P660RT3

Модем ADSL2+ с портом Ethernet

P660RU3

Модем ADSL2+ с портами Ethernet и USB

Руководство пользователя

Версия 3.40
04/2010
Редакция 1

НАСТРОЙКИ ПО УМОЛЧАНИЮ	
IP-адрес	**http://192.168.1.1**
Имя пользователя	**admin**
Пароль	**1234**

ZyXEL

www.zyxel.com

О данном руководстве пользователя

Для кого предназначено данное руководство

Данное руководство предназначено для тех, кто планирует производить настройку P660 с помощью Web-конфигуратора. Для работы с руководством необходимо обладать основными знаниями о топологии и принципах организации сетей TCP/IP.

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

Сопроводительная документация

- Краткое руководство

  Краткое руководство разработано с целью помочь вам изучить устройство и начать работать с ним. В нем содержится информация о настройке сети и организации доступа в Интернет.

Рекомендуется выполнять настройку P660 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:

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

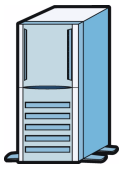
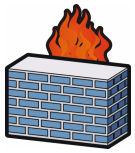
Значком «примечание» помечается важная информация (например, необходимость настройки других параметров или полезные подсказки), рекомендации, относящиеся к теме.

Условные обозначения

- Далее в данном руководстве модели P660RT3 и P660RU3 могут именоваться как «P660», «устройство», «система» или «продукт».
- Надписи на изделии, названия экранов, имена полей и пункты меню обозначаются **жирным** шрифтом.
- Названия клавиш указаны прописными буквами в квадратных скобках, например, [ENTER] означает клавишу «ввод» или «возврат каретки» на клавиатуре.
- Указание «Введите» означает, что следует набрать один или несколько символов и затем нажать клавишу [ENTER]. «Выберите» означает, что следует использовать один из предложенных вариантов.
- Правая угловая скобка (>) между названиями окон означает нажатие кнопки мыши. Например, **Maintenance > 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. Значок P660 является схематичным изображением устройства.

P660 	Компьютер 	Ноутбук 
Сервер 	Брандмауэр 	Телефон 
Маршрутизатор 	Коммутатор 	

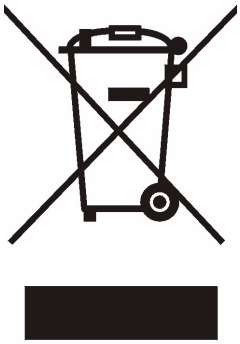
Техника безопасности

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.

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



Содержание

Оглавление

Перечень рисунков

Перечень таблиц

Часть I
Введение

1

Знакомство с устройством P660

В этой главе рассказывается об основных функциях и сферах применения устройства P660, а также о способах управления устройством P660.

1.1 Обзор

Модемы ZyXEL P660RT3 и P660RU3 — 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. Объединяя в себе маршрутизатор с технологией трансляции адресов Cone NAT, DHCP-сервер и множество других функциональных возможностей, они позволяют вам принимать информацию втрое быстрее обычного модема ADSL и в сотни раз быстрее модема 56K для коммутируемых линий. Модем P660RT3 обладает одним портом Ethernet, и к нему можно подключить один компьютер напрямую, либо целую сеть через дополнительный коммутатор. В модели P660RU3 наличие портов Ethernet и USB обеспечивает подключение к Интернету одновременно до двух компьютеров или одного компьютера и ресивера IP-телевидения.

Необходимо использовать встроенное программное обеспечение устройства P660 строго в соответствии с конкретной моделью устройства. См. наклейку, находящуюся на нижней панели устройства P660.

Все экраны, показанные в данном руководстве пользователя, предполагают использование модели P660RU3.

Полный список функций см. в характеристиках устройства.

1.2 Способы управления устройством P660

Для управления устройством P660 используются следующие средства:

- Программа ZyXEL NetFriend. Рекомендуется для простой настройки доступа в Интернет, разработана для пользователей любого уровня подготовки. Находится на прилагаемом к модему диске. Информация по использованию NetFriend приведена в кратком руководстве.
- Web-конфигуратор. Рекомендуется для повседневного управления устройством P660 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 встроенного программного 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 P660

Для обеспечения безопасной и более эффективной работы устройства P660 рекомендуется регулярное и правильное выполнение описанных далее процедур для устройства P660.

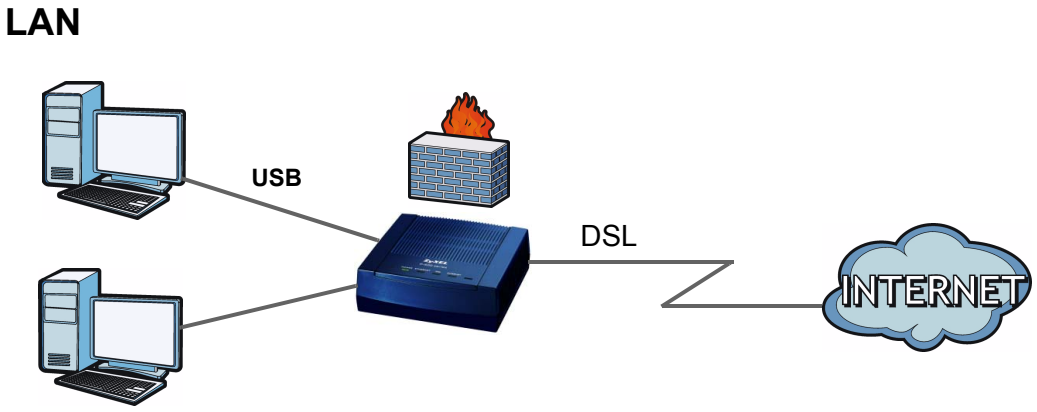
- Изменение пароля. Необходимо использовать пароль, который не поддается легкому угадыванию и состоит из символов различных типов, например, из букв и цифр.
- Запишите пароль и храните его в безопасном месте.
- Сделайте резервное сохранение конфигурации (необходимо знать, как выполнить восстановление 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 P660 к настройкам, установленным изготовителем по умолчанию. При наличии файла предыдущей рабочей конфигурации не придется заново выполнять полную настройку устройства P660. Можно просто восстановить последнюю конфигурацию.

1.4 Сферы применения устройства P660

Далее приведено несколько примеров наиболее подходящего применения устройства P660.

Ваше устройство P660 обеспечивает совместный доступ в Интернет за счет подключения порта DSL к гнезду **DSL** или **MODEM** на сплиттере. Компьютеры могут подключаться к локальным портам LAN устройства P660.

Рис. 1 Функции маршрутизатора устройства P660



Можно также настроить брандмауэр и контент-фильтрацию на устройстве P660 для безопасного доступа в Интернет. По умолчанию устройство P660 блокирует атаки DDOS, LAND и Ping of Death независимо от того, включен или отключен брандмауэр. При включении брандмауэра можно блокировать атаки SYN Flood и Port Scanner.

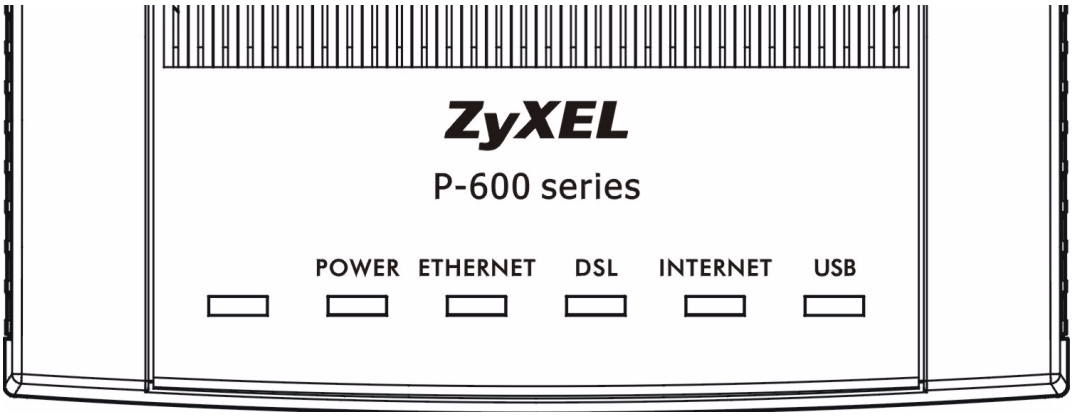
Используйте контент-фильтрацию для блокировки доступа к конкретным веб-сайтам с помощью URL, содержащего указанные вами ключевые слова. Например, можно блокировать доступ детей к определенным веб-сайтам.

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 P660 обеспечивало наивысший приоритет для голосовых вызовов по Интернету и/или ограничить полосу частот, выделенную для выгрузки важных файлов.

1.5 LED (светодиоды)

На приведенном ниже рисунке указаны поля светодиодов.

Рис. 2 Светодиоды в верхней части устройства



Ни один из светодиодов не работает, если устройство P660 не получает питания.

Табл. 1 Описание светодиодов

СВЕТОДИОД	ЦВЕТ	СТАТУС	ОПИСАНИЕ
POWER	Зеленый	Горит	Устройство P660 получает питание и готово к работе.
		Мигает	Выполняется самотестирование устройства P660.
		Выкл	Устройство P660 не получает питания.
ETHERNET	Зеленый	Горит	Устройство P660 имеет Ethernet-подключение к устройству в локальной вычислительной сети (LAN).
		Мигает	Устройство P660 передает/принимает данные из/в LAN.
		Выкл.	Устройство P660 не имеет Ethernet-подключения к LAN.
DSL	Зеленый	Горит	Соединение DSL установлено.
		Мигает	P660 инициализирует линию DSL.
		Выкл	Канал DSL не работает.
INTERNET	Зеленый	Горит	Устройство P660 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 P660 передает или принимает IP-трафик.
	Красный	Горит	Устройство P660 пыталось безуспешно установить IP-подключение. Возможные причины: нет отклика от сервера DHCP, нет отклика от PPPoE, сбой аутентификации PPPoE.
		Выкл	Устройство P660 не имеет IP-подключения.
USB (P660RU3)	Зеленый	Горит	Есть USB-подключение.
		Мигает	Устройство P660 передает или принимает данные через порт USB.
		Выкл	Нет USB-подключения.

Подключение встроенного программного обеспечения описано в Кратком руководстве.

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 все конфигурации, настроенные прежде, будут утрачены, а пароль будет возвращен к установленному по умолчанию значению «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** в течение десяти секунд или 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 Порт USB 1.1 (только для P660RU3)

Порт USB полезен, если у вас есть компьютер, подключаемый к USB, для которого не требуется сетевая интерфейсная карта для подключения к сети Ethernet. См. ниже разделы с описанием процедур установки драйвера USB в вашей операционной системе.

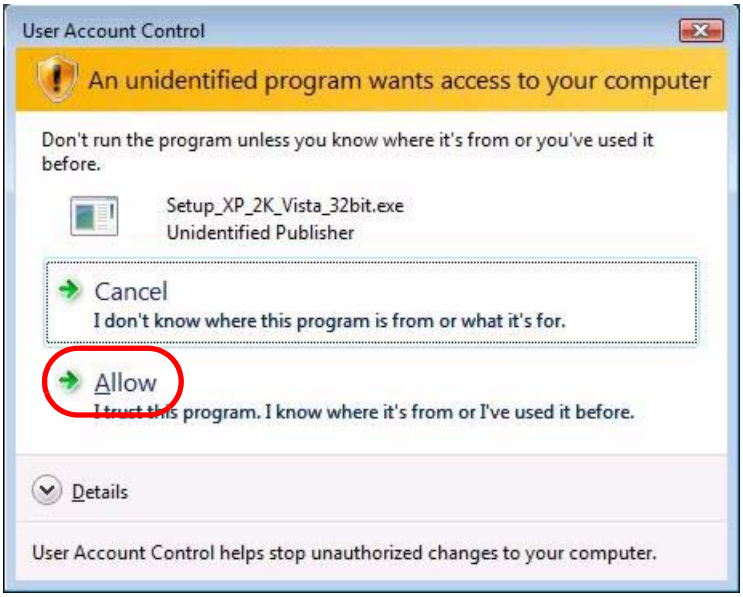
Системные требования

- Windows 98 (Second Edition), Windows Me (Millennium Edition), Windows 2000, Windows XP или Windows Vista
- Доступный порт USB

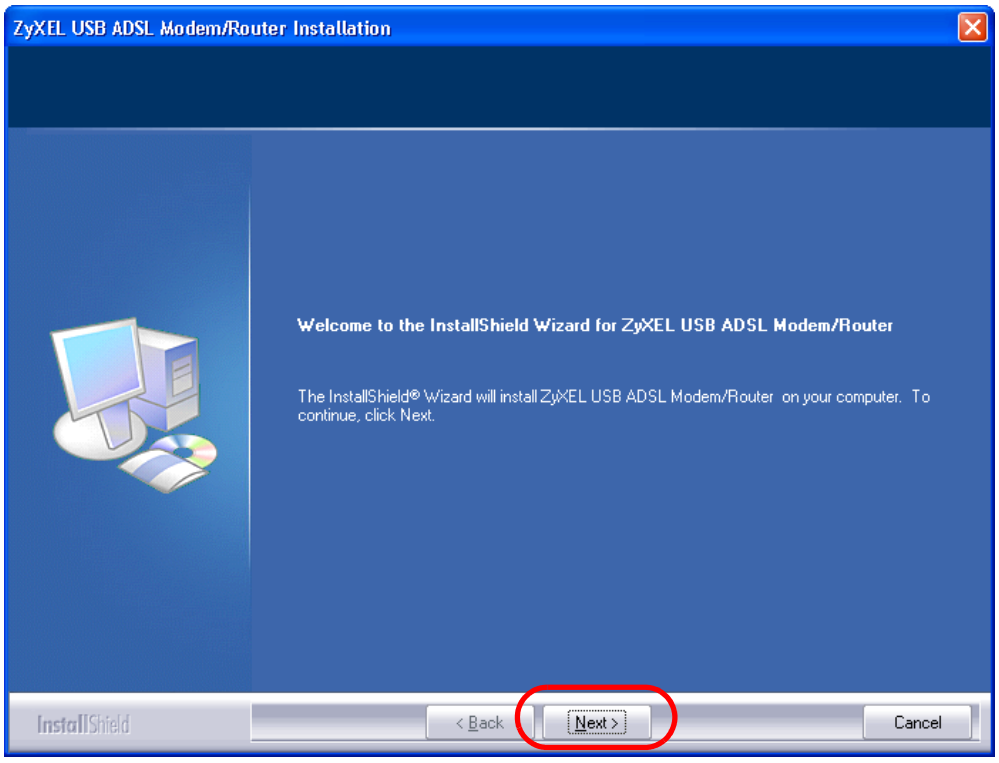
Устанавливайте драйвер USB до подключения устройства P660 к порту USB.

1.7.1 Установка драйвера USB в Windows (только для P660RU3)

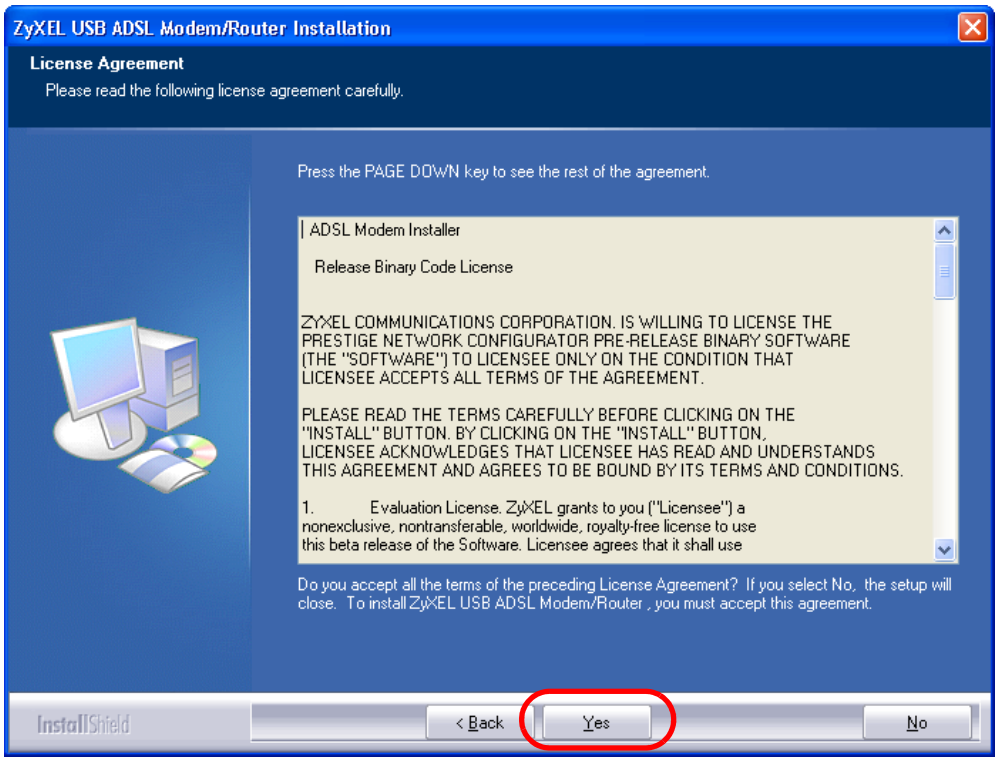
1. Сохраните работу и закройте все приложения.
2. Вставьте прилагаемый CD. Диск запускается автоматически и при этом отображается главный экран.
3. Щелкните на значке **Установка USB драйвера** на главном экране.
4. Предупреждение об установке может появиться в ОС Windows Vista. Нажмите **Allow** для продолжения.



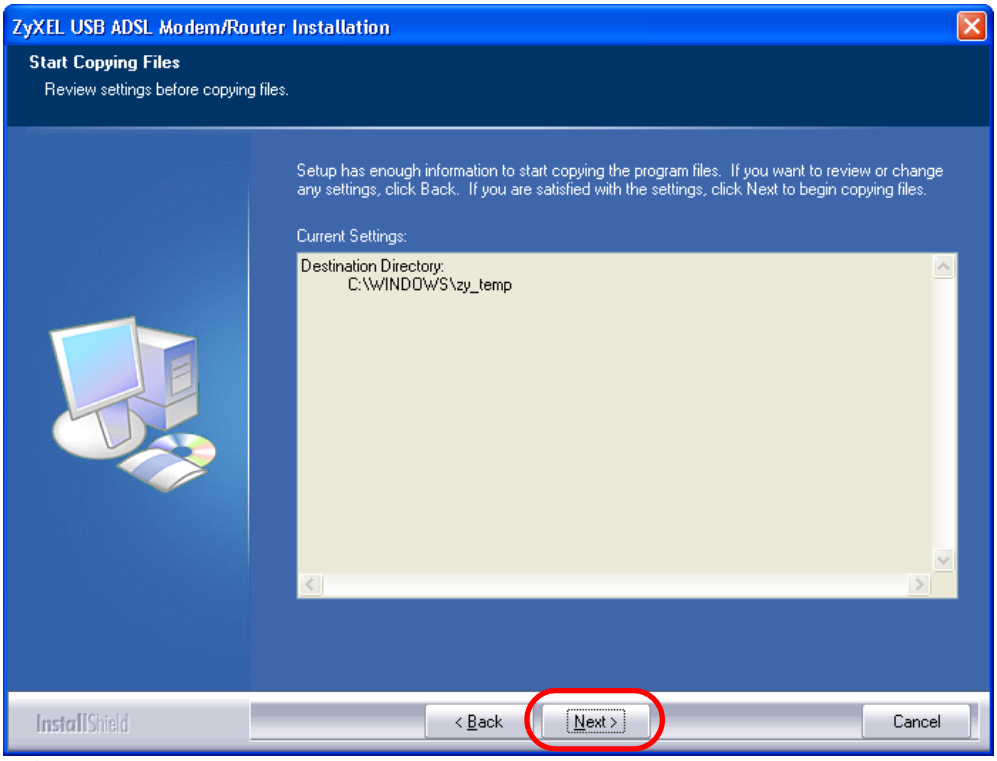
5 Нажмите **Next** на экране с приветствием для запуска мастер-программы для установки USB. Следуйте подсказкам по установке. В конце установки возможно потребуется перезапуск компьютера.



6 Нажмите **Yes**, если вы согласны с условиями лицензионного соглашения.

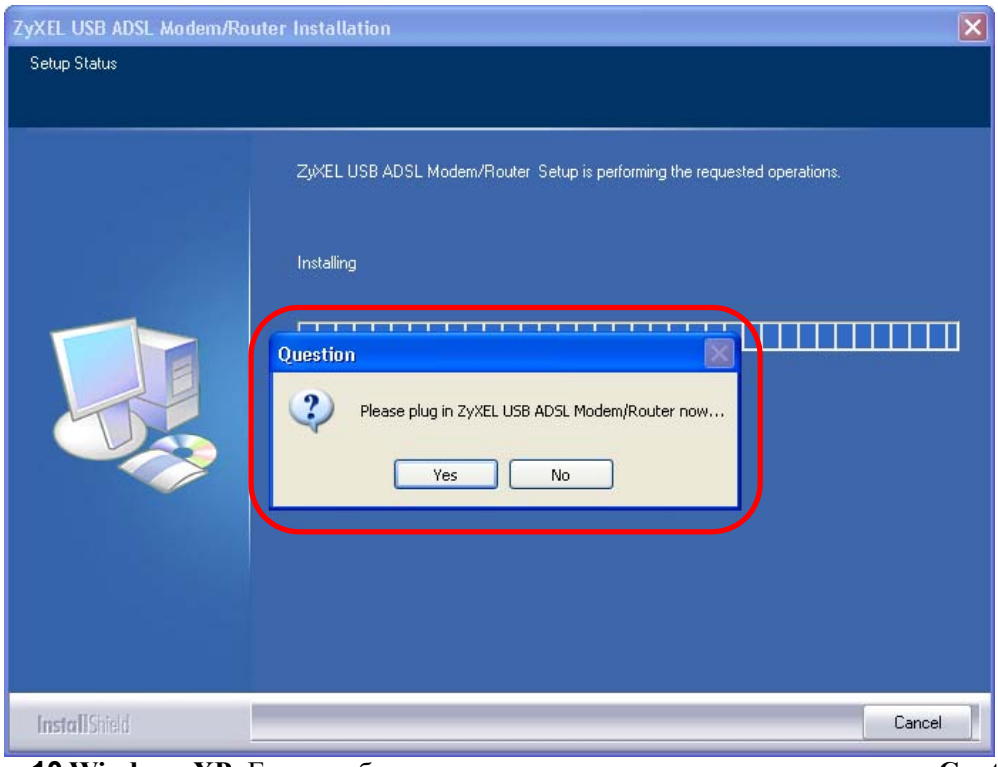


7 Отображается экран **Start Copying Files**. Нажмите **Next**.

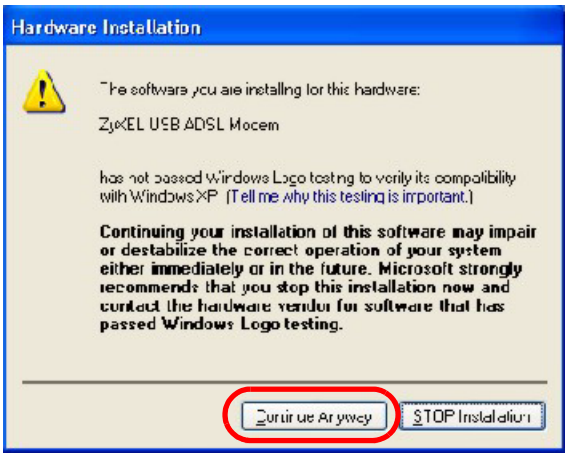


8 **Windows 98/Me**: Выберите **Yes, I want to restart my computer now (Да, перезагрузить сейчас)** и нажмите **OK**.

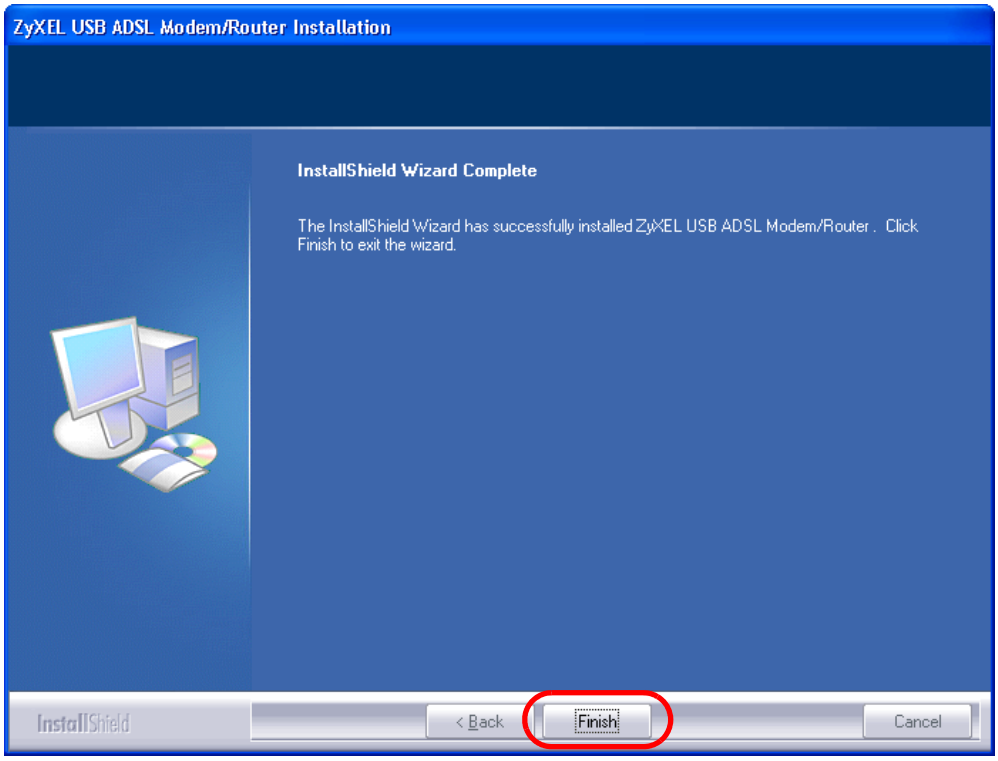
9 **Windows 2000/XP**: Подключите устройство P660 к порту USB компьютера после получения соответствующей подсказки. Отображается окно, в котором указывается, что система обнаружила новое оборудование.



10 **Windows XP**: Если отображается окно с предупреждением, нажмите **Continue Anyway (Все равно продолжить)**.



11 Нажмите **Finish** для завершения установки. При появлении запроса перезагрузите компьютер.

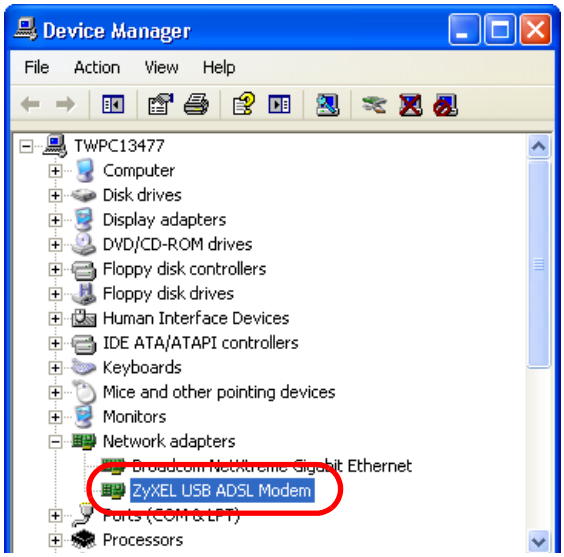


1.7.2 Проверка установки USB

Проверьте статус устройства P660 в окне **Device Manager (Диспетчер устройств)**. Нажмите **Start (Пуск)** > **Settings (Настройка)** > **Control Panel (Панель управления)** > **System (Система)** > **Hardware (Оборудование)**, а затем нажмите **Device Manager (Диспетчер устройств)**. (Последовательность действий может быть разной, в зависимости от версии Windows.)

Проверьте статус устройства P660 в папке **Network adapters (Сетевые платы)**. Убедитесь, что на значке устройства P660 отсутствует вопросительный знак.

Здесь показан экран для Windows XP.



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, либо Netscape Navigator версии 7.0 и выше. Рекомендуемое разрешение экрана: 1024 на 768 пикселей.

Чтобы воспользоваться Web-конфигуратором, необходимо включить следующие параметры:

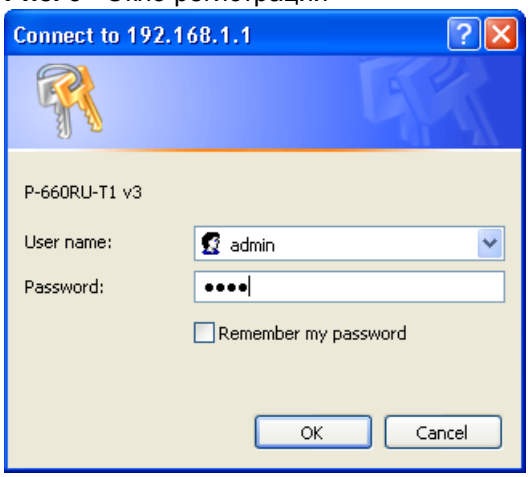
- Инициированные модемом всплывающие окна в веб-браузере. Блокировка всплывающих окон активирована по умолчанию в Windows XP SP2.
- Поддержка JavaScript (по умолчанию активирована).
- Разрешения Java (Java permissions) (по умолчанию активированы).

Если нужно узнать, разрешены ли эти функции в Internet Explorer, см. Прил. B на с. 191.

2.1.1 Доступ к Web-конфигуратору

1. Убедитесь, что ваше устройство P660 подключено правильно (см. «Краткое руководство»).
2. Запустите веб-браузер.
3. Наберите 192.168.1.1 как URL.
4. На экране появится окно регистрации. Для доступа к административному Web-конфигуратору и управления устройством P660 введите имя пользователя (по умолчанию - admin) и пароль (по умолчанию - 1234) на экране регистрации, затем нажмите **OK**. Если вы изменили пароль, введите свой пароль и нажмите **OK**.

Рис. 3 Окно регистрации

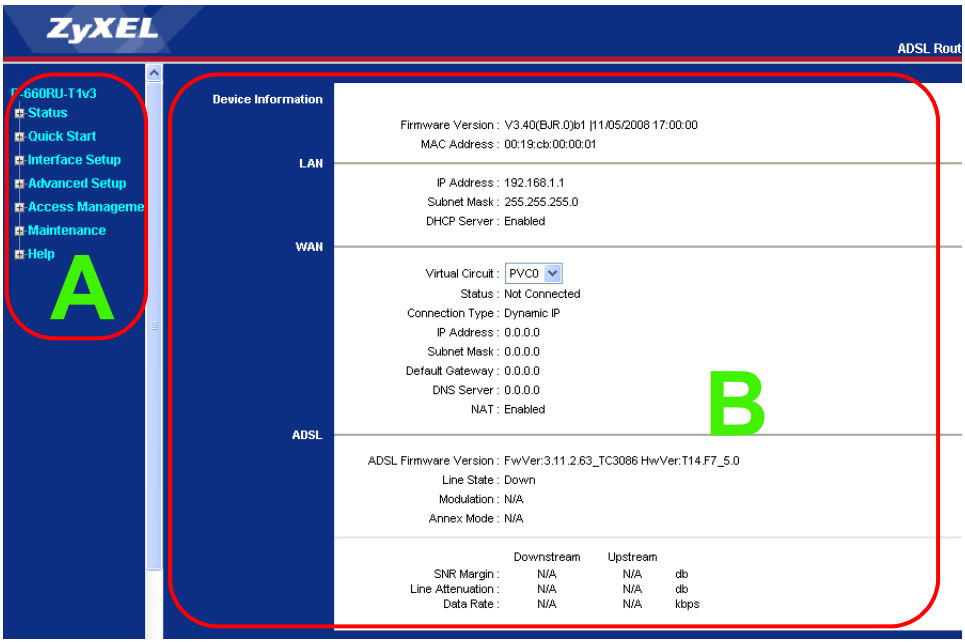


По соображениям безопасности устройство может потребовать сменить пароль на доступ к настройкам. Впишите новый пароль и запомните его.

По соображениям безопасности устройство P660 автоматически выводит вас из системы, если вы не используете Web-конфигуратор в течение пяти минут (по умолчанию). Если это произойдет, просто зарегистрируйтесь еще раз.

2.2 Главный экран Web-конфигуратора

Рис. 4 Главный экран



Как показано выше главный экран разделен на следующие части:

- **A** — панель навигации
- **B** — главное окно

2.2.1 Панель навигации

Используйте позиции меню на панели навигации, чтобы открывать экраны для настройки функций устройства P660. В приведенных ниже таблицах показаны все позиции меню.

Табл. 2 Краткое описание панели навигации

ССЫЛКА	ЗАКЛАДКА	ФУНКЦИЯ
Status		
Device Info		На этом экране показано главное устройство P660 и данные статуса в сети.
System Log		Используйте этот экран для отображения регистрационных журналов устройства.
Statistics		Используйте этот экран для просмотра статистики устройства P660.
Quick Start		
Quick Start		Используйте данную мастер-программу для установки подключения к Интернету.

Табл. 2 Краткое описание панели навигации

ССЫЛКА	ЗАКЛАДКА	ФУНКЦИЯ
Interface Setup		
Internet	Internet	Используйте этот экран для настройки параметров Интернет-провайдера, IP-адресов глобальной сети WAN и других дополнительных свойств.
	PVC Summary Table	Используйте этот экран для отображения настроек канала PVC.
LAN	LAN	Используйте этот экран для настройки протокола TCP/IP в локальной сети LAN, параметров DHCP и других свойств.
	DHCP IP Pool Summary	Используйте этот экран для отображения IP- и MAC-адресов компьютеров локальной сети LAN.
Advanced Setup		
Routing	Routing Table List	Используйте этот экран для отображения статических маршрутов вашего устройства P660.
	Static Route	Используйте этот экран для настройки статического маршрута IP, чтобы сообщать устройству о сети, находящихся вне непосредственно подключенных удаленных узлов.
NAT	NAT	Используйте этот экран для настройки параметров NAT.
	DMZ	Используйте этот экран для настройки параметров DMZ.
	Virtual Server	Используйте этот экран для переадресации входных запросов на услугу, поступающих на сервер(ы) вашей локальной сети.
	IP Address Mapping	Используйте этот экран для изменения настроек отображения адреса вашего устройства P660.
QoS	QoS	Используйте этот экран для включения QoS, задания приоритета для трафика и настройки управления полосой частот в глобальной сети WAN.
	QoS Settings Summary	Используйте этот экран для проверки правил и операций QoS, которые вы настроили для устройства P660.
ADSL		Используйте этот экран для настройки параметров ADSL вашего устройства P660.
Firewall		Используйте этот экран для включения/выключения брандмауэра и/или SPI вашего устройства P660.
Access Management		
ACL		Используйте этот экран для определения того, какое приложение может работать с интерфейсом устройства P660 с ваших компьютеров.
Filter	IP/MAC Filter	Используйте экран для создания правил фильтра IP/MAC.
	Application Filter	Используйте этот экран для установки расписания, по которому ваше устройство будет выполнять контент-фильтрацию.
	URL Filter	Используйте этот экран для того, чтобы разрешить или отклонить трафик для некоторых типов приложений.
SNMP		Используйте этот экран для настройки параметров вашего устройства P660 для управления простым протоколом управления сетью.
UPnP		Используйте этот экран для включения или отключения UPnP.
DDNS		Этот экран позволяет вам использовать статический псевдоним вместо динамического IP-адреса.
CWMP		Используйте этот экран для того, чтобы управляющий сервер управлял устройством P660.

Табл. 2 Краткое описание панели навигации

ССЫЛКА	ЗАКЛАДКА	ФУНКЦИЯ
Maintenance		
Administraton		Используйте этот экран для настройки пароля устройства.
Time Zone		Используйте этот экран для изменения даты и времени на вашем устройстве P660.
Firmware		Используйте этот экран для управления файлами конфигурации и выгрузки встроенного программного обеспечения в ваше устройство.
SysRestart		Этот экран позволяет выполнить перезагрузку P660 без выключения электропитания.
Diagnostic		Используйте этот экран для проверки подключений к другим устройствам.

2.2.2 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. 43 с подробными сведениями об экране **Status**.

Часть II
Статус

3

Информация об устройстве

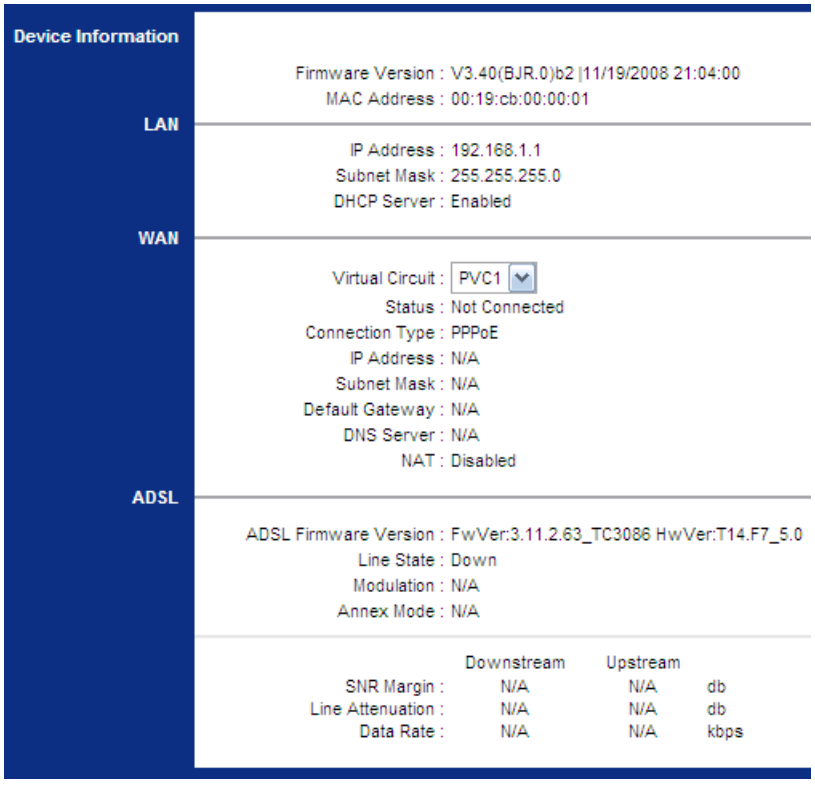
3.1 Обзор

Используйте экран **Device Info** для просмотра текущего состояния устройства, системных ресурсов и интерфейсов (LAN и WAN).

3.2 Экран с информацией об устройстве

Используйте этот экран для просмотра статуса устройства P660. Нажмите **Status** > **Device Info**, чтобы открыть приведенный ниже экран.

Рис. 5 Status > Device Information



В приводимой ниже таблице даны описания полей этого экрана.

Табл. 3 Status > Device Information

ПОЛЕ	ОПИСАНИЕ
Device Information	
Firmware Version	Это текущая версия аппаратного обеспечения внутри устройства. Кроме того, здесь указывается дата создания версии встроенного программного обеспечения.
MAC Address	MAC (управление доступом к среде) или Ethernet адрес, уникальный для вашего устройства P660.
LAN	
IP Address	Текущий IP-адрес устройства P660 в LAN.
Subnet Mask	Текущая маска подсети в локальной сети LAN.
DHCP Server	В этом поле отображаются службы DHCP, которые устройство P660 предусматривает для LAN. Доступные варианты: **Enabled** — Устройство P660 используется в качестве сервера DHCP в LAN. Оно может присваивать IP-адреса другим компьютерам в LAN. **Relay** — Устройство P660 действует в качестве фиктивного DHCP-сервера и обеспечивает передачу запросов и ответов DHCP между удаленным сервером и клиентами. **Disabled** — Устройство P660 не обеспечивает услуги DHCP для LAN.
WAN	
Virtual Circuit	Используйте разворачивающееся меню для выбора виртуального канала PVC. В показанных ниже полях отображается информация о выбранном вами виртуальном канале.
Status	Статус подключения глобальной сети WAN.
Connection Type	Тип соединения, поддерживаемый вашим Интернет-провайдером.
IP Address	Текущий IP-адрес устройства P660 в WAN, если он используется.
IP Subnet Mask	Текущая маска подсети в WAN, если она используется.
Default Gateway	IP-адрес шлюза по умолчанию, если он применяется.
DNS Server	Текущий DNS-сервер в WAN, если он используется.
NAT	Это поле указывает, используется ли NAT (трансляция сетевых адресов).
ADSL	
ADSL Firmware Version	Текущая версия кода DSL-модема устройства.
Line State	Статус вашего соединения ADSL.
Modulation	ADSL-модуляция вашего устройства P660.
Annex Mode	Дополнительный режим вашего устройства P660.
Downstream	Скорость входящего потока данных на вашем устройстве ZyXEL.
Upstream	Скорость исходящего потока данных на вашем устройстве ZyXEL.
SNR Margin	Предел соотношения сигнал-шум (SNR). SNR представляет собой соотношение величины принятого сигнала к шумовом порогу системы. Чем выше значение SNR, тем лучше качество линии.
Line Attenuation	Разница (в дБ) между принимаемым питанием на нижнем и дальнем концах.
Data Rate	Это скорость передачи данных для вашего устройства P660.

4

Системные журналы

4.1 Обзор

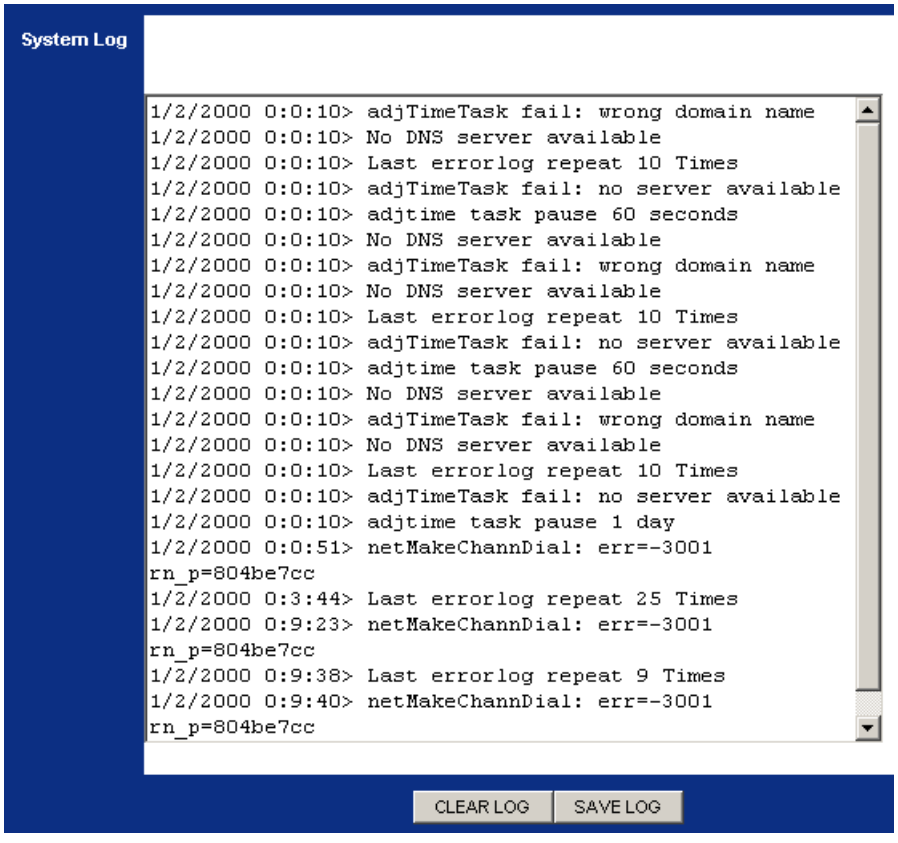
В этой главе содержится информация о просмотре регистрационных журналов устройства P660.

Журнал регистрации представляет собой сообщение о событии, которое произошло на вашем устройстве P660. Например, если кто-то входит в систему устройства P660.

4.2 Экран системного журнала

Используйте этот экран для просмотра регистрационных журналов вашего устройства P660. Нажмите **Status > System Log**, чтобы открыть приведенный ниже экран.

Рис. 6 Status > System Log



В приводимой ниже таблице даны описания полей этого экрана.

Табл. 4 Status > System Log

ПОЛЕ	ОПИСАНИЕ
System Log	В этом поле отображаются сообщения регистрационных журналов вашего устройства P660.
CLEAR LOG	Нажмите эту кнопку для удаления всех регистрационных журналов.
SAVE LOG	Нажмите эту кнопку для сохранения регистрационных журналов в текстовом файле.

5

Статистика трафика

5.1 Обзор

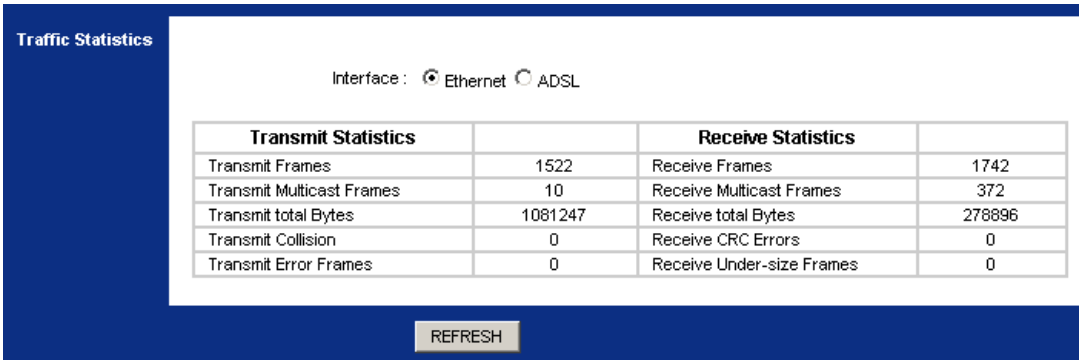
В этой главе приводится информация о том, как посмотреть статистику трафика на вашем устройстве P660.

5.2 Экран статистики

Используйте этот экран для проверки статистики трафика вашего устройства P660. Нажмите **Status > Statistics**, чтобы открыть приведенный ниже экран. Этот экран может меняться в зависимости от того, какой тип порта вы выбрали в поле **Interface**.

На приведенном ниже экране отображается статистика трафика для порта Ethernet.

Рис. 7 Status > Statistics (Ethernet)



В приводимой ниже таблице даны описания полей этого экрана.

Табл. 5 Status > Statistics (Ethernet)

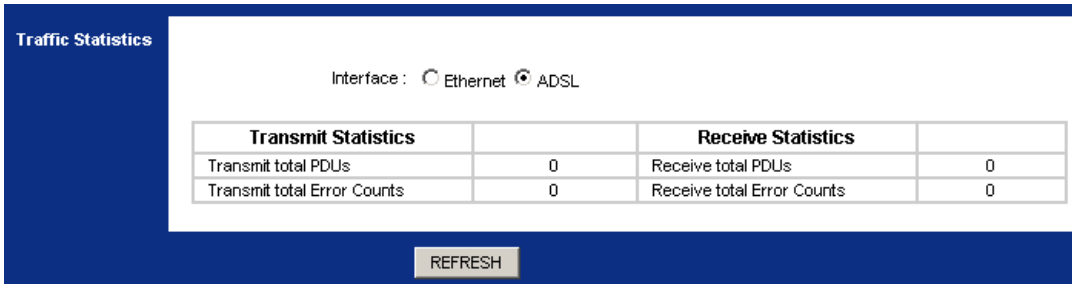
ПОЛЕ	ОПИСАНИЕ
Interface	Выберите **Ethernet** или **ADSL** для отображения статистики трафика через порт.
Transmit Statistics	
Transmit Frames	В этом поле отображается количество кадров, переданных через этот порт.
Transmit Multicast Frames	В этом поле отображается количество переданных многоадресных кадров.
Transmit total Bytes	В этом поле отображается количество байт, переданных через этот порт.

Табл. 5 Status > Statistics (Ethernet) (продолжение)

ПОЛЕ	ОПИСАНИЕ
Transmit Collision	В этом поле отображается информация о конфликтах во время передачи кадров.
Transmit Error Frames	В этом поле отображается количество ошибок, переданных через этот порт.
Receive Statistics	
Receive Frames	В этом поле отображается количество кадров, принятых через этот порт.
Receive Multicast Frames	В этом поле отображается количество принятых многоадресных кадров.
Receive total Bytes	В этом поле отображается количество байтов, принятых через этот порт.
Receive CRC errors	В этом поле отображается количество кадров, принятых с ошибками проверки циклической контрольной суммы (CRC).
Receive Under-size Frames	В этом поле отображается количество принятых кадров неподходящего размера (менее 60 октет или более 1522 октет).
REFRESH	Нажмите эту кнопку для обновления экрана.

На приведенном ниже экране отображается статистика трафика для порта ADSL.

Рис. 8 Status > Statistics (ADSL)



В приводимой ниже таблице даны описания полей этого экрана.

Табл. 6 Status > Statistics (ADSL)

ПОЛЕ	ОПИСАНИЕ
Transmit Statistics	
Transmit total PDUs	В этом поле отображается количество блоков протокольных данных (PDU), переданных на этот порт.
Transmit total Error Counts	В этом поле отображается количество ошибок, переданных через этот порт.
Receive Statistics	
Receive total PDUs	В этом поле отображается количество блоков протокольных данных PDU, принятых через этот порт.
Receive total Error Counts	В этом поле отображается количество ошибок, принятых через этот порт.
REFRESH	Нажмите эту кнопку для обновления экрана.

Часть III
Настройка сетевых интерфейсов

6

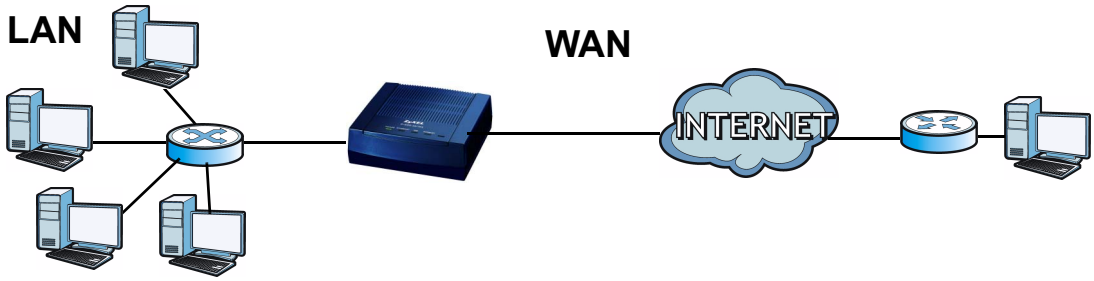
Настройка Интернета

6.1 Обзор

В этой главе описывается настройка глобальной вычислительной сети на экранах **Internet**. Используйте эти экраны для настройки устройства P660 для доступа в Интернет.

Подключение WAN представляет собой внешнее подключение к другой сети или 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. 9 LAN и WAN



6.1.1 Что можно сделать на экранах Интернет

- Используйте экран **Internet** (Разд. 6.2 на с. 53) для настройки параметров WAN устройства P660 для доступа в Интернет.
- Используйте экран **PVCs Summary** (Разд. 6.2.5 на с. 61) для отображения сводной таблицы настроек PVC.

6.1.2 Что нужно знать о доступе в Интернет через ADSL

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. Если ваш Интернет-провайдер предлагает подключение к Интернету по телефонной линии с помощью PPPoE (Протокол «точка-точка» поверх Ethernet), то он должен также дать вам имя пользователя и пароль (и наименование службы) для аутентификации пользователя.

Условия работы ADSL

Постоянный виртуальный канал (PVC) — это соединение вашего устройства с Интернет-провайдером. Вам необходимы VPI (Идентификатор виртуального пути) и VCI (Идентификатор виртуального канала) для определения виртуального канала. Мультиплексирование — это способ переноса протоколов в PVC. Эту информацию вам должен предоставить ваш Интернет-провайдер.

IP-адрес WAN

IP-адрес глобальной сети WAN представляет собой IP-адрес устройства P660, обеспечивая доступ к нему из внешней сети. Он используется устройством P660 для связи с другими устройствами в других сетях. Он может быть статичным (фиксированным) или динамически присваиваться Интернет-провайдером каждый раз, когда устройство P660 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).

ATM QoS (Качество услуг ATM)

Асинхронный режим передачи (ATM) — это сетевые технологии LAN и WAN, обеспечивающие высокую скорость передачи данных. В ATM используются пакеты информации фиксированного размера, называемые ячейками. С помощью ATM может быть гарантировано высокое QoS (качество предоставляемых услуг). QoS — это соглашение об обслуживании, которое гарантирует определенную скорость даже при переполнении сети. ATM QoS определяется пиковой скоростью ячеек (PCR), поддерживаемой скоростью ячеек (SCR) и максимальным размером пакета (MBS).

NAT

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

Многоадресная рассылка

Обычно передача пакетов IP 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 пакетов IP 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 фильтрацию источника, игнорирование трафика или отчет о трафике с конкретного адрес источника на конкретный узел сети.

Дополнительные сведения

См. Разд. 6.3 на с. 61 для поиска технической вводной информации о WAN.

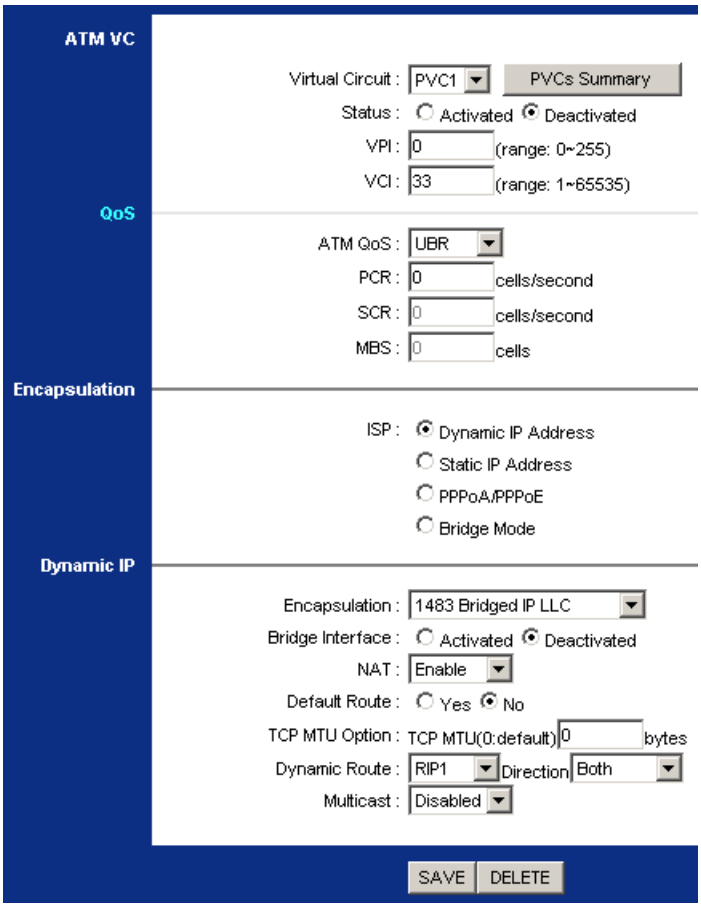
6.1.3 Перед началом

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

6.2 Экран Internet

Используйте этот экран для изменения настроек WAN устройства P660. Нажмите **Interface Setup > Internet**. Этот экран отличается в зависимости от выбранной инкапсуляции.

Рис. 10 Interface Setup > Internet



В приводимой ниже таблице даны описания полей этого экрана.

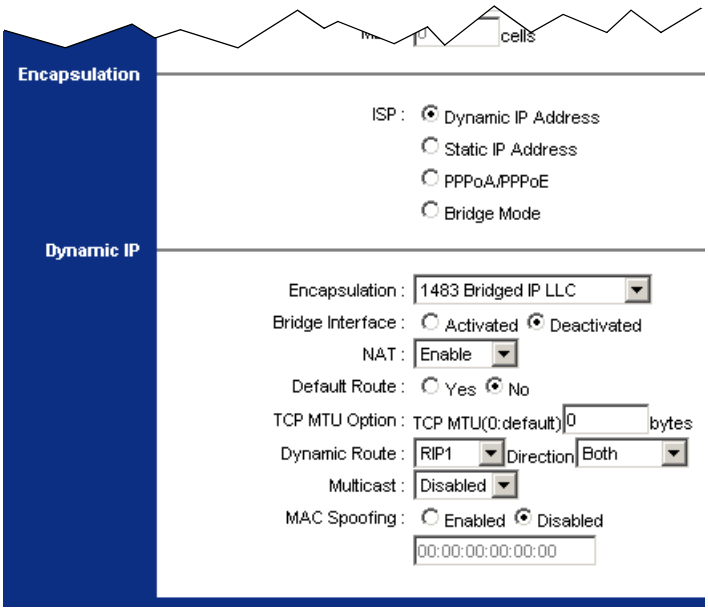
Табл. 7 Interface Setup > Internet

ПОЛЕ	ОПИСАНИЕ
ATM VC	
Virtual Circuit	Выберите из разворачивающегося списка в окне виртуальный канал (PVC), который вы хотите настроить.
PVCs Summary	Нажмите эту кнопку для отображения сводной таблицы настроек PVC на вашем устройстве P660. Более подробную информацию см. в Разд. 6.2.5 на с. 61.
Status	Используйте это поле для включения или отключения PVC.
VPI	Идентификатор виртуального пути (VPI) определяет виртуальный канал. Более подробную информацию см. в приложении. Введите назначенный идентификатор виртуального пути.
VCI	Идентификатор виртуального канала (VCI) определяет виртуальный канал. Введите назначенный идентификатор виртуального канала. Более подробную информацию см. в приложении.
QoS	
ATM QoS	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 **rtVBR** (real-time Variable Bit Rate — Переменная скорость передачи в реальном времени) приложений с пульсирующим трафиком, который требует тщательного контроля задержки и изменений задержки. Выберите **nrtVBR** (non real-time Variable Bit Rate — Переменная скорость передачи вне реального времени) для подключений, которые не требуют тщательного контроля задержки и изменений задержки.
PCR	Разделите скорость передачи DSL-линии (в битах в секунду) на 424 (размер ячейки ATM), чтобы определить пиковую скорость ячеек (PCR). Максимальная скорость, с которой отправитель может передавать ячейки. Введите PCR в это поле.
SCR	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.
MBS	MBS (Maximum Burst Size — Максимальный размер пакета) — это максимальное количество ячеек, которое может быть передано на пиковой скорости. Введите MBS, который должен быть меньше 65535.
Encapsulation	Выберите тип подключения, поддерживаемый вашим Интернет-провайдером. Последующие поля меняются в зависимости от используемого типа подключения. Подробнее см. в следующих разделах.
SAVE	Нажмите эту кнопку для сохранения своих изменений.
DELETE	Нажмите эту кнопку для сброса значений PVC на значения по умолчанию.

6.2.1 Динамический IP-адрес

На экране **Interface Setup** > **Internet** выберите **Dynamic IP Address** в поле **ISP** для отображения следующего экрана.

Рис. 11 Interface Setup > Internet (Dynamic IP)



В приводимой ниже таблице даны описания полей этого экрана.

Табл. 8 Interface Setup > Internet (Dynamic IP)

ПОЛЕ	ОПИСАНИЕ
Encapsulation	В разворачивающемся списке выберите способ мультиплексирования, используемый вашим Интернет-провайдером. Доступные варианты: **1483 Bridged IP LLC**, **1483 Bridged IP VC-Mux**, **1483 Routed IP LLC(IPoA)** и **1483 Routed IP VC-Mux**.
Bridge Interface	Это поле доступно только в том случае, если вы выбрали **1483 Bridged IP LLC** или **1483 Bridged IP VC-Mux** в поле **Encapsulation**. Используйте это поле для включения или отключения мостового режима. Активизируйте мостовой режим, 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.
NAT	Используйте это поле для включения или отключения трансляции сетевых адресов (NAT).
Default Route	Выберите **Yes** для указания направления трафика, не указанного в таблице маршрутов, на шлюз по умолчанию. Выберите **No** для остановки трафика, не указанного в таблице маршрутов.
TCP MTU Option	Максимальный размер единицы передаваемой информации (MTU) определяет наибольший размер пакета, допустимого для интерфейса или подключения. Введите MTU в этом поле.
Dynamic Route	RIP (Протокол обмена информацией о маршрутизации) позволяет маршрутизатору обмениваться информацией о маршрутизации с другими маршрутизаторами. Выберите версию RIP из **RIP1**, **RIP2-B** и **RIP2-M**.

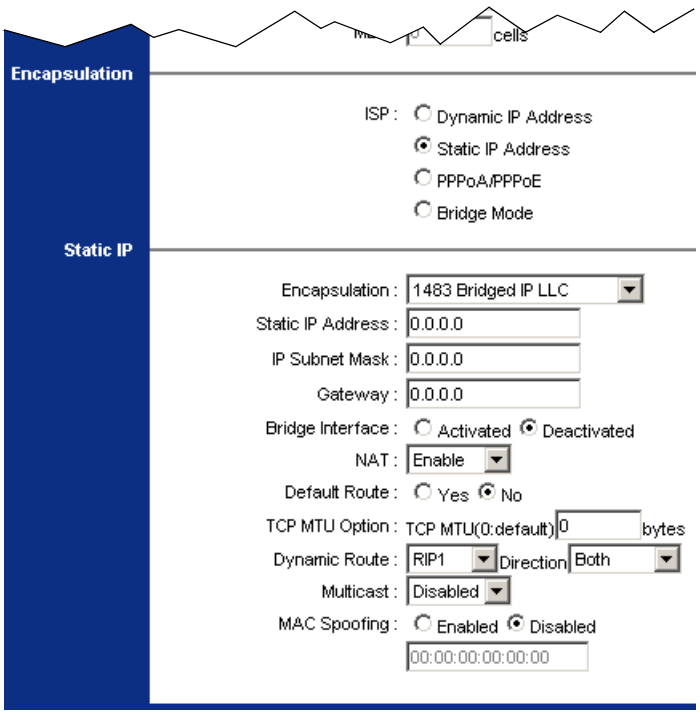
Табл. 8 Interface Setup > Internet (Dynamic IP) (продолжение)

ПОЛЕ	ОПИСАНИЕ
Direction	Используйте это поле для управления объемом информацией о маршрутизации, которую устройство P660 передает и принимает по подсети. Выберите направление RIP из **None**, **Both**, **In Only** и **Out Only**.
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 — это протокол сетевого уровня, используемый для установления принадлежности к группе многоадресной рассылки. Устройство P660 поддерживает **IGMP v1**, **IGMP v2** и **IGMP v3**. Выберите **Disabled** для отключения этой функции.
MAC Spoofing	Это поле доступно только в том случае, если вы выбрали **1483 Bridged IP LLC** или **1483 Bridged IP VC-Mux** в поле **Encapsulation**. Используйте это поле для изменения MAC-адреса так, чтобы PVC в устройстве P660 смог установить соединение с сетью.

6.2.2 Статический IP-адрес

На экране **Interface Setup** > **Internet** выберите **Static IP Address** в поле **ISP** для отображения следующего экрана.

Рис. 12 Interface Setup > Internet (Static IP)



В приводимой ниже таблице даны описания полей этого экрана.

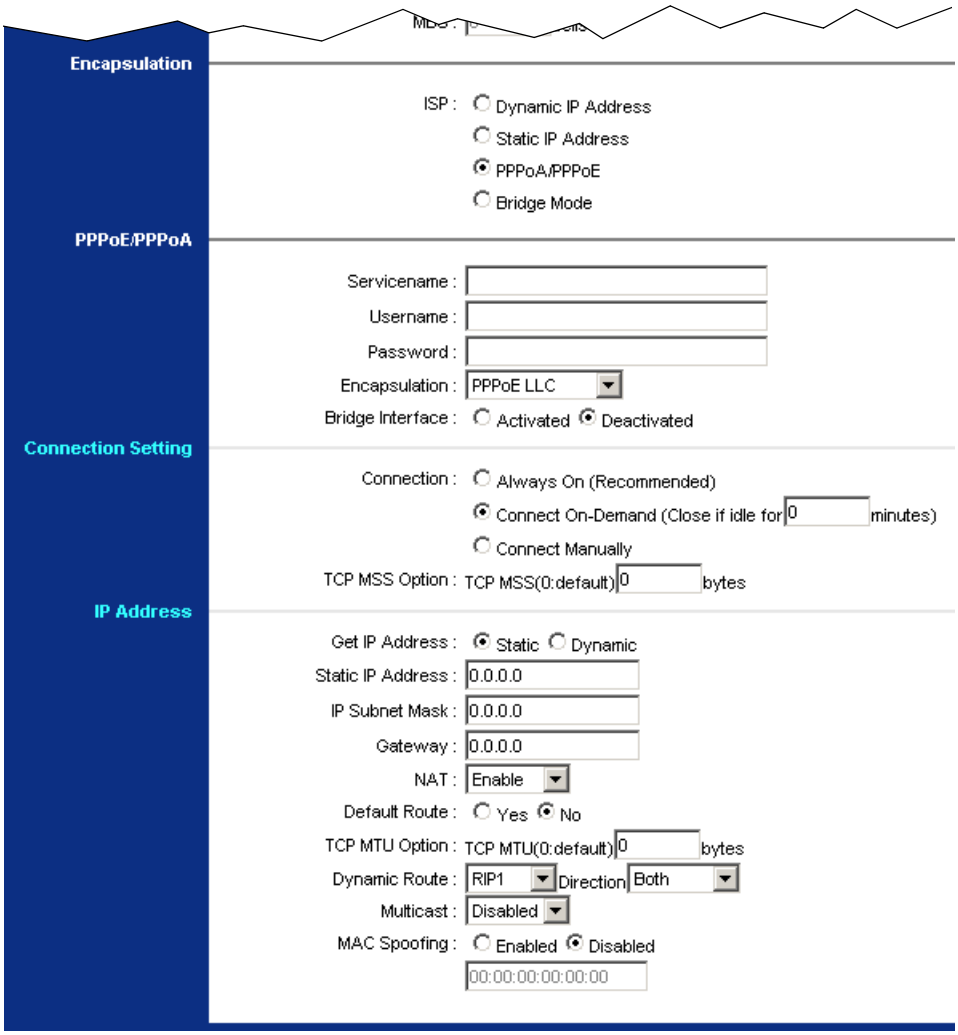
Табл. 9 Interface Setup > Internet (Static IP)

ПОЛЕ	ОПИСАНИЕ
Encapsulation	В разворачивающемся списке выберите способ мультиплексирования, используемый вашим Интернет-провайдером. Доступные варианты: **1483 Bridged IP LLC**, **1483 Bridged IP VC-Mux**, **1483 Routed IP LLC(IPoA)** и **1483 Routed IP VC-Mux**.
Static IP Address	Статический IP-адрес — это фиксированный IP-адрес, который назначает Интернет-провайдер. Наберите в этом поле IP-адрес, присвоенный вам Интернет-провайдером.
IP Subnet Mask	Введите маску подсети в десятичном виде с разделительными точками.
Gateway	Введите IP-адрес шлюза, предоставленный Интернет-провайдером.
Bridge Interface	Это поле доступно только в том случае, если вы выбрали **1483 Bridged IP LLC** или **1483 Bridged IP VC-Mux** в поле **Encapsulation**. Используйте это поле для включения или отключения мостового режима. Активизируйте мостовой режим, 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.
NAT	Используйте это поле для включения или отключения трансляции сетевых адресов (NAT).
Default Route	Выберите **Yes** для указания направления трафика, не указанного в таблице маршрутов, на шлюз по умолчанию. Выберите **No** для остановки трафика, не указанного в таблице маршрутов.
TCP MTU Option	Максимальный размер единицы передаваемой информации (MTU) определяет наибольший размер пакета, допустимого для интерфейса или подключения. Введите MTU в этом поле.
Dynamic Route	RIP (Протокол обмена информацией о маршрутизации) позволяет маршрутизатору обмениваться информацией о маршрутизации с другими маршрутизаторами. Выберите версию RIP из **RIP1**, **RIP2-B** и **RIP2-M**.
Direction	Используйте это поле для управления объема информацией о маршрутизации, которую устройство P660 передает и принимает по подсети. Выберите направление RIP из **None**, **Both**, **In Only** и **Out Only**.
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 — это протокол сетевого уровня, используемый для установления принадлежности к группе многоадресной рассылки. Устройство P660 поддерживает **IGMP v1**, **IGMP v2** и **IGMP v3**. Выберите **Disabled** для отключения этой функции.
MAC Spoofing	Это поле доступно только в том случае, если вы выбрали **1483 Bridged IP LLC** или **1483 Bridged IP VC-Mux** в поле **Encapsulation**. Используйте это поле для изменения MAC-адреса так, чтобы PVC в устройстве P660 смог установить соединение с сетью.

6.2.3 PPPoA/PPPoE

На экране **Interface Setup** > **Internet** выберите **PPPoA/PPPoE** в поле **ISP** для отображения следующего экрана.

Рис. 13 Interface Setup > Internet (PPPoA/PPPoE)



В приводимой ниже таблице даны описания полей этого экрана.

Табл. 10 Interface Setup > Internet (PPPoA/PPPoE)

ПОЛЕ	ОПИСАНИЕ
PPPoE/PPPoA	
Servicename	В этом поле наберите название своей службы.
Username	Введите имя пользователя в точности так, как назначено Интернет-провайдером. Если имя назначается в формате user@domain, где domain означает имя услуги, то вводите оба элемента имени в полном соответствии с данными от провайдера.
Password	Введите пароль, соответствующий имени пользователя, указанному выше.

Табл. 10 Interface Setup > Internet (PPPoA/PPPoE) (продолжение)

ПОЛЕ	ОПИСАНИЕ
Encapsulation	В разворачивающемся списке выберите способ мультиплексирования, используемый вашим Интернет-провайдером. Доступные варианты: **PPPoE LLC**, **PPPoE VC-Mux**, **PPPoA LLC** и **PPPoA VC-Mux**.
Bridge Interface	Это поле доступно только в том случае, если вы выбрали **PPPoE LLC** или **PPPoE VC-Mux** в поле **Encapsulation**. Используйте это поле для включения или отключения мостового режима. Активизируйте мостовой режим, 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.
Connection Setting	
Connection	Выберите **Always On (Recommended)** если вы хотите иметь постоянное подключение. Устройство P660 постарается автоматически восстановить соединение в случае его отключения. Выберите **Connect On-Demand**, если вы не хотите постоянное подключение и укажите время простоя в минутах. Установкой по умолчанию является 0 мин, что означает, что сеанс связи с Интернетом не должен прерываться. Выберите **Connect Manually** для установления подключения только, когда это необходимо. ПРИМЕЧАНИЕ: Не устанавливайте постоянное соединение, если телефонная компания не предлагает услугу единого тарифа (без повременного учета) или если вам необходима постоянная связь, а стоимость не очень велика.
TCP MSS Option	Максимальный размер сегмента TCP (MSS) определяет наибольший размер пакета, допустимого для интерфейса или подключения. Введите в этом поле TCP MSS. Обычно TCP MSS равно 1452.
IP Address	
Get IP Address	Выберите тип IP-адреса, поддерживаемый вашим Интернет-провайдером. Статический IP-адрес — это фиксированный IP-адрес, который назначает Интернет-провайдер. Динамический IP-адрес не фиксирован; Интернет-провайдер каждый раз назначает новый адрес при подключении к Интернету.
Static IP Address	Наберите в этом поле IP-адрес, присвоенный вам Интернет-провайдером.
IP Subnet Mask	Введите маску подсети в десятичном виде с разделительными точками.
Gateway	Введите IP-адрес шлюза, предоставленный Интернет-провайдером.
NAT	Используйте это поле для включения или отключения трансляции сетевых адресов (NAT).
Default Route	Выберите **Yes** для указания направления трафика, не указанного в таблице маршрутов, на шлюз по умолчанию. Выберите **No** для остановки трафика, не указанного в таблице маршрутов.
TCP MTU Option	Максимальный размер единицы передаваемой информации (MTU) определяет наибольший размер пакета, допустимого для интерфейса или подключения. Введите MTU в этом поле.
Dynamic Route	RIP (Протокол обмена информацией о маршрутизации) позволяет маршрутизатору обмениваться информацией о маршрутизации с другими маршрутизаторами. Выберите версию RIP из **RIP1**, **RIP2-B** и **RIP2-M**.

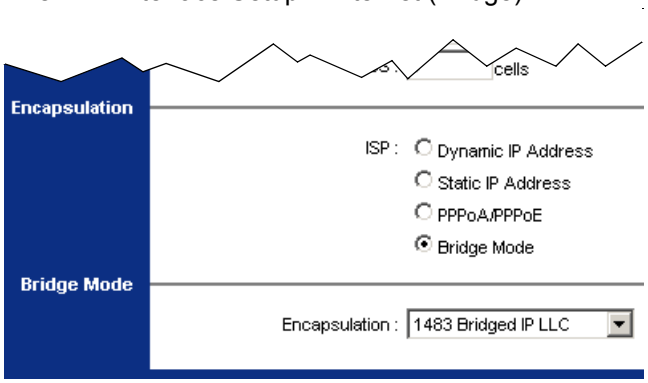
Табл. 10 Interface Setup > Internet (PPPoA/PPPoE) (продолжение)

ПОЛЕ	ОПИСАНИЕ
Direction	Используйте это поле для управления объема информацией о маршрутизации, которую устройство P660 передает и принимает по подсети. Выберите направление RIP из **None**, **Both**, **In Only** и **Out Only**.
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 — это протокол сетевого уровня, используемый для установления принадлежности к группе многоадресной рассылки. Устройство P660 поддерживает **IGMP v1**, **IGMP v2** и **IGMP v3**. Выберите **Disabled** для отключения этой функции.
MAC Spoofing	Это поле доступно только в том случае, если вы выбрали **1483 Bridged IP LLC** или **1483 Bridged IP VC-Mux** в поле **Encapsulation**. Используйте это поле для изменения MAC-адреса так, чтобы PVC в устройстве P660 смог установить соединение с сетью.

6.2.4 Режим межсетевого моста

На экране **Interface Setup** > **Internet** выберите **Bridge Mode** в поле **ISP** для отображения следующего экрана.

Рис. 14 Interface Setup > Internet (Bridge)



В приводимой ниже таблице даны описания полей этого экрана.

Табл. 11 Interface Setup > Internet (Bridge)

ПОЛЕ	ОПИСАНИЕ
Encapsulation	В разворачивающемся списке выберите способ мультиплексирования, используемый вашим Интернет-провайдером. Доступные варианты: **1483 Bridged IP LLC** и **1483 Bridged IP VC-Mux**.

6.2.5 Сводный экран постоянного виртуального канала

Используйте это поле для проверки ваших настроек PVC. На экране **Interface Setup** > **Internet** нажмите **PVCs Summary** в поле **Virtual Circuit** для отображения следующего экрана.

Рис. 15 Interface Setup > PVCs Summary

Service Information Summary

#	Active	VPI	VCI	ENCAP	Mux	IP Address	Status
PVC0	Yes	0	33	PPPoE	LLC	Dynamic	Idle
PVC1	-	-	-	-	-	-	-
PVC2	No	1	34	ENET ENCAP	LLC	Dynamic	N/A
PVC3	-	-	-	-	-	-	-
PVC4	-	-	-	-	-	-	-
PVC5	-	-	-	-	-	-	-
PVC6	-	-	-	-	-	-	-
PVC7	-	-	-	-	-	-	-

В приводимой ниже таблице даны описания полей этого экрана.

Табл. 12 Interface Setup > PVCs Summary

ПОЛЕ	ОПИСАНИЕ
#	В этом поле отображается индекс соответствующего PVC.
Active	В этом поле указывается, активен ли виртуальный канал PVC.
VPI	В этом поле отображается значение VPI.
VCI	В этом поле отображается значение VCI.
ENCAP	В данном поле отображается тип инкапсуляции.
Mux	В этом поле отображается способ мультиплексирования.
IP Address	В этом поле отображается тип IP-адреса.
Status	В этом поле отображается статус подключения PVC.

6.3 Техническое руководство WAN

В этом разделе приводится некоторая вводная техническая информация о темах данной главы.

6.3.1 Инкапсуляция

Убедитесь, что используется метод инкапсуляции, предписанный вашим Интернет-провайдером. Ниже перечислены методы инкапсуляции, поддерживаемые устройством P660.

PPP over Ethernet

Устройство P660 поддерживает протокол PPPoE (Point-to-Point Protocol over Ethernet — Протокол «точка-точка» поверх Ethernet). — 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 выполняется непосредственно на P660 (а не на отдельных компьютерах), установка программного обеспечения PPPoE на компьютерах локальной сети не требуется, поскольку эта процедура полностью выполняется устройством P660. Кроме того, с NAT доступ обеспечивается для всех компьютеров LAN.

PPPoA

PPPoA означает Протокол «точка-точка» через уровень 5 адаптации ATM (AAL5). Функции подключения PPPoA аналогичны коммутируемому подключению к Интернету. Устройство P660 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. Информацию по PPP см. в комментарии RFC 1661.

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.

6.3.2 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.

6.3.3 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.

6.3.4 Назначение IP-адреса

Статический IP-адрес — это фиксированный IP-адрес, который назначает Интернет-провайдер. Динамический IP-адрес не фиксирован, Интернет-провайдер каждый раз назначает новый адрес. Но при этом назначенный метод инкапсуляции влияет на ваш выбор IP-адреса.

Назначение IP-адреса с помощью инкапсуляции 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-адреса с помощью инкапсуляции RFC 1483

В этом случае назначение IP-адреса должно быть статическим.

6.3.5 Постоянное подключение (PPP)

Постоянное подключение (Always on) — это коммутируемая линия, которая всегда подключена независимо от требования трафика. Устройство P660 выполняет при постоянном соединении два действия. Первое заключается в том, что оно отключает функцию времени простоя. Второе заключается в том, что устройство P660 пытается восстановить соединение при включении питания, а также при разрыве соединения. Постоянное соединение может быть очень дорогостоящим по очевидным причинам.

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

6.3.6 Качество услуг ATM (ATM QoS)

ATM QoS — это функция формирования трафика, которая 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.

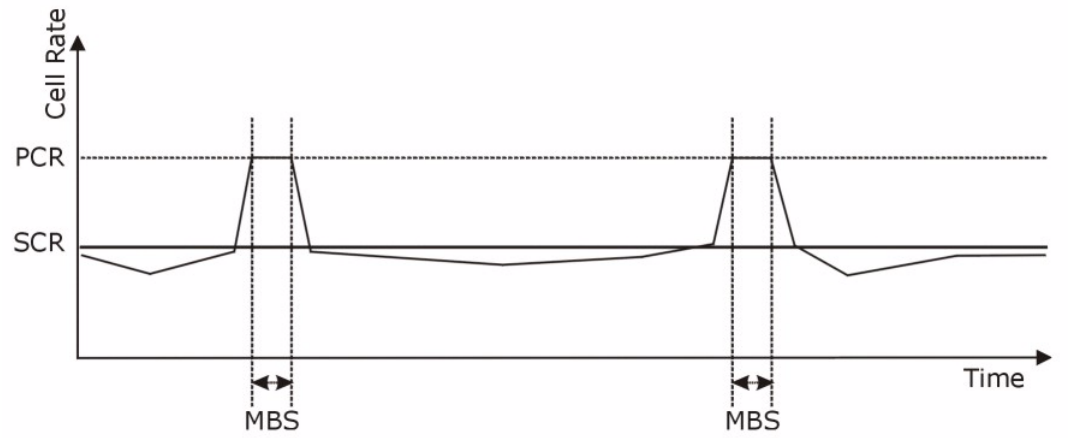
SCR (Sustained Cell Rate — Поддерживаемая скорость ячеек) — это средняя скорость ячеек каждого источника пульсирующего трафика. Она определяет максимальную среднюю скорость, с которой ячейки могут передаваться по виртуальному соединению. Поддерживаемая скорость ячеек не может быть больше, чем скорость 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. 16 Пример ATM QoS



6.3.7 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 ATM (Variable Bit Rate — Переменная скорость передачи) 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 пакетной передачи данных. Но при использовании UBR не гарантируется величина пропускной способности, и трафик передается, только когда сеть имеет ресурсы. Примером применения UBR является фоновая передача файлов.

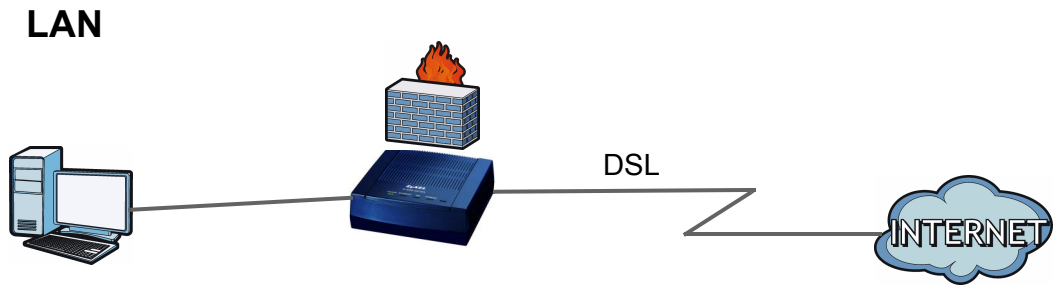
7

Настройка LAN

7.1 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.

Используйте экран LAN для помощи в настройке сервера DHCP локальной сети и для управления IP-адресами.



7.1.1 Что можно сделать на экранах LAN

- Используйте экран **LAN** (Разд. 7.2 на с. 68) для установки IP-адреса LAN и маски подсети вашего устройства ZyXEL. На этом экране можно также редактировать RIP, многоадресные рассылки и настройки DHCP вашего устройства P660.
- Используйте экран **DHCP IP Pool Summary** (Разд. 7.2.1 на с. 71) для проверки IP- и MAC-адресов компьютеров вашей локальной сети LAN.

7.1.2 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 встроенный в P660 сервер DHCP (протокол динамической конфигурации узла) присваивает вашему компьютеру или другому сетевому устройству IP-адрес, маску подсети, DNS и другую информацию о маршрутизации.

RIP

RIP (Протокол обмена информацией о маршрутизации) позволяет маршрутизатору обмениваться информацией о маршрутизации с другими маршрутизаторами.

Многоадресная рассылка

Обычно передача пакетов IP 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 фильтрацию 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

См. Разд. 7.3 на с. 71 для поиска технической вводной информации о LAN.

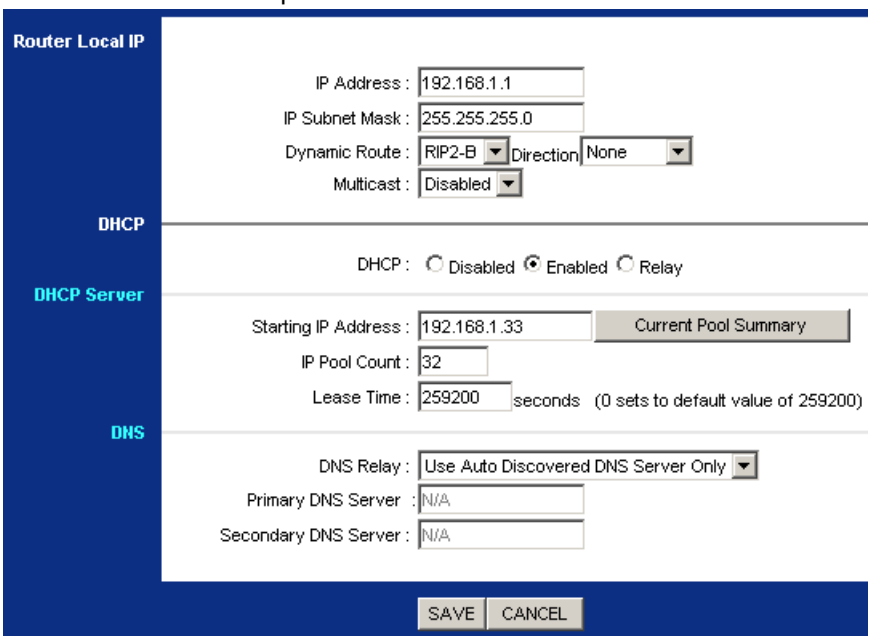
7.2 Экран LAN

Этот экран используется для настройки локальной сети LAN. Нажмите **Interface Setup > LAN**, чтобы открыть приведенный ниже экран.

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 P660.
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 **SAVE** для сохранения настроек.

Рис. 17 Interface Setup > LAN



В приводимой ниже таблице даны описания полей этого экрана.

Табл. 13 Interface Setup > LAN

ПОЛЕ	ОПИСАНИЕ
Router Local IP	
IP Address	Введите IP-адрес LAN, который вы хотите присвоить устройству P660 в десятичном виде с разделительными точками, например, 192.168.1.1 (установленный изготовителем по умолчанию).
IP Subnet Mask	Введите маску подсети вашей сети в десятичном виде с разделительными точками, например, 255.255.255.0 (установлена изготовителем по умолчанию). Ваше устройство P660 автоматически подсчитает маску подсети на основании введенного вами IP-адреса, поэтому не следует вносить изменения в это поле, если для этого нет особых указаний.
Dynamic Route	RIP (Протокол обмена информацией о маршрутизации) позволяет маршрутизатору обмениваться информацией о маршрутизации с другими маршрутизаторами. Выберите версию RIP из **RIP1**, **RIP2-B** и **RIP2-M**.
Direction	Используйте это поле для управления объема информацией о маршрутизации, которую устройство P660 передает и принимает по подсети. Выберите направление RIP из **None**, **Both**, **In Only** и **Out Only**.
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 — это протокол сетевого уровня, используемый для установления принадлежности к группе многоадресной рассылки. Устройство P660 поддерживает **IGMP v1**, **IGMP v2** и **IGMP v3**. Выберите **Disabled** для отключения этой функции.

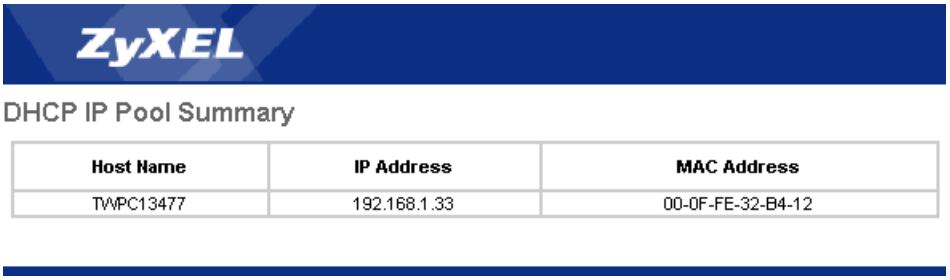
Табл. 13 Interface Setup > LAN

ПОЛЕ	ОПИСАНИЕ
DHCP	
DHCP	При установке **Enabled** ваше устройство P660 может присваивать IP-адреса, IP-шлюз по умолчанию и серверы DNS операционным системам, поддерживающим DHCP-клиент. Если установлено **Disabled**, то функция сервера DHCP будет отключена. Если установлено значение **Relay**, то устройство P660 выступает в качестве фиктивного DHCP-сервера и передает запросы и ответы между удаленным сервером и клиентами.
DHCP Server	
Starting IP Address	Это поле определяет первый из непрерывных адресов в пуле непрерывных IP-адресов.
Current Pool Summary	Нажмите эту кнопку для отображения сводной таблицы диапазона непрерывных IP-адресов. Более подробную информацию см. в Разд. 7.2.1 на с. 71. В P660 установлен диапазон IP-адресов клиентов DHCP (диапазон DHCP). См. характеристики устройства в приложениях. Не присваивайте статические IP-адреса из диапазона DHCP компьютерам в вашей локальной сети.
IP Pool Count	В этом поле задается размер пула непрерывных IP-адресов.
Lease Time	Период времени в течение которого можно использовать назначенные сервером DHCP адреса. DHCP автоматически присваивает IP-адреса клиентам в момент их входа в систему. DHCP централизует управление IP-адресами на центральных компьютерах, где работает программа сервера DHCP. DHCP дает в аренду адреса на некоторый период времени, что означает, что прошлые адреса используются заново и доступны для будущих назначений в других системах.
DNS	
DNS Relay	Выберите **Auto Discovered DNS Server Only**, если ваш Интернет-провайдер предоставляет динамическую информацию о сервере DNS (а также IP-адрес WAN устройства P660). Выберите **User Discovered DNS Server Only**, если у вас есть IP-адрес сервера DNS. Следует указать основной и дополнительный серверы DNS в указанных ниже полях.
Primary DNS Server	Введите IP-адрес для основного сервера DNS.
Secondary DNS Server	Введите IP-адрес для дополнительного сервера DNS.
DHCP Server IP for Relay Agent	Это поле отображается только при выборе **Relay** в поле **DNS Relay**. Введите в этом поле IP-адрес фактического удаленного сервера DHCP.
SAVE	Нажмите эту кнопку для сохранения своих изменений.
CANCEL	Нажмите эту кнопку для восстановления ранее заданных настроек.

7.2.1 Сводный экран диапазона IP-адресов сервера DHCP

Эта таблица позволяет увидеть IP-адреса и MAC-адреса индивидуальных компьютеров вашей локальной сети LAN. На экране **Interface Setup > LAN** нажмите кнопку **Current Pool Summary**, чтобы открыть следующий экран.

Рис. 18 Interface Setup > LAN > DHCP IP Pool Summary



В приводимой ниже таблице даны описания полей этого экрана.

Табл. 14 Interface Setup > LAN > DHCP IP Pool Summary

ПОЛЕ	ОПИСАНИЕ
Host Name	В этом поле отображается имя компьютера, который получает IP-адрес из устройства P660.
IP Address	В этом поле отображается IP-адрес компьютера, который получает IP-адрес из устройства P660.
MAC Address	В этом поле отображается MAC-адрес компьютера, который получает IP-адрес из устройства P660.

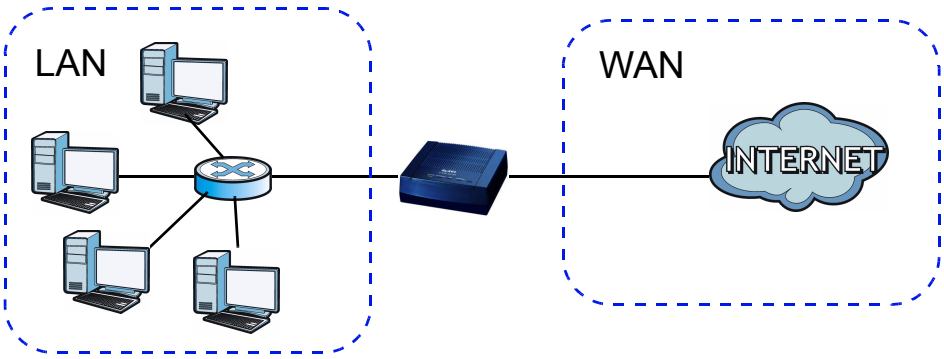
7.3 Техническое руководство LAN

В этом разделе приводится некоторая вводная техническая информация о темах данной главы.

7.3.1 Локальные, глобальные сети и устройство ZyXEL

Фактическое физическое соединение определяет, являются ли порты P660 портами локальной или глобальной сети. Существуют две отдельные IP-сети, одна внутренняя локальная сеть (LAN), другая внешняя глобальная сеть (WAN), как показано ниже.

Рис. 19 Локальные и глобальные IP-адреса



7.3.2 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 P660 как сервер DHCP или отключить эту функцию. При работе в режиме сервера P660 предоставляет клиентам конфигурацию TCP/IP. Если вы отключаете сервер DHCP, то необходимо иметь в LAN другой сервер DHCP, в противном случае придется конфигурировать компьютеры вручную.

7.3.3 Адреса сервера DNS

Служба DNS (Domain Name System — Система имен доменов) выполняет преобразование доменного имени в соответствующий IP-адрес и наоборот. Сервер DNS играет крайне важную роль, так как без него нужно было бы точно знать IP-адрес каждого компьютера, к которому нужно получить доступ. Адреса сервера DNS, которые задаются при настройке DHCP, передаются клиентским машинам вместе с назначенным IP-адресом и маской подсети.

Существует два способа распространения адресов серверов DNS Интернет-провайдером.

- Интернет-провайдер сообщает адреса серверов DNS, обычно в виде информационного листка при оформлении подписки. Если Интернет-провайдер назначает адреса серверов DNS, введите их в поля **Primary** и **Secondary DNS Server**.
- 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 P660 поддерживает расширения IPCP сервера DNS посредством функции прокси-сервера DNS.

  Если DHCP установлен на **Relay**, то устройство P660 сообщает DHCP-клиентам, что оно само является сервером DNS. Когда компьютер посылает запрос DNS на устройство P660, то устройство P660 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 работает только тогда, когда Интернет-провайдер использует DNS-расширения IPCP. Это не означает, что можно не включать серверы DNS в настройки DHCP при любых обстоятельствах. Если ваш Интернет-провайдер дает вам адреса серверов DNS в явной форме, то удостоверьтесь, что вы вводите их IP-адреса.

7.3.4 Настройка TCP/IP локальной сети

P660 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.

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

Если Интернет-провайдер не предоставляет явным образом сетевой IP-адрес, то вероятнее всего вы имеете учетную запись одиночного пользователя, и Интернет-провайдер назначает при установлении соединения динамический IP-адрес. В этом случае рекомендуется выбрать IP-адрес из диапазона 192.168.0.0 – 192.168.255.0 и включить в устройство P660 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). Иными словами, первые три числа задают номер сети, а остальные определяют конкретный компьютер в этой сети.

Выбрав номер сети, выберите для P660 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. P660 автоматически рассчитывает маску подсети для заданного IP-адреса. Нельзя изменять маску подсети, вычисленную P660, без прямых указаний к этому.

IP-адреса для частных сетей

Каждый компьютер в сети Интернет должен иметь уникальный адрес. Если сеть изолирована от Интернет, напр., 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».

7.3.5 Настройка RIP

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

- **Both —** устройство P660 осуществляет периодическую широковещательную рассылку своей маршрутной таблицы и полученных данных RIP.
- **In Only —** устройство P660 не посылает пакеты RIP, но принимает все входящие пакеты RIP.
- **In Only —** устройство P660 посылает пакеты RIP, но не принимает никакие входящие пакеты RIP.
- **None —** устройство P660 не посылает пакеты RIP и игнорирует все входящие пакеты RIP.

Поле **Version** управляет форматом и методом широковещательной рассылки пакетов RIP, которые рассылает устройство P660 (оба формата распознаются при приеме). Формат RIP-1 является общепринятым; но формат RIP-2 содержит больше информации. Для большинства сетей подходит RIP-1, если только сеть не имеет какой-либо специфической топологии.

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

7.3.6 Многоадресная рассылка

Обычно передача пакетов IP 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 фильтрацию 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 назначен ни одной группе и используется компьютерами, осуществляющими многоадресную рассылку IP. Адрес 224.0.0.1 используется для запросов и назначается постоянной группе, в которую входят все IP хост-машины (включая шлюзы). Для участия в IGMP хост-машина должна принадлежать к группе 224.0.0.1. Адрес 224.0.0.2 назначается группе маршрутизаторов, участвующих в многоадресной рассылке.

Устройство P660 поддерживает IGMP версии 1 (**IGMP-v1**), IGMP версии 2 (**IGMP-v2**) и IGMP версии 3 (**IGMP-v3**). При запуске устройство P660 запрашивает все непосредственно подключенные сети о принадлежности к группе. После получения информации устройство P660 периодически обновляет ее. В устройстве P660 многоадресную рассылку IP можно включить/отключить на интерфейсах LAN и/или WAN с помощью Web-конфигуратора (**LAN**; **WAN**). Для отключения многоадресной рассылки IP на этих интерфейсах выберите **None**.

Часть IV
Дополнительные настройки

8

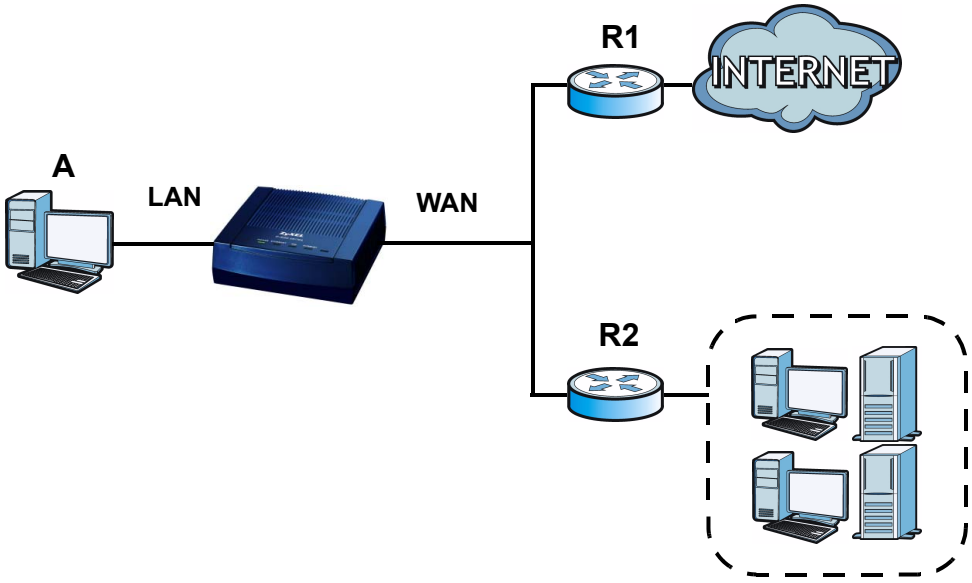
Статический маршрут

8.1 Обзор

Маршрутизатор P660 обычно использует заданный по умолчанию шлюз для маршрутизации исходящего трафика от компьютеров, находящихся в локальной сети, в Интернет. Чтобы маршрутизатор устройства P660 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 P660. Маршрутизатор устройства P660 направляет большую часть трафика от компьютера **A** в Интернет через основной шлюз устройства P660, заданный по умолчанию (**R1**). Создается один статический маршрут для подключения к службам, предоставляемым Интернет-провайдером за маршрутизатором **R2**.

Рис. 20 Пример топологии статической маршрутизации



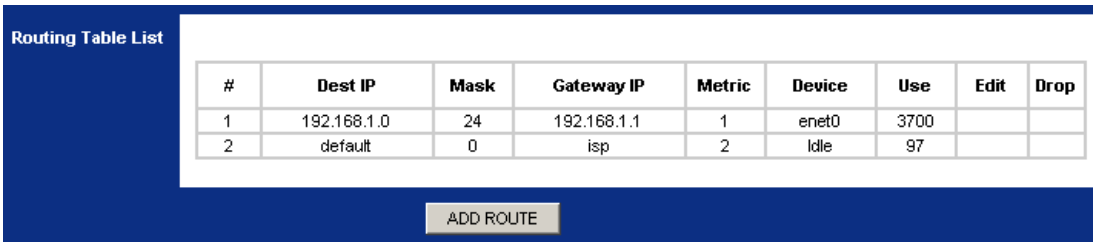
8.1.1 Что можно сделать на экранах статического маршрута

- Используйте экран **Routing Table List** (Разд. 8.2 на с. 80) для просмотра статических маршрутов в устройстве P660.
- Используйте экран **Static Route** (Разд. 8.2.1 на с. 81) для добавления и редактирования правил статической маршрутизации в устройстве P660.

8.2 Экран списка маршрутных таблиц

Используйте этот экран для просмотра правил статической маршрутизации. Нажмите **Advanced Setup > Routing**, чтобы открыть приведенный ниже экран.

Рис. 21 Advanced Setup > Routing Table List



В приводимой ниже таблице даны описания полей этого экрана.

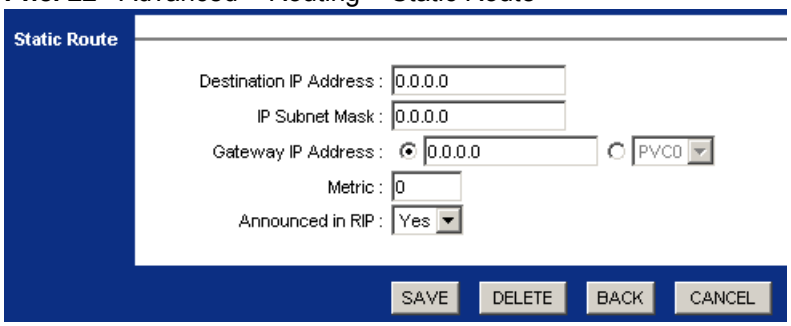
Табл. 15 Advanced Setup > Routing Table List

ПОЛЕ	ОПИСАНИЕ
#	Номер конкретного маршрута.
Dest IP	Данный параметр определяет IP-адрес сети конечного адресата. Маршрутизация всегда основывается на сетевом номере.
Mask	Данный параметр определяет маску подсети конечного назначения для IP-сети.
Gateway IP	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.
Metric	В этом поле отображается приоритет каждого маршрута устройства P660.
Device	Сетевой интерфейс данного маршрута.
Use	Количество раз, которое использовался маршрут.
Edit	Нажмите эту кнопку для перехода к экрану, где можно изменить параметры статического маршрута P660. Маршруты по умолчанию редактировать нельзя.
Drop	Щелкните на этом поле для удаления статического маршрута в устройстве P660. Маршруты по умолчанию удалять нельзя.
ADD ROUTE	Щелкните на этом поле для добавления нового статического маршрута в устройстве P660.

8.2.1 Экран статических маршрутов

Используйте это окно для настройки параметров статического маршрута. Выберите указатель статического маршрута и нажмите **Edit** или кнопку **ADD ROUTE** на экране **Routing Table List**. При этом откроется показанный ниже экран.

Рис. 22 Advanced > Routing > Static Route



В приводимой ниже таблице даны описания полей этого экрана.

Табл. 16 Advanced > Static Route: Edit

ПОЛЕ	ОПИСАНИЕ
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 в это поле IP-маску подсети.
Gateway IP Address	Можно задать статический маршрут, используя IP-адрес шлюза или номер PVC. 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. Выберите PVC из разворачивающегося списка для установки статического маршрута. Более подробные сведения о настройке PVC см. в Разд. 6.2 на с. 53.
Metric	В этом поле устанавливается приоритет маршрута среди маршрутов, используемых устройством P660. Метрика определяет «стоимость передачи». Маршрутизатор определяет лучший маршрут для передачи, выбирая траекторию с наименьшей «стоимостью». Маршрутизация RIP использует счетчик переходов по сети в качестве своего рода единицы стоимости, с минимальным значением равным «1» для прямого соединения. Число должно находиться в диапазоне от «1» до «15»; число больше, чем «15» означает, что связь отсутствует. Чем меньше число, тем меньше «стоимость».
Announced in RIP	RIP (Протокол обмена информацией о маршрутизации) позволяет маршрутизатору обмениваться информацией о маршрутизации с другими маршрутизаторами. Выберите **Yes**, чтобы разрешить RIP передавать информацию об этом статическом маршруте в другие маршрутизаторы. Выберите **No**, чтобы не разрешать RIP передавать информацию об этом статическом маршруте в другие маршрутизаторы.
SAVE	Нажмите эту кнопку для сохранения своих изменений.
DELETE	Нажмите эту кнопку для удаления статического маршрута.
BACK	Нажмите эту кнопку для возврата к предыдущему экрану без сохранения.
CANCEL	Нажмите эту кнопку для восстановления ранее заданных настроек.

9

Трансляция сетевых адресов (NAT)

9.1 Обзор

В этой главе рассказывается, как настроить функцию NAT в P660. NAT (Network Address Translation/Трансляция сетевых адресов — NAT, RFC 1631) — это преобразование IP-адреса хоста в пакете, напр., адрес источника исходящего пакета, используемого в одной сети, в другой IP-адрес, известный в другой сети.

9.1.1 Что можно сделать на экранах NAT

- Используйте экран **NAT** (Разд. 9.2 на с. 84) для настройки параметров NAT.
- Используйте экран **DMZ** (Разд. 9.3 на с. 85) для настройки параметров DMZ.
- Используйте экран **Virtual Server** (Разд. 9.4 на с. 86) для пересылки на сервер(ы) вашей локальной сети входных запросов на услугу.
- Используйте экран **IP Address Mapping** (Разд. 9.5 на с. 89) для изменения параметров отображения адреса P660.

9.1.2 Что нужно знать о NAT

Внутренний/Внешний

«Внутренний/внешний» означает расположение узла относительно устройства P660, например, компьютеры ваших абонентов являются внутренними узлами, тогда как веб-серверы Интернета являются внешними узлами.

Общедоступный/Локальный

Определение «общедоступный/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 общедоступный 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 хосту.

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.

Одиночный IP-адрес относительно NAT

Одиночный IP-адрес — это реализация в операционной системе ZyNOS подмножества NAT, которое поддерживает два типа отображения: **Many-to-One** и **Server**. Устройство P660 поддерживает также многочисленные IP-адреса для отображения многочисленных общедоступных IP-адресов для многочисленных частных IP-адресов LAN клиентов или серверов с использованием различных типов отображения.

- Выберите **Single IP** если имеется только один общедоступный IP-адрес в глобальной сети для вашего устройства P660.
- Выберите **Multiple IPs** если имеется несколько общедоступных IP-адресов в глобальной сети для вашего устройства P660.

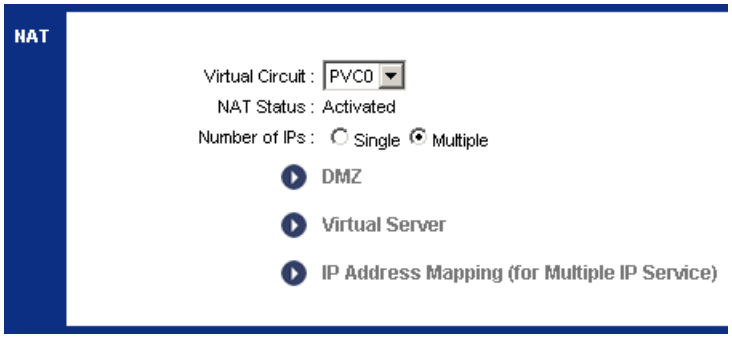
Дополнительные сведения

См. Разд. 9.6 на с. 91 для поиска технической вводной информации о NAT.

9.2 Экран NAT

Используйте этот экран для настройки NAT в каждом канале PVC. Нажмите **Advanced Setup > NAT**, чтобы открыть приведенный ниже экран.

Рис. 23 Advanced Setup > NAT



В приводимой ниже таблице даны описания полей этого экрана.

Табл. 17 Network > NAT > General

ПОЛЕ	ОПИСАНИЕ
Virtual Circuit	Выберите из разворачивающегося списка в окне виртуальный канал (PVC), который вы хотите настроить.
NAT Status	Это поле указывает, включена ли NAT. Более подробные сведения о работе NAT см. Разд. 6.2 на с. 53.
Number of IPs	Выберите **Single** если имеется только один общедоступный IP-адрес в глобальной сети для вашего устройства P660. Выберите **Multiple** если имеется несколько общедоступных IP-адресов в глобальной сети для вашего устройства P660.
DMZ	Нажмите эту кнопку для настройки параметров DMZ. Более подробную информацию см. в Разд. 9.3 на с. 85.
Virtual Server	Нажмите эту кнопку для установки правил переадресации порта для вашего устройства P660. Более подробную информацию см. в Разд. 9.4 на с. 86.
IP Address Mapping	Это поле отображается только при выборе **Multiple** в поле **Number of IPs**. Нажмите эту кнопку для установки правил отображения адресов для вашего устройства P660. Более подробную информацию см. в Разд. 9.5 на с. 89.

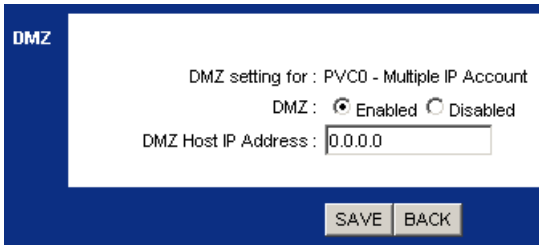
9.3 Экран DMZ

Демилитаризованная зона (DMZ) предлагает путь к общедоступным серверам (Web, e-mail, FTP и т. д.) видимый для внешнего мира (при этом он по-прежнему остается защищенным от атак DoS (отказ от обслуживания) таких как переполнение SYN и Ping of Death). К этим общедоступным серверам возможен также доступ из защищенной LAN.

По умолчанию брандмауэр допускает трафик между WAN и DMZ, а трафик из DMZ в LAN отклоняется, но разрешен трафик из LAN в DMZ. У пользователей Интернета имеется доступ к хост-серверам в DMZ, но нет доступа к LAN, если не стоят специальные фильтры, настроенные администратором, или же если пользователь является санкционированным удаленным пользователем.

Используйте этот экран для настройки отдельных независимых сетей из LAN, в которой можно установить ваши серверы. Нажмите **Advanced Setup > NAT** > **DMZ**, чтобы открыть приведенный ниже экран.

Рис. 24 Advanced Setup > NAT > DMZ



В приводимой ниже таблице даны описания полей этого экрана.

Табл. 18 Advanced Setup > NAT > DMZ

ПОЛЕ	ОПИСАНИЕ
DMZ setting for	В этом поле отображается PVC, который вы хотите настроить.
DMZ	Используйте это поле для включения или отключения DMZ.
DMZ Host IP Address	Введите IP-адрес DMZ в десятичном виде с разделительными точками. ПРИМЕЧАНИЕ: Убедитесь, что IP-адреса LAN, WAN и DMZ находятся в раздельных подсетях.
SAVE	Нажмите эту кнопку для сохранения настроек.
BACK	Нажмите эту кнопку для возврата к предыдущему экрану без сохранения.

9.4 Экран виртуального сервера

Компьютеры в локальной сети LAN обычно имеют частный IP-адрес, присвоенный DHCP, на который закрыт прямой доступ непосредственно из глобальной сети WAN. Используйте этот экран, чтобы устройство P660 могло переадресовать трафик на серверы в LAN.

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.

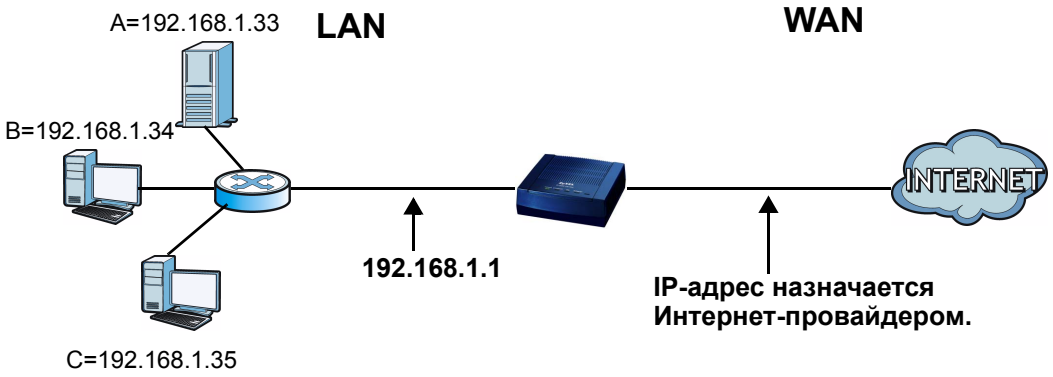
Чаще всего используют номера портов и службы, приведенные в Прил. D на с. 207. Дополнительную информацию по номерам портов можно получить в RFC 1700.

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.

9.4.1 Пример настройки серверов, расположенных после портов переадресации

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. 25 Пример: несколько серверов расположены за NAT



В таблице показаны все настройки из приведенного выше примера.

Табл. 19 Пример: несколько серверов расположены за NAT

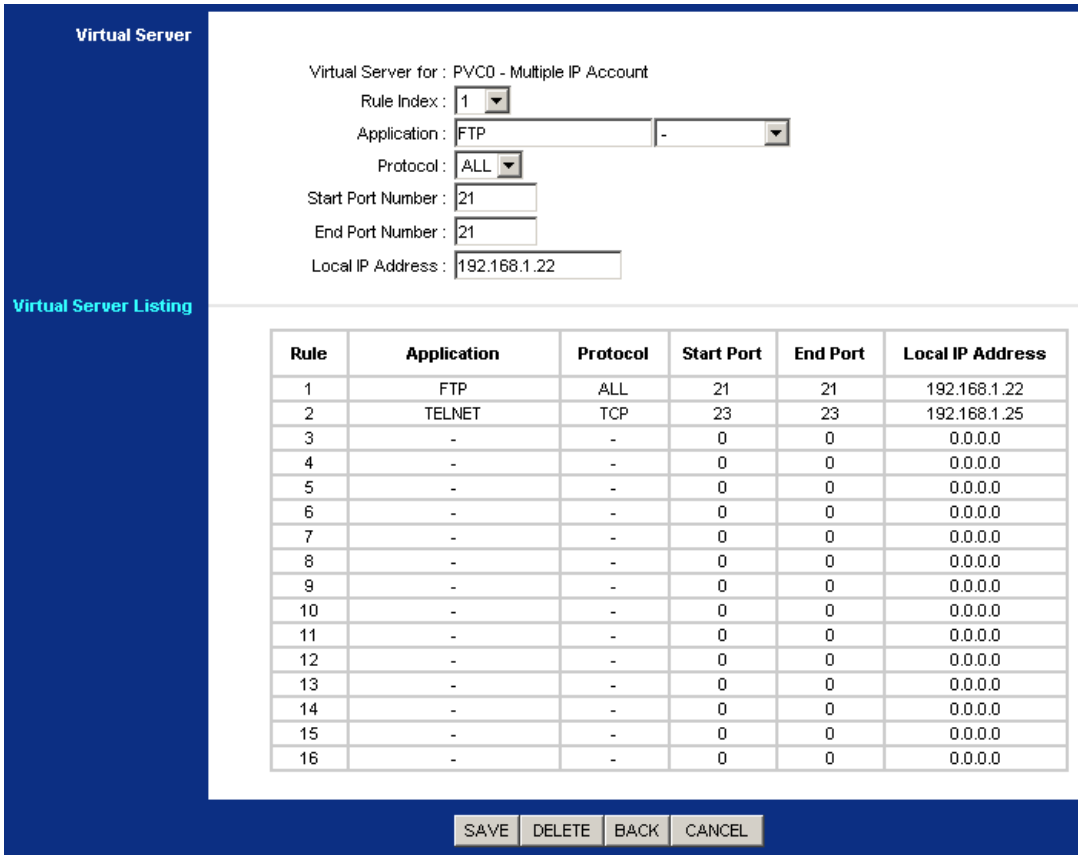
	СЕРВЕРЫ	ПОРТЫ	IP-СЕРВЕР ПО УМОЛЧАНИЮ
A	FTP	21-22	192.168.1.33
B	Telnet	23	192.168.1.34
C	SMTP	25	192.168.1.35

9.4.2 Настройка экрана виртуального сервера

Нажмите **Advanced Setup > NAT > Virtual Server**, чтобы открыть приведенный ниже экран.

См. Прил. D на с. 207 для справки по номерам портов, обычно используемых для конкретных служб.

Рис. 26 Advanced Setup > NAT > Virtual Server



В приводимой ниже таблице даны описания полей этого экрана.

Табл. 20 Advanced Setup > NAT > Virtual Server

ПОЛЕ	ОПИСАНИЕ
Virtual Server	
Virtual Server for	Канал PVC, который будет использоваться данным виртуальным сервером.
Rule Index	Выберите указатель правила из разворачивающегося списка.
Application	Используйте разворачивающийся список для выбора типа сервера, использующегося в вашей сети. Приложения или службы определяются своим протоколом (TCP или UDP) и номером порта. Например, порт 80 TCP определяет трафик в сети (HTTP). Если у вас в сети имеется веб-сервер, необходимо переадресовать приложения HTTP (TCP порт 80) на IP-адрес сервера. Доступные варианты: **FTP**, **SSH**, **TELNET**, **SMTP**, **HTTP_Server**, **POP3**, **HTTPS**, **T.120**, **H.323**, **PPTP**, **pcAnywhere**, **VNC** и **CUSeeMe**.
Protocol	Используйте разворачивающийся список для выбора IP-порта (**ALL**, **TCP** или **UDP**), определяющего вашу службу.

Табл. 20 Advanced Setup > NAT > Virtual Server

ПОЛЕ	ОПИСАНИЕ
Start Port Number	Введите в это поле номер порта. Для переадресации трафика только одного порта, введите его номер еще раз в поле **End Port Number**. Для переадресации трафика серии портов введите в это поле номер первого порта, а в поле **End Port Number** — номер последнего порта.
End Port Number	Введите в это поле номер порта. Для переадресации трафика только одного порта, введите его номер в поле **Start Port Number**, а затем введите этот же номер еще раз в это поле. Для переадресации трафика серии портов введите номер последнего порта серии портов, которая начинается с номера порта, установленного в поле **Start Port Number**.
Local IP Address	Введите в это поле внутренний IP-адрес сервера.
Virtual Server Listing	
Rule	Порядковый номер правила.
Application	Здесь отображается имя службы.
Protocol	IP-порт.
Start Port	Номер первого порта, определяющего службу.
End Port	Номер последнего порта, определяющего службу.
Local IP Address	IP-адрес сервера.
SAVE	Нажмите эту кнопку для сохранения своих изменений.
DELETE	Нажмите эту кнопку для удаления данного правила.
BACK	Нажмите эту кнопку для возврата к предыдущему экрану без сохранения.
CANCEL	Нажмите эту кнопку для восстановления ранее заданных настроек.

9.5 Экран отображения IP-адресов

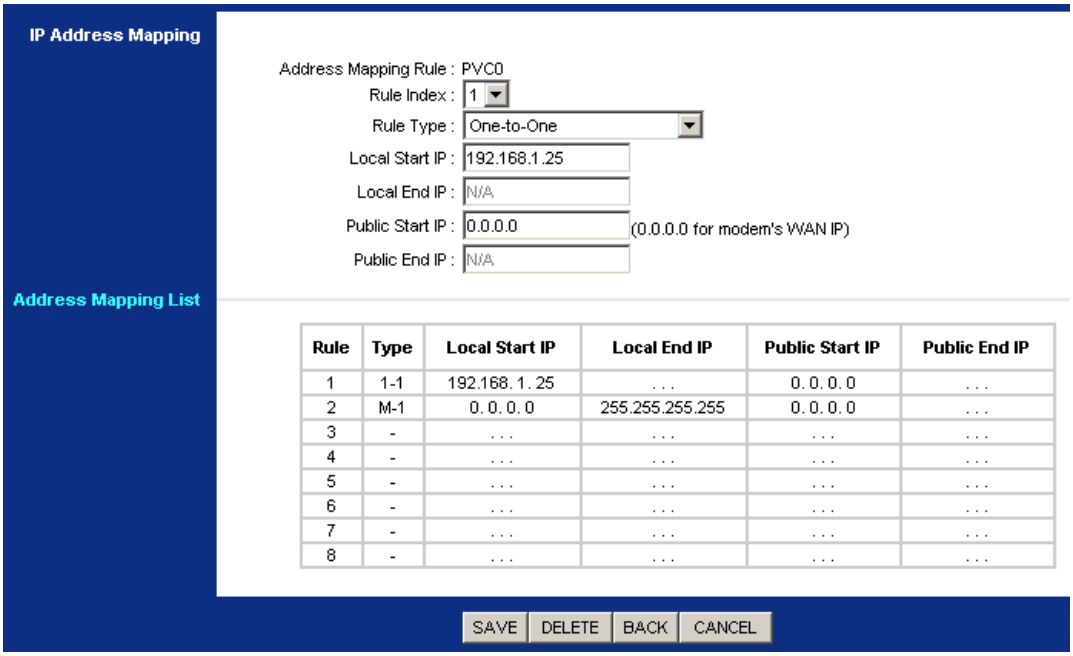
Настройте этот экран, если у вас имеются многочисленные IP-адреса от вашего Интернет-провайдера и если вы хотите отобразить их для частных IP-адресов вашей LAN.

Экран **Address Mapping** доступен только в том случае, если вы выбрали **Multiple** для **Number of IPs** на экране **NAT**.

Порядок следования правилам имеет большое значение, так как устройство P660 применяет правила в установленном порядке. Когда текущий пакет соответствует какому-либо правилу устройства, P660 выполняет соответствующее действие и игнорирует остальные правила.

Используйте этот экран для изменения настройки отображения адреса вашего устройства P660. Нажмите **Advanced Setup > NAT > IP Address Mapping**, чтобы открыть приведенный ниже экран.

Рис. 27 Advanced Setup > NAT > IP Address Mapping



В приводимой ниже таблице даны описания полей этого экрана.

Табл. 21 Network > NAT > Address Mapping

ПОЛЕ	ОПИСАНИЕ
IP Address Mapping	
Address Mapping Rule	Правила, задаваемые на этом экране, относятся только к данному каналу PVC.
Rule Index	Выберите указатель правила из разворачивающегося списка.
Rule Type	Выберите тип отображения портов из следующих вариантов. **One-to-One**: В этом режиме один локальный IP-адрес преобразуется в один общедоступный IP-адрес. Следует отметить, что номера портов при преобразовании NAT типа One-to-one не изменяются. **Many-to-One**: В этом режиме многочисленные локальные IP-адреса преобразуется в один общедоступный IP-адрес. Это эквивалент функции **Single IP**, которая поддерживалась предыдущими моделями маршрутизаторов ZyXEL. **Many-to-Many Overload**: В этом режиме многочисленные локальные IP-адреса преобразуется в совместные общедоступные IP-адреса. **Many-to-Many No Overload**: В этом режиме каждый локальный IP-адрес преобразуется в уникальные общедоступные IP-адреса. **Server**: Этот режим позволяет назначить внутренние серверы различного типа в обход NAT и открыть к ним доступ со стороны внешнего мира.
Local Start IP	Начальный локальный IP-адрес. Локальные IP-адреса недоступны (**N/A**) для типа отображения портов **Server**.
Local End IP	Конечный локальный IP-адрес. 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**.

Табл. 21 Network > NAT > Address Mapping (продолжение)

ПОЛЕ	ОПИСАНИЕ
Public Start IP	Начальный общедоступный IP-адрес. Если вы используете динамический IP-адрес, назначаемый Интернет-провайдером, введите в это поле 0.0.0.0.
Public End IP	Конечный общедоступный IP-адрес. В этом поле отображается **N/A** для типов отображения **One-to-One**, **Many-to-One** и **Server**.
Address Mapping List	
Rule	Порядковый номер правила.
Type	**1-1**: В этом режиме один локальный IP-адрес преобразуется в один общедоступный IP-адрес. Следует отметить, что в режиме отображения NAT один-к-одному номера портов не изменяются. **M-1**: В этом режиме несколько локальных IP-адресов преобразуются в один общедоступный IP-адрес. Это эквивалент функции **Single IP**, которая поддерживалась предыдущими моделями маршрутизаторов ZyXEL. **M-M Ov** (Overload): В этом режиме несколько локальных IP-адресов преобразуются в коллективные общедоступные IP-адреса. **MM No** (No Overload): В этом режиме каждый локальный IP-адрес преобразуется в уникальные общедоступные IP-адреса. **Server**: Этот режим позволяет назначить внутренние серверы различного типа в обход NAT и открыть к ним доступ со стороны внешнего мира.
Local Start IP	Начальный внутренний локальный IP-адрес. Локальные IP-адреса недоступны (**N/A**) для типа отображения портов **Server**.
Local End IP	Конечный внутренний локальный IP-адрес. 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**.
Public Start IP	Начальный внутренний общедоступный IP-адрес. 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**.
Public End IP	Конечный внутренний общедоступный IP-адрес. В этом поле отображается **N/A** для типов отображения **One-to-One**, **Many-to-One** и **Server**.
SAVE	Нажмите эту кнопку для сохранения своих изменений.
DELETE	Нажмите эту кнопку для удаления данного правила.
BACK	Нажмите эту кнопку для возврата к предыдущему экрану без сохранения.
CANCEL	Нажмите эту кнопку для восстановления ранее заданных настроек.

9.6 Техническое руководство NAT

В этом разделе содержится дополнительная информация о NAT.

9.6.1 Определения NAT

«Внутренний/внешний» означает расположение узла относительно устройства P660, например, компьютеры ваших абонентов являются внутренними узлами, тогда как веб-серверы Интернета являются внешними узлами.

Определение «общедоступный/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 общедоступный 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 «общедоступный/локальный» относится к IP-адресу узла в пакете. Таким образом, внутренний локальный адрес — это IP-адрес внутреннего узла в пакете, когда пакет находится в пределах локальной сети, тогда как внутренний общедоступный адрес — это IP-адрес того же внутреннего узла, когда пакет находится в глобальной сети. В следующей таблице приведена сводная информация.

Табл. 22 Определения NAT

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

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

9.6.2 Назначение NAT

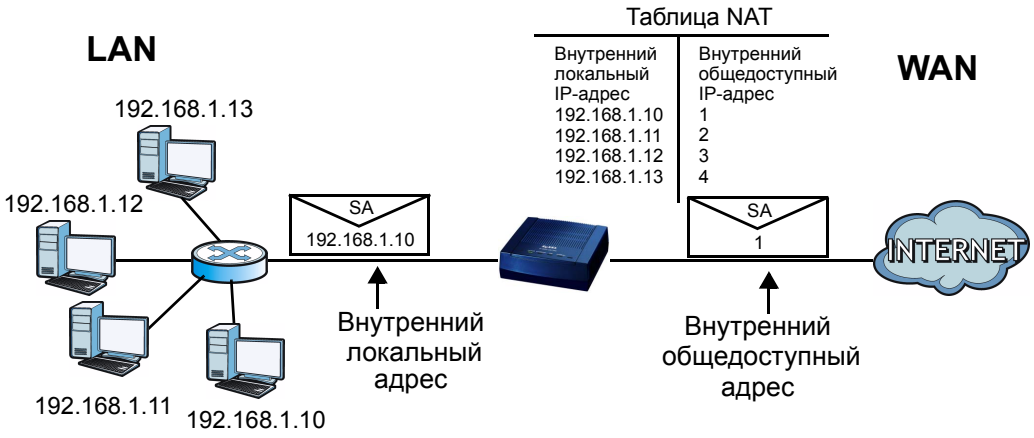
В простейшем случае NAT изменяет IP-адрес источника в пакете, принятом от абонента (внутренний локальный адрес) на другой (внутренний общедоступный адрес) перед передачей пакета в глобальную сеть WAN. При получении ответа, NAT преобразовывает адрес назначения (внутренний общедоступный адрес) обратно во внутренний локальный адрес перед пересылкой исходному внутреннему хосту.

Общедоступные 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 серверы не определены, NAT дает возможность работать под защитой брандмауэра. Если серверы не установлены, устройство P660 отфильтровывает все входящие запросы, таким образом предотвращая зондирование вашей сети злоумышленниками.

9.6.3 Как работает NAT

Каждый пакет содержит два адреса — адрес источника и адрес назначения. Для исходящих пакетов, внутренний локальный адрес является адресом источника в локальной сети LAN, а внутренний общедоступный адрес — адресом источника в глобальной сети WAN. Для входящих пакетов внутренний локальный адрес — это адрес получателя в локальной сети, а внутренний общедоступный адрес — адрес получателя в глобальной сети. NAT преобразовывает частные (локальные) IP-адреса в уникальные глобальные, что необходимо для связи с узлами в других сетях. NAT заменяет исходный IP-адрес источника (и номера портов источника TCP или UDP на отображение много-к-одному и много-ко-многим с перекрытием) в каждом пакете и затем пересылает его в Интернет. P660 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. 28 Как работает NAT



10

Качество услуги (QOS)

10.1 Обзор

Используйте экран **QoS** для настройки вашего устройства P660, чтобы использовать QoS для управления трафиком.

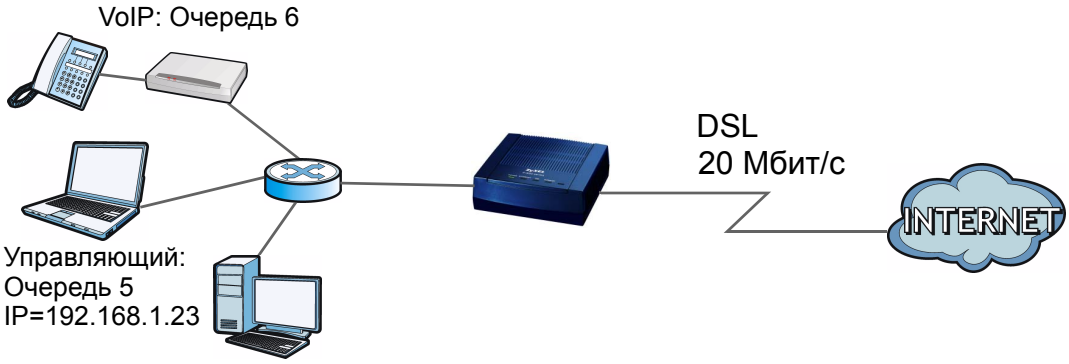
Качество услуги (QoS) относится как к возможности сети передавать данные с минимальной задержкой, так и к сетевым методам управления полосой частот. QoS позволяет устройству P660 группировать и назначать приоритет трафику приложений и обеспечивать точную настройку производительности сети.

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 P660 присваивает каждому 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.

На приведенном ниже рисунке ваше подключение к Интернету имеет скорость передачи данных 20 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 P660.

Рис. 29 Пример QoS



10.1.1 Что можно сделать на экранах QoS

- Используйте экран **QoS** (Разд. 10.2 на с. 97) для настройки параметров QoS в устройстве P660.
- Используйте экран **QoS Settings Summary** (Разд. 10.2.1 на с. 99) для проверки сводных правил и действий QoS, которые вы установили для устройства P660.

10.1.2 Что нужно знать о QoS

802.1p

QoS используется для установки приоритета для потоков трафика источник-адресат. Пакеты, находящиеся в одном потоке, имеют одинаковый приоритет. 802.1p — это способ управления трафиком в сети за счет группирования вместе одинаковых типов трафика и обработки каждого типа как класса. Можно использовать 802.1p для назначения разных приоритетов различным типам пакетов.

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

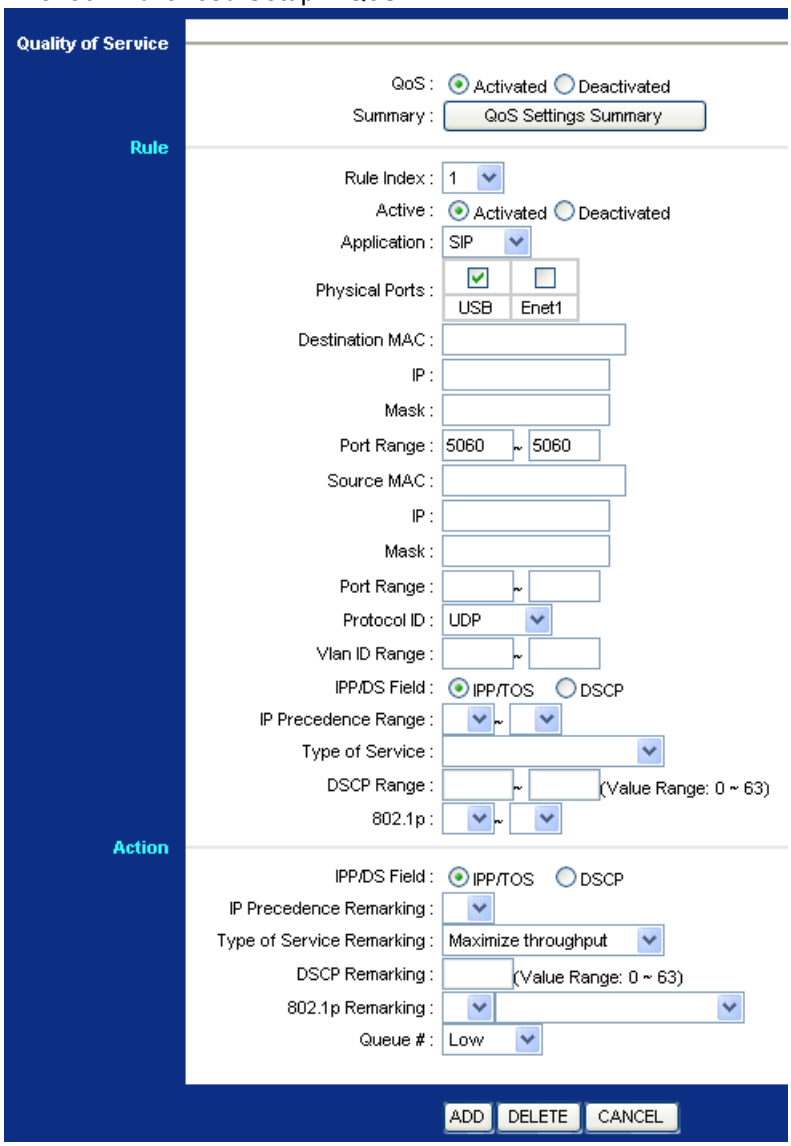
См. Разд. 10.3 на с. 100 для поиска технической вводной информации о QoS.

10.2 Экран QoS

Используйте этот экран для включения или отключения QoS, настройте ваше устройство P660, чтобы оно присваивало уровень приоритета трафику в соответствии с диапазоном портов, уровнем приоритета IEEE 802.1p и/или очередностью IP-адреса.

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

Рис. 30 Advanced Setup > QoS



В приводимой ниже таблице даны описания полей этого экрана.

Табл. 23 Advanced Setup > QoS

ПОЛЕ	ОПИСАНИЕ
Quality of Service	
QoS	Используйте это поле для включения QoS с целью улучшения производительности сети. Можно установить приоритет для трафика, который устройство P660 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.
Summary	Нажмите эту кнопку для открытия сводной таблицы с параметрами QoS. Более подробную информацию см. в Разд. 10.2.1 на с. 99.
Rule	
Rule Index	Выберите указатель правила из разворачивающегося списка.
Active	Используйте это поле для включения или отключения правила.
Application	Выберите приложение из раскрывающегося списка. Поля **Destination Port Range** и **Protocol ID** могут меняться в зависимости от типа выбранного приложения.
Physical Ports	Выберите **Enet1**, чтобы применить правило к порту Ethernet или выберите **USB**, чтобы использовать это правило для порта USB.
Destination MAC	Наберите здесь MAC-адрес назначения. После этого QoS будет применяться к трафику, содержащему этот MAC-адрес назначения. Оставьте это поле пустым, чтобы применить правило ко всем MAC-адресам.
IP	Введите IP-адрес назначения в десятичном виде с разделительными точками. После этого QoS будет применяться к трафику, содержащему IP-адрес назначения. Пустое поле IP-адреса означает любой IP-адрес.
Mask	Введите маску подсети получателя.
Port Range	Используйте значение по умолчанию, задаваемое выбранным приложением, или введите номер порта, к которому должно применяться правило.
Source MAC	Наберите здесь MAC-адрес источника. После этого QoS будет применяться к трафику, содержащему MAC-адрес источника. Оставьте это поле пустым, чтобы применить правило ко всем MAC-адресам.
IP	Введите IP-адрес источника в десятичном виде с разделительными точками. После этого QoS будет применяться к трафику, содержащему IP-адрес источника. Пустое поле означает любой IP-адрес источника.
Mask	Введите маску подсети источника.
Port Range	Введите номер порта, к которому должно применяться правило. 0 означает любой порт источника. См. Прил. D на с. 207 с указанием распространенных служб и номеров портов.
Protocol ID	Выберите тип протокола IP из разворачивающегося списка.
Vlan ID Range	Введите в этом поле идентификатор VLAN источника.
IPP/DS Field	Выберите **IPP/TOS**, чтобы указать диапазон IP-очередности и тип службы. Выберите **DSCP**, чтобы указать диапазон кода службы DiffServ Code Point (DSCP).
IP Precedence Range	Выберите диапазон от 0 до 7 для IP-очередности. Ноль — самый низкий приоритет, а семь — самый высокий.

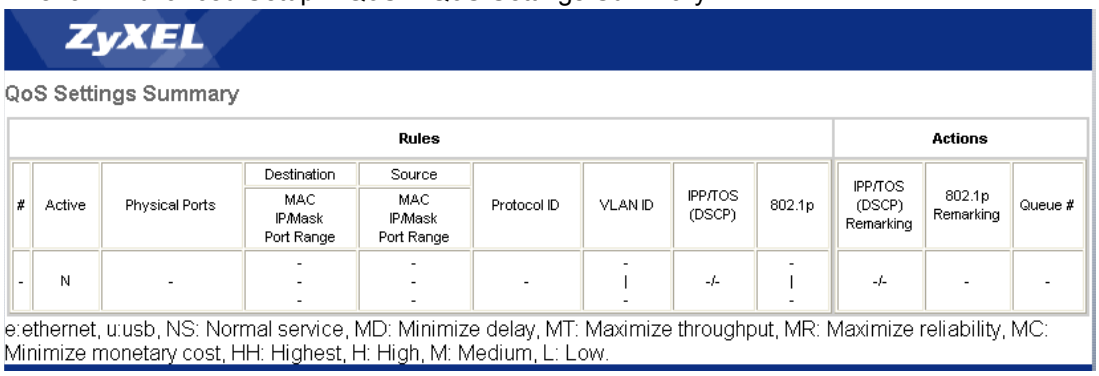
Табл. 23 Advanced Setup > QoS

ПОЛЕ	ОПИСАНИЕ
Type of Service	Выберите из данного разворачивающегося списка тип услуги. Доступные варианты: **Normal service**, **Minimize delay**, **Maximize throughput**, **Maximize reliability** и **Minimize monetary cost**.
DSCP Range	Укажите в этом поле номер DSCP от 0 до 63.
802.1p	Выберите из разворачивающегося списка уровень приоритета (от 0 до 7).
Action	
IPP/DS Field	Выберите **IPP/TOS**, чтобы указать диапазон IP-очередности и тип службы. Выберите **DSCP**, чтобы указать диапазон кода службы DiffServ Code Point (DSCP).
IP Precedence Remarking	Выберите от 0 до 7, чтобы переназначить IP-очередность для совпадающего трафика. Ноль — самый низкий приоритет, а семь — самый высокий.
Type of Service Remarking	Выберите тип службы, чтобы переназначить уровень приоритета для совпадающего трафика. Доступные варианты: **Normal service**, **Minimize delay**, **Maximize throughput**, **Maximize reliability** и **Minimize monetary cost**.
DSCP Remarking	Укажите номер DSCP от 0 до 63 и переназначьте уровень приоритета для совпадающего трафика.
802.1p Remarking	Выберите уровень приоритета (от 0 до 7), чтобы переназначить уровень приоритета для совпадающего трафика.
Queue #	Укажите тег очередности **Low**, **Medium**, **High** или **Highest** для совпадающего трафика. Трафик, которому присвоен более высокий номер очереди, передается при переполнении сети быстрее, чем для трафик с низким номером.
ADD	Нажмите эту кнопку для добавления данного правила.
DELETE	Нажмите эту кнопку для удаления данного правила.
CANCEL	Нажмите эту кнопку для восстановления ранее заданных настроек.

10.2.1 Сводный экран параметров QoS

Используйте этот экран для отображения сводки правил и действий, заданных для устройства P660. На экране **Advanced > QoS** нажмите кнопку **QoS Settings Summary**, чтобы открыть следующий экран.

Рис. 31 Advanced Setup > QoS > QoS Settings Summary



В приводимой ниже таблице даны описания полей этого экрана.

Табл. 24 Advanced Setup > QoS > QoS Settings Summary

ПОЛЕ	ОПИСАНИЕ
Rules	
#	Порядковый номер правила.
Active	Показывает, включено или отключено правило.
Physical Ports	Физический порт, к которому применяется правило.
Destination MAC and IP/Mask Port Ranges	Диапазон портов для MAC-адреса назначения и IP-адреса.
Source MAC and IP/Mask Port Ranges	Диапазон портов для MAC-адреса источника и IP-адреса.
Protocol ID	Идентификатор протокола, к которому применяется правило.
VLAN ID	Идентификатор VLAN, связанный с правилом.
IPP/TOS (DSCP)	Здесь показаны параметры IPP/TOS или DSCP.
802.1p	Уровень приоритета 802.1p.
Actions	
IPP/TOS (DSCP) Remarking	Устройство P660 переназначает значения приоритета в указанном поле для совпадающего трафика.
802.1p Remarking	Устройство P660 переназначает уровни приоритета в указанном поле для совпадающего трафика.
Queue #	Устройство P660 присваивает уровень очередности в указанном поле для совпадающего трафика.

10.3 Техническое руководство QoS

В этом разделе приводится некоторая вводная техническая информация о темах данной главы.

10.3.1 IEEE 802.1p

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. 25 Уровень приоритета IEEE 802.1p и тип трафика

УРОВЕНЬ ПРИОРИТЕТА	ТИП ТРАФИКА
Уровень 7	Обычно используется для управления сетевым трафиком, например, сообщениями о конфигурации маршуртизатора.
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).

Табл. 25 Уровень приоритета IEEE 802.1p и тип трафика

УРОВЕНЬ ПРИОРИТЕТА	ТИП ТРАФИКА
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).

10.3.2 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.

10.3.3 Автоматическое задание приоритета в очереди

Если включить QoS в устройстве P660, то устройство P660 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 P660. В устройстве P660, трафик, которому присваивается высокий приоритет очередности, движется быстрее, а трафик с низкими индексами очередности при переполнении останавливается.

Табл. 26 Отображение внутренних уровней 2 и 3 QoS

ПРИОРИТЕТ ОЧЕРЕДНОСТИ	УРОВЕНЬ 2	УРОВЕНЬ 3		
	ПРИОРИТЕТ ПОЛЬЗОВАТЕЛЯ IEEE 802.1P (ПРИОРИТЕТ ETHERNET)	ТИП УСЛУГИ (IP-ОЧЕРЕДНОСТЬ)	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	

Табл. 26 Отображение внутренних уровней 2 и 3 QoS

ПРИОРИТЕТ ОЧЕРЕДНОСТИ	УРОВЕНЬ 2	УРОВЕНЬ 3		
	ПРИОРИТЕТ ПОЛЬЗОВАТЕЛЯ IEEE 802.1P (ПРИОРИТЕТ ETHERNET)	ТИП УСЛУГИ (IP-ОЧЕРЕДНОСТЬ)	DSCP	ДЛИНА IP-ПАКЕТА (БАЙТ)
5	5	3	011110 011100 011010 011000	<250
6	6	4	100110 100100 100010 100000	
		5	101110 101000	
7	7	6	110000 111000	
		7		

11

ADSL

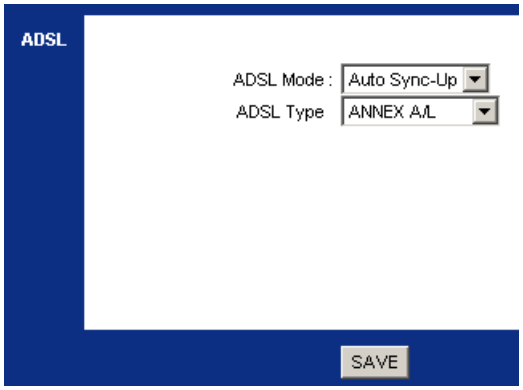
11.1 Обзор

В этой главе содержится информация о конфигурировании параметров ADSL для вашего устройства P660.

11.2 Экран ADSL

Используйте этот экран для выбора режима и типа ADSL для вашего устройства P660. Нажмите **Advanced Setup > ADSL**, чтобы открыть приведенный ниже экран.

Рис. 32 Advanced Setup > ADSL



В приводимой ниже таблице даны описания полей этого экрана.

Табл. 27 Advanced Setup > ADSL

ПОЛЕ	ОПИСАНИЕ
ADSL Mode	Выберите режим, поддерживаемый вашим Интернет-провайдером. Используйте **Auto Sync-Up**, если вы не знаете точно, какой режим следует выбрать. Устройство P660 осуществляет динамическую диагностику режима, поддерживаемого Интернет-провайдером, и выбирает для подключения наиболее совместимый режим. Другие варианты: **ADSL2+**, **ADSL2**, **G.DMT**, **T1.413** и **G.lite**.
ADSL Type	Выберите тип, поддерживаемый вашим Интернет-провайдером. Доступные варианты: **ANNEX A**, **ANNEX A/L**, **ANNEX M** и **ANNEX A/L/M**.
SAVE	Нажмите эту кнопку для сохранения своих изменений.

12

Брандмауэр

12.1 Обзор

В этой главе рассказывается, как включить брандмауэр устройства P660. Используйте брандмауэр для защиты вашего устройства P660 и сети от атак хакеров в Интернете и для управления 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;
- блокирует атаки SYN и Port Scanner.

По умолчанию устройство P660 блокирует атаки DDOS, LAND и Ping of Death независимо от того, включен или отключен брандмауэр.

12.1.1 Что можно сделать на экране брандмауэра

Используйте экран **Firewall** (Разд. 12.2 на с. 106) для подключения брандмауэра и/или SPI на устройстве P660.

12.1.2 Что нужно знать о брандмауэре

SYN атака

SYN-атака приводит к заполнению целевой системы сериями пакетов с символами синхронизации (SYN). Каждый пакет вынуждает целевую систему давать ответ SYN-ACK. Пока атакуемая система ожидает ACK, которое следует за SYN-ACK, она отслеживает все ожидающие выполнения ответы SYN-ACK, известные как очередь журнала запросов. Ответы SYN-ACK выводятся из очереди только при возвращении ACK или после того, как внутренний таймер завершает трехстороннее квитирование. Когда очередь переполнена, система игнорирует все входящие запросы SYN, делая систему недоступной для легальных пользователей.

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. Устройство ZyXEL изначально сконфигурирован для автоматического обнаружения и предотвращения всех известных атак DoS.

DDoS

DDoS атака - это одна из тех атак, при которых многочисленные взломанные системы атакуют одну цель, вызывая тем самым отказ от обслуживания для пользователей атакуемой системы.

LAND-атака

При LAND-атаке хакеры посылают пакеты SYN в сеть с ложным IP-адресом источника атакуемой системы. В результате все выглядит так, как будто хост посылает пакеты самому себе, делая систему недоступной, в то время как атакуемая система пытается ответить самой себе.

Ping of Death

Атака Ping of Death использует утилиту «эхо-тестирование» для создания и отправки пакета IP, превышающего максимальный объем данных в 65 536 байт, допускаемый спецификацией IP. Это может привести к обрушению, зависанию или перезагрузке системы.

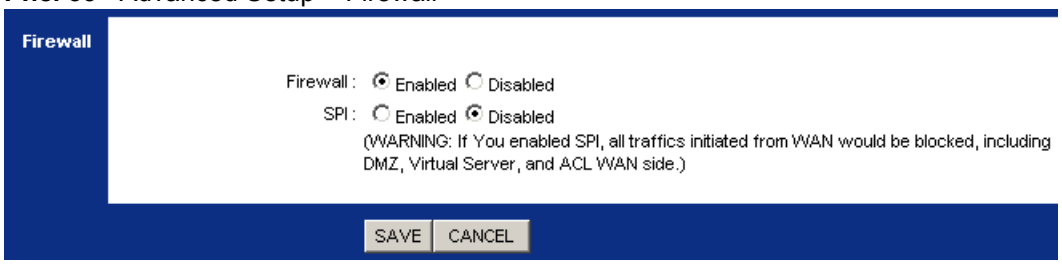
SPI

Инспекция пакетов с учетом состояния (SPI) отслеживает каждое подключение, проходящее через брандмауэр и подтверждает его достоверность. Решения о фильтрации зависят не только от правил, но и от содержания. Например, для трафика из глобальной сети WAN проход через брандамауэр разрешается только в том случае, если это ответ на запрос из локальной сети LAN.

12.2 Экран брандмауэра

Используйте этот экран для подключения брандмауэра и/или SPI. Нажмите **Advanced Setup > Firewall**, чтобы открыть приведенный ниже экран.

Рис. 33 Advanced Setup > Firewall



В приводимой ниже таблице даны описания полей этого экрана.

Табл. 28 Advanced > Firewall

ПОЛЕ	ОПИСАНИЕ
Firewall	Используйте это поле для включения или отключения брандмауэра на вашем устройстве P660.
SPI	Используйте это поле для включения или отключения SPI на вашем устройстве P660.
SAVE	Нажмите эту кнопку для сохранения своих изменений.
CANCEL	Нажмите эту кнопку для восстановления ранее заданных настроек.

При включении SPI блокируется весь трафик со стороны глобальной сети WAN, включая DMZ, виртуальный сервер и ACL на стороне WAN.

Часть V
Управление доступом

13

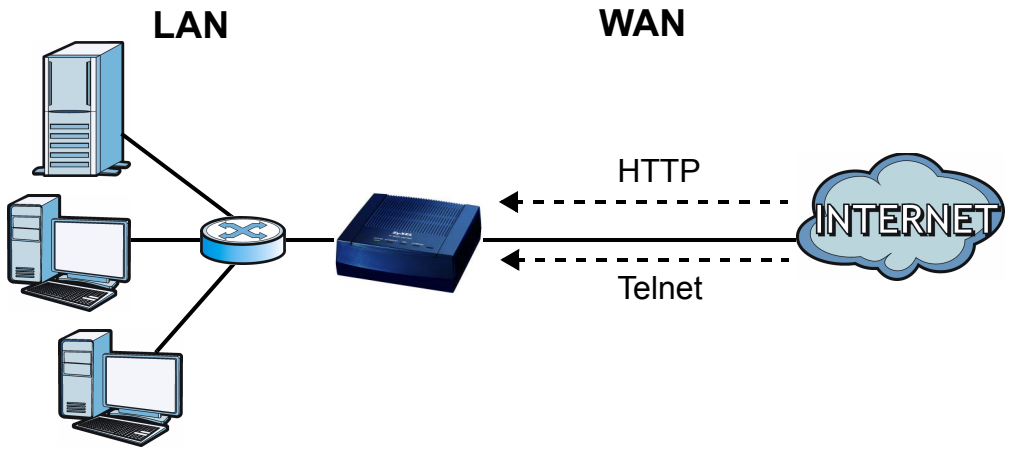
Управление доступом

13.1 Обзор управления доступом

Управление доступом позволяет задать приложения, которые могут получить доступ к определенным интерфейсам устройств P660 с определенных компьютеров.

На приведенном ниже рисунке показан доступ к устройству P660 из глобальной сети WAN только для HTTP (сеть) и Telnet.

Рис. 34 Управление доступом



13.1.1 Экран настройки управления доступом

Используйте этот экран, чтобы показать где и как пользователи могут обратиться к устройству P660.

13.1.2 Интерфейсы управления доступом

Управлять устройством P660 можно через:

- **WAN**
- **LAN**
- **Обе** (LAN и WAN)

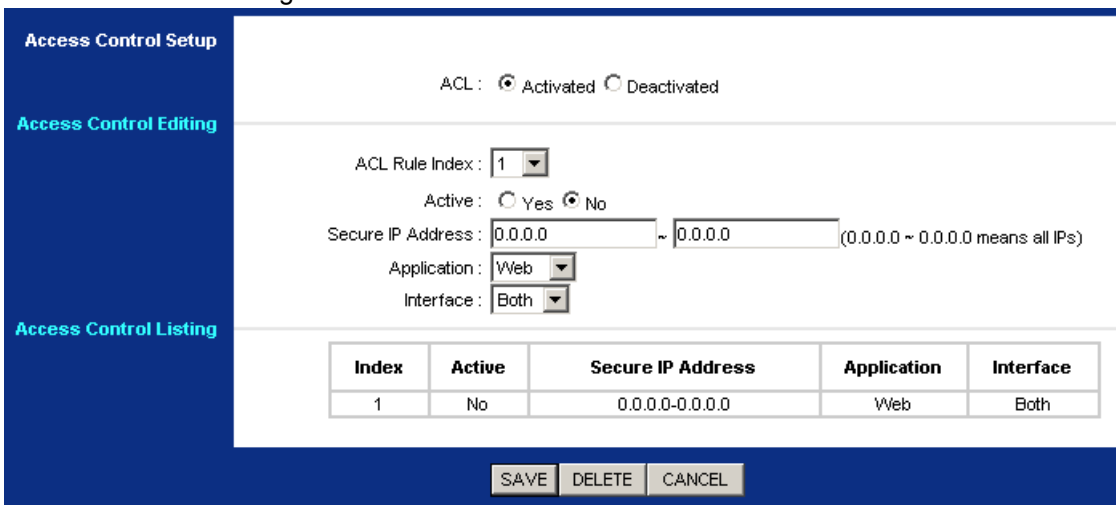
13.1.3 Время простоя системы

Максимальное время простоя системы во время сеанса управления по умолчанию установлено на 5 минут (300 секунд). Устройство P660 автоматически завершает сеанс управления при простое, превышающем этот период. Сеанс управления не разрывается, если в окне статистики проводится опрос системы.

13.1.4 Конфигурация экрана настройки управления доступом

Нажмите **Access Management** > **ACL**, чтобы открыть приведенный ниже экран.

Рис. 35 Access Management > ACL



В приводимой ниже таблице даны описания полей этого экрана.

Табл. 29 Access Management > ACL

ПОЛЕ	ОПИСАНИЕ
Access Control Setup	
ACL	Выберите **Activated** для включения функции управления доступом в устройстве P660 или выберите **Deactivated** для ее отключения.
Access Control Editing	
ACL Rule Index	Выберите номер правила указателя для его редактирования или удаления.
Active	Выберите **Yes** для включения активного правила управления или **No** для его отключения.
Secure IP Address	Введите область IP-адресов компьютеров, которые имеют допуск к устройству. 0.0.0.0 ~ 0.0.0.0 означает, что любой компьютер имеет допуск к устройству P660. Если вы хотите, чтобы только один компьютер имел доступ к устройству P660, введите его IP-адрес в обоих полях.

Табл. 29 Access Management > ACL (продолжение)

ПОЛЕ	ОПИСАНИЕ
Application	Выберите службу, с помощью которой компьютер получает доступ к устройству. • Если вы хотите разрешить пользователю доступ к устройству P660 с помощью Web-конфигуратора, выберите **Web**. • Если вы хотите разрешить пользователю доступ к устройству P660 с помощью Telnet, выберите **Telnet**. • Если вы хотите разрешить пользователю загрузить аппаратное обеспечение в устройство P660, выберите **FTP**. • Если вы хотите разрешить администратору отправлять команды SNMP, выберите **SNMP**. • Если вы хотите разрешить пользователю искать в сети устройство P660 (например, для поиска и устранения неисправностей), выберите **Ping**. • Выберите **ALL** для разрешения доступа ко всем службам. Нельзя выбрать комбинацию служб.
Interface	Выберите порт, с помощью которого вы можете получить доступ к устройству. Выберите **Both**, для получения доступа через любой порт. Если вы указываете 0.0.0.0 ~ 0.0.0.0 **Secure IP Address**, **ALL** и интерфейс **WAN**, то вы не сможете получить доступ к устройству из LAN, пока не укажете другое правило доступа для LAN.
Access Control Listing	В сводной таблице отображаются сконфигурированные параметры для выбранной линии.
SAVE	Нажмите эту кнопку для сохранения изменений.
DELETE	Выберите номер указателя правила управления доступом и нажмите эту кнопку для его удаления.
CANCEL	Нажмите эту кнопку для восстановления ранее заданных настроек.

14

Фильтры

14.1 Обзор

В этой главе представлено описание трех видов фильтров, поддерживаемых устройством P660. Можно задать правила для ограничения трафика по IP-адресам, MAC-адресам, типам приложений и/или URL.

14.1.1 Что можно сделать на экране фильтров

- Используйте экран **IP/MAC Filter** (Разд. 14.2 на с. 116) для формирования правил фильтра IP/MAC.
- Используйте экран **Application Filter** (Разд. 14.3 на с. 118) для разрешения или отклонения трафика от определенных видов приложений.
- Используйте экран **URL Filter** (Разд. 14.4 на с. 119) для блокирования доступа к веб-сайтам.

14.1.2 Что нужно знать о фильтрации

Структура фильтра IP/MAC

Фильтрующий набор IP/MAC включает в себя одно или несколько правил фильтрации. Устройство P660 позволяет задать настройку до двенадцати фильтрующих наборов по шесть правил для каждого набора; итого в системе используется 72 правила фильтрации.

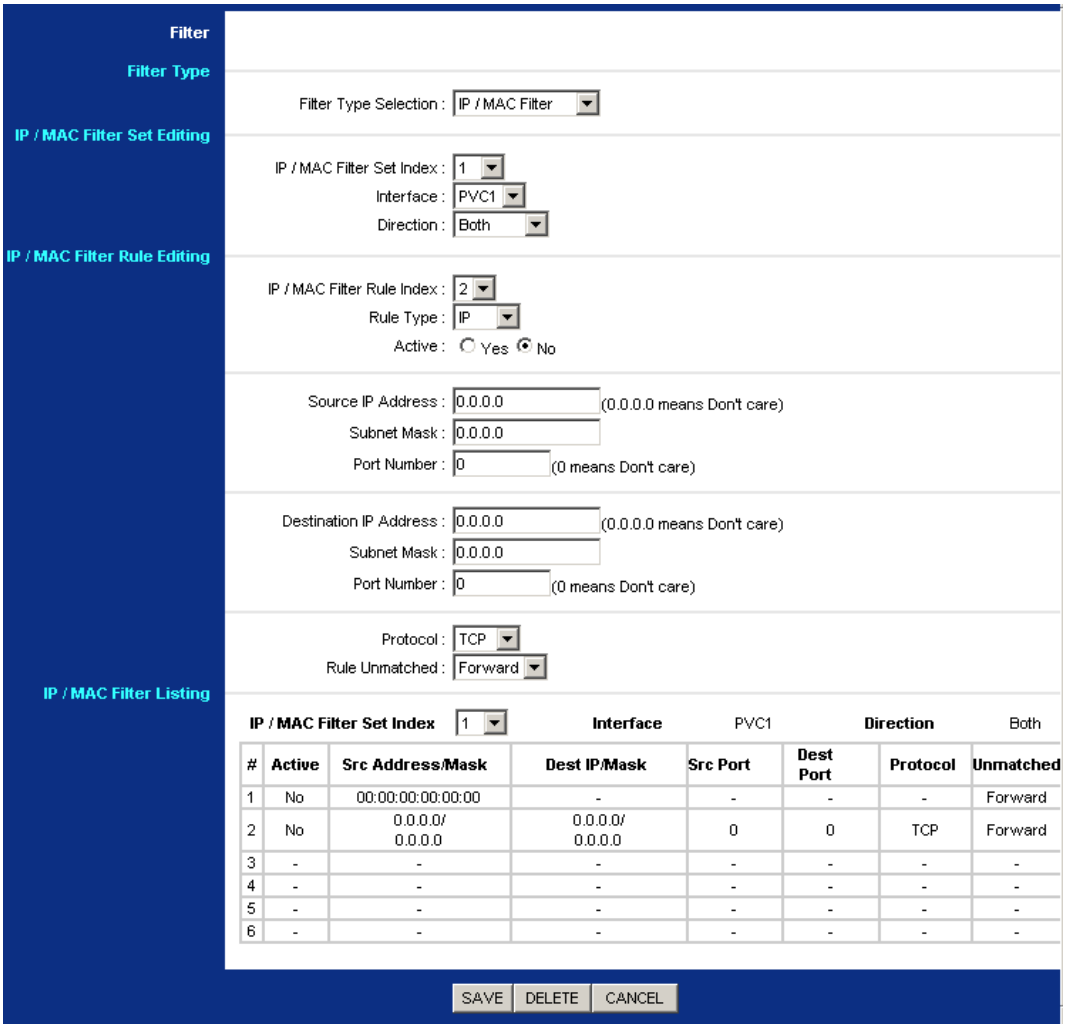
URL

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.

14.2 Экран фильтра IP/MAC

Используйте этот экран для формирования и применения фильтров IP/MAC. Нажмите **Access Management** > **Filter** и выберите **IP/MAC Filter** в поле **Filter Type Selection**. Отображается показанный ниже экран.

Рис. 36 Access Management > Filter (IP/MAC)



В приводимой ниже таблице даны описания полей этого экрана.

Табл. 30 Access Management > Filter (IP/MAC)

ПОЛЕ	ОПИСАНИЕ
Filter Type	
Filter Type Selection	Выберите тип фильтра из разворачивающегося списка. Допустимые варианты **IP/MAC Filter**, **Application Filter** и **URL Filter**.
IP/MAC Filter Set Editing	
IP/MAC Filter Set Index	Выберите номер указателя для набора фильтров.
Interface	Выберите постоянный виртуальный канал (PVC), для которого используется фильтр.
Direction	Используйте фильтр для направления трафика **Both**, **Incoming** или **Outgoing**.

Табл. 30 Access Management > Filter (IP/MAC) (продолжение)

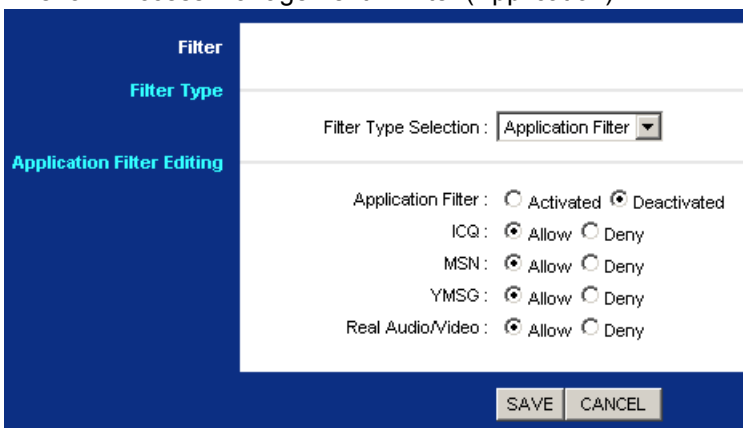
ПОЛЕ	ОПИСАНИЕ
IP/MAC Filter Rule Editing	
IP/MAC Filter Rule Index	Выберите индекс правила фильтра.
Rule Type	Выберите тип **IP** или **MAC** для задания правила. Используйте **IP Filter** для блокировки трафика по IP-адресам. Используйте **MAC Filter** для блокировки трафика по MAC-адресам.
Active	Используйте это поле для включения или отключения правила.
Source IP Address	Введите исходный IP-адрес пакетов, которые вы хотите отфильтровать. Это поле игнорируется, если вы указываете 0.0.0.0.
Subnet Mask	Введите маску IP-подсети для исходного IP-адреса.
Port Number	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.
Destination IP Address	Введите IP-адрес назначения для пакетов, которые вы хотите отфильтровать. Это поле игнорируется, если вы указываете 0.0.0.0.
Subnet Mask	Введите маску IP-подсети для IP-адреса назначения.
Port Number	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.
Protocol	Выберите **ICMP**, **TCP** или **UDP** для протокола верхнего уровня.
MAC Address	Это поле отображается только при выборе **MAC** в поле **Rule Type**. Введите MAC-адрес для пакетов, которые вы хотите отфильтровать.
Rule Unmatched	Выберите операцию для пакетов, которые не соответствуют правилу. Выберите **Forward**, чтобы сразу же переадресовать трафик и пропустить проверку оставшихся правил. Выберите **Next** для проверки последующего правила.
IP/MAC Filter Listing	
IP/MAC Filter Set Index	Выберите индекс набора фильтров из разворачивающегося списка.
Interface	Интерфейс, для которого используется набор фильтров.
Direction	Набор фильтров применяется в этом направлении трафика.
#	Индекс правила в наборе фильтров.
Active	Это поле указывает, активировано ли правило.
Src Address/Mask	IP-адрес источника и маска подсети при выборе **IP** в качестве типа правила. MAC-адрес при выборе **MAC** в качестве типа правила.
Dest IP/Mask	IP-адрес назначения и маска подсети.
Src Port	Номер порта источника.
Dest Port	Номер порта назначения.
Protocol	Протокол верхнего уровня.
Unmatched	Если пакет не соответствует правилу, то тогда устройство P660 выполняет это действие.
SAVE	Нажмите эту кнопку для сохранения своих изменений.
DELETE	Нажмите эту кнопку для удаления правила фильтра.
CANCEL	Нажмите эту кнопку для восстановления ранее заданных настроек.

14.3 Экран фильтра приложения

Используйте этот экран для того, чтобы разрешить или отклонить трафик для некоторых типов приложений. Фильтр приложений обеспечивает удобный способ управления различными приложениями в сети.

Нажмите **Access Management** > **Filter** и выберите **Application Filter** в поле **Filter Type Selection**. Отображается показанный ниже экран.

Рис. 37 Access Management > Filter (Application)



В приводимой ниже таблице даны описания полей этого экрана.

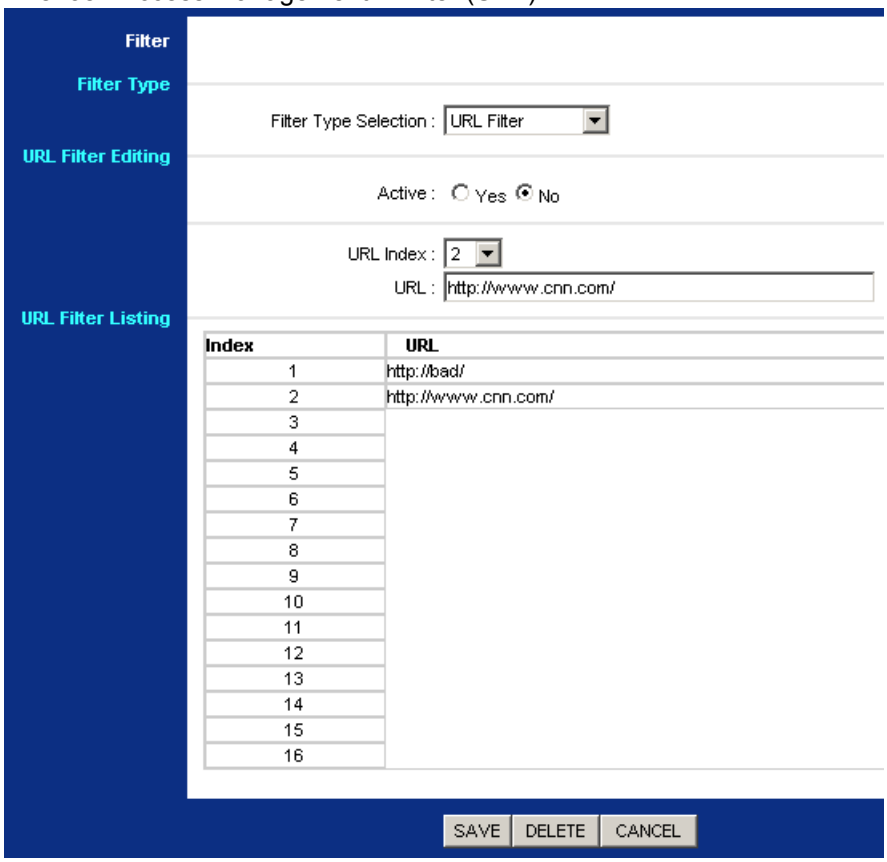
Табл. 31 Access Management > Filter (Application)

ПОЛЕ	ОПИСАНИЕ
фильтр приложений	Используйте это поле для включения или отключения фильтра приложения.
ICQ	Используйте это поле для разрешения или отклонения трафика ICQ.
MSN	Используйте это поле для разрешения или отклонения трафика MSN.
YMSG	Используйте это поле для разрешения или отклонения трафика Yahoo Messenger.
Real Audio/Video	Используйте это поле для разрешения или отклонения передачи файлов в формате RealPlayer.
SAVE	Нажмите эту кнопку для сохранения своих изменений.
CANCEL	Нажмите эту кнопку для восстановления ранее заданных настроек.

14.4 Экран фильтра URL

Используйте этот экран для блокировки веб-сайтов по URL. Нажмите **Access Management** > **Filter** и выберите **URL Filter** в поле **Filter Type Selection**. Отображается показанный ниже экран.

Рис. 38 Access Management > Filter (URL)



В приводимой ниже таблице даны описания полей этого экрана.

Табл. 32 Access Management > Filter (URL)

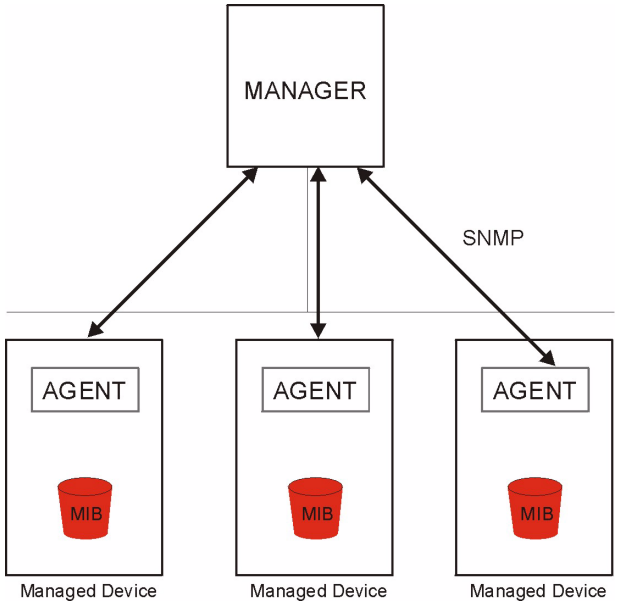
ПОЛЕ	ОПИСАНИЕ
URL Filter Editing	
Active	Используйте это поле для включения или отключения фильтра URL.
URL Index	Выберите индекс фильтра.
URL	Введите URL для его блокировки устройством P660.
URL Filter Listing	
Index	Индекс правила фильтра.
URL	Адрес URL, который будет блокироваться устройством P660.
SAVE	Нажмите эту кнопку для сохранения своих изменений.
DELETE	Нажмите эту кнопку для удаления правила фильтра.
CANCEL	Нажмите эту кнопку для восстановления ранее заданных настроек.

15 SNMP

15.1 Обзор

SNMP (Simple Network Management Protocol - Простой протокол управления сетью) используется для обмена информацией об управлении между сетевыми устройствами. SNMP входит в состав набора протоколов TCP/IP. Устройство P660 поддерживает функцию агента SNMP, что позволяет выполнять управление и мониторинг P660 с управляющей станции по сети. Устройство P660 поддерживает протокол SNMP версии один (SNMPv1) и версии два (SNMPv2).Следующий рисунок иллюстрирует функцию управления по протоколу SNMP.

Рис. 39 Модель управления SNMP



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

Агент представляет собой модуль программы управления, находящийся в управляемом устройстве (устройство P660). Агент преобразует информацию о локальном управлении, получаемую от управляемого устройства, в форму, совместимую с протоколом SNMP. В качестве управляющей программы выступает консоль, при помощи которой сетевые администраторы осуществляют управление сетью. Через консоль происходит запуск приложений, предназначенных для контроля и мониторинга управляемых устройств.

Управляемые устройства содержат объектные переменные/управляемые объекты, которые определяют, какой вид информации об устройстве необходимо собрать. 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 обмениваться друг с другом информацией, необходимой для доступа к данным объектам.

Сам по себе протокол SNMP является простым протоколом типа «запрос-ответ», работающим по модели «управляющая программа/агент». Управляющая программа выдает запрос, а агент возвращает ответы с помощью следующих операций протокола:

- Get — позволяет управляющей программе извлечь объектную переменную из агента.
- Set — позволяет управляющей программе устанавливать значения для объектных переменных, находящихся внутри агента.

15.1.1 Поддерживаемые базы управляющей информации (MIB)

Устройство P660 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.

15.2 Экран SNMP

Используйте этот экран для изменения настроек WAN устройства P660. Нажмите **Access Management > SNMP**, чтобы открыть приведенный ниже экран.

Рис. 40 Access Management > SNMP

В приводимой ниже таблице даны описания полей этого экрана.

Табл. 33 Access Management > SNMP

ПОЛЕ	ОПИСАНИЕ
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.
SAVE	Нажмите эту кнопку для сохранения своих изменений.

16

Универсальная функция Plug and Play (UPnP)

16.1 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, предоставлять свои ресурсы и собирать информацию о других устройствах сети. В свою очередь, устройство может беспрепятственно и автоматически покидать сеть, когда оно больше не используется.

16.1.1 Что можно сделать на экране UPnP

Используйте экран **UPnP** (Разд. 16.2 на с. 124) для включения функции UPnP в устройстве P660 и для возможности использования приложения с функцией Plug and Play для автоматической настройки устройства P660.

16.1.2 Что нужно знать о UpnP

Идентификация устройств с функцией UPnP

Аппаратное обеспечение UPnP идентифицируется значком в папке Network Connections (Windows XP). Каждое совместимое с UPnP устройство, установленное в сети, появляется в виде отдельного значка. Выбор значка устройства UPnP позволяет получить доступ к информации и свойствам данного устройства.

NAT Traversal

Функция NAT Traversal с поддержкой UPnP автоматизирует процесс работы приложения через NAT. Сетевые устройства UPnP могут автоматически настраивать сетевую адресацию, объявлять о своем присутствии в сети другим устройствам UPnP и производить обмен простыми сообщениями о программных продуктах и службах. Функция NAT Traversal позволяет следующее:

- Динамическое отображение портов
- Распознавание общедоступных IP-адресов
- Назначение времени аренды для отображений

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

Подробней об этом — см. главу по трансляции сетевых адресов (NAT).

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 средах сетевая информация и конфигурация могут быть получены и изменены пользователями.

Когда устройство UPnP подключается к сети, оно объявляет о своем присутствии с помощью многоадресной рассылки сообщения. В целях повышения безопасности устройство P660 разрешает многоадресную рассылку сообщений только по локальной сети.

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

UPnP и ZyXEL

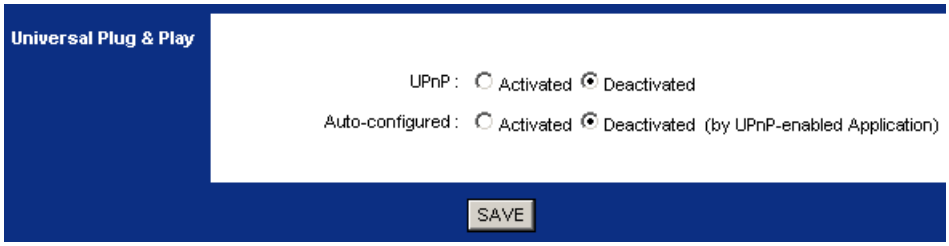
Корпорация ZyXEL получила сертификат от организации Universal Plug and Play Forum UPnP™ Implementers Corp. (UIC). Реализация UPnP ZyXEL поддерживает функцию IGD 1.0 (Internet Gateway Device — шлюзовое устройство подключения к Интернету).

Примеры установки и использования UPnP см. в следующих разделах.

16.2 Экран UPnP

Используйте следующий экран для настройки параметров UPnP вашего устройства P660. Нажмите **Access Management > UPnP** для отображения экрана, показанного ниже.

Рис. 41 Access Management > UPnP



В приводимой ниже таблице даны описания полей этого экрана.

Табл. 34 Access Management > UPnP

ПОЛЕ	ОПИСАНИЕ
UPnP	Используйте это поле для включения или отключения UPnP. Помните, что любой может с помощью приложения UPnP открыть окно регистрации Web-конфигуратора без ввода IP-адреса устройства P660 (хотя для доступа к Web-конфигуратору необходимо ввести пароль).
Auto-configured	Используйте это поле, чтобы разрешить приложениям с функцией UPnP автоматически настраивать устройство P660 с целью взаимодействия через устройство P660, например, используя NAT traversal, приложения UPnP автоматически зарезервируют порт, чтобы взаимодействовать с другими устройствами UPnP; это предотвращает необходимость ручной настройки переадресации портов для приложения UPnP.
SAVE	Нажмите эту кнопку для сохранения своих изменений.

16.3 Пример установки UPnP в Windows

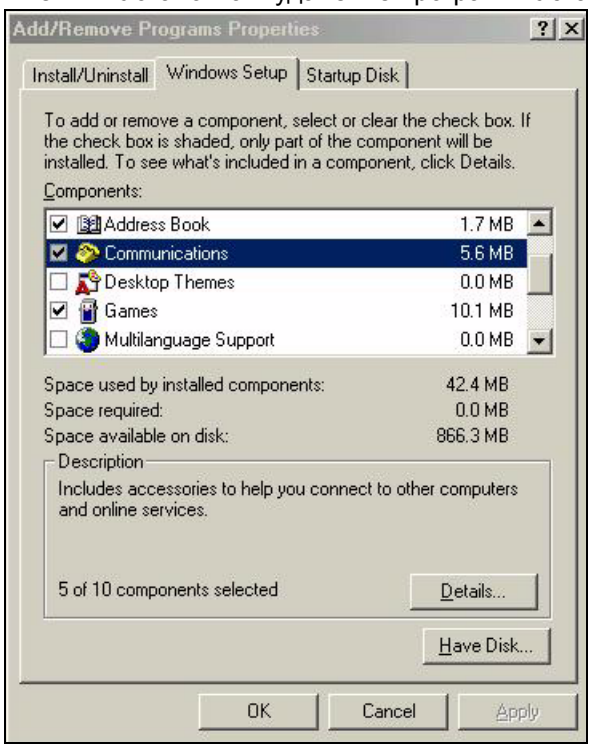
В данном разделе описывается установка UPnP в Windows Me и Windows XP.

Установка UPnP в Windows Me

Выполните следующие действия для установки UPnP в Windows Me.

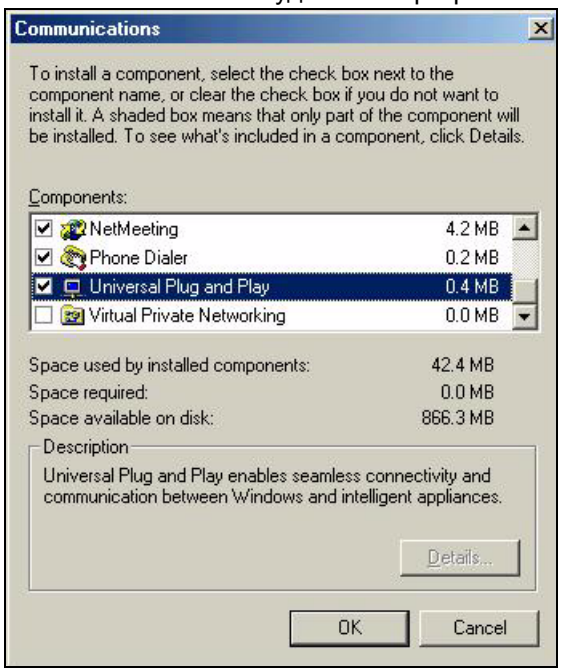
1. Нажмите **Start (Пуск)** и выберите пункт **Control Panel (Панель управления)**. Дважды щелкните пункт **Add/Remove Programs (Установка и удаление программ)**.
2. Выберите закладку **Windows Setup (Установка Windows)** и выберите **Communication (Связь)** в поле **Components (Компоненты)**. Нажмите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

Рис. 42 Установка и удаление программ: Установка Windows: Связь



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

Рис. 43 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.

Установка UPnP в Windows XP

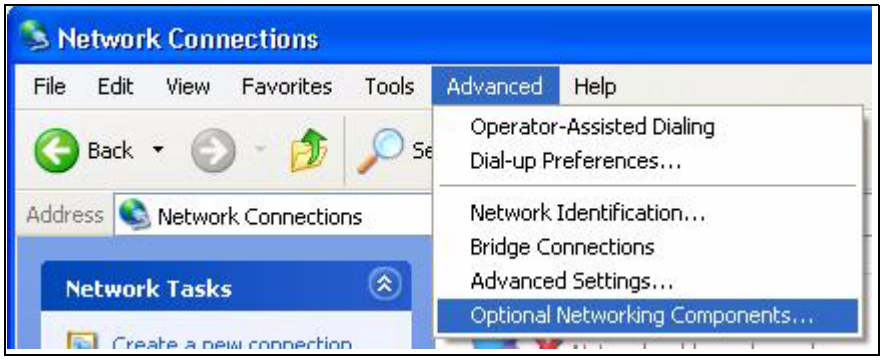
Выполните следующие действия для установки UPnP в Windows XP.

1 Нажмите **Start (Пуск)** и выберите пункт **Control Panel (Панель управления)**.

2 Дважды щелкните значок **Network Connections (Сетевые подключения)**.

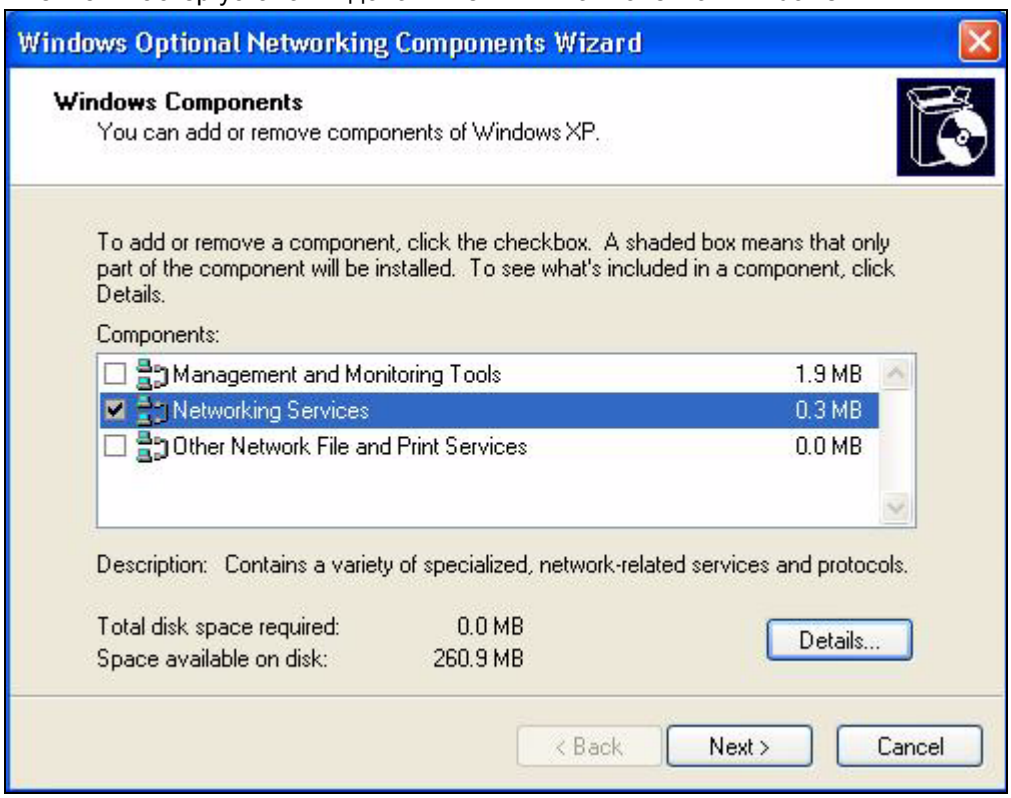
3 В окне **Network Connections (Сетевые подключения)** нажмите кнопку **Advanced (Дополнительно)** в главном меню и выберите **Optional Networking Components… (Дополнительные сетевые компоненты...)**.

Рис. 44 Сетевые подключения



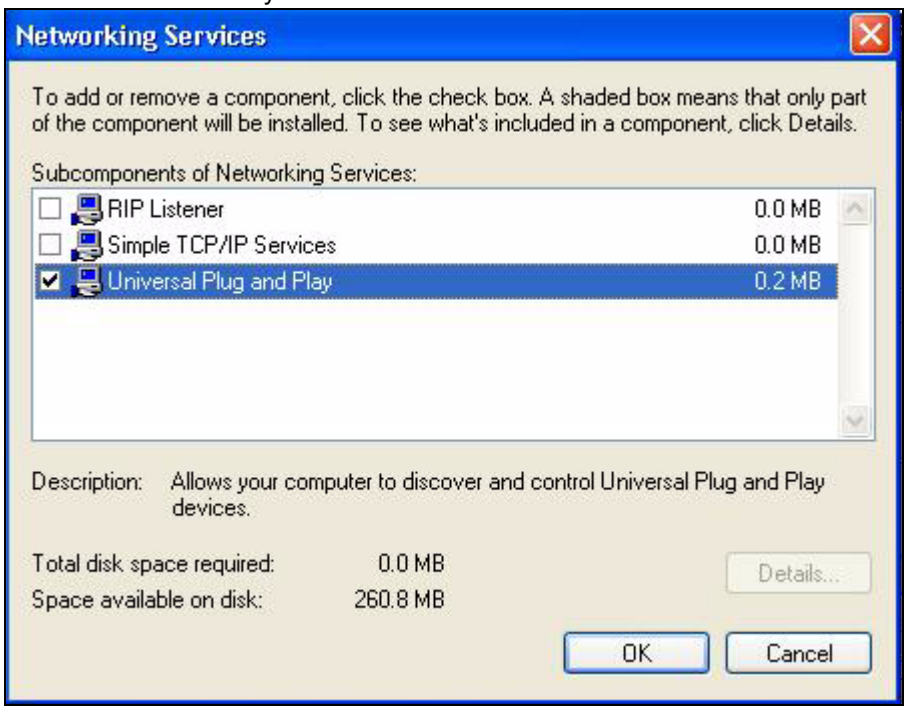
4 Появляется окно **Windows Optional Networking Components Wizard (Мастер установки дополнительных сетевых компонентов Windows)**. Выберите **Networking Services (Сетевые службы)** в поле **Components (Компоненты)** и нажмите **Details (Состав)**.

Рис. 45 Мастер установки дополнительных компонентов Windows



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

Рис. 46 Сетевые службы



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

16.4 Пример использования UPnP в Windows XP

В этом разделе описывается использование функции UPnP в Windows XP. Функция UPnP уже должна быть установлена в Windows XP и включена в модеме P660.

Убедитесь, что компьютер подключен к порту LAN модема P660. Включите компьютер и P660.

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. 47 Сетевые подключения

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

Рис. 48 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. 49 Свойства подключения к Интернет: Дополнительные настройки

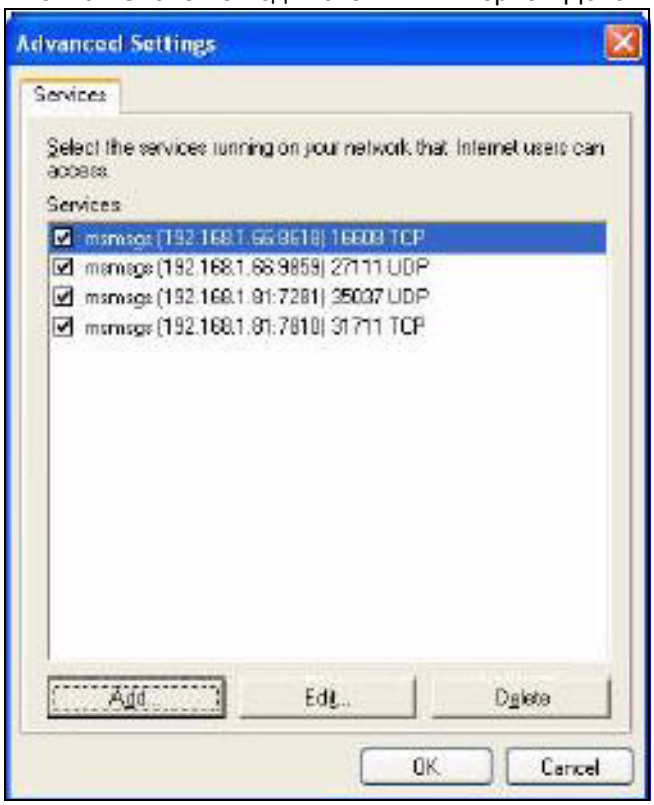
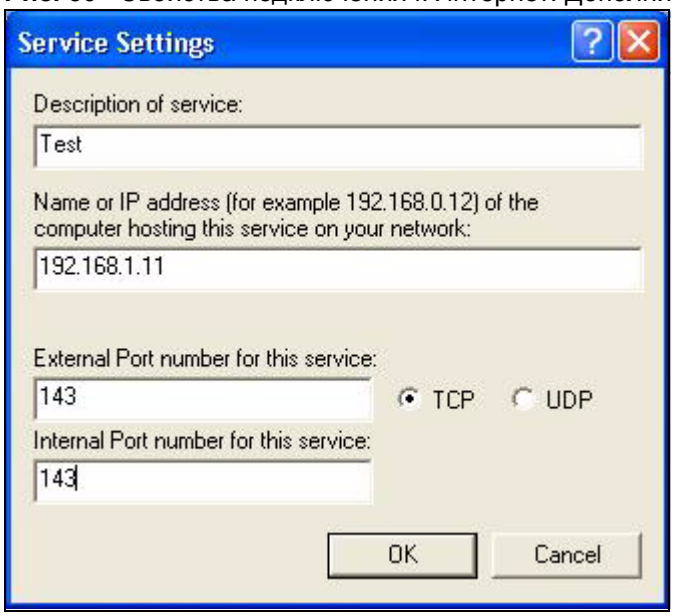


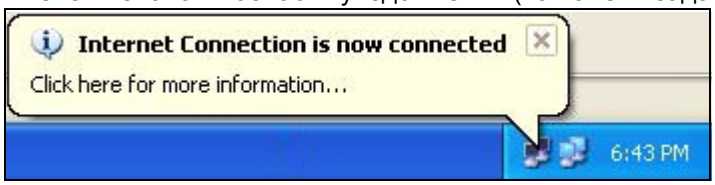
Рис. 50 Свойства подключения к Интернет: Дополнительные настройки: Добавить



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. 51 Значок в области уведомлений (на панели задач)



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

Рис. 52 Состояние подключения к Интернет

Простой доступ к Web-конфигуратору

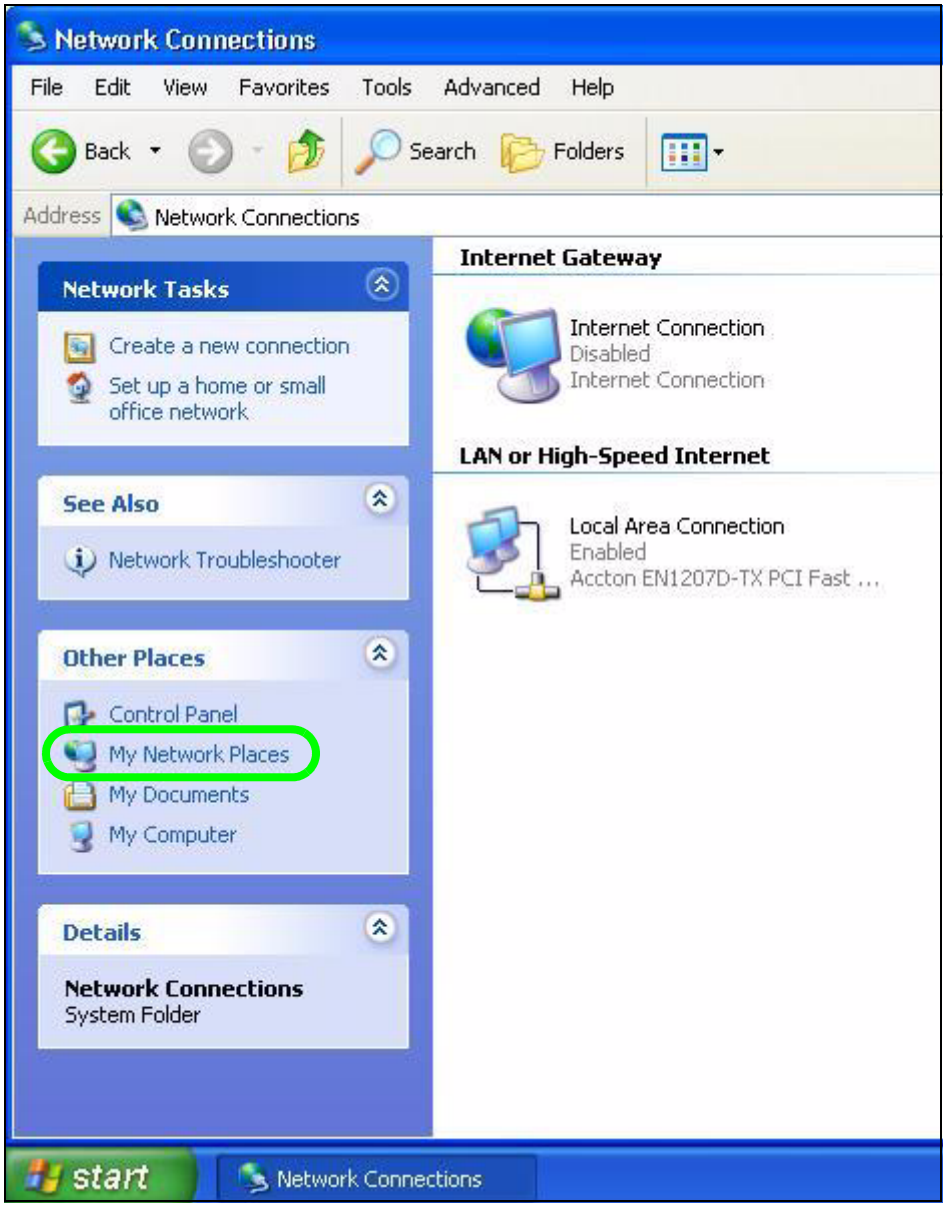
С помощью UPnP вы можете получить доступ к программе настройки P660 на основе Web технологии без предварительного выяснения IP-адреса P660. Это может оказаться полезным, если вы не знаете IP-адрес P660.

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)**.

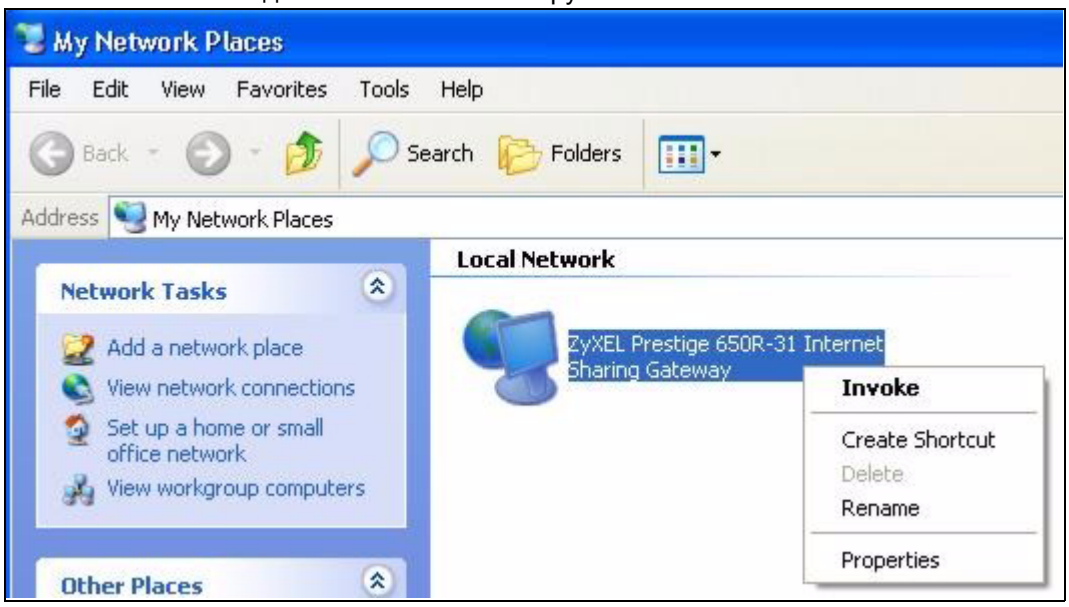
Рис. 53 Сетевые подключения



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

5 Щелкните правой кнопкой мыши по значку P660 и выберите **Invoke (Запустить)**. Появится окно регистрации Web-конфигуратора.

Рис. 54 Сетевые подключения: Сетевое окружение



6 Щелкните правой кнопкой мыши по значку P660 и выберите **Properties (Свойства)**. Появится окно свойств с основной информацией об модеме P660.

Рис. 55 Пример — Сетевые подключения: Сетевое окружение: Свойства

17

Настройка динамической системы доменных имен (DYNDNS)

17.1 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 получить доступ к вашему ресурсу, даже если они не знают точного IP-адреса.

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

17.1.1 Что можно сделать на экране DDNS

Используйте экран **Dynamic DNS** (Разд. 17.2 на с. 136) для включения DDNS и настройки параметров DDNS в модели P660.

17.1.2 Что нужно знать о DDNS

Шаблон DYNDNS

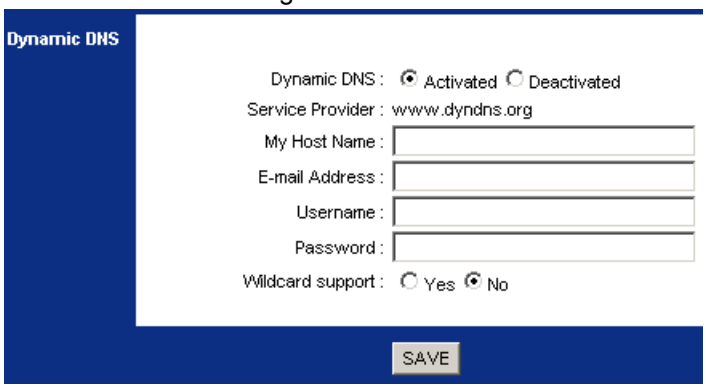
Использование масок позволяет соотносить имена вида *.yourhost.dyndns.org с тем же IP-адресом, что и имя yourhost.dyndns.org. Данная функция полезна, если вы хотите иметь возможность использовать, например, адрес www.yourhost.dyndns.org и при этом предоставлять доступ к вашему узлу.

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

17.2 Экран настройки динамической системы доменных имен

Используйте этот экран для изменения DDNS вашего устройства P660. Нажмите **Access Management > DDNS**. Отображается показанный ниже экран.

Рис. 56 Access Management > DDNS



В приводимой ниже таблице даны описания полей этого экрана.

Табл. 35 Advanced > Dynamic DNS

ПОЛЕ	ОПИСАНИЕ
Dynamic DNS	Используйте это поле для включения или отключения динамической системы доменных имен (DDNS).
Service Provider	Имя провайдера услуг динамической DNS.
My Host Name	Введите доменное имя, назначенное устройству P660 провайдером услуг динамической DNS.
E-mail Address	Введите адрес электронной почты.
Username	Наберите свое пользовательское имя.
Password	Введите назначенный пароль.
Wildcard support	Используйте это поле для включения или отключения шаблона DYNDNS.
SAVE	Нажмите эту кнопку для сохранения своих изменений.

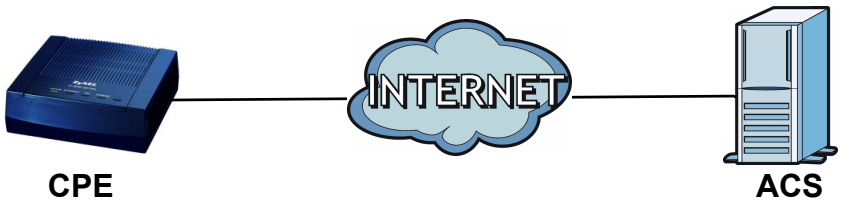
18 CWMP

18.1 Обзор

Устройство P660 поддерживает Поправку 1 TR-069 (CPE WAN Management Protocol Release 2.0) и Поправку 2 TR-069 (CPE WAN Management Protocol v1.1, Release 3.0).

TR-069 представляет собой протокол, определяющий способы управления вашим устройством P660 (**CPE**) через управляющий сервер (**ACS**), например Vantage Access для устройства ZyXEL.

Рис. 57 LAN и WAN



Администратор может использовать управляющий сервер для удаленной настройки устройства ZyXEL, изменения параметров, выполнения обновлений микропрограммы, а также мониторинга и диагностики устройства ZyXEL.

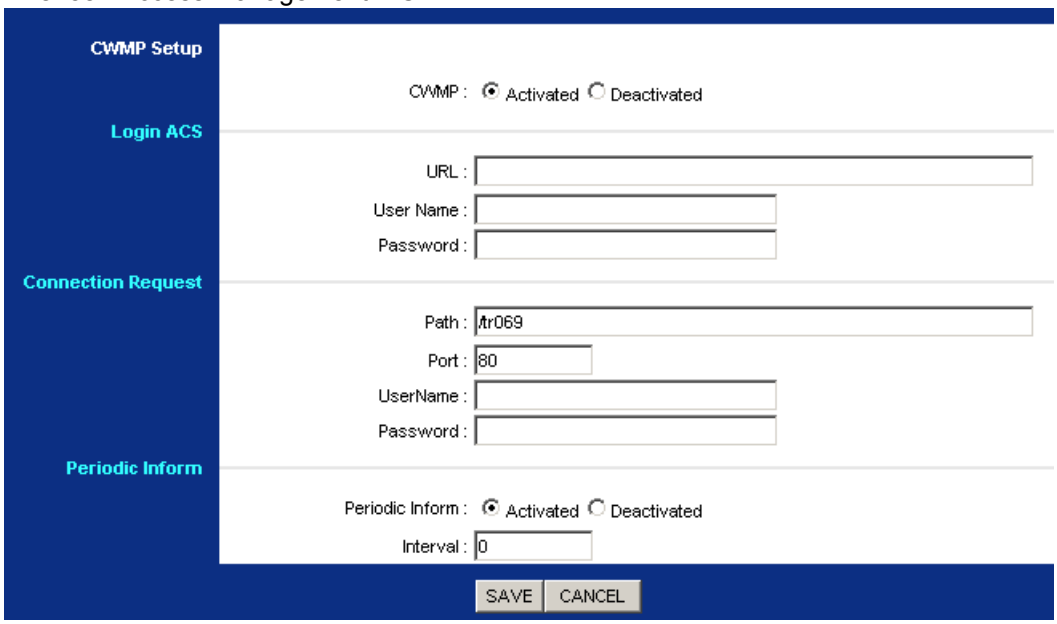
Для того чтобы использовать CWMP, необходимо провести поэтапную настройку:

1. Активируйте CWMP.
2. Укажите URL, имя пользователя и пароль.
3. Активируйте периодическое отображение информации и укажите значение интервала.

18.2 Экран настройки CWMP

Используйте этот экран для настройки устройства P660, чтобы им мог управлять управляющий сервер. Нажмите **Access Management** > **CWMP**, чтобы открыть приведенный ниже экран.

Рис. 58 Access Management > CWMP



В приводимой ниже таблице даны описания полей этого экрана.

Табл. 36 Access Management > CWMP

ССЫЛКА	ОПИСАНИЕ
CWMP Setup	
CWMP	Выберите **Activated**, чтобы управляющий сервер мог управлять устройством P660 или выберите **Deactivated**, чтобы управляющий сервер не мог управлять устройством P660.
Login ACS	Настройте эту часть экрана, чтобы можно было зайти на управляющий сервер.
URL	Наберите IP-адрес или имя домена управляющего сервера. Если устройство P660 расположено после маршрутизатора NAT, который присваивает индивидуальный IP-адрес, то необходимо на маршрутизаторе Nat задать правило переадресации порта NAT.
User Name	Имя пользователя используется для аутентификации устройства P660 при подключении к управляющему серверу. Имя пользователя для управляющего сервера должно быть таким же, как и для устройства P660. Наберите имя пользователя, длина которого может быть до 255 печатных знаков, имеющихся на английской клавиатуре. Допускается использование пробелов и символов @#$%^&*()_+.
Password	Пароль используется для аутентификации устройства P660 при подключении к управляющему серверу. Пароль для управляющего сервере должно быть таким же, как и для устройства P660. Наберите пароль пользователя, длина которого может быть до 255 печатных знаков, имеющихся на английской клавиатуре.
Connection Request	Используйте эту часть экрана, чтобы разрешить управляющему серверу подключиться к устройству P660 после успешной регистрации.
Path	Наберите IP-адрес или имя домена устройства P660. Управляющий сервер использует этот путь для проверки устройства P660.

Табл. 36 Access Management > CWMP (продолжение)

ССЫЛКА	ОПИСАНИЕ
Port	Портом по умолчанию для доступа к устройству P660 с управляющего сервера является порт HTTP, порт 80. Если вы его изменяете, то убедитесь, что он не конфликтует с другим портом вашей сети; при этом рекомендуется использовать номер порта больше 1024 (не часто используемый порт). Управляющий сервер должен использовать этот порт для подключения к устройству P660. Возможно потребуется изменить правила переадресации порта NAT, если они уже были заданы.
UserName	Имя пользователя используется для аутентификации управляющего сервера при подключении к устройству P660. Наберите имя пользователя, длина которого может быть до 255 печатных знаков, имеющихся на английской клавиатуре. Допускается использование пробелов и символов @#$%^&*()_+.
Password	Пароль используется для аутентификации управляющего сервера при подключении к устройству P660. Наберите пароль пользователя, длина которого может быть до 255 печатных знаков, имеющихся на английской клавиатуре. Пробелы не допускаются.
Periodic Inform	Выберите **Activated**, чтобы устройство P660 периодически передавало информацию на управляющий сервер (рекомендуется при включении CWMP), или выберите **Deactivated** чтобы устройство P660 периодически передавало информацию на управляющий сервер
Interval	Интервал — это продолжительность времени в секундах, в течение которого устройство P660 должно попытаться подключиться к управляющему серверу, чтобы передать информацию и проверить обновления настроек. Введите значение от 1 до 86400.
SAVE	Нажмите эту кнопку для сохранения своих изменений.
CANCEL	Нажмите эту кнопку для восстановления ранее заданных настроек.

Часть VI
Администрирование

19

Настройка администратора

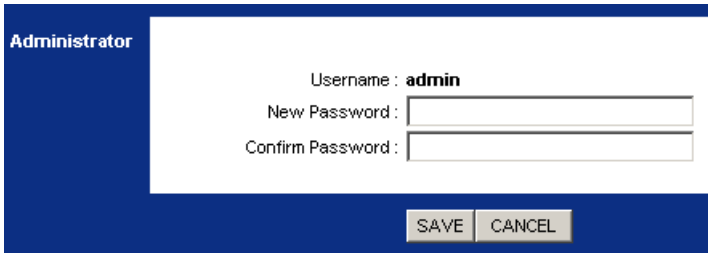
19.1 Обзор

В этой главе показано, как можно изменить пароль системы.

19.2 Экран администратора

Используйте этот экран для установки нового пароля на ваше устройство P660.
Нажмите **Maintenance > Administraton**, чтобы открыть приведенный ниже экран.

Рис. 59 Maintenance > Administraton



В приводимой ниже таблице даны описания полей этого экрана.

Табл. 37 Maintenance > Administraton

ПОЛЕ	ОПИСАНИЕ
New Password	Введите новый пароль длиной до 30 символов. При вводе пароля вводимые символы заменяются на экране на символ *. После изменения пароля для доступа к устройству P660 необходимо использовать новый пароль.
Confirm Password	Введите новый пароль еще раз для подтверждения.
SAVE	Нажмите эту кнопку для сохранения своих изменений.
CANCEL	Нажмите эту кнопку для восстановления ранее заданных настроек.

20

Часовой пояс

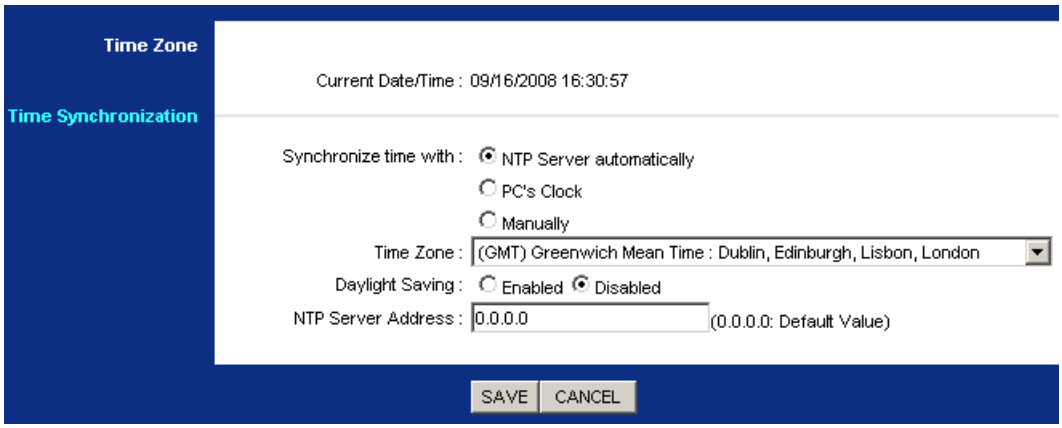
20.1 Обзор

В этой главе содержится информация о настройке параметров времени для вашего устройства P660.

20.2 Экран часового пояса

Этот экран используется для установки времени в устройстве P660 в соответствии с вашим часовым поясом. Для изменения даты и времени в устройстве P660 нажмите **Maintenance > Time Zone**. Отображается показанный ниже экран.

Рис. 60 Maintenance > Time Zone



В приводимой ниже таблице даны описания полей этого экрана.

Табл. 38 Maintenance > Time Zone

ПОЛЕ	ОПИСАНИЕ
Time Zone	
Current Date/Time	В этом поле отображаются дата и время для вашего устройства P660.
Time Synchronization	
Synchronize time with	Выберите **NTP Server automatically**, чтобы устройство P660 получило время и дату с сервера времени. Формат Time (RFC) представляет собой 4-байтовое целое число, означающее общее количество секунд, истекшее с 1970/1/1:0:0, 0. Выберите **PC's Clock**, чтобы устройство P660 могло синхронизировать время с вашим ПК. Выберите **Manually** для установки времени и даты вручную.

Табл. 38 Maintenance > Time Zone (продолжение)

ПОЛЕ	ОПИСАНИЕ
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. Выберите **Enabled** если вы используете переход на летнее время.
NTP Server Address	Введите IP-адрес или URL сервера времени длиной до 20 символов расширенного набора ASCII. Если вы не уверены в правильности имеющейся у вас информации, то уточните ее у Интернет-провайдера или у сетевого администратора.
Date	Это поле доступно только в том случае, если вы устанавливаете время и дату вручную. Введите дату в этом поле.
Time	Это поле доступно только в том случае, если вы устанавливаете время и дату вручную. Введите время в этом поле.
SAVE	Нажмите эту кнопку для сохранения своих изменений.
CANCEL	Нажмите эту кнопку для восстановления ранее заданных настроек.

21

Встроенное программное обеспечение

21.1 Обзор

В этой главе описывается, как загружать новое встроенное программное обеспечение и управлять файлами конфигурации.

Используйте инструкции в данной главе для изменения файла конфигурации устройства или для обновления его аппаратного 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. Встроенное программное обеспечение определяет доступные возможности и функции устройства. Можно загружать новые выпуски встроенного программного обеспечения с сайта ZyXEL (или www.zyxel.ru), чтобы обновить рабочие характеристики вашего устройства.

Необходимо использовать встроенное программное обеспечение строго в соответствии с конкретной моделью устройства. См. наклейку, находящуюся на нижней панели устройства P660.

21.1.1 Что нужно знать о встроенном программном обеспечении

Имена 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 P660, 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 встроенное программное обеспечение системы, файлы системы имеют расширение bin. Это встроенное программное обеспечение находится по адресу www.zyxel.ru. У большинства FTP и TFTP-клиентов имена файлов схожи с представленными ниже.

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

Это пример сеанса FTP для передачи файла firmware.bin с компьютера в устройство P660.

```
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 P660 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 P660, а имя внешнего файла обозначает файл не в устройстве P660, т. е. в вашем компьютере, локальной сети или на FTP-сайте, поэтому имя (но не расширение) может меняться. После загрузки нового встроенного программного обеспечения посмотрите на экран **Status**, чтобы убедиться, что загружена правильная версия встроенного программного обеспечения.

Табл. 39 Соглашение по именам файлов

ТИП ФАЙЛА	ВНУТРЕННЕЕ ИМЯ	ВНЕШНЕЕ ИМЯ	ОПИСАНИЕ
Файл конфигурации	Rom-0	Имя файла конфигурации, находящегося на устройстве P660. При выгрузке файла rom-0 происходит замена всей файловой системы ПЗУ, включая конфигурацию вашего устройства P660, данные, относящиеся к системе (в том числе и пароля по умолчанию), журнал регистрации ошибок и журнал регистрации результатов трассировки.	*.rom
Встроенное программное обеспечение	Ras	Базовое имя для встроенного программного обеспечения ZyNOS на устройстве P660.	*.bin

Ограничения FTP

FTP не работает в том случае когда:

1. Отключена служба FTP на экране **Remote Management**.
2. 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.

21.1.2 Перед началом

Убедитесь, что служба FTP не отключена на экране Remote Management.

21.1.3 Примеры встроенного программного обеспечения и файлов конфигурации

В этом разделе содержатся примеры управления файлами конфигурации и загрузки встроенного программного обеспечения на ваше устройство P660.

Использование FTP 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. 61 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. 21.1.1 на с. 147.

Загрузка встроенного программного обеспечения и файлов конфигурации с помощью FTP and TFTP

В этих примерах описывается, как выгрузить файлы встроенного программного обеспечения и файлы конфигурации.

НЕ ПРЕРЫВАЙТЕ процесс передачи файла, так как это может привести к НЕУСТРАНИМЫМ ПОВРЕЖДЕНИЯМ устройства.

Предпочтительным методом выгрузки файлов встроенного программного обеспечения и файлов конфигурации является FTP. Для того, чтобы им воспользоваться, на вашем компьютере должен быть установлен FTP-клиент. В приведенных ниже разделах приведены примеры того, как загружать встроенное программное 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 устройства вашего устройства через пробел.
3. В диалоговом окне введите имя пользователя и нажмите клавишу [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 встроенное программное 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 встроенного программного обеспечения

Рис. 62 Пример сеанса FTP по выгрузке файла встроенного программного 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. 21.1.1 на с. 147.

Выгрузка файлов по протоколу TFTP

Устройство поддерживает загрузку файлов встроенного программного 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 встроенного программного программного 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 консоли, введите команду «sys stdio 0». При этом передача данных по протоколу TFTP не прервется. По окончании передачи файла, для восстановления 5-минутного интервала простоя SMT (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 встроенного программного 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 встроенного программного обеспечения, находящегося на компьютере), на удаленный хост («ras» — имя встроенного программного 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 устройства вашего устройства P660.
3. В диалоговом окне введите имя пользователя и нажмите клавишу [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 P660 на ваш компьютер, например, «`get rom-0 config.rom`». Эта команда передает файл конфигурации, находящийся на устройстве P660 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. 63 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. 40 Основные команды для FTP-клиентов с графическим интерфейсом.

КОМАНДА	ОПИСАНИЕ
Host Address	Введите адрес хост-сервера.
Login Type	Анонимный. Этот тип регистрации используется в случаях, когда идентификатор пользователя и пароль автоматически передаются серверу для получения анонимного доступа. Анонимная регистрация возможна, только если администратор услуг Интернет-провайдера включил данную опцию. Стандартный. Для регистрации необходимо ввести уникальный идентификатор пользователя и пароль.
Transfer Type	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).

21.2 Экран встроенного программного обеспечения

Используйте этот экран для управления файлами конфигурации и выгрузки встроенного программного обеспечения в ваше устройство P660.

Обновление встроенного программного обеспечения

Следуйте указаниям на этом экране для загрузки встроенного программного обеспечения в ваше устройство P660. Для загрузки используется протокол HTTP (Hypertext Transfer Protocol — Протокол передачи гипертекста), загрузка может занять до двух минут. После успешной загрузки встроенного программного обеспечения система перезапускается. Для обновления встроенного программного обеспечения с помощью команд FTP/TFTP см. Разд. 21.1.3 на с. 149.

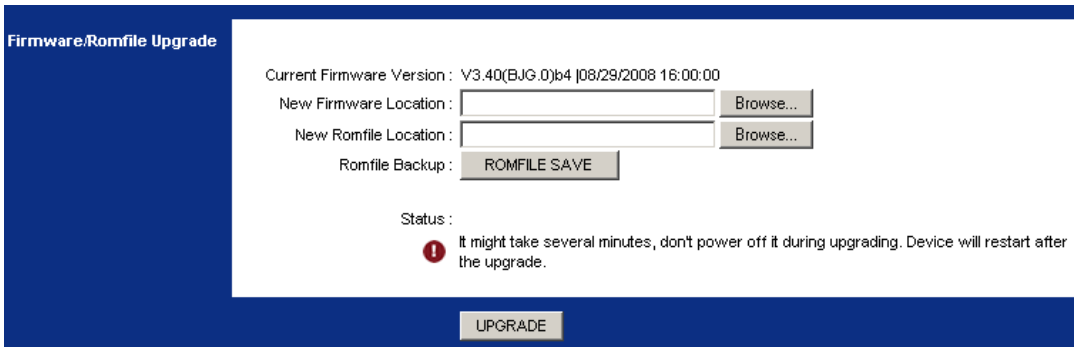
НЕЛЬЗЯ выключать питание устройства P660 во время загрузки встроенного программного обеспечения!

Резервирование файла конфигурации

Резервное сохранение конфигурации позволяет сохранить текущую конфигурацию устройства P660 в файле на компьютере. Если настройка устройства P660 выполнена, и устройство работает нормально, то перед внесением каких-либо изменений настоятельно рекомендуется создать резервную копию файла конфигурации. Файл с резервной копией конфигурации пригодится в случае, если вам придется вернуться к предыдущим настройкам.

Нажмите **Maintenance > Firmware**, чтобы открыть приведенный ниже экран.

Рис. 64 Maintenance > Firmware



В приводимой ниже таблице даны описания полей этого экрана.

Табл. 41 Maintenance > Firmware

ПОЛЕ	ОПИСАНИЕ
Current Firmware Version	Текущая версия и дата создания встроенной программы.
New Firmware Location	Нажмите **Browse...**, чтобы указать местонахождение файла с расширением .bin, который вы хотите загрузить. Необходимо помнить, что архивированные файлы (.zip) необходимо распаковать, прежде чем выполнять загрузку в модем.
New Romfile Location	Функция восстановления конфигурации позволяет загрузить с компьютера в ваше устройство P660 новый или предварительно сохраненный файл конфигурации. Нажмите **Browse...**, чтобы найти файл для загрузки. Необходимо помнить, что архивированные файлы (.zip) необходимо распаковать, прежде чем выполнять загрузку в модем.
Romfile Backup	Нажмите эту кнопку для сохранения текущей конфигурации устройства P660 на компьютере.
UPGRADE	Нажмите эту кнопку для запуска процесса загрузки.

22

Перезапуск системы

22.1 Обзор

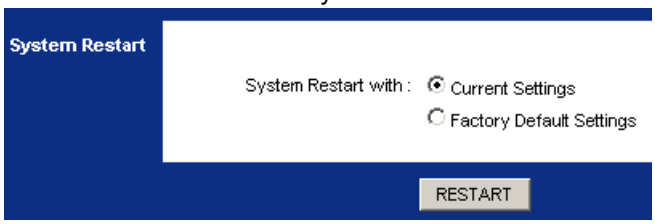
В этой главе описывается, как перезапустить ваше устройство P660.

22.2 Экран перезапуска системы

Этот экран позволяет выполнить удаленную перезагрузку устройства P660 без выключения электропитания. Вам может это потребоваться, например, при зависании устройства P660.

Нажмите **Maintenance** > **SysRestart**, чтобы открыть приведенный ниже экран.

Рис. 65 Maintenance > System Restart



В приводимой ниже таблице даны описания полей этого экрана.

Табл. 42 Maintenance > System Restart

ПОЛЕ	ОПИСАНИЕ
System Restart with	Выберите **Current Settings** для сохранения параметров конфигурации после перезагрузки устройства P660. Это не влияет на конфигурацию устройства P660. Выберите **Factory Default Settings** для удаления всех данных конфигурации пользователя и возврата настроек устройства P660 к заводским значениям по умолчанию.
RESTART	Нажмите эту кнопку для перезагрузки устройства P660.

23

Диагностика

23.1 Обзор

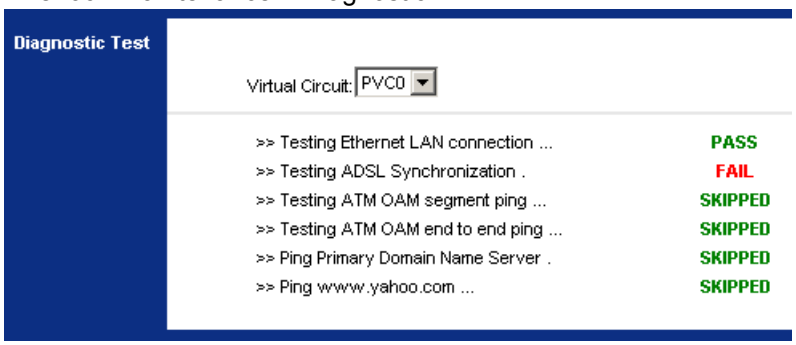
Информация в этих окнах представлена в режиме только для чтения и призвана помочь определить неисправность устройства P660.

23.2 Экран диагностики

Используйте этот экран для проверки вашего подключения и тестирования IP-адреса. Выберите из разворачивающегося списка в окне виртуальный канал, который вы хотите проверить.

Нажмите **Maintenance > Diagnostic**, чтобы открыть показанный ниже экран.

Рис. 66 Maintenance > Diagnostic



Часть VII
Поиск и устранение неисправностей и характеристики устройства

24

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 систему устройства P660
- Доступ в Интернет

24.1 Питание, подключение оборудования и светодиоды

? Устройство P660 не включается. Ни один из светодиодов не светится.

1. Убедитесь, что устройство P660 включено.
2. Убедитесь, что используется адаптер или кабель питания из комплекта поставки устройства P660.
3. Убедитесь, что адаптер или кабель питания подключен к устройству P660 и к соответствующему источнику питания. Убедитесь, что источник питания включен.
4. Выключите и снова включите устройство P660.
5. Если неисправность не устранена, свяжитесь с поставщиком оборудования.

? Один из светодиодов работает неправильно.

1. Убедитесь, что вы знаете, как светодиод должен работать в нормальном режиме. См. Разд. 1.5 на с. 27.
2. Проверьте подключение оборудования. См. Краткое руководство.
3. Убедитесь, что кабели не повреждены. Для замены поврежденных кабелей свяжитесь с поставщиком оборудования.
4. Выключите и снова включите устройство P660.
5. Если неисправность не устранена, обратитесь к поставщику оборудования.

24.2 Доступ и регистрация в систему устройства P660

Потеряна информация об IP-адресе устройства P660.

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 P660, установленный для шлюза по умолчанию на компьютере. Чтобы выполнить это на компьютере под управлением Windows, нажмите кнопку **Start (Пуск) > Run (Выполнить)**, введите команду **cmd** и затем **ipconfig**. IP-адрес **Default Gateway (Шлюз по умолчанию)** может являться IP-адресом устройства P660 (это зависит от конкретной сети). Введите этот IP-адрес в Интернет-браузере.
3. Если этот пароль не работает, выполните сброс устройства к заводским настройкам. См. Разд. 1.6 на с. 28.

Утерян пароль.

1. По умолчанию установлен пароль **1234**.
2. Если этот пароль не работает, выполните сброс устройства к заводским настройкам. См. Разд. 1.6 на с. 28.

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. 7.2 на с. 68), 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 P660.
2. Проверьте подключение оборудования и удостоверьтесь, что светодиоды работают в нормальном режиме. См. Краткое руководство.
3. Убедитесь, что Интернет-браузер не блокирует всплывающие окна и обеспечивает поддержку JavaScripts и Java. См. Прил. B на с. 191.
4. Если в вашей сети есть сервер DHCP, убедитесь, что ваш компьютер использует динамический IP-адрес. См. Прил. A на с. 175. По умолчанию устройство P660 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 P660. См. Прил. A на с. 175.

5 Выполните сброс устройства к заводским настройкам по умолчанию и попробуйте получить доступ к устройству P660 с IP-адресом по умолчанию. См. Разд. 1.6 на с. 28.
6 Если неисправность не устранена, обратитесь к сетевому администратору или поставщику оборудования или выполните дополнительные рекомендации.

Дополнительные рекомендации

- Попробуйте получить доступ к устройству P660 с использованием другой службы, например, Telnet. Если доступ к устройству P660 существует, проверьте параметры удаленного управления и правила брандмауэра, чтобы выяснить причину, по которой устройство P660 не отвечает по HTTP.

Экран **Login** отображается, но невозможно выполнить вход в систему устройства P660.

1 Убедитесь, что пароль введен правильно. По умолчанию установлен пароль **1234**. Символы в это поле вводятся с учетом регистра, поэтому убедитесь, что клавиша [Caps Lock] выключена.
2 Нельзя получить доступ к Web-конфигуратору, если другой пользователь подключился к P660 через Telnet. Подключитесь к устройству P660 позднее или попросите зарегистрированного пользователя выполнить выход из системы.
3 Выключите и снова включите устройство P660.
4 Если этот пароль не работает, выполните сброс устройства к заводским настройкам. См. Разд. 1.6 на с. 28.

Невозможно подключиться к устройству P660 через Telnet.

См. рекомендации по поиску и устранению неисправностей в 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 микропрограммы с помощью FTP.

См. рекомендации по поиску и устранению неисправностей в Не отображается окно Web-конфигуратора Login или отсутствует доступ в систему. Рекомендации по настройке браузера сюда не относятся.

24.3 Доступ в Интернет

Невозможно получить доступ в Интернет.

1. Проверьте подключение оборудования и удостоверьтесь, что светодиоды работают в нормальном режиме. См. Краткое руководство и Разд. 1.5 на с. 27.
2. Проверьте правильность ввода параметров учетной записи, предоставленных Интернет-провайдером. Символы в эти поля вводятся с учетом регистра, поэтому убедитесь, что клавиша [Caps Lock] выключена.
3. Если вы пытаетесь подключиться к сети Интернет по беспроводной связи, убедитесь, что клиентские настройки беспроводного клиента совпадают с настройками в точке доступа.
4. Отключите все кабели от устройства и еще раз выполните инструкции Краткого руководства пользователя.
5. Если неисправность не устранена, обратитесь к Интернет-провайдеру.

Невозможно получить доступ в Интернет. Доступ в Интернет настроен через устройство P660, но подключение к Интернету больше не работает.

1. Проверьте подключение оборудования и удостоверьтесь, что светодиоды работают в нормальном режиме. См. Краткое руководство и Разд. 1.5 на с. 27.
2. Выключите и снова включите устройство P660.
3. Если неисправность не устранена, обратитесь к Интернет-провайдеру.

Подключение к Интернету работает медленно или нестабильно.

1. Возможно, что локальная сеть перегружена. Посмотрите на светодиоды и проверьте их работу согласно Разд. 1.5 на с. 27. Если устройство P660 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 P660, 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 P660.
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.

25

Характеристики устройства

В следующей таблице представлены характеристики оборудования и программного обеспечения устройства P660.

25.1 Технические характеристики оборудования

Табл. 43 Технические характеристики оборудования

Габариты	110(Ш) x 107(Д) x 36(В) мм
Вес	165 г
Питание	При коммутации 9 В постоянного тока 1 А
Порт Ethernet LAN	1 порт Ethernet MDI/MDI-X 10/100 Мбит/с RJ-45 с автоматическим выбором скорости
Порт ADSL	1 порт RJ-11 FXS POTS
Порт USB (P660RU3)	1 порт USB 1.1
Кнопка RESET	Восстанавливает заводские значения по умолчанию
Рабочая температура	0° C ~ 40° C
Температура хранения	-20 °C ~ 60 °C
Рабочая влажность	20 % ~ 85 %
Относительная влажность при хранении	20 % ~ 90 %

25.2 Характеристики программного обеспечения

Табл. 44 Характеристики программного обеспечения

IP-адрес по умолчанию	192.168.1.1
Маска подсети по умолчанию	255.255.255.0 (24 бита)
Имя пользователя по умолчанию	admin
Пароль по умолчанию	1234
IP-диапазон сервера DHCP	от 192.168.1.32 до 192.168.1.64

Табл. 44 Характеристики программного обеспечения (продолжение)

Управление устройством	Web-конфигуратор упрощает настройку широкого спектра функций устройства P660.
Обновление встроенного программного обеспечения	Загрузите новую версию микропрограммы (если есть) с веб-сайта ZyXEL в устройство P660 с помощью Web-конфигуратора, по FTP или TFTP. ПРИМЕЧАНИЕ: Необходимо загружать встроенное программное обеспечение строго в соответствии с конкретной моделью устройства!
Резервное сохранение и восстановление конфигурации	Сделайте копию конфигурации устройства P660. Эту копию можно загрузить в устройство P660 позже, если потребуется вернуться к предыдущей конфигурации.
Трансляция сетевых адресов (NAT)	Каждый компьютер в сети должен иметь уникальный IP-адрес. Используйте функцию NAT для преобразования общедоступного IP-адреса(ов) в несколько частных IP-адресов для компьютеров вашей сети.
Переадресация портов	Если в сети есть сервер (например, 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 P660 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.
Поддержка динамических DNS	Поддержка динамической DNS (Domain Name System – Система доменных имен) позволяет использовать фиксированный URL, например, www.zyxel.com с динамическим IP-адресом. Для использования этой услуги необходимо зарегистрироваться у провайдера услуг динамического DNS.
Многоадресная рассылка IP	Многоадресная рассылка IP используется для отправки трафика определенной группе компьютеров. Устройство P660 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 P660. Время также можно установить вручную. Дата и время используются в регистрационных журналах.
Журналы регистрации	Используйте журналы регистрации для поиска и устранения неисправностей.
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 от обслуживания). 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).
Фильтры IP/MAC-адресов	Функции фильтрации пакетов вашего устройства позволяют повысить уровень защиты и управления сетью.
Фильтр приложений	Фильтр приложений позволяет блокировать программы мгновенных сообщений.

Табл. 44 Характеристики программного обеспечения (продолжение)

Фильтр URL	Фильтрация по URL дает возможность блокировать доступ к веб-сайтам по определенным ключевым словам в URL.
Качество услуги (QOS)	Для определенных типов трафика и определенных компьютеров вашей сети можно зарезервировать полосу пропускания и задать им приоритет для повышения эффективности управления трафиком.
Удаленное управление	Удаленное управление позволяет с помощью выбранной службы (например, HTTP или FTP) с компьютера в сети (LAN или WAN) подключиться к устройству P660.
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
Поддержка множества PVC (Permanent Virtual Circuits/Постоянные виртуальные каналы)	Ваше устройство поддерживает до 8 постоянных виртуальных каналов (PVC).
Стандарты ADSL	ANSI T1.413, изд. 2 G.dmt(G.992.1); G.lite (G.992.2) ADSL2 G.dmt.bis (G.992.3) ADSL2 G.lite.bis (G.992.4) 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 A/L/M TR-067/TR-100

Табл. 44 Характеристики программного обеспечения (продолжение)

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
Управление	Встроенный Web-конфигуратор CLI (Интерпретатор командной строки) SNMP v1 & v2c с MIB II Встроенный сервер FTP/TFTP для обновления аппаратного обеспечения, а также обновления и восстановления файла конфигурации Удаленное управление: Telnet Удаленное управление: Telnet, FTP, Web, SNMP и DNS Удаленное обновление микропрограммы Системный журнал TR-069 F4/F5 OAM

Далее приводится неполный список стандартов, поддерживаемых устройством P660.

Табл. 45 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 – Протокол управления группами сети Интернет (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: Протокол управления группами сети Интернет (версия 2)
RFC 2364	Протокол «точка-точка» поверх уровня адаптации AAL, уровень 5 (PPP через ATM через ADSL)

Табл. 45 Стандарты, поддерживаемые устройством (продолжение)

СТАНДАРТ	ОПИСАНИЕ
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
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.
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.
MBM v2	Управление пропускной способностью среды передачи (версия 2)
RFC 2383	ST2+ через спецификацию протокола ATM — версии UNI 3.1
TR-069	Стандарт форума DSL TR-069 для управления оборудованием глобальной связи, расположенным на территории клиента.
1.363.5	Совместимый с уровнем AAL5 подуровень сегментации и сборки (SAR)

25.3 Характеристики адаптера питания

Табл. 46 P660: характеристики последовательного адаптера питания

СЕВЕРОАМЕРИКАНСКИЕ СТАНДАРТЫ	
Модель адаптера питания переменного тока	При коммутации 9 В постоянного тока 1.0 A US
Входное питание	100-240 В переменного тока, 50/60 Гц
Выходная мощность	Пост. ток 9 В/1.0A
Потребляемая мощность	Макс. 9 Вт
Нормы техники безопасности	ANSI/UL 60950-1, CSA 60950-1

Табл. 46 P660: характеристики последовательного адаптера питания (продолжение)

СТАНДАРТ ЕВРОПЕЙСКОГО СОЮЗА	
Модель адаптера питания переменного тока	При коммутации 9 В постоянного тока 1.0 A EU
Входное питание	100-240 В переменного тока, 50/60 Гц
Выходная мощность	Пост. ток 9 В/1.0A
Потребляемая мощность	Макс. 9 Вт
Нормы техники безопасности	CE, GS или TUV, EN60950-1
СТАНДАРТЫ ВЕЛИКОБРИТАНИИ	
Модель адаптера питания переменного тока	При коммутации 9 В постоянного тока 1.0 A UK
Входное питание	100-240 В переменного тока, 50/60 Гц
Выходная мощность	Пост. ток 9 В/1.0A
Потребляемая мощность	Макс. 9 Вт
Нормы техники безопасности	CE, GS или TUV, EN60950-1

Часть VIII Приложения и алфавитный указатель

В приложениях приводится общая информация. Описание некоторых деталей может не относиться в 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.

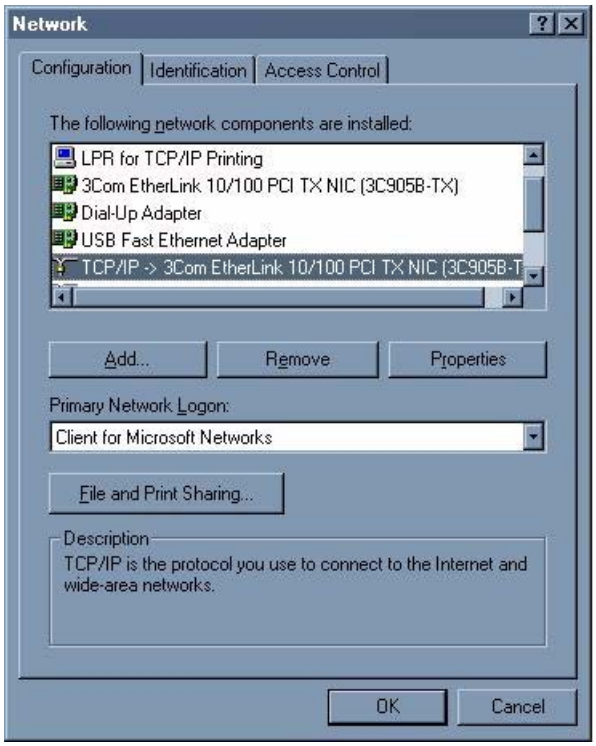
После установки компонентов TCP/IP, настройте параметры TCP/IP для соединения с сетью.

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. 67 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**.

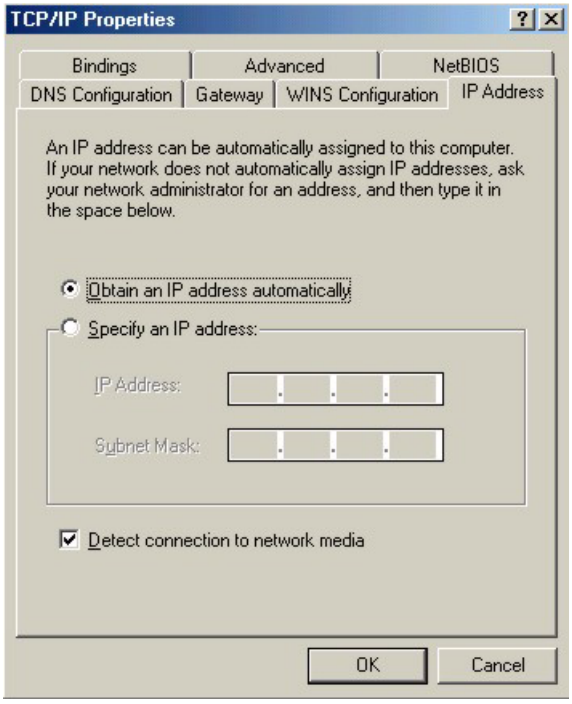
Если необходимо установить Клиента для сетей Microsoft:

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

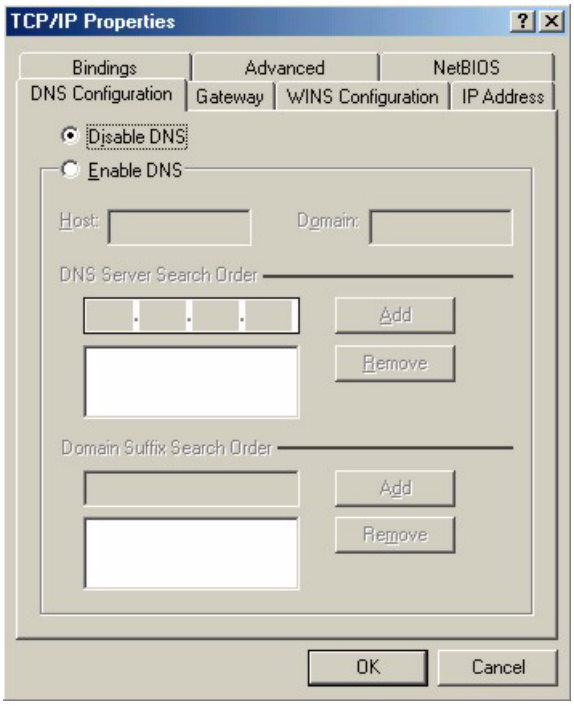
1. В окне **Network (Сеть)** выберите закладку **Configuration (Конфигурация)**, выберите пункт TCP/IP для вашей сетевой платы и нажмите **Properties (Свойства)**.
2. Выберите закладку **IP-адрес**.
   - Если вы используете динамический IP-адрес, выберите **Obtain an IP address automatically (Получить 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. 68 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. 69 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

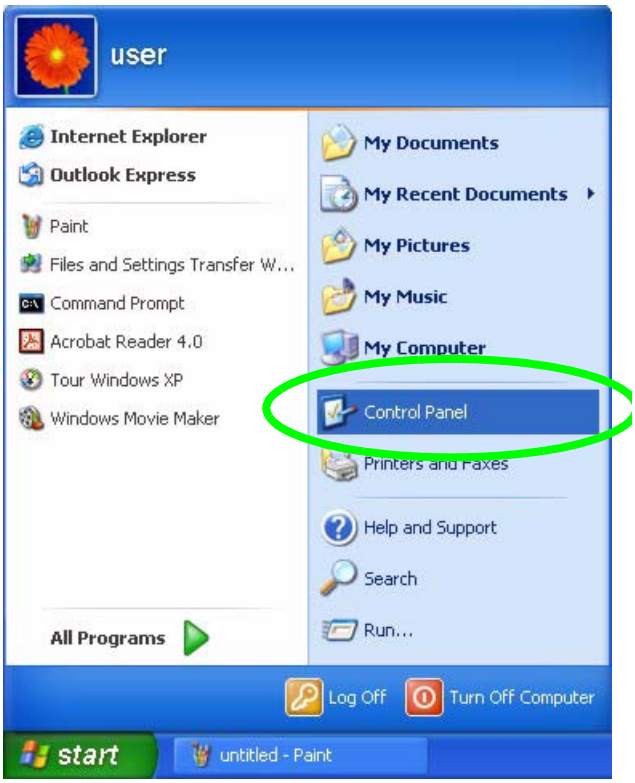
1 Нажмите кнопку **Start (Пуск)**, а затем выберите пункт **Run (Выполнить)**.
2 В окне **Run (Выполнить)** введите команду «winipcfg», а затем нажмите **OK** для отображения окна **IP Configuration (Конфигурация IP)**.
3 Выберите свой сетевой адаптер. При этом должны отображаться IP-адрес и маска подсети 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. 70 Windows XP: Меню Пуск

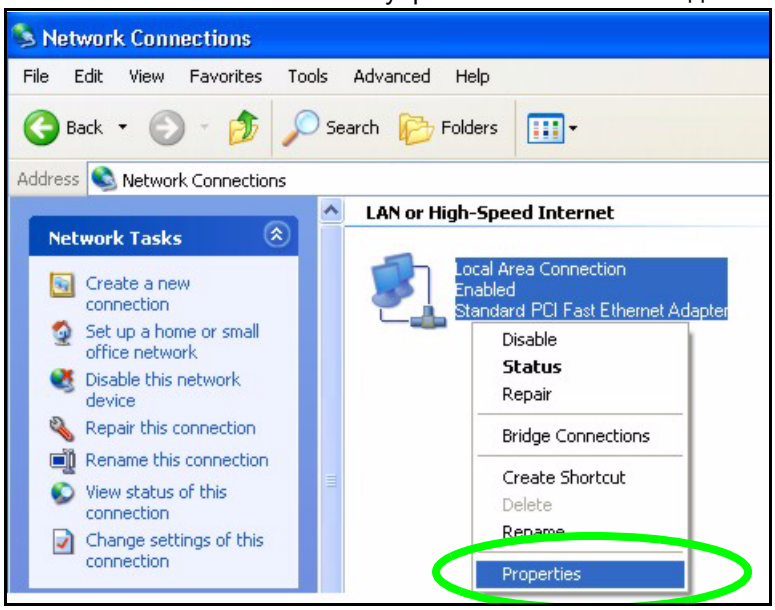


2 На **Панели управления** дважды щелкните **Network Connections (Сетевые подключения)** (**Network and Dial-up Connections (Сеть и удаленный доступ к сети)** в Windows 2000/NT).

Рис. 71 Windows XP: Control Panel (Windows XP: Панель управления)

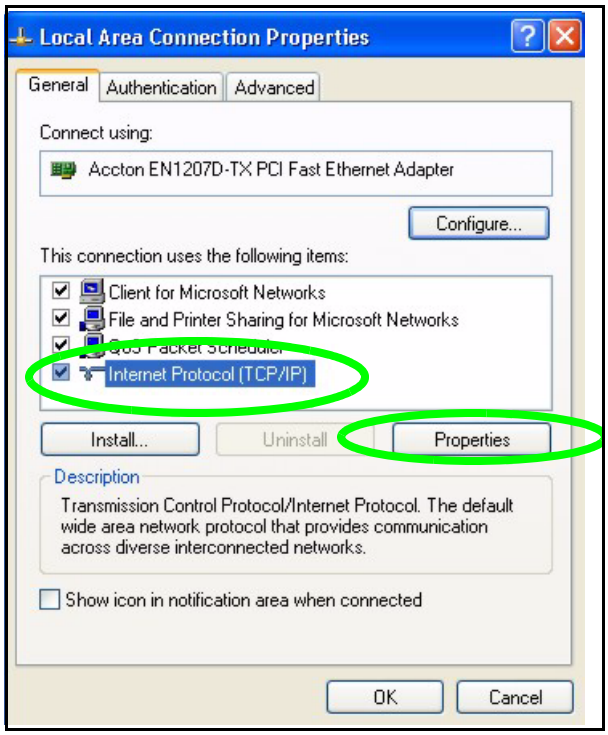
3 Щелкните правой кнопкой мыши значок **Local Area Connection (Подключение по локальной сети)** и выберите **Properties (Свойства)**.

Рис. 72 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)**.

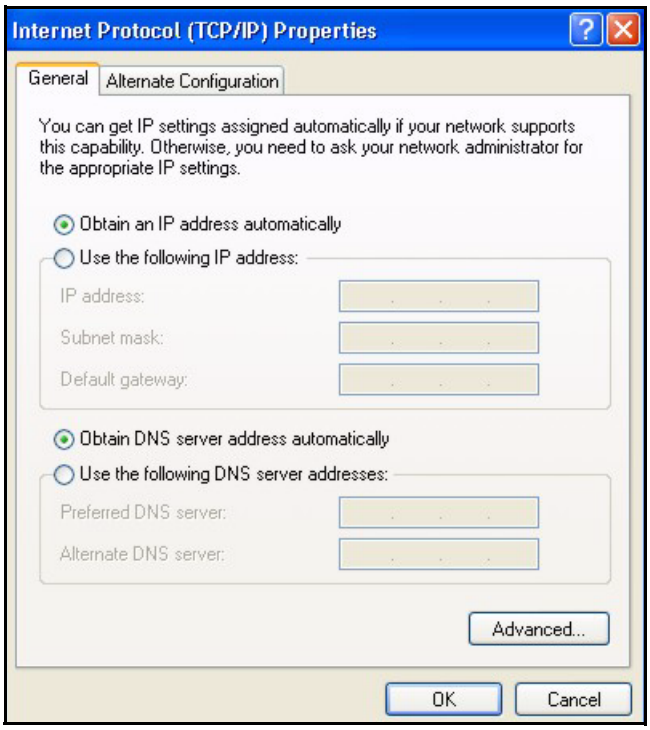
Рис. 73 Windows XP: Подключение по локальной сети: Свойства



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. 74 Windows XP: Свойства: Протокол Интернета (TCP/IP)



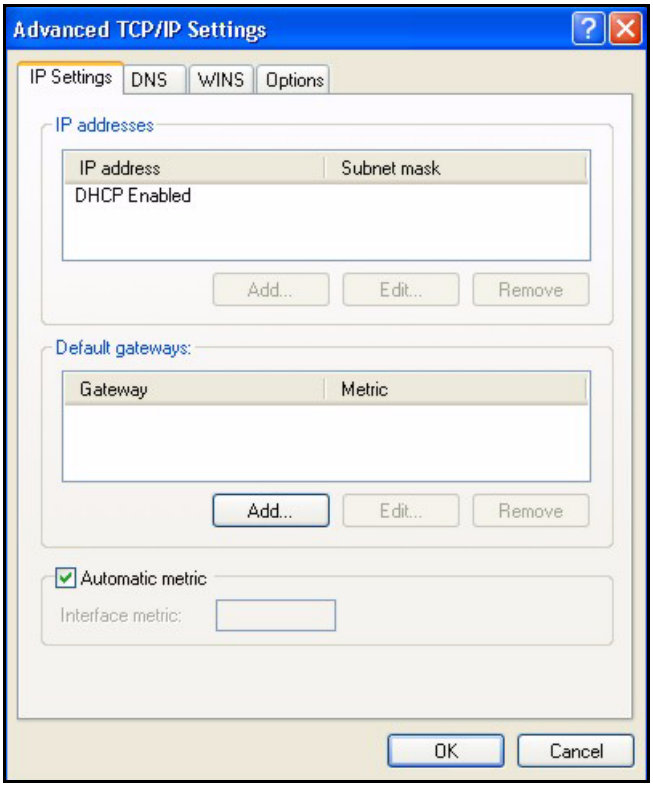
6 Если вы не знаете IP-адрес шлюза, удалите все предварительно настроенные шлюзы на закладке **IP Settings (Параметры IP)** и нажмите **OK**.

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. 75 Windows XP: Дополнительные свойства TCP/IP

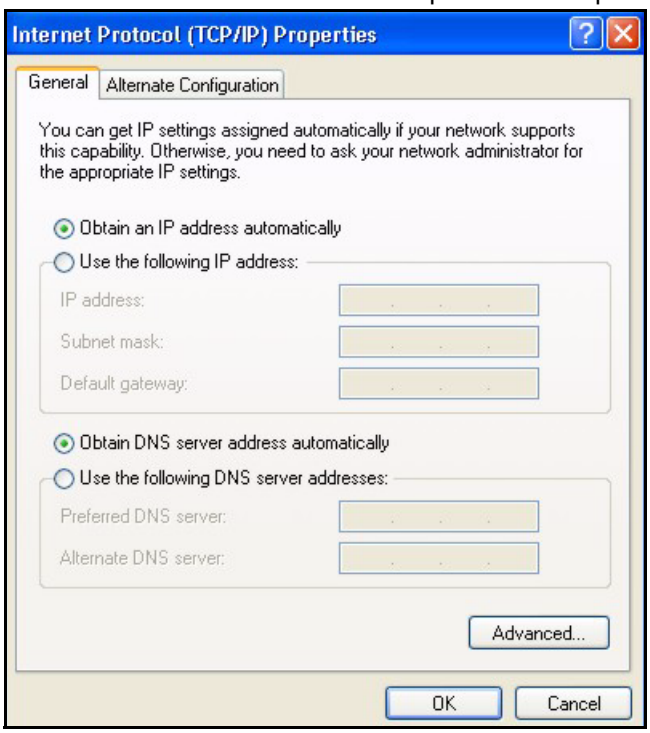


7 В окне **Internet Protocol TCP/IP Properties (Свойства: Протокол Интернета (TCP/IP))** на закладке **General (Общие)** в Windows XP:

- 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. 76 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

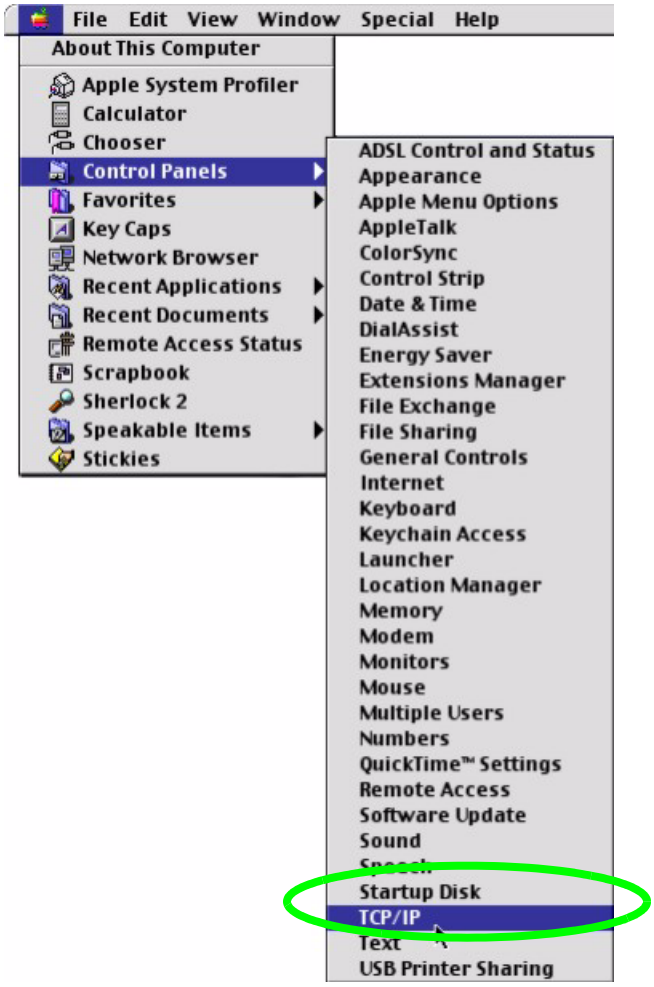
1 Щелкните **Start (Пуск), All Programs (Все программы), Accessories (Стандартные)**, а затем **Command Prompt (Командная строка)**.

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

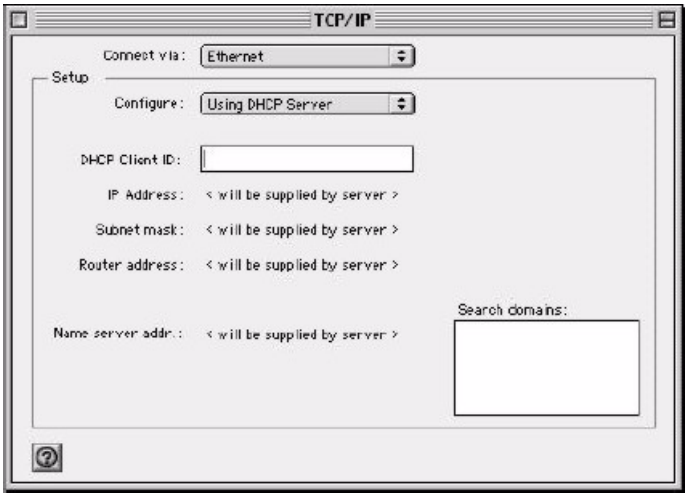
1 Нажмите кнопку меню **Apple**, выберите **Control Panel (Панель управления)**, а затем дважды щелкните **TCP/IP**, чтобы открыть **TCP/IP Control Panel (Панель управления TCP/IP)**.

Рис. 77 Macintosh OS 8/9: Меню Apple



2 Выберите **Ethernet built-in (Встроенный сетевой контроллер)** из списка **Connect via (Подключение через...)**.

Рис. 78 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.

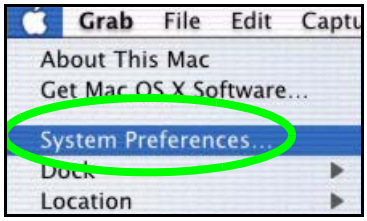
Проверка настроек

Проверьте свойства TCP/IP в окне **TCP/IP Control Panel (Панель управления TCP/IP)**.

Macintosh OS X

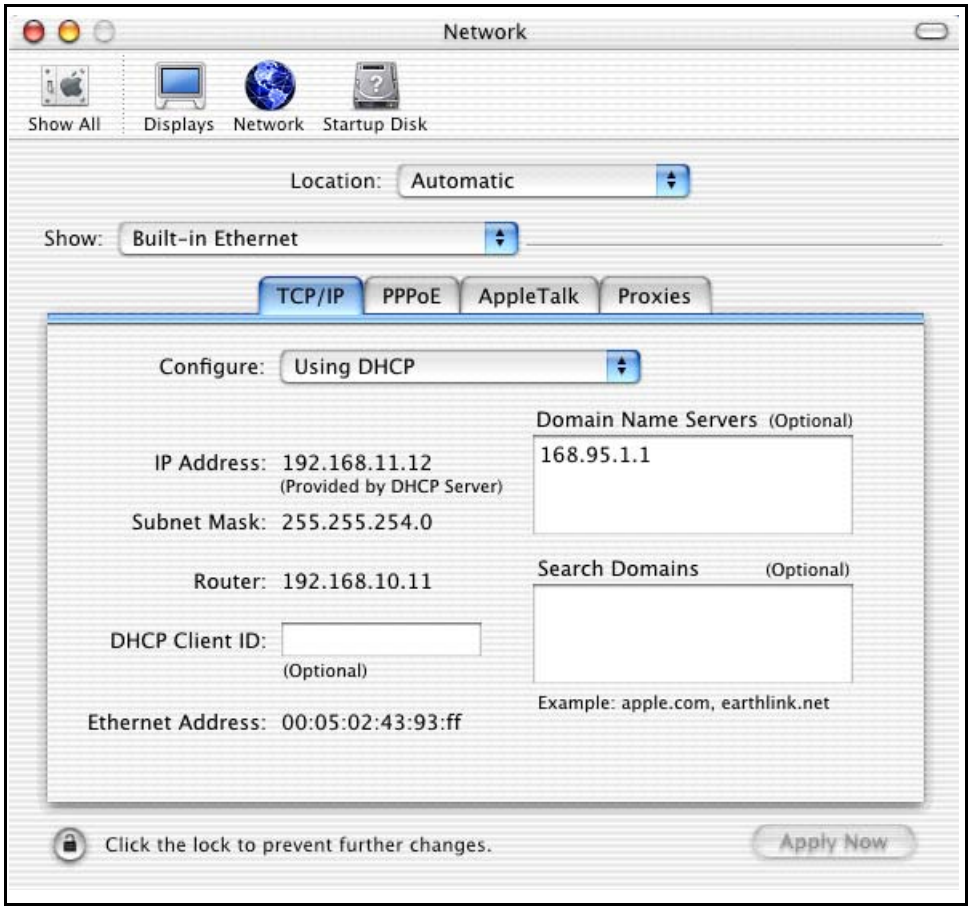
1 Нажмите кнопку меню **Apple** и затем **System Preferences (Настройки системы)**, чтобы открыть окно **System Preferences (Настройки системы)**.

Рис. 79 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. 80 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.

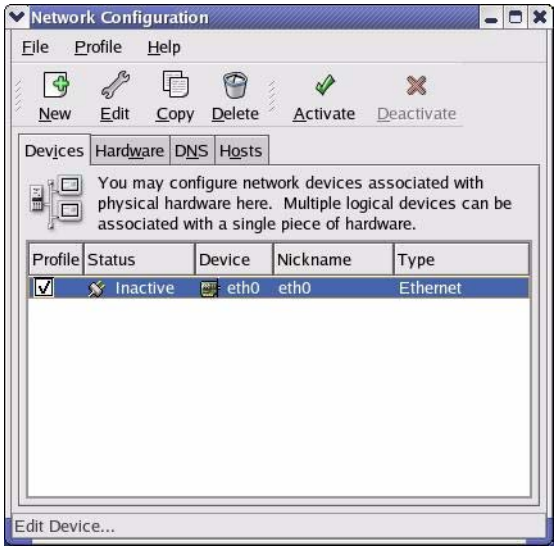
Вы должны быть зарегистрированы в системе в качестве корневого администратора.

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. 81 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)**.

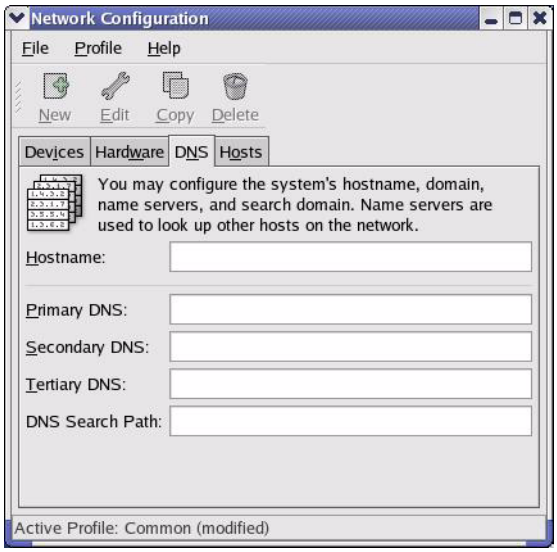
Рис. 82 Red Hat 9.0: KDE: Устройство Ethernet: Общие

- 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.

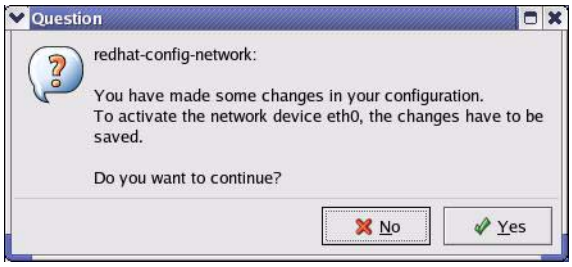
Рис. 83 Red Hat 9.0: KDE: Конфигурация сети: DNS



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. 84 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, 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. 85 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. 86 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. 87 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. 88 Red Hat 9.0: Перезапуск карты Ethernet

```
[root@localhost init.d]# network restart

Shutting down interface eth0:                  [OK]
Shutting down loopback interface:              [OK]
Setting network parameters:                    [OK]
Bringing up loopback interface:                [OK]
Bringing up interface eth0:                    [OK]
```

Проверка настроек

Чтобы проверить настройки TCP/IP, введите «`ifconfig`» в окне терминала.

Рис. 89 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 Web-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

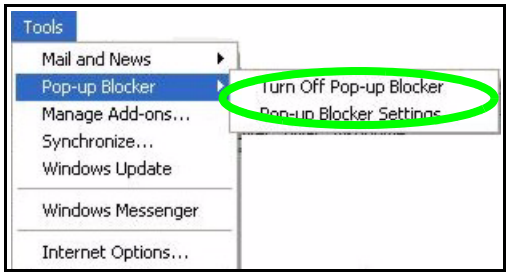
При регистрации пользователя устройства может возникнуть необходимость отключения блокирования всплывающих окон.

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)**

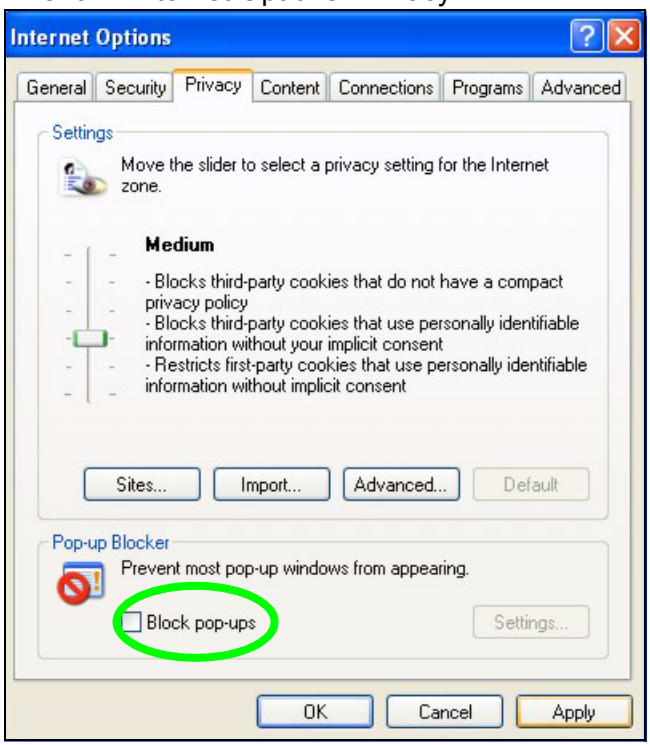
Рис. 90 Pop-up Blocker



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. 91 Internet Options: Privacy



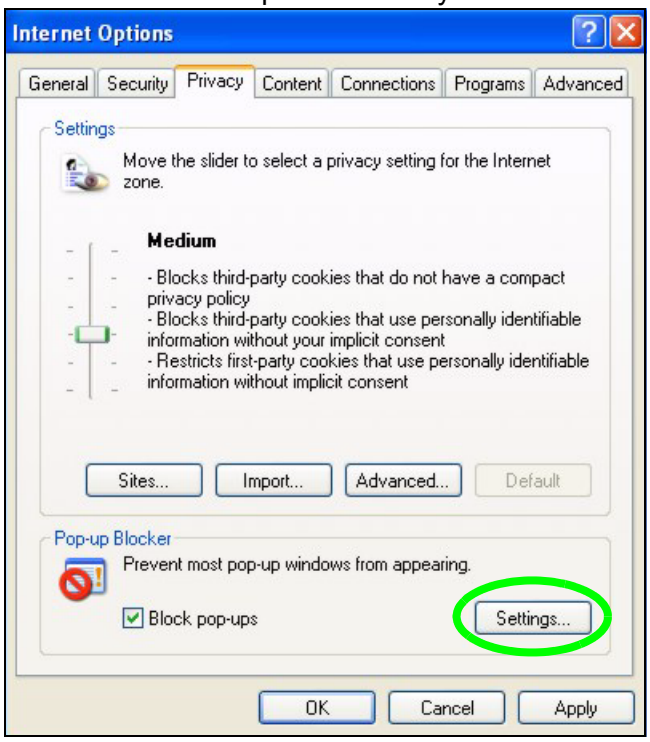
3. Нажмите **Apply**, чтобы сохранить настройки.

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)**.

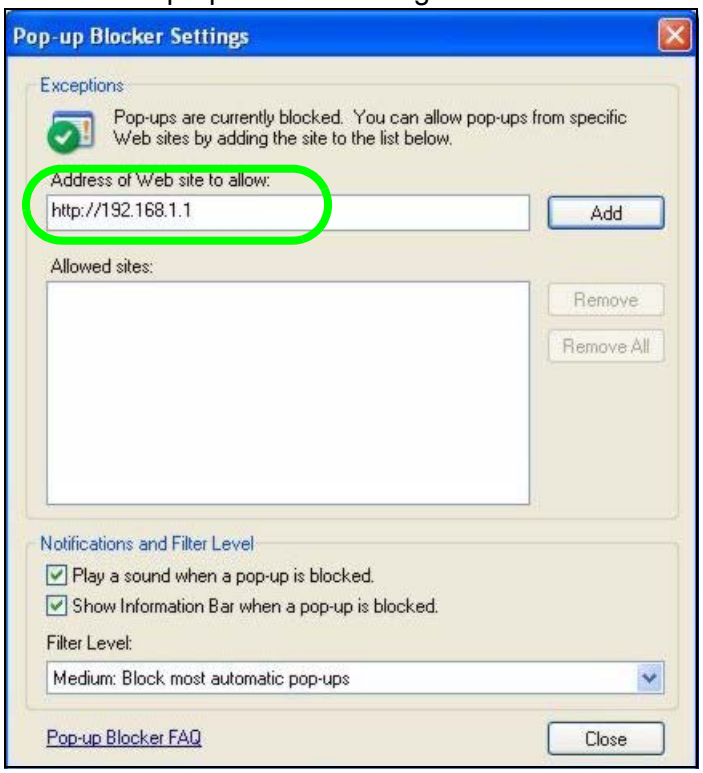
Рис. 92 Internet Options: Privacy



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. 93 Pop-up Blocker Settings



5 Для возврата на вкладку **Privacy (Конфиденциальность)** нажмите кнопку **Close (Закрыть)**.

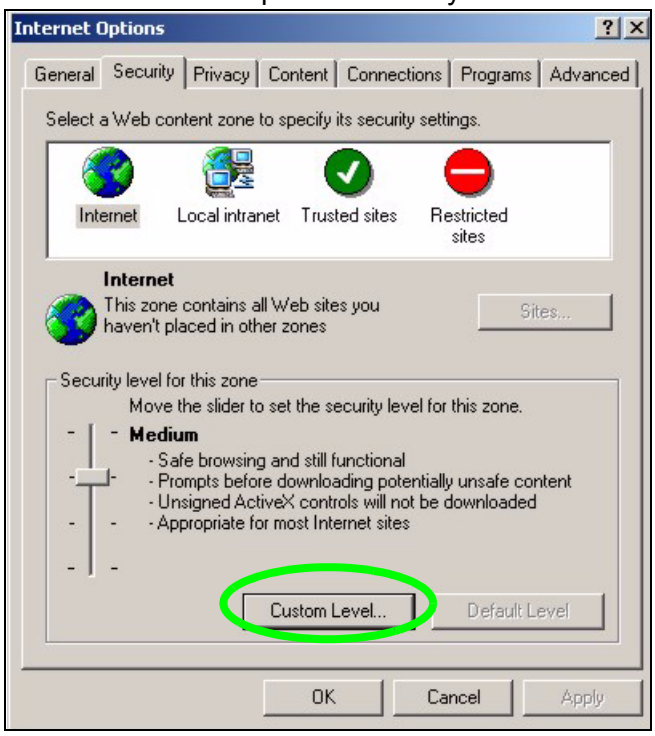
6 Нажмите кнопку **Apply (Применить)**, чтобы сохранить настройки.

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. 94 Internet Options: Security



2 Нажмите кнопку **Custom Level... (Другой...)**.

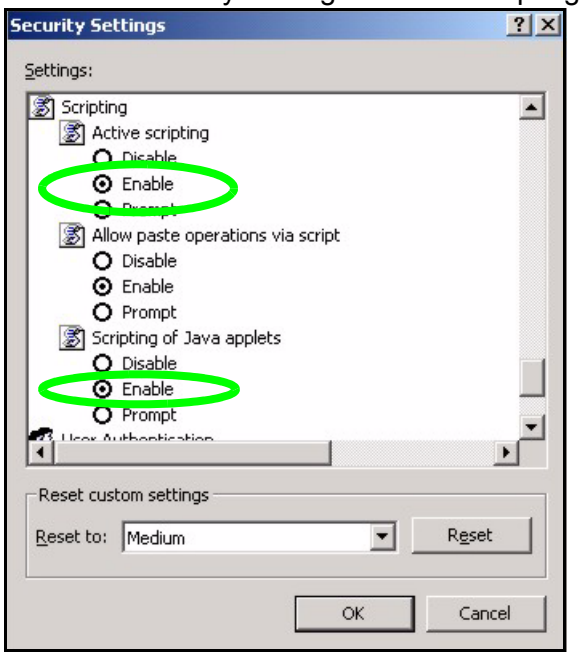
3 Пролистайте до раздела **Scripting (Сценарии)**.

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.

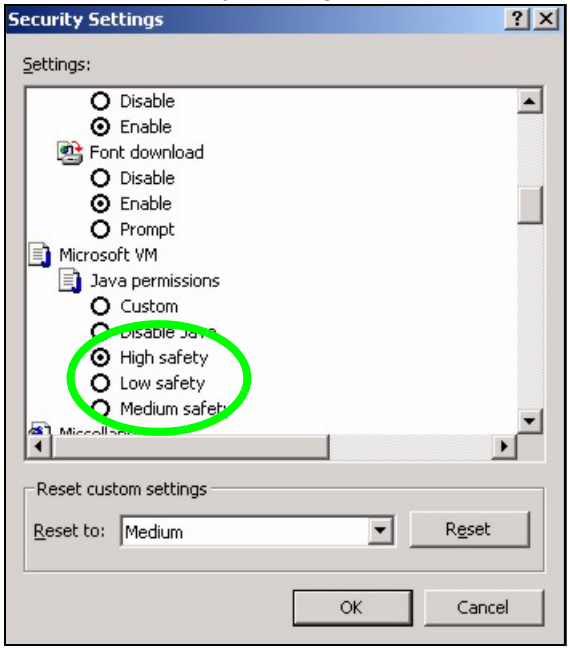
Рис. 95 Security Settings — Java Scripting



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.

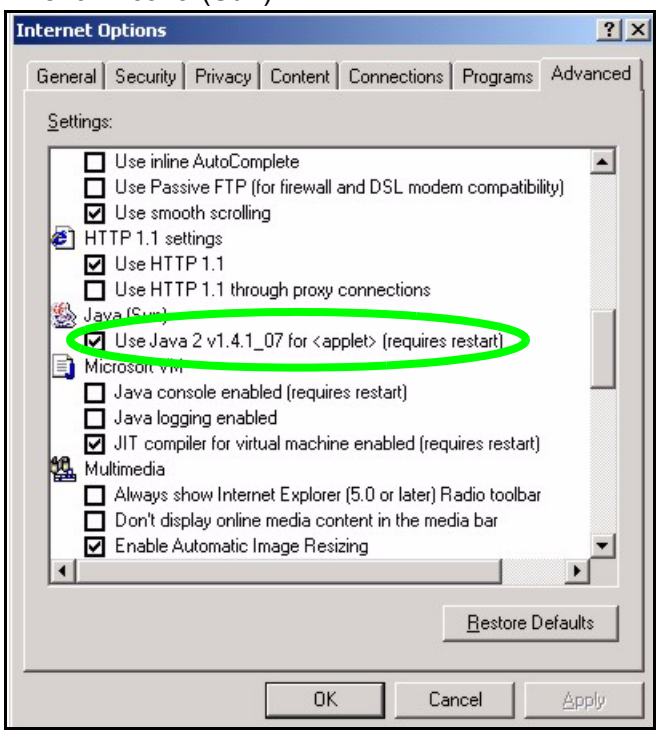
Рис. 96 Security Settings — Java



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.

Рис. 97 Java (Sun)



C

IP-адреса и организация подсетей

В этом приложении представлена информация об IP-адресах и масках подсети.

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

Описание IP-адресов

Одна часть IP-адреса является номером сети, а другая часть — номером узла. Так же, как все дома, находящиеся на одной улице, имеют общее название улицы, все узлы в локальной сети имеют общий номер сети. Так же, как каждый дом имеет индивидуальный номер, каждый узел в сети имеет уникальный идентификационный номер — идентификатор узла. Номер сети используется маршрутизаторами при отправке пакетов в соответствующую сеть, а идентификатор узла определяет конкретное устройство в этой сети для доставки этих пакетов.

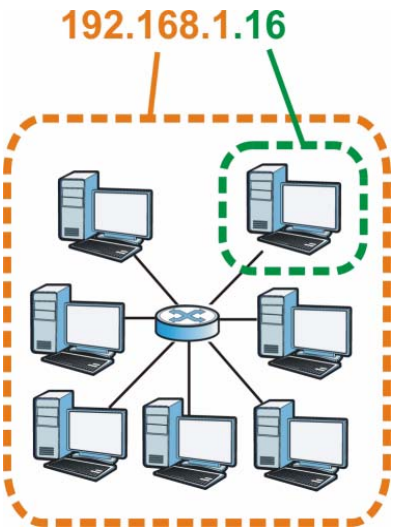
Структура

IP-адрес состоит их четырех частей, записанных в десятичном виде с разделительными точками, например: 192.168.1.1. Каждая из четырех частей называется байтом. Байт — это восьмизначное двоичное число (например, число 11000000 в десятичном представлении равно 192).

Следовательно, каждый байт имеет диапазон возможных значений от 00000000 до 11111111 в двоичном формате, или от 0 до 255 в десятичном.

На следующем рисунке показан пример IP-адреса, в котором три первых байта (192.168.1) являются номером сети, а четвертый байт (16) является идентификатором узла.

Рис. 98 Номер сети и идентификатор узла



То, какую часть IP-адреса занимает номер сети, а какую — идентификатор узла, определяется маской подсети.

Маски подсети

С помощью маски подсети можно определить, какие биты являются частью номера сети, а какие — частью идентификатора узла (используя операцию логического «И»). Термин «подсеть» это сокращенное название для «физически независимого сегмента сети».

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.

В следующем примере показаны маска подсети, определяющая номер сети (жирным шрифтом), и идентификатор узла для IP-адреса 192.168.1.2.

Табл. 47 Маска подсети — указывает номер сети

	1-Й БАЙТ: (192)	**2-Й БАЙТ: (168)**	**3-Й БАЙТ: (1)**	**4-Й БАЙТ: (2)**
IP-адрес (в двоичной форме)	11000000	10101000	00000001	00000010
Маска подсети (в двоичной форме)	**11111111**	**11111111**	**11111111**	00000000
Номер сети	**11000000**	**10101000**	**00000001**	
Идентификатор узла				00000010

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.

Маски подсети определяют какую часть в адресе составляет номер сети (т. е. биты со значением «1»). Например, «8-битная маска» означает, что первые 8 битов маски являются единицами, а оставшиеся 24 бита — нулями.

Маски подсети записываются в десятичном виде с разделительными точками, так же, как и IP-адреса. В следующем примере показаны 8-битные, 16-битные, 24-битные и 29-битные маски подсети в двоичном и десятичном виде.

Табл. 48 Маски подсети

	ДВОИЧНАЯ ФОРМА				В ДЕСЯТИЧНОМ ВИДЕ
	1-Й БАЙТ:	2-Й БАЙТ:	3-Й БАЙТ:	4-Й БАЙТ:	
8-битная маска	11111111	00000000	00000000	00000000	255.0.0.0
16-битная маска	11111111	11111111	00000000	00000000	255.255.0.0
24-битная маска	11111111	11111111	11111111	00000000	255.255.255.0
29-битная маска	11111111	11111111	11111111	11111000	255.255.255.248

Размер сети

Размер сети определяет максимально возможное число узлов, которое может находиться в сети. Чем больше число битов в номере сети, тем меньше число битов, остающихся для идентификатора узла.

IP-адрес, в котором идентификатор узла состоит только из нулей, является IP-адресом сети (например, 192.168.1.0 с 24-битной маской подсети). IP-адрес, в котором идентификатор узла состоит только из единиц, является широковещательным адресом для этой сети (например, 192.168.1.255 с 24-битной маской подсети).

Поскольку эти два IP-адреса нельзя использовать для отдельных узлов, максимально возможное число узлов в сети рассчитывается следующим образом:

Табл. 49 Максимальное число узлов

МАСКА ПОДСЕТИ		РАЗМЕР ИДЕНТИФИКАТОРА УЗЛА В АДРЕСЕ		МАКСИМАЛЬНОЕ ЧИСЛО УЗЛОВ
8 бита	255.0.0.0	24 бита	$2^{24} – 2$	16777214
16 бита	255.255.0.0	16 бита	$2^{16} – 2$	65534
24 бита	255.255.255.0	8 бита	$2^{8} – 2$	254
29 бита	255.255.255.248	3 бита	$2^{3} – 2$	6

Записи маски подсети

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 путем записи после адреса символа «/» и количества бит с единицами.

Например, запись 192.1.1.0 /25 равносильна записи 192.1.1.0 с маской подсети 255.255.255.128.

В следующей таблице показаны несколько масок подсети с использованием обоих видов записи.

Табл. 50 Альтернативные варианты записи маски подсети

МАСКА ПОДСЕТИ	АЛЬТЕРНАТИВНАЯ ЗАПИСЬ	ПОСЛЕДНИЙ БАЙТ (В ДВОИЧНОЙ ФОРМЕ)	ПОСЛЕДНИЙ БАЙТ (В ДЕСЯТИЧНОЙ ФОРМЕ)
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

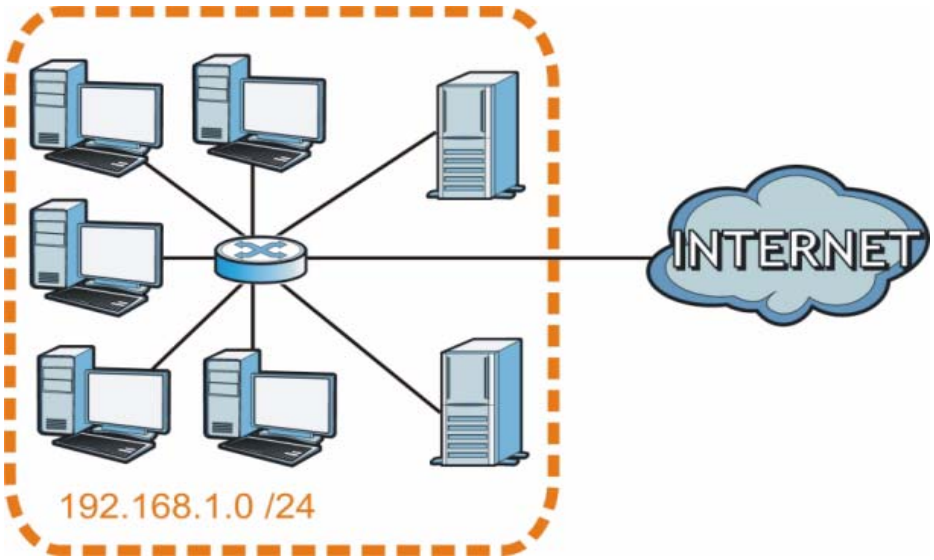
Организация подсетей

Маски подсети также используются для разделения сети на несколько подсетей. В следующем примере сетевой администратор создал 2 подсети, чтобы изолировать группу серверов от остальной сети компании в целях безопасности.

В этом примере адрес сети компании — 192.168.1.0. Первые 3 байта адреса (192.168.1) являются номером сети, а оставшийся байт является идентификатором узла, следовательно, максимальное число узлов в этой сети равно 2^8 – 2 или 254.

На следующем рисунке показана сеть компании до разделения на подсети.

Рис. 99 Пример организации подсетей: до разделения на подсети

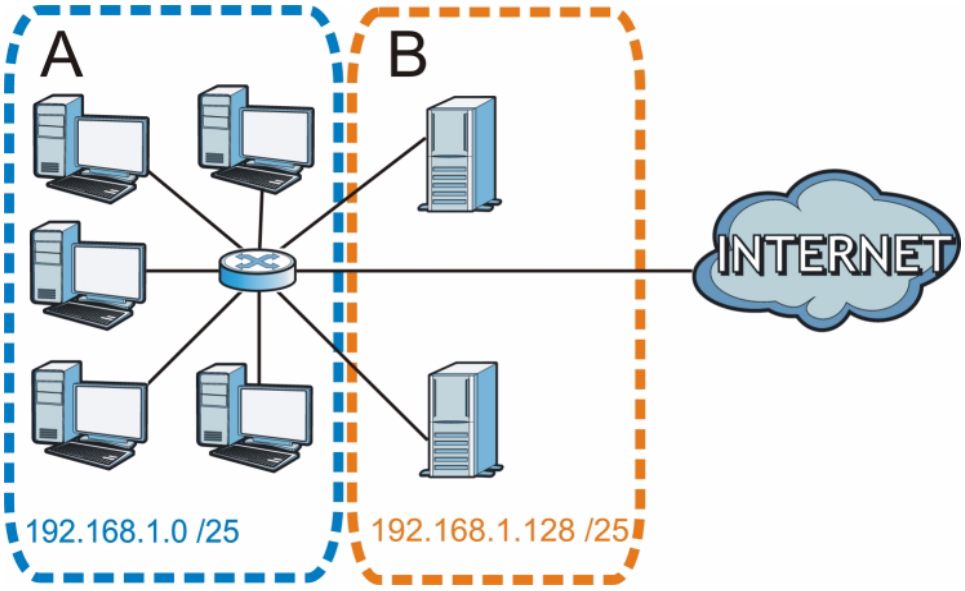


Можно «занять» один бит идентификатора узла для разделения сети 192.168.1.0 на две отдельные подсети. Маска подсети состоит теперь из 25 битов (255.255.255.128 или /25).

«Заимствованный» бит идентификатора узла может принимать значения 0 или 1, давая, таким образом, две подсети; 192.168.1.0 /25 и 192.168.1.128 /25.

На следующем рисунке показана сеть компании после разделения на подсети. Теперь организовано две подсети, **A** и **B**.

Рис. 100 Пример организации подсетей: после разделения на подсети



При 25-битной маске подсети в идентификаторе узла остается 7 битов, следовательно, максимальное число узлов в каждой подсети равно $2^7 – 2$ или 126 (идентификатор узла, состоящий только из нулей является адресом самой подсети, а состоящий только из единиц — широковещательным адресом этой подсети).

Адрес 192.168.1.0 с маской 255.255.255.128 определяет подсеть **A**, а 192.168.1.127 с маской 255.255.255.128 является ее широковещательным адресом. Следовательно, самый младший IP-адрес, который может быть назначен действительному узлу для подсети **A** — 192.168.1.1, а старший — 192.168.1.126.

Подобным образом рассчитывается диапазон идентификаторов узлов для подсети **B**: от 192.168.1.129 до 192.168.1.254.

Пример: четыре подсети

В предыдущем примере продемонстрировано использование 25-битной маски подсети для разделения 24-битного адреса на две подсети. Аналогично для разделения 24-битного адреса 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 $2^6 – 2$ или 62 узла в каждой подсети (все нули в индентификаторе узла обозначают саму подсеть, все единицы являются широковещательным адресом этой подсети).

Табл. 51 Подсеть 1

IP/МАСКА ПОДСЕТИ	НОМЕР СЕТИ	ЗНАЧЕНИЯ БИТОВ ПОСЛЕДНЕГО БАЙТА
IP-адрес (в десятичной форме)	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	Младший идентификатор узла: 192.168.1.1	
Широковещательный адрес: 192.168.1.63	Старший идентификатор узла: 192.168.1.62	

Табл. 52 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	Младший идентификатор узла: 192.168.1.65	
Широковещательный адрес: 192.168.1.127	Старший идентификатор узла: 192.168.1.126	

Табл. 53 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	Младший идентификатор узла: 192.168.1.129	
Широковещательный адрес: 192.168.1.191	Старший идентификатор узла: 192.168.1.190	

Табл. 54 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	Младший идентификатор узла: 192.168.1.193	
Широковещательный адрес: 192.168.1.255	Старший идентификатор узла: 192.168.1.254	

Пример: восемь подсетей

Аналогично используется 27-битная маска для создания 8 подсетей (000, 001, 010, 011, 100, 101, 110 и 111).

В следующей таблице приведены значения битов последнего байта IP-адреса для каждой подсети.

Табл. 55 Восемь подсетей

ПОДСЕТЬ	АДРЕС ПОДСЕТИ	ПЕРВЫЙ АДРЕС	ПОСЛЕДНИЙ АДРЕС	ШИРОКО-ВЕЩАТЕЛЬНЫЙ 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

Проектирование подсетей

В следующей таблице представлена сводка для проектирования подсетей в сети с 24-битным номером сети.

Табл. 56 Проектирование подсетей в сети с 24-битным номером сети

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

В следующей таблице представлена сводка для проектирования подсетей в сети с 16-битным номером сети.

Табл. 57 Проектирование подсетей в сети с 16-битным номером сети

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

Настройка IP-адресов

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

Если Интернет-провайдер не предоставляет явным образом сетевой IP-адрес, то вероятнее всего вы имеете учетную запись одиночного пользователя, и Интернет-провайдер назначает при установлении соединения динамический IP-адрес. В этом случае рекомендуется установить IP-адрес в диапазоне от 192.168.0.0 до 192.168.255.0. Этот диапазон IP-адресов специально зарезервирован Агентством по назначению имен и уникальных параметров протоколов Интернет (IANA) для частного использования. Если не предписано иное, не следует использовать адреса за пределами этого диапазона. Необходимо также включить функцию трансляции сетевых адресов NAT в P660.

Выбрав номер сети, выберите для P660 IP-адрес, который легко запоминается, например, 192.168.1.1, но убедитесь, что никакое другое устройство в вашей сети не использует этот IP-адрес.

Маска подсети определяет сетевую часть IP-адреса. P660 автоматически рассчитывает маску подсети для заданного IP-адреса. Нельзя изменять маску подсети, вычисленную P660, без прямых указаний.

IP-адреса для частных сетей

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

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

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

Независимо от конкретной ситуации, не 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 (Назначение адресов в частных сетях)* и RFC 1466, *Guidelines for Management of IP Address Space (Руководство по управлению пространством IP-адресов).*

D

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. 58 Примеры служб

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.
ESP (IPSEC_TUNNEL)	User-Defined	50	Эта служба используется протоколом туннелирования IPSEC ESP (Протокол обеспечения безопасности инкапсуляции).

Табл. 58 Примеры служб (продолжение)

ИМЯ	ПРОТОКОЛ	ПОРТ(Ы)	ОПИСАНИЕ
FINGER	TCP	79	Finger — 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.

Табл. 58 Примеры служб (продолжение)

ИМЯ	ПРОТОКОЛ	ПОРТ(Ы)	ОПИСАНИЕ
NEWS	TCP	144	Протокол для групп новостей.
NFS	udp	2049	Сетевая файловая система — NFS, распределенная файловая служба клиент/сервер, обеспечивающая прозрачное совместное использование файлов в сети.
NNTP	TCP	119	Network News Transport Protocol (Сетевой протокол передачи новостей) — система доставки для групп новостей USENET.
PING	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.

Табл. 58 Примеры служб (продолжение)

ИМЯ	ПРОТОКОЛ	ПОРТ(Ы)	ОПИСАНИЕ
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.
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.
SSDP	udp	1900	Simple Service Discovery Protocol supports Universal Plug-and-Play (протокол обнаружения подключенных периферийных устройств на основе Plug & Play).
SSH	TCP/UDP	22	Программа безопасной удаленной регистрации.
STRM WORKS	udp	1558	Протокол передачи потоков Stream Works.
SYSLOG	udp	514	Системный журнал — позволяет отправлять журналы системы серверу UNIX.
TACACS	udp	49	Login Host Protocol (Протокол регистрации узла), используется для Terminal Access Controller Access Control System (Системы управления доступом на основе контроллера доступа к терминалу).

Табл. 58 Примеры служб (продолжение)

ИМЯ	ПРОТОКОЛ	ПОРТ(Ы)	ОПИСАНИЕ
Telnet	TCP	23	Telnet — протокол регистрации и эмуляции терминала, общий для среды Интернет и UNIX. Он работает в сетях TCP/IP. Его главная функция заключается в обеспечении регистрации пользователей на удаленных узлах.
TFTP	udp	69	Trivial File Transfer Protocol (Упрощенный протокол передачи файлов) — это протокол передачи файлов в Интернет, подобный FTP, но использующий UDP (Протокол передачи дейтаграмм пользователя), а не TCP (Протокол управления передачей).
VDOLIVE	TCP udp	7000 User-Defined	Решение для проведения видеоконференций. Номер порта UDP задается в приложении.

Алфавитный указатель

N

P

Q

R

S

T

U

V

W

А

Б

В

Г

Д

Ж

И

К

Л

М

Н

О

П

P

C

T

У

Ф

Ч

Ш