки маркера в кадр на уровне MAC, маркер содержит биты для определения класса услуг.

VLAN IEEE 802.1Q с маркировкой кадров

В виртуальной сети с маркировкой кадров используется явный маркер (VLAN ID – идентификатор виртуальной локальной сети) в заголовке уровня MAC для установления принадлежности пакета к виртуальной LAN при прохождении через мосты – виртуальные сети не ограничиваются устройством, где они были созданы. Идентификатор виртуальной сети указывает на принадлежность пакета к конкретной VLAN и содержит информацию, необходимую для коммутаторов в процессе обработки пакета при перемещении его в сети.

PVC

Виртуальный канал представляет собой логический канал «точка-точка» между клиентскими узлами. Это постоянный канал, так как он препрограммирован владельцем в качестве маршрута в сети. Его не нужно устанавливать или разрывать для каждой сессии.

переадресация маркированных и немаркированных кадров

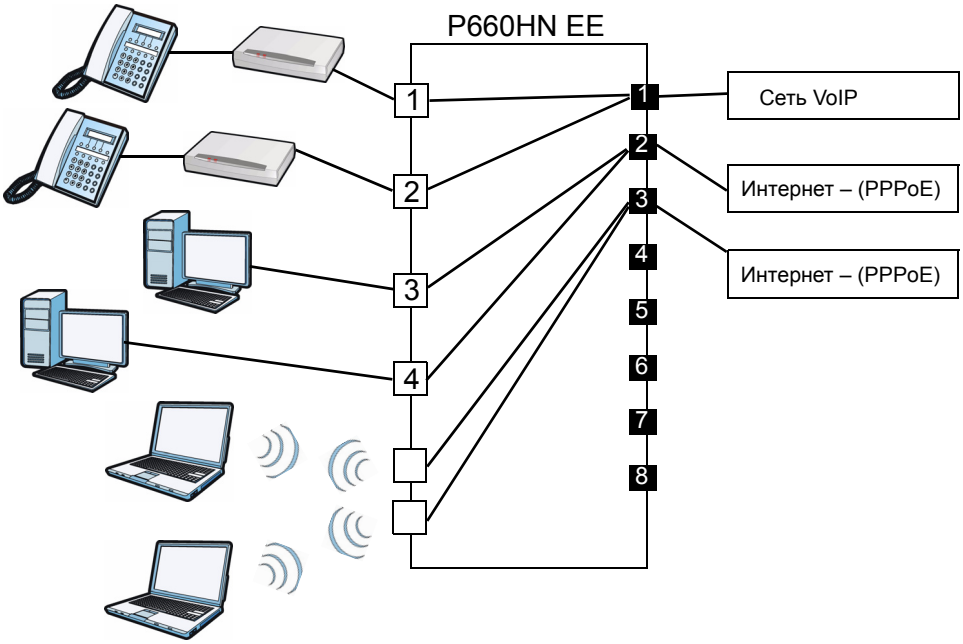
Каждый порт устройства может пересылать как маркированные, так и немаркированные кадры. Чтобы переслать кадр от устройства, имеющего информацию о VLAN 802.1Q к устройству без такой информации, устройство P660HN сначала решает, куда переслать кадр, а затем удаляет маркер VLAN. Чтобы переслать кадр от устройства, не имеющего информации о VLAN 802.1Q к устройству с 802.1Q, устройство P660HN сначала решает, куда переслать кадр, а затем вставляет маркер VLAN, в котором установлен VID входного порта по умолчанию. PVID по умолчанию обозначает VLAN1 для всех портов, но он может быть изменен.

Будет ли присвоен маркер исходящему кадру зависит от установки выходного порта в отношении VLAN на базе порта (напомним, что порт может принадлежать нескольким VID). Если для выходного порта включено присвоение маркеров, кадр передается с маркировкой; в противном случае, он передается как немаркированный кадр.

13.1.3 Пример 802.1Q/1P

В этой главе описывается настройка параметров 802.1Q/1P в устройстве P660HN.

Рис. 107 Пример 802.1Q/1P

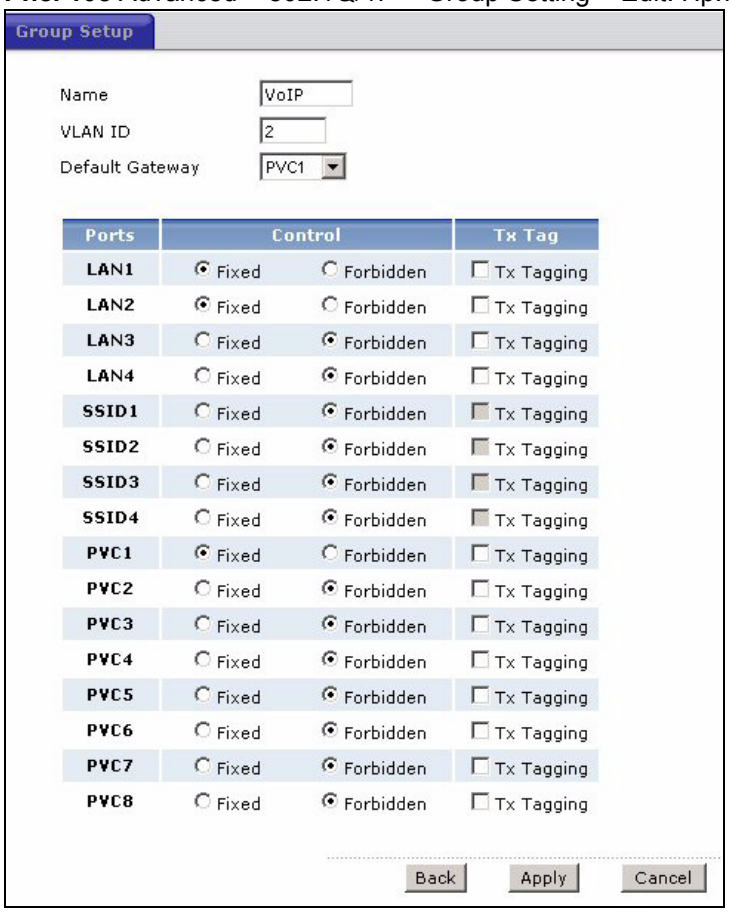


LAN1 и LAN2 подключены к аппаратам аналоговой телефонной связи (ATA) и используются для трафика VoIP. Вам необходимо присвоить высокий приоритет трафику такого типа; вы хотите объединить эти порты в один VLAN (VLAN2), а затем в PVC (PVC1), которому назначен приоритет высокого уровня.

Вам необходимо начать со следующих действий.

1. Нажмите **Advanced** > **802.1Q/1P** > **Group Setting**, а затем нажмите кнопку **Edit** для отображения следующего экрана.
2. В поле **Name** введите VoIP для идентификации группы.
3. В поле **VLAN ID** напечатайте цифру 2 для идентификации группы VLAN.
4. Выберите **PVC1** из выпадающего списка **Default Gateway**.
5. В поле **Control** выберите **Fixed** для LAN1, LAN2 и PVC1, чтобы назначить их постоянными членами группы VLAN.
6. Нажмите **Apply**.

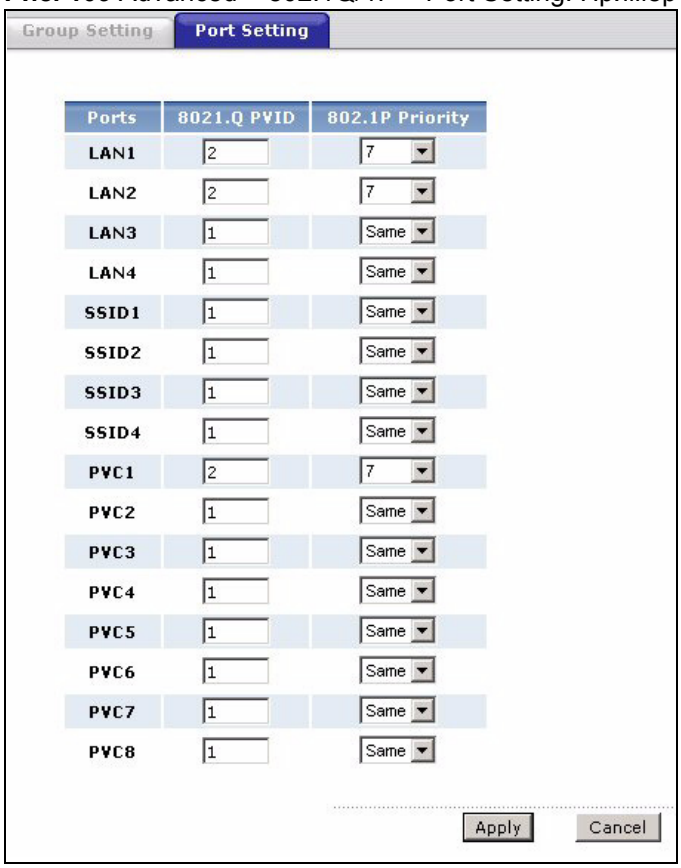
Рис. 108 Advanced > 802.1Q/1P > Group Setting > Edit: Пример



Для того чтобы установить высокий приоритет для трафика VoIP, выполните следующие действия.

1. Нажмите **Advanced** > **802.1Q/1P** > **Port Setting** для отображения следующего экрана.
2. Напечатайте цифру 2 в колонке **802.1Q PVID** для LAN1, LAN2 и PVC1.
3. Выберите **7** из выпадающего списка **802.1P Priority** для LAN1, LAN2 и PVC1.
4. Нажмите **Apply**.

Рис. 109 Advanced > 802.1Q/1P > Port Setting: Пример

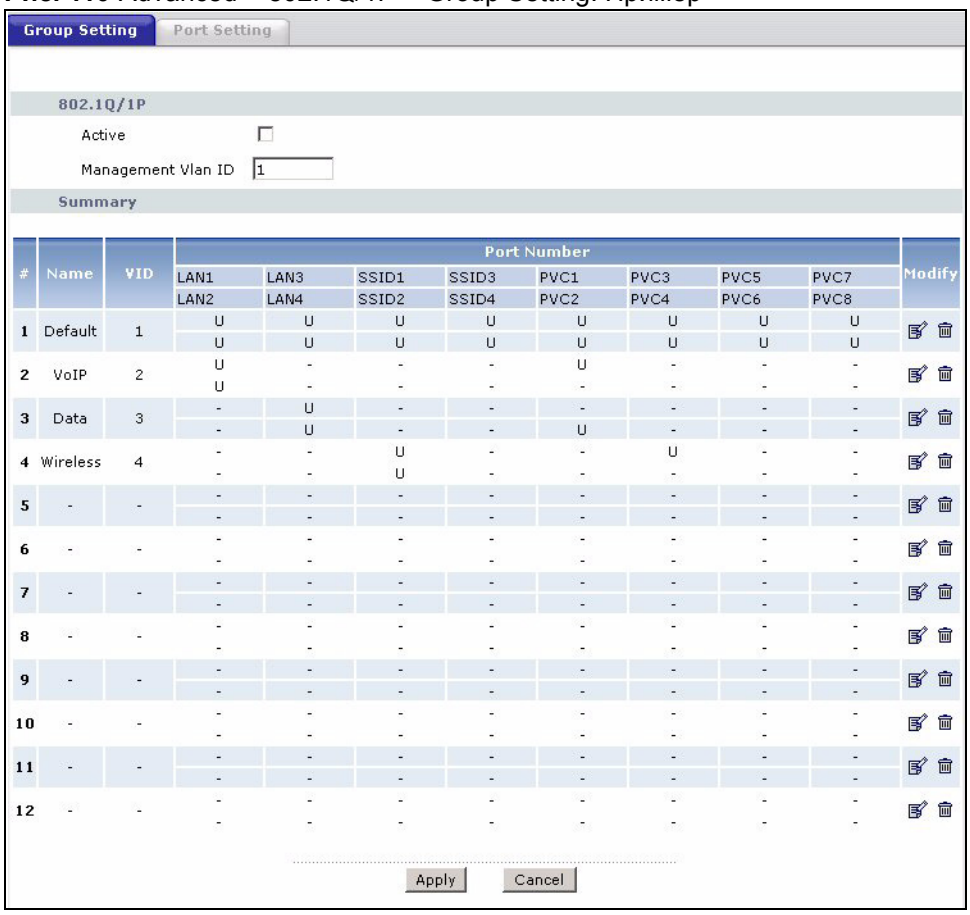


К портам 3 и 4 подключены настольные компьютеры; эти порты используются для Интернет-трафика. Вам необходимо присвоить низкий приоритет трафику такого типа; вы хотите объединить эти порты и PVC2 в один VLAN (VLAN3). PVC2 назначен приоритет низкого уровня.

SSID1 и SSID2 являются двумя беспроводными сетями. Вам необходимо присвоить средний приоритет трафику такого типа; вы хотите объединить эти порты и PVC3 в один VLAN (VLAN4). PVC3 назначен приоритет среднего уровня.

Выполните те же действия, что и в случае с VLAN2, для настройки параметров VLAN3 и VLAN4. Экран сводки будет выглядеть следующим образом.

Рис. 110 Advanced > 802.1Q/1P > Group Setting: Пример

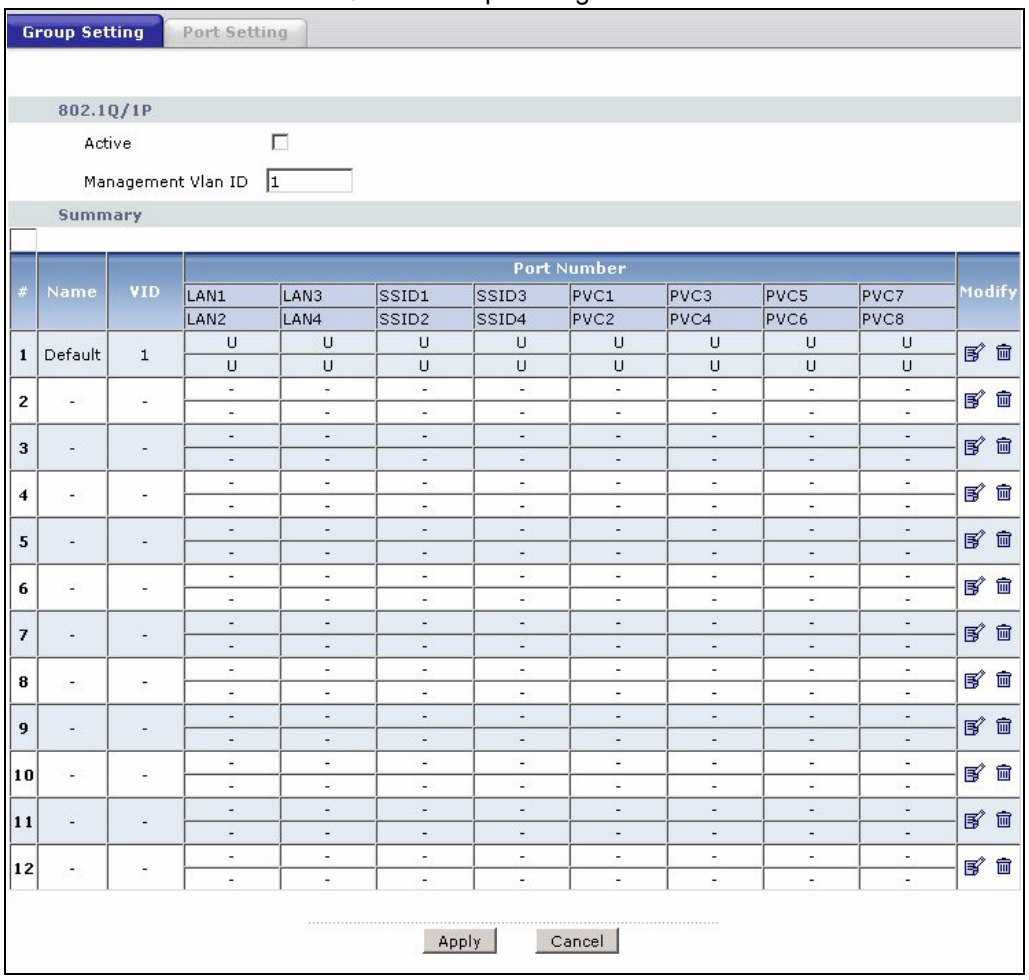


На этом настройка 802.1Q/1P завершена.

13.2 Экран настройки группы 802.1Q/1P

Этот экран используется для активации 802.1Q/1P и отображения групп VLAN. Нажмите **Advanced > 802.1Q/1P** для отображения следующего экрана.

Рис. 111 Advanced > 802.1Q/1P > Group Setting



В следующей таблице даны описания полей этого экрана.

Табл. 71 Advanced > 802.1Q/1P > Group Setting

ПОЛЕ	ОПИСАНИЕ
802.1P/1Q	
Active	Поставьте флажок для активации функции 802.1P/1Q.
Management Vlan ID	Введите идентификатор группы VLAN. Все интерфейсы (порты, SSID и PVC) по умолчанию принадлежат управляющей VLAN. Если вы отключите управляющую VLAN, то не сможете получить доступ к устройству P660HN.
Summary	
#	В этом поле отображается порядковый номер группы VLAN.
Name	В этом поле отображается имя группы VLAN.
VID	В этом поле отображается номер идентификатора группы VLAN.

Табл. 71 Advanced > 802.1Q/1P > Group Setting (продолжение)

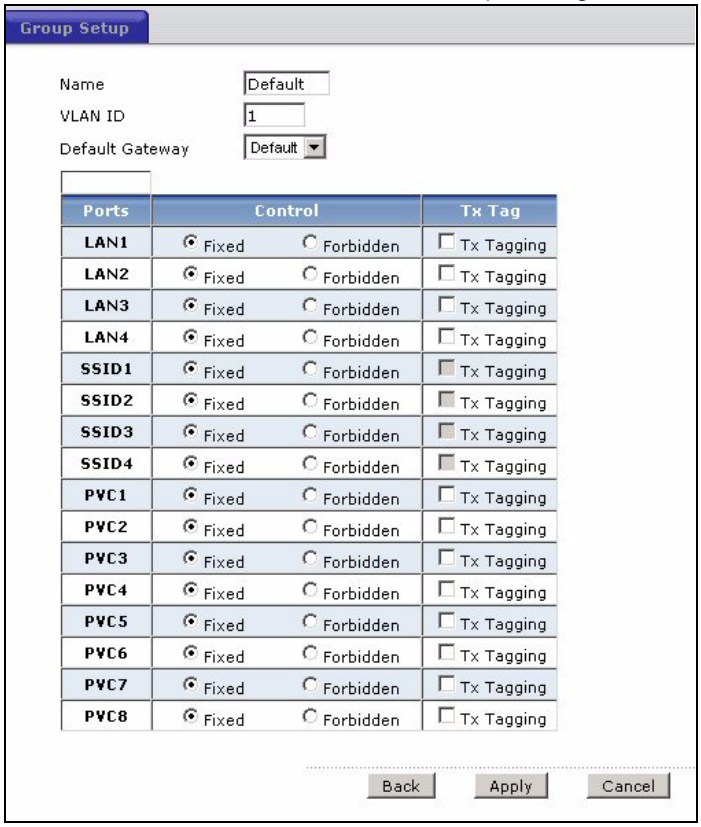
ПОЛЕ	ОПИСАНИЕ
Port Number	В этих колонках отображаются настройки VLAN для каждого порта. Маркированный порт обозначается **T**, немаркированный порт обозначается **U**, а порты, не принадлежащие этой виртуальной сети обозначаются как «**–**».
Modify	Нажмите кнопку **Edit** для изменения параметров портов в группе VLAN. Нажмите кнопку **Remove** для удаления группы VLAN.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

13.2.1 Редактирование настроек группы 802.1Q/1P

Этот экран используется для настройки параметров каждой группы VLAN.

На экране **802.1Q/1P** нажмите кнопку **Edit** в поле **Modify** для отображения следующего экрана.

Рис. 112 Advanced > 802.1Q/1P > Group Setting > Edit



В следующей таблице даны описания полей этого экрана.

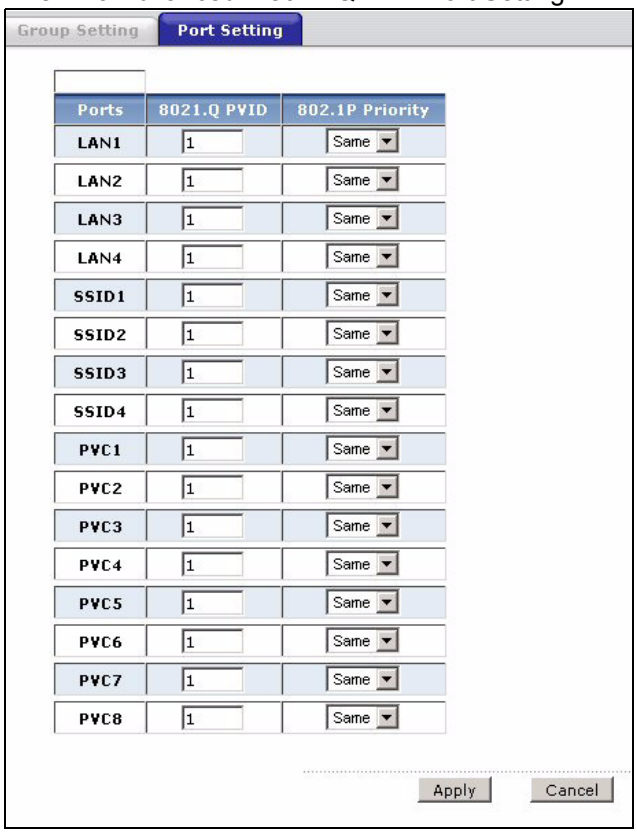
Табл. 72 Advanced > 802.1Q/1P > Group Setting > Edit

ПОЛЕ	ОПИСАНИЕ
Name	Введите описательное имя группы VLAN в целях идентификации. Текст может состоять не более, чем из 8 букв, цифр и символов «-», «_» и «@».
VLAN ID	Назначьте группе VLAN идентификатор (VLAN ID). Допустимый диапазон VID: от 1 до 4094.
Default Gateway	Выберите шлюз по умолчанию для группы VLAN.
Ports	В этом поле отображаются типы портов, которые могут подключиться к группе VLAN.
Control	Выберите **Fixed** для порта, который будет постоянным членом группы VLAN. Выберите **Forbidden**, если вы хотите запретить порту подключаться к данной группе VLAN.
Tx Tag	Выберите **Tx Tagging**, если вы хотите, чтобы порт добавлял маркеры ко всем исходящим пакетам, проходящим через эту группу VLAN. Выберите эту опцию, если вы хотите создавать группы VLAN на разных устройствах, а не только на устройстве P660HN.
Back	Нажмите эту кнопку для возврата к предыдущему экрану без сохранения.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

13.3 Экран настройки портов 802.1Q/1P

Этот экран используется для настройки PVID и назначения приоритета по трафику для каждого порта. Нажмите **Advanced** > **802.1Q/1P** > **Port Setting** для отображения следующего экрана.

Рис. 113 Advanced > 802.1Q/1P > Port Setting



В следующей таблице даны описания полей этого экрана.

Табл. 73 Advanced > 802.1Q/1P > Port Setting

ПОЛЕ	ОПИСАНИЕ
Ports	В этом поле отображаются типы портов, которые могут подключиться к группе VLAN.
802.1Q PVID	Назначьте порту идентификатор (VLAN ID). Допустимый диапазон VID: от 1 до 4094. Устройство P660HN назначает PVID немаркированным кадрам или маркированным по приоритету кадрам, поступающим на этот порт.
802.1P Priority	Назначьте приоритет трафику, проходящему через этот порт. Выберите **Same**, если не хотите изменять приоритет. Вы можете выбрать уровень приоритета **от 0 до 7**, где 0 – самый низкий уровень, а 7 – самый высокий.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

14

Качество услуги (QOS)

14.1 Обзор

Экран **QoS** используется для настройки вашего устройства P660HN, чтобы использовать QoS для управления трафиком.

Качество услуги (QoS) относится как к возможности сети передавать данные с минимальной задержкой, так и к сетевым методам управления полосой частот. QoS позволяет устройству P660HN группировать и назначать приоритет трафику приложений и обеспечивать точную настройку производительности сети.

Без QoS все данные трафика будут потеряны при переполнении сети. Это может привести к снижению производительности сети и неудовлетворительной работе зависящих от времени приложений, например, видео по требованию.

Устройство P660HN присваивает каждому исходящему (т. е. передаваемому в сторону провайдера) пакету приоритет, а затем в соответствии с приоритетом устанавливает очередность этого пакета. Пакеты, которым присвоен высокий приоритет, при переполнении сети обрабатываются быстрее, чем пакеты с низким приоритетом, что улучшает работу приложений, зависящих от времени. Времязависимые приложения включают в себя приложения с низким уровнем времени ожидания (задержкой) и с низким уровнем «дрожания» (изменений задержки), например для Voice over IP (VoIP) или игр в Интернете, а также те, для которых само «дрожание» уже представляет собой проблему: Интернет-радио или потоковое видео.

14.1.1 Что можно сделать на экранах QoS

- Экран **General** (Разд. 14.2 на с. 219) используется для включения QoS на устройстве P660HN, определения максимально допустимой пропускной способности с помощью QoS и конфигурирования настроек отображения приоритета для трафика, который не соответствует пользовательскому классу.
- Экран **Class Setup** (Разд. 14.3 на с. 220) используется для настройки классификаторов, сортирующих трафик на разные потоки, присваивающих им приоритет и определяющих действия, которые необходимо выполнять с классифицированным потоком трафика.
- Экран **Monitor** (Разд. 14.4 на с. 226) используется для просмотра статистики пакетов, относящихся к QoS на устройстве P660HN.

14.1.2 Что нужно знать о QoS

QoS и CoS

QoS (Quality of Service – Качество обслуживания) используется для установки приоритета для потоков трафика источник-адресат. Пакеты, находящиеся в одном потоке, имеют одинаковый приоритет. CoS (Class of Service – Класс обслуживания) это способ управления трафиком в сети за счет группирования вместе одинаковых типов трафика и обработки каждого типа как класса. Можно использовать CoS для назначения разных приоритетов различным типам пакетов.

Технологии CoS включают присвоение маркеров по уровню 2 IEEE 802.1p и дифференцированное обслуживание (DiffServ или DS). При присвоении маркеров IEEE 802.1p используется три бита заголовка пакета, а DiffServ является новым протоколом, который создает новое поле DS, заменяющее восьмибитное поле типа обслуживания (TOS) в IP-заголовке.

Присвоение тегов и маркировка

В классе QoS можно добавить или изменить значение кода службы (DSCP), уровень приоритета IEEE 802.1p и идентификационный номер VLAN в совпадающем пакете. Когда пакет проходит через совместимую сеть, то сетевое устройство, такое как магистральный коммутатор, может обеспечить специальную обработку или обслуживание на основании тега или маркера.

Дополнительные сведения

Техническую вводную информацию о QoS см. в Разд. 14.5 на с. 227.

14.1.3 Пример установки класса QoS

На приведенном ниже рисунке ваше подключение к Интернету имеет скорость передачи данных 50 Мбит/с. Вы настраиваете классификатор, чтобы присвоить наивысший приоритет очереди (6) для трафика VoIP из интерфейса LAN так, чтобы голосовой трафик не задерживался при переполнении сети. Трафик с IP-адреса управляющего (например, 192.168.1.23) отображается как приоритет очереди 5. Трафик, который не соответствует этим двум классам присваиваемого приоритета, основывается на внутренней таблице отображений QoS в устройстве P660HN.

Рис. 114 Пример QoS

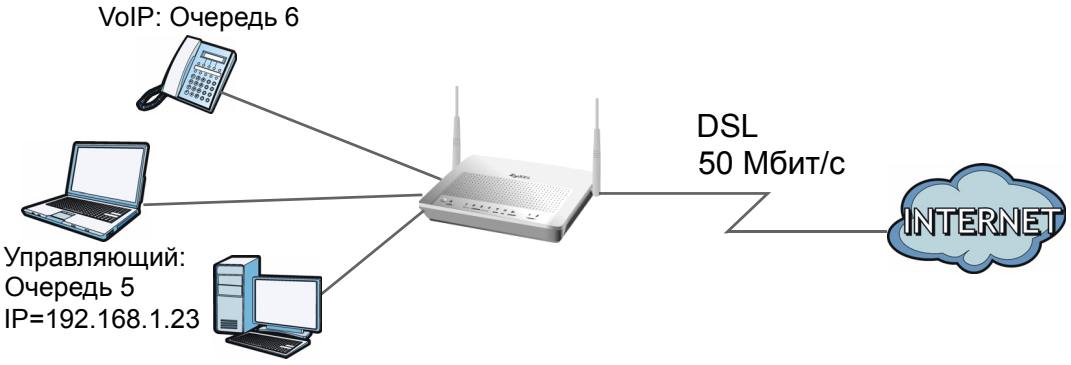


Рис. 115 Пример установки класса QoS: VoIP -1

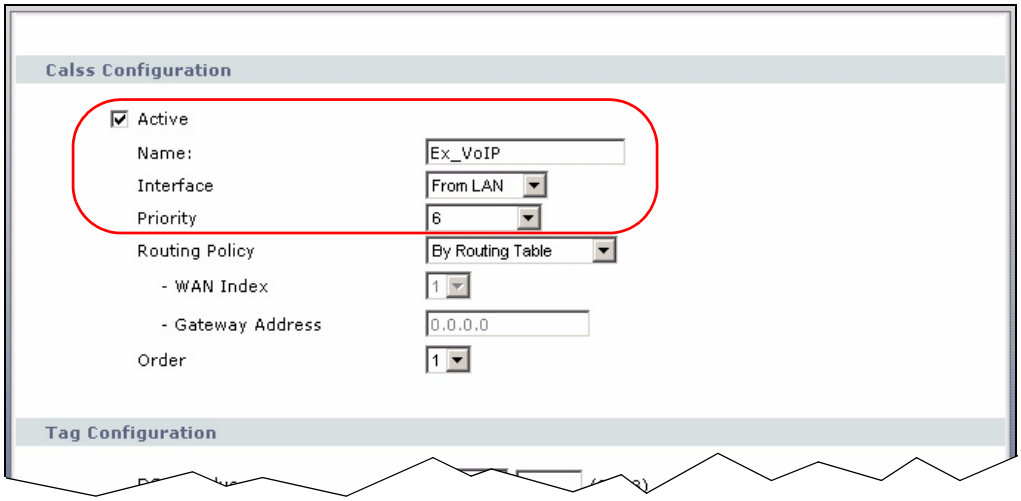


Рис. 116 Пример установки класса QoS: VoIP -2

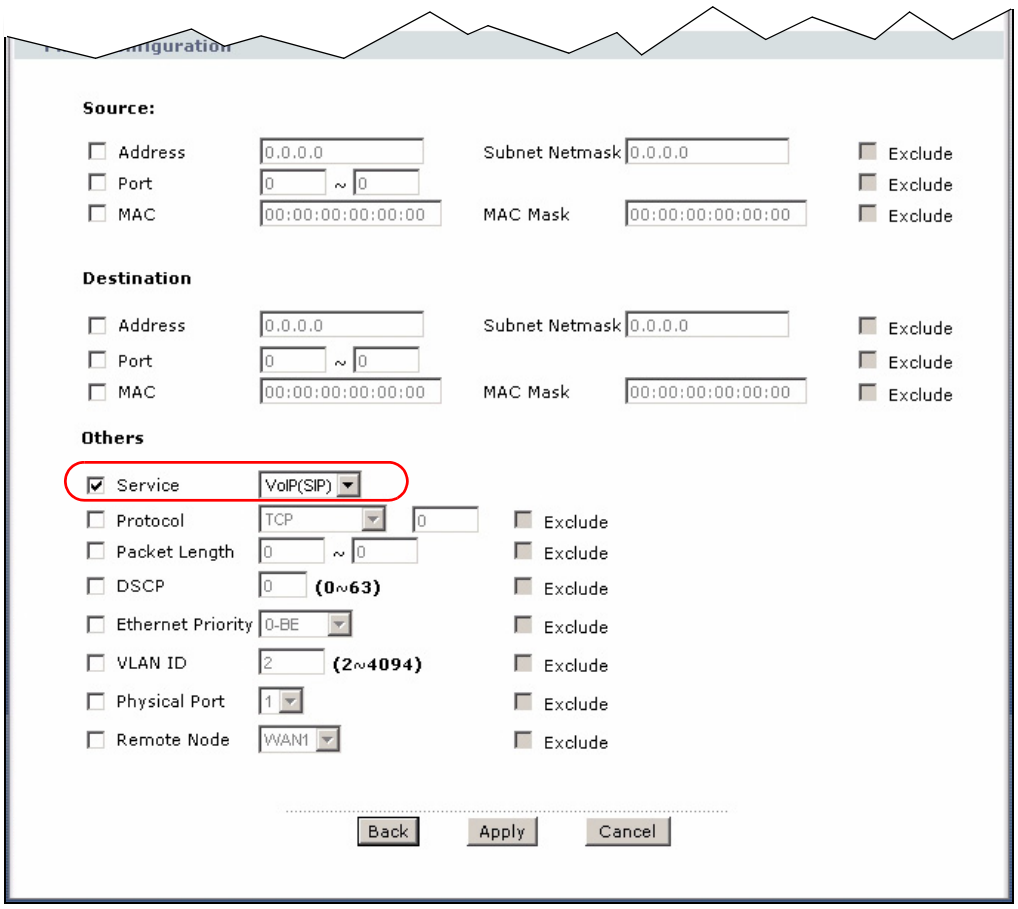


Рис. 117 Пример установки класса QoS: Управляющий -1

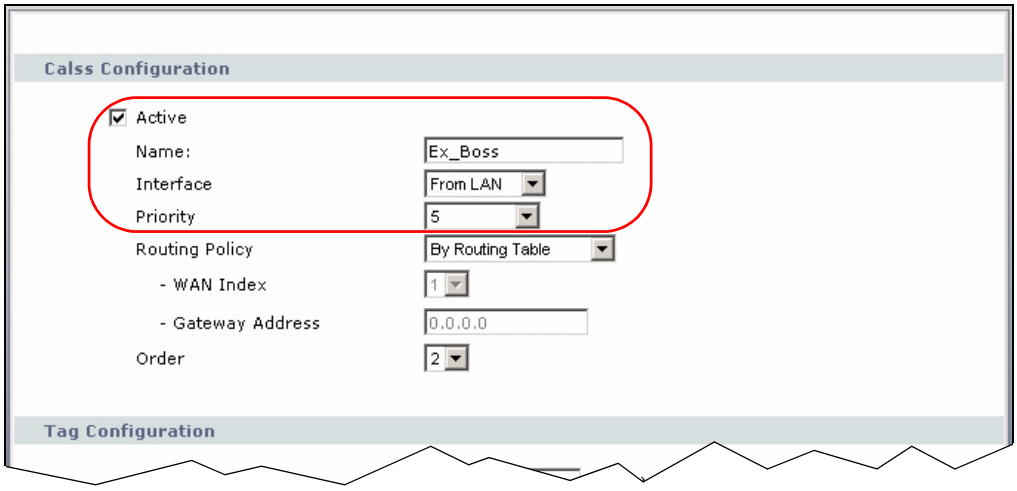
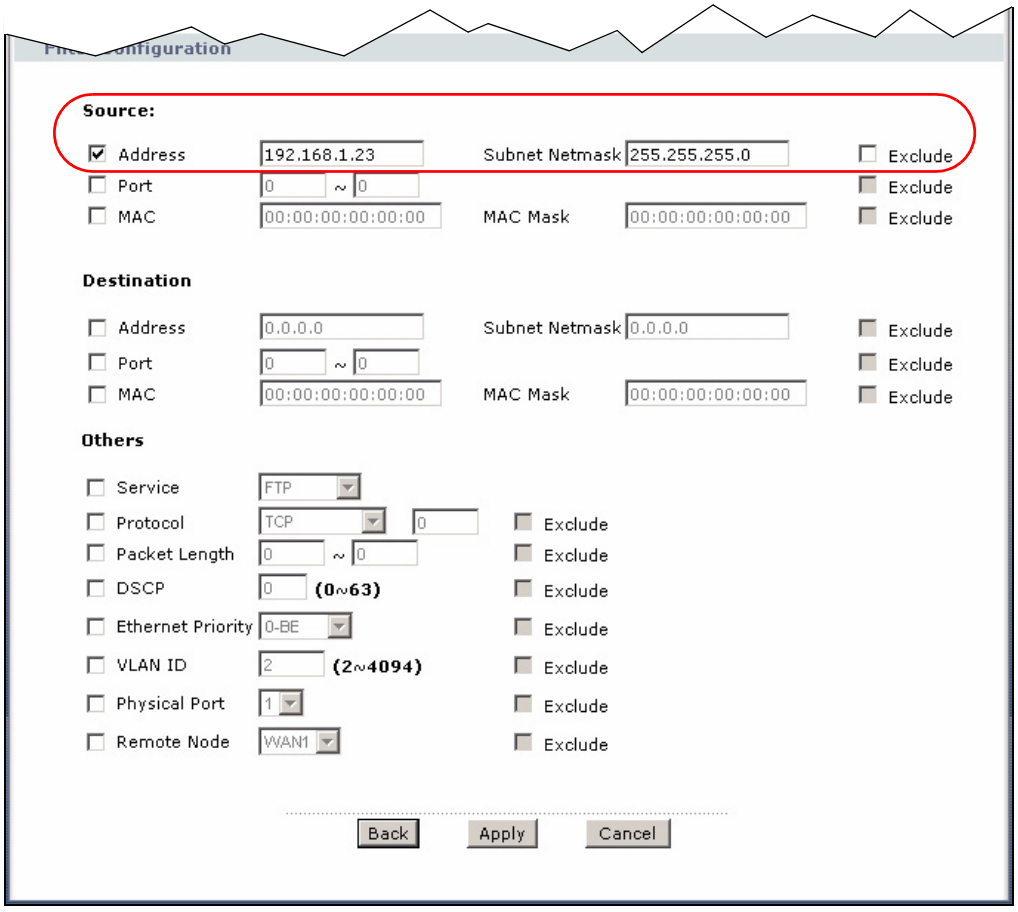


Рис. 118 Пример установки класса QoS: Управляющий -2

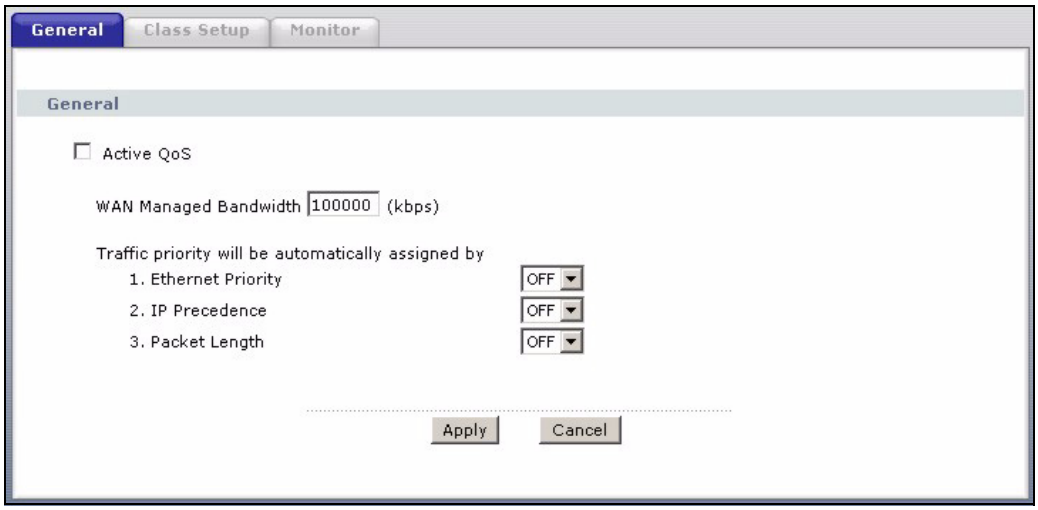


14.2 Экран общей настройки QoS

Этот экран используется для включения или отключения QoS и настройки вашего устройства P660HN так, чтобы оно автоматически присваивало уровень приоритета трафику в соответствии с уровнем приоритета IEEE 802.1p, очередностью IP-адреса и/или длиной пакета.

Нажмите **Advanced > QoS**, чтобы открыть приведенный ниже экран.

Рис. 119 Advanced > QoS > General



В следующей таблице даны описания полей этого экрана.

Табл. 74 Advanced > QoS > General

ПОЛЕ	ОПИСАНИЕ
Active QoS	Поставьте флажок для включения QoS с целью улучшения производительности сети. Можно установить приоритет для трафика, который устройство P660HN пересылает через интерфейс WAN. Установите высокий приоритет для голосовых и видео-данных, чтобы обеспечить равномерность их передачи. Аналогичным образом, установите низкий приоритет для многочисленных объемных загружаемых файлов так, чтобы они не понизили качество работы других приложений.
WAN Managed Bandwidth	Введите пропускную способность интерфейса WAN, которую необходимо назначить с помощью QoS. Рекомендуется установить скорость, соответствующую фактической скорости передачи интерфейса. Например, установите скорость интерфейса WAN равной 100000 кбит/с, если подключение к Интернету имеет скорость **исходящего** потока 100 Мбит/с. Это значение можно установить выше, чем фактическая скорость передачи интерфейса. При этом передача трафика с более низким приоритетом будет остановлена, если трафик с более высоким приоритетом использует всю пропускную способность. Также это значение можно установить ниже, чем фактическая скорость передачи интерфейса. Вследствие этого устройство P660HN будет не полностью использовать доступную пропускную способность.

Табл. 74 Advanced > QoS > General (продолжение)

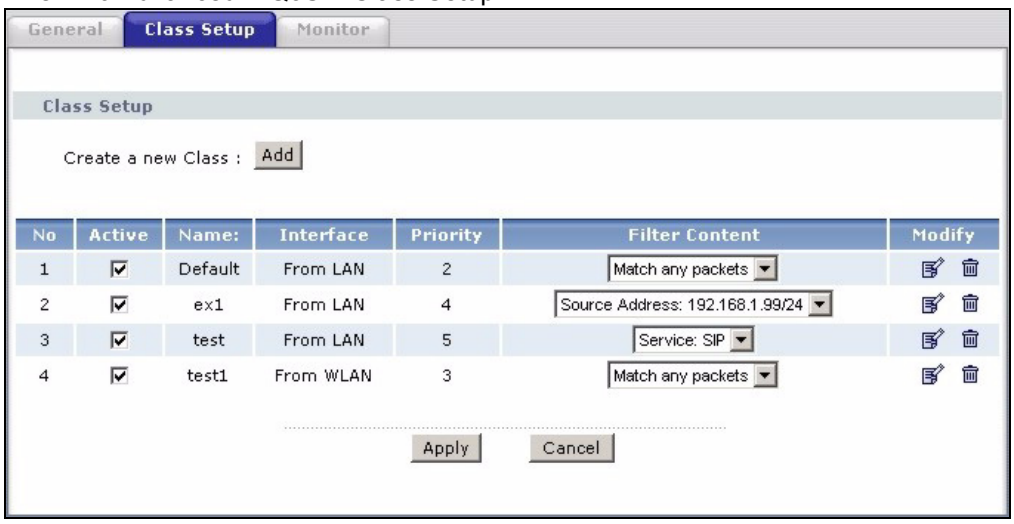
ПОЛЕ	ОПИСАНИЕ
Traffic priority will be automatically assigned by	Эти поля игнорируются, если трафик соответствует классу, настроенному на экране **Class Setup**. При выборе **ON** и несоответствии трафика классу, настроенному на экране **Class Setup**, устройство P660HN назначает приоритет несоответствующему трафику на основании уровня приоритетов стандарта IEEE 802.1p, IP-очередности и/или длины пакетов. Более подробную информацию см. в Разд. 14.5.4 на с. 229. При выборе **OFF** трафик, не соответствующий классу, отображается как приоритет очереди 2.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

14.3 Экран настройки класса

Этот экран используется для добавления, редактирования или удаления классификаторов. Классификатор группирует трафик в потоки данных по специальным критериям, таким как адрес источника, адрес назначения, номер порта источника, номер порта назначения или входящего интерфейса. Например, можно настроить классификатор, чтобы он выбирал трафик с одного и того же порта протокола (например, Telnet) для формирования потока.

Нажмите **Advanced > QoS > Class Setup**, чтобы открыть приведенный ниже экран.

Рис. 120 Advanced > QoS > Class Setup



В следующей таблице даны описания полей этого экрана.

Табл. 75 Advanced > QoS > Class Setup

ПОЛЕ	ОПИСАНИЕ
Create a new Class	Нажмите для создания нового классификатора.
No	В этом поле отображается номер классификатора. Порядок следования классификаторов очень важен, так как они применяются по очереди.
Active	Поставьте флажок в этом поле для включения классификатора.
Name	Это имя классификатора.

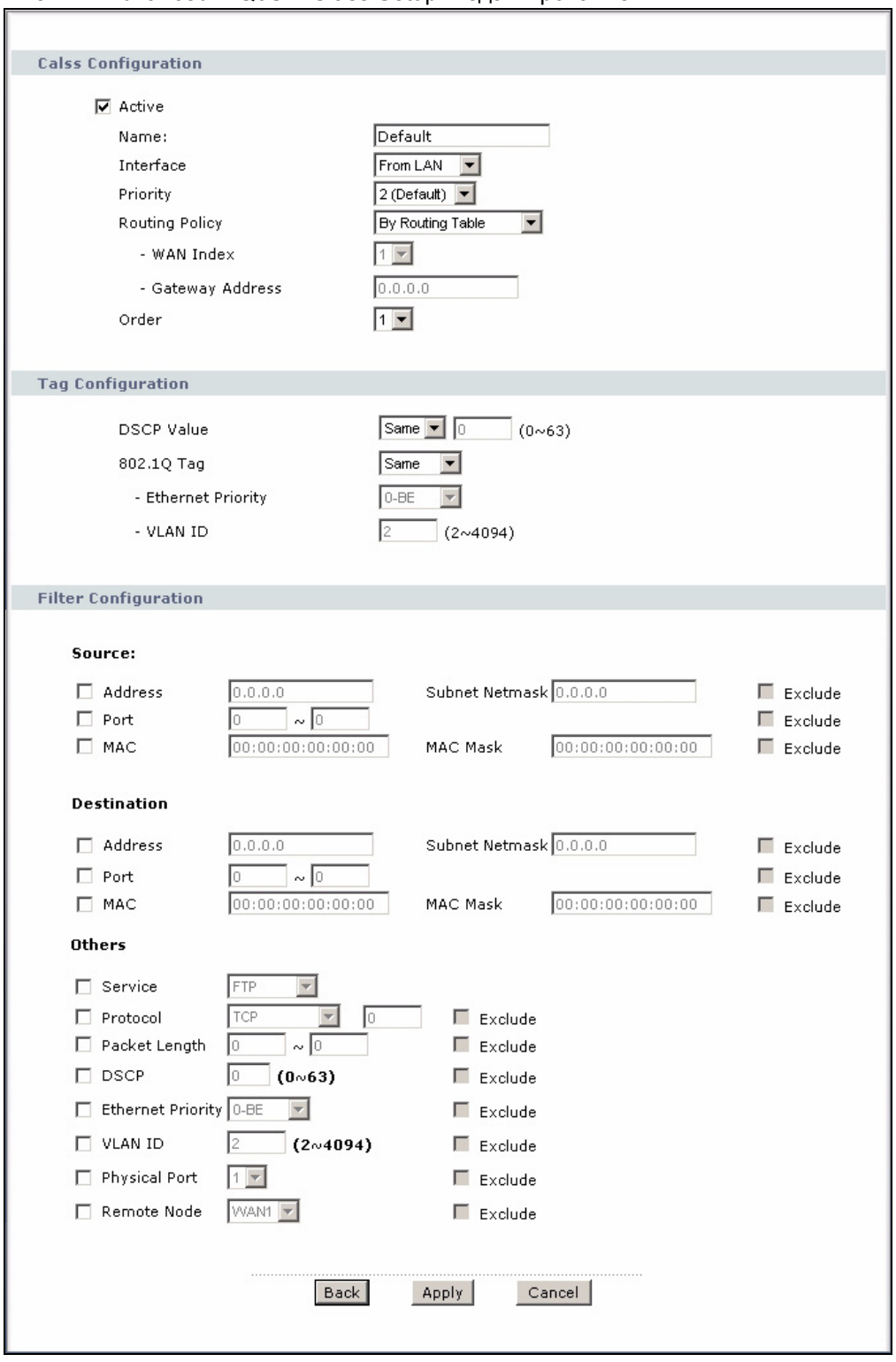
Табл. 75 Advanced > QoS > Class Setup (продолжение)

ПОЛЕ	ОПИСАНИЕ
Interface	Здесь указан интерфейс, с которого должен поступать трафик этого классификатора.
Priority	Это приоритет, назначенный трафику этого классификатора.
Filter Content	Здесь указаны критерии этого классификатора.
Modify	Щелкните по иконке редактирования для перехода к экрану, где можно менять параметры классификатора. Для удаления существующего классификатора щелкните по иконке удаления.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

14.3.1 Экран конфигурирования параметров класса

Этот экран используется для конфигурирования параметров классификатора. Нажмите кнопку **Add** или щелкните по иконке **Edit** в поле **Modify** для отображения следующего экрана.

Рис. 121 Advanced > QoS > Class Setup: Редактирование



Список широко используемых служб см. в Прил. E на с. 354. В следующей таблице даны описания полей этого экрана.

Табл. 76 Advanced > QoS > Class Setup: Редактирование

ПОЛЕ	ОПИСАНИЕ
Class Configuration	
Active	Поставьте флажок в этом поле для включения классификатора.
Name	Текст может состоять не более, чем из 20 букв, цифр и любых печатаемых символов, расположенных на стандартной англоязычной клавиатуре.
Interface	Выберите, с какого интерфейса должен поступать трафик этого класса.
Priority	Выберите уровень приоритетности (от 0 до 7) или выберите **Auto** для того, чтобы устройство P660HN отображало соответствующий трафик в очереди в соответствии с внутренней таблицей отображений QoS. Более подробную информацию см. в Разд. 14.5.4 на с. 229. Ноль – самый низкий приоритет, а семь – самый высокий.
Routing Policy	Выберите следующий транзитный пункт, на который должен быть перенаправлен трафик этого типа. Выберите **By Routing Table**, чтобы устройство P660HN использовало таблицу маршрутизации для поиска следующего транзитного пункта и автоматически перенаправляло совпадающие пакеты. Выберите **To WAN Index** для маршрутизации совпадающих пакетов через указанный PVC. Эта опция доступна, только если типом WAN является ADSL. Выберите **To Gateway Address** для маршрутизации совпадающих пакетов на маршрутизатор или коммутатор, указанный в поле **Gateway Address**.
WAN Index	Выберите порядковый номер PVC.
Gateway IP Address	Введите IP-адрес шлюза, который должен быть маршрутизатором или коммутатором в том же сегменте, что и интерфейс устройства P660HN, способный переправить пакет в место назначения.
Order	Здесь указывается порядковый номер классификатора. Выберите существующий номер позиции, куда вы хотели бы поместить классификатор, и нажмите **Apply** для того, чтобы переместить классификатор на ту позицию, которую вы выбрали. Например, при выборе «2», классификатор, который вы перемещаете, получает номер 2, а прежний классификатор смещается вниз на одну позицию.
Tag Configuration	
DSCP Value	Выберите **Same** для сохранения полей DSCP в пакетах. Выберите **Auto** для автоматического отображения значения DSCP как уровня приоритета 802.1. Выберите **Mark**, чтобы установить в поле DSCP значение, которое можно сконфигурировать в этом поле.
802.1Q Tag	Выберите **Same** для сохранения настройки приоритета и идентификатора VLAN кадров. Выберите **Auto** для автоматического отображения уровня приоритета 802.1 как значения DSCP. Выберите **Remove** для удаления маркировки приоритета очереди и идентификатора VLAN кадров. Выберите **Mark** для замены значения в поле приоритета 802.1 и идентификатора VLAN значением, которое указано в полях ниже. Выберите **Add** для того, чтобы оставить все совпадающие пакеты без маркировки, и добавить маркировку второго приоритета очереди и VLAN.
Ethernet Priority	Выберите из разворачивающегося списка уровень приоритета (от 0 до 7).
VLAN ID	Укажите номер идентификатора VLAN между 2 и 4094.

Табл. 76 Advanced > QoS > Class Setup: Редактирование (продолжение)

ПОЛЕ	ОПИСАНИЕ
Filter Configuration	Используйте следующие поля для конфигурирования классификации трафика.
Source	
Address	Установите флажок и введите IP-адрес источника в десятичном виде с разделительными точками. Пустое поле означает любой IP-адрес источника.
Subnet Netmask	Введите маску подсети отправителя. Для получения дополнительной информации о подсетях IP см. приложение.
Port	Установите флажок и введите номер порта источника. 0 означает любой порт источника. См. Прил. E на с. 354 с указанием распространенных служб и номеров портов.
MAC	Установите флажок и введите MAC-адрес источника пакета.
MAC Mask	Введите маску для указанного MAC-адреса для определения того, каким битам MAC-адрес пакета должен соответствовать. Введите «f» для каждого бита указанного MAC-адреса источника, которому должен соответствовать MAC-адрес трафика. Введите «0» для бита(ов) MAC-адреса совпадающих пакетов трафика, которые могут состоять из любого шестнадцатеричного символа(ов). Например, если вы укажете MAC-адрес 00:13:49:00:00:00, а маску – ff:ff:ff:00:00:00, то пакет с MAC-адресом 00:13:49:12:34:56 будет соответствовать этому критерию.
Exclude	Выберите эту опцию для того, чтобы исключить пакеты, совпадающие с указанными критериями, из этого классификатора.
Destination	
Address	Установите флажок и введите IP-адрес назначения в десятичном виде с разделительными точками.
Subnet Netmask	Введите маску подсети получателя. Для получения дополнительной информации о подсетях IP см. приложение.
Port	Установите флажок и введите номер порта назначения.0 означает любой порт источника. См. Прил. E на с. 354 с указанием распространенных служб и номеров портов.
MAC	Установите флажок и введите MAC-адрес назначения пакета.
MAC Mask	Введите маску для указанного MAC-адреса для определения того, каким битам MAC-адрес пакета должен соответствовать. Введите «f» для каждого бита указанного MAC-адреса назначения, которому должен соответствовать MAC-адрес трафика. Введите «0» для бита(ов) MAC-адреса совпадающих пакетов трафика, которые могут состоять из любого шестнадцатеричного символа(ов). Например, если вы укажете MAC-адрес 00:13:49:00:00:00, а маску – ff:ff:ff:00:00:00, то пакет с MAC-адресом 00:13:49:12:34:56 будет соответствовать этому критерию.
Exclude	Выберите эту опцию для того, чтобы исключить пакеты, совпадающие с указанными критериями, из этого классификатора.
Others	

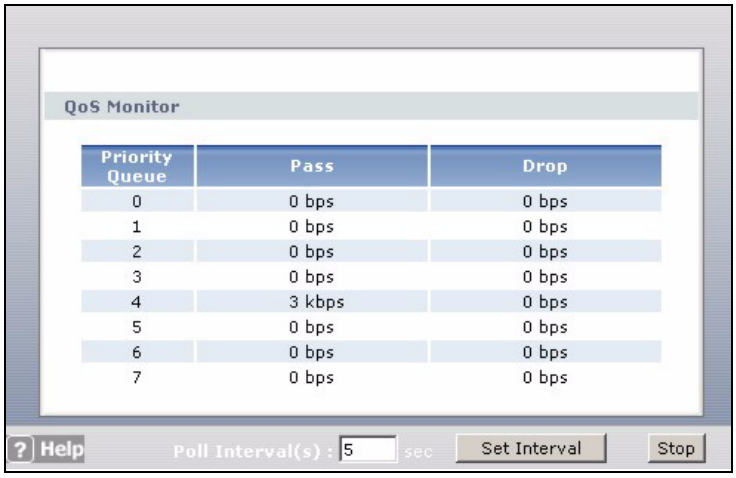
Табл. 76 Advanced > QoS > Class Setup: Редактирование (продолжение)

ПОЛЕ	ОПИСАНИЕ
Service	Это поле упрощает настройку классификатора, так как позволяет выбрать стандартное приложение. При выборе стандартного приложения вы не настраиваете остальные поля фильтра. SIP (Протокол инициирования сеанса) представляет собой протокол, используемый в Интернет-телефонии, рассылке сообщений и прочих приложениях VoIP (Передача голоса по IP). Установите флажок и выберите из выпадающего списка **VoIP(SIP)**, чтобы настроить этот классификатор для трафика, использующего 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. Установите флажок и выберите **FTP** из выпадающего списка для настройки этого классификатора для трафика FTP.
Protocol	Выберите эту опцию и протокол (**TCP** или **UDP**) или установите **User defined** и введите номер протокола (тип службы). 0 означает любой номер протокола.
Packet Length	Выберите эту опцию и введите в полях минимальную и максимальную длину пакета (от 28 до 1500).
DSCP	Выберите эту опцию и укажите в поле номер DSCP (DiffServ Code Point – значение кода службы) от 0 до 63.
Ethernet Priority	Выберите эту опцию и установите в разворачивающемся списке уровень приоритета (от 0 до 7). Ноль – самый низкий приоритет, а семь – самый высокий.
VLAN ID	Выберите эту опцию и укажите номер идентификатора VLAN от 2 до 4094.
Physical Port	Выберите эту опцию и укажите порт LAN.
Remote Node	Выберите эту опцию и в выпадающем списке выберите удаленный узел. Если тип WAN – **Ethernet** на экране **WAN > Internet Access Setup**, то можно выбрать только **WAN1**.
Exclude	Выберите эту опцию для того, чтобы исключить пакеты, совпадающие с указанными критериями, из этого классификатора.
Back	Нажмите эту кнопку для возврата к предыдущему экрану без сохранения.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

14.4 Экран QoS Monitor

Этот экран используется для просмотра статистики пакетов QoS на устройстве P660HN. Нажмите **Advanced > QoS > Monitor**. При этом откроется показанный ниже экран.

Рис. 122 Advanced > QoS > Monitor



В следующей таблице даны описания полей этого экрана.

Табл. 77 Advanced > QoS > Monitor

ПОЛЕ	ОПИСАНИЕ
Priority Queue	Здесь указан индекс приоритета очередности. Трафик, которому присваивается высокий индекс очередности, движется быстрее, а трафик с низкими индексами очередности при переполнении останавливается.
Pass	Здесь указано, сколько пакетов, которым назначен данный приоритет очередности, будут переданы успешно.
Drop	Здесь указано, сколько пакетов, которым назначен данный приоритет очередности, будут сброшены.
Poll Interval(s)	В это поле вводится интервал обновления статистики.
Set Interval	Нажмите эту кнопку, чтобы применить новый интервал опроса, заданный в поле **Poll Interval(s)**.
Stop	Нажмите эту кнопку для прерывания обновления статистики.

14.5 Техническое руководство QoS

В этом разделе приводится некоторая вводная техническая информация по темам данной главы.

14.5.1 Маркировка IEEE 802.1Q

Стандарт IEEE 802.1Q определяет явный маркер VLAN в заголовке уровня MAC для установления принадлежности пакета к виртуальной LAN при прохождении через мосты. Маркер VLAN включает в себя 12-битный идентификатор VLAN и 3-битный приоритет пользователя. Идентификатор виртуальной сети указывает на принадлежность пакета к конкретной VLAN и содержит информацию, необходимую для коммутаторов в процессе обработки пакета при перемещении его в сети.

IEEE 802.1p указывает поле с уровнем приоритета пользователя и определяет до восьми отдельных видов трафика. В приведенной ниже таблице показаны виды трафика, определенные в стандарте IEEE 802.1d (который включает в себя 802.1p).

Табл. 78 Уровень приоритета IEEE 802.1p и тип трафика

УРОВЕНЬ ПРИОРИТЕТА	ТИП ТРАФИКА
Уровень 7	Обычно используется для управления сетевым трафиком, например, сообщениями о конфигурации маршрутизатора.
Уровень 6	Обычно используется для трафика передачи речи, который очень чувствителен к дрожанию (дрожание – это изменение величины задержки).
Уровень 5	Обычно используется для видеоданных, которые используют широкую полосу частот и чувствительны к дрожанию.
Уровень 4	Обычно используется для времячувствительного трафика с управляемой нагрузкой, например операций SNA (Архитектура систем в сетях).
Уровень 3	Обычно используется для трафика с лучшим качеством (excellent effort) или выше по приоритету, чем трафик с наилучшим возможным качеством (best-effort) и может включать важный деловой трафик, который допускает некоторую задержку.
Уровень 2	Используется для «запасной полосы частот».
Уровень 1	Обычно используется для второстепенного низкоприоритетного трафика (background), такого как основная масса данных, которая передается, но не влияет на другие приложения и пользователей.
Уровень 0	Обычно используется для трафика с наилучшим возможным качеством (best-effort).

14.5.2 IP-очередность

Аналогично установке приоритета на уровне 2 стандарта IEEE 802.1p вы можете использовать IP-очередность для установки приоритетов в пакетах сети уровня 3. В IP-очередности используется три бита восьмибитного поля ToS (тип услуги) в IP-заголовке. В IP-очередности имеется восемь классов услуг (от 0 до 7). Ноль – самый низкий приоритет, а семь – самый высокий.

14.5.3 DiffServ

QoS (Quality of Service – Качество обслуживания) используется для установки приоритета для потоков трафика источник-адресат. Пакеты, находящиеся в одном потоке, имеют одинаковый приоритет. CoS используется для назначения разного приоритета различным типам пакетов.

Дифференцированное обслуживание (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.

Обработка по точкам кодирования на транзитных пунктах

DiffServ создает новое поле DS, 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.

DSCP (6 бит)	Не используемые (2 бита)

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 маркировку разных типов маршрутизации. При этом ресурсы распределяются в соответствии со значениями DSCP и установленными политиками.

14.5.4 Автоматическое задание приоритета в очереди

Если включить QoS в устройстве P660HN, то устройство P660HN может на основании уровня приоритетов стандарта IEEE 802.1p, IP-очередности и/или длины пакетов присвоить приоритет трафику, который не совпадает с классом.

В приводимой ниже таблице показано отображение внутреннего уровня-2 и уровня-3 QoS в устройстве P660HN. В устройстве P660HN, трафик, которому присваивается высокий приоритет очередности, движется быстрее, а трафик с низкими индексами очередности при переполнении останавливается.

Табл. 79 Отображение внутренних уровней 2 и 3 QoS

ПРИОРИТЕТ ОЧЕРЕДНОСТИ	УРОВЕНЬ 2	УРОВЕНЬ 3		
	ПРИОРИТЕТ ПОЛЬЗОВАТЕЛЯ IEEE 802.1P (ПРИОРИТЕТ ETHERNET)	ТИП УСЛУГИ (IP-ОЧЕРЕД-НОСТЬ)	DSCP	ДЛИНА IP-ПАКЕТА (БАЙТ)
0	1	0	000000	
1	2			
2	0	0	000000	> 1100
3	3	1	001110 001100 001010 001000	250~1100
4	4	2	010110 010100 010010 010000	
5	5	3	011110 011100 011010 011000	<250
6	6	4	100110 100100 100010 100000	
		5	101110 101000	
7	7	6	110000 111000	
		7		

15

Настройка динамической системы доменных имен (DYNDNS)

15.1 Обзор

Динамическая система доменных имен 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 веб-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 связаться с вами, даже если они не знают вашего текущего 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.

15.1.1 Что можно сделать на экране DDNS

Экран **Dynamic DNS** (Разд. 15.2 на с. 231) используется для включения DDNS и настройки параметров DDNS в модели устройства P660HN.

15.1.2 Что нужно знать о DDNS

Шаблон DYNDNS

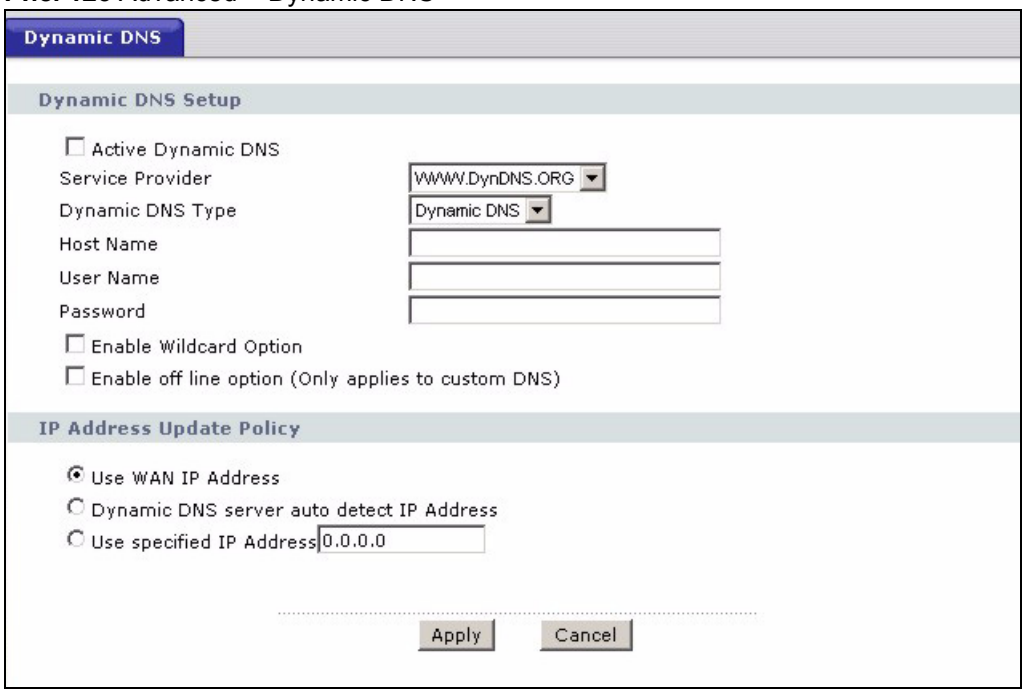
Использование масок позволяет соотносить имена вида *.yourhost.dyndns.org с тем же IP-адресом, что и имя yourhost.dyndns.org. Данная функция полезна, если вы хотите иметь возможность использовать, например, адрес www.yourhost.dyndns.org и при этом предоставлять доступ к вашему узлу.

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

15.2 Экран настройки динамической системы доменных имен

Этот экран используется для изменения DDNS вашего устройства P660HN. Нажмите **Advanced > Dynamic DNS**. При этом откроется показанный ниже экран.

Рис. 123 Advanced > Dynamic DNS



В следующей таблице даны описания полей этого экрана.

Табл. 80 Advanced > Dynamic DNS

ПОЛЕ	ОПИСАНИЕ
Dynamic DNS Setup	
Active Dynamic DNS	Установите этот флажок для использования динамической службы доменных имен.
Service Provider	Имя провайдера услуг динамической DNS.
Dynamic DNS Type	Выберите тип службы, предоставляемой вашим провайдером услуг динамической DNS
Host Name	Введите доменное имя, назначенное устройству P660HN провайдером услуг динамической DNS. Можно ввести в это поле 2 имени, разделенных запятой («,»).
User Name	Введите имя пользователя.
Password	Введите назначенный пароль.
Enable Wildcard Option	Установите этот флажок для включения маски DYNDNS.
Enable off line option	Это поле доступно, только если в поле **DDNS Type** установлено **Custom DNS**. Проверьте, что провайдер услуг динамической DNS обеспечивает перенаправление трафика на указанный вами URL во время отсутствия подключения к сети.
IP Address Update Policy	

Табл. 80 Advanced > Dynamic DNS (продолжение)

ПОЛЕ	ОПИСАНИЕ
Use WAN IP Address	Выберите эту опцию для обновления IP-адреса для имени узла (узлов) на IP-адрес в глобальной сети.
Dynamic DNS server auto detect IP Address	Выберите эту опцию, если присутствует один или несколько NAT-маршрутизаторов между устройством P660HN 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 P660HN и сервером DDNS присутствует прокси-сервер HTTP, сервер DDNS не сможет обнаружить соответствующий IP-адрес.
Use specified IP Address	Введите IP-адрес для имени узла (узлов). Выберите эту опцию, если используется статический IP-адрес.
Apply	Нажмите эту кнопку для сохранения своих изменений
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

16

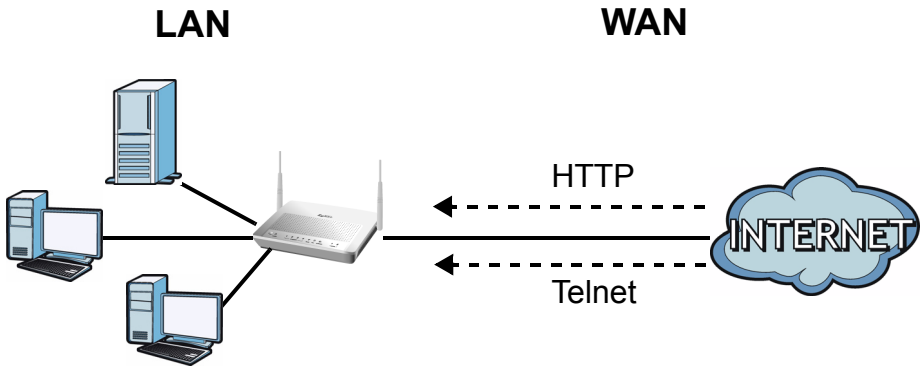
Удаленное управление

16.1 Обзор

При помощи удаленного управления можно определить службы/протоколы для доступа к устройству P660HN, интерфейс управления, а также компьютеры, с которых можно выполнять управление устройством.

На следующем рисунке изображена схема удаленного управления устройством P660HN через глобальную вычислительную сеть (WAN).

Рис. 124 Удаленное управление через глобальную вычислительную сеть (WAN)



При установке параметров конфигурации удаленного управления, предназначенного для реализации функций управления через глобальную вычислительную сеть (WAN), необходимо также настроить правило брандмауэра разрешения доступа к устройству. Необходимо также учитывать, что некоторые провайдеры блокируют входящие подключения на стандартные порты управления (например 80,21,23 и т. д.). Поэтому если на стандартных портах удаленный доступ не работает, попробуйте поменять номера портов на нестандартные.

Возможны следующие режимы удаленного управления устройством P660HN:

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

Для отключения удаленного управления конкретной службой выберите **Disable** в соответствующем поле **Access Status**.

Одновременно допускается проведение только одного сеанса удаленного управления. Устройство P660HN 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

16.1.1 Что можно сделать на экране удаленного управления

- На экране **WWW** (Разд. 16.2 на с. 235) можно определить, через какие интерфейсы и с каких IP-адресов пользователям разрешается выполнять управление устройством P660HN по протоколу HTTP.
- На экране **Telnet** (Разд. 16.3 на с. 238) можно определить, через какие интерфейсы и с каких IP-адресов пользователям разрешается выполнять управление устройством P660HN по протоколу Telnet.
- На экране **FTP** (Разд. 16.4 на с. 239) можно определить, через какие интерфейсы и с каких IP-адресов пользователям разрешается выполнять управление устройством P660HN по протоколу FTP.
- Экран **SNMP** (Разд. 16.5 на с. 240) используется для настройки параметров вашего устройства P660HN для управления простым протоколом управления сетью.
- На экране **DNS** (Разд. 16.6 на с. 243) можно определить, через какие интерфейсы и с каких IP-адресов пользователи могут посылать запросы DNS к устройству P660HN.
- Экран **ICMP** (Разд. 16.7 на с. 244) используется для настройки отклика вашего устройства P660HN на эхо-тестирование и зондирование тех услуг, которые вы сделали недоступными.

16.1.2 Что нужно знать об удаленном управлении

Ограничения на удаленное управление

Удаленное управление не работает в следующих случаях:

- Эта служба не подключена в интерфейсе на соответствующем экране удаленного управления.
- Эта служба отключена на экране настройки удаленного управления.
- IP-адрес, установленный в поле **Secured Client IP** не совпадает с IP-адресом клиента. В случае несовпадения устройство P660HN 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 брандмауэра, блокирующее удаленное управление.
- Провайдер блокирует входящие подключения на соответствующий порт

Удаленное управление и NAT

При включении функции NAT:

- При управлении из глобальной сети необходимо использовать IP-адрес устройства P660HN в глобальной сети.
- При управлении из локальной сети необходимо использовать IP-адрес устройства P660HN в локальной сети.

Время простоя системы

Максимальное время простоя системы во время сеанса управления по умолчанию установлено на 5 минут (300 секунд). Устройство P660HN автоматически завершает сеанс управления при простое, продолжающемся более этого периода. Сеанс управления не разрывается, если на экране статистики проводится опрос системы.

16.2 Экран WWW

Этот экран используется для указания того, как подключиться к устройству P660HN через веб-браузер, напр. Internet Explorer.

16.2.1 WWW и HTTPS

HTTPS (Протокол передачи гипертекста по Протоколу защищенных сокетов или «HTTP по SSL») – это веб-протокол, который шифрует и дешифрует веб-страницы. Протокол защищенных сокетов (SSL) – это протокол уровня приложений, который делает возможной безопасную передачу данных, обеспечивая конфиденциальность информации (предотвращается несанкционированный доступ к передаваемым данным), аутентификацию (один участник может идентифицировать другого) и целостность данных (в случае изменения данных, вам становится это известно).

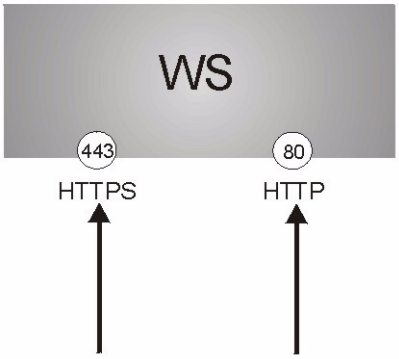
Он зависит от сертификатов, открытых и секретных ключей (более подробную информацию см. в Гл. 11 на с. 173).

HTTPS устройства P660HN используется для безопасного доступа к устройству P660HN с помощью Web-конфигуратора. Протокол SSL предписывает SSL-серверу (устройство P660HN) всегда идентифицировать себя для SSL-клиента (компьютера, запрашивающего HTTPS-подключение к устройству P660HN), в то время, как SSL-клиент должен идентифицировать себя только по запросу SSL-сервера (выберите **Authenticate Client Certificates** на экране **Remote MGMT > WWW**). При выборе опции **Authenticate Client Certificates** SSL-клиент должен отправить сертификат устройству P660HN. Вам необходимо подписаться на сертификат от центра сертификации (CA), являющийся доверенным для устройства P660HN.

См. следующий рисунок.

1. Соединение HTTPS требует у веб-браузера, поддерживающего SSL, перехода к порту 443 (по умолчанию) на веб-сервер устройства P660HN.
2. Соединение HTTP требует у веб-браузера перехода к порту 80 (по умолчанию) на веб-сервер устройства P660HN.

Рис. 125 Реализация HTTPS

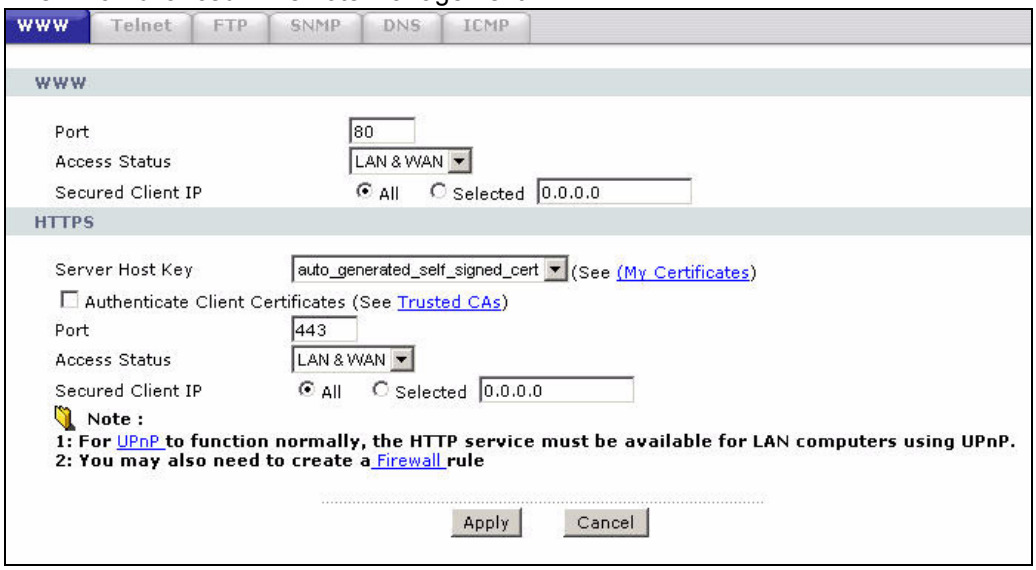


При отключении службы **WWW** на экране **Remote MGMT > WWW** устройство P660HN будет блокировать все попытки HTTP-соединений.

16.2.2 Настройки на экране WWW

Нажмите **Advanced > Remote MGMT** для отображения экрана **WWW**.

Рис. 126 Advanced > Remote Management > WWW



В следующей таблице даны описания полей этого экрана.

Табл. 81 Advanced > Remote Management > WWW

ПОЛЕ	ОПИСАНИЕ
WWW	
Port	При необходимости можно изменить номер порта сервера для службы. Однако, нужно указывать тот же номер порта для использования этой службы при удаленном управлении.

Табл. 81 Advanced > Remote Management > WWW (продолжение)

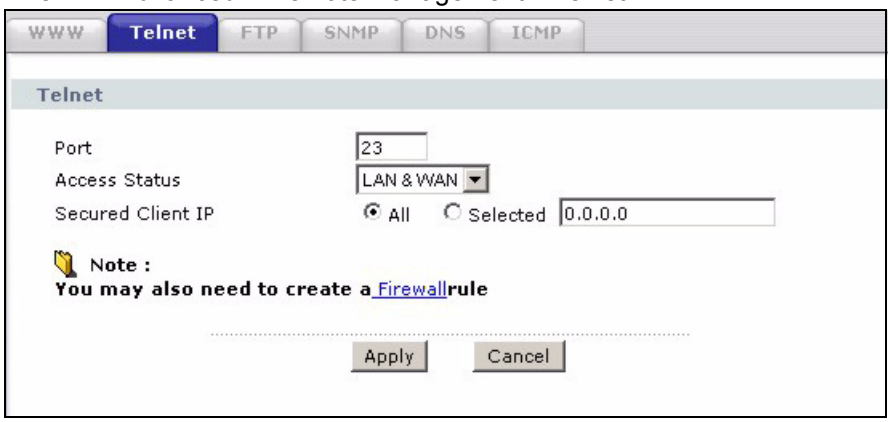
ПОЛЕ	ОПИСАНИЕ
Access Status	Выберите интерфейс(ы), через который компьютер сможет получить доступ к устройству P660HN при использовании этой службы.
Secured Client IP	Защищенный клиент – это «доверенный» компьютер, которому разрешается подключаться к устройству P660HN при использовании этой службы. Выберите **All**, чтобы разрешить любому компьютеру доступ к устройству P660HN при использовании этой службы. Выберите **Selected**, чтобы разрешить доступ к устройству P660HN только компьютеру с указанным IP-адресом при использовании этой службы.
HTTPS	
Server Host Key	Выберите **Server Host Key**, который устройство P660HN будет использовать для самоидентификации. Устройство P660HN представляет собой SSL-сервер и всегда должно идентифицировать себя для SSL-клиента (компьютера, запрашивающего HTTPS-подключение с устройством P660HN).
Authenticate Client Certificates	Выберите **Authenticate Client Certificates** (опция), чтобы требовать от SSL-клиентов самоидентификации для устройства P660HN путем отправки сертификата устройству P660HN. Для этого SSL-клиент должен иметь подписанный центром сертификации сертификат, полученный от центра сертификации, который был загружен, как доверенный в устройство P660HN.
Port	Если требуется, номер порта службы можно изменить, но необходимо использовать такой же номер порта при использовании этой службы для удаленного управления.
Access Status	Выберите интерфейс(ы), через который компьютер сможет получить доступ к устройству P660HN при использовании этой службы.
Secured Client IP	Защищенный клиент – это «доверенный» компьютер, которому разрешается подключаться к устройству P660HN при использовании этой службы. Выберите **All**, чтобы разрешить любому компьютеру доступ к устройству P660HN при использовании этой службы. Выберите **Selected**, чтобы разрешить доступ к устройству P660HN только компьютеру с указанным IP-адресом при использовании этой службы.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

16.3 Экран Telnet

Для доступа к интерфейсу командной строки устройства P660HN можно использовать протокол Telnet. Укажите, какие интерфейсы разрешают доступ по Telnet и с каких IP-адресов можно осуществлять доступ.

Нажмите вкладку **Advanced > Remote MGMT** > **Telnet** для отображения экрана, показанного ниже.

Рис. 127 Advanced > Remote Management > Telnet



В следующей таблице даны описания полей этого экрана.

Табл. 82 Advanced > Remote Management > Telnet

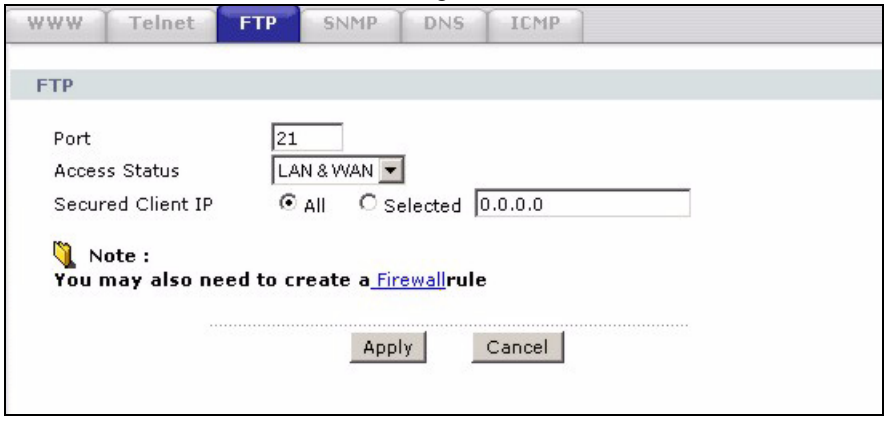
ПОЛЕ	ОПИСАНИЕ
Port	Если требуется, номер порта службы можно изменить, но необходимо использовать такой же номер порта при использовании этой службы для удаленного управления.
Access Status	Выберите интерфейс(ы), через который компьютер сможет получить доступ к устройству P660HN при использовании этой службы.
Secured Client IP	Защищенный клиент – это «доверенный» компьютер, которому разрешается подключаться к устройству P660HN при использовании этой службы. Выберите **All**, чтобы разрешить любому компьютеру доступ к устройству P660HN при использовании этой службы. Выберите **Selected**, чтобы разрешить доступ к устройству P660HN только компьютеру с указанным IP-адресом при использовании этой службы.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

16.4 Экран FTP

Протокол FTP (File Transfer Protocol – Протокол передачи файлов) можно использовать для загрузки в устройство P660HN микропрограммного обеспечения и файлов конфигурации. Подробнее см. главу Руководства пользователя о микропрограммном обеспечении и сопровождении файлов конфигурации. Для использования данной функции на компьютере должен быть установлен FTP-клиент.

Укажите, какие интерфейсы разрешают доступ по Telnet и с каких IP-адресов можно осуществлять доступ. Для изменения настроек FTP в устройстве P660HN нажмите **Advanced > Remote MGMT** > **FTP**. При этом откроется показанный ниже экран.

Рис. 128 Advanced > Remote Management > FTP



В следующей таблице даны описания полей этого экрана.

Табл. 83 Advanced > Remote Management > FTP

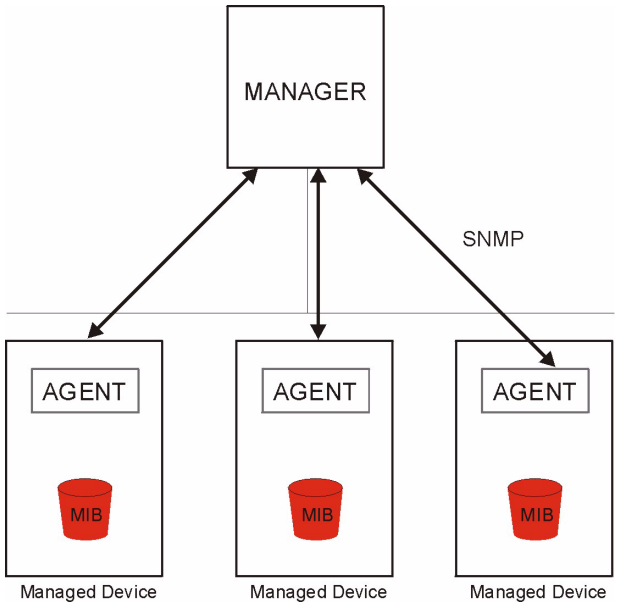
ПОЛЕ	ОПИСАНИЕ
Port	При необходимости можно изменить номер порта сервера для службы. Однако, нужно указывать тот же номер порта для использования этой службы при удаленном управлении.
Access Status	Выберите интерфейс(ы), через который компьютер сможет получить доступ к устройству P660HN при использовании этой службы.
Secured Client IP	Защищенный клиент – это «доверенный» компьютер, которому разрешается подключаться к устройству P660HN при использовании этой службы. Выберите **All**, чтобы разрешить любому компьютеру доступ к устройству P660HN при использовании этой службы. Выберите **Selected**, чтобы разрешить доступ к устройству P660HN только компьютеру с указанным IP-адресом при использовании этой службы.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

16.5 Экран SNMP

Простой протокол управления сетью (SNMP – Simple Network Management Protocol) используется для осуществления обмена управляющей информацией между сетевыми устройствами. SNMP является одним из элементов стека протоколов TCP/IP. Устройство P660HN поддерживает функцию агента SNMP, что позволяет выполнять управление и мониторинг устройства P660HN с управляющей станции по сети. Устройство P660HN поддерживает протокол SNMP версии один (SNMPv1) и версии два (SNMPv2). На следующем рисунке показана модель управления по протоколу.

Протокол SNMP является доступным, только если настроен TCP/IP.

Рис. 129 Модель управления SNMP



Сеть, управляемая протоколом SNMP, состоит из двух основных компонентов: агентов и менеджера.

Агент представляет собой модуль программы управления, находящийся в управляемом устройстве (устройстве P660HN). Агент производит преобразование информации локального управления от управляемого устройства в форму, совместимую с SNMP. В качестве управляющей программы выступает консоль, при помощи которой сетевые администраторы осуществляют управление сетью. С помощью консоли запускаются приложения 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 станции 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 станции установить значения для объектных переменных внутри агента.
- Trap (Прерывание) – Используется агентом для информирования управляющей программы о произошедших событиях.

16.5.1 Поддерживаемые базы управляющей информации (MIB)

Устройство P660HN 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.

16.5.2 Прерывания SNMP

Устройство P660HN посылает прерывания на управляющую станцию SNMP, когда происходит какое-либо из следующих событий:

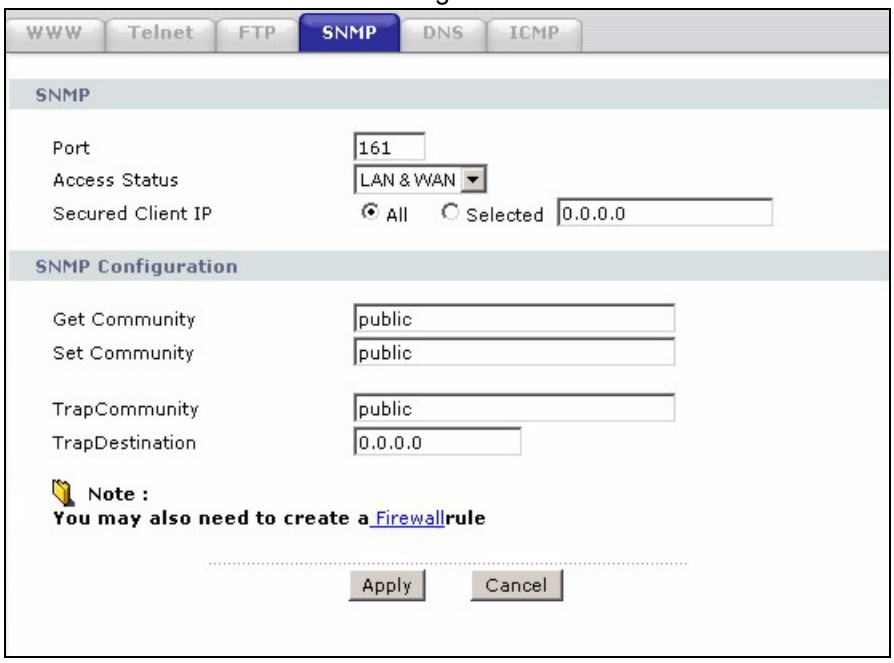
Табл. 84 Прерывания SNMP

НОМЕР ПРЕРЫ-ВАНИЯ	ИМЯ ПРЕРЫВАНИЯ	ОПИСАНИЕ
0	coldStart (описывается в *RFC-1215*)	Прерывание посылается после начальной загрузки (включения питания).
1	warmStart (описывается в *RFC-1215*)	Прерывание посылается после загрузки (программная перезагрузка).
4	authenticationFailure (описывается в *RFC-1215*)	Прерывание направляется в адрес управляющей программы в случае получения требований SNMP «Get» или «Set» с неправильным паролем.
6	whyReboot (описывается в ZYXEL-MIB)	Прерывание посылается с указанием кода причины перезапуска перед перезагрузкой, 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.

16.5.3 Конфигурирование SNMP

Для изменения настроек SNMP в устройстве P660HN нажмите **Advanced > Remote MGMT** > **SNMP**. При этом откроется показанный ниже экран.

Рис. 130 Advanced > Remote Management > SNMP



В следующей таблице даны описания полей этого экрана.

Табл. 85 Advanced > Remote Management > SNMP

ПОЛЕ	ОПИСАНИЕ
SNMP	
Port	При необходимости можно изменить номер порта сервера для службы. Однако, нужно указывать тот же номер порта для использования этой службы при удаленном управлении.
Access Status	Выберите интерфейс(ы), через который компьютер сможет получить доступ к устройству P660HN при использовании этой службы.
Secured Client IP	Защищенный клиент – это «доверенный» компьютер, которому разрешается подключаться к устройству P660HN при использовании этой службы. Выберите **All**, чтобы разрешить любому компьютеру доступ к устройству P660HN при использовании этой службы. Выберите **Selected**, чтобы разрешить доступ к устройству P660HN только компьютеру с указанным IP-адресом при использовании этой службы.
SNMP Configuration	
Get Community	Введите пароль **Get Community**, который является паролем для входящих запросов Get и GetNext от управляющей станции. По умолчанию установлен пароль «public» и разрешаются все запросы.
Set Community	Введите пароль **Set community**, который является паролем для входящих запросов Set от управляющей станции. По умолчанию установлен пароль «public» и разрешаются все запросы.
TrapCommunity	Наберите в этом поле пароль прерывания, который отправляется с каждым прерыванием в адрес управляющей станции SNMP. По умолчанию установлен пароль «public» и разрешаются все запросы.

Табл. 85 Advanced > Remote Management > SNMP (продолжение)

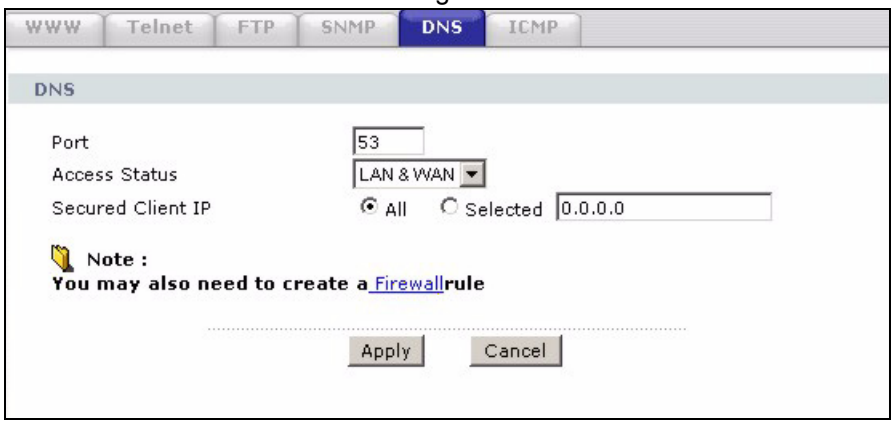
ПОЛЕ	ОПИСАНИЕ
TrapDestination	Введите IP-адрес устройства, на которое будут посылаться прерывания SNMP.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

16.6 Экран DNS

DNS (Система доменных имен) предназначена для отображения доменного имени на соответствующий ему IP-адрес и наоборот. Для дополнительной информации см. Гл. 5 на с. 71.

Этот экран используется для установки IP-адреса, с которого устройство P660HN будет принимать запросы DNS, а также интерфейса, через который устройство P660HN будет отправлять параметры DNS на эти запросы. Эта функция недоступна, если на устройстве P660HN установлен режим межсетевого моста. Нажмите **Advanced > Remote MGMT** > **DNS** для изменения настроек DNS на устройстве P660HN.

Рис. 131 Advanced > Remote Management > DNS



В следующей таблице даны описания полей этого экрана.

Табл. 86 Advanced > Remote Management > DNS

ПОЛЕ	ОПИСАНИЕ
Port	Номер служебного порта DNS – 53, и его нельзя изменить здесь.
Access Status	Выберите интерфейс(ы), через который компьютер сможет посылать устройству P660HN запросы DNS.
Secured Client IP	Защищенный клиент – это «доверенный» компьютер, которому разрешается посылать устройству P660HN запросы DNS. Выберите **All**, чтобы разрешить любому компьютеру посылать устройству P660HN запросы DNS. Выберите **Selected**, чтобы разрешить только компьютеру с указанным IP-адресом посылать запросы DNS устройству P660HN.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

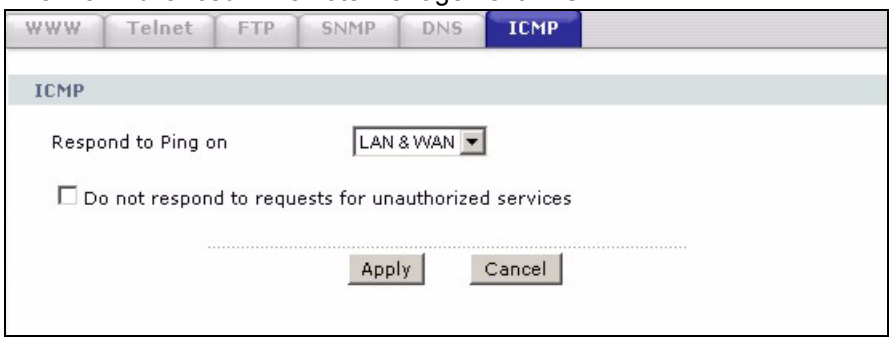
16.7 Экран ICMP

Для изменения настроек безопасности в устройстве P660HN нажмите **Advanced > Remote MGMT** > **ICMP**. При этом откроется показанный ниже экран.

Если внешний пользователь попытается прозондировать неподдерживаемый порт устройства P660HN, ему будет автоматически отправлен ответный пакет ICMP. Это позволяет внешнему пользователю узнать о существовании устройства P660HN. Также устройство P660HN поддерживает блокирование зондирования без отправки ответного пакета ICMP. Это позволяет скрыть существование устройство P660HN от посторонних лиц при попытке зондирования неподдерживаемого порта.

Если вы хотите, чтобы ваше устройство осуществляло отклик на эхо-тестирование и зондирование несанкционированных служб, вам также необходимо настроить параметры брандмауэра, относящиеся к блокированию эхо-тестирования.

Рис. 132 Advanced > Remote Management > ICMP



В следующей таблице даны описания полей этого экрана.

Табл. 87 Advanced > Remote Management > 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 Интернет-протокола (IP), но сообщения обрабатываются программным обеспечением TCP/IP, и напрямую видимы пользователю приложений.
Respond to Ping on	Устройство P660HN не отвечает на входящие запросы эхо-тестирования, если в поле **Disable** установлен флажок. Выберите **LAN** для ответа на входящие эхо-запросы из локальной сети. Выберите **WAN** для ответа на входящие эхо-запросы по глобальной сети. В противном случае выберите **LAN & WAN** для ответа на эхо-запросы как из локальной, так и глобальной сети.

Табл. 87 Advanced > Remote Management > ICMP (продолжение)

ПОЛЕ	ОПИСАНИЕ
Do not respond to requests for unauthorized services	Установите флажок, чтобы предотвратить обнаружение хакерами устройства P660HN посредством зондирования неиспользуемых портов. Если флажок установлен, устройство P660HN не будет отвечать на запросы на неиспользуемые порты. Таким образом, неиспользуемые порты и устройство P660HN остаются невидимыми. Если флажок снят, устройство P660HN 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 проверку по правилам брандмауэра устройства P660HN. Следовательно, если правило брандмауэра блокирует зондирующий пакет, реакция устройства P660HN производится на основе правила брандмауэра: 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	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

17

Универсальная функция Plug and Play (UPnP)

17.1 Обзор

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 подключаться к сети, получать IP-адрес, передавать свои функциональные возможности и собирать информацию о других устройствах сети. Кроме того, устройство может беспрепятственно и автоматически покидать сеть, если оно больше не используется.

17.1.1 Что можно сделать на экране UPnP

Экран **UPnP** (Разд. 17.2 на с. 247) используется для включения функции UPnP в устройстве P660HN и для использования приложения с функцией Plug and Play с целью автоматической настройки устройства P660HN.

17.1.2 Что нужно знать о UpnP

Идентификация устройств с функцией UPnP

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

Функция 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 отображениям

Windows Messenger является примером приложения, которое поддерживает NAT traversal и UPnP.

Для получения более подробной информации о NAT см. главу по трансляции сетевых адресов.

Предупреждения по использованию UPnP

Автоматический характер приложений NAT traversal при установке их собственных служб и открывании портов брандмауэра 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 устройство P660HN разрешает многоадресную рассылку сообщений только по локальной сети.

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

UPnP и ZyXEL

Корпорация ZyXEL получила сертификат от организации Universal Plug and Play Forum UPnP™ Implementers Corp. (UIC). Реализация UPnP корпорации ZyXEL поддерживает IGD 1.0 (Internet Gateway Device – Устройство Интернет-шлюза).

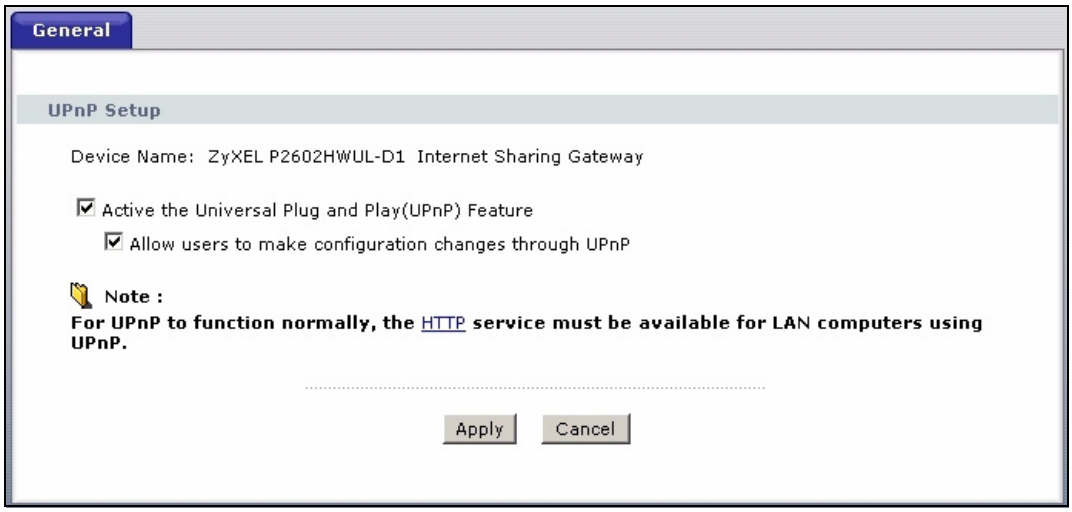
Примеры установки и использования UPnP см. в следующих разделах.

17.2 Экран UPnP

Следующий экран используется для настройки параметров UPnP вашего устройства P660HN. Нажмите **Advanced > UPnP** для отображения экрана, показанного ниже.

Более подробную информацию см. в Разд. 17.1 на с. 246.

Рис. 133 Advanced > UPnP > General



В следующей таблице даны описания полей этого экрана.

Табл. 88 Advanced > UPnP > General

ПОЛЕ	ОПИСАНИЕ
Active the Universal Plug and Play (UPnP) Feature	Установите флажок в этом окне для включения UPnP. Помните, что любой может с помощью приложения UPnP открыть экран регистрации Web-конфигуратора без ввода IP-адреса устройства P660HN (хотя для доступа к Web-конфигуратору необходимо ввести пароль).
Allow users to make configuration changes through UPnP	Установите этот флажок, чтобы разрешить приложениям UPnP автоматически настраивать устройство P660HN с целью взаимодействия через устройство P660HN, например, используя NAT traversal, приложения UPnP автоматически зарезервируют порт, чтобы взаимодействовать с другими устройствами UPnP; это исключит необходимость ручной настройки порта пересылки для UPnP-совместимых приложений.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

17.3 Пример установки UPnP в Windows

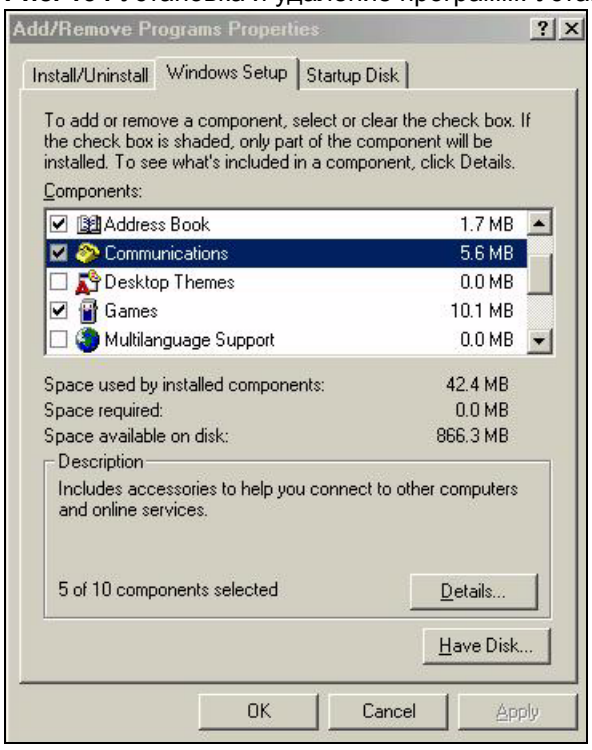
В данном разделе описывается установка UPnP в Windows Me и Windows XP.

17.3.1 Установка UPnP в Windows Me

Выполните следующие действия для установки UPnP в Windows Me.

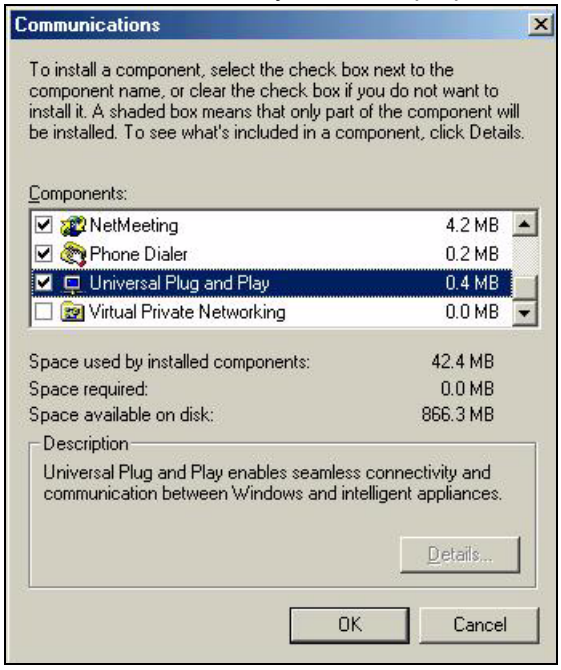
1. Нажмите **Start (Пуск)** и выберите пункт **Control Panel (Панель управления)**. Дважды щелкните пункт **Add/Remove Programs (Установка и удаление программ)**.
2. Выберите закладку **Windows Setup (Установка Windows)** и выберите **Communication (Связь)** в поле **Components (Компоненты)**. Нажмите **Details (Состав)**.

Рис. 134 Установка и удаление программ: Установка Windows: Связь



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

Рис. 135 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.

17.3.2 Установка UPnP в Windows XP

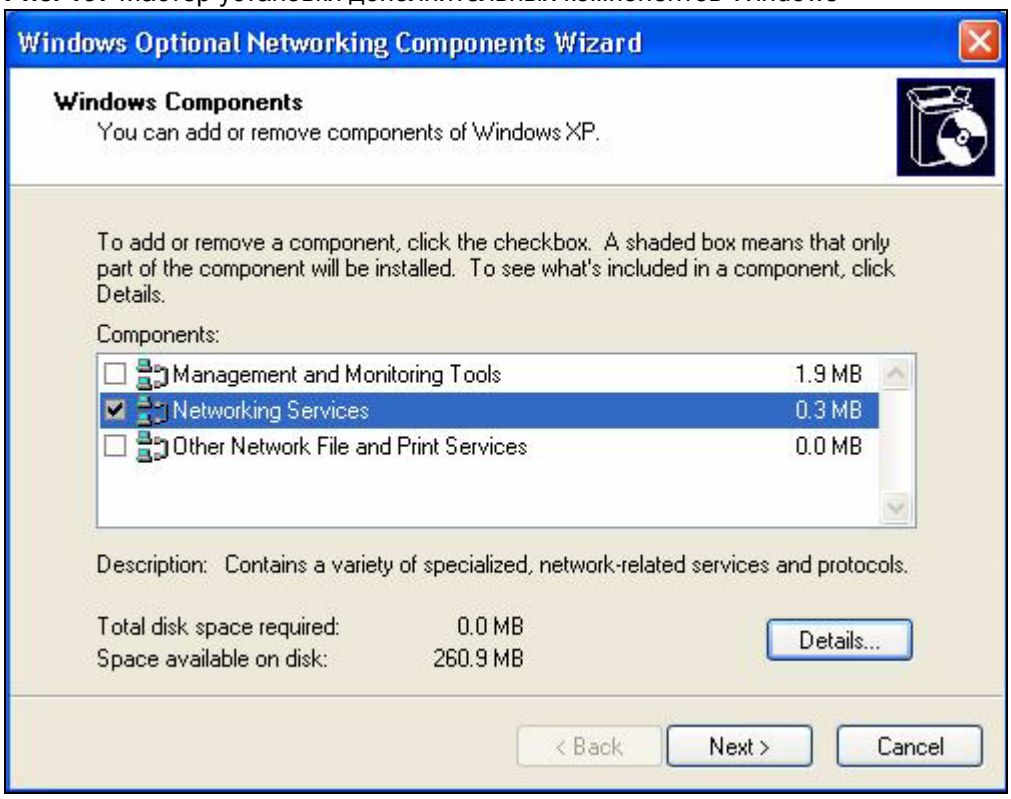
Выполните следующие действия для установки UPnP в Windows XP.

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)** нажмите кнопку **Advanced (Дополнительно)** в главном меню и выберите **Optional Networking Components… (Дополнительные сетевые компоненты...)**.

Рис. 136 Сетевые подключения

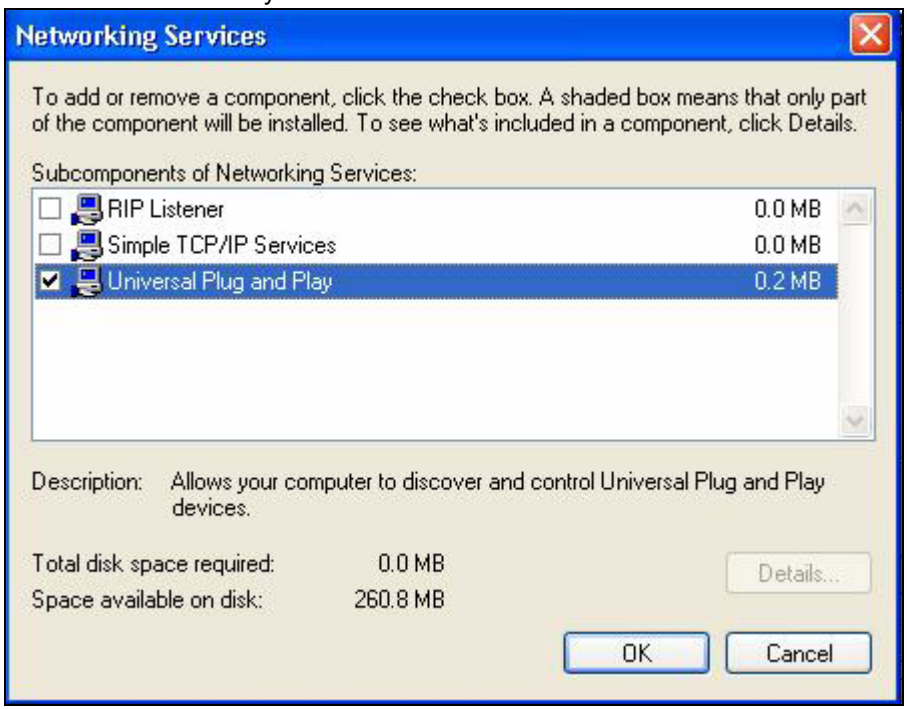
4. Появляется окно **Windows Optional Networking Components Wizard (Мастер установки дополнительных сетевых компонентов Windows)**. Выберите **Networking Services (Сетевые службы)** в поле **Components (Компоненты)** и нажмите **Details (Состав)**.

Рис. 137 Мастер установки дополнительных компонентов Windows



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

Рис. 138 Сетевые службы



6 Нажмите **OK** для возврата в окно **Windows Optional Networking Component Wizard (Мастер установки дополнительных сетевых компонентов Windows)** и нажмите **Next (Далее)**.

17.3.3 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 P660HN.

Убедитесь, что компьютер подключен к порту LAN интернет-центра P660HN. Включите компьютер и P660HN.

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 в Интернет)** отображается значок.

2 Щелкните правой кнопкой мыши на этом значке и выберите **Properties (Свойства)**.

Рис. 139 Сетевые подключения

3 В окне **Internet Connection Properties (Свойства подключения к Интернет)**, нажмите **Settings (Настройки)** для просмотра автоматически созданных правил отображения портов.

Рис. 140 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. 141 Свойства подключения к Интернет: Дополнительные настройки

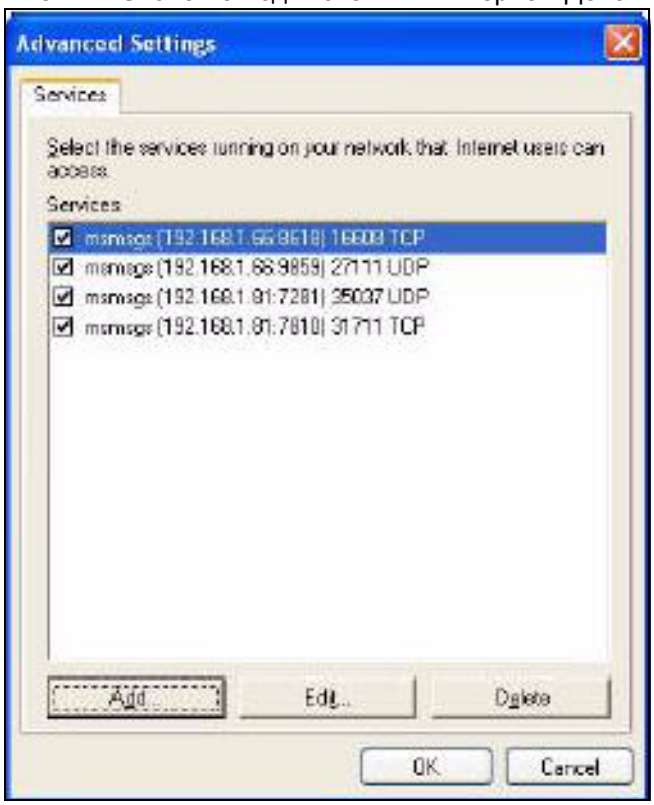
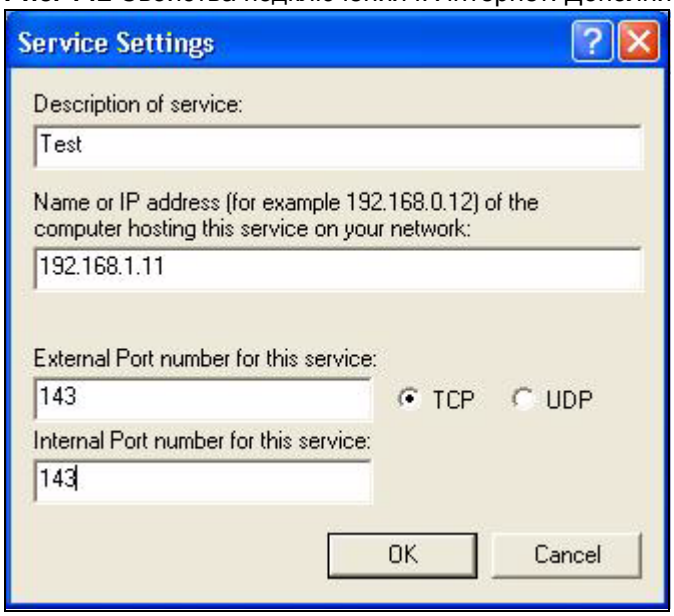


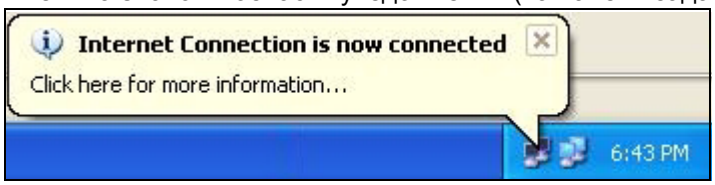
Рис. 142 Свойства подключения к Интернет: Дополнительные настройки: Добавить



5 При отключении устройства UPnP от компьютера все правила отображения портов автоматически удаляются.

6 Выберите **Show icon in notification area when connected (При подключении вывести значок в области уведомлений)** и нажмите **OK**. На панели задач появится значок.

Рис. 143 Значок в области уведомлений (на панели задач)



7 Дважды щелкните значок для отображения текущего состояния подключения к Интернету.

Рис. 144 Состояние подключения к Интернет

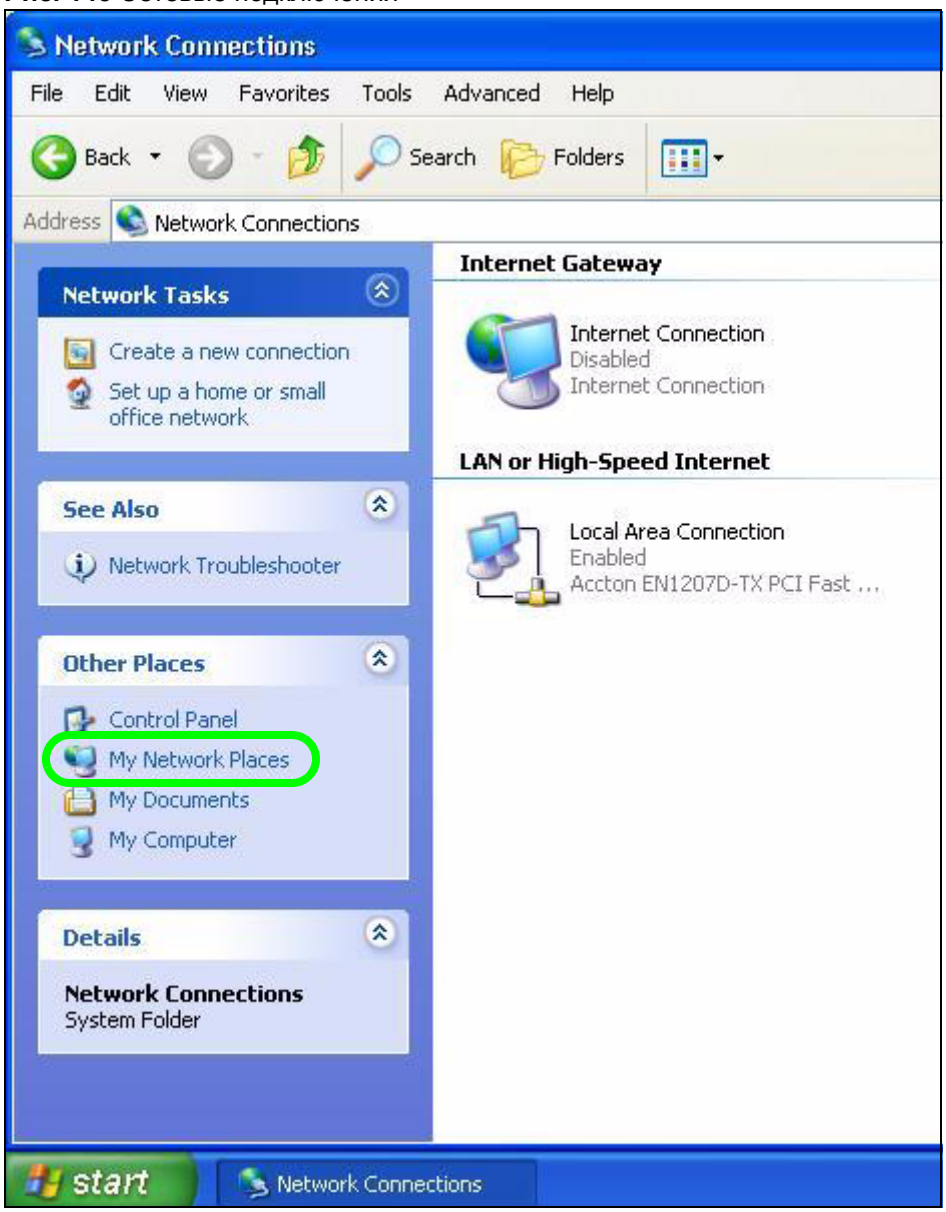
Простой доступ к Web-конфигуратору

С помощью UPnP вы можете получить доступ к программе настройки P660HN на основе Web технологии без предварительного выяснения IP-адреса P660HN. Это может оказаться полезным, если вы не знаете IP-адрес P660HN.

Выполните следующие действия для доступа к Web-конфигуратору.

1 Нажмите кнопку **Start (Пуск)** и выберите пункт **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)**.

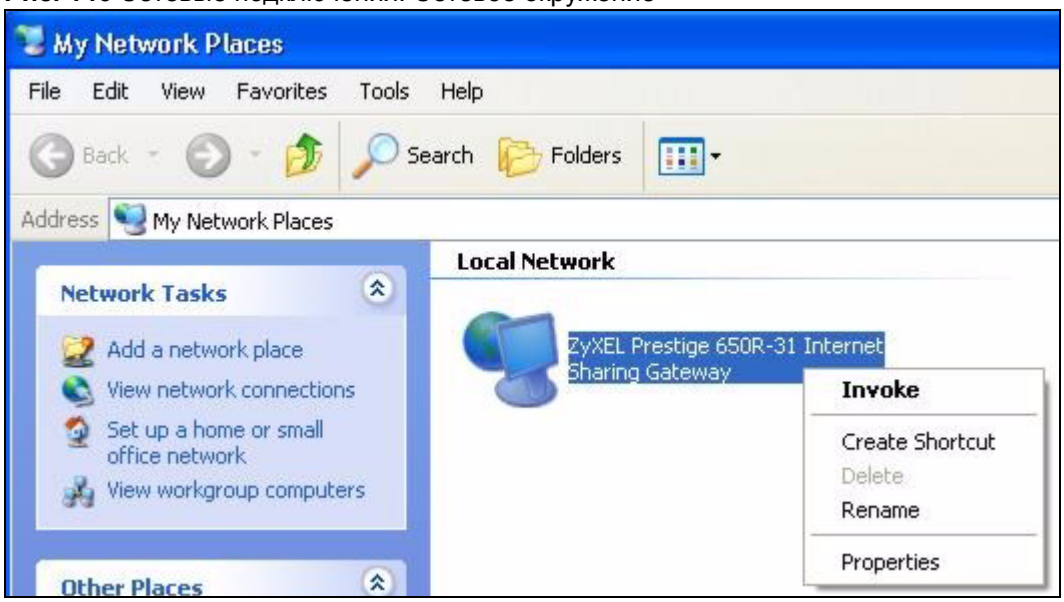
Рис. 145 Сетевые подключения



4 В разделе **Local Network (Локальная сеть)** для каждого UPnP-совместимого устройства отображается значок с описанием.

5 Щелкните правой кнопкой мыши по значку P660HN и выберите **Invoke (Запустить)**. Появится окно регистрации Web-конфигуратора.

Рис. 146 Сетевые подключения: Сетевое окружение



6 Щелкните правой кнопкой мыши по значку P660HN и выберите **Properties (Свойства)**. Появится окно свойств с основной информацией об интернет-центре P660HN.

Рис. 147 Пример – Сетевые подключения: Сетевое окружение: Свойства

Часть V
Сопровождение

18

Настройки системы

18.1 Обзор

В этой главе описывается процедура проведения настроек системы, таких как, системное время, пароль, имя системы, имя домена и интервал простоя при бездействии.

18.1.1 Что можно сделать на экранах системных настроек

- Экран **General** (Разд. 18.2 на с. 259) используется для настройки системных параметров.
- На экране **Time Setting** (Разд. 18.3 на с. 261) проведите настройку системного времени.

18.1.2 Что нужно знать о системных настройках

DHCP

DHCP (протокол динамической конфигурации узла) – это способ получения IP-адресов устройствами в сети от сервера DHCP. Зачастую эта функция выполняется вашим Интернет-провайдером или маршрутизатором.

LAN

LAN (локальная вычислительная сеть) – это, как правило, сеть, покрывающая небольшую область, состоящая из компьютеров и других устройств, совместно использующих ресурсы, такие как доступ в Интернет, принтеры и т. д.

18.2 Экран общей настройки

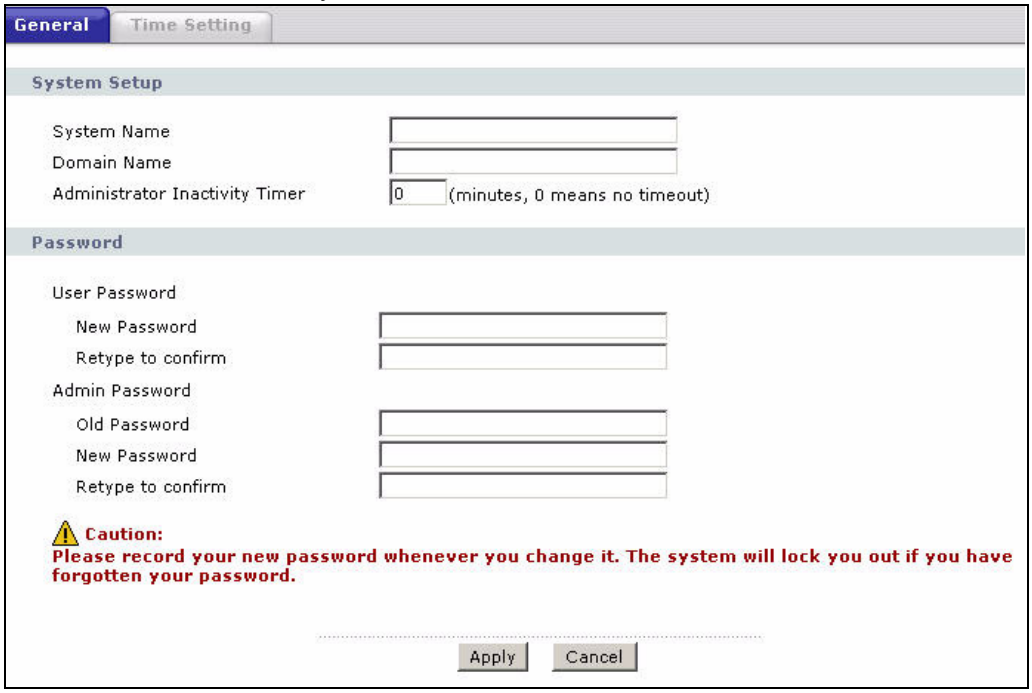
На этом экране можно настроить параметры системы, такие как имя системы и домена, интервал простоя при бездействии и системный пароль.

System Name используется для идентификации. Однако, поскольку некоторые Интернет-провайдеры проверяют это имя, следует вводить имя вашего компьютера. Найдите системное имя вашего компьютера Windows, выполнив следующие действия.

- В Windows 95/98 нажмите **Start**, **Settings**, **Control Panel**, **Network**. Щелкните по закладке Identification, запишите имя, установленное в поле **Computer Name**, и введите его в качестве **System Name**.
- В Windows 2000 нажмите **Start**, **Settings**, **Control Panel** и дважды щелкните **System**. Выберите закладку **Network Identification**, а затем нажмите кнопку **Properties**. Запишите имя, установленное в поле **Computer name**, и введите его в качестве **System Name**.
- В Windows XP нажмите **Start**, **My Computer**, **View system information**, а затем выберите вкладку **Computer Name**. Запишите имя, установленное в поле **Full computer name**, и введите его в качестве **System Name** устройства P660HN.

Нажмите **Maintenance > System**, чтобы открыть экран **General**.

Рис. 148 Maintenance > System > General



В следующей таблице даны описания полей этого экрана.

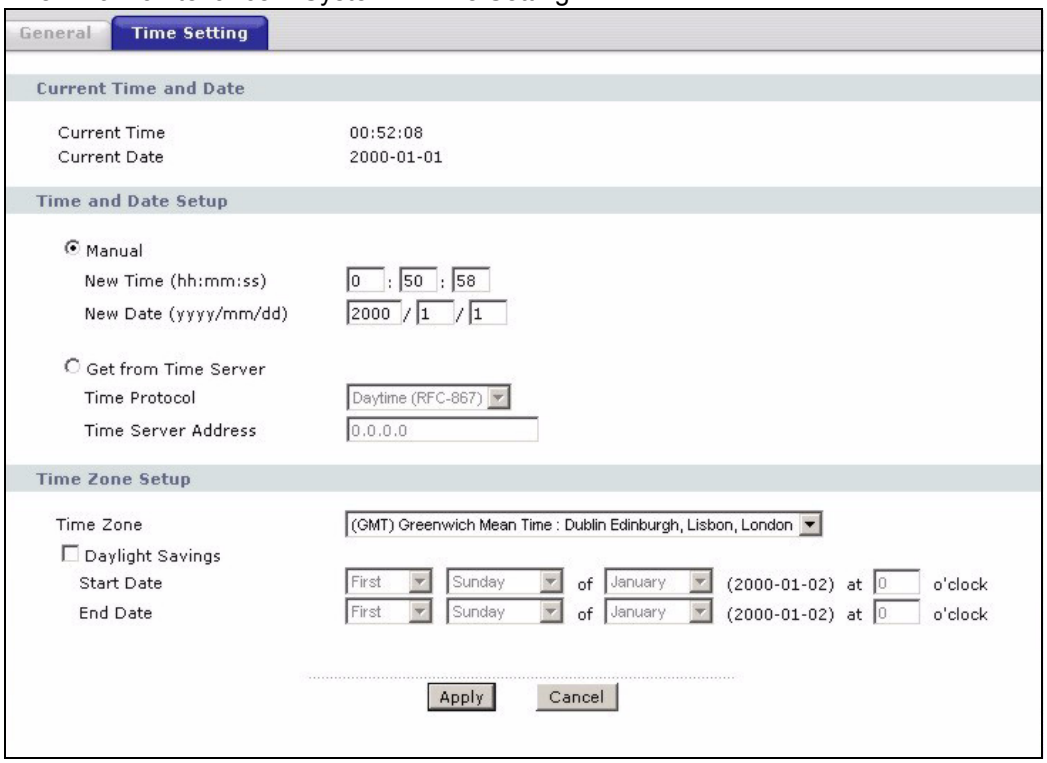
Табл. 89 Maintenance > System > General

ПОЛЕ	ОПИСАНИЕ
System Setup	
System Name	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	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. Запись **Domain Name** передается клиентам DHCP в локальной сети.
Administrator Inactivity Timer	Введите время простоя в минутах, по истечении которого сеанс управления (через Web-конфигуратор или telnet) 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 будет прерван, вне зависимости от времени бездействия (не рекомендуется).
Password	
User Password	
New Password	Введите новый пароль пользователя длиной до 30 символов. При вводе пароля вводимые символы заменяются на экране на символ *. После изменения пароля для доступа к устройству P660HN необходимо использовать новый пароль.
Retype to confirm	Введите новый пароль еще раз для подтверждения.
Admin Password	
Old Password	Введите в это поле пароль по умолчанию или существующий пароль, используемый для доступа в систему.
New Password	Введите новый системный пароль длиной до 30 символов. При вводе пароля вводимые символы заменяются на экране на символ *. После изменения пароля для доступа к устройству P660HN необходимо использовать новый пароль.
Retype to confirm	Введите новый пароль еще раз для подтверждения.
Apply	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

18.3 Экран настройки времени

Этот экран используется для настройки времени в устройстве P660HN в соответствии с вашим часовым поясом. Для изменения даты и времени устройства P660HN, нажмите **Maintenance > System > Time Setting**. При этом откроется показанный ниже экран.

Рис. 149 Maintenance > System > Time Setting



В следующей таблице даны описания полей этого окна.

Табл. 90 Maintenance > System > Time Setting

ПОЛЕ	ОПИСАНИЕ
Current Time and Date	
Current Time	В этом поле отображается время в устройстве P660HN. При каждой перезагрузке этой страницы устройство P660HN синхронизирует время с сервером времени.
Current Date	В этом поле отображается дата в устройстве P660HN. При каждой перезагрузке этой страницы устройство P660HN синхронизирует дату с сервером времени.
Time and Date Setup	
Manual	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 и Daylight Saving не влияют на них.
New Time (hh:mm:ss)	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** режима **Manual**, введите в это поле новое время и нажмите **Apply**.

Табл. 90 Maintenance > System > Time Setting (продолжение)

ПОЛЕ	ОПИСАНИЕ
New Date (yyyy/mm/dd)	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** режима **Manual** введите в это поле новую дату и нажмите кнопку **Apply**.
Get from Time Server	Выберите эту опцию, чтобы устройство P660HN синхронизировало время и дату с сервером, указанным в поле ниже.
Time Protocol	Введите сервисный протокол, с помощью которого ваш сервер времени посылает данные при включении устройства P660HN. 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 (RFC 868).
Time Server Address	Введите IP-адрес или URL сервера времени длиной до 20 символов расширенного набора ASCII. Если вы не обладаете этой информацией, следует обратиться к Интернет-провайдеру/сетевому администратору.
Time Zone Setup	
Time Zone	Выберите часовой пояс вашего местонахождения. Это поле устанавливает разницу между вашим часовым поясом и временем по Гринвичу (Greenwich Mean Time – GMT).
Daylight Saving	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	Введите день и время, когда начинается летнее время, если выбран вариант **Enable Daylight Savings**. В поле **o'clock** используется 24 часовой формат. Далее приводится два примера: В большинстве частей Соединенных Штатов переход на летнее время начинается во второе воскресенье марта. В каждой временной зоне Соединенных Штатов переход осуществляется в 2 часа ночи по местному времени. Таким образом, в Соединенных Штатах необходимо установить **Second**, **Sunday**, **March** и 2 в поле **o'clock**. 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 GMT или UTC. Таким образом, в странах Европейского союза необходимо установить **Last**, **Sunday**, **March**. Время, которое нужно ввести в поле **o'clock** 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. 90 Maintenance > System > Time Setting (продолжение)

ПОЛЕ	ОПИСАНИЕ
End Date	Введите месяц и день, когда заканчивается летнее время, если выбран вариант **Enable Daylight Saving**. В поле **o'clock** используется 24 часовой формат. Далее приводится два примера: В Соединенных Штатах летнее время заканчивается в первое воскресенье ноября. В каждой временной зоне Соединенных Штатов переход осуществляется в 2 часа ночи по местному времени. Таким образом, в Соединенных Штатах необходимо установить **First**, **Sunday**, **November** и 2 в поле **o'clock**. В странах Европейского Союза летнее время заканчивается в последнее воскресенье октября. Во всех временных зонах Европейского Союза переход осуществляется в одно время – в 1 час ночи по GMT или UTC. Таким образом, в странах Европейского Союза необходимо установить **Last**, **Sunday**, **October**. Время, которое нужно ввести в поле **o'clock** 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	Нажмите эту кнопку для сохранения своих изменений.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

19

Журналы регистрации

19.1 Обзор

В этой главе описывается настройка общих параметров журналов регистрации, а также порядок просмотра журналов устройства P660HN.

Web-конфигуратор позволяет выбрать категории событий и/или предупреждений, которые устройство P660HN должно регистрировать, а затем заносить в журналы или отправлять администратору в виде сообщений электронной почты или на сервер системных журналов.

19.1.1 Что можно сделать на экране журналов регистрации

- В окне **View Log** (Разд. 19.2 на с. 265) можно посмотреть журнальные записи по категориям, выбранным в окне **Log Settings**.
- В окне **Log Settings** (Разд. 19.3 на с. 266) можно установить следующие параметры для почтового сервера и сервера хранения системных журналов: когда отправлять журналы и какие журналы.

19.1.2 Что нужно знать о журналах

Предупреждения

Предупреждение – это сообщение, порождаемое возникновением события. К предупреждениям относятся сообщения о системных ошибках, атаках (управление доступом) и попытках доступа к заблокированным сайтам. Некоторые категории, такие как **System Errors** состоят как из журнальных записей, так и предупреждений. Вы можете различить их по цвету в окне **View Log**. Предупреждения отображаются красным цветом, а обычные журнальные записи – черным.

Журналы регистрации

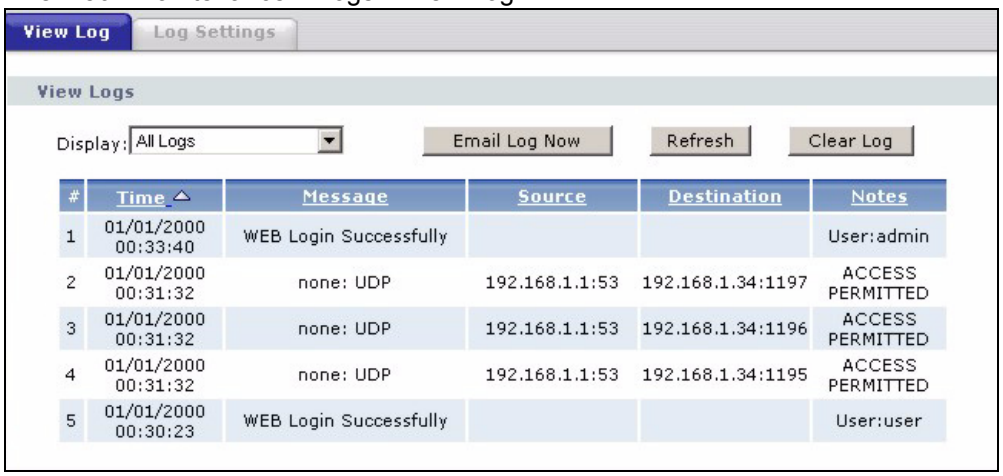
Журнал регистрации представляет собой сообщение о событии, которое произошло на вашем устройстве P660HN. Например, если кто-либо входит в систему устройства P660HN, можно настроить параметры расписания: как часто включается функция журнала регистрации, или как часто журнал отправляется на сервер системных журналов.

19.2 Экран просмотра журнала

В окне **View Log** можно посмотреть журнальные записи по категориям, выбранным в окне **Log Settings** (см. Разд. 19.3 на с. 266). Нажмите **Maintenance > Logs** для отображения окна **View Log**.

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. 150 Maintenance > Logs > View Log



В следующей таблице даны описания полей этого экрана.

Табл. 91 Maintenance > Logs > View Log

ПОЛЕ	ОПИСАНИЕ
Display	Категории, выбранные вами в окне **Log Settings** отобразятся в раскрывающемся списке. Выберите категорию записей для просмотра. Выберите функцию **All Logs**, чтобы просмотреть все категории записей, выбранные на экране **Log Settings**.
Email Log Now	Нажмите сюда для отправки журнала по адресу электронной почты, указанному в окне **Log Settings** (для этого сначала нужно заполнить поля **E-mail Log Settings** в окне **Log Settings**).
Refresh	Нажмите сюда для обновления экрана регистрационных записей.
Clear Log	Нажмите эту кнопку для удаления всех журналов регистрации.
#	В этом поле содержится последовательная величина, она не связана с вводом информации.
Time	В этом поле отображается время, когда была зарегистрирована запись.
Message	В этом поле приводится причина внесения записи в журнал.
Source	В этом поле указываются IP-адрес источника и номер порта входящего пакета.
Destination	В этом поле указываются IP-адрес получателя и номер порта входящего пакета.
Notes	В этом поле выводится дополнительная информация о регистрационной записи.

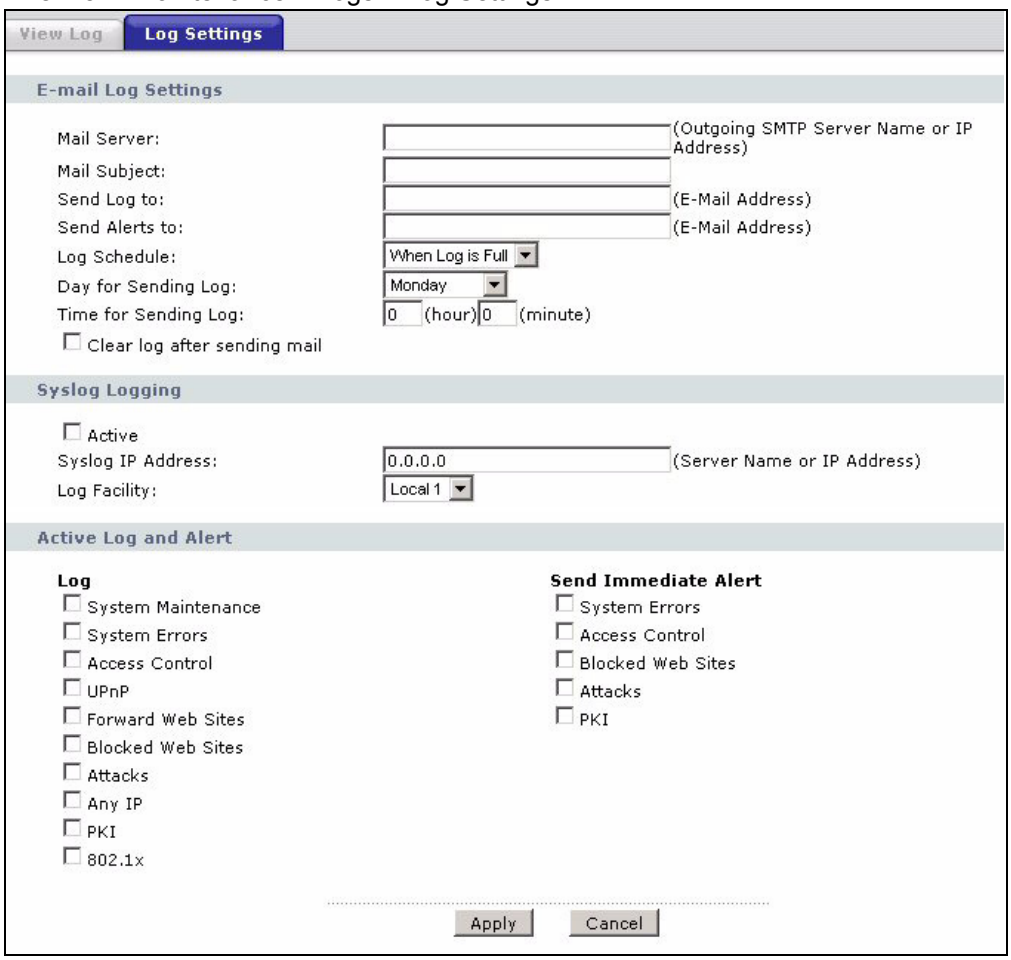
19.3 Окно настроек журнала

В окне **Log Settings** можно установить следующие параметры для почтового сервера и сервера хранения системных журналов: когда отправлять журналы и какие журналы.

Для изменения настроек журналов устройства P660HN нажмите **Maintenance > Logs** > **Log Settings**. При этом откроется показанный ниже экран.

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 **Access Control**) может привести к тому, что будет рассылаться большое количество сообщений электронной почты.

Рис. 151 Maintenance > Logs > Log Settings



В следующей таблице даны описания полей этого экрана.

Табл. 92 Maintenance > Logs > Log Settings

ПОЛЕ	ОПИСАНИЕ
E-mail Log Settings	
Mail Server	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 отправляться по электронной почте.

Табл. 92 Maintenance > Logs > Log Settings (продолжение)

ПОЛЕ	ОПИСАНИЕ
Mail Subject	Введите заголовок для помещения в строку «subject» (тема) сообщения электронной почты, отправляемого устройством P660HN. Это поле присутствует не во всех моделях устройств P660HN.
Send Log to	Устройство P660HN отправляет журналы регистрации по адресам электронной почты, указанным в этом поле. Если это поле оставить пустым, устройство P660HN не отправляет журналы по электронной почте.
Send Alerts to	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 попытках доступа к заблокированным веб-сайтам. Если это поле оставить пустым, предупреждающие сообщения не будут отправляться по электронной почте.
Log Schedule	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 (Никогда) При выборе опции **Weekly** или **Daily** необходимо указать время дня для рассылки электронных сообщений. При выборе опции **Weekly** также необходимо указать день недели для рассылки сообщений. При выборе опции **When Log is Full** сообщение посылается только при условии, что журнал заполнен. При выборе **None** сообщения не отправляются.
Day for Sending Log	Из раскрывающегося списка выберите день недели, в который должны отправляться записи.
Time for Sending Log	Введите время отправки журнальных записей в 24-часовом формате (например, 23:00 для 11 часов вечера).
Clear log after sending mail	Установите здесь флажок для удаления всех записей после их отправки устройством P660HN по электронной почте.
Syslog Logging	Устройство P660HN отправляет журнал на внешний сервер системного журнала.
Active	Для активации системного журнала нажмите **Active**.
Syslog IP Address	Введите имя сервера или IP-адрес сервера системных журналов, который будет регистрировать выбранные категории сообщений.
Log Facility	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	
Log	Выберите категории журнальных записей, которые необходимо регистрировать.
Send Immediate Alert	Выберите категории журналов, для которых устройство P660HN будет отправлять предупреждения по электронной почте немедленно.
Apply	Нажмите эту кнопку, чтобы сохранить измененные настройки и выйти из этого окна.
Cancel	Нажмите эту кнопку для восстановления ранее заданных настроек.

19.4 Сообщения об ошибках SMTP

При возникновении каких-либо трудностей при отправке электронной почты появляется следующее сообщение об ошибке.

«SMTP action request failed. ret= ??». Значения «??» приводятся в следующей таблице.

Табл. 93 Сообщения об ошибках SMTP

-1 означает, что устройство P660HN отключено от сети
-2 означает ошибку tcp SYN fail
-3 означает ошибку smtp server OK fail
-4 означает ошибку HELO fail
-5 означает ошибку MAIL FROM fail
-6 означает ошибку RCPT TO fail
-7 означает ошибку DATA fail
-8 означает ошибку mail data send fail

19.4.1 Пример журнала, высылаемого по электронной почте

Сообщение «End of Log» появляется каждый раз, когда отправляется полностью заполненный журнал. Ниже приводится пример журнала, посланного по электронной почте.

- Разрешено редактировать заглавие объекта.
- Сообщение «`End of Log`» означает, что отправлен весь журнал.

Рис. 152 Пример журнала, высылаемого по электронной почте

```
Subject:
        Firewall Alert From
   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
```

19.5 Описание сообщений журнала

В данном разделе приводится описание примеров сообщений в журнале регистрации.

Табл. 94 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 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.
`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.

Табл. 94 Журнальные сообщения, связанные с обслуживанием системы (продолжение)

СООБЩЕНИЕ	ОПИСАНИЕ
`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. 95 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. 96 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 брандмауэра, заданной по умолчанию, заблокирована либо переадресована, 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 брандмауэра (обозначается номером), заблокирована или переадресована согласно этому правилу.
`Triangle route packet forwarded: [TCP | UDP | IGMP | ESP | GRE | OSPF]`	Брандмауэр 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 веб-сайту.

Табл. 97 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 узлу).
`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: См. **TCP Maximum Incomplete** на экране **Firewall Attack Alerts**.
`Peer TCP state out of order, sent TCP RST`	Маршрутизатор отправил пакет сброса счетчика TCP при обнаружении сбоя в подключении через TCP. Примечание: Для проверки состояния подключения через TCP брандмауэр обращается к RFC793 (рис. 6).
`Firewall session time out, sent TCP RST`	Маршрутизатор отправил пакет сброса TCP по истечении времени простоя динамического сеанса связи через брандмауэр. Время простоя сеансов связи по умолчанию: Время простоя сеанса ICMP: 60 Время простоя сеанса UDP: 60 Время ожидания соединения TCP (трехстороннее согласование установления связи): 30 Время ожидания TCP FIN: 60 Время простоя соединения через TCP (установленного): 3600
`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. (Подсчет незавершенных подключений производится для всех подключений по TCP и UDP через брандмауэр.) Примечание: Когда количество незавершенных подключений (TCP + UDP) превышает верхний предел (Maximum Incomplete High), маршрутизатор отправляет пакеты сброса (TCP RST) для подключений через TCP и начинает удалять динамические сеансы связи через брандмауэр (TOS), пока количество незавершенных подключений не окажется меньше нижнего предела (Maximum Incomplete Low).
`Access block, sent TCP RST`	Маршрутизатор отправит пакет TCP RST и создаст эту запись в журнале, если вы включите механизм сброса TCP брандмауэра (с помощью команды интерпретатора «sys firewall tcprst»).

Табл. 98 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.

Подробное описание типов и кодов приведено в Табл. 107 на с. 275.

Табл. 99 Журнальные сообщения ICMP

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.
`Firewall rule [NOT] match: ICMP <Packet Direction>, <rule:%d>, <type:%d>, <code:%d>`	Доступ через ICMP, подпадающий (либо не подпадающий) под действие правила для брандмауэров (идентифицированное своим номером) и блокированный или переадресованный в соответствии с правилом.
`Triangle route packet forwarded: ICMP`	Брандмауэр 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`	Брандмауэр не поддерживает такие пакеты ICMP либо произошел сбой в пакетах ICMP.
`Router reply ICMP packet: ICMP`	Маршрутизатор послал ответный пакет ICMP отправителю.

Табл. 100 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. 101 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.

Табл. 101 Журнальные сообщения PPP (Протокол «точка-точка») (продолжение)

СООБЩЕНИЕ	ОПИСАНИЕ
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. 102 Журнальные сообщения UPnP

СООБЩЕНИЕ	ОПИСАНИЕ
UPnP pass through Firewall	Пакеты UPnP могут проходить через брандмауэр.

Табл. 103 Журнальные сообщения о фильтровании контента

СООБЩЕНИЕ	ОПИСАНИЕ
%s: block keyword	На запрошенной веб-странице имеется заданное пользователем ключевое слово.
%s	Система переадресовала содержание.

Подробное описание типов и кодов приведено в Табл. 107 на с. 275.

Табл. 104 Журнальные сообщения об атаках

СООБЩЕНИЕ	ОПИСАНИЕ
attack [TCP | UDP | IGMP | ESP | GRE | OSPF]	Брандмауэр обнаружил атаку TCP/UDP/IGMP/ESP/GRE/ OSPF.
attack ICMP (type:%d, code:%d)	Брандмауэр обнаружил атаку ICMP.
land [TCP | UDP | IGMP | ESP | GRE | OSPF]	Брандмауэр обнаружил атаку по TCP/UDP/IGMP/ESP/GRE/ OSPF на каталог локальной сети (LAND).
land ICMP (type:%d, code:%d)	Брандмауэр обнаружил атаку ICMP на каталог локальной сети (LAND).
ip spoofing - WAN [TCP | UDP | IGMP | ESP | GRE | OSPF]	Брандмауэр обнаружил атаку с подменой IP-адреса на порт WAN.
ip spoofing - WAN ICMP (type:%d, code:%d)	Брандмауэр обнаружил атаку с подменой IP-адреса ICMP на порт WAN.
icmp echo: ICMP (type:%d, code:%d)	Брандмауэр обнаружил атаку с использованием отклика ICMP.
syn flood TCP	Брандмауэр обнаружил синхронную атаку TCP.
ports scan TCP	Брандмауэр обнаружил атаку TCP со сканированием портов.
teardrop TCP	Брандмауэр обнаружил Teardrop-атаку TCP.
teardrop UDP	Брандмауэр обнаружил Teardrop-атаку UDP.

Табл. 104 Журнальные сообщения об атаках (продолжение)

СООБЩЕНИЕ	ОПИСАНИЕ
`teardrop ICMP (type:%d, code:%d)`	Брандмауэр обнаружил Teardrop-атаку ICMP.
`illegal command TCP`	Брандмауэр обнаружил атаку TCP с недопустимой командой.
`NetBIOS TCP`	Брандмауэр обнаружил атаку TCP NetBIOS.
`ip spoofing - no routing entry [TCP | UDP | IGMP | ESP | GRE | OSPF]`	Брандмауэр классифицировал пакет без записи о маршрутизации от источника как атаку с подстановкой IP (IP spoofing).
`ip spoofing - no routing entry ICMP (type:%d, code:%d)`	Брандмауэр классифицировал пакет ICMP без указания источника как атаку с подстановкой IP (IP spoofing).
`vulnerability ICMP (type:%d, code:%d)`	Брандмауэр обнаружил атаку ICMP на уязвимость.
`traceroute ICMP (type:%d, code:%d)`	Брандмауэр обнаружил атаку ICMP с отслеживанием маршрута.

Табл. 105 Журнальные сообщения 802.1X

СООБЩЕНИЕ	ОПИСАНИЕ
`RADIUS accepts user.`	Подлинность пользователя была установлена сервером RADIUS.
`RADIUS rejects user. Pls check RADIUS Server.`	Подлинность пользователя не была установлена сервером RADIUS. Проверьте сервер RADIUS.
`User logout because of session timeout expired.`	Маршрутизатор вывел из системы пользователя с истекшим сроком действия сеанса связи.
`User logout because of user deassociation.`	Маршрутизатор вывел из системы пользователя, завершившего сеанс связи.
`User logout because of no authentication response from user.`	Маршрутизатор вывел из системы пользователя, от которого не поступил ответ на аутентификацию.
`User logout because of idle timeout expired.`	Маршрутизатор вывел из системы пользователя, у которого превышен лимит времени простоя.
`User logout because of user request.`	Пользователь вышел из системы.
`No response from RADIUS. Pls check RADIUS Server.`	Нет ответа от сервера RADIUS, проверьте сервер RADIUS.
`Use RADIUS to authenticate user.`	Сервер RADIUS работает в качестве аутентификационного сервера.
`No Server to authenticate user.`	Отсутствует аутентификационный сервер, способный установить подлинность пользователя.

Табл. 106 Настройка списка управления доступом (ACL)

НАПРАВЛЕНИЕ ПАКЕТОВ	НАПРАВЛЕНИЕ	ОПИСАНИЕ
(L – W)	от LAN к WAN	Список контроля доступа (ACL) для пакетов, пересылаемых из локальной сети (LAN) в глобальную (WAN).
(W – L)	от WAN к LAN	Список управления доступом (ACL) для пакетов, пересылаемых из глобальной сети (WAN) в локальную (LAN).
(L – L/устройство P660HN)	от LAN к LAN/ устройство P660HN (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 устройство P660HN.
(W – W/устройство P660HN)	от WAN к WAN/ устройство P660HN (глобальная сеть – глобальная сеть/ устройство)	Список управления доступом (ACL) для пакетов, пересылаемых из одной глобальной сети в другую или в устройство P660HN.

Табл. 107 Записи ICMP

ТИП	КОД	ОПИСАНИЕ
0		Эхо-ответ
	0	Сообщение с эхо-ответом
3		Адресат недоступен
	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 назначения.
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

Табл. 107 Записи ICMP (продолжение)

ТИП	КОД	ОПИСАНИЕ
	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. 108 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: MAIN MENU->LOGS->Log Settings 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 2408

Табл. 109 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

20

Программные средства

20.1 Обзор

В этой главе описывается, как загружать новое микропрограммное обеспечение, управлять файлами конфигурации и перезагружать устройство P660HN.

Используйте инструкции в данной главе для изменения файла конфигурации устройства или для обновления его микропрограммного обеспечения. После настройки конфигурации своего устройства вы можете записать резервную копию файла конфигурации на компьютер. Таким образом, если у вас в дальнейшем собьется настройка устройства, можно загрузить резервный файл конфигурации для возврата системы к предыдущим настройкам. Можно также загрузить заводской файл конфигурации с настройками по умолчанию, если вы хотите вернуться к исходным настройкам по умолчанию. Микропрограммное обеспечение определяет доступные возможности и функции устройства. Можно загружать новые версии микропрограммного обеспечения с сайта *zyxel.ru*, чтобы обновить рабочие характеристики вашего устройства.

Необходимо использовать микропрограммное обеспечение строго в соответствии с конкретной моделью устройства. См. наклейку, находящуюся на нижней панели устройства P660HN.

20.1.1 Что можно сделать на экранах программных средств

- Экран **Firmware Upgrade** (Разд. 20.2 на с. 285) используется для обновления микропрограммного обеспечения в устройстве.
- Экран **Configuration** (Разд. 20.3 на с. 287) используется для создания резервной копии/восстановления файла конфигурации. Можно также сбросить настройки устройства к заводским настройкам по умолчанию.
- Экран **Restart** (Разд. 20.4 на с. 290) используется для перезапуска устройства ZyXEL.

20.1.2 Что нужно знать о программных средствах

Соглашение по именам файлов

Файл конфигурации (часто называемый также romfile или rom-0) содержит настройки, установленные изготовителем по умолчанию, например: пароль, настройки DHCP, настройки TCP/IP и т. д. Этот файл поставляется корпорацией ZyXEL и имеет расширение rom. Если вы изменили настройки устройства P660HN, то эти изменения можно сохранить в файле под другим именем, по вашему выбору.

ZyNOS (Сетевая операционная система корпорации ZyXEL, иногда называемая «ras файл») представляет собой микропрограммное обеспечение системы; файлы системы имеют расширение bin. Это микропрограммное обеспечение можно найти на сайте www.zyxel.com. У большинства клиентов FTP и TFTP имена файлов схожи с представленными ниже.

```
ftp> put firmware.bin ras
```

Это пример сеанса FTP для передачи файла firmware.bin с компьютера в устройство P660HN

```
ftp> get rom-0 config.cfg
```

Это пример сеанса FTP для сохранения на компьютере текущей конфигурации модема в файл `config.cfg`.

Если ваш (T)FTP-клиент не допускает, чтобы имя полученного файла отличалось от имени файла-источника, то вам потребуется переименовать оба файла, поскольку устройство P660HN распознает только файлы с расширением «rom-0» и «ras». Обязательно сохраните не измененные копии обоих первоначальных файлов, они потребуются в дальнейшем.

Ниже представлена таблица, содержащая сводную информацию. Следует отметить, что имя внутреннего файла обозначает файл, находящийся на устройстве P660HN, а имя внешнего файла обозначает файл не в устройстве P660HN, т. е. в вашем компьютере, локальной сети или на FTP-сайте, поэтому имя (но не расширение) может меняться. После загрузки нового микропрограммного обеспечения посмотрите на экран **Status**, чтобы убедиться, что загружена правильная версия микропрограммного обеспечения.

Табл. 110 Соглашение по именам файлов

ТИП ФАЙЛА	ВНУТРЕННЕЕ ИМЯ	ВНЕШНЕЕ ИМЯ	ОПИСАНИЕ
Файл конфигурации	Rom-0	Имя файла конфигурации, находящегося на устройстве P660HN. При выгрузке файла rom-0 происходит замена всей файловой системы ПЗУ, включая конфигурацию вашего устройства P660HN, данные, относящиеся к системе (в том числе и пароля по умолчанию), журнал регистрации ошибок и журнал регистрации результатов трассировки.	*.rom
Микропрограммное обеспечение	Ras	Базовое имя для микропрограммного обеспечения ZyNOS на устройстве P660HN.	*.bin

Ограничения FTP

FTP не работает в том случае когда:

1. Брандмауэр включен (выключите брандмауэр или создайте правило для разрешения доступа из глобальной сети).
2. Отключена служба FTP на экране **Remote Management**.
3. IP-адрес, установленный в поле «Secured Client IP» (IP-адрес доверенного клиента), не совпадает с IP-адресом клиента. В этом случае устройство немедленно запрещает сеанс связи.

20.1.3 Перед началом

- Убедитесь в том, что вы создали правило брандмауэра для разрешения доступа из глобальной сети или выключили брандмауэр; в противном случае FTP работать не будет.
- Убедитесь, что служба FTP не отключена на экране Remote Management.

20.1.4 Примеры программных средств

Использование FTP или TFTP для восстановления конфигурации

В данном примере описывается порядок восстановления предварительно сохраненных параметров конфигурации. Следует иметь в виду, что при выполнении данной функции, прежде, чем резервная конфигурация будет восстановлена, текущая конфигурация – удаляется. Поэтому, прежде чем запустить процесс восстановления, убедитесь, что файл с резервной копией конфигурации сохранен на диске.

Наиболее предпочтительным способом восстановления текущей конфигурации компьютера для вашего устройства является протокол FTP потому, что он быстрее остальных. Следует помнить, что после завершения процесса загрузки файла, необходимо дождаться автоматической перезагрузки системы.

НЕ ПРЕРЫВАЙТЕ процесс передачи файла, так как это может привести к НЕУСТРАНИМЫМ ПОВРЕЖДЕНИЯМ устройства. После завершения процесса восстановления конфигурации устройство автоматически перезапускается.

Пример восстановления конфигурации с помощью сеанса FTP

Рис. 153 Пример восстановления конфигурации с помощью сеанса FTP

```
ftp> put config.rom rom-0
200 Port command okay
150 Opening data connection for STOR rom-0
226 File received OK
221 Goodbye for writing flash
ftp: 16384 bytes sent in 0.06Seconds 273.07Kbytes/sec.
ftp> quit
```

Информацию о настройках, которые не позволяют использовать TFTP и FTP по глобальной сети, см. в Разд. 20.1.2 на с. 279.

Загрузка микропрограммного обеспечения и файлов конфигурации с помощью FTP и TFTP

В этих примерах описывается, как выгрузить файлы микропрограммного обеспечения и файлы конфигурации.

НЕ ПРЕРЫВАЙТЕ процесс передачи файла, так как это может привести к НЕУСТРАНИМЫМ ПОВРЕЖДЕНИЯМ устройства.

Предпочтительным методом выгрузки файлов микропрограммного обеспечения и файлов конфигурации является FTP. Для использования данной функции на компьютере должен быть установлен FTP-клиент. В приведенных ниже разделах приведены примеры того, как загружать микропрограммное обеспечение и файлы конфигурации.

Пример команды выгрузки файла FTP из подсказки DOS

1. Запустите FTP-клиент на вашем компьютере.
2. Введите команду «open», а затем – IP-адрес вашего устройства через пробел.
3. В диалоговом окне введите имя пользователя и нажмите кнопку [ENTER].
4. В окне запроса введите пароль (по умолчанию «1234»).
5. Введите «bin» для того, чтобы установить двоичный режим передачи.
6. Для передачи файлов с вашего компьютера на ваше устройство, используйте команду «put», например, «put firmware.bin ras». Эта команда передает микропрограммное обеспечение (firmware.bin) с вашего компьютера на ваше устройство и переименовывает его в «ras». Точно также, команда «put config.rom rom-0» передает файл конфигурации (config.rom) с вашего компьютера на ваше устройство и переименовывает его в «rom-0». Так же команда «get rom-0 config.rom» передает файл конфигурации с вашего устройства на ваш компьютер и переименовывает его в «config.rom.» Более подробно о соглашении по именам файлов, см. выше в данной главе.
7. Для выхода из режима FTP, введите команду «quit».

Пример сеанса FTP по выгрузке файла микропрограммного обеспечения

Рис. 154 Пример сеанса FTP по выгрузке файла микропрограммного обеспечения

```
331 Enter PASS command
Password:
230 Logged in
ftp>bin
200 Type I OK
ftp> put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 1103936 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

Другие команды описаны выше в данной главе, в разделе, посвященном FTP-клиентам с графическим интерфейсом.

Информацию о настройках, которые не позволяют использовать TFTP и FTP по глобальной сети, см. в Разд. 20.1.2 на с. 279.

Выгрузка файлов по протоколу TFTP

Устройство поддерживает загрузку файлов микропрограммного обеспечения с помощью протокола TFTP (Trivial File Transfer Protocol – Простейший протокол передачи данных) по локальной сети. Хотя TFTP также работает и по глобальной сети, этого делать не рекомендуется.

Для того чтобы использовать протокол TFTP, на вашем компьютере должны быть установлены и клиент Telnet, и TFTP-клиент. Для передачи микропрограммного обеспечения и файла конфигурации выполните описанную ниже процедуру.

1. При помощи сетевого теледоступа (Telnet), установленного на вашем компьютере, подключитесь к устройству и зарегистрируйтесь. Поскольку протокол TFTP не обладает функциями проверки для защиты информации, устройство записывает IP-адрес Telnet-клиента и принимает запросы TFTP только с этого адреса.
2. Для отключения интервала простоя системы во время сеанса управления введите команду «sys stdio 0». При этом передача данных по протоколу TFTP не прервется. По окончании передачи файла, для восстановления 5-минутного интервала простоя системы во время сеанса управления (значение, устанавливаемое по умолчанию), введите команду «sys stdio 5».
3. Запустите на вашем компьютере TFTP-клиент и подключитесь к устройству. Прежде чем начать процесс передачи данных, установите двоичный режим передачи.
4. Для передачи файлов между устройством и компьютером используйте TFTP-клиент (см. пример ниже). Имя файла микропрограммного обеспечения – «ras».

Следует помнить, что подключение через Telnet должно быть активно, а устройство должно находиться в режиме командного процессора (CI mode) как до, так и во время передачи по протоколу TFTP. Более подробно о командах TFTP (см. следующий пример) можно узнать в сопроводительной документации к клиентской программе TFTP. Если вы работаете в системе UNIX, то команду «get» используйте для передачи файлов с устройства на компьютер, команду «put», наоборот, для передачи файлов с компьютера на устройство, а команду «binary» – для установки двоичного режима передачи данных.

Пример команды для загрузки файла с помощью сеанса TFTP

Ниже приводится пример команды TFTP:

```
tftp [-i] host put firmware.bin ras
```

Где «i» указывает на двоичный режим передачи (этот режим используется для передачи двоичных файлов), «host» – IP-адрес устройства, а «put» – команда передачи файла, находящегося на компьютере («firmware.bin» – имя файла микропрограммного обеспечения, находящегося на компьютере), на удаленный узел («ras» – имя микропрограммного обеспечения, находящегося на устройстве).

Перечень команд, используемых в TFTP-клиентах с графическим интерфейсом, приведен выше в этой главе.

Использование команд FTP для резервирования конфигурации

1. Запустите FTP-клиент на вашем компьютере.
2. Введите команду «`open`», а затем через пробел – IP-адрес вашего устройства P660HN.
3. В диалоговом окне введите имя пользователя и нажмите кнопку [ENTER].
4. В окне запроса введите пароль (по умолчанию «1234»).
5. Введите «`bin`» для того, чтобы установить двоичный режим передачи.
6. Используйте команду «`get`» для передачи файлов с устройства P660HN на ваш компьютер, например, «`get rom-0 config.rom`». Эта команда передает файл конфигурации, находящийся на устройстве P660HN на ваш компьютер и переименовывает его в «`config.rom`». Более подробно о соглашении по именам файлов, см. выше в данной главе.
7. Для выхода из режима FTP, введите команду «`quit`».

Пример резервирования конфигурации команды FTP

На этом рисунке приведен пример использования команд FTP из командной строки DOS для сохранения конфигурации устройства в вашем компьютере.

Рис. 155 Пример сеанса FTP

```
331 Enter PASS command
Password:
230 Logged in
ftp>bin
200 Type I OK
ftp> get rom-0 zyxel.rom
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 16384 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

Резервирование конфигурации с помощью FTP-клиентов с графическим интерфейсом

В таблице ниже приводятся описания некоторых команд, используемых в TFTP-клиентах с графическим интерфейсом (GUI).

Табл. 111 Основные команды для FTP-клиентов с графическим интерфейсом

КОМАНДА	ОПИСАНИЕ
Host Address	Введите адрес хост-сервера.
Login Type	Anonymous. Этот тип регистрации используется в случаях, когда идентификатор пользователя и пароль автоматически передаются серверу для получения анонимного доступа. Анонимная регистрация возможна, только если администратор услуг Интернет-провайдера включил данную опцию. Normal. Для регистрации необходимо ввести уникальный идентификатор пользователя и пароль.

Табл. 111 Основные команды для FTP-клиентов с графическим интерфейсом (продолжение)

КОМАНДА	ОПИСАНИЕ
Transfer Type	Передача файлов либо в режиме ASCII (формат обычного текста), либо в двоичном режиме.
Initial Remote Directory	Укажите удаленный каталог по умолчанию (путь).
Initial Local Directory	Укажите локальный каталог по умолчанию (путь).

Резервное копирование конфигурации с помощью TFTP

Устройство P660HN поддерживает загрузку/выгрузку микропрограммного обеспечения и файла конфигурации с помощью протокола TFTP (Trivial File Transfer Protocol – Простейший протокол передачи данных) по локальной сети. Хотя TFTP также работает и по глобальной сети, этого делать не рекомендуется.

Для того, чтобы использовать протокол TFTP, на вашем компьютере должны быть установлены и клиент Telnet, и TFTP-клиент. Для создания резервной копии файла конфигурации, выполните указанные ниже операции.

1. При помощи сетевого теледоступа (Telnet), установленного на вашем компьютере, подключитесь к P660HN и зарегистрируйтесь. Поскольку протокол TFTP не обладает функциями проверки для защиты информации, устройство P660HN записывает IP-адрес Telnet-клиента и принимает запросы TFTP только с этого адреса.
2. Для отключения интервала простоя системы во время сеанса управления, введите команду «`sys stdio 0`». При этом передача данных по протоколу TFTP не прервется. По окончании передачи файла для восстановления 5-минутного интервала простоя системы во время сеанса управления (значение, устанавливаемое по умолчанию) введите команду «`sys stdio 5`».
3. Запустите на вашем компьютере TFTP-клиент и подключитесь к устройству P660HN. Прежде чем начать процесс передачи данных, установите двоичный режим передачи.
4. Для передачи файлов между устройством P660HN и компьютером, используйте TFTP-клиент (см. пример ниже). Для файла конфигурации используется имя «`rom-0`» (rom-ноль, а не заглавная буква O).

Следует помнить, что подключение через Telnet должно быть активно как до, так и во время передачи по протоколу TFTP. Более подробно о командах TFTP (см. следующий пример) можно узнать в сопроводительной документации к клиентской программе TFTP. Если вы работаете в системе UNIX, то команду «`get`» используйте для передачи файлов с устройства P660HN на компьютер, а команду «binary» – для установки двоичного режима передачи данных.

Пример резервирования конфигурации команды TFTP

Ниже приводится пример команды TFTP:

```
tftp [-i] host get rom-0 config.rom
```

где «`i`» обозначает двоичный режим передачи (этот режим используется при передаче файлов в двоичном коде), «`host`» – IP-адрес устройства P660HN, «`get`» выполняет передачу файла источника, находящегося в устройстве P660HN (`rom-0` – имя файла конфигурации устройства P660HN) на компьютер и переименовывает его в config.rom.

Резервирование конфигурации с помощью FTP-клиентов с графическим интерфейсом

В таблице ниже приводятся описания некоторых команд, используемых в TFTP-клиентах с графическим интерфейсом (GUI).

Табл. 112 Основные команды TFTP-клиентов на основе GUI

КОМАНДА	ОПИСАНИЕ
Host	Введите IP-адрес принт-сервера устройства P660HN. При поставке, IP-адресом устройства P660HN по умолчанию является: 192.168.1.1.
Send/Fetch	Для того, чтобы выгрузить файл с компьютера на устройство P660HN, используется команда «Send», а для того, чтобы загрузить файл на компьютер с устройства – команда «Fetch».
Local File	Введите путь и имя файла микропрограммного обеспечения (расширение файла: *.bin) или файла конфигурации (расширение файла: *.rom), находящегося на вашем компьютере.
Remote File	Имя файла, находящегося на устройстве P660HN. Для файла микропрограммного обеспечения используется имя «ras», а для файла конфигурации -«rom-0».
Binary	Передача файла в двоичном режиме.
Abort	Остановка процесса передачи файла.

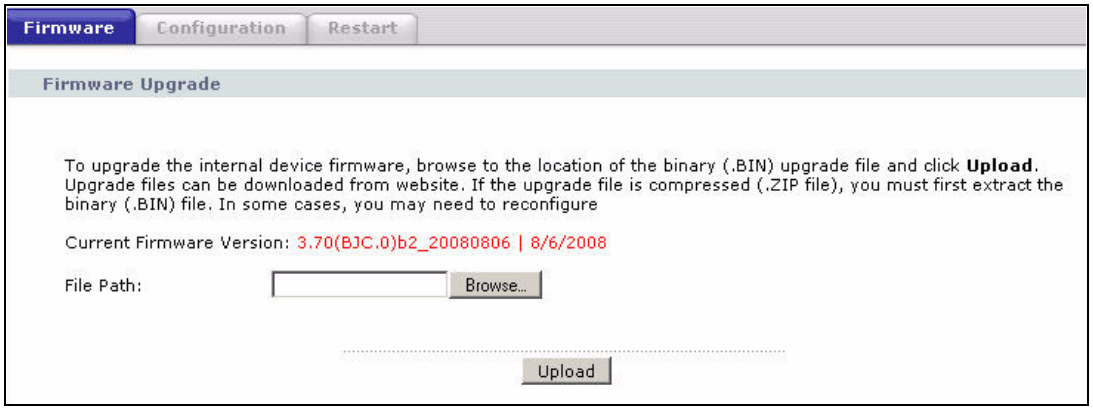
Информацию о настройках, которые не позволяют использовать TFTP и FTP по глобальной сети, см. в Разд. 20.1.2 на с. 279.

20.2 Экран микропрограммного обеспечения

Нажмите **Maintenance > Tools**, чтобы открыть экран **Firmware**. Следуйте указаниям на этом экране для загрузки микропрограммного обеспечения в устройство P660HN. Для загрузки используется протокол HTTP (Hypertext Transfer Protocol – Протокол передачи гипертекста), загрузка может занять до 2-х минут. После успешной загрузки микропрограммы система перезапускается. Для обновления микропрограммного обеспечения с помощью команд FTP/TFTP см. Разд. 20.1.4 на с. 280.

НЕЛЬЗЯ выключать питание устройства P660HN во время загрузки микропрограммного обеспечения!

Рис. 156 Maintenance > Tools > Firmware



В следующей таблице даны описания полей этого экрана.

Табл. 113 Maintenance > Tools > Firmware

ПОЛЕ	ОПИСАНИЕ
Current Firmware Version	Здесь отображается текущая версия и дата создания микропрограммного обеспечения.
File Path	Введите в это поле путь к файлу, который требуется загрузить, или нажмите **Browse...** для его поиска.
Browse...	Нажмите эту кнопку для поиска файла .bin, который требуется загрузить. Архивированные файлы (.zip) необходимо распаковать, прежде чем выполнять загрузку.
Upload	Нажмите эту кнопку для запуска процесса загрузки. Процесс загрузки может занять до 2 минут.

После появления экрана **Firmware Upload in Progress**, подождите 2 минуты, прежде чем снова регистрироваться в устройстве P660HN.

Рис. 157 Выполняется загрузка микропрограммного обеспечения

Устройство P660HN автоматически перезапускается, что вызывает временное отключение устройства от сети. В некоторых операционных системах может появиться следующая иконка на рабочем столе.

Рис. 158 Временное отключение сети

По истечении 2 минут снова зарегистрируйтесь и проверьте версию нового микропрограммного обеспечения на экране **Status**.

Если загрузку не удалось завершить успешно, появляется следующий экран. Нажмите **Return** для возврата к экрану **Firmware**.

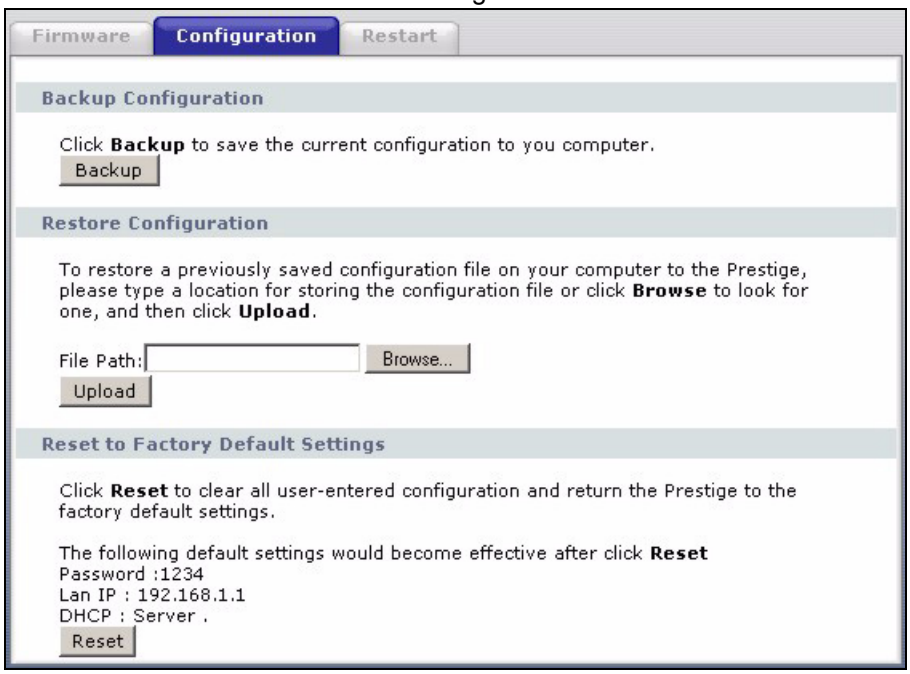
Рис. 159 Сообщение об ошибке

20.3 Экран параметров

Информацию по переносу файлов конфигурации с помощью команд FTP/TFTP см. в Разд. 20.1.4 на с. 280.

Нажмите **Maintenance > Tools > Configuration**. На этом экране отображается информация о заводских настройках по умолчанию, резервном сохранении и восстановлении конфигурации.

Рис. 160 Maintenance > Tools > Configuration



Резервная конфигурация

Резервное копирование конфигурации позволяет сохранить текущую конфигурацию устройства P660HN в файле на компьютере. Если настройка устройства P660HN 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 необходимо вернуться к предыдущим настройкам.

Для сохранения текущей конфигурации устройства P660HN на компьютере нажмите **Backup**.

Восстановление конфигурации

Функция восстановления конфигурации позволяет загрузить с компьютера в устройство P660HN новый или предварительно сохраненный файл конфигурации.

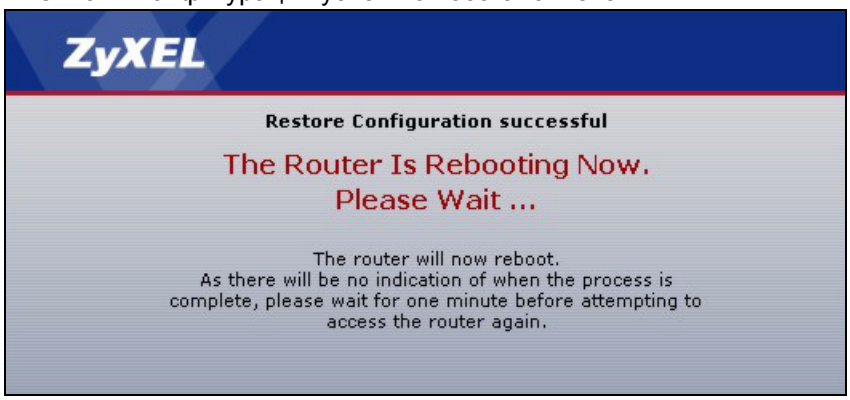
Табл. 114 Восстановление конфигурации

ПОЛЕ	ОПИСАНИЕ
File Path	Введите в это поле путь к файлу, который требуется загрузить, или нажмите **Browse...** для его поиска.
Browse...	Нажмите эту кнопку для поиска файла, который требуется загрузить. Архивированные файлы (.zip) необходимо распаковать, прежде чем выполнять загрузку.
Upload	Нажмите эту кнопку для запуска процесса загрузки.

НЕЛЬЗЯ выключать питание устройства P660HN во время загрузки файла конфигурации!

После появления экрана «Restore Configuration successful» (Конфигурация успешно восстановлена), необходимо подождать одну минуту, прежде чем снова регистрироваться в устройстве P660HN.

Рис. 161 Конфигурация успешно восстановлена



Устройство P660HN автоматически перезапускается, что вызывает временное отключение устройства от сети. В некоторых операционных системах может появиться следующая иконка на рабочем столе.

Рис. 162 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 по умолчанию (192.168.1.1). Подробней о задании IP-адреса для компьютера – см. Прил. A на с. 309.

Если загрузку не удалось завершить успешно, появляется следующий экран. Нажмите **Return** для возврата к экрану **Configuration**.

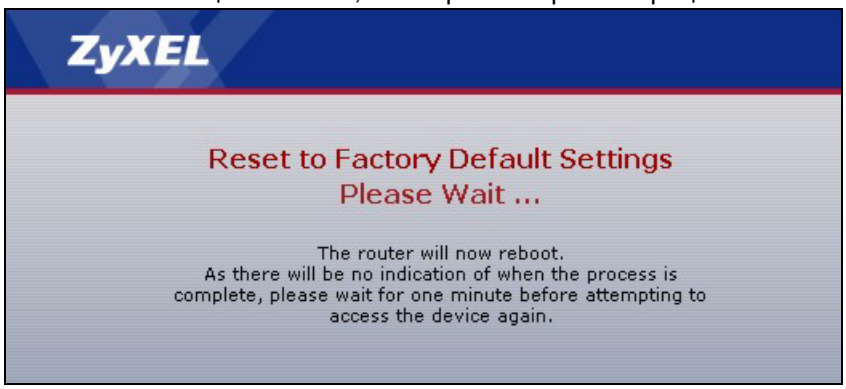
Рис. 163 Ошибка загрузки файла конфигурации

Сброс к заводским настройкам по умолчанию

Нажмите кнопку **Reset** для полного удаления пользовательской конфигурации и сброса параметров устройства P660HN к заводским настройкам по умолчанию. Появится следующий экран с предупреждением.

Рис. 164 Предупреждающее сообщение о сбросе настроек

Рис. 165 Сообщение о том, что сброс настроек в процессе



Восстановление заводских настроек устройства P660HN также можно выполнить, нажав кнопку **RESET** на задней панели устройства. Подробнее о кнопке **Reset** см. в Разд. 1.6 на с. 31.

20.4 Экран перезапуска

Этот экран позволяет выполнить удаленную перезагрузку устройства P660HN без выключения электропитания. Вам может это потребоваться, например, при зависании устройства P660HN.

Нажмите **Maintenance > Tools** > **Restart**. Нажмите **Restart** для перезагрузки устройства P660HN. Эта операция не влияет на конфигурацию устройства P660HN.

Рис. 166 Maintenance > Tools > Restart

21

Диагностика

21.1 Обзор

Информация в этих экранах представлена в режиме только для чтения и предназначена, чтобы помочь определить неисправность устройства P660HN.

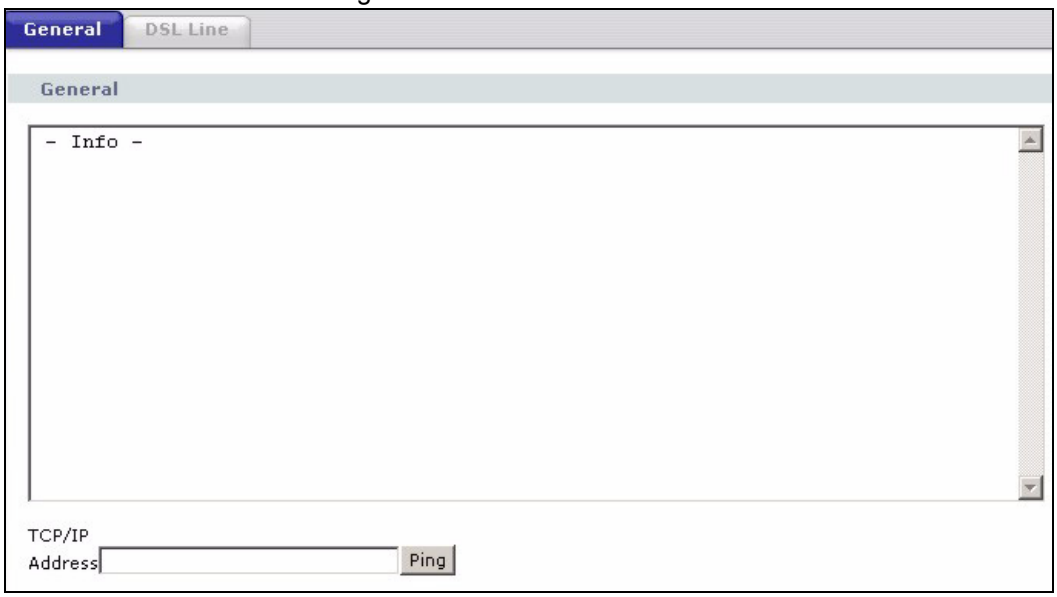
21.1.1 Что можно сделать на экранах диагностики

- Экран **General Diagnostic** (Разд. 21.2 на с. 291) используется для тестирования IP-адреса.
- Экран **DSL Line Diagnostic** (Разд. 21.3 на с. 292) используется для просмотра статистики линии DSL и сброса линии ADSL.

21.2 Экран общей диагностики

Этот экран используется для тестирования IP-адреса. Нажмите **Maintenance > Diagnostic**, чтобы открыть показанный ниже экран.

Рис. 167 Maintenance > Diagnostic > General



В следующей таблице даны описания полей этого экрана.

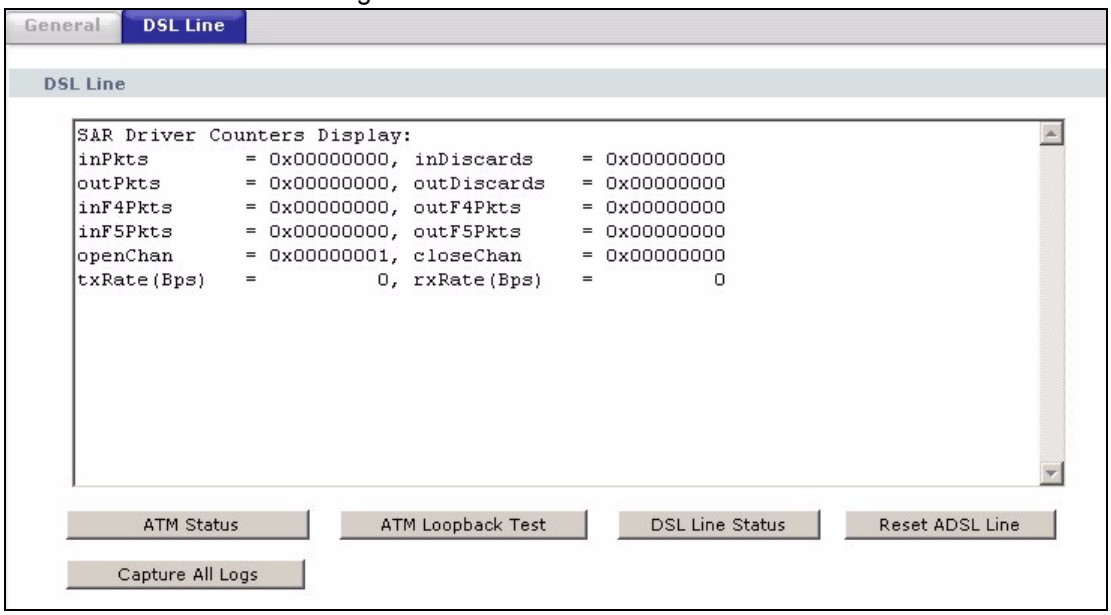
Табл. 115 Maintenance > Diagnostic > General

ПОЛЕ	ОПИСАНИЕ
TCP/IP Address	Введите IP-адрес компьютера, который необходимо протестировать с помощью команды «ping», чтобы проверить соединение.
Ping	Нажмите эту кнопку для тестирования устройства с введенным IP-адресом с помощью команды «ping».

21.3 Экран диагностики линии DSL

Этот экран используется для просмотра статистики линии DSL и сброса линии ADSL. Нажмите **Maintenance > Diagnostic** > **DSL Line**, чтобы открыть показанный ниже экран.

Рис. 168 Maintenance > Diagnostic > DSL Line



В следующей таблице даны описания полей этого экрана.

Табл. 116 Maintenance > Diagnostic > DSL Line

ПОЛЕ	ОПИСАНИЕ
ATM Status	Нажмите для просмотра статистики ATM (Asynchronous Transfer Mode – Асинхронный режим передачи) вашего DSL-соединения. ATM является сетевой технологией, обеспечивающей высокую скорость передачи данных. В ATM используются пакеты информации фиксированного размера, называемые ячейками. С помощью ATM может быть гарантировано высокое качество предоставляемых услуг (QoS). Драйвер SAR (Segmentation and Reassembly – сегментация и сборка) переводит пакеты в ячейки ATM. Он также получает ячейки ATM и перетранслирует их в пакеты. При каждом запуске устройства счетчики ячеек устанавливаются на ноль. **inPkts** – количество полученных рабочих ячеек ATM. **inDiscards** – количество полученных ячеек ATM, которые были отклонены. **outPkts** – количество отправленных ячеек ATM. **outDiscards** – количество отправленных ячеек ATM, которые были отклонены. **inF4Pkts** – количество полученных ячеек ATM OAM F4 (Operations, Administration, Management – операции, администрирование, управление). Подробную информацию о OAM для ATM см. в рекомендациях ITU I.610. **outF4Pkts** – количество отправленных ячеек ATM OAM F4. **inF5Pkts** – количество полученных ячеек ATM OAM F5. **outF5Pkts** – количество отправленных ячеек ATM OAM F5. **openChan** – количество случаев открытия устройством P660HN логического DSL-канала. **closeChan** – количество случаев закрытия устройством P660HN логического DSL-канала. **txRate** – скорость передачи данных в байтах в секунду. **rxRate** – скорость приема данных в байтах в секунду.
ATM Loopback Test	Нажмите 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. Устройство P660HN посылает пакет OAM F5 на коммутатор DSLAM/ATM, после чего он возвращается обратно в устройство P660HN. Кольцевое тестирование ATM используется для поиска и устранения неисправностей в сети ATM.

Табл. 116 Maintenance > Diagnostic > DSL Line (продолжение)

ПОЛЕ	ОПИСАНИЕ
DSL Line Status	Нажмите для просмотра статистики по DSL-соединениям. **noise margin downstream** – это соотношение «сигнал/помеха» для входящего потока данных для этого соединения (от Интернет-провайдера к устройству P660HN). Измеряется в децибелах. Чем больше это число, тем лучше сигнал и меньше помехи. **output power upstream** – мощность (в децибелах), которую устройство P660HN использует для передачи данных к Интернет-провайдеру. **attenuation downstream** – уменьшение амплитуды (в децибелах) сигналов DSL от Интернет-провайдера к устройству P660HN. Модуляция DMT (Discrete Multi-Tone modulation – цифровая многочастотная модуляция) разделяет полосу частот линии на подканалы частотой 4,3125 кГц, называемые тональными сигналами. Остальная часть – это отображение распределения битов в линии. Отображается как количество битов (в шестнадцатеричном формате), переданных каждым тональным сигналом. Это используется для определения качества соединения: имеет ли петля на конкретной поднесущей достаточный запас помехоустойчивости, чтобы поддерживать скорость передачи ADSL, а также существуют ли в линии помехи особенного типа или затухание. Для получения информации по DMT см. рекомендации ITU-T G.992.1. Чем выше качество линии (или линия короче), тем будет больше количество битов, передаваемых тональным сигналом DMT. Максимальное количество битов, передаваемое каждым тональным сигналом DMT, равно 15. Некоторые тональные сигналы будут вообще без битов, так как должно быть некоторое расстояние между исходящим и входящим каналом.

Reset ADSL Line	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	Нажмите для отображения статистики ATM устройства P660HN, статистики DSL-соединений, информации о настройках DHCP, версии микропрограммного обеспечения, IP-адресе WAN и шлюза, IP-адресе VPI/VCI и LAN.

Часть VI
Устранение неисправностей и спецификации

22

Характеристики устройства

В следующей таблице представлены характеристики оборудования и микропрограммного обеспечения устройства P660HN.

22.1 Технические характеристики оборудования

Табл. 117 Технические характеристики оборудования

Габариты	189(Ш) x 132(Д) x 42(В) мм
Вес	325 г без адаптера питания
Питание	12 В DC (постоянный ток), 1 А
Встроенный коммутатор	Четыре порта Ethernet MDI/MDI-X 10/100 Мбит/с RJ-45 с автоматическим выбором скорости
Порт ADSL	1 порт RJ-11
Кнопка RESET	Восстанавливает заводские значения по умолчанию
Антенна	Две съемные антенны, 5 дБ
Кнопка WPS	1–5 секунд: включение или выключение WLAN 5–10 секунд: включение WPS (настройка безопасности Wi-Fi)
Рабочая температура	0 °C–40 °C
Температура хранения	-20 °C–60 °C
Рабочая влажность	20 %–90 %
Относительная влажность при хранении	20 %–90 %

22.2 Характеристики микропрограммного обеспечения

Табл. 118 Характеристики микропрограммного обеспечения

IP-адрес по умолчанию	192.168.1.1
Маска подсети по умолчанию	255.255.255.0 (24 бита)
Стандартный пароль пользователя (User Password)	user
Стандартный пароль администратора (Admin Password)	1234
IP-диапазон сервера DHCP	192.168.1.32 – 192.168.1.64
Статические адреса DHCP	10
Контент-фильтрование	Блокировка веб-сайтов по ключевому слову в URL.
Статические маршруты	16
Управление устройством	Web-конфигуратор упрощает настройку широкого спектра функций устройства P660HN.
Функции беспроводной связи (только для беспроводных устройств)	Устройство P660HN поддерживает беспроводное подключение клиентов по стандартам IEEE 802.11b, IEEE 802.11g и/или IEEE 802.11n. Для защиты беспроводной сети можно задействовать функции безопасности (WEP, WPA(2), WPA(2)-PSK) и фильтрование на основе MAC-адресов.
Обновление встроенного микропрограммного обеспечения	Загрузите новую версию микропрограммного обеспечения (если есть) с веб-сайта ZyXEL в устройство P660HN с помощью Web-конфигуратора, по FTP или TFTP. Примечание: Необходимо загружать микропрограммное обеспечение строго в соответствии с конкретной моделью устройства!
Резервное копирование и восстановление конфигурации	Сделайте копию конфигурации устройства P660HN. Эту копию можно загрузить в устройство P660HN 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 вашей домашней сети есть сервер (например, веб-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 устройство P660HN назначает IP-адреса, шлюз IP по умолчанию и серверы DNS компьютерам локальной сети. Ваше устройство также может функционировать как фиктивный сервер DHCP (ретранслятор DHCP), т. е. передавать клиентам назначенные IP-адреса от настоящего сервера DHCP.

Табл. 118 Характеристики микропрограммного обеспечения (продолжение)

Поддержка динамических DNS	Поддержка динамических DNS (Domain Name System – Система доменных имен) позволяет использовать фиксированный URL с динамическим IP-адресом. Для использования этой услуги необходимо зарегистрироваться у провайдера услуг динамического DNS.
Многоадресная рассылка IP	Многоадресная рассылка IP используется для отправки трафика определенной группе компьютеров. Устройство P660HN 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).
Время и дата	Можно синхронизировать текущее время и дату с внешним сервером времени при включении питания устройства P660HN. Время также можно установить вручную. Дата и время используются в журналах регистрации.
Журналы регистрации	Используйте журналы регистрации для поиска и устранения неисправностей. Устройство P660HN позволяет отправлять журналы на внешний сервер хранения системных журналов.
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.
Брандмауэр	В вашем устройстве реализован полнофункциональный брандмауэр с защитой от DoS (Denial of Service – Отказ в обслуживании). По умолчанию, когда брандмауэр включен, весь входящий трафик от глобальной вычислительной сети (WAN) к локальной (LAN) блокируется, если только он не инициируется локальной сетью (LAN). Брандмауэр контролирует TCP/UDP, распознает и предотвращает атаки DoS, посылает предупредительные сообщения и ведет регистрацию событий и сообщений.
Контент-фильтрование	Контент-фильтрование дает возможность блокировать доступ к веб-сайтам по определенным ключевым словам в URL. Можно составить график выполнения контент-фильтрования и предоставлять доверенным компьютерам локальной сети нефильтруемый доступ в Интернет по IP-адресам.
Качество услуги (QoS)	Для определенных типов трафика и определенных компьютеров вашей сети можно зарезервировать полосу пропускания и задать им приоритет для повышения эффективности управления исходящим трафиком.
Удаленное управление	Удаленное управление позволяет с помощью выбранной службы (например, HTTP или FTP) с компьютера в сети (LAN или WAN) подключиться к устройству P660HN.
Функция Any IP	Функция Any IP позволяет компьютеру получить доступ в Интернет и к настройкам устройства P660HN без изменения сетевых параметров компьютера (таких как IP-адрес и маска подсети), если IP-адреса компьютера и устройства P660HN находятся в разных подсетях.
Поддержка PPPoE (RFC2516)	PPPoE (Протокол «точка-точка» через Ethernet) эмулирует коммутируемое соединение. Он позволяет Интернет-провайдеру использовать существующую конфигурацию сети совместно с новейшими широкополосными технологиями, такими как ADSL. Драйвер PPPoE в вашем устройстве является «прозрачным» для компьютеров в локальной сети, которые работают только по Ethernet и не поддерживают протокол PPPoE, что устраняет необходимость настраивать PPPoE-клиенты на отдельных компьютерах.
Другие характеристики PPPoE	Время простоя PPPoE Предоставление канала по требованию PPPoE

Табл. 118 Характеристики микропрограммного обеспечения (продолжение)

Поддержка множества PVC (Permanent Virtual Circuits – Постоянные виртуальные каналы)	Ваше устройство поддерживает до 8 постоянных виртуальных каналов (PVC).
Псевдоним IP	Псевдоним IP позволяет разделить физическую сеть на несколько логических сетей с помощью одного интерфейса Ethernet. Ваше устройство поддерживает три логических интерфейса LAN через один физический интерфейс Ethernet, при этом само устройство выступает в качестве шлюза для каждой сети LAN.
Фильтры пакетов	Функции фильтрования пакетов вашего устройства позволяют повысить уровень защиты и управления сетью.
Стандарты ADSL	ANSI T1.413, изд. 2 G.dmt (G.992.1) ADSL2 G.dmt.bis (G.992.3) ADSL2+ (G.992.5) Расширенный ADSL (RE ADSL) SRA (Seamless Rate Adaptation – Плавная регулировка скорости передачи) Адаптация с автоматическим выбором скорости передачи Физическое подключение ADSL ATM AAL5 (5-й уровень адаптации ATM) Подключение по нескольким протоколам через AAL5 (RFC2684/1483) PPP через ATM AAL5 (RFC2364) PPP через Ethernet для DSL-подключения (RFC2516) Мультиплексирование на базе VC и LLC I.610 F4/F5 OAM Annex L/M TR-067/TR-100
Поддержка других протоколов	Протокол канального уровня PPP (Point-to-Point Protocol – Протокол «точка-точка») Маршрутизация IP Прозрачная передача протоколов для неподдерживаемых протоколов сетевого уровня RIP I/RIP II ICMP ATM QoS SNMP v1 и v2c с поддержкой MIB II (RFC 1213) Многоадресная рассылка IP IGMP v1, v2 и v3 Proxy-сервер IGMP 802.1Q/1P
Управление	Программа ZyXEL NetFriend Встроенный Web-конфигуратор CLI (Интерпретатор командной строки) SNMP v1 & v2c с MIB II Встроенный сервер FTP/TFTP для обновления микропрограммного обеспечения, а также обновления и восстановления файла конфигурации Удаленное управление: Telnet, FTP, Web, SNMP и DNS Удаленное обновление микропрограммного обеспечения Системный журнал TR-069 F4/F5 OAM

22.3 Беспроводные функции

Табл. 119 Беспроводные функции

Внешняя антенна	Устройство P660HN оборудовано внешними антеннами, обеспечивающими четкую передачу радиосигнала между беспроводными устройствами и точками доступа.
Фильтрование MAC-адресов: для беспроводной сети	Устройство может проверять MAC-адреса базы данных настроек пользователя согласно списку допущенных или отвергнутых MAC-адресов.
WEP-шифрование	WEP (Конфиденциальность, равная конфиденциальности в проводных сетях) кодирует пакеты данные до их передачи через беспроводную сеть для обеспечения соблюдения конфиденциальности связи в сети.
Защищенный доступ Wi-Fi (WPA)	Защищенный доступ Wi-Fi (WPA) представляет собой подкласс стандарта безопасности IEEE 802.11i. Основные различия между WPA и WEP заключаются в применении аутентификации пользователя и усовершенствованном шифровании данных.
WPA2	WPA2 представляет собой стандарт безопасности беспроводной связи, обеспечивающий более защищенные по сравнению с WPA методы шифрования, аутентификации и управления ключами.
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.
Другие беспроводные функции	Соответствует стандарту IEEE 802.11n Диапазон частот: 2,4 ГГц ISM Band (промышленный, научный и медицинский диапазон) Автоматический выбор канала Расширенное ортогональное мультиплексирование с разделением частот (OFDM). Скорость передачи данных: 54 Мбит/с, 11 Мбит/с, 5,5 Мбит/с, 2 Мбит/с и 1 Мбит/с с автоматическим понижением скорости WPA2 WMM IEEE 802.11i IEEE 802.11e WEP-шифрование 64/128/256 бит (Wired Equivalent Privacy – Конфиденциальность, равная конфиденциальности в проводных сетях) Мост WLAN–LAN До 32 фильтров MAC-адресов IEEE 802.1x Возможность сохранения до 32 пользовательских профилей с помощью EAP-MD5 (встроенная база данных пользователей) Внешний сервер RADIUS, использующий EAP-MD5, TLS, TTLS График работы беспроводной сети

Далее приводится неполный список стандартов, поддерживаемых устройством P660HN.

Табл. 120 Стандарты, поддерживаемые устройством

СТАНДАРТ	ОПИСАНИЕ
RFC 867	Daytime Protocol
RFC 868	Time Protocol
RFC 1058	RIP-1: Routing Information Protocol – Протокол обмена информацией о маршрутизации
RFC 1112	IGMP v1: Internet Group Management Protocol – Межсетевой протокол управления группами (версия 1)
RFC 1157	SNMPv1: Simple Network Management Protocol – Простой протокол управления сетью (версия 1)
RFC 1305	NTPv3: Network Time Protocol — Протокол сетевого времени (версия 3)
RFC 1441	SNMPv2: Simple Network Management Protocol – Простой протокол управления сетью (версия 2)
RFC 1483	Многопротокольная инкапсуляция поверх адаптации ATM, уровень 5
RFC 1631	NAT – Трансляция сетевых IP-адресов
RFC 1661	PPP – Протокол «точка-точка»
RFC 1723	RIP-2: Routing Information Protocol – Протокол обмена информацией о маршрутизации
RFC 1901	SNMPv2c: Simple Network Management Protocol – Простой протокол управления сетью (версия 2c)
RFC 2236	IGMPv2: Internet Group Management Protocol – Межсетевой протокол управления группами (версия 2)
RFC 2364	Протокол «точка-точка» поверх уровня адаптации AAL5 (PPP через ATM через ADSL)
RFC 2408	ISAKMP: Протокол Интернет-безопасности и протокол управления ключами
RFC 2516	PPPoE: Метод передачи от точки к точке через сеть Интернет
RFC 2684	Многопротокольная инкапсуляция поверх адаптации ATM, уровень 5.
RFC 2766	NAT: Протокол трансляции сетевых адресов
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 ГГц
IEEE 802.11g	Использует диапазон частот 2,4 ГГц
IEEE 802.11d	Стандарты локальных сетей и сетей уровня города: мосты протокола управления доступом к среде передачи (MAC)
IEEE 802.11x	Контроль доступа в сеть через порты.
IEEE 802.11e QoS	Стандарт беспроводной локальной связи IEEE 802.11 e для качества обслуживания
ANSI T1.413, изд. 2	ADSL: Стандарт асимметричной цифровой абонентской линии
G dmt (G.992.1)	G.992.1 ADSL: Трансиверы стандарта асимметричной цифровой абонентской линии G.992.1
ITU G.992.1 (G.DMT)	Стандарт международного союза по электросвязи для ADSL с использованием цифровой многоканальной тональной модуляции.

Табл. 120 Стандарты, поддерживаемые устройством (продолжение)

СТАНДАРТ	ОПИСАНИЕ
ITU G.992.2 (G. Lite)	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 ADSL2), разрешающий более высокие скорости передачи данных, чем ADSL.
ITU G.992.4 (G.lite.bis)	Стандарт международного союза по электросвязи (также называемый ADSL2), разрешающий более высокие скорости передачи данных, чем ADSL.
ITU G.992.5 (ADSL2+)	Стандарт международного союза по электросвязи (также называемый ADSL2+), обеспечивающий вдвое количество входящих битов.
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)

22.4 Характеристики адаптера питания

Табл. 121 Устройство P660HN: характеристики последовательного адаптера питания

Модель адаптера питания переменного тока	
Входное питание	Перем. ток 230 В/50 Гц
Выходная мощность	Пост. ток 12 В/1,0 А
Потребляемая мощность	Макс. 8,3 Вт
Нормы техники безопасности	CE, GS или TUV, EN60950-1

23

Поиск и устранение неисправностей

В этой главе рассказывается об устранении возможных неисправностей, которые могут появиться при работе с устройством. Возможные неисправности можно разделить на следующие категории:

- Питание, подключение оборудования и светодиоды
- Доступ и регистрация в системе устройства P660HN
- Доступ в Интернет

23.1 Питание, подключение оборудования и светодиоды

? Устройство P660HN не включается. Ни один из светодиодов не светится.

1. Убедитесь, что устройство P660HN включено.
2. Убедитесь, что используется адаптер или кабель питания из комплекта поставки устройства P660HN.
3. Убедитесь, что адаптер или кабель питания подключен к устройству P660HN и к соответствующему источнику питания. Убедитесь, что источник питания включен.
4. Выключите и снова включите устройство P660HN.
5. Если неисправность не устранена, обратитесь к поставщику оборудования.

? Один из светодиодов работает неправильно.

1. Убедитесь, что вы знаете, как светодиод должен работать в нормальном режиме. См. Разд. 1.5 на с. 30.
2. Проверьте подключение оборудования. См. Инструкцию по применению.
3. Убедитесь, что кабели не повреждены. Для замены поврежденных кабелей свяжитесь с поставщиком оборудования.
4. Выключите и снова включите устройство P660HN.
5. Если неисправность не устранена, обратитесь к поставщику оборудования.

23.2 Доступ и регистрация в системе устройства P660HN

Потеряна информация об IP-адресе устройства P660HN.

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 устройства P660HN, установленный для шлюза по умолчанию на компьютере. Чтобы выполнить это на компьютере под управлением Windows, нажмите кнопку **Start > Run**, введите команду **cmd** и затем **ipconfig**. IP-адрес **Default Gateway** может являться IP-адресом устройства P660HN (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. 1.6 на с. 31.

Утерян пароль.

1. Пароль администратора по умолчанию – **1234**, пароль пользователя по умолчанию – **user**.
2. Если эти пароли не работают, выполните сброс параметров устройства к заводским настройкам по умолчанию. См. Разд. 1.6 на с. 31.

Не отображается окно Web-конфигуратора **Login** 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. 5.2 на с. 73), 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 устройства P660HN.
2. Проверьте подключение оборудования и удостоверьтесь, что светодиоды работают в нормальном режиме. См. Инструкцию по применению.
3. Убедитесь, что Интернет-браузер не блокирует всплывающие окна и обеспечивает поддержку JavaScripts и Java. См. Прил. B на с. 325.

4 Если функция **Any IP** (Разд. 5.6.7 на с. 85) отключена, проверьте, что компьютер находится в той же подсети, что и устройство P660HN. (Пропустите этот шаг, если известно, что между компьютером и устройством P660HN имеются маршрутизаторы.)
   - Если в вашей сети есть сервер DHCP, убедитесь, что ваш компьютер использует динамический IP-адрес. См. Прил. A на с. 309. По умолчанию устройство P660HN выполняет функцию DHCP-сервера.
   - Если в вашей сети нет другого сервера DHCP, убедитесь, что IP-адреса компьютеров входят в ту же подсеть, что и устройство P660HN. См. Прил. A на с. 309.
5 Выполните сброс параметров устройства к заводским настройкам по умолчанию и попробуйте получить доступ к устройству P660HN с IP-адресом по умолчанию. См. Разд. 1.6 на с. 31.
6 Если неисправность не устранена, обратитесь к сетевому администратору или поставщику оборудования или последуйте дополнительным рекомендациям.

Дополнительные рекомендации

- Попробуйте получить доступ к устройству P660HN с использованием другой службы, например, Telnet. Если доступ к устройству P660HN существует, проверьте параметры удаленного управления и правила брандмауэра, чтобы выяснить причину, по которой устройство P660HN не отвечает по HTTP.
- Если ваш компьютер не подключен к порту **WAN** или подключен по беспроводной связи, используйте компьютер, подключенный к порту **ETHERNET**.

? Экран **Login** отображается, но невозможно выполнить вход в систему устройства P660HN.

1 Убедитесь, что пароль введен правильно. Пароль администратора по умолчанию – **1234**, пароль пользователя по умолчанию – **user**. Символы в это поле вводятся с учетом регистра, поэтому убедитесь, что кнопка [Caps Lock] выключена.
2 Нельзя получить доступ к Web-конфигуратору, если другой пользователь подключился к устройству P660HN через Telnet. Подключитесь к устройству P660HN позднее или попросите зарегистрированного пользователя выполнить выход из системы.
3 Выключите и снова включите устройство P660HN.
4 Если это не поможет, выполните сброс параметров устройства к заводским настройкам по умолчанию. См. Разд. 23.1 на с. 303.

? Невозможно подключиться к устройству P660HN через Telnet.

См. рекомендации по поиску и устранению неисправностей в разделе Не отображается окно Web-конфигуратора Login 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 микропрограммного обеспечения с помощью FTP.

См. рекомендации по поиску и устранению неисправностей в разделе Не отображается окно Web-конфигуратора Login 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. Инструкцию по применению и Разд. 1.5 на с. 30.
2. Проверьте правильность ввода параметров учетной записи, предоставленных Интернет-провайдером. Символы в эти поля вводятся с учетом регистра, поэтому убедитесь, что кнопка [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 Инструкции по применению.
5. Если неисправность не устранена, обратитесь к Интернет-провайдеру.

Невозможно получить доступ в Интернет. Доступ в Интернет настроен через устройство P660HN, но подключение к Интернет больше не работает.

1. Проверьте подключение оборудования и удостоверьтесь, что светодиоды работают в нормальном режиме. См. Инструкцию по применению и Разд. 1.5 на с. 30.
2. Выключите и снова включите устройство P660HN.
3. Если неисправность не устранена, обратитесь к Интернет-провайдеру.

Подключение к сети Интернет работает медленно или нестабильно.

1. Возможно, что локальная сеть перегружена. Посмотрите на светодиоды и проверьте их работу согласно Разд. 1.5 на с. 30. Если устройство P660HN посылает и передает большие объемы информации, закройте программы, которые используют Интернет, особенно одноранговые приложения.
2. Проверьте уровень сигнала. Если сигнал слабый, переместите свой компьютер ближе к устройству P660HN, если это возможно, и обратите внимание на устройства, которые могут создавать помехи беспроводной сети (например, микроволновые печи, другие беспроводные сети и т. д.).
3. Выключите и снова включите устройство P660HN.
4. Если неисправность не устранена, обратитесь к сетевому администратору или поставщику оборудования или выполните дополнительные рекомендации.

Дополнительные рекомендации

- Проверьте настройки качества обслуживания (QoS). Если управление отключено, попробуйте его включить. Если включено, можно попробовать повысить или понизить приоритет для некоторых приложений.

Часть VII Приложения и алфавитный указатель

В приложениях приводится общая информация. Описание некоторых деталей может не относиться к вашему устройству ZyXEL.

A

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. 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.

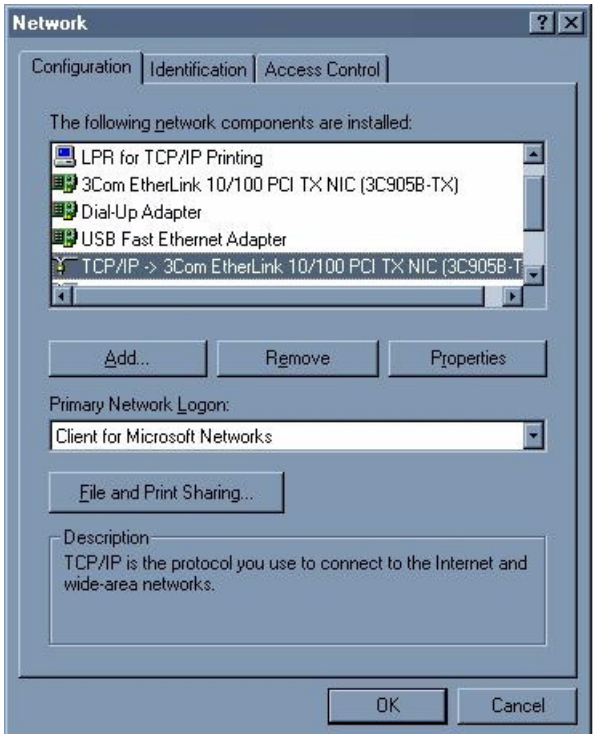
После установки компонентов TCP/IP, настройте параметры TCP/IP для соединения с сетью.

Если параметры IP назначаются вручную вместо динамического назначения, убедитесь, что ваши компьютеры имеют IP-адреса, относящиеся к той же подсети, что и порт LAN интернет-центра.

Windows 95/98/Me

Нажмите **Start (Пуск)**, **Settings (Настройка)**, **Control Panel (Панель управления)** и дважды щелкните по значку **Network (Сеть)**, чтобы открыть окно **Network**.

Рис. 169 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 плату:

1. В окне **Network (Сеть)** нажмите **Add (Добавить)**.
2. Выберите **Adapter (Сетевая плата)** и нажмите **Add (Добавить)**.
3. Выберите производителя и модель вашей сетевой платы 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**.

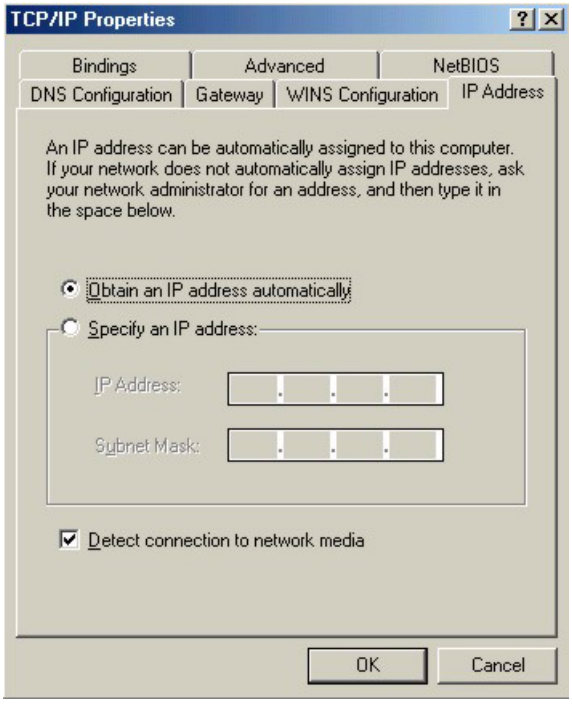
Если необходимо установить Клиента для сетей Microsoft:

1. Нажмите кнопку **Add (Добавить)**.
2. Выберите **Client (Клиент)** и нажмите кнопку **Add (Добавить)**.
3. Выберите **«Microsoft»** из списка производителей.
4. Выберите **Client for Microsoft Networks (Клиент для сетей Microsoft)** из списка сетевых клиентов и нажмите кнопку **OK**.
5. Перезагрузите компьютер, чтобы произведенные изменения вступили в силу.

Настройка

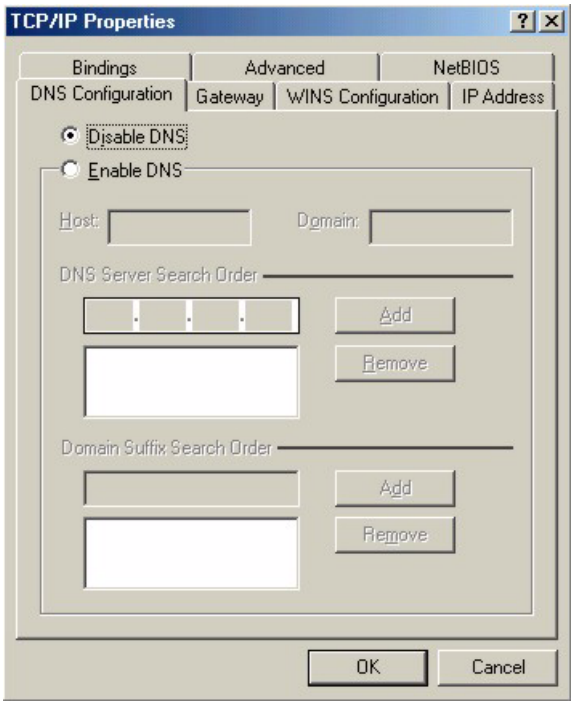
1. В окне **Network (Сеть)** выберите закладку **Configuration (Конфигурация)**, выберите пункт TCP/IP для вашей сетевой платы и нажмите **Properties (Свойства)**.
2. Выберите закладку **IP-адрес**.
   - Если вы используете динамический IP-адрес, выберите **Obtain an IP address automatically (Получить 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. 170 Windows 95/98/Me: Свойства протокола 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. 171 Windows 95/98/Me: Свойства протокола 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 интернет-центр и перезагрузите компьютер при появлении запроса.

Проверка настроек

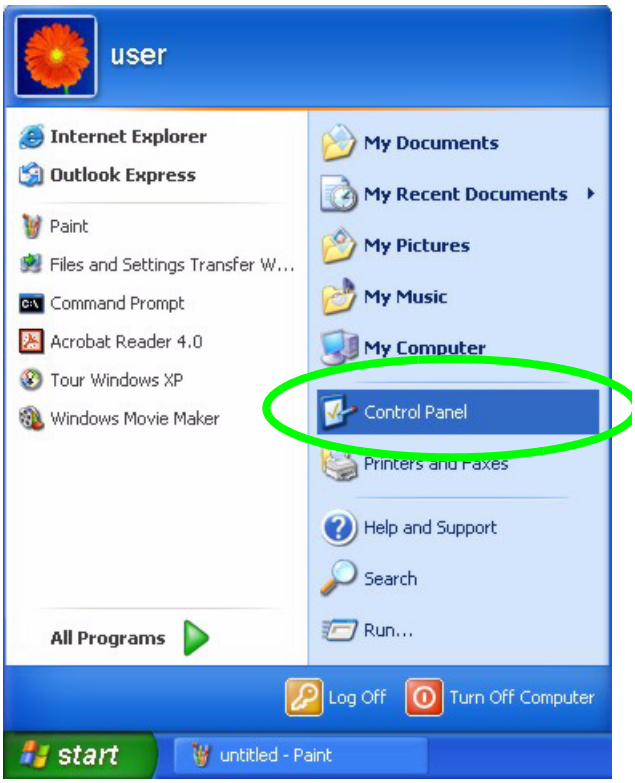
1 Нажмите кнопку **Start (Пуск)**, а затем выберите пункт **Run (Выполнить)**.
2 В окне **Run (Выполнить)** введите команду «winipcfg», а затем нажмите **OK** для отображения окна **IP Configuration (Конфигурация IP)**.
3 Выберите свой сетевой адаптер. При этом должны отображаться IP-адрес и маска подсети вашего компьютера, а также шлюз по умолчанию.

Windows 2000/NT/XP

В следующих рисунках 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. 172 Windows XP: Меню Пуск

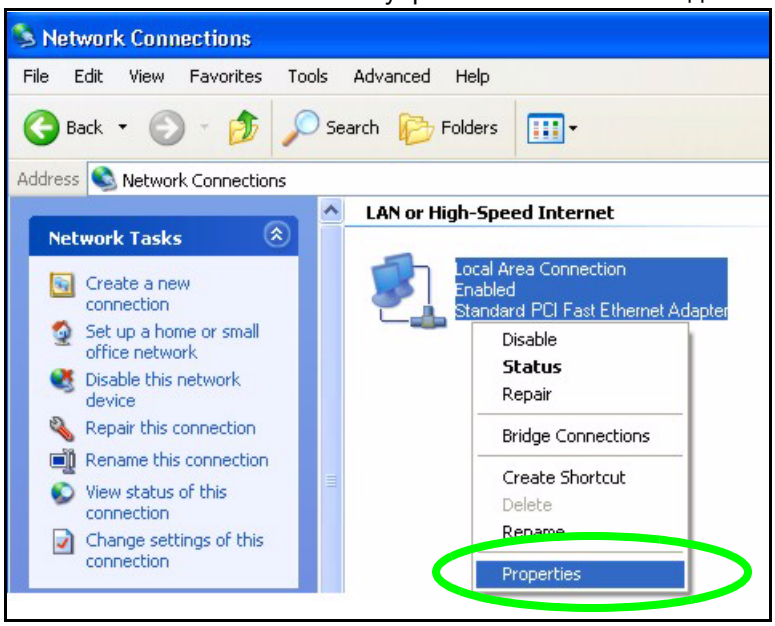


2 На **Панели управления** дважды щелкните **Network Connections (Сетевые подключения)** (**Network and Dial-up Connections (Сеть и удаленный доступ к сети)** в Windows 2000/NT).

Рис. 173 Windows XP: Control Panel (Windows XP: Панель управления)

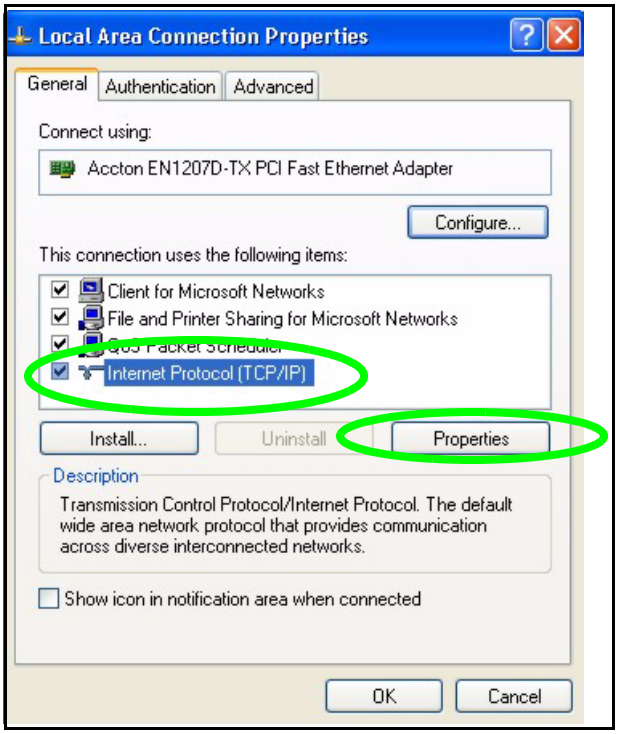
3 Щелкните правой кнопкой мыши значок **Local Area Connection (Подключение по локальной сети)** и выберите **Properties (Свойства)**.

Рис. 174 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)**.

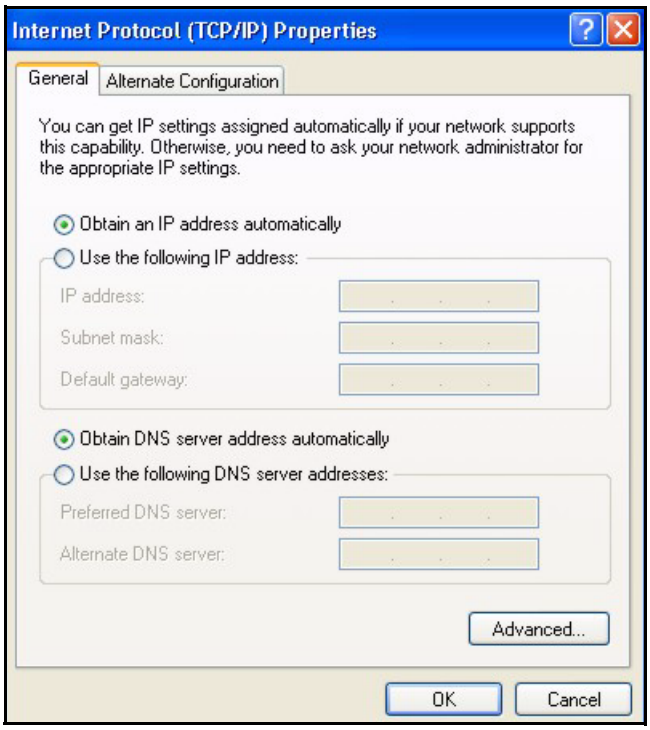
Рис. 175 Windows XP: Подключение по локальной сети: Свойства



5 Откроется 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. 176 Windows XP: Свойства: Протокол Интернета (TCP/IP)



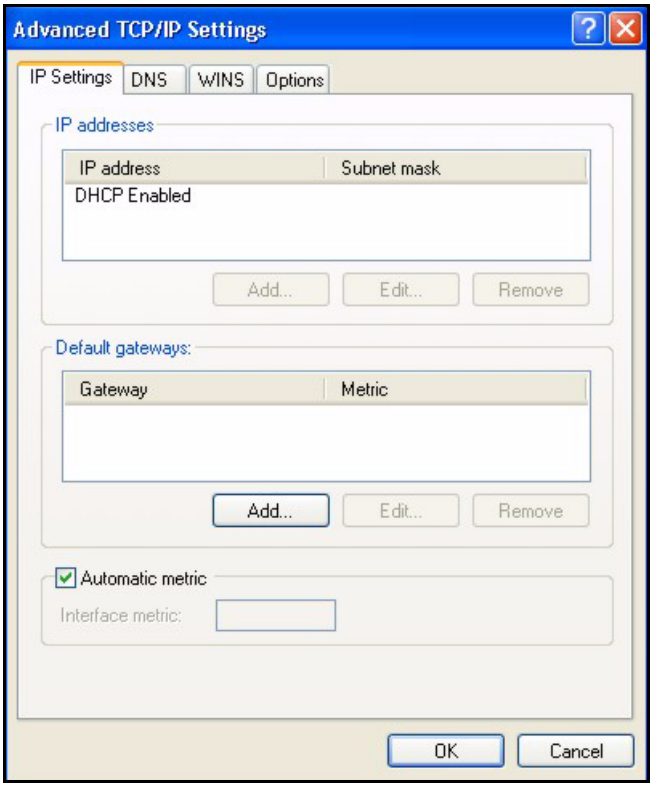
6 Если вы не знаете IP-адрес шлюза, удалите все предварительно настроенные шлюзы на закладке **IP Settings (Параметры IP)** и нажмите **OK**.

Для настройки дополнительных IP-адресов выполните следующие действия:

- На закладке **IP Settings (Параметры IP)** в поле для IP-адресов нажмите **Add (Добавить)**.
- В окне **TCP/IP Address (Адрес TCP/IP)** введите IP-адрес в поле **IP address (IP-адрес)** и маску подсети в поле **Subnet mask (Маска подсети)**, затем нажмите кнопку **Add (Добавить)**.
- 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.
- По завершении настройки нажмите кнопку **OK**.

Рис. 177 Windows XP: Дополнительные свойства TCP/IP

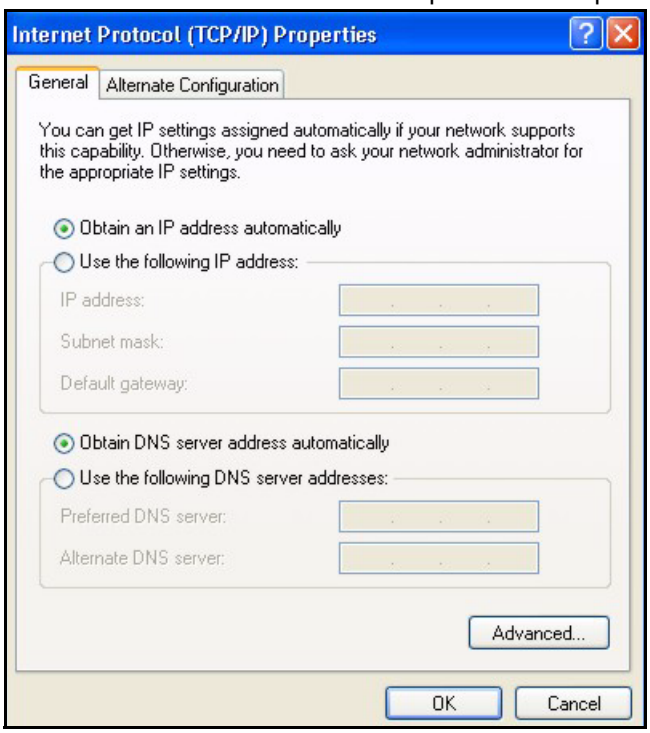


7 В окне **Internet Protocol TCP/IP Properties (Свойства: Протокол Интернета (TCP/IP))** на закладке **General (Общие)** в Windows XP:

- 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. 178 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 кнопку **Close (Закрыть)** (**OK** в Windows 2000/NT), чтобы закрыть окно **Local Area Connection Properties (Свойства подключения по локальной сети)**.

10 Закройте окно **Network Connections (Сетевые подключения)** (**Network and Dial-up Connections (Сеть и удаленный доступ к сети)** в Windows 2000/NT).

11 Включите интернет-центр и перезагрузите компьютер при появлении запроса.

Проверка настроек

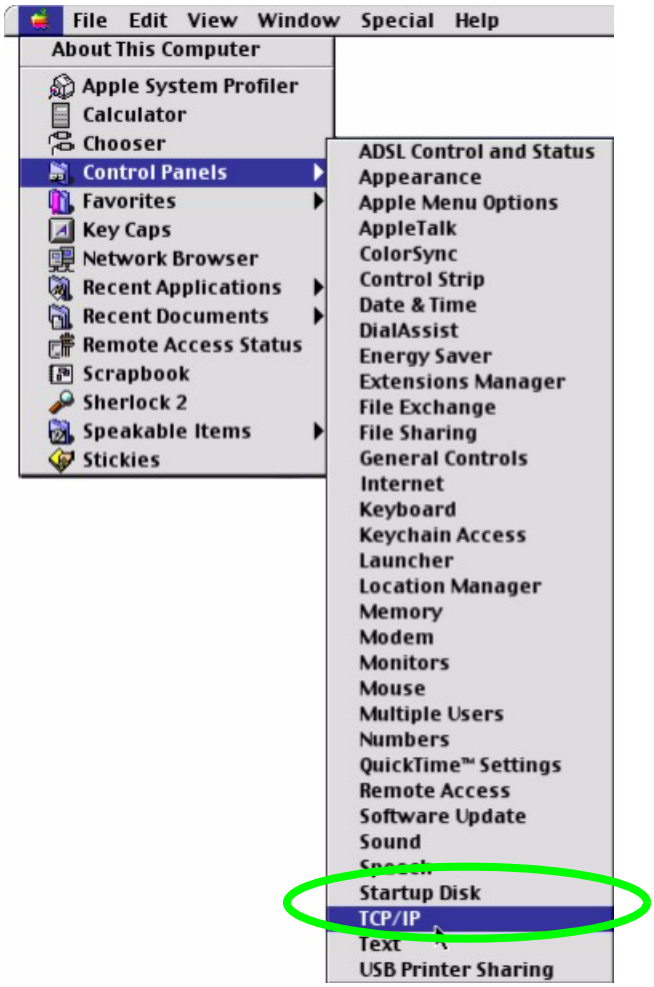
1 Щелкните **Start (Пуск), All Programs (Все программы), Accessories (Стандартные)**, а затем **Command Prompt (Командная строка)**.

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

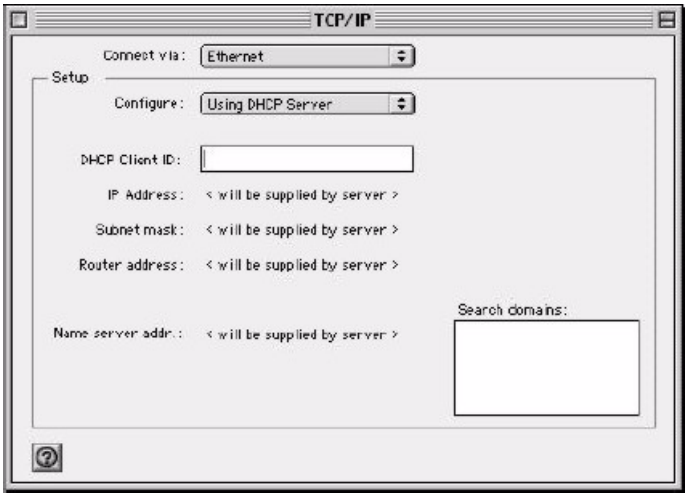
1 Нажмите кнопку меню **Apple**, выберите **Control Panel (Панель управления)**, а затем дважды щелкните **TCP/IP**, чтобы открыть **TCP/IP Control Panel (Панель управления TCP/IP)**.

Рис. 179 Macintosh OS 8/9: Меню Apple



2 Выберите **Ethernet built-in (Встроенный сетевой контроллер)** из списка **Connect via (Подключение через...)**.

Рис. 180 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 интернет-центра в поле **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 интернет-центр и перезагрузите компьютер при появлении запроса.

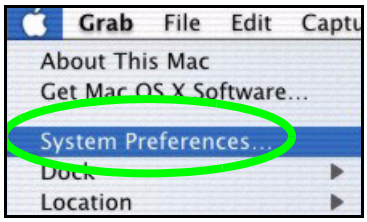
Проверка настроек

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)**.

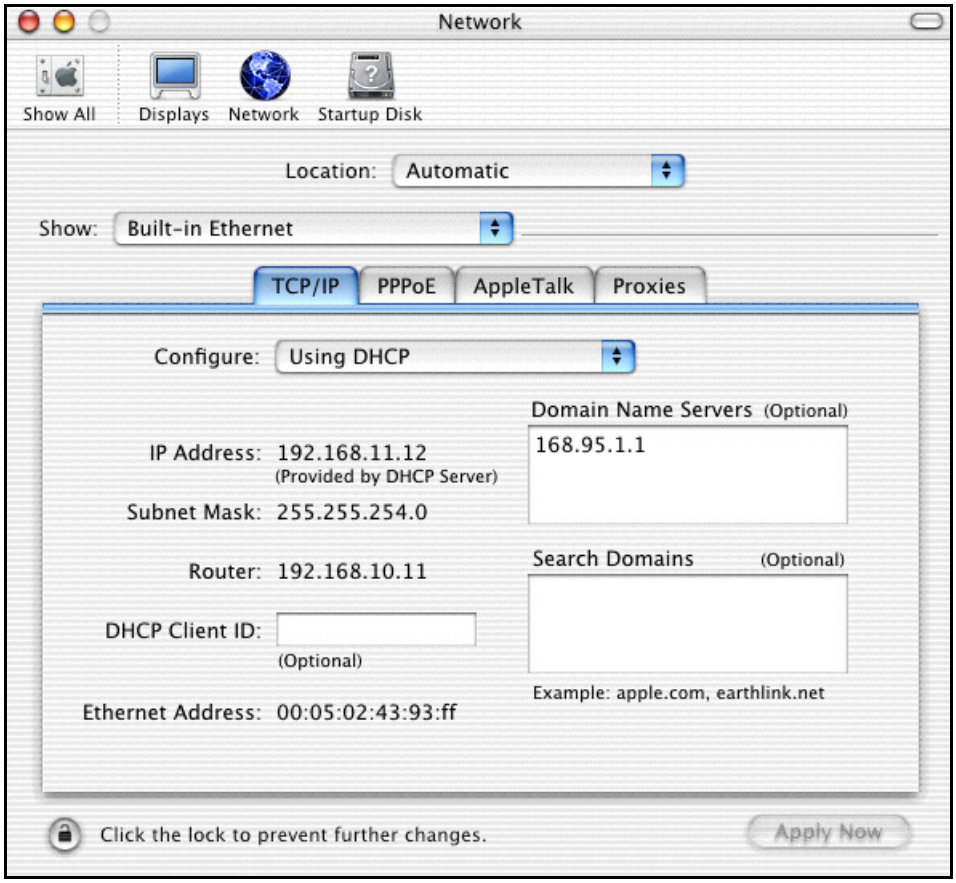
Рис. 181 Macintosh OS X: Меню Apple



2 Нажмите **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 настройки динамических параметров выберите **Using DHCP (Использовать DHCP)** в списке **Configure (Настроить)**.

Рис. 182 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 интернет-центра в поле **Router address (Адрес маршрутизатора)**.

5 Нажмите **Apply Now (Применить)** и закройте окно.

6 Включите интернет-центр 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.

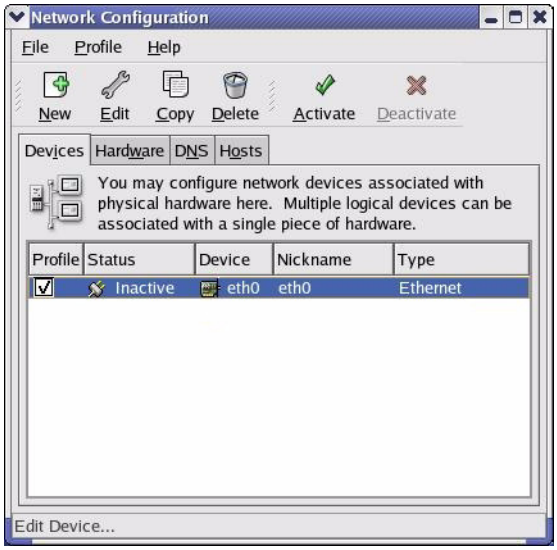
Вы должны быть зарегистрированы в системе в качестве корневого администратора.

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. 183 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)**.

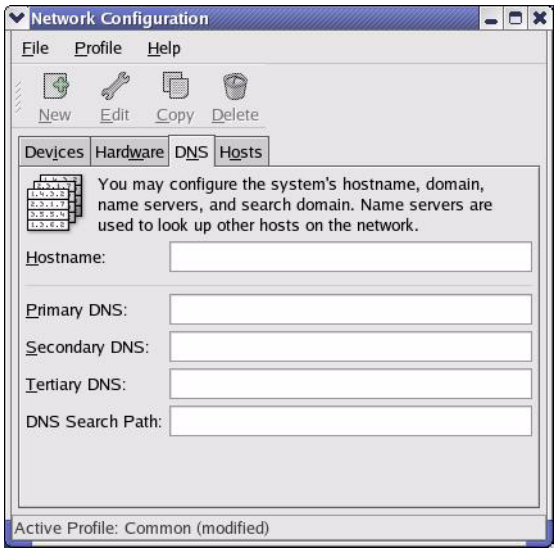
Рис. 184 Red Hat 9.0: KDE: Устройство Ethernet: Общие

- 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**.

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.

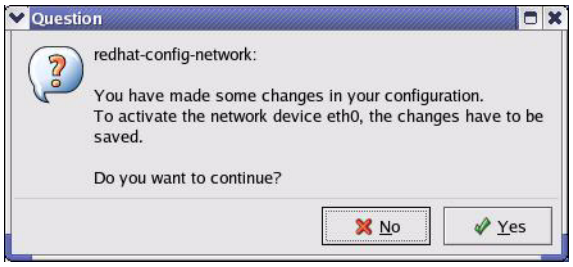
Рис. 185 Red Hat 9.0: KDE: Конфигурация сети: DNS



5 Выберите закладку **Devices (Устройства)**.

6 Нажмите кнопку **Activate (Активировать)** для вступления изменений в силу. Появится следующее окно. Нажмите **Да (Yes)**, чтобы сохранить изменения во всех окнах**.**

Рис. 186 Red Hat 9.0: KDE: Конфигурация сети: Включить



7 По завершении перезагрузки сетевой карты убедитесь, что **Status (Статус)** = **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. 187 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. 188 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. 189 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. 190 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]
```

23.3.1 Проверка настроек

Чтобы проверить настройки TCP/IP, введите «`ifconfig`» в окне терминала.

Рис. 191 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]#
```

B

Всплывающие окна, сценарии и разрешения Java

Чтобы воспользоваться веб-конфигуратором, необходимо включить следующие параметры:

- Инициированные модемом всплывающие окна в веб-браузере.
- Поддержка JavaScript (по умолчанию активирована).
- Разрешения Java (Java permissions) (по умолчанию активированы).

В настоящем руководстве использованы снимки экранов Internet Explorer 6. Экраны в других версиях Internet Explorer могут отличаться.

Блокирование всплывающих окон в Internet Explorer

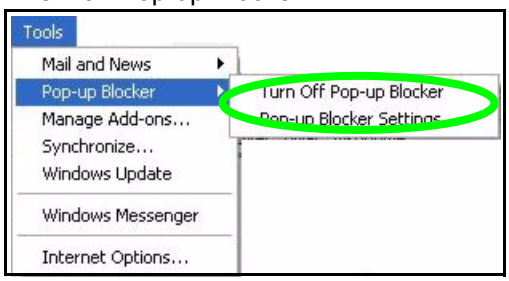
При регистрации пользователя устройства может возникнуть необходимость отключения блокирования всплывающих окон.

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)**, затем **Turn Off Pop-up Blocker (Выключить блокирование всплывающих окон)**

Рис. 192 Pop-up Blocker

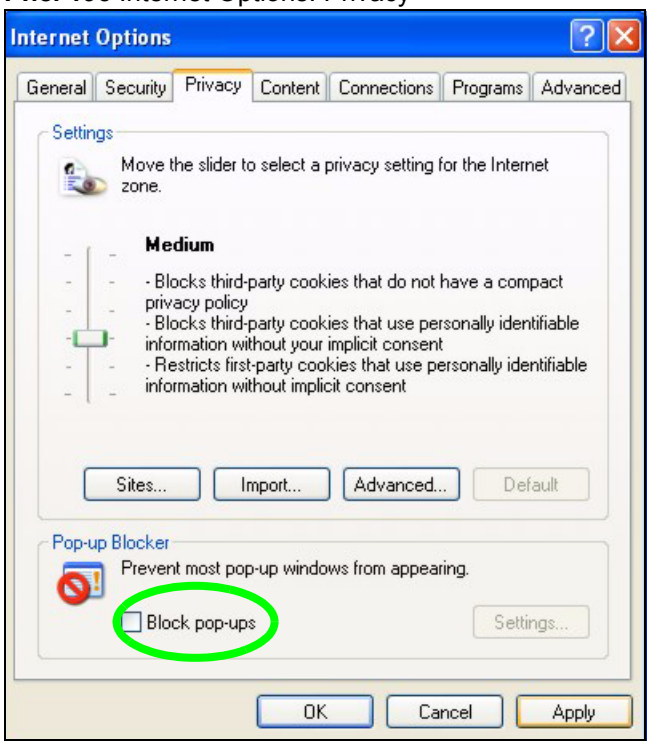


Вы также можете проверить, отключено ли блокирование всплывающих окон в разделе **Pop-up Blocker (Блокирование всплывающих окон)** на вкладке **Privacy (Конфиденциальность)**.

1 Откройте Internet Explorer, выберите пункт **Tools (Сервис)**, **Internet Options (Свойства обозревателя)**, **Privacy (Конфиденциальность)**.

2 Снимите флажок **Block pop-ups (Блокировать всплывающие окна)** в разделе **Pop-up Blocker (Блокирование всплывающих окон)** в нижней части окна. Это отключит блокирование всплывающих окон.

Рис. 193 Internet Options: Privacy



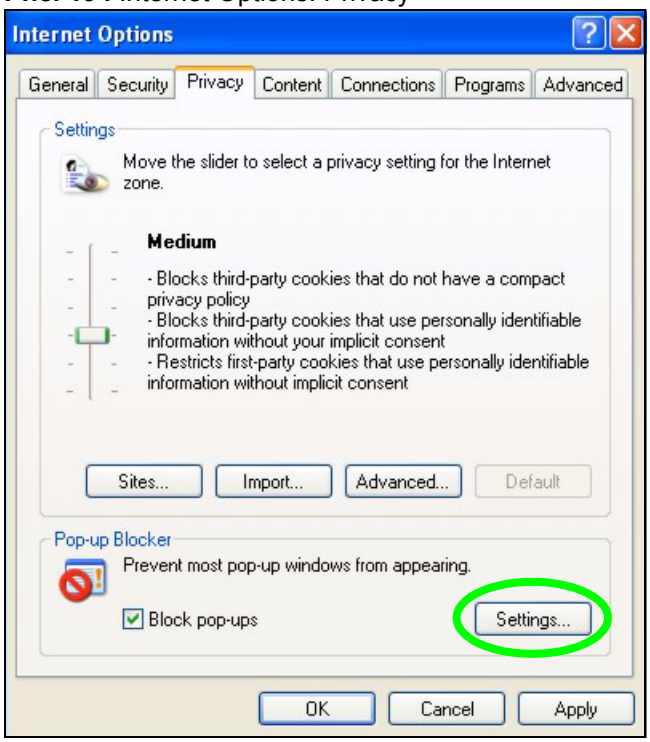
3 Нажмите **Apply (Применить)**, чтобы сохранить настройки.

Включение блокировки всплывающих окон с исключениями

Если же вы хотите, чтобы всплывающие окна были разрешены лишь на вашем устройстве, то можно сделать следующее.

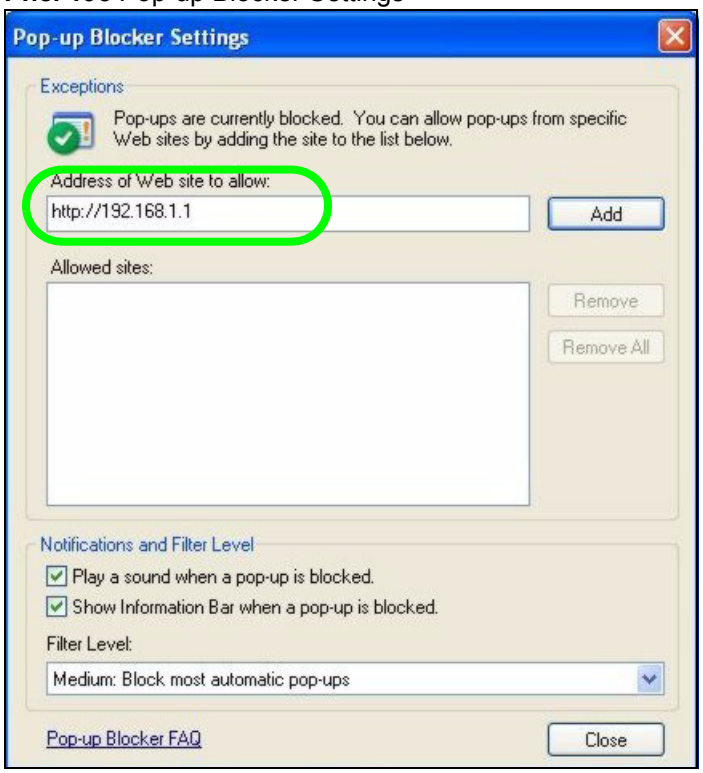
1. Откройте Internet Explorer, выберите пункт **Tools (Сервис)**, **Internet Options (Свойства обозревателя)**, **Privacy (Конфиденциальность)**.
2. Выберите **Settings… (Параметры...)** – откроется окно **Pop-up Blocker Settings (Параметры блокирования всплывающих окон)**.

Рис. 194 Internet Options: Privacy



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. 195 Pop-up Blocker Settings



5 Для возврата на вкладку **Privacy (Конфиденциальность)** нажмите кнопку **Close (Закрыть)**.

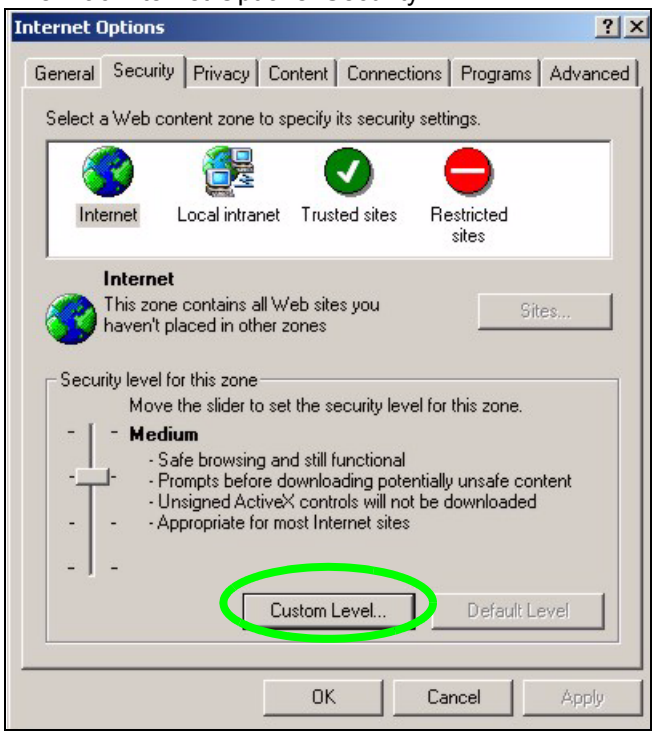
6 Нажмите кнопку **Apply (Применить)**, чтобы сохранить настройки.

Сценарии Java (JavaScripts)

Если страницы Web-конфигуратора отображаются в Internet Explorer некорректно, проверьте, разрешено ли использование сценариев Java.

1 Откройте Internet Explorer, выберите **Tools (Сервис)**, **Internet Options (Свойства обозревателя)** и закладку **Security (Безопасность)**.

Рис. 196 Internet Options: Security



2 Нажмите кнопку **Custom Level... (Другой...)**.

3 Пролистайте до раздела **Scripting (Сценарии)**.

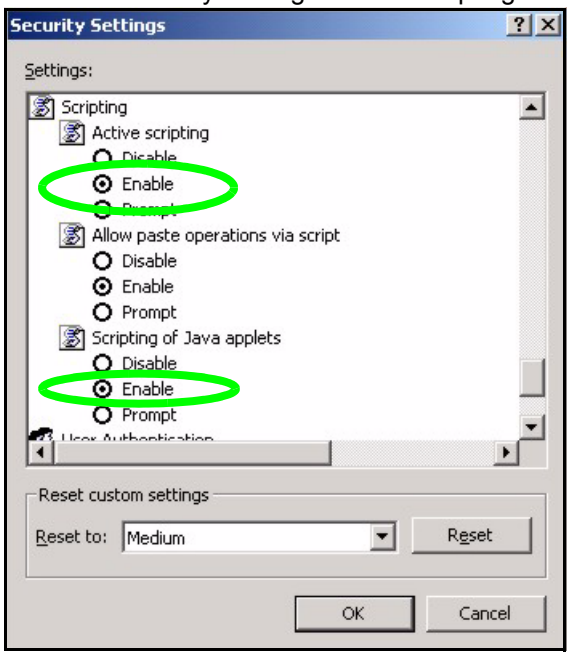
4 В разделе **Active scripting (Активные сценарии)** должно быть установлено **Enable (Разрешить)** (значение по умолчанию).

5 В разделе **Scripting of Java applets (Выполнять сценарии приложений Java)** также должно быть установлено **Enable (Разрешить)** (значение по умолчанию).

6 Нажмите кнопку **OK**, чтобы закрыть окно.

7 Нажмите **OK**, чтобы закрыть окно.

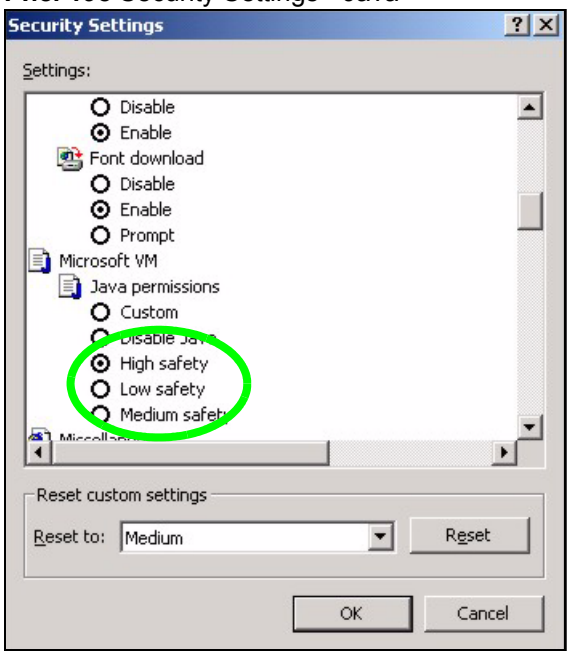
Рис. 197 Security Settings – Java Scripting



Разрешения Java

1. Откройте Internet Explorer, выберите **Tools (Сервис)**, **Internet Options (Свойства обозревателя)** и затем закладку **Security (Безопасность)**.
2. Нажмите кнопку **Custom Level... (Другой...)**.
3. Спуститесь вниз к разделу **Microsoft VM**.
4. В разделе **Java permissions (Разрешения Java)** выберите уровень безопасности.
5. Нажмите кнопку **OK**, чтобы закрыть окно.
6. Нажмите **OK**, чтобы закрыть окно.

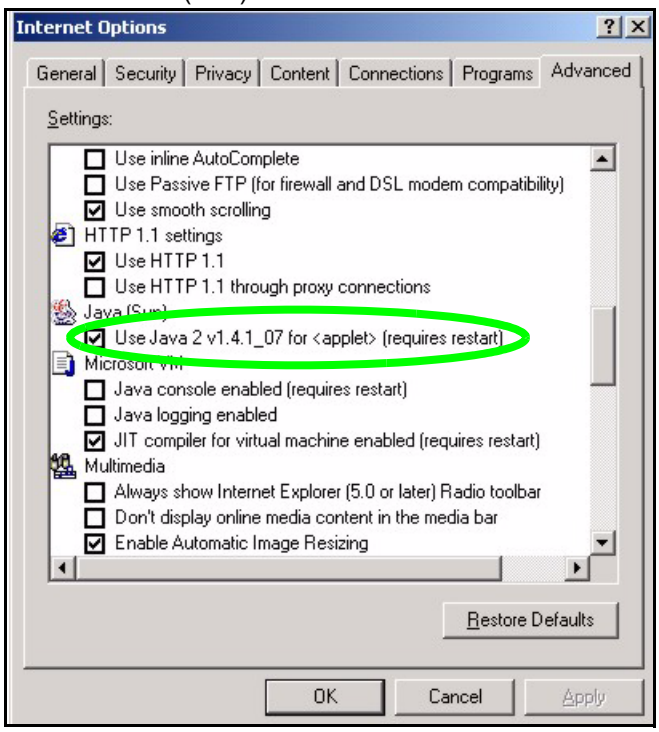
Рис. 198 Security Settings - Java



JAVA (Sun)

1. Откройте Internet Explorer, выберите **Tools (Сервис), Internet Options (Свойства обозревателя), Advanced (Дополнительно)**.
2. Убедитесь, в разделе **Java (Sun)** установлено **Use Java 2 for <applet> (Использовать Java 2 для приложения)**.
3. Нажмите кнопку **OK**, чтобы закрыть окно.
4. Нажмите **OK**, чтобы закрыть окно.

Рис. 199 Java (Sun)



C

IP-адреса и организация подсетей

В этом приложении представлена информация об IP-адресах, классах IP-адресов и масках подсети. Маски подсети используются для разделения сети на логические сети меньшего размера.

Описание IP-адресов

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.

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 255 в десятичном.)

Существует несколько классов IP-адресов. Первые три числа в адресе (в вышеприведенном примере 192) определяют класс IP-адреса. Классы определяются следующим образом:

- Класс A: от 0 до 127
- Класс B: от 128 до 191
- Класс C: от 192 до 223
- Класс D: от 224 до 239
- Класс E: от 240 до 255

Классы IP-адресов и 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. 122 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 (например, 192.168.1.0). IP-адрес, в котором идентификатор узла состоит только из единиц, является широковещательным адресом для данной сети (например, 192.168.1.255). 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. 123 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 00000000 до 01111111	от 0 до 127
Класс B	от 10000000 до 10111111	от 128 до 191
Класс C	от 11000000 до 11011111	от 192 до 223
Класс D	от 11100000 до 11101111	от 224 до 239
Класс E (зарезер-вированы)	от 11110000 до 11111111	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. 124 «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 единиц в начале и непрерывной последовательности нулей в оставшихся битах и имеет длину 32 бита, можно просто указывать количество единиц вместо того, чтобы записывать 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. 125 Альтернативные варианты записи маски подсети

МАСКА ПОДСЕТИ	МАСКА ПОДСЕТИ ПРИ ЗАПИСИ КОЛИЧЕСТВА ЕДИНИЦ	ЗНАЧЕНИЯ БИТОВ ПОСЛЕДНЕГО БАЙТА	В ДЕСЯТИЧ-НОМ ВИДЕ
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

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. 126 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. 127 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 циркулярной рассылки: 192.168.1.127	Максимальный идентификатор узла: 192.168.1.126	

Табл. 128 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 циркулярной 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. 129 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 циркулярной рассылки: 192.168.1.63	Максимальный идентификатор узла: 192.168.1.62	

Табл. 130 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
Адрес подсети: 192.168.1.64	Минимальный идентификатор узла: 192.168.1.65	
Адрес циркулярной рассылки: 192.168.1.127	Максимальный идентификатор узла: 192.168.1.126	

Табл. 131 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 циркулярной рассылки: 192.168.1.191	Максимальный идентификатор узла: 192.168.1.190	

Табл. 132 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 циркулярной рассылки: 192.168.1.255	Максимальный идентификатор узла: 192.168.1.254	

Пример: восемь подсетей

Аналогично используется 27-битная маска для создания 8 подсетей (000, 001, 010, 011, 100, 101110111).

В следующей таблице приведены значения битов последнего байта адреса класса C для каждой подсети.

Табл. 133 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. 134 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. 122 на с. 334) для организации подсетей.

В следующей таблице приведены сводные данные по организации подсетей класса B.

Табл. 135 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

D

Беспроводные локальные сети

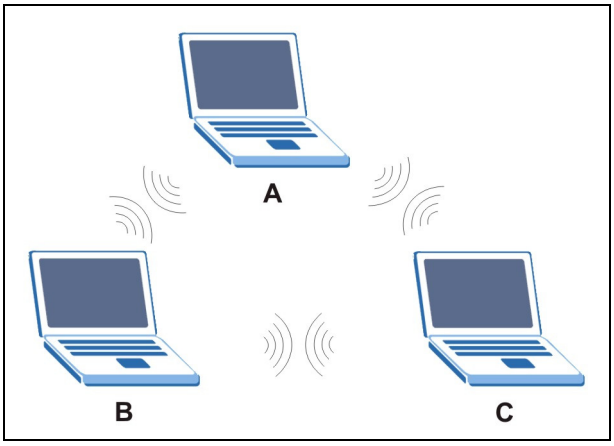
Топологии беспроводных локальных сетей

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 (временная) WLAN, объединяющая группу компьютеров с беспроводными устройствами (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. 200 Одноранговая связь во временной (Ad-hoc) беспроводной сети

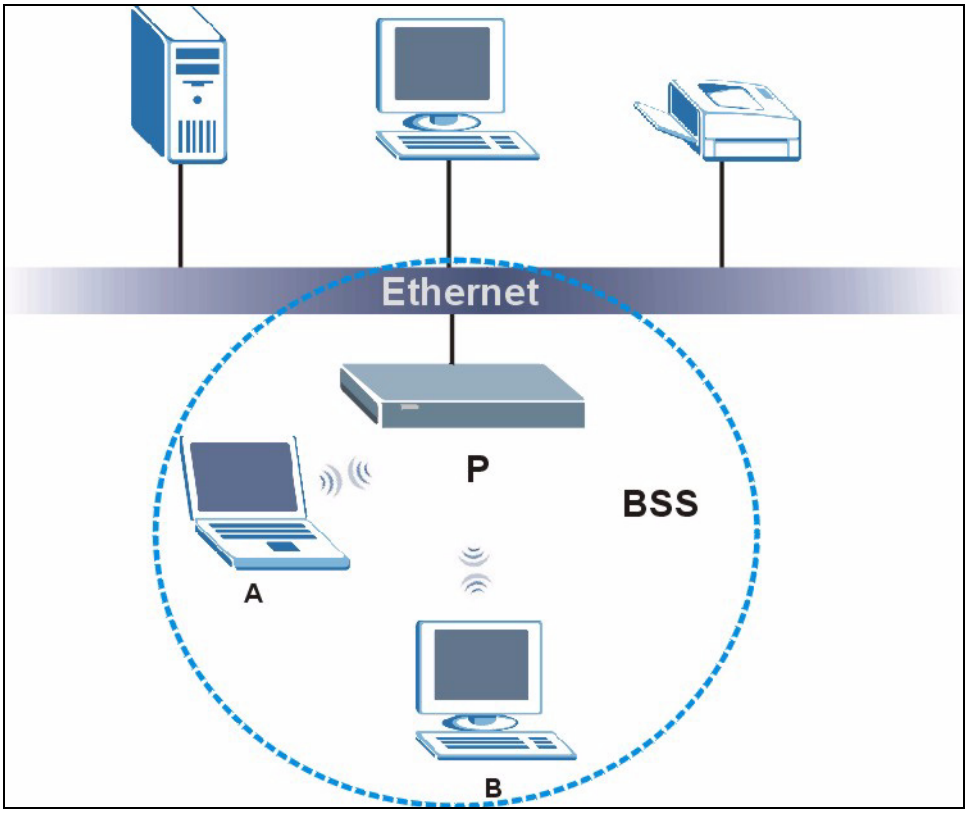


BSS (Базовый набор служб)

Базовый набор служб (BSS) существует тогда, когда весь трафик между беспроводными устройствами или между беспроводным устройством и клиентом проводной сети идет через одну точку доступа (AP).

Intra-BSS трафик – это трафик между беспроводными устройствами в пределах одного базового набора служб. При активации Intra-BSS трафика беспроводные устройства A и B могут получить доступ к проводной сети и обмениваться информацией между собой. При отключении Intra-BSS трафика беспроводные устройства A и B все равно могут получить доступ к проводной сети, однако не могут обмениваться информацией между собой.

Рис. 201 Базовый набор служб



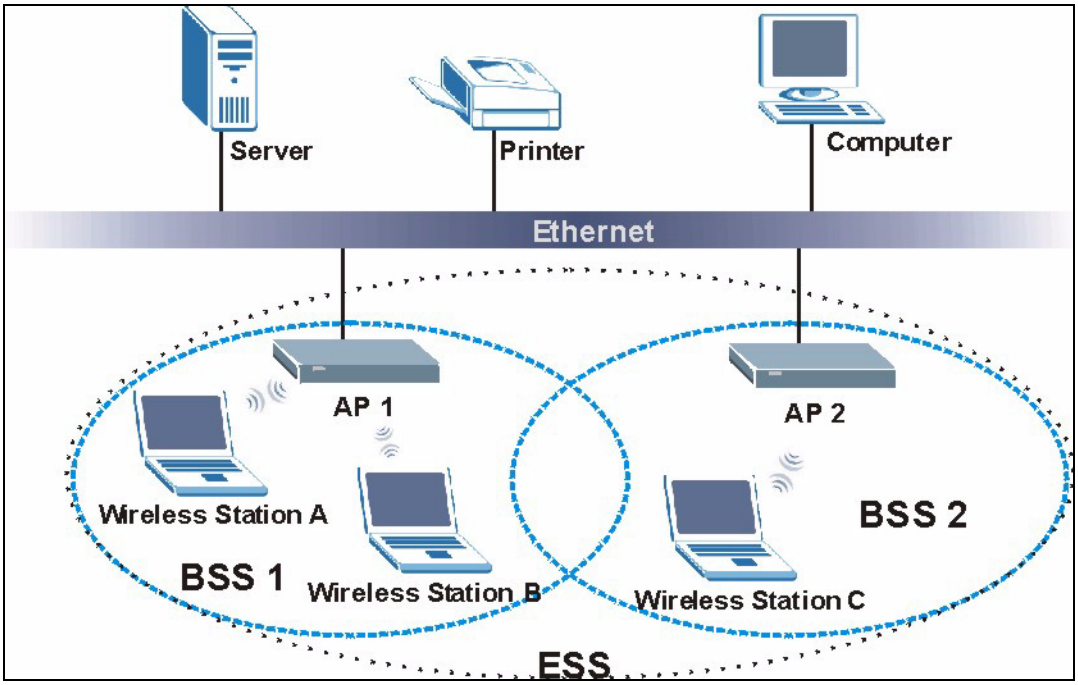
ESS (Расширенный набор служб)

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 устройства в одном ESS должны иметь одинаковый идентификатор ESS.

Рис. 202 Фиксированная беспроводная сеть



Канал

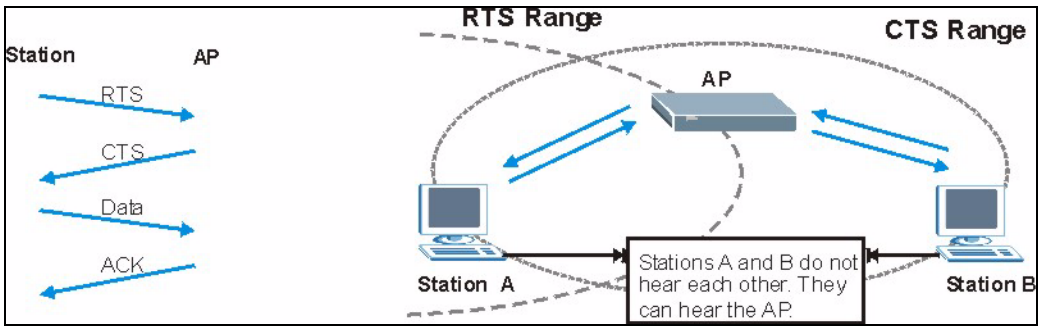
Канал представляет собой радиочастоту(ы), используемую(ые) беспроводными устройствами IEEE 802.11b/g. Доступность каналов зависит от географического положения. В некоторых регионах каналов может быть несколько, поэтому для снижения уровня помех следует использовать канал, отличающийся от канала ближайшей 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. 203 RTS/CTS



Когда устройство A посылает данные в точку доступа, оно может не знать, что устройство B уже использует 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 без 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, отправившего запрос, это сообщение одновременно подтверждает временные рамки, отведенные на передачу данных.

Кадры, меньше указанных в RTS/CTS, устройства могут посылать непосредственно в AP, без запроса на передачу.

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/CTS.

Если значение RTS/CTS превышает значение порога фрагментации (см. далее), квитирование RTS/CTS 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 (вводная часть) используется для синхронизации времени передачи в беспроводной сети. Существует 2 режима заголовка: длинный и короткий.

Режим «Short» (Короткий заголовок) требует меньше времени на обработку и минимизирует издержки, поэтому его следует использовать в хорошей беспроводной сети, если он поддерживается всеми беспроводными устройствами.

Режим «Long» (Длинный заголовок) следует выбрать в случае, если в сети высок уровень «шума» либо нет уверености относительно того, какой режим заголовков поддерживают используемые беспроводные устройства (все беспроводные адаптеры стандарта IEEE 802.11b должны поддерживать длинные заголовки). Однако не все беспроводные адаптеры поддерживают короткие заголовки. Используйте длинный заголовок, если вы не уверены, какой режим заголовков поддерживают беспроводные адаптеры. В этом случае будет гарантировано взаимопонимание между точкой доступа и беспроводными устройствами, и связь в сетях с высоким уровнем «шума» станет более надежной.

Выберите «Dynamic» (Динамический), чтобы точка доступа автоматически использовала короткий заголовок, если он поддерживается всеми беспроводными устройствами, и длинный заголовок в остальных случаях.

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. 136 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)

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 устройств.

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

В этом приложении рассматриваются несколько распространенных типов аутентификации: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP и LEAP.

Непосредственно используемый тип аутентификации зависит от сервера RADIUS и точки доступа. Подробную информацию можно получить у сетевого администратора.

EAP-MD5 (Алгоритм представления сообщения в краткой форме 5)

Аутентификация по методу MD5 – это простейший способ односторонней аутентификации. Сервер аутентификации отправляет беспроводному устройству запрос. Беспроводное устройство подтверждает знание пароля, для чего оно 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 устройствам для двусторонней аутентификации необходимы цифровые удостоверения. 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 влечет 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.

Dynamic WEP Key Exchange (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. 137 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 пароля	Отсутствует	Сильная	Сильная	Сильная	Средняя
Сложность применения	Простое	Сложное	Среднее	Среднее	Среднее
Защита персональных данных клиентского устройства	Нет	Нет	Да	Да	Нет

WPA(2)

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(2) от WEP заключаются в более совершенных методах шифрования данных и аутентификации пользователя.

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 (ключ сети 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-разрядные 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 устройствами. 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 в нем используется один, более легкий в использовании, постоянный буквенно-цифровой пароль для получения парного главного ключа, который применяется для генерирования уникальных временных ключей шифрования. 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 – Расширяемый протокол аутентификации) для аутентификации беспроводных устройств 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.

Обзор параметров безопасности

В этой таблице приведены прочие параметры безопасности, которые нужно настроить для каждого метода аутентификации/протокола управления ключами. MAC-адрес фильтров не зависит от конфигурации этих характеристик безопасности.

Табл. 138 Сравнительная таблица беспроводной безопасности

МЕТОД АУТЕНТИФИКАЦИИ/ ПРОТОКОЛ УПРАВЛЕНИЯ КЛЮЧАМИ	МЕТОД ШИФРОВАНИЯ	РУЧНОЙ ВВОД КЛЮЧА	IEEE 802.1X
Открытый	Отсутствует	Нет	Отключен
			Включен с динамическим ключом WEP
Открытый	WEP	Нет	Включен с динамическим ключом WEP
		Да	Включен с динамическим ключом WEP
		Да	Отключен
Коллективный	WEP	Нет	Включен с динамическим ключом WEP
		Да	Включен с динамическим ключом WEP
		Да	Отключен
WPA	TKIP/AES	Нет	Включен
WPA-PSK	TKIP/AES	Да	Отключен
WPA2	TKIP/AES	Нет	Включен
WPA2-PSK	TKIP/AES	Да	Отключен

E

Службы

23.3.2 Службы

В следующей таблице содержатся распространенные службы и связанные с ними протоколы и номера портов.

- **Имя**: короткое описательное имя службы. Можно использовать это имя или создать другое.
- **Протокол**: тип протокола IP, используемый для данной службы. Если используется **TCP/UDP**, то служба использует одинаковый с TCP и UDP номер порта. Если используется **User-defined**, параметр **Порт(ы)** является номером протокола IP, но не номером порта.
- **Порт(ы)**: данное значение зависит от значения параметра **Протокол**.
  - Если значение **Протокола** – **TCP**, **UDP**, или **TCP/UDP**, то это номер порта IP.
  - Если значение **Протокола** – **USER**, то это номер протокола IP.

Описание: краткое описание приложений, которые используют данную службу, или ситуации, в которых используется данная служба.

Табл. 139 Наиболее часто используемые службы

ИМЯ	ПРОТОКОЛ	ПОРТ(Ы)	ОПИСАНИЕ
AH (IPSEC_TUNNEL)	User-Defined	51	Эта служба используется протоколом туннелирования IPSEC AH (Заголовок аутентификации).
AIM	TCP	5190	Служба Internet Messenger AOL.
AUTH	TCP	113	Протокол аутентификации, используется некоторыми серверами.
BGP	TCP	179	Протокол пограничного шлюза.
BOOTP_CLIENT	udp	68	Клиент DHCP.
BOOTP_SERVER	udp	67	Сервер DHCP.
CU-SEEME	TCP/UDP TCP/UDP	7648 24032	Популярное решение для проведения видеоконференций от White Pines Software.
DNS	TCP/UDP	53	Сервер имен доменов – служба, определяющая соответствие веб-имен (например, www.zyxel.com) и номеров IP.

Табл. 139 Наиболее часто используемые службы (продолжение)

ИМЯ	ПРОТОКОЛ	ПОРТ(Ы)	ОПИСАНИЕ
ESP (IPSEC_TUNNEL)	User-Defined	50	Эта служба используется протоколом туннелирования IPSEC ESP (Протокол обеспечения безопасности инкапсуляции).
FINGER	TCP	79	Команда для UNIX или Интернет, используемая для проверки нахождения пользователя в сети.
FTP	TCP 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.
ICMP	User-Defined	1	Internet Control Message Protocol (Протокол межсетевых управляющих сообщений) часто используется в целях диагностики.
ICQ	udp	4000	Популярная система интерактивного общения в Интернет.
IGMP (многоадресная рассылка)	User-Defined	2	Internet Group Multicast Protocol (Широковещательный протокол взаимодействия групп в сети Интернет) используется для отправки пакетов определенным группам узлов.
IKE	udp	500	Алгоритм обмена ключами в Интернет, используется для распределения ключей и управления ими.
IMAP4	TCP	143	Internet Message Access Protocol 4 (протокол интерактивного доступа к электронной почте).
IMAP4S	TCP	993	Более защищенная версия протокола IMAP4, работающая через SSL-соединение.
IRC	TCP/UDP	6667	Еще одна программа интерактивного общения в Интернет.
MSN Messenger	TCP	1863	Протокол для передачи сообщений в сетях Microsoft.
NetBIOS	TCP/UDP TCP/UDP TCP/UDP TCP/UDP	137 138 139 445	Network Basic Input/Output System (сетевая базовая система ввода-вывода), используется для взаимодействия компьютеров в LAN.
NEW-ICQ	TCP	5190	Программа для обмена текстовыми сообщениями между абонентами сети Internet в реальном времени.
NEWS	TCP	144	Протокол для групп новостей.

Табл. 139 Наиболее часто используемые службы (продолжение)

ИМЯ	ПРОТОКОЛ	ПОРТ(Ы)	ОПИСАНИЕ
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	User-Defined	1	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).
POP3S	TCP	995	Более защищенная версия протокола POP3, работающая через SSL-соединение.
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)	User-Defined	47	PPTP (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.
ROADRUNNER	TCP/UDP	1026	Интернет-провайдер, предоставляющий их, в основном, через кабельные модемы.
RTELNET	TCP	107	Удаленный доступ через Telnet.
RTSP	TCP/UDP	554	Real Time Streaming Protocol (Протокол воспроизведения в реальном времени) – это удаленное управление для мультимедиа в Интернете.
SFTP	TCP	115	Simple File Transfer Protocol (Простой протокол передачи файлов) - устаревший способ обмена файлами между компьютерами.
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.
SMTPS	TCP	465	Более защищенная версия протокола SMTP, работающая через SSL-соединение.

Табл. 139 Наиболее часто используемые службы (продолжение)

ИМЯ	ПРОТОКОЛ	ПОРТ(Ы)	ОПИСАНИЕ
SNMP	TCP/UDP	161	Simple Network Management Program (Простой протокол управления сетью).
SNMP-TRAPS	TCP/UDP	162	Traps for use with the 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.

Алфавитный указатель

L

M

N

P

Q

R

S

T

U

V

W

А

Б

В

Г

Д

Ж

З

И

К

Л

М

Н

О

П

P

C

Т

У

Ф

Ц

Ч

Ш

Э