

D-Link DI-804HV

**Широкополосный аппаратный
VPN маршрутизатор**

Руководство пользователя

D-Link

Building Networks for People

Содержание

Комплект поставки.....	3
Введение.....	4
Начало работы	10
Использование меню настройки	11
Основы сетевых технологий.....	68
Сброс DI-804HV к заводским установкам по умолчанию	94
Технические характеристики	95
Часто задаваемые вопросы.....	96
Обращение в службу технической поддержки	142

Комплект поставки



Содержимое комплекта:

- **D-Link DI-804HV**
Широкополосный аппаратный VPN маршрутизатор
- Адаптер питания – 5В постоянного тока
- Руководство пользователя и гарантия на CD
- Руководство по быстрой установке
- Кабель Ethernet (UTP категории 5/прямой)

Примечание: Использование источника питания с характеристиками отличными от характеристик адаптера, прилагаемого к DI-804HV, может привести к выходу из строя устройства и потере гарантии.

Если что-либо из перечисленного отсутствует, обратитесь к вашему поставщику.

Системные требования для настройки устройства:

- DSL или кабельный модем с поддержкой Ethernet
- Компьютер с ОС Windows, Macintosh или Linux и установленным адаптером Ethernet
- Internet Explorer 6.0 или Netscape Navigator 6.0 или выше с поддержкой JavaScript

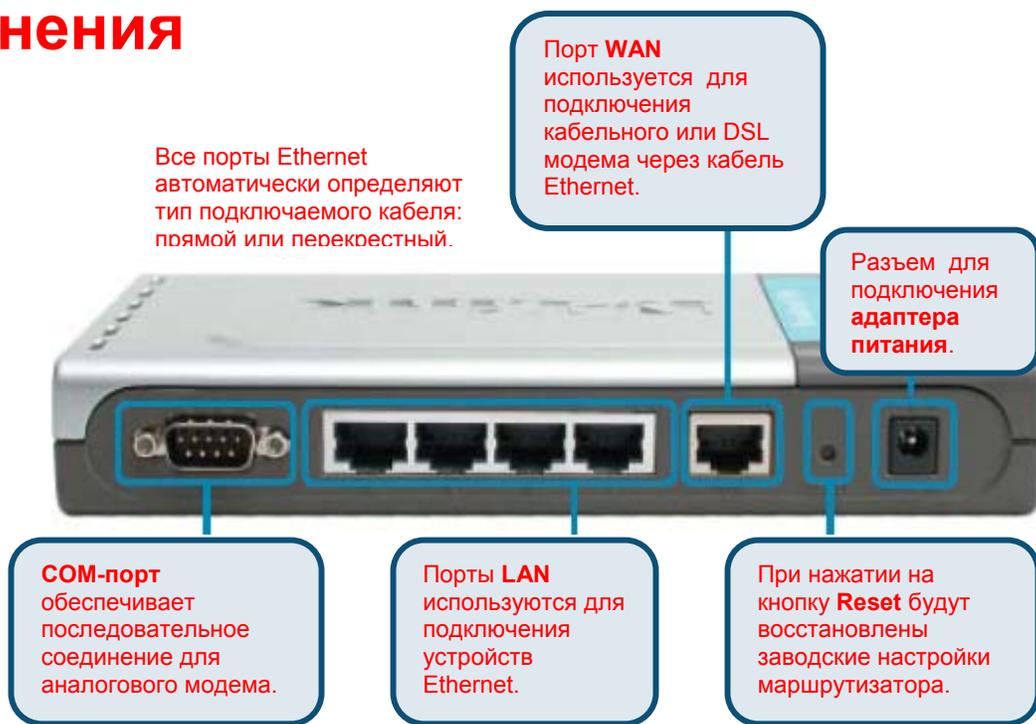
Введение

D-Link DI-804HV – это 4-портовый широкополосный маршрутизатор с функциональностью VPN (Virtual Private Network, виртуальная частная сеть). Он обеспечивает законченное решение для подключения к Интернет, организации совместного доступа к ресурсам офиса и защищенного доступа к удаленным корпоративным сетям. Это идеальный способ расширения сети и увеличения числа подключенных к сети компьютеров.

После выполнения всех шагов, описанных в *Руководстве по быстрой установке* (входит в комплект поставки), Вы сможете обеспечить совместный доступ к информации и ресурсам.

DI-804HV совместим с большинством популярных операционных систем, включая Macintosh, Linux и Windows, и может быть интегрирован в крупную сеть.

Соединения



Характеристики

- **Широкополосный модем и совместное использование одного IP-адреса.** Подключает множество компьютеров к широкополосному (кабельному или DSL) модему для организации доступа в Интернет.
- **Коммутатор Ethernet с автоматическим определением типа кабеля.** Оснащен 4-портовым коммутатором Ethernet с автоматическим определением типа подключаемого кабеля.
- **Аппаратное терминальное устройство VPN.** Поддерживает до 40 туннелей VPN.
- **Поддержка VPN Pass-Through.** Поддерживает сессии VPN pass-through и позволяет настроить VPN-сервер и VPN-клиентов.
- **Межсетевой экран.** Нежелательные пакеты, вторгающиеся в сеть, могут быть заблокированы для защиты сети.
- **Поддержка сервера DHCP.** Все подключенные к сети компьютеры могут получать параметры TCP/IP автоматически от DI-804HV.
- **Web-интерфейс управления.** Возможность настройки с любого подключенного к сети компьютера с помощью web-браузера Netscape или Internet Explorer.
- **Поддержка управления доступом.** Позволяет назначить различным пользователям различные права доступа.
- **Поддержка пакетного фильтра. Пакетный фильтр** позволяет управлять доступом к сети путем анализа входящих и исходящих пакетов, в результате которого пакеты будут пропускаться или блокироваться на основании IP-адреса источника или назначения.
- **Поддержка виртуального сервера.** Позволяет открыть доступ из Интернет к WWW, FTP и другим серверам, находящимся в локальной сети.
- **Определяемый пользователем туннель, распознающий тип приложения.** Можно определить атрибуты, например, открыть специальные порты для входящих пакетов, чтобы обеспечить поддержку специальных приложений, требующих множества одновременных соединений, таких как Интернет-игры, видеоконференции и Интернет-телефония. DI-804HV может распознать тип приложения и открыть для него многопортовый туннель.
- **Поддержка узлов DMZ.** Позволяет подключенному к сети компьютеру быть полностью видимым из Интернет; Эта функция используется, когда функция “Определяемый пользователем туннель, распознающий тип приложения” не может позволить приложения работать правильно.

Введение в технологию широкополосной маршрутизации

Маршрутизатор – это устройство, которое продвигает пакеты от источника до точки назначения. Маршрутизаторы передают пакеты, используя IP-адреса, а не MAC-адреса. Маршрутизатор будет передавать данные из Интернет к определенному компьютеру в локальной сети.

Информация, находящаяся в Интернет, распространяется по Интернет при помощи маршрутизаторов. Когда Вы нажимаете на ссылку на web-странице, Вы отправляете серверу запрос на показ следующей страницы. Принимаемая и отправляемая компьютером информация передается на сервер с помощью маршрутизатора. Маршрутизатор также определяет наилучший маршрут, по которому информация должна следовать, чтобы гарантировать правильность ее доставки.

Маршрутизатор управляет всем потоком данных, проходящим через сеть, удаляя информацию, которая не должна здесь находиться. Это обеспечивает защиту компьютеров, подключенных к маршрутизатору, поскольку находящиеся вне сети компьютеры не могут получить доступ или отправить информацию компьютеру, находящемуся в локальной сети. Маршрутизатор определяет, какому компьютеру должна быть передана информация, и передает ее. Если информация не предназначена какому-либо компьютеру в локальной сети, данные отбрасываются. Это предотвращает передачу нежелательной или вредоносной информации в сеть.

Введение в технологию межсетевых экранов

Межсетевой экран - это устройство, располагающееся между компьютером и Интернет, которое предотвращает неавторизованный доступ в сеть или из сети. Межсетевой экран может быть обычным компьютером, на котором установлен программный межсетевой экран, или специализированное устройство, разработанное специально для работы в качестве межсетевого экрана. В большинстве случаев, межсетевой экран используется для предотвращения неавторизованного доступа пользователей Интернет к частной сети или корпоративной сети и Интранет.

Межсетевой экран просматривает всю информацию, передаваемую в сеть и из сети, и анализирует каждый фрагмент данных. Каждый фрагмент данных проверяется на соответствие набору критериев, установленных администратором. Если данные не удовлетворяют условиям, они блокируются и отбрасываются. Иначе данные передаются далее. Этот метод носит название пакетного фильтра.

Межсетевой экран также выполняет специфические функции обеспечения безопасности на основании типа приложения или используемого порта. Например, межсетевой экран может быть настроен на работу с сервером FTP или Telnet. Или он может быть настроен на работу с определенными портами UDP или TCP, позволяя конкретным приложениям или играм правильно работать через Интернет.

Введение в технологию локальных сетей

Локальная сеть (Local Area Networking, LAN) – это термин, используемый для обозначения нескольких соединенных между собой компьютеров на небольшой территории, такой как здание или группа зданий. Локальные сети могут быть объединены на большой территории. Группа локальных сетей, объединенных на большой территории, называется глобальной сетью (Wide Area Network, WAN).

LAN состоит из множества объединенных друг с другом компьютеров. Существует множество сред передачи, с помощью которых можно соединить компьютеры вместе. Самый популярный способ соединения – кабель категории 5 (витая пара UTP или STP). Каждый компьютер должен иметь сетевой адаптер (Network Interface Card, NIC), который передает данные между компьютерами. NIC – это обычно сетевая карта 10Мбит/с или 10/100Мбит/с или беспроводной сетевой адаптер. Беспроводные локальные сети (Wireless Local Area Networks, WLAN) не используют проводов; вместо этого они передают данные с помощью радиосигнала.

Большинство сетей используют аппаратные устройства, такие как концентраторы или коммутаторы, к которым с помощью кабелей подключаются взаимодействующие компьютеры. Концентратор просто принимает данные, поступившие на порт, и передает их на все остальные порты. Коммутатор более совершенен, он может определить порт назначения для определенного фрагмента данных. Коммутатор минимизирует сетевой трафик и ускоряет взаимодействие по сети.

Планирование и правильная реализация сети занимает определенное время. Существует много способов настроить сеть. Вы можете уделить некоторое время на определение наиболее подходящей инфраструктуры сети.

Введение в технологию виртуальных частных сетей

Виртуальные частные сети (Virtual Private Networking, VPN) используют общедоступную проводную сеть (Интернет) для организации защищенного соединения между двумя различными сетями так, будто они составляют одну сеть. Например, работник может получить доступ к корпоративной сети из дома, используя VPN, что позволит ему получить доступ к файлам, базам данных и другим сетевым ресурсам. Вот несколько различных реализаций VPN, которые могут быть использованы.

Протокол туннелирования «точка-точка» (PPTP)

Протокол туннелирования PPTP (Point-to-Point Tunneling Protocol) использует запатентованные методы соединения двух частных сетей через Интернет. PPTP защищает информацию, шифруя данные внутри пакета.

Протокол IP Security (IPSec)

IPSec обеспечивает более защищенное соединение сеть-сеть через Интернет или глобальную сеть (WAN). IPSec шифрует все взаимодействие между клиентом и сервером, в то время как PPTP шифрует только пакеты данных.

Обе этих реализации VPN используются, поскольку не существует стандарта на серверное ПО VPN. По этой причине каждый провайдер услуг Интернет или компания может реализовать собственную сеть VPN, сохраняя способность к взаимодействию.

Светодиодные индикаторы

DI-804HV имеет следующие индикаторы, которые описаны ниже:

Индикатор	Описание
Power	Постоянно горит при правильном подключении источника питания.
M1	Мигает один раз в секунду, указывая на активность системы.
M2	Загорается, когда устройство установило соединение с Интернет.
WAN	Постоянно горит при подключении к порту WAN. Мигает при передаче данных.
COM	Постоянно горит при подключении к внешнего аналогового коммутируемого модема.
LAN (порты 1-4)	Постоянно горит при подключении к порту 1-4 компьютера с адаптером Ethernet. Мигает при передаче данных.

Начало работы



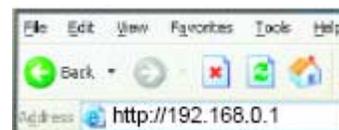
Для типичной установки беспроводной сети дома или в офисе (как показано выше), пожалуйста, выполните следующее:

1. Вам понадобится широкополосное подключение к Интернет (кабельная или DSL абонентская линия дома или в офисе).
2. Проконсультируйтесь у своего провайдера кабельных или DSL услуг, чтобы правильно установить модем.
3. Подключите кабельный или DSL модем к DI-804HV. (См. печатное Руководство по быстрой установке, прилагаемое к DI-804HV)
4. Если Вы подключаете к сети настольный компьютер и требуется соединение Ethernet, можно установить адаптер D-Link DFE-530TX+ в свободный слот PCI настольного компьютера. (См. печатное Руководство по быстрой установке, прилагаемое к сетевому адаптеру)
5. Если Вы подключаете к сети портативный компьютер, установите адаптер Ethernet для шины CardBus (например, D-Link DFE-690TXD) в портативный компьютер. (См. печатное Руководство по быстрой установке, прилагаемое к сетевому адаптеру)
6. Кроме того, можно подключить аналоговый модем к DI-804HV для создания резервного канала связи. Для этого необходимо коммутируемое подключение к Интернет.

Использование меню настройки

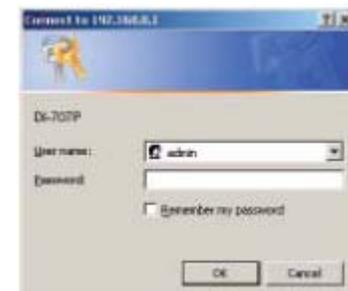
Всякий раз, когда Вы хотите произвести настройку сети или DI-804HV, Вы можете получить доступ к меню настройки, открыв Web-браузер и введя IP-адрес DI-804HV. IP-адрес DI-804HV установленный по умолчанию, показан на рисунке:

- Откройте web-браузер
- Введите **IP-адрес** DI-804HV (http://192.168.0.1)

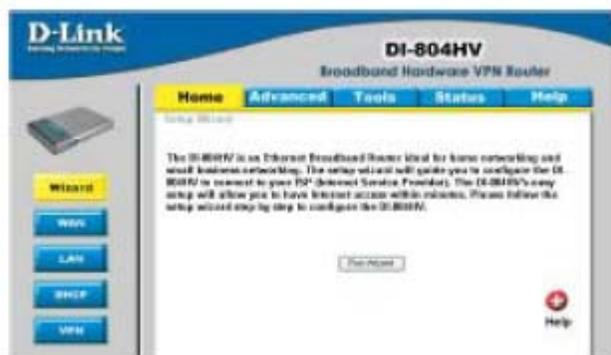


Примечание: Если Вы изменили IP-адрес, назначенный DI-804HV по умолчанию, убедитесь, что был введен правильный IP-адрес.

По умолчанию имя пользователя (**User name**) - **admin**, а пароль (**Password**) не задан. Рекомендуется изменить пароль администратора в целях безопасности. Пожалуйста, перейдите на вкладку **Tools>Admin** для смены пароля.



Home > Wizard



Появится окно **Home>Wizard**. Пожалуйста, обращайтесь к *Руководству по быстрой установке* за дополнительной информацией относительно Мастера настройки (Setup Wizard).



Apply

При нажатии **Apply** произведенные на странице изменения будут сохранены



Cancel

При нажатии **Cancel** произведенные на странице изменения будут стерты



Restart

При нажатии **Restart** маршрутизатор будет перезагружен. (Требуется для изменения некоторых параметров.)



Help

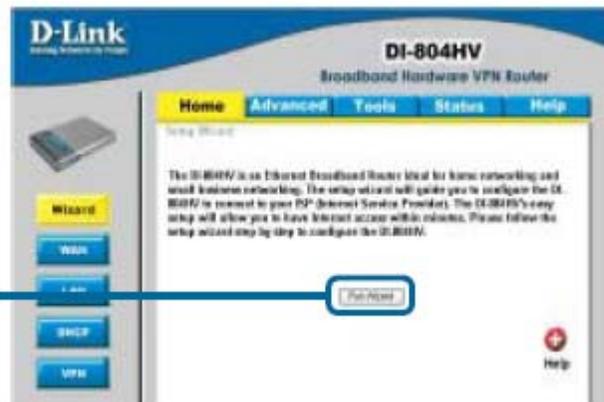
При нажатии **Help** появится помощь по данной странице.

Использование меню настройки (продолжение)

Мастер установки

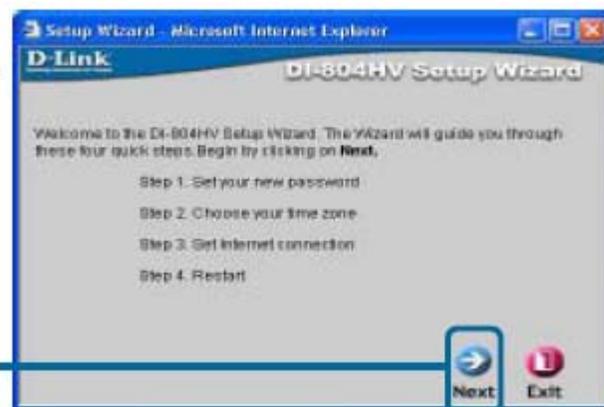
После регистрации появится окно **Home**.

Нажмите **Run Wizard**



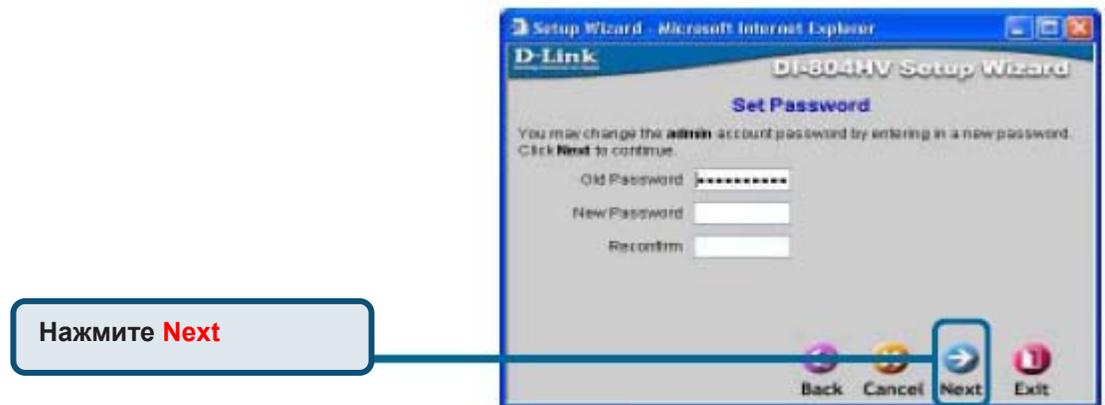
Здесь описаны шаги, которые необходимо выполнить для завершения установки. Нажмите **Next** для продолжения.

Нажмите **Next**



Использование меню настройки (продолжение)

Setup Wizard > Set Password



Old Password- Введите старый пароль.

New Password- Введите новый пароль для учетной записи **admin**.

Reconfirm- Повторите ввод пароля для его подтверждения. Нажмите **Next** для продолжения мастера установки.

Использование меню настройки (продолжение)

Setup Wizard > Time Zone

Выберите подходящий часовой пояс

Выберите часовой пояс из выпадающего меню. Нажмите **Next** для продолжения.

Нажмите **Next**

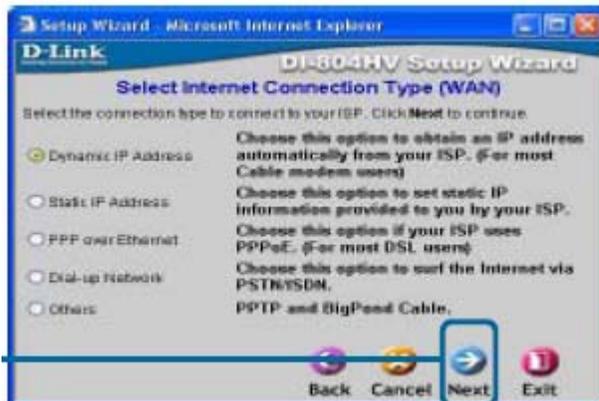


Setup Wizard > Connection Type (WAN)

Выберите тип подключения к Интернет

Появится запрос на выбор типа подключения к Интернет маршрутизатора. Выберите подходящий тип и затем нажмите **Next** для продолжения.

Нажмите **Next**



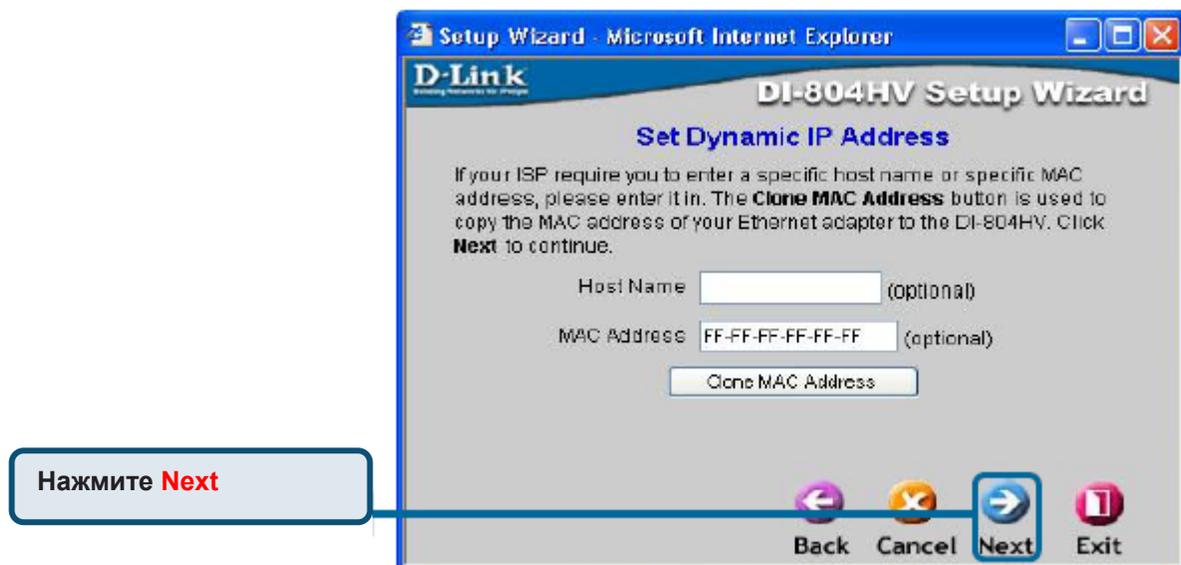
Если не уверены, что выбрать, пожалуйста, обратитесь к своему провайдеру услуг Интернет.



Выберите **Others**, только если используете PPTP в Европе или Big Pond в Австралии.

Использование меню настройки (продолжение)

Setup Wizard > Set Dynamic IP Address

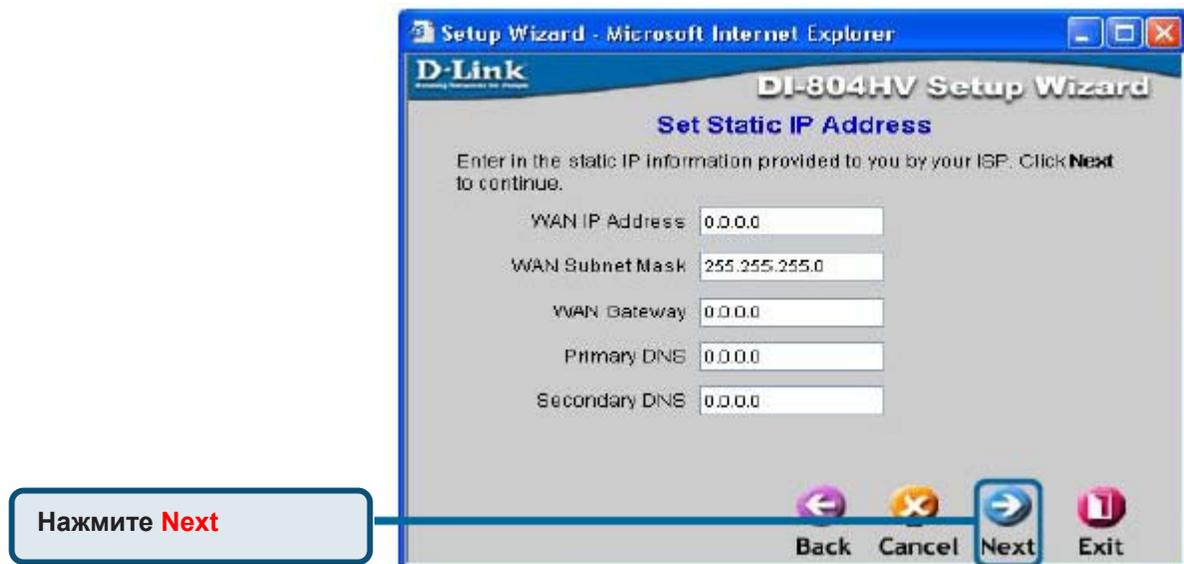


Если Ваш ISP использует подключение с динамическим IP-адресом (**Dynamic IP Address**), появится это окно (используется в основном для кабельного подключения):

- Host Name-** В поле Host Name можно ввести имя Вашего ISP. Это опция дополнительная и не требует ввода.
- MAC Address-** Каждый сетевой адаптер имеет собственный MAC-адрес (Media Access Control, управление доступом к среде передачи). Обратите внимание, что некоторые компьютеры и периферийные устройства имеют встроенные сетевые адаптеры.
- Clone MAC Address-** При нажатии на кнопку Clone MAC Address DI-804HV автоматически скопирует MAC-адрес сетевого адаптера компьютера. Также можно вручную ввести MAC-адрес. Нажмите **Next** для продолжения.

Использование меню настройки (продолжение)

Setup Wizard > Set Static IP Address

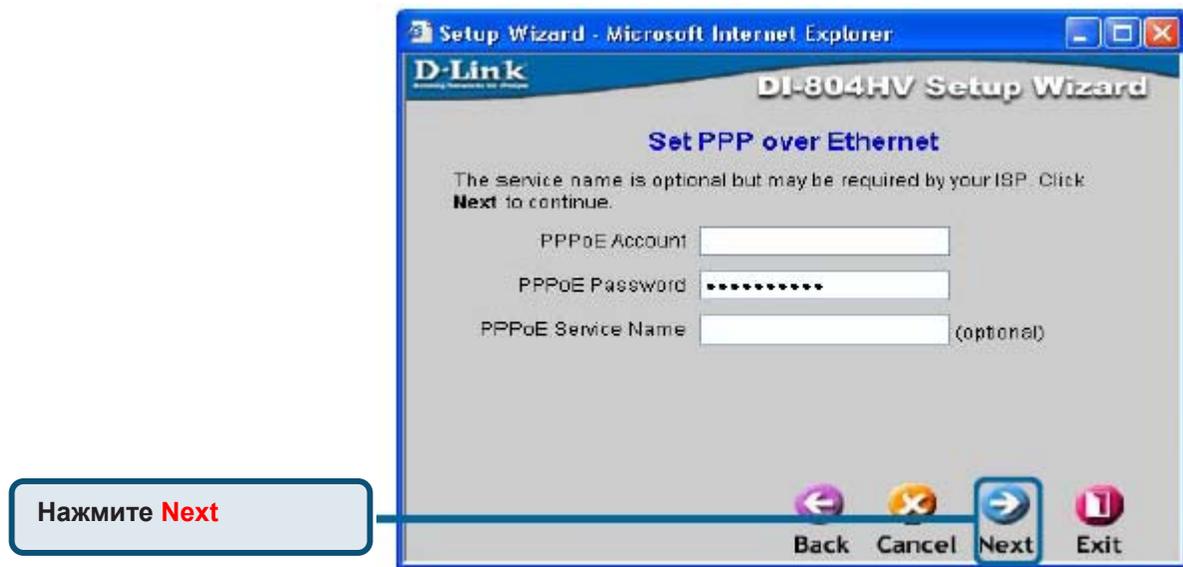


Если Ваш ISP использует подключение со статическим IP-адресом (**Static IP Address**), появится это окно.

- WAN IP Address-** Если Ваш ISP требует назначение статического IP-адреса, и выбрана эта опция, появится данное окно. Введите параметры IP, предоставленные ISP. Необходимо заполнить все требуемые поля.
- WAN Subnet Mask-** По умолчанию маска подсети для DI-804HV равна 255.255.255.0. Ее можно изменить, но это не рекомендуется. Опцию предназначена для опытных пользователей.
- WAN Gateway-** Адрес шлюза предоставляется ISP.
- Primary DNS-** Адрес основного сервера DNS предоставляется ISP.
- Secondary DNS-** Адрес дополнительного сервера DNS предоставляется ISP.

Использование меню настройки (продолжение)

Setup Wizard > PPPoE



Если Ваш ISP использует **PPPoE** (Point-to-Point Protocol over Ethernet), и выбрана эта опция, появится данное окно (используется в основном для DSL-подключения к Интернет.)

PPPoE Account- Введите имя пользователя, предоставленное Вам ISP.

PPPoE Password- Введите пароль, предоставленный Вам ISP.

PPPoE Service Name- Введите имя Вашего провайдера услуг Интернет. Это дополнительная опция и не требует ввода.

Использование меню настройки (продолжение)

Setup Wizard

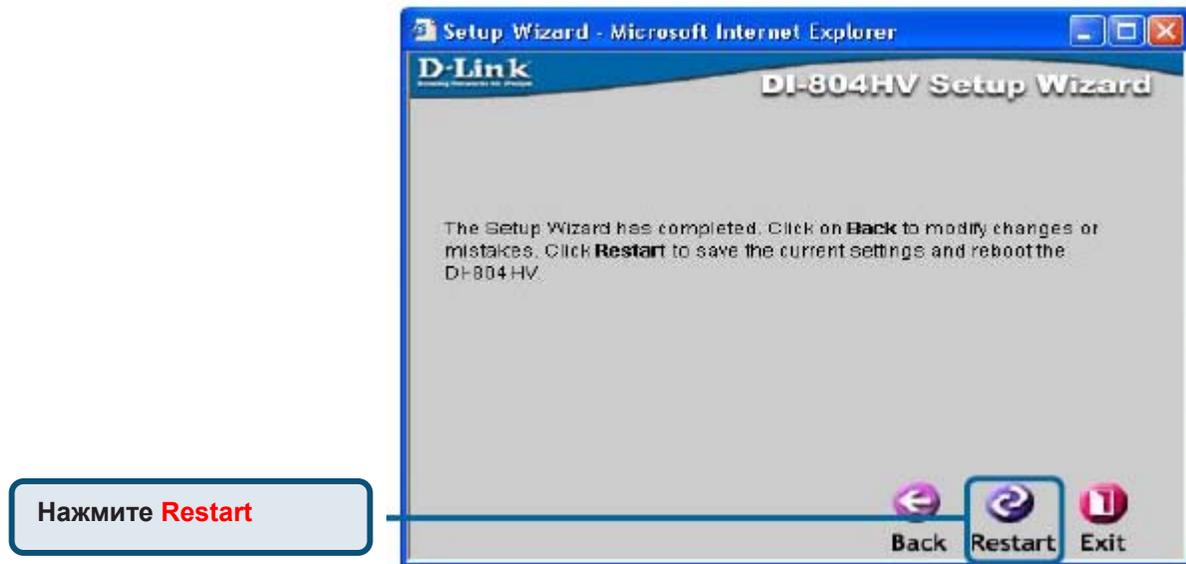


В этом окне необходимо настроить параметры, только если у Вас есть коммутируемое подключение к Интернет. В противном случае нажмите **Next**, чтобы пропустить этот шаг.

- Dial-up Telephone-** Номер телефона для соединения с ISP.
- Dial-up Account-** Введите имя пользователя, предоставленное Вам ISP.
- Dial-up Password-** Введите используемый при регистрации пароль.
- Primary DNS-** Адрес основного сервера DNS предоставляется ISP.
- Secondary DNS-** Адрес дополнительного сервера DNS предоставляется ISP.

Использование меню настройки (продолжение)

Setup Wizard



Back-

Нажмите кнопку **Back** для перехода на предыдущую страницу.

Restart-

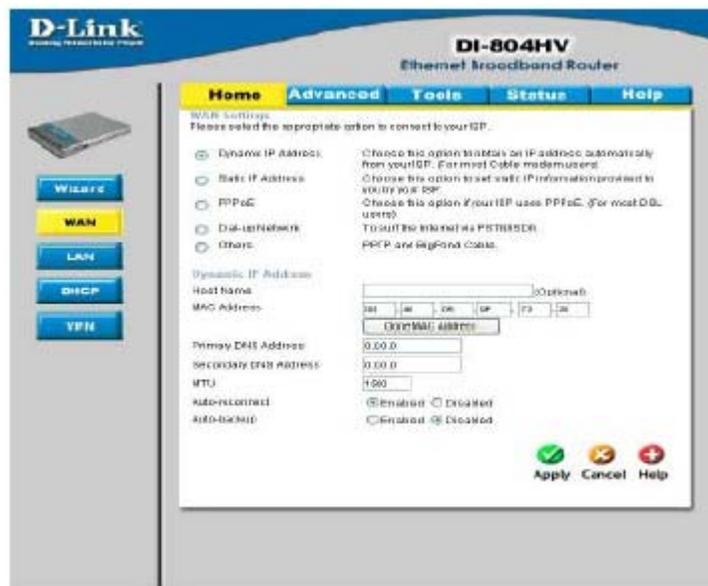
Нажмите кнопку **Restart** для завершения настройки.

Exit-

Нажмите кнопку **Exit** для выхода из мастера установки без сохранения изменений.

Использование меню настройки (продолжение)

Home > WAN



Выберите тип подключения WAN:

WAN расшифровывается как **Wide Area Network (глобальная сеть)**. В данном случае WAN представляет собой режим, в котором Вы подключаетесь к Интернет. Если Вы не знаете, какой тип подключения выбрать, обратитесь к своему ISP за информацией о том, какой из следующих режимов выбрать:

- Dynamic IP Address-** Автоматическое получение IP-адреса от ISP (в основном используется для кабельного подключения).
- Static IP Address-** Ваш ISP назначит статический IP-адрес.
- PPPoE-** Некоторые ISP требуют использовать PPPoE для подключения к их сервисам (в основном для DSL-подключения).
- Dial-up Network -** Можно выбрать эту опцию, если подключение к ISP устанавливается с помощью аналогового модема в случае недоступности широкополосного подключения.
- Others-**
 - PPTPBig** Только для использования в Европе.
 - Pond Cable-** Только для использования в Австралии.

Использование меню настройки (продолжение)

Home > WAN > Dynamic IP Address



Большинство пользователей подключения через кабельный модем должны выбрать эту опцию для получения IP-адреса автоматически от ISP.

Host Name-

Опция Host Name (имя узла) является дополнительной, но может требоваться некоторыми ISP. Имя узла по умолчанию - это имя устройства и может быть изменено.

MAC Address-

По умолчанию MAC-адрес устанавливается равным MAC-адресу физического интерфейса WAN широкополосного маршрутизатора.

Clone MAC Address-

Можно использовать кнопку "Clone MAC Address" для копирования MAC-адреса адаптера Ethernet и замены MAC-адреса интерфейса WAN маршрутизатора MAC-адресом этого адаптера Ethernet. Не рекомендуется менять MAC-адрес по умолчанию до тех пор, пока этого не потребует ISP.

Primary DNS Address-

Введите адрес основного сервера DNS, предоставленный ISP.

Secondary DNS Address-

Введите адрес дополнительного сервера DNS, предоставленный ISP.

MTU

Введите значение MTU, если этого требует ISP. В противном случае, оставьте значение по умолчанию - 1500.

Auto-reconnect -

Если выбрано, маршрутизатор будет автоматически устанавливать соединение с ISP после перезагрузки или после разрыва соединения.

Auto-backup -

Если выбрана эта опция, маршрутизатор будет подключаться к Интернет через коммутируемое соединение, если широкополосное соединение станет недоступно. Для работы функции резервирования необходимо иметь коммутируемое соединение с ISP.

Использование меню настройки (продолжение)

Home > WAN > Static IP Address



Если Вы используете подключение со статическим IP-адресом, необходимо ввести следующие параметры, предоставленные ISP.

IP Address-

Введите IP-адрес, предоставленный ISP.

Subnet Mask-

Введите маску подсети, предоставленную ISP.

ISP Gateway Address-

Введите адрес шлюза, предоставленный ISP.

Primary DNS Address-

Введите IP-адрес основного сервера DNS, предоставленный ISP.

Secondary DNS Address-

IP-адрес дополнительного сервера DNS, предоставленный ISP (дополнительно).

MTU

Введите значение MTU, если этого требует ISP. В противном случае, оставьте значение по умолчанию - 1500.

Использование меню настройки (продолжение)

Home > WAN > PPPoE

The screenshot shows the configuration interface for a D-Link DI-804HV Ethernet Broadband Router. The 'WAN' tab is selected, and the 'PPPoE' option is chosen. The 'Dynamic PPPoE' radio button is selected. The 'User Name' field is empty, and the 'Password' and 'Retype Password' fields contain asterisks. The 'Service Name' field is empty with '(Optional)' next to it. The 'IP Address' field is empty. The 'Primary DNS Address' and 'Secondary DNS Address' fields are empty. The 'Maximum Idle Time' is set to 0 minutes. The 'MTU' is set to 1492. The 'Auto-reconnect' and 'Auto-dialup' checkboxes are both checked.

Большинство пользователей сервисов DSL выберут эту опцию для получения IP-адреса автоматически от ISP по протоколу PPPoE.

User Name- Имя пользователя для подключения PPPoE, предоставленное ISP.

Password- Пароль для подключения PPPoE, предоставленный ISP.

Retype Password- Повторите ввод пароля PPPoE.

Service Name- Обратитесь к ISP за информацией о том, требуется ли вводить имя сервиса (дополнительно).

IP Address- Введите IP-адрес, если Вы используете подключение PPPoE со статическим IP-адресом (дополнительно).

Primary DNS Address- Вы будете получать IP-адрес сервера DNS автоматически от ISP, но можно ввести IP-адрес другого сервера DNS, если хотите использовать его вместо получаемого автоматически.

Secondary DNS Address- IP-адрес дополнительного сервера DNS (дополнительно).

Maximum Idle Time- Введите максимальный интервал времени, в течение которого соединение с Интернет будет поддерживаться, даже если не было активности. Для отключения этой функции выберите *Autoreconnect*.

MTU MTU (Maximum Transmission Unit, максимальный размер передаваемого пакета) по умолчанию равен 1492. Вы можете изменить MTU для достижения оптимальной производительности с определенным ISP.

Использование меню настройки (продолжение)

Home > WAN > Dial-up Network

The screenshot shows the WAN configuration page for a D-Link DI-804HV router. The 'Dial-up Network' option is selected under the 'WAN Settings' section. The page includes the following fields and options:

- Dial-up Telephone:** A text input field.
- DSN# (ACCOUNT):** A text input field.
- Dial-up Password:** A text input field with a password mask.
- Primary DNS:** A text input field with the value "0.0.0.0".
- Secondary DNS:** A text input field with the value "0.0.0.0".
- Assigned IP Address:** A text input field with the value "0.0.0.0" and a "(Optional)" label.
- Extra Settings:** A dropdown menu set to "None".
- Maximum Idle Time:** A text input field with the value "0" and a "Minutes" label.
- Baud Rate:** A dropdown menu set to "115200" and a "bps" label.
- Disable auto-dial autoreconnect:** A checkbox that is checked.

At the bottom right, there are three buttons: "Apply", "Cancel", and "Help".

Большинство пользователей коммутируемого подключения выберут эту опцию для соединения с ISP через аналоговый модем. Такое подключение можно использовать в качестве резервного в случае недоступности широкополосного подключения.

- Dial-up Telephone -** Номер телефона для соединения с ISP.
- Dial-up Account-** Введите имя пользователя, предоставленное Вам ISP.
- Dial-up Password-** Введите используемый при регистрации пароль.
- Primary DNS** Если введено значение "0.0.0.0," адреса серверов DNS будут получены автоматически при установлении соединения.
- Seconday DNS**
- Assigned IP Address-** Введите IP-адрес, если был назначен статический IP-адрес.
- Extra Settings-** Дополнительные параметры используются для оптимизации качества соединения между ISP и аналоговым модемом (строка инициализации) – дополнительно.
- Maximum Idle Time-** Введите максимальный интервал времени, в течение которого соединение с Интернет будет поддерживаться, даже если не было активности. Для отключения этой функции выберите *Autoreconnect*.
- Baud Rate-** Скорость соединения между DI-804HV и аналоговым модемом.

Использование меню настройки (продолжение)

Home > WAN > PPTP



Протокол туннелирования точка-точка PPTP (Point-to-Point Tunneling Protocol) используется для подключения WAN в Европе.

My IP Address- Введите IP-адрес.

My Subnet Mask- Введите маску подсети.

Server IP Address- Введите IP-адрес сервера.

PPTP Account- Введите имя учетной записи PPTP.

PPTP Password- Введите используемый при регистрации пароль.

Connection ID- Введите идентификатор соединения, если этого требует ISP.

Maximum Idle Time- Введите максимальный интервал времени, в течение которого соединение с Интернет будет поддерживаться, даже если не было активности. Для отключения этой функции выберите *Autoreconnect*.

Использование меню настройки (продолжение)

Home > WAN > BigPond Cable



Подключение WAN BigPond с динамическим IP-адресом используется в Австралии.

User Name- Введите имя учетной записи BigPond.

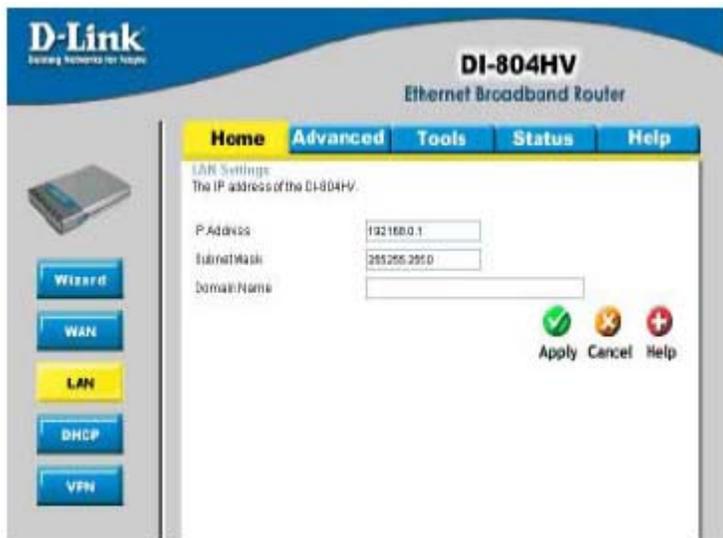
Password- Введите используемый при регистрации пароль.

Login Server IP- Введите имя сервера регистрации, если требуется (дополнительно).

Renew IP forever- Если выбрана эта опция, маршрутизатор будет автоматически устанавливать соединение с ISP после перезагрузки или при разрыве соединения.

Использование меню настройки (продолжение)

Home > LAN



LAN (Local Area Network, Локальная сеть) – это Ваша внутренняя сеть. Здесь настраиваются параметры IP интерфейса LAN DI-804HV. Их можно назвать частными параметрами. Если требуется, можно изменить IP-адрес интерфейса LAN. IP-адрес интерфейса LAN является частным во внутренней сети и не виден в Интернет.

LAN IP Address- IP-адрес интерфейса LAN. По умолчанию равен 192.168.10.1.

Subnet Mask- Маска подсети интерфейса LAN. По умолчанию равна 255.255.255.0.

Local Domain- Введите имя локального домена (дополнительно).

Использование меню настройки (продолжение)

Home >DHCP



DHCP расшифровывается как *Dynamic Host Control Protocol* – протокол динамического конфигурирования узла. DI-804HV имеет встроенный сервер DHCP. Сервер DHCP будет автоматически назначать IP-адреса компьютерам локальной/частной сети. Не забудьте настроить компьютеры на работу в качестве клиентов DHCP, используя параметр TCP/IP "Получить IP-адрес автоматически". После включения все компьютеры автоматически загрузят правильные параметры TCP/IP, полученные от DI-804HV. Сервер DHCP автоматически выделит неиспользуемый IP-адрес запрашивающему компьютеру из пула свободных адресов. Вы можете указать начальный и конечный адрес пула IP-адресов.

DHCP Server- Включите (**Enabled**) или отключите (**Disabled**) сервер DHCP. По умолчанию - **Enabled**.

Starting IP Address- Начальный IP-адрес диапазона адресов, выделяемых сервером DHCP.

Ending IP Address- Конечный IP-адрес диапазона адресов, выделяемых сервером DHCP.

Lease Time- Период аренды IP-адреса. Введите время, на которое IP-адрес будет выделяться.

DHCP Clients List- Список клиентов DHCP, подключенных к DI-804HV. Нажмите **Refresh** для обновления списка. В таблице показаны имя узла (Host Name), IP-адрес (IP Address) и MAC-адрес (MAC Address) клиента DHCP.

Использование меню настройки (продолжение)

Home >VPN Settings



Параметры VPN (VPN Settings) – это параметры, используемые для создания виртуальных частных туннелей к удаленным шлюзам VPN. Технология туннелирования обеспечивает конфиденциальность данных, целостность данных и аутентификацию, используя протоколы инкапсуляции, алгоритмы шифрования и алгоритмы хэширования.

VPN Выберите эту опцию, чтобы включить туннели VPN. Если Вы не используете VPN, то лучше отключить опцию VPN.

NetIOS broadcast- Выберите эту опцию, чтобы разрешить рассылку широковещательных сообщений NetBIOS через VPN-туннель.

Max. number of tunnels- Выберите максимальное количество туннелей.

Tunnel Name- Введите имя создаваемого туннеля.

Method- Протокол VPN IPSec поддерживает два способа установления ключей: ручное назначение и автоматический обмен ключами. Ручное назначение ключей подразумевает, что ввод ключей шифрования и настройка аутентификации будет производиться на обоих концах VPN-туннеля вручную администратором. Однако, можно использовать протокол IKE для автоматического обмена ключами. Администраторы шлюзов на обоих концах туннеля должны будут лишь ввести один и тот же первичный общий ключ (pre-shared key).

More- Для более детальной настройки параметров IKE или вводимого вручную ключа нажмите **More**.

Использование меню настройки (продолжение)

Home >VPN Settings > Tunnel > Method>IKE



- Tunnel Name-** Имя текущего туннеля.
- Aggressive Mode-** Включение этого режима ускорит установление туннеля, но он будет менее защищенным.
- Local Subnet-** Подсеть локальной сети, к которой относится шлюз VPN. Это может быть отдельный узел, часть подсети или вся подсеть.
- Local Netmask-** Локальная маска подсети вместе с локальной подсетью формируют домен подсети.
- Remote Subnet-** Подсеть удаленной локальной сети, к которой относится шлюз VPN. Это может быть отдельный узел, часть подсети или вся подсеть.
- Remote Netmask-** Маска удаленной подсети вместе с удаленной подсетью формируют домен удаленной подсети.
- Remote Gateway-** IP-адрес интерфейса WAN удаленного шлюза VPN.
- Preshared Key-** Первоначальный ключ, на основе которого механизм IKE устанавливает будущие ключи безопасности для шлюзов на обоих концах туннеля VPN. Первичный общий ключ должен совпадать на обоих концах туннеля.
- IKE Proposal index-** Нажмите на эту кнопку для настройки набора часто используемых схем IKE и выберите схему IKE из набора для туннеля.
- IPSec Proposal index-** Нажмите на эту кнопку для настройки набора часто используемых схем IPSec и выберите схему IPSEC из набора для туннеля.

Использование меню настройки (продолжение)

Home > VPN Settings > Tunnel > Method > IKE > Select IKE Proposal



IKE Proposal index-

Список выбранных схем из пула доступных схем IKE, показанных внизу.

Proposal Name-

Имя, используемое для классификации схемы IKE.

DH Group-

Можно выбрать одну из трех групп: group 1 (MODP768), group 2 (MODP1024), group 5 (MODP1536).

Encrypt algorithm-

Можно выбрать один из двух алгоритмов шифрования: 3DES или DES.

Auth algorithm-

Можно выбрать один из двух алгоритмов аутентификации: SHA1 или MD5.

Использование меню настройки (продолжение)

Home > VPN Settings > Tunnel > Method > IKE > Select IKE Proposal (продолжение)



Life Time- Введите время жизни схемы.

Life Time Unit- Единица измерения времени жизни: Sec.(секунды) или KB (Кбайты).

Proposal ID- Можно выбрать идентификатор схемы IKE для добавления соответствующей схемы в выделенный туннель.

Add to- Нажмите для добавления схемы IKE с указанным Proposal ID в список схем IKE (IKE Proposal Index).

Использование меню настройки (продолжение)

Home > VPN Settings > Tunnel > Method > IKE > Select IPSEC Proposal



IPSec Proposal index-

Список выбранных схем из пула доступных схем IPsec, показанных внизу.

Proposal Name-

Имя, используемое для классификации схемы IPsec.

DH Group-

Можно выбрать одну из трех групп: group 1 (MODP768), group 2 (MODP1024), group 5 (MODP1536).

Encap protocol-

Можно выбрать один из двух протоколов инкапсуляции: ESP или AH.

Encrypt algorithm-

Можно выбрать один из двух алгоритмов шифрования: 3DES или DES.

Auth algorithm-

Можно выбрать один из двух алгоритмов аутентификации: SHA1 или MD5.

Использование меню настройки (продолжение)

Home > VPN Settings > Tunnel > Method > IKE > Select IPSEC Proposal (продолжение)



Life Time- Введите время жизни схемы.

Life Time Unit- Единица измерения времени жизни: Sec.(секунды) или KB (Кбайты).

Proposal ID- Можно выбрать идентификатор схемы IPsec для добавления соответствующей схемы в выделенный туннель.

Add to- Нажмите для добавления схемы IPsec с указанным Proposal ID в список схем IPsec (IPsec Proposal Index).

Использование меню настройки (продолжение)

Home >VPN Settings > Tunnel > Manual



- Tunnel Name-** Имя текущего туннеля.
- Aggressive Mode-** Включение этого режима ускорит установление туннеля, но он будет менее защищенным.
- Local Subnet-** Подсеть локальной сети, к которой относится шлюз VPN. Это может быть отдельный узел, часть подсети или вся подсеть.
- Local Netmask-** Локальная маска подсети вместе с локальной подсетью формируют домен подсети.
- Remote Subnet-** Подсеть удаленной локальной сети, к которой относится шлюз VPN. Это может быть отдельный узел, часть подсети или вся подсеть.
- Remote Netmask-** Маска удаленной подсети вместе с удаленной подсетью формируют домен удаленной подсети.
- Remote Gateway-** IP-адрес интерфейса WAN удаленного шлюза VPN.
- Method-** Набор правил, применяемых при подключении к шлюзу VPN.
- Local SPI-** Значение локального индекса SPI должно быть указано в шестнадцатеричном виде.
- Remote SPI-** Значение удаленного индекса SPI должно быть указано в шестнадцатеричном виде.

Использование меню настройки (продолжение)

Home >VPN Settings > Tunnel > Manual (продолжение)



Encapsulation Protocol-

Можно выбрать один из двух протоколов инкапсуляции: ESP или AH.

Encrypt algorithm-

Можно выбрать один из двух алгоритмов шифрования: 3DES или DES.

Encryption Key-

Для DES: ключ шифрования длиной 8 байт (16 шестнадцатеричных символов). Для 3DES: ключ шифрования длиной 24 байт (48 шестнадцатеричных символов).

Authentication Algorithm-

Можно выбрать один из двух алгоритмов аутентификации: SHA1 или MD5.

Authentication Key-

Для MD5: ключ аутентификации длиной 16 байт (32 шестнадцатеричных символов). Для SHA1: ключ аутентификации длиной 20 байт (40 шестнадцатеричных символов).

Life Time-

Введите время жизни схемы.

Life Time Unit-

Единица измерения времени жизни: Sec.(секунды) или KB (Кбайты).

Использование меню настройки (продолжение)

Home >VPN Settings > Dynamic VPN Tunnel



VPN Settings - IKE

Необходимо настроить три вида параметров IKE для выделенного туннеля: основные параметры, параметры схемы IKE и параметры схемы IPSec. Основные параметры включают в себя следующие: локальная подсеть (local subnet), маска локальной подсети (local netmask), удаленная подсеть (remote subnet), маска удаленной подсети (remote netmask), удаленный шлюз (remote gateway) и первичный общий ключ (pre-shared key). Имя туннеля берется с предыдущей страницы настройки параметров VPN. Настройка параметров схемы IKE включает в себя настройку набора часто используемых схем IKE и выбор одной из них.

Tunnel Name-

Имя текущего туннеля.

Dynamic VPN

Эта функция работает с программным клиентом VPN, поэтому DI-804HV не требуется знать IP-адрес удаленного клиента.

Aggressive Mode-

Включение этого режима ускорит установление туннеля, но он будет менее защищенным.

Local Subnet-

Подсеть локальной сети, к которой относится шлюз VPN. Это может быть отдельный узел, часть подсети или вся подсеть.

Local Netmask-

Локальная маска подсети вместе с локальной подсетью формируют домен подсети.

Использование меню настройки (продолжение)

Home >VPN Settings > Dynamic VPN Tunnel (продолжение)



Preshared Key-

Первоначальный ключ, на основе которого механизм IKE устанавливает будущие ключи безопасности для шлюзов на обоих концах туннеля VPN. Первичный общий ключ должен совпадать на обоих концах туннеля.

IKE Proposal index-

Нажмите на эту кнопку для настройки набора часто используемых схем IKE и выберите схему IKE из набора для туннеля.

IPSec Proposal index-

Нажмите на эту кнопку для настройки набора часто используемых схем IPSec и выберите схему IPSec из набора для туннеля.

Использование меню настройки (продолжение)

Home >VPN Settings > Dynamic VPN Tunnel > Set IKE Proposal



IKE Proposal index- Список выбранных схем из пула доступных схем IKE, показанных внизу.

Proposal Name- Имя схемы показывает, какая схема IKE выбрана. Если первый символ имени равен 0x00, схема IKE недоступна.

DH Group- Можно выбрать одну из трех групп: group 1 (MODP768), group 2 (MODP1024), group 5 (MODP1536).

Encrypt algorithm- Можно выбрать один из двух алгоритмов шифрования: 3DES или DES.

Auth algorithm- Можно выбрать один из двух алгоритмов аутентификации: SHA1 или MD5.

Использование меню настройки (продолжение)

Home >VPN Settings > Dynamic VPN Tunnel > Set IKE Proposal (продолжение)



Life Time- Введите время жизни схемы.

Life Time Unit- Единица измерения времени жизни: Sec.(секунды) или KB (Кбайты).

Proposal ID- Можно выбрать идентификатор схемы IKE для добавления соответствующей схемы в выделенный туннель.

Add to- Нажмите для добавления схемы IKE с указанным Proposal ID в список схем IKE (IKE Proposal Index).

Использование меню настройки (продолжение)

Home >VPN Settings > Dynamic VPN Tunnel > Set IPSEC Proposal



IPSec Proposal index- Список выбранных схем из пула доступных схем IPSec, показанных внизу.

Proposal Name- Имя, используемое для классификации схемы IPSec.

DH Group- Можно выбрать одну из трех групп: group 1 (MODP768), group 2 (MODP1024), group 5 (MODP1536).

Encap protocol- Можно выбрать один из двух протоколов инкапсуляции: ESP или AH.

Encrypt algorithm- Можно выбрать один из двух алгоритмов шифрования: 3DES или DES.

Auth algorithm- Можно выбрать один из двух алгоритмов аутентификации: SHA1 или MD5.

Использование меню настройки (продолжение)

Home >VPN Settings > Dynamic VPN Tunnel > Set IPSEC Proposal (продолжение)



Life Time- Введите время жизни схемы.

Life Time Unit- Единица измерения времени жизни: Sec.(секунды) или KB (Кбайты).

Proposal ID- Можно выбрать идентификатор схемы IPsec для добавления соответствующей схемы в выделенный туннель.

Add to- Нажмите для добавления схемы IPsec с указанным Proposal ID в список схем IPsec (IPsec Proposal Index).

Использование меню настройки (продолжение)

Home >VPN Settings > L2TP Server Setting

The screenshot shows the configuration interface for the L2TP Server on a D-Link DI-804HV router. The page is titled "L2TP Server" and has a navigation bar with "Home", "Advanced", "Tools", "Status", and "Help". On the left, there are buttons for "Wireless", "WAN", "LAN", "DHCP", and "VPN". The main content area is divided into two sections: "Basic" and "Tunnel Setting".

Item	Setting
L2TP Server	<input type="checkbox"/> Enable
Virtual IP of L2TP Server	10 . 1 . 1 . 1
Authentication Protocol	<input checked="" type="radio"/> PAP <input type="radio"/> CHAP <input type="radio"/> MSCHAP

Tunnel Setting

Tunnel Name	<input type="text"/>
User Name	<input type="text"/>
Password	<input type="text"/>

Buttons: Back, Apply, Cancel, Help

Tunnel Name	User Name	Password
-------------	-----------	----------

Enable L2TP Server-

Выберите Enabled для включения сервера L2TP.

Virtual IP of L2TP Server-

Введите виртуальный IP-адрес, используемый для доступа к серверу L2TP.

Authentication Protocol-

Выберите один из протоколов аутентификации: PAP, CHAP, MSCHAP.

Tunnel Name-

Имя туннеля.

User Name-

Введите имя пользователя учетной записи L2TP.

Password-

Введите пароль учетной записи L2TP.

Использование меню настройки (продолжение)

Home >VPN Settings >PPTP Server Setting

The screenshot shows the configuration page for the PPTP Server on a D-Link DI-804HV Ethernet Broadband Router. The page is titled "PPTP Server" and has a navigation bar with "Home", "Advanced", "Tools", "Status", and "Help". On the left side, there are buttons for "WLAN", "WAN", "LAN", "DHCP", and "VPN". The main content area is divided into two sections: "Basic" and "Tunnel Setting".

Basic

Item	Setting
PPTP Server	<input type="checkbox"/> Enable
Virtual IP of PPTP Server	10 . 0 . 0 . 1
Authentication Protocol	<input checked="" type="radio"/> PAP <input type="radio"/> CHAP <input type="radio"/> MSCHAP

Tunnel Setting

Tunnel Name	<input type="text"/>
User Name	<input type="text"/>
Password	<input type="text"/>

At the bottom right of the "Tunnel Setting" section, there are four buttons: "Back", "Apply", "Cancel", and "Help". Below the form, there is a table with columns for "Tunnel Name", "User Name", and "Password".

Enable PPTP Server-

Выберите Enabled для включения сервера PPTP.

Virtual IP of PPTP Server-

Введите виртуальный IP-адрес, используемый для доступа к серверу PPTP.

Authentication Protocol-

Выберите один из протоколов аутентификации: PAP, CHAP, MSCHAP.

Tunnel Name-

Имя туннеля.

User Name-

Введите имя пользователя учетной записи PPTP.

Password-

Введите пароль учетной записи PPTP.

Использование меню настройки (продолжение)

Advanced > Application



Некоторые приложения требуют множество одновременных соединений, например, Интернет-игры, видеоконференции, Интернет-телефония и другие. Эти приложения имеют трудности при работе через NAT (Network Address Translation, Трансляция сетевых адресов). Функция **Special Applications** (специальные приложения) делает возможным работу таких приложений с DI-804HV. Если необходимо запустить приложение, требующее множество соединений, укажите порт, обычно назначенный данному приложению в поле **Trigger Port**, выберите тип протокола TCP или UDP, а затем введите публичные порты в поле **Public Ports**, связанные с фиксированным портом (trigger port), чтобы разрешить входящий трафик на эти порты.

DI-804HV имеет предустановленные параметры для некоторых приложений. Они показаны в таблице в нижней части web-страницы. Выберите приложение из выпадающего списка и выберите идентификатор ID, который хотите использовать. Затем нажмите кнопку "Copy to", и поля будут заполнены соответствующей информацией. Затем необходимо включить сервис. Если механизм специальных приложений также не позволяет приложению работать, попробуйте использовать узел DMZ.

Примечание! Только один ПК может использовать каждый туннель для специального приложения.

Enabled- Выберите **Enabled** для активизации созданного правила.

Trigger Port- Порт, используемый для фиксации приложения. Это может быть одиночный порт или диапазон портов.

Public Ports- Номер порта на стороне WAN, который будет использоваться для доступа к приложению. Можно указать одиночный порт или диапазон портов. Можно использовать запятую для указания нескольких портов или диапазонов портов.

Использование меню настройки (продолжение)

Advanced > IP Filter



Фильтры используются для разрешения или запрещения компьютерам локальной сети доступа в Интернет. DI-804HV можно настроить на запрещение внутренним компьютерам доступа по их IP-адресам.

IP Filter-

Используйте IP-фильтры для запрещения доступа в Интернет компьютерам локальной сети по IP-адресам. Можно закрыть определенные номера портов или все порты для указанного IP-адреса.

Enabled or Disabled-

Выберите **Enabled** для активизации созданного правила фильтрации или **Disabled** для создания неактивного правила фильтрации (правило можно включить позднее).

IP Address-

Введите диапазон IP-адресов компьютеров, к которым будет применяться данное правило. Если необходимо указать только один компьютер, введите IP-адрес компьютера в поле Start Source IP, а поле End Source IP оставьте пустым.

Port Range-

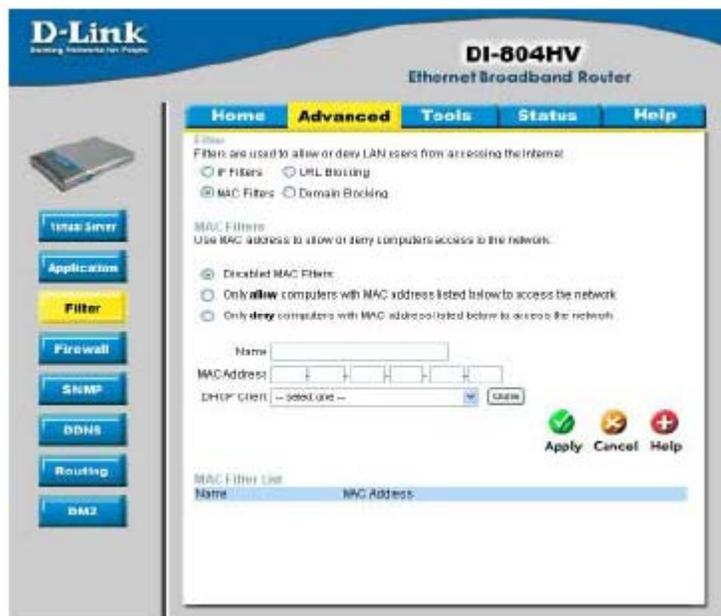
Введите диапазон портов TCP/UDP, к которым будет применяться данное правило. Если необходимо указать только один порт, введите номер порта в поле Start Port, а поле End Port оставьте пустым. Если нужно указать все порты, можно оставить оба поля пустыми.

Schedule:

Расписание применения IP-фильтра (когда фильтр будет работать): выберите **Always (всегда)** или **Time (время)**, чтобы выбрать нужный временной интервал.

Использование меню настройки (продолжение)

Advanced > MAC Filters



Используйте MAC-фильтры (Media Access Control, управление доступом к среде передачи) для запрещения компьютерам локальной сети доступа в Интернет по их MAC-адресам.

В нижней части страницы показан список MAC-адресов клиентов DHCP, подключенных в данный момент к DI-804HV. Можно выбрать MAC-адрес из выпадающего списка. После нажатия кнопки “Apply” DI-804HV автоматически заполнит нужные поля.

Disabled MAC Filter-

Выберите эту опцию, если не хотите использовать фильтры по MAC-адресам.

Only allow computers with MAC address listed below to access the network-

Выберите эту опцию, чтобы разрешить доступ к сети и к Интернет только тем компьютерам, MAC-адреса которых внесены в список. Всем остальным компьютерам доступ к сети и к Интернет будет запрещен.

Only deny computers with MAC address listed below to access the network-

Выберите эту опцию, чтобы запретить доступ к сети и к Интернет только тем компьютерам, MAC-адреса которых внесены в список. Всем остальным компьютерам доступ к сети и к Интернет будет разрешен..

MAC Address-

Введите MAC-адрес для фильтрации.

Использование меню настройки (продолжение)

Advanced > URL Blocking



Блокирование URL используется для запрещения доступа компьютерам локальной сети к определенным web-сайтам по URL. URL – это текстовая строка специального формата, определяющая размещение ресурса в Интернет. Если какая-либо часть URL содержит блокируемое слово, сайт не будет доступен, и web-страница не будет отображаться.

Disabled URL Blocking- Выберите эту опцию, если не хотите использовать функцию блокирования URL.

Использование меню настройки (продолжение)

Advanced > Domain Blocking



Блокирование доменов (Domain Blocking) используется для разрешения или запрещения доступа компьютерам LAN к указанным доменам Интернет. Блокирование доменов будет блокировать все запросы к указанному домену, например, http и ftp. Можно разрешить доступ компьютерам к определенным сайтам и запретить доступ ко всем другим сайтам.

Disabled Domain Blocking-

Выберите эту опцию, если не хотите использовать функцию блокирования доменов.

Allow users to access all domains except "Blocked Domains"-

Выберите эту опцию, чтобы разрешить доступ ко всем доменам, кроме заблокированных (**Blocked Domains**).

Deny users to access all domains except "Permitted Domains"-

Выберите эту опцию, чтобы запретить доступ ко всем доменам, кроме разрешенных (**Permitted Domains**).

Использование меню настройки (продолжение)

Advanced > Firewall



Правила межсетевого экрана (Firewall Rules) – это особая функция, используемая для запрещения или разрешения трафика, проходящего через DI-804HV. Она работает подобно IP-фильтрам с некоторыми дополнительными настройками. Межсетевой экран позволяет установить более детализированные правила доступа на DI-804HV.

Enabled or Disabled-

Выберите **Enabled** для активизации созданного правила или **Disabled** для создания неактивного правила (правило можно включить позднее).

Name-

Введите имя правила.

Action-

Выберите действие: **Allow (разрешить)** или **Deny (запретить)** трафик через DI-804HV.

Source-

Выберите источник: LAN (локальная сеть) или WAN (интерфейс WAN). Звездочка означает выбор обоих источников.

IP Start-

Начальный IP-адрес для применяемого правила. Оставьте это поле пустым для указания всех IP-адресов.

IP End-

Конечный IP-адрес для применяемого правила. Оставьте это поле пустым для указания всех IP-адресов.

Destination-

Выберите сеть назначения: LAN (локальная сеть) или WAN (интерфейс WAN). Звездочка означает выбор обоих источников.

Использование меню настройки (продолжение)

Advanced > Firewall (продолжение)

D-Link
Ethernet Broadband Router

DI-804HV

Home **Advanced** Tools Status Help

Firewall Rules
Firewall Rules can be used to allow or deny traffic from passing through the DI-804HV.

Enabled Disabled

Name:

Action: Allow Deny

Interface: IP Start: IP End: Protocol: Port Range:

Source: Destination: TCP

Schedule: Always From

Time: To:
day: to:

Apply Cancel Help

ActionName	Source	Destination	Protocol
<input type="checkbox"/> Allow Allow to Ping WAN port	WAN	LAN 192.168.0.1	ICMP
<input type="checkbox"/> Deny Default	**	LAN 192.168.0.1	**
<input type="checkbox"/> Allow Default	LAN	*.192.168.0.1	**

IP Address-

Введите диапазон IP-адресов компьютеров, к которым будет применяться данное правило. Если необходимо указать только один компьютер, введите его IP-адрес в поле Start Source IP, а поле End Source IP оставьте пустым.

Protocol-

Выберите один из следующих протоколов: TCP, UDP или ICMP.

Port Range-

Введите диапазон портов TCP/UDP, к которым будет применяться данное правило. Если необходимо указать только один порт, введите его номер в поле Start Port, а поле End Port оставьте пустым. Если необходимо указать все порты, можно оставить оба поля пустыми.

Schedule-

Расписание применения правила: выберите **Always (всегда)** или **From**, чтобы выбрать нужный временной интервал.

Использование меню настройки (продолжение)

Advanced > SNMP



SNMP (Simple Network Management Protocol, Простой протокол сетевого управления) – это широко используемый протокол сетевого мониторинга и управления. Он может предоставлять администратору сети информацию о работе каждого сетевого устройства. SNMP может быть использован для мониторинга трафика и сбора статистических данных о работе DI-804HV. DI-804HV поддерживает SNMP v1 и v2c

Enable SNMP

Активизация управления по протоколу SNMP для:

Local-

локальной сети

Remote-

интерфейса WAN

Get Community-

Введите пароль **public** в это поле для включения доступа «только для чтения» для сетевого управления по SNMP. При этом можно будет только просматривать сетевые параметры, но не изменять их.

Set Community-

Введите пароль **private** в это поле для включения доступа «на чтение и на запись» для сетевого управления по SNMP. При этом администратор сети сможет настраивать параметры устройства.

SNMP v1-

Протокол SNMP – это протокол уровня приложений, который облегчает обмен управляющей информацией между сетевыми устройствами.

SNMP v2-

Расширенная версия протокола SNMP v1 с дополнительными протокольными операциями, такими как UDP, IP, CLNS, DDP и IPX.

Использование меню настройки (продолжение)

Tools > DDNS



DDNS (Dynamic Domain Name System, Система динамических доменных имен) поддерживает связь динамического IP-адреса (например, IP-адреса, назначенного сервером DHCP) с доменным именем. Пользователи, имеющие учетную запись Dynamic DNS, могут использовать эту функцию на DI-804HV.

- DDNS-** Когда IP-адрес автоматически назначается сервером DHCP, DDNS автоматически обновляет сервер DNS. Выберите **Disabled (отключено)** или **Enabled (включено)**.
- Provider-** Выберите из выпадающего меню провайдера DDNS.
- Host Name-** Введите имя хоста.
- Username/Email-** Введите имя пользователя или адрес email.
- Password/Key-** Введите пароль или ключ.

Использование меню настройки (продолжение)

Advanced > Routing



Dynamic Routing-

Параметры динамической маршрутизации (Dynamic Routing) позволяют маршрутизатору VPN маршрутизировать IP-пакеты в другую сеть автоматически. Используется протокол RIP, который периодически распространяет маршрутную информацию на другие маршрутизаторы сети. По умолчанию динамическая маршрутизация отключена. Нажмите RIPv1 или RIPv2, чтобы включить динамическую маршрутизацию по соответствующему протоколу.

RIP v1-

Протокол, с помощью которого информация об IP-адресах распространяется через Интернет.

RIP v2-

Улучшенная версия RIP v1 с новыми функциями, такими как аутентификация, домены маршрутизации, информация о следующем переходе и обмен масками подсети.

Использование меню настройки (продолжение)

Advanced > DMZ



Если есть клиентский ПК, который не может правильно запускать Интернет-приложения за DI-804HV, можно настроить неограниченный доступ в Интернет для такого клиента. Введите IP-адрес компьютера внутренней сети, который будет узлом DMZ. Добавление клиента в DMZ (Demilitarized Zone, незащищенная зона) может снизить безопасность сети, поэтому используйте эту опцию только в крайнем случае.

DMZ- **Включите (Enabled)** или **отключите (Disabled)** DMZ. DMZ (Demilitarized Zone, незащищенная зона) позволяет одному компьютеру получить незащищенный доступ в Интернет. По умолчанию DMZ **отключена**.

IP Address- Введите IP-адрес компьютера, перемещаемого в зону **DMZ**.

Использование меню настройки (продолжение)

Tools > Admin



На данной странице администратор DI-804HV может изменить системный пароль. Существует две учетные записи, позволяющие получить доступ к Web-интерфейсу управления маршрутизатора. Это администратор (admin) и пользователь (user). Администратор имеет права на чтение/запись, а пользователь – доступ только на чтение. Пользователь может только просматривать параметры, но не может их менять. Рекомендуется изменить пароль администратора, установленный по умолчанию. По умолчанию оба пароля пустые (не заданы).

Password

Для изменения паролей необходимо ввести новый пароль дважды для его подтверждения.

Remote Management-

Удаленное управление позволяет настраивать DI-804HV через интерфейс WAN из Интернет при помощи Web-браузера. Имя пользователя и пароль требуются для доступа к Web-интерфейсу управления. Обычно только член Вашей сети может просматривать встроенные web-страницы для администрирования. Удаленное управление позволяет выполнять задачи администрирования с удаленного узла.

IP Address-

IP-адрес компьютера в Интернет, которому будет разрешен доступ к маршрутизатору. Если ввести 0.0.0.0 в это поле, любой компьютер сможет получить доступ к маршрутизатору. Ввод 0.0.0.0 в данное поле снижает безопасность, и поэтому не рекомендуется.

Port-

Номер порта, используемый для доступа к маршрутизатору. Например, <http://x.x.x.x:8080>, где x.x.x.x – это IP-адрес интерфейса WAN маршрутизатора, а порт 8080 используется для доступа к Web-интерфейсу.

Использование меню настройки (продолжение)

Tools > Time



Установите системное время, введя его вручную или используя протокол NTP (Network Time Protocol, Протокол сетевого времени). Протокол NTP – это стандартный протокол Интернет, используемый для синхронизации времени DI-804HV.

Enable NTP-

Выберите эту опцию для включения протокола NTP и синхронизации системного времени с сервером NTP.

Default NTP Server-

Если протокол NTP включен, необходимо ввести адрес основного сервера NTP.

Time Zone-

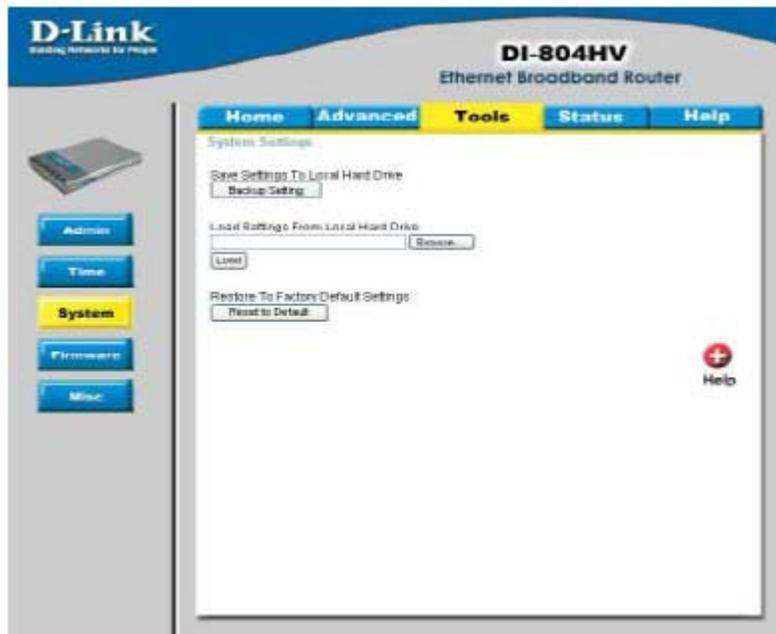
Выберите часовой пояс из выпадающего меню.

Set Device Date and Time-

Для установки времени вручную введите год (Year), месяц (Month), день (Day), час (Hour), минуту (Minute) и секунду (Second).

Использование меню настройки (продолжение)

Tools > System



Текущие параметры системы можно сохранить как файл на локальном жестком диске. Сохраненный файл и другие сохраненные конфигурационные файлы затем можно загрузить обратно на DI-804HV. Для загрузки конфигурационного файла на маршрутизатор нажмите кнопку **Browse**, найти и выбрать файл на локальном диске. Кроме того, можно выполнить сброс маршрутизатора к параметрам, установленным по умолчанию, нажав кнопку **Restore**. Используйте эту функцию только при необходимости. При сбросе маршрутизатора к установкам по умолчанию будут стерты все настроенные параметры. Перед выполнением сброса к установкам по умолчанию не забудьте сохранить текущие параметры системы в файл на жестком диске.

Save Settings to Local Hard Drive- Нажмите **Backup Setting** для сохранения текущих параметров в файл на жестком диске.

Load Settings from Local Hard Drive- Нажмите **Browse** для поиска сохраненного конфигурационного файла и затем нажмите **Load**.

Restore to Factory Default Settings- Нажмите **Restore to Default** для восстановления установленных по умолчанию параметров.

Использование меню настройки (продолжение)

Tools > Firmware



Данная страница позволяет обновить ПО маршрутизатора. Убедитесь, что ПО, которое Вы хотите использовать, находится на локальном жестком диске компьютера. Нажмите **Browse** для выбора локального жесткого диска и файла ПО на нем, который будет использоваться для обновления. Пожалуйста, обращайтесь на Web-сайт поддержки D-Link <http://support.dlink.com> за новыми версиями ПО. Вы можете загрузить обновления ПО на локальный жесткий диск с сайта D-Link. Обновление ПО не влияет на какие-либо системные параметры, но рекомендуется сохранить системные параметры в файл на жестком диске перед обновлением.

Browse-

После загрузки нового ПО нажмите **Browse** в данном окне для поиска файла обновления ПО на жестком диске. Нажмите **Apply** для завершения процедуры обновления ПО.



Внимание! Не выключайте питание устройства во время процедуры обновления ПО. Когда обновление завершено, устройство автоматически перезагрузится.

Использование меню настройки (продолжение)

Tools > Misc



Ping Test-

Ping-тест используется для тестирования соединения. Введите URL (например, www.dlink.com) или IP-адрес, который хотите протестировать, и нажмите **Ping**.

Restart Device-

Нажмите **Reboot** для перезагрузки DI-804HV.

Block WAN Ping-

Выберите **Enabled** для блокирования ping-теста интерфейса WAN. Если включить блокировку Ping-теста интерфейса WAN, IP-адрес интерфейса WAN DI-804HV не будет отвечать на тестовые пакеты. Блокирование Ping-теста может обеспечить дополнительный уровень защиты.

SPI Mode-

Когда включена данная функция, маршрутизатор будет записывать информацию о проходящих через него пакетах, такую как IP-адрес, номер порта, ACK, номер SEQ и т.д. Маршрутизатор будет также проверять каждый входящий пакет на корректность.

DoS-

Когда функция DoS включена, маршрутизатор будет предотвращать атаки Denial of Service (отказ в обслуживании) для всех компьютеров, подключенных к DI-804HV.

Использование меню настройки (продолжение)

Tools > Misc (продолжение)



UPnP

UPnP – это сокращение для Universal Plug and Play. Это сетевая архитектура, обеспечивающая совместимость сетевого оборудования, программного обеспечения и периферийных устройств. DI-804HV поддерживает UPnP и будет работать только с устройствами/ПО, совместимыми с UPnP. Если Вы не хотите использовать UPnP, то отключите его, выбрав **Disabled**.

VPN Pass Through-

DI-804HV поддерживает VPN (Virtual Private Network, виртуальная частная сеть) в режиме pass-through и для PPTP (Point-to-Point Tunneling Protocol, Протокол туннелирования «точка-точка»), и для IPSec (IP Security, Протокол безопасности IP). Если режим VPN pass-through включен, нет необходимости открывать виртуальные сервисы. Через DI-804HV можно установить множество соединений VPN. Это может быть полезно, когда в локальной сети находится большое количество клиентов VPN.

PPTP- выберите **Enabled (включен)** или **Disabled (отключен)**.

IPSec- выберите **Enabled (включен)** или **Disabled (отключен)**.

Non-standard FTP port-

Если FTP-сервер, к которому Вы хотите получить доступ, не использует стандартный порт 21, тогда введите номер порта, который использует FTP-сервер.

Использование меню настройки (продолжение)

Status > Device Info

D-Link
Building Networks for People

DI-804HV
Ethernet Broadband Router

Home Advanced Tools **Status** Help

Device Information
Firmware Version: V1.33b01, Wed, Jul 2 2003

LAN
MAC Address: 00-40-05-0F-73-27
IP Address: 192.168.0.1
Subnet Mask: 255.255.255.0
DHCP Server: Enabled

WAN
MAC Address: 00-40-05-0F-73-26
Connection: DHCP Client Connected
DHCP Renew DHCP Release
Remaining Lease Time: 71:17:34
IP Address: 10.80.1.246
Subnet Mask: 255.0.0.0
Gateway: 10.10.10.100
DNS Name Server: 10.10.10.41, 10.10.10.45

Peripheral
Dial-up Modem: Not ready

Device Time: Tue Jul 22 17:23:05 2003

Help

На данной странице показаны текущие параметры DI-804HV.

DHCP Renew- Нажмите эту кнопку для получения нового IP-адреса от сервера DHCP.

DHCP Release- Нажмите эту кнопку для освобождения IP-адреса, полученного от сервера DHCP.

Использование меню настройки (продолжение)

Status > Log



На данной странице показан журнал событий DI-804HV.

- First Page-** Переход на первую страницу журнала.
- Last Page-** Переход на последнюю страницу журнала.
- Previous-** Переход на предыдущую страницу журнала.
- Next-** Переход на следующую страницу журнала.
- Clear-** Очистка текущей страницы журнала.
- Log Settings-** Переход в меню настройки параметров журнала (см. следующую страницу).

Использование меню настройки (продолжение)

Status > Log Settings



E-Mail Alert-

DI-804HV можно настроить на отправку файла журнала событий на определенный адрес email.

SMTP Server IP -

Адрес сервера SMTP, который будет использоваться для отправки сообщений.

Email Address -

Адрес email, на который будут отправляться сообщения о регистрируемых событиях.

Send Mail Now-

Нажмите **Send Mail Now** для немедленной отправки email.

IP Address of the Syslog Server-

Введите IP-адрес сервера syslog в сети. Нажмите **Enable** для включения функции пересылки журнала событий на сервер syslog. DI-804HV будет отправлять журнал событий на указанный сервер syslog.

Log Type-

Выберите тип отправляемых сообщений. По умолчанию выбраны все типы.

Использование меню настройки (продолжение)

Status > Stats



В данном окне показывается статистика по трафику. Можно посмотреть, какое количество пакетов прошло через DI-804HV по портам WAN и LAN. Счетчик сбрасывается при каждой перезагрузке устройства.

Refresh-

Нажмите для обновления страницы.

Reset-

Нажмите для сброса накопленной статистики.

WAN-

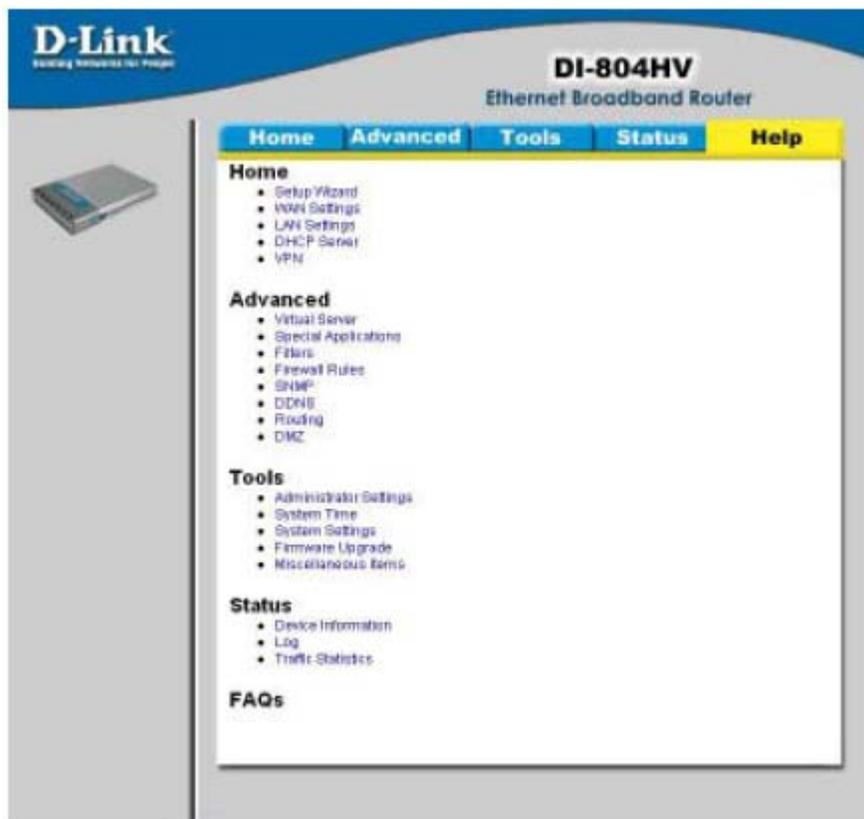
Показывает количество принятых/переданных пакетов для порта WAN.

LAN-

Показывает количество принятых/переданных пакетов для порта LAN.

Использование меню настройки (продолжение)

Help



Для получения помощи нажмите на вкладку **Help**. Меню Help позволяет получить более подробную информацию по нужному пункту меню настройки.

Основы сетевых технологий

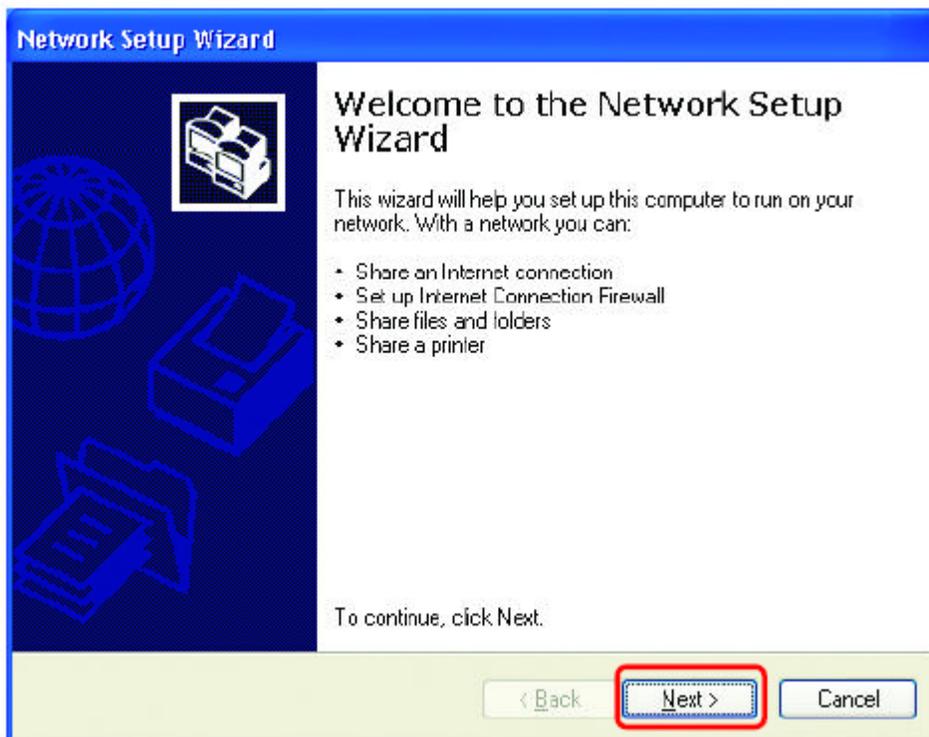
Использование мастера установки сети в Windows XP

В данном разделе Вы получите информацию о том, как настроить сеть дома или в офисе, используя **Microsoft Windows XP**.

Примечание: Пожалуйста, обращайтесь на web-сайты, такие как <http://www.homenethelp.com> и <http://www.microsoft.com/windows2000>, за более подробной информацией о настройке сети из компьютеров под управлением Windows 2000, ME или 98.

Выберите **Пуск>Панель управления>Сетевые подключения**

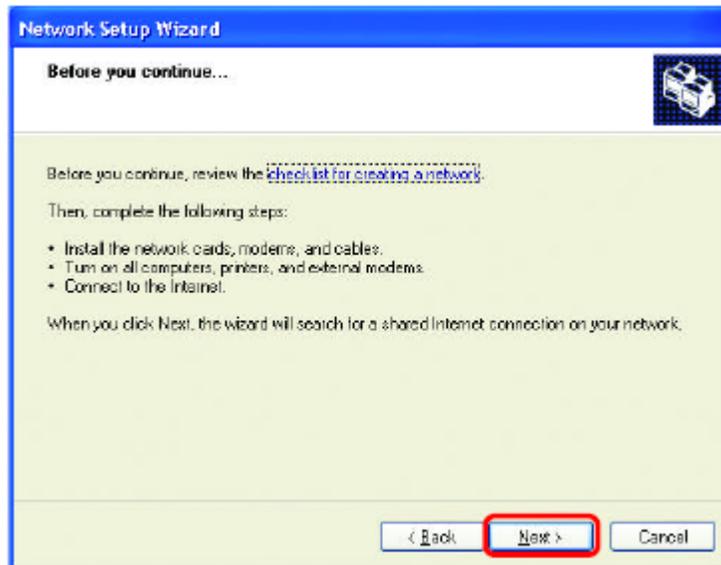
Нажмите **Мастер установки сети**



Когда появится это окно, нажмите **Далее**.

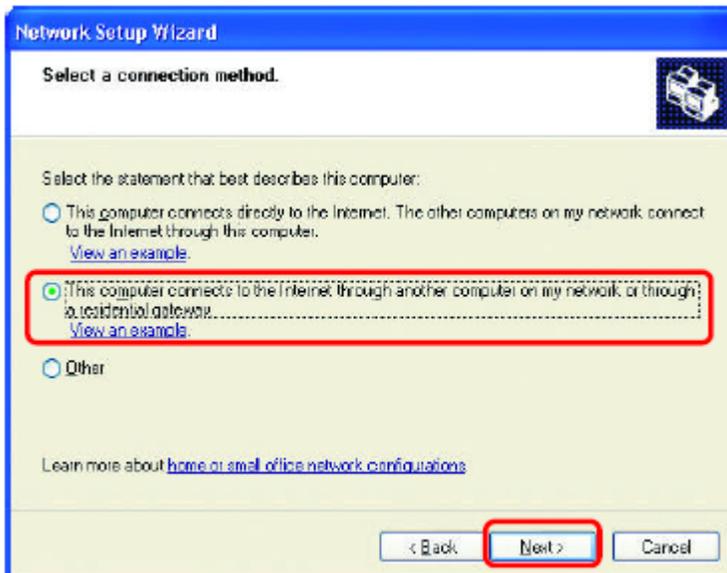
ОСНОВЫ СЕТЕВЫХ ТЕХНОЛОГИЙ

Пожалуйста, следуйте инструкциям, приведенным в данном окне:



Нажмите **Далее**

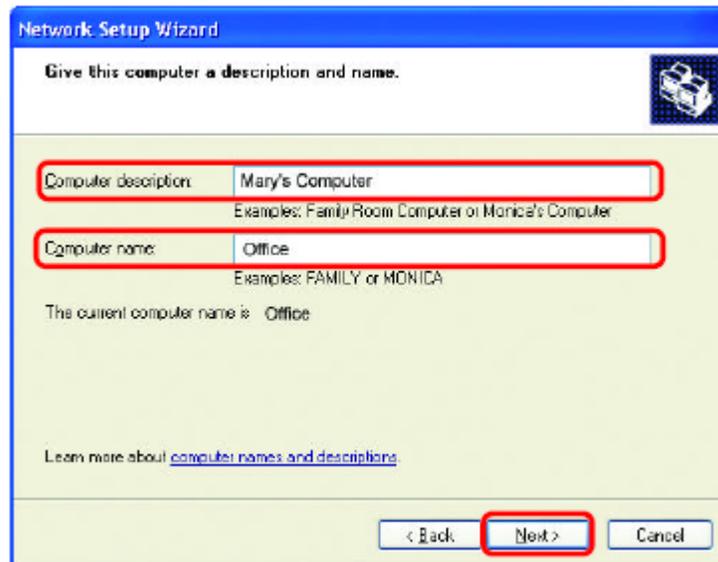
В следующем окне выберите наиболее подходящее описание Вашего компьютера. Если компьютер подключен к Интернет через шлюз/маршрутизатор, выберите вторую опцию, как показано на рисунке.



Нажмите **Далее**

Основы сетевых технологий

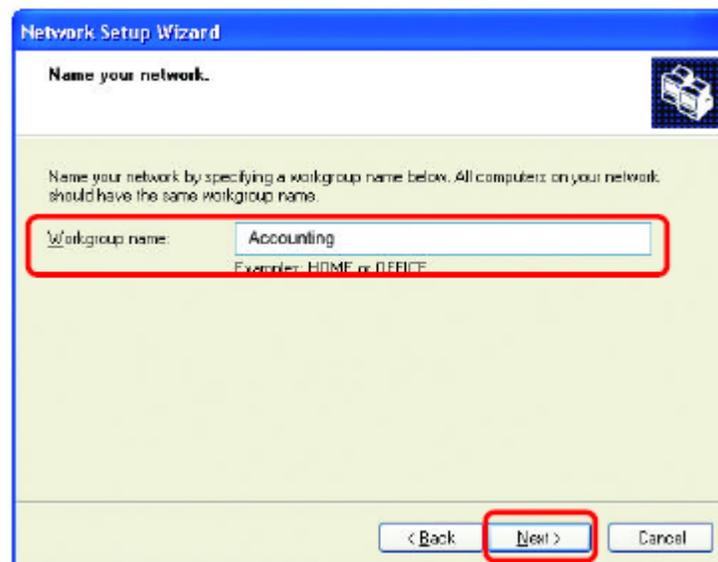
Введите **Описание компьютера** и **Имя компьютера** (дополнительно).



The screenshot shows the 'Network Setup Wizard' window with the title 'Give this computer a description and name.' It features two text input fields: 'Computer description' containing 'Mary's Computer' and 'Computer name' containing 'Office'. Below the 'Computer name' field, it states 'The current computer name is: Office'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a red box.

Нажмите **Далее**

Введите имя **Рабочей группы**. Все компьютеры сети должны иметь одно и то же **имя рабочей группы**.

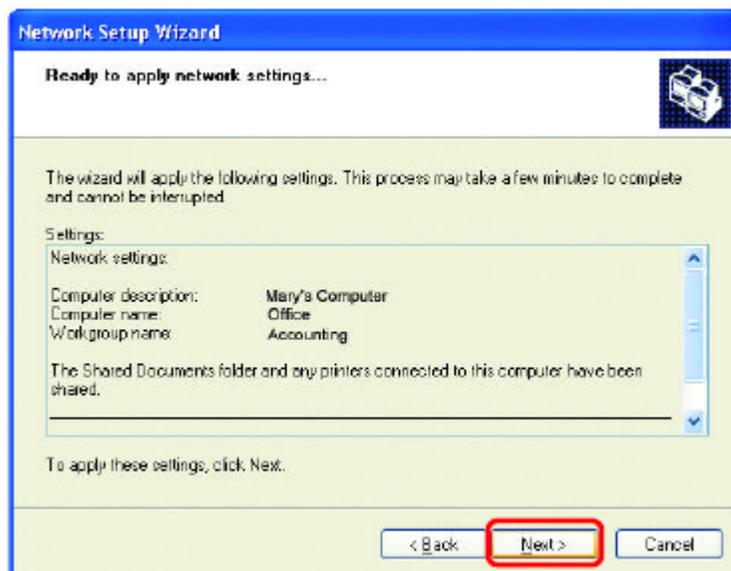


The screenshot shows the 'Network Setup Wizard' window with the title 'Name your network.' It contains a text input field for 'Workgroup name' with the value 'Accounting'. Below the field, it says 'Examples: HOME or OFFICE'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a red box.

Нажмите **Далее**

Основы сетевых технологий

Пожалуйста, подождите пока **Мастер установки сети** внесет изменения.



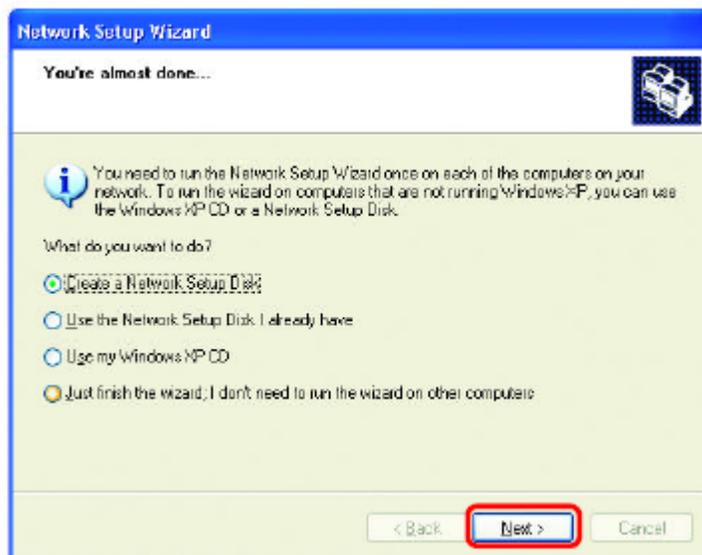
После завершения процедуры, нажмите **Далее**.

Пожалуйста, подождите пока **Мастер установки сети** настроит компьютер. Это может занять несколько минут.



Основы сетевых технологий

В следующем окне выберите опцию, которая соответствует Вашим требованиям. В данном примере было выбрано **Создать диск настройки сети**. Этот диск нужно будет запустить на каждом компьютере, подключаемом к сети. Нажмите **Далее**.



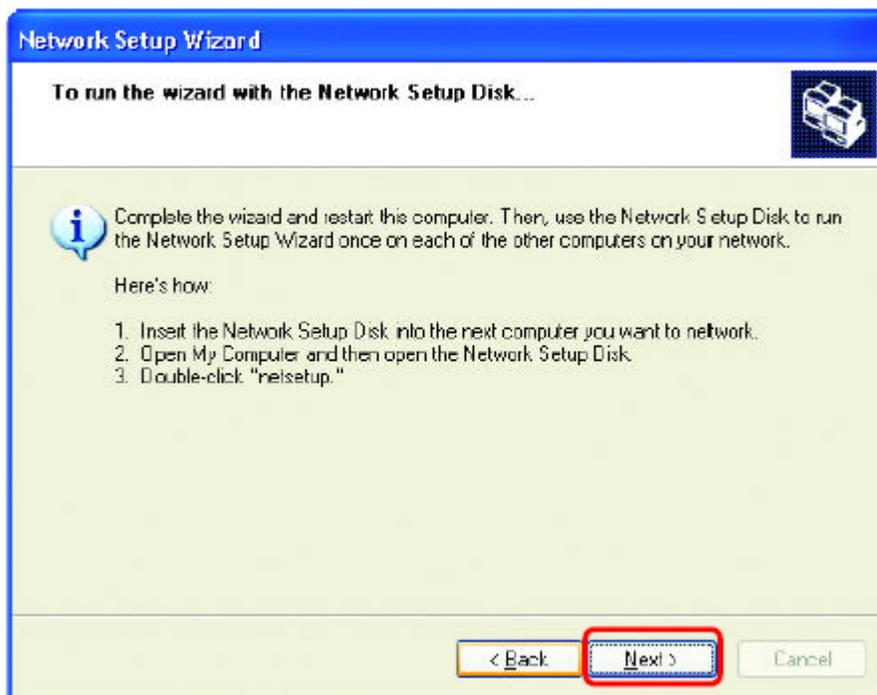
Вставьте дискету в привод для гибких дисков, в данном случае дисковод **A**.



Нажмите **Далее**

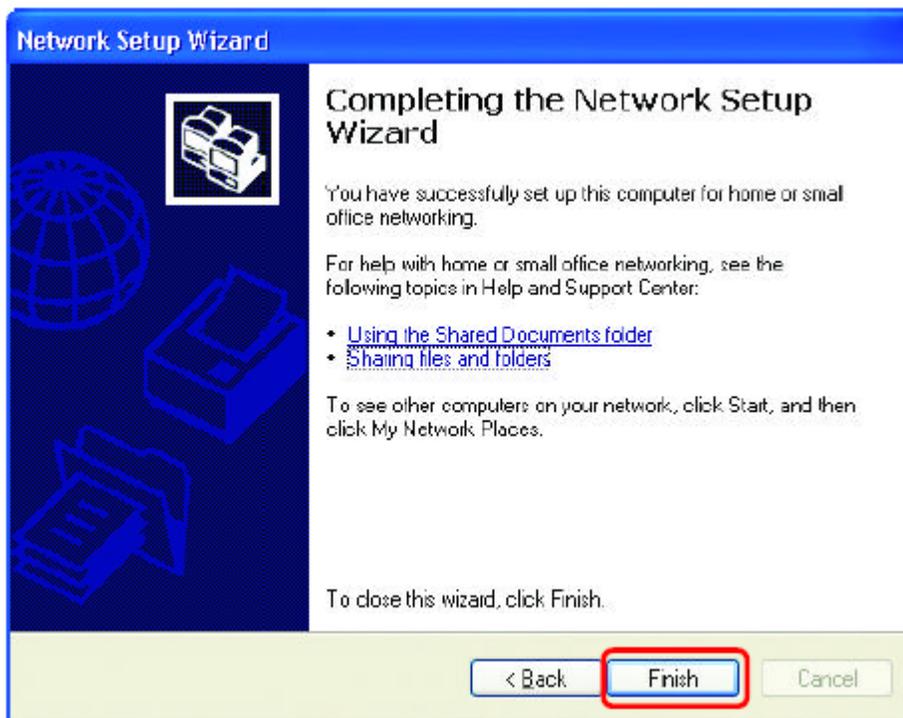


Пожалуйста, прочтите информацию под заголовком **Для этого выполните следующие действия** в следующем окне. После завершения работы **Мастера установки сети** нужно будет использовать **Диск настройки сети** для запуска **Мастера установки сети** на каждом компьютере сети. Для продолжения нажмите **Далее**.



Основы сетевых технологий

Пожалуйста, прочтите информацию, приведенную в данном окне, затем нажмите **Готово** для завершения **Мастера установки сети**.



Новые параметры вступят в силу после перезагрузки компьютера. Нажмите **Да** для перезагрузки компьютера.



Настройка данного компьютера завершена. Далее, необходимо запустить **Диск настройки сети** на каждом компьютере, подключаемом к сети. После запуска **Диска настройки сети** на всех компьютерах созданная сеть будет готова к работе.

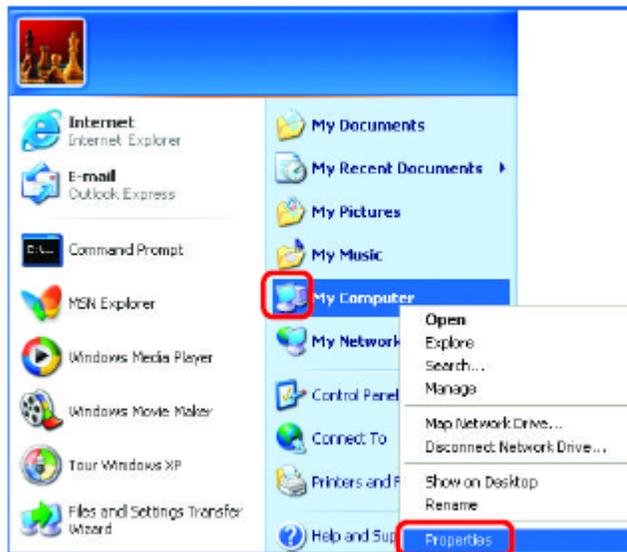
ОСНОВЫ СЕТЕВЫХ ТЕХНОЛОГИЙ

Назначение имени компьютеру

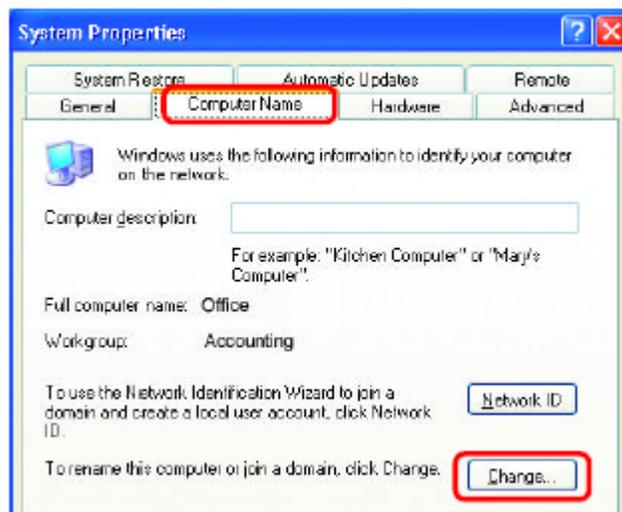
Для назначения имени компьютеру, пожалуйста, следуйте приведенным инструкциям.

В **Windows XP**:

- Нажмите **Пуск** (в нижнем левом углу экрана)
- Щелкните правой кнопкой на значке **Мой компьютер**
- Нажмите **Свойства**



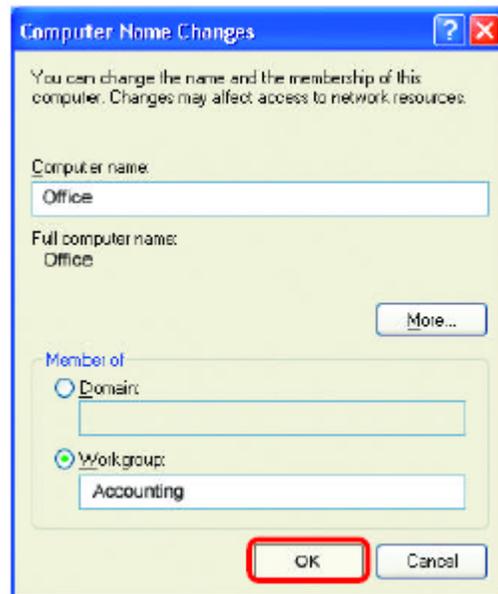
- Выберите вкладку **Имя компьютера** в окне Свойства системы.
- Вы можете ввести **Описание** компьютера; это дополнительная опция.
- Для переименования компьютера и присоединения к домену нажмите **Изменить**.



Основы сетевых технологий

Назначение имени компьютеру

- В данном окне введите **Имя компьютера**
- Выберите **Рабочая группа** и введите имя **рабочей группы**
- Все компьютеры в сети должны иметь одно и то же имя **Рабочей группы**.
- Нажмите **ОК**



Проверка IP-адреса в Windows XP

Компьютеры с сетевыми адаптерами, находящиеся в одной сети, должны иметь IP-адреса из одного и того же диапазона. (см. раздел *Начало работы* данного руководства пользователя, где дано определение диапазона IP-адресов.) Для проверки IP-адреса адаптера, пожалуйста, выполните следующее:

- Щелкните правой кнопкой на значке **Подключение по локальной сети** на панели задач
- Нажмите **Состояние**

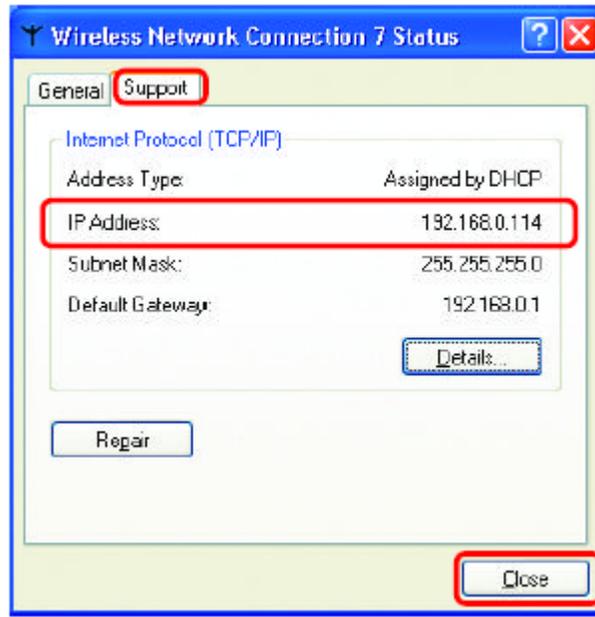


ОСНОВЫ СЕТЕВЫХ ТЕХНОЛОГИЙ

Проверка IP-адреса в Windows XP

Появится следующее окно.

- Выберите вкладку **Поддержка**
- Нажмите **Заккрыть**

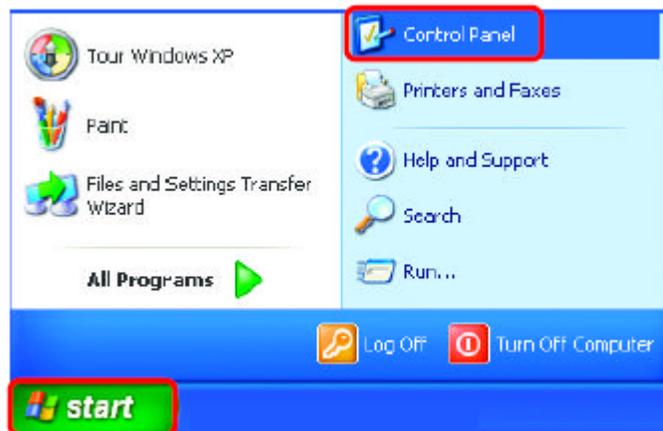


Назначение статического IP-адреса в Windows XP/2000

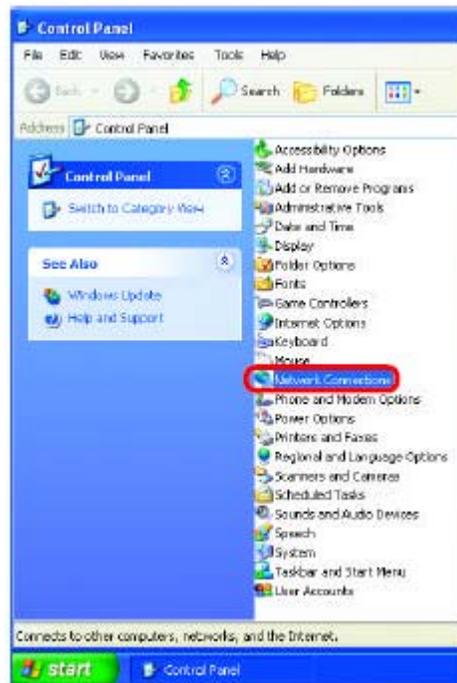
Примечание: Резидентные шлюзы/широкополосные маршрутизаторы будут автоматически назначать IP-адреса компьютерам в сети, используя протокол DHCP (Dynamic Host Configuration Protocol). Если Вы используете шлюз/маршрутизатор с поддержкой DHCP, то нет необходимости назначать статические IP-адреса.

Если не используется шлюз/маршрутизатор с поддержкой DHCP или необходимо назначить статические IP-адреса, пожалуйста, следуйте приведенным далее инструкциям:

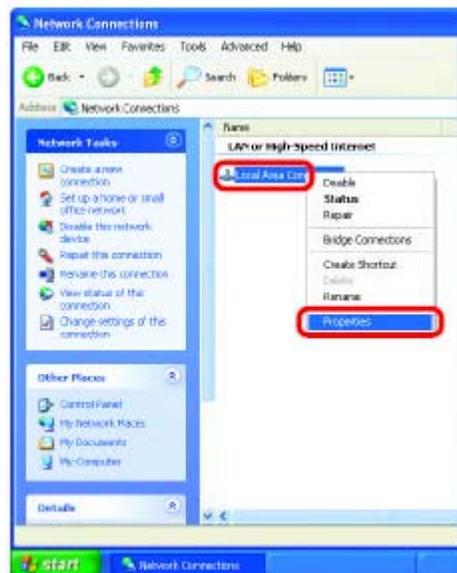
- Нажмите **Пуск**
- Дважды щелкните на **Панель управления**



- Дважды щелкните на **Сетевые подключения**



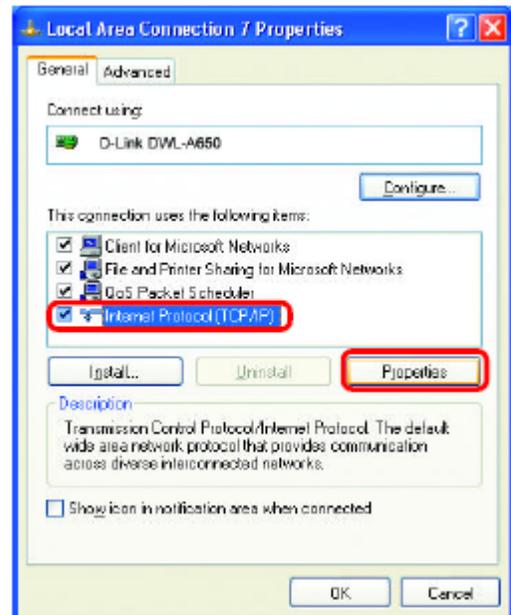
- Щелкните правой кнопкой на **Подключение по локальной сети**



- Нажмите **Свойства**

Назначение статического IP-адреса в Windows XP/2000

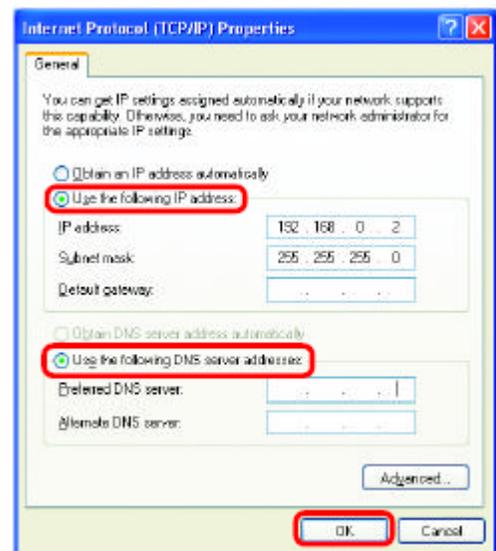
- Нажмите на **Протокол Интернета (TCP/IP)**
- Нажмите **Свойства**
- Введите **IP-адрес** и **маску подсети**. (IP-адреса всех устройств сети должны находиться в одном диапазоне. Например, если один компьютер имеет IP-адрес 192.168.0.2, то другие компьютеры должны иметь IP-адреса, которые будут последовательны, как например 192.168.0.3 и 192.168.0.4. Маска подсети должна быть одинакова для всех компьютеров сети.)



- Введите **адреса серверов DNS**. (Примечание: Если Вы ввели адрес сервера DNS, необходимо ввести IP-адрес Основного шлюза.)

Адреса серверов DNS будут предоставлены ISP.

- Нажмите **ОК**



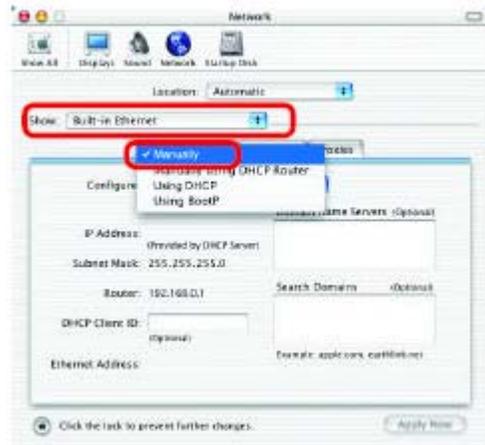
ОСНОВЫ СЕТЕВЫХ ТЕХНОЛОГИЙ

Назначение статического IP-адреса в Macintosh OSX

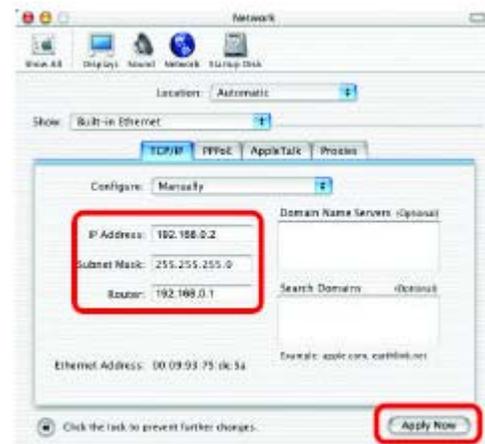
- Нажмите **Apple Menu** и выберите **System Preferences**
- Нажмите **Network**



- Выберите **Built-in Ethernet** из выпадающего меню **Show**
- Выберите **Manually** из выпадающего меню **Configure**



- Введите статический IP-адрес в поле **Static IP Address**, маску подсети в поле **Subnet Mask** и адрес основного шлюза в поле **Router IP Address**
- Нажмите **Apply Now**



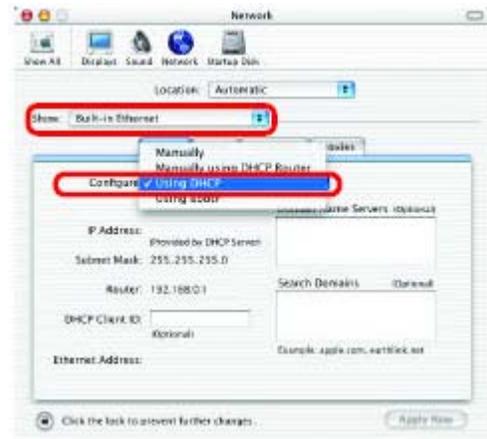
ОСНОВЫ СЕТЕВЫХ ТЕХНОЛОГИЙ

Назначение динамического IP-адреса в Macintosh OSX

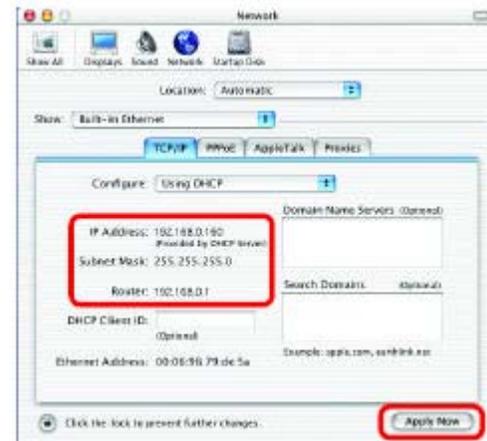
- Нажмите **Apple Menu** и выберите **System Preferences**
- Нажмите **Network**



- Выберите **Built-in Ethernet** из выпадающего меню **Show**
- Выберите **Using DHCP** из выпадающего меню **Configure**



- Нажмите **Apply Now**
- Через несколько секунд статический IP-адрес, маска подсети и адрес основного шлюза появятся в соответствующих полях **Static IP Address**, **Subnet Mask** и **Router IP Address**



Основы сетевых технологий

Добавление и организация совместного доступа к принтерам в Windows XP

После запуска **Мастера установки сети** на всех компьютерах в сети (пожалуйста, смотрите раздел **Мастер установки сети** в начале главы **Основы сетевых технологий**), можно использовать **Мастер установки принтеров** для добавления или организации совместного доступа к принтеру в сети. Всякий раз, когда необходимо добавить **локальный принтер** (принтер, подключенный напрямую к одному компьютеру), организовать совместный доступ к **LPR-принтеру** (принтер, подключенный к принт-серверу) или организовать совместный доступ к **сетевому принтеру** (принтер, подключенный к сети через шлюз/маршрутизатор), используйте **Мастер установки принтеров**. Пожалуйста, следуйте приведенным ниже инструкциям:

Во-первых, убедитесь, что Мастер установки сети был запущен на всех компьютерах сети.

На последующих страницах будет показано 3 способа использования **Мастера установки принтеров**:

- 1. Добавление локального принтера**
- 2. Организация совместного доступа к сетевому принтеру**
- 3. Организация совместного доступа к LPR-принтеру.**

(другие сетевые задачи)

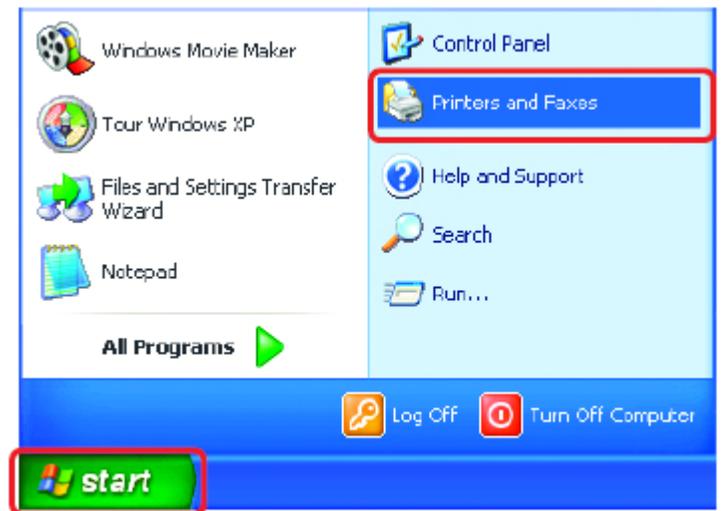
За помощью по другим сетевым задачам, не описанным здесь, для домашней или небольшой офисной сети, пожалуйста, обращайтесь к папке **Использование общих документов** и **Совместный доступ к файлам и папкам** в **Центре справки и поддержки** в Microsoft **Windows XP**.

Основы сетевых технологий

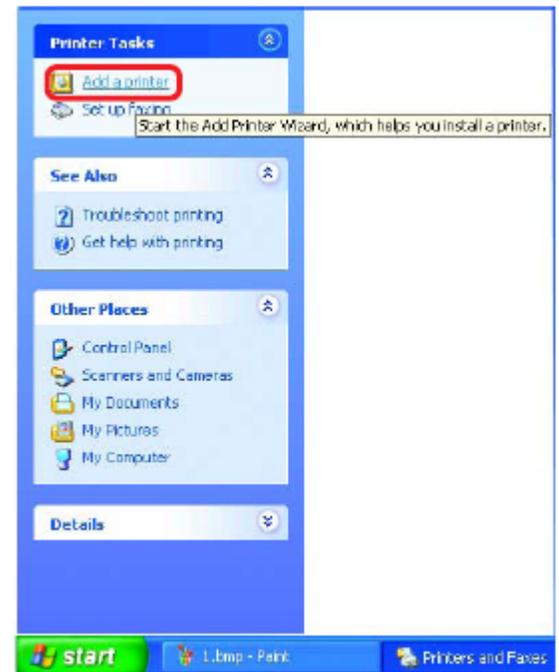
Добавление локального принтера (принтер, подключенный напрямую к компьютеру)

Принтер, не являющийся общим в сети, и подключенный напрямую к одному компьютеру, называется **локальным принтером**. Если не нужно организовывать совместный доступ к принтеру в сети, выполните следующие действия для добавления принтера на компьютер.

- Нажмите Пуск → Принтеры и факсы



- Нажмите Установка принтера

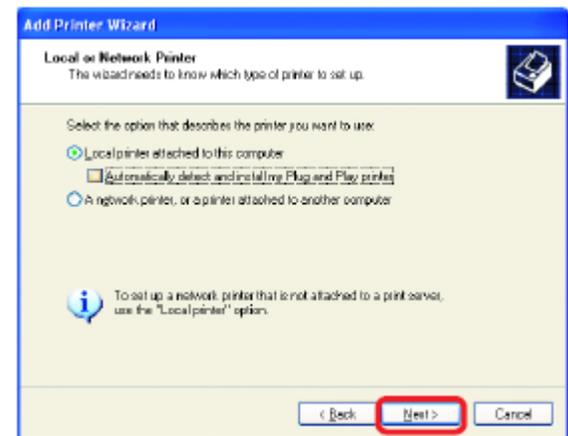


Добавление локального принтера

- Нажмите **Далее**



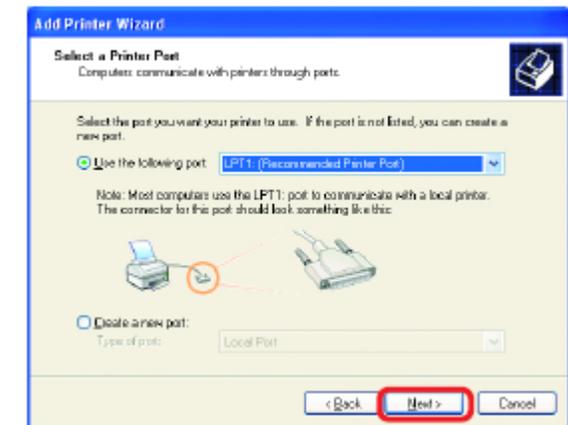
- Выберите **Локальный принтер**
- (Снимите флажок **Автоматическое определение и установка принтера "Plug and Play"**, если он установлен.)



- Нажмите **Далее**

- Выберите **Использовать порт:**
- Из выпадающего меню **выберите нужный порт** для Вашего принтера.

(Большинство компьютеров используют порт **LPT1:**, как показано на рисунке.)



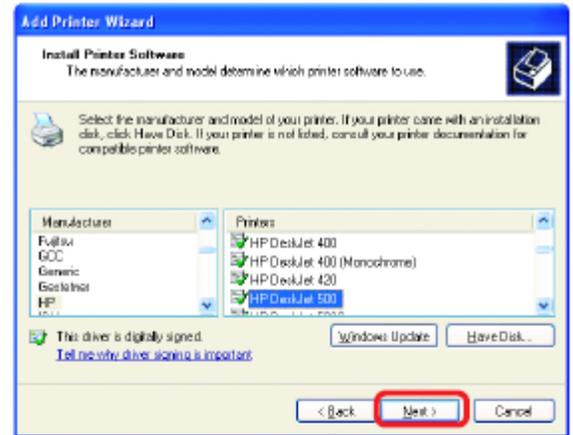
- Нажмите **Далее**

Основы сетевых технологий

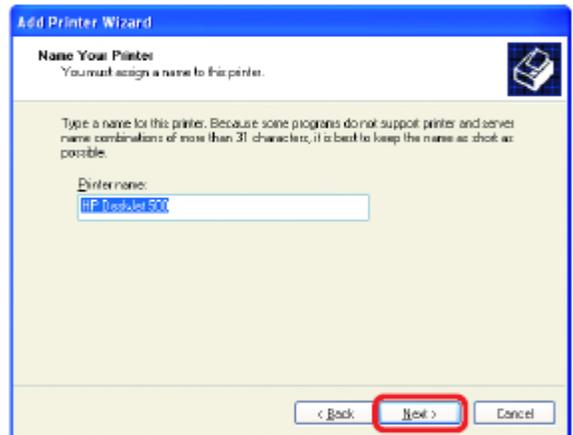
Добавление локального принтера

- Выберите **правильный драйвер** для принтера.
- Нажмите **Далее**

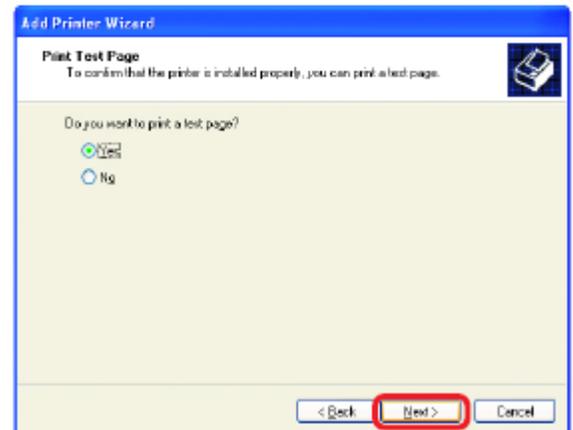
*(Если в списке нет правильного драйвера, вставьте CD или дискет, поставляемую вместе с принтером, и нажмите **Установить с диска.**)*



- В этом окне можно изменить имя принтера (дополнительно).



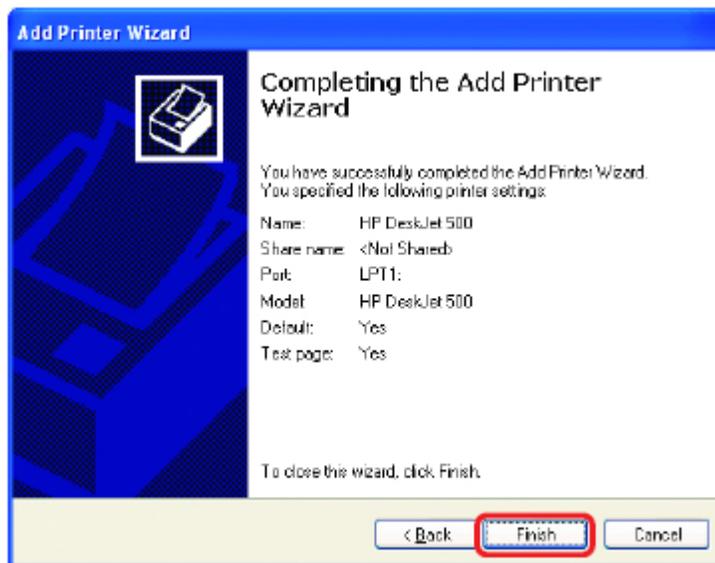
- Нажмите **Далее**
- Выберите **Да**, чтобы напечатать пробную страницу. Успешная печать подтвердит правильность выбора драйвера.
- Нажмите **Далее**



Основы сетевых технологий

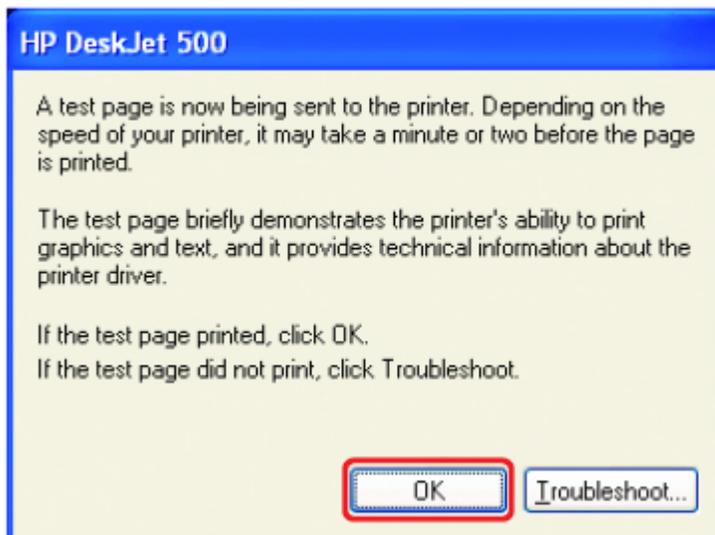
Добавление локального принтера

В данном окне показана информация о принтере.



Нажмите **Готово**

Когда тестовая страница будет напечатана,



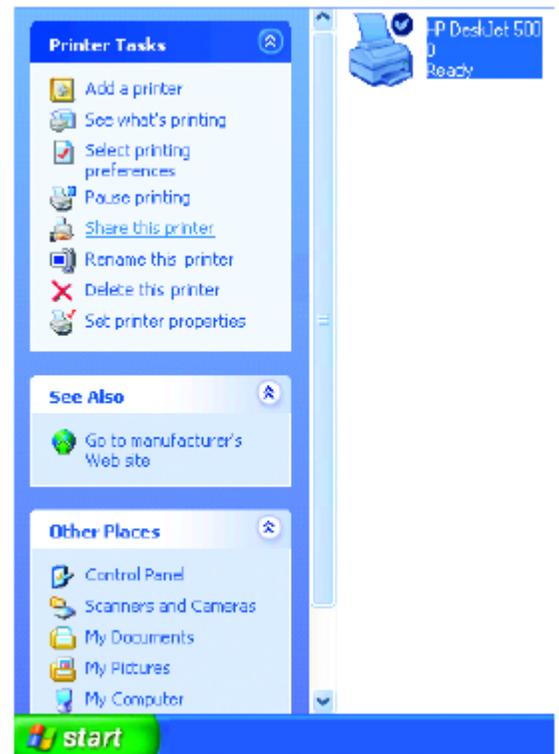
Нажмите **ОК**

Добавление локального принтера

- Нажмите **Пуск > Принтеры и факсы**

При успешной установке появится значок принтера, как показано на рисунке справа.

Установка локального принтера прошла успешно.



Совместный доступ к сетевому принтеру

После запуска **Мастера установки сети** на всех компьютерах в сети, можно запустить **Мастер установки принтеров** на всех компьютерах. Пожалуйста, выполните следующие действия для организации совместного доступа к принтеру с помощью **Мастера установки принтеров**:

- Нажмите **Пуск > Принтеры и факсы**



ОСНОВЫ СЕТЕВЫХ ТЕХНОЛОГИЙ

Совместный доступ к сетевому принтеру

- Нажмите **Установка принтера**



- Нажмите **Далее**



- Выберите **Сетевой принтер**

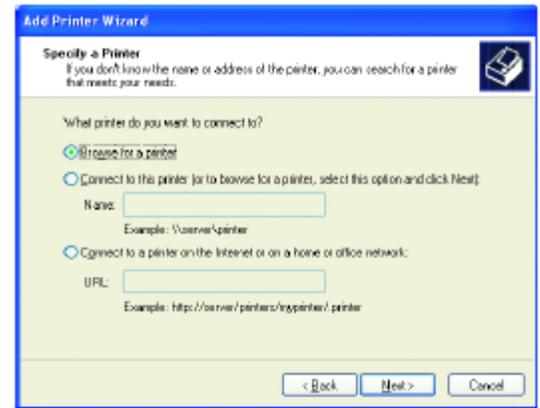


- Нажмите **Далее**

ОСНОВЫ СЕТЕВЫХ ТЕХНОЛОГИЙ

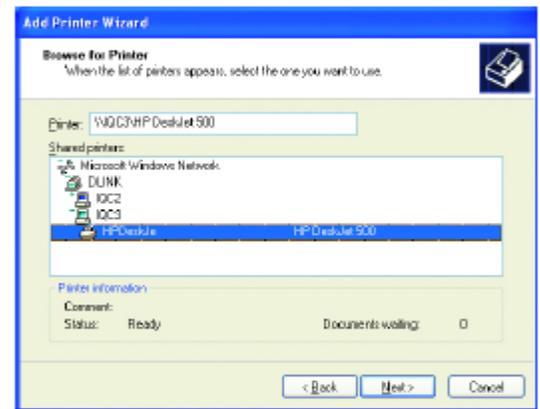
Совместный доступ к сетевому принтеру

- Выберите **Обзор принтеров**



- Нажмите **Далее**

Выберите **принтер**, который хотите добавить.



- Нажмите **Далее**

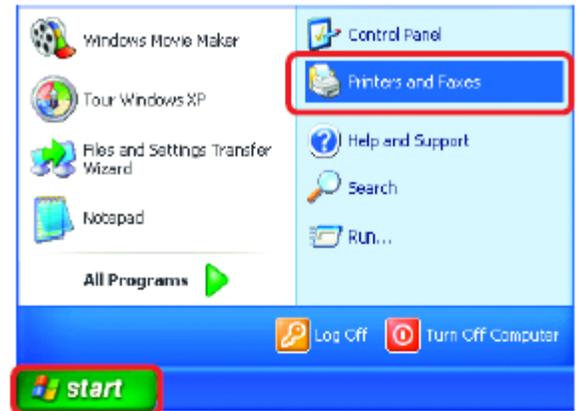


- Нажмите **Готово**

Основы сетевых технологий

Совместный доступ к сетевому принтеру

- Для проверки правильности установки
- Нажмите **Пуск > Принтеры и факсы**



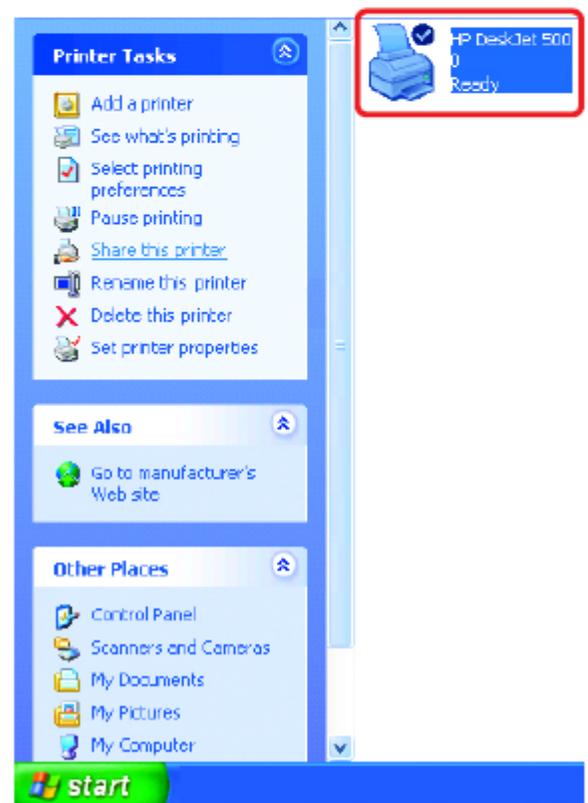
При успешной установке появится значок принтера, как показано на рисунке справа.

Добавление сетевого принтера прошло успешно.

Для добавления сетевого принтера:

- Запомните **имя принтера**
- Запустите **Мастер установки принтеров** на всех компьютерах сети
- Перед этим не забудьте запустить **Мастер установки сети** на всех компьютерах сети

После запуска **Мастера установки принтеров** на всех компьютерах сети, принтер станет общим.



ОСНОВЫ СЕТЕВЫХ ТЕХНОЛОГИЙ

Совместный доступ к LPR-принтеру

Для организации совместного доступа к **LPR-принтеру** (используя принт-сервер), необходим принт-сервер, такой как **DP-101P+**. Пожалуйста, не забудьте запустить **Мастер установки сети** на всех компьютерах сети. Для организации совместного доступа к **LPR-принтеру**, пожалуйста, выполните следующее:

- Нажмите **Пуск → Принтеры и факсы**
- Нажмите **Установка принтера**

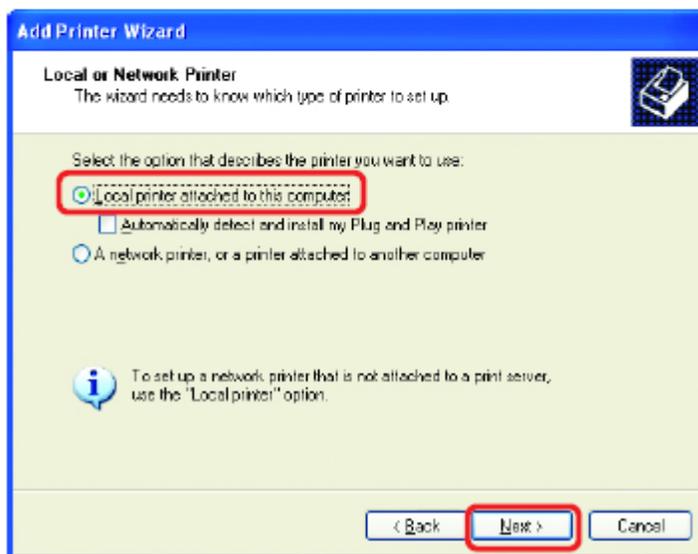
Появится окно, показанное на рисунке справа.

- Нажмите **Далее**



- Выберите **Локальный принтер**

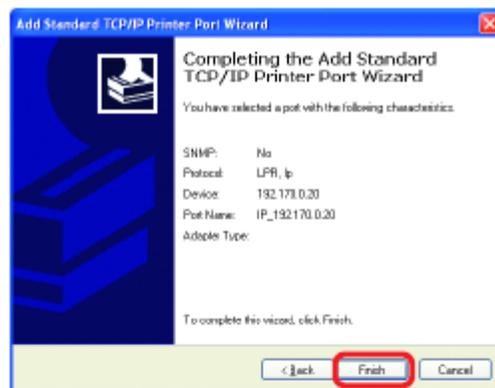
- Нажмите **Далее**



ОСНОВЫ СЕТЕВЫХ ТЕХНОЛОГИЙ

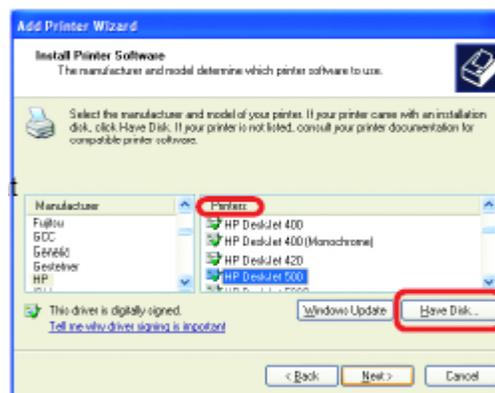
Совместный доступ к LPR-принтеру

- В окне будет показана информация о принтере.



- Нажмите **Готово**

- Выберите добавляемый **принтер** из списка **принтеры**.

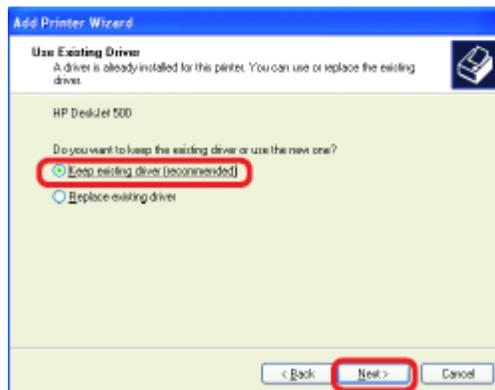


- Вставьте диск с драйвером, поставляемый вместе с принтером.

- Нажмите **Установить с диска**

Если драйвер уже установлен, выполните следующее:

- Выберите **Сохранить существующий драйвер**



- Нажмите **Далее**

Совместный доступ к LPR-принтеру

- Можно переименовать принтер. Это дополнительно.
- *Пожалуйста, запомните имя принтера. Эта информация пригодится при запуске **Мастера установки принтеров** на всех компьютерах сети.*

- Нажмите **Далее**



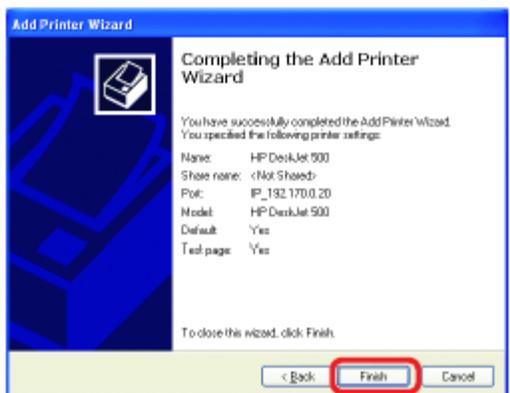
- Нажмите **Да** для печати тестовой страницы

- Нажмите **Далее**



В данном окне будет показана информация о принтере.

- Нажмите **Готово** для завершения процедуры добавления принтера.
- Пожалуйста, запустите **Мастер установки принтеров** на всех компьютерах сети для организации совместного доступа к принтеру.



Примечание: Необходимо запустить **Мастер установки сети** на всех компьютерах сети до запуска **Мастера установки принтеров**.

Сброс DI-804HV к заводским установкам по умолчанию

После того, как Вы испробовали все остальные методы поиска и устранения неисправностей в сети, можно выполнить сброс DI-804HV к заводским установкам по умолчанию.



Для аппаратного сброса DI-804HV к установкам по умолчанию, пожалуйста, выполните следующее:

- Найдите кнопку **Reset** на задней панели DI-804HV
- Используя скрепку для бумаги, нажмите кнопку **Reset**
- Нажимайте на кнопку примерно в течение 5 секунд (не нажимайте слишком долго) и затем отпустите (или отпустите, когда индикаторы M1 и M2 одновременно замигают).
- После этого будут восстановлены заводские установки DI-804HV

Технические характеристики

Стандарты

- IEEE 802.3 10BASE-T Ethernet
- IEEE 802.3u 100BASE-TX Fast Ethernet
- Управление потоком IEEE 802.3x
- ANSI/IEEE 802.3 NWay автосогласование

VPN в режиме Pass Through

- PPTP
- L2TP
- IPSec

Управление устройством:

- Web-интерфейс: Internet Explorer v. 6 или выше; Netscape Navigator v 6x или выше; или другой браузер с поддержкой Java.

Индикаторы

- WAN
- LAN
- M1
- M2
- COM

Рабочая температура

- От 5°C до 55°C

Влажность:

- 10-90%

Источник питания:

- Постоянный ток 5В

Физические размеры:

- L (длина) = 192 мм
- W (ширина) = 48 мм
- H (высота) = 31 мм

Вес:

- 0.3 кг

Порты:

- 4 порта NWay 10BASE-T/100BASE-TX Fast Ethernet LAN (автоопределение типа подключаемого кабеля)
- 1 порт NWay 10BASE-T/100BASE-TX Fast Ethernet WAN (автоопределение типа подключаемого кабеля)
- 1 COM-порт (для аналогового модема)

Часто задаваемые вопросы

Почему я не могу получить доступ к Web-интерфейсу управления?

При вводе IP-адреса DI-804HV (192.168.0.1), Вы не подключаетесь к Интернет и не должны быть подключены к Интернет. Устройство имеет утилиту, встроенную в чип ROM. Ваш компьютер должен находиться в той же IP-подсети, чтобы подключиться к Web-интерфейсу управления.

Для разрешения проблем, связанных с доступом к web-интерфейсу управления, пожалуйста, выполните следующие шаги.

Шаг 1 Проверьте физическое соединение, индикатор соединения должен при этом постоянно гореть. Если индикатор не горит постоянно, попробуйте использовать другой кабель или подключиться к другому порту устройства, если возможно. Если компьютер выключен, индикатор соединения может не гореть.

Какой тип кабеля необходимо использовать?

Для следующих подключений требуется перекрестный кабель:

- Компьютер к компьютеру
- Компьютер к порту Uplink
- Компьютер к точке доступа
- Компьютер к принт-серверу
- Компьютер/XBOX/PS2 к DWL-810
- Компьютер/XBOX/PS2 к DWL-900AP+
- Порт Uplink к порту Uplink (концентратора/коммутатора)
- Обычный порт к обычному порту (концентратора/коммутатора)

Для следующих подключений требуется прямой кабель:

- Компьютер к резидентному шлюзу/маршрутизатору
- Компьютер к обычному порту (концентратора/коммутатора)
- Точка доступа к обычному порту (концентратора/коммутатора)
- Принт-сервер к обычному порту (концентратора/коммутатора)
- Порт Uplink к обычному порту (концентратора/коммутатора)

Правило: "Если индикатор горит, кабель подключен правильно".

Часто задаваемые вопросы (продолжение)

Почему я не могу получить доступ к Web-интерфейсу управления? (продолжение)

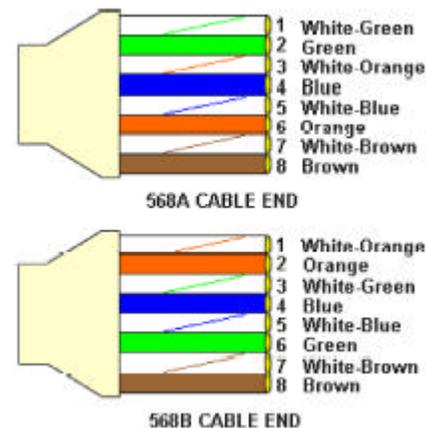
Какой тип кабеля необходимо использовать? (продолжение)

Какая разница между перекрестным кабелем и прямым кабелем?

Разводка проводов в перекрестном кабеле и прямом кабеле отличается. Два типа кабеля имеют различное назначение для различных применений в локальной сети. EIA/TIA 568A/568B определяет стандарты разводки и допускает два различных цветовых обозначения, как показано на рисунке.

**Провода с цветной изоляцией могут иметь белые полоски и фигурировать в таком виде в различных документах.*

Как различить прямой кабель и перекрестный: Основной способ различения двух типов кабелей – сравнить разводку проводов на разных концах кабеля. Если разводка совпадает на обоих концах кабеля, это прямой кабель. Если один из концов имеет противоположную разводку, это перекрестный кабель.



Все, что нужно знать для правильного изготовления кабеля, это разводка проводов на двух концах кабеля и следующие правила:

Прямой кабель имеет одинаковую разводку на обоих концах

Перекрестный кабель имеет различную разводку на концах кабеля

Нет функциональной разницы, каким стандартом Вы руководствуетесь при изготовлении прямого кабеля, поскольку оба конца кабеля имеют одинаковую разводку. Начинать изготовление перекрестного кабеля можно с любого конца, поскольку другой конец отличается лишь разводкой. Нет принципиальной разницы, какой конец кабеля будет каким. Важна лишь разводка проводов кабеля. Использование образца разводки, отличного от показанного на рисунке, может привести к проблемам при подключении.

Когда использовать перекрестный кабель и когда использовать прямой кабель:

Компьютер к компьютеру – перекрестный

Компьютер к обычному порту концентратора/коммутатора - прямой

Компьютер к порту uplink концентратора/коммутатора - перекрестный

Порт uplink концентратора/коммутатора к порту uplink другого концентратора/коммутатора – перекрестный

Порт uplink концентратора/коммутатора к обычному порту другого концентратора/коммутатора - прямой

Часто задаваемые вопросы (продолжение)

Почему я не могу получить доступ к Web-интерфейсу управления? (продолжение)

Шаг 2 Отключите любое установленное на компьютере ПО обеспечения безопасности. Программные межсетевые экраны, такие как Zone Alarm, Black Ice, Sygate, Norton Personal Firewall и т.д. могут блокировать доступ к Web-интерфейсу управления. Обратитесь к встроенной в программный межсетевой экран справке за более подробной информацией об отключении и настройке межсетевого экрана.

Шаг 3 Настройте параметры Интернет

Нажмите **Пуск>Настройка>Панель управления**. Дважды щелкните на значке **Свойства обозревателя**. На вкладке **Безопасность**

Нажмите кнопку **По умолчанию** для восстановления параметров по умолчанию.



Выберите вкладку **Подключения** и выберите опцию **Никогда не использовать**. Нажмите кнопку **Настройка LAN**



Ничего не требуется менять. Нажмите **ОК**



Выберите вкладку **Дополнительно** и нажмите кнопку **Восстановить значения по умолчанию** для восстановления параметров к значениям по умолчанию.



Нажмите **ОК**. Перейдите на рабочий стол и закройте все открытые окна.

Часто задаваемые вопросы (продолжение)

Почему я не могу получить доступ к Web-интерфейсу управления? (продолжение)

Шаг 4 Проверьте IP-адрес. Компьютер должен иметь IP-адрес из того же диапазона, что и устройство, к которому Вы хотите получить доступ. Большинство устройств D-Link использует диапазон адресов 192.168.0.X.

Как найти IP-адрес в Windows 95, 98 или ME?

Шаг 1 Нажмите **Пуск**, затем нажмите **Выполнить**.

Шаг 2 Появится диалоговое окно **Выполнить**. Введите **winipcfg**, как показано на рисунке, и нажмите **ОК**.



Шаг 3 Появится окно **Настройка параметров IP**, показывающее **информацию об адаптере Ethernet**.

- Выберите адаптер из выпадающего меню.
- Если Вы не видите свой адаптер в меню, адаптер установлен не правильно.



Шаг 4 После выбора нужного адаптера в окне появятся IP-адрес, маска подсети и адрес основного шлюза.

Шаг 5 Нажмите **ОК**, что закрыть окно **настройки параметров IP**.

Часто задаваемые вопросы (продолжение)

Почему я не могу получить доступ к Web-интерфейсу управления? (продолжение)

Шаг 4 (продолжение) Проверьте IP-адрес. Компьютер должен иметь IP-адрес из того же диапазона, что и устройство, к которому Вы хотите получить доступ. Большинство устройств D-Link использует диапазон адресов 192.168.0.X.

Как найти IP-адрес в Windows 2000/XP?

Шаг 1 Нажмите **Пуск** и затем **Выполнить**.

Шаг 2 Введите **cmd** и затем нажмите **ОК**.



Шаг 3 В командной строке введите **ipconfig**. Команда вернет IP-адрес, маску подсети и адрес основного шлюза.

```
D:\WINNT\system32\CMD.EXE
Microsoft Windows [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

D:\>ipconfig

Microsoft Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 192.168.0.174
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 192.168.0.1

D:\>_
```

Шаг 4 Введите **exit**, чтобы закрыть командную строку.

Часто задаваемые вопросы (продолжение)

Почему я не могу получить доступ к Web-интерфейсу управления? (продолжение)

Шаг 4 (продолжение) Проверьте IP-адрес. Компьютер должен иметь IP-адрес из того же диапазона, что и устройство, к которому Вы хотите получить доступ. Большинство устройств D-Link использует диапазон адресов 192.168.0.X.

Убедитесь, что Вы помните IP-адрес основного шлюза компьютера. Адресом основного шлюза является IP-адрес маршрутизатора D-Link. По умолчанию его адрес равен 192.168.0.1.

Как назначить статический IP-адрес в Windows XP?

Шаг 1

Нажмите **Пуск > Панель управления > Сетевые подключения**.

Шаг 2 См. [Шаг 2](#) для Windows 2000 и далее.

Как назначить статический IP-адрес в Windows 2000?

Шаг 1 Щелкните правой кнопкой на **Сетевое окружение** и выберите **Свойства**.

Шаг 2 Щелкните правой кнопкой на **Подключение по локальной сети**, относящееся к Вашей сети, и выберите **Свойства**.

Выберите **Протокол Интернета (TCP/IP)** и нажмите **Свойства**.



Часто задаваемые вопросы (продолжение)

Почему я не могу получить доступ к Web-интерфейсу управления?
(продолжение)

Как назначить статический IP-адрес в Windows 2000? (продолжение)

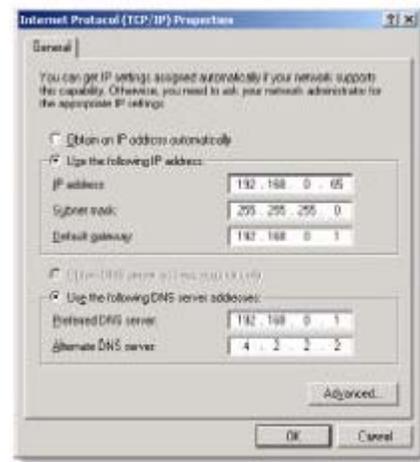
Нажмите **Использовать следующий IP-адрес** и введите IP-адрес из того же диапазона, что и IP-адрес Вашего маршрутизатора в LAN. Например: Если IP-адрес маршрутизатора в LAN равен 192.168.0.1, вводимый IP-адрес должен равняться 192.168.0.X, где X = 2 - 99. Убедитесь, что введенный IP-адрес не используется каким-либо устройством в сети.

Введите адрес **основного шлюза** из того же диапазона, что и IP-адрес Вашего маршрутизатора в LAN (192.168.0.1).

Введите адрес **предпочитаемого DNS-сервера** из того же диапазона, что и IP-адрес Вашего маршрутизатора в LAN (192.168.0.1).

Адрес **альтернативного DNS-сервера** вводить не требуется или можно ввести адрес DNS-сервера ISP.

Нажмите **ОК** два раза. Может появиться запрос на перезагрузку компьютера. Нажмите **Да**.



Как назначить статический IP-адрес в Windows 98/ME?

Шаг 1 Щелкните правой кнопкой на значке **Сетевое окружение** на рабочем столе и выберите **Свойства**.

Выберите **TCP/IP** и нажмите кнопку **Свойства**. Если в системе установлено более одного адаптера, для каждого адаптера будет показана «связка» TCP/IP. Выберите **TCP/IP > (нужный сетевой адаптер)** и затем нажмите **Свойства**.



Почему я не могу получить доступ к Web-интерфейсу управления? (продолжение)

Как назначить статический IP-адрес в Windows 98/ME? (продолжение)

Шаг 2 Выберите **Указать IP-адрес**.

Введите IP-адрес из того же диапазона, что и IP-адрес Вашего маршрутизатора в LAN. Например: Если IP-адрес маршрутизатора в LAN равен 192.168.0.1, вводимый IP-адрес должен равняться 192.168.0.X, где X = 2 - 99. Убедитесь, что введенный IP-адрес не используется каким-либо устройством в сети.



Шаг 3 Выберите вкладку **Шлюз**.

Введите IP-адрес маршрутизатора в LAN (192.168.0.1). Нажмите **Добавить** после ввода.



Шаг 4 Выберите вкладку **Настройка DNS**.

Нажмите **Включить DNS**. Введите имя **узла** (можно ввести любое слово). В списке серверов DNS введите IP-адрес маршрутизатора в LAN (192.168.0.1). Нажмите **Добавить**.



Шаг 5 Нажмите **ОК** два раза.

Когда появится запрос на перезагрузку, нажмите **Да**. После перезагрузки компьютеру будет назначен статический IP-адрес (частный).

Шаг 5 Подключитесь к Web-интерфейсу управления. Откройте web-браузер и введите IP-адрес маршрутизатора D-Link в адресной строке. Должна появиться страница регистрации для получения доступа к Web-интерфейсу управления. Следуйте инструкциям для регистрации и завершите настройку.

Часто задаваемые вопросы (продолжение)

Как нужно настроить маршрутизатор на работу через подключение по кабельному модему?

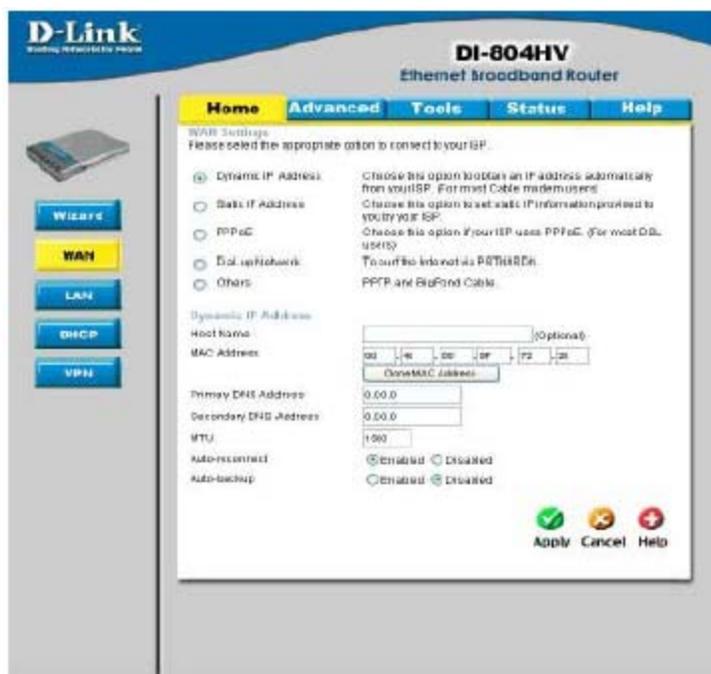
Кабельное подключение с динамическим IP-адресом

(IE AT&T-BI, Cox, Adelphia, Rogers, Roadrunner, Charter и Comcast).

Примечание: Пожалуйста, настройте маршрутизатор при помощи компьютера, который подключался последним напрямую к кабельному модему.

Шаг 1 Подключитесь к Web-интерфейсу управления, введя IP-адрес (по умолчанию:192.168.0.1) маршрутизатора в адресной строке браузера. Имя пользователя (User Name) - **admin** (все буквы в нижнем регистре), пароль (Password) не задан (оставьте поле пустым).

Шаг 2 Выберите вкладку **Home** и нажмите кнопку **WAN**. По умолчанию используется подключение с динамическим IP-адресом (Dynamic IP Address), но если эта опция не выбрана, выберите ее, нажав Dynamic IP Address. Нажмите **Clone Mac Address**. Нажмите **Apply** и затем **Continue** для сохранения изменений.



Часто задаваемые вопросы (продолжение)

Как нужно настроить маршрутизатор на работу через подключение по кабельному модему? (продолжение)

Шаг 3 Цикл включения кабельного модема и маршрутизатора:

Выключите кабельный модем (первым). Выключите маршрутизатор. Оставьте их выключенными на 2 минуты.** Включите кабельный модем (первым). Дождитесь, пока индикатор соединения на кабельном модеме не станет гореть постоянно. Включите маршрутизатор. Подождите 30 секунд.

** Если у Вас модем Motorola (Surf Board), оставьте устройства выключенными как минимум на 5 минут.

Шаг 4 Заново выполните шаг 1 и подключитесь к Web-интерфейсу управления. Выберите вкладку **Status** и нажмите кнопку **Device Info**. Если под заголовком **WAN** все еще не появился публичный IP-адрес, нажмите кнопки **DHCP Renew** и **Continue**.

Кабельное подключение со статическим IP-адресом

Шаг 1 Подключитесь к Web-интерфейсу управления, введя IP-адрес (по умолчанию: 192.168.0.1) маршрутизатора в адресной строке браузера. Имя пользователя (User Name) - **admin** (все буквы в нижнем регистре), пароль (Password) не задан (оставьте поле пустым).



Шаг 2 Выберите вкладку **Home** и нажмите кнопку **WAN**. Выберите **Static IP Address** и введите статический IP-адрес и другие параметры, предоставленные ISP.

Если Вы не знаете значения требуемых параметров, необходимо обратиться к ISP.

Шаг 3 Нажмите **Apply** и затем **Continue** для сохранения изменений.

Шаг 4 Выберите вкладку **Status** и нажмите кнопку **Device Info**. Заданные параметры IP должны отображаться под заголовком **WAN**.



Часто задаваемые вопросы (продолжение)

Как нужно настроить маршрутизатор на работу через Earthlink DSL или какое-либо подключение PPPoE?

Не забудьте отключить или удалить любое установленное на компьютере ПО PPPoE, такое как WinPoet или Enternet 300, иначе подключиться к Интернет будет невозможно.

Шаг 1 Обновите ПО (firmware), если требуется. (Пожалуйста, обращайтесь на web-сайт поддержки D-Link: <http://support.dlink.com> за последними обновлениями ПО.)

Шаг 2 Возьмите скрепку для бумаг и выполните аппаратный сброс. При включенном питании устройства нажмите на кнопку Reset на задней панели устройства на 10 секунд. Затем отпустите кнопку, маршрутизатор перезагрузится, индикаторы замигают и затем стабилизируются.

Шаг 3 После стабилизации состояния маршрутизатора, откройте браузер и введите 192.168.0.1 в адресной строке и нажмите **Enter**. Когда появится окно регистрации, введите **admin** в поле User Name, а поле Password **оставьте пустым**. Нажмите **OK**.

Если окно регистрации не появилось, повторите **Шаг 2**.

Примечание: Не запускайте мастер настройки.

Шаг 4 Выберите вкладку **WAN** на левой стороне экрана. Выберите **PPPoE**.

Шаг 5 Выберите **Dynamic PPPoE** (если ISP не предоставил статический IP-адрес).

Шаг 6 В поле Username введите **ELN/username@earthlink.net** и свой пароль, где username – это Ваше имя пользователя.

Пользователи SBC Global должны ввести **username@sbcglobal.net**.

Пользователи Ameritech должны ввести **username@ameritech.net**.

Пользователи BellSouth должны ввести **username@bellsouth.net**.

Пользователи Mindspring должны ввести **username@mindspring.com**.

Пользователи большинства других ISP должны ввести **username**.

Шаг 7 Значение параметра **Maximum Idle Time** должно быть равно 0. Установите значение **MTU** 1492, если ISP не указал иное значение, и установите опцию **Autoreconnect** в значение **Enabled**.

Примечание: Если постоянно возникают проблемы с доступом к определенным web-сайтам и/или email, пожалуйста, установите меньшее значение MTU, например, 1472, 1452 и т.д. Обратитесь к ISP за более подробной информацией и подходящим значением MTU.

Часто задаваемые вопросы (продолжение)

Как нужно настроить маршрутизатор на работу через Earthlink DSL или какое-либо подключение PPPoE? (продолжение)

Шаг 8 Нажмите **Apply**, а затем **Continue**. После обновления экрана отключите питание маршрутизатора D-Link.

Шаг 9 Выключите DSL-модем на 2-3 минуты. Затем включите. После того, как модем установит соединение с ISP, включите питание маршрутизатора. Подождите около 30 секунд и подключитесь к Web-интерфейсу управления маршрутизатора.

Шаг 10 Выберите вкладку **Status**, где показана информация об устройстве. Под заголовком **WAN** нажмите **Connect**. Затем нажмите **Continue**. Вы должны увидеть среди параметров назначенный публичный IP-адрес. Это означает, что устройство успешно подключилось к серверу и получило IP-адрес.

Можно ли использовать широкополосный маршрутизатор D-Link для организации совместного использования подключения к Интернет, предоставленного AOL DSL Plus?

В большинстве случаев можно. AOL DSL+ может использовать PPPoE для аутентификации, обходя клиентское ПО. В этом случае, маршрутизатор сможет работать с данным сервисом. Пожалуйста, обратитесь в AOL, если Вы не уверены.

Для настройки маршрутизатора:

Шаг 1 Подключитесь к web-интерфейсу управления (192.168.0.1) и настройте интерфейс WAN на использование PPPoE.

Шаг 2 Введите свое регистрационное имя, завершающееся строкой @aol.com. Введите пароль AOL в поле Password.

Шаг 3 Необходимо установить значение MTU 1400. AOL DSL не допускает значения MTU выше 1400.

Шаг 4 Примените новые параметры.

Шаг 5 Выключите питание модема на 1 минуту, а затем аналогично выключите питание маршрутизатора. Подождите 1 или 2 минуты, пока будет установлено подключение.

Если Вы подключаетесь к Интернет через другого провайдера услуг Интернет и хотите использовать ПО AOL, можно подключаться без изменения настроек межсетевого экрана. Необходимо настроить ПО AOL на подключение через стек TCP/IP.

Обращайтесь на <http://www.aol.com> за более подробной информацией о настройке ПО AOL.

Часто задаваемые вопросы (продолжение)

Как настроить маршрутизатор на работу с другим маршрутизатором DI-804HV?

Шаг 1 Подключитесь к Web-интерфейсу управления, введя IP-адрес (по умолчанию: 192.168.0.1) маршрутизатора в адресной строке браузера. По умолчанию имя пользователя (User Name) - **admin** (все буквы в нижнем регистре), пароль (Password) не задан (оставьте поле пустым).



Шаг 2 Нажмите кнопку VPN в колонке слева, выберите опцию Enable the VPN и затем в поле Max. number of tunnels введите максимально допустимое число создаваемых туннелей VPN.



Шаг 3 Далее в поле Tunnel Name введите имя туннеля с идентификатором ID, равным 1, выберите IKE и нажмите More.



Часто задаваемые вопросы (продолжение)

Как настроить маршрутизатор на работу с другим маршрутизатором DI-804HV? (продолжение)

Шаг 4 В поля Local Subnet и Local Netmask введите идентификатор локальной сети DI-804HV и соответствующую маску подсети.



Шаг 5 В поля Remote Subnet и Remote Netmask введите идентификатор удаленной сети DI-804HV и соответствующую маску подсети.



Шаг 6 В поле Remote Gateway введите IP-адрес интерфейса WAN удаленного маршрутизатора DI-804HV, а в поле Preshared Key введите ключ, который должен совпадать с ключом Preshared Key, указанным на удаленном DI-804HV.

Шаг 7 Нажмите Apply и затем нажмите Select IKE Proposal...



Часто задаваемые вопросы (продолжение)

Как настроить маршрутизатор на работу с другим маршрутизатором DI-804HV? (продолжение)

Шаг 8 Введите имя схемы IKE с ID, равным 1, и выберите Group 1, 2 или 5 из выпадающего меню DH Group.



Шаг 9 Выберите DES или 3DES в качестве алгоритма шифрования в поле Encryption Algorithm и или SHA-1, или MD5 в качестве алгоритма аутентификации в поле Authentication Algorithm.



Шаг 10 Введите время жизни схемы в поле Lifetime и затем выберите или Sec. (секунды), или KByte (КБайты) в качестве единицы измерения времени жизни.



Часто задаваемые вопросы (продолжение)

Как настроить маршрутизатор на работу с другим маршрутизатором DI-804HV? (продолжение)

Шаг 11 Выберите 1 из выпадающего меню Proposal ID и нажмите кнопку Add To. Только что настроенная схема IKE будет добавлена в индекс IKE Proposal Index. Нажмите Apply и затем Back.

Шаг 12 Нажмите Select IPsec Proposal...

Шаг 13 Введите имя для схемы с ID, равным 1, и выберите Group 1, 2, 5, или None из выпадающего меню DH Group.

Шаг 14 Выберите ESP или AH в качестве протокола инкапсуляции в поле Encapsulation Protocol.



Часто задаваемые вопросы (продолжение)

Как настроить маршрутизатор на работу с другим маршрутизатором DI-804HV? (продолжение)

Шаг 15 Выберите DES или 3DES в качестве алгоритма шифрования в поле Encryption Algorithm и или SHA-1, или MD5 в качестве алгоритма аутентификации в поле Authentication Algorithm.



Шаг 16 Введите время жизни схемы в поле Lifetime и затем выберите или Sec. (секунды), или KByte (КБайты) в качестве единицы измерения времени жизни.



Шаг 17 Выберите 1 из выпадающего меню Proposal ID и нажмите кнопку Add To. Только что настроенная схема IPsec будет добавлена в индекс IPsec Proposal Index. Нажмите Apply и затем Restart.



Часто задаваемые вопросы (продолжение)

Как настроить маршрутизатор на работу с другим маршрутизатором DI-804HV? (продолжение)

Шаг 18 Выполните те же действия для настройки другого маршрутизатора DI-804HV, используя те же самые параметры схем IKE и IPSec. Кроме того, обратите внимание, что на шаге 4 вводятся параметры локальной для DI-804HV сети, а на шаге 5 и 6 – удаленной относительно DI-804HV сети, поэтому при настройке другого маршрутизатора необходимо поменять местами параметры локальной и удаленной сети.

Шаг 19 Для установления соединения откройте командную строку и выполните ping-тест IP-адреса компьютера, находящегося в удаленной сети. Как только компьютер начал отвечать на ping-тест, туннель установлен.

Как настроить маршрутизатор на работу с маршрутизатором DI-804V?

Вначале необходимо настроить Ваш маршрутизатор DI-804HV.

Шаг 1 Подключитесь к Web-интерфейсу управления, введя IP-адрес (по умолчанию: 192.168.0.1) маршрутизатора в адресной строке браузера. По умолчанию имя пользователя (User Name) - **admin** (все буквы в нижнем регистре), пароль (Password) не задан (оставьте поле пустым).



Шаг 2 Нажмите кнопку VPN в колонке слева, выберите опцию Enable the VPN и затем в поле Max. number of tunnels введите максимально допустимое число создаваемых туннелей VPN.

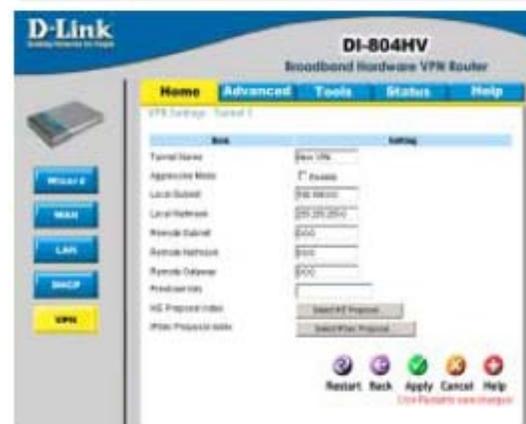
Часто задаваемые вопросы (продолжение)

Как настроить маршрутизатор на работу с маршрутизатором DI-804V? (продолжение)

Шаг 3 Далее в поле Tunnel Name введите имя туннеля с идентификатором ID, равным 1, выберите IKE и нажмите More.



Шаг 4 В поля Local Subnet и Local Netmask введите идентификатор локальной сети DI-804HV и соответствующую маску подсети.



Шаг 5 В поля Remote Subnet и Remote Netmask введите идентификатор удаленной сети DI-804HV (локальной сети DI-804V) и соответствующую маску подсети.



Часто задаваемые вопросы (продолжение)

Как настроить маршрутизатор на работу с маршрутизатором DI-804V? (продолжение)

Шаг 6 В поле Remote Gateway введите IP-адрес интерфейса WAN удаленного маршрутизатора DI-804V, а в поле Preshared Key введите ключ, который должен совпадать с ключом Preshared Key, указанным на удаленном DI-804V.



Шаг 7 Нажмите Apply и затем нажмите Select IKE Proposal...

Шаг 8 Введите имя схемы IKE с ID, равным 1, и выберите Group 2 из выпадающего меню DH Group.

Шаг 9 Выберите 3DES в качестве алгоритма шифрования в поле Encryption Algorithm и SHA-1 в качестве алгоритма аутентификации в поле Authentication Algorithm.

Шаг 10 Введите 28800 в качестве времени жизни схемы в поле Lifetime и затем выберите Sec. (секунды) в качестве единицы измерения времени жизни.



Часто задаваемые вопросы (продолжение)

Как настроить маршрутизатор на работу с маршрутизатором DI-804V? (продолжение)

Шаг 11 Выберите 1 из выпадающего меню Proposal ID и нажмите кнопку Add To. Только что настроенная схема IKE будет добавлена в индекс IKE Proposal Index. Нажмите Apply и затем Back.

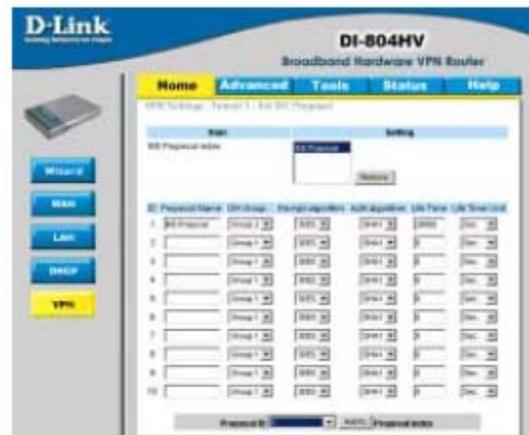
Шаг 12 Нажмите Select IPsec Proposal...

Шаг 13 Введите имя для схемы с ID, равным 1, и выберите None из выпадающего меню DH Group.

Шаг 14 Выберите ESP в качестве протокола инкапсуляции в поле Encapsulation Protocol.

Шаг 15 Выберите 3DES в качестве алгоритма шифрования в поле Encryption Algorithm и MD5 в качестве алгоритма аутентификации в поле Authentication Algorithm.

Шаг 16 Введите 3600 в качестве времени жизни схемы в поле Lifetime и затем выберите Sec. (секунды) в качестве единицы измерения времени жизни.



Часто задаваемые вопросы (продолжение)

Как настроить маршрутизатор на работу с маршрутизатором DI-804V? (продолжение)

Шаг 17 Выберите 1 из выпадающего меню Proposal ID и нажмите кнопку Add To. Только что настроенная схема IPSec будет добавлена в индекс IPSec Proposal Index. Нажмите Apply и затем Restart.



Далее необходимо настроить маршрутизатор DI-804V.

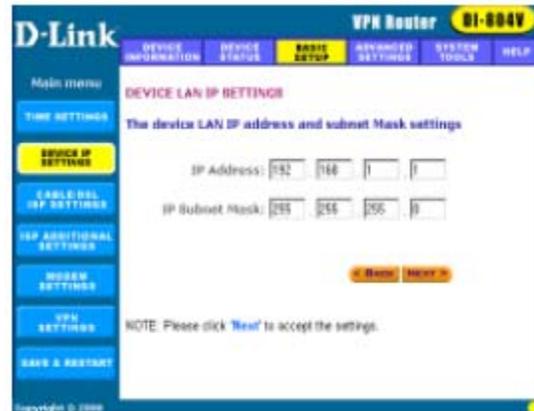
Шаг 1 Подключитесь к Web-интерфейсу управления, введя IP-адрес (по умолчанию: 192.168.0.1) маршрутизатора в адресной строке браузера. Зарегистрируйтесь, используя свой пароль. По умолчанию имя пользователя (User Name) - **admin** (все буквы в нижнем регистре), пароль (Password) не задан (оставьте поле пустым).

Шаг 2 Нажмите Basic Setup и затем выберите слева Device IP Settings.

Шаг 3 Измените IP-адрес LAN таким образом, чтобы локальные сети DI-804V и DI-804HV находились в разных подсетях.

Шаг 4 Нажимайте Next до тех пор, пока не появится страница Save & Restart. Нажмите Save & Restart и затем нажмите Basic Setup сразу после перезагрузки устройства.

Шаг 5 Нажмите VPN Settings.



Часто задаваемые вопросы (продолжение)

Как настроить маршрутизатор на работу с маршрутизатором DI-804V? (продолжение)

Шаг 6 Введите имя VPN-соединения и нажмите ADD.

Шаг 7 В поля Remote IP Network и Remote IP Netmask введите идентификатор сети и соответствующую маску подсети локальной сети DI-804HV.

Шаг 8 В поле Remote Gateway IP введите IP-адрес интерфейса WAN DI-804HV и убедитесь, что Network Interface установлен в значение WAN Ethernet.

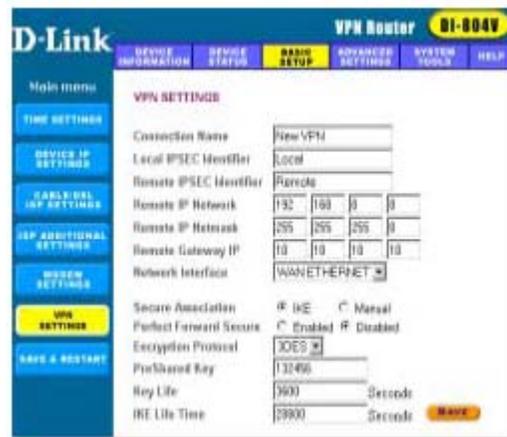


Шаг 9 Проверьте, установлен ли параметр Secure Association в значение IKE, а параметр Perfect Forward Secure в значение Disabled.

Шаг 10 Проверьте, установлен ли параметр Encryption Protocol в значение 3DES, и введите ключ Preshared Key.

Примечание: Ключ Preshared Key должен совпадать с аналогичным ключом, указанным на DI-804HV.

Шаг 11 Оставьте значения по умолчанию параметров Key Life и IKE Life Time и нажмите SAVE.



Шаг 12 Нажмите Next и затем нажмите Save & Restart.

SAVE & RESTART

Часто задаваемые вопросы (продолжение)

Как настроить маршрутизатор на работу с маршрутизатором DI-804V? (продолжение)

После настройки обоих маршрутизаторов необходимо установить соединение.

Шаг 1 Откройте командную строку на компьютере, находящемся во внутренней сети DI-804HV, и выполните ping-тест IP-адреса компьютера, находящегося во внутренней сети DI-804H, или наоборот.

Шаг 2 Как только компьютер начал отвечать на ping-тест, туннель установлен.

Шаг 3 Чтобы посмотреть статус VPN на DI-804V, нажмите Device Status.

Шаг 4 На странице Device Status нажмите VPN Status.

Шаг 5 Когда VPN-туннель установлен его статус будет отображаться как Active.

```
Dr:\>ipconfig
Windows 2000 IP Configuration
Ethernet adapter Local Area Connection 10:
    Connection-specific DNS Suffix  . : 
    IP Address . . . . . : 192.168.1.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Dr:\>ping 192.168.0.100

Pinging 192.168.0.100 with 32 bytes of data:
Reply from 192.168.0.100: bytes=32 time=18ms TTL=126
Reply from 192.168.0.100: bytes=32 time=13ms TTL=126
Reply from 192.168.0.100: bytes=32 time=14ms TTL=126
Reply from 192.168.0.100: bytes=32 time=14ms TTL=126

Ping statistics for 192.168.0.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 8ms, Maximum = 18ms, Average = 8ms
```



Как настроить маршрутизатор на работу с межсетевым экраном DFL-300?

Вначале необходимо настроить Ваш маршрутизатор DI-804HV.

Шаг 1 Подключитесь к Web-интерфейсу управления, введя IP-адрес (по умолчанию:192.168.0.1) маршрутизатора в адресной строке браузера. По умолчанию имя пользователя (User Name) - **admin** (все буквы в нижнем регистре), пароль (Password) не задан (оставьте поле пустым).

Шаг 2 Нажмите кнопку VPN в колонке слева, выберите опцию Enable the VPN и затем в поле Max. number of tunnels введите максимально допустимое число создаваемых туннелей VPN.

Часто задаваемые вопросы (продолжение)

Как настроить маршрутизатор на работу с межсетевым экраном DFL-300? (продолжение)

Шаг 3 Далее в поле Tunnel Name введите имя туннеля с идентификатором ID, равным 1, выберите IKE и нажмите More.



Шаг 4 В поля Local Subnet и Local Netmask введите идентификатор локальной сети DI-804HV и соответствующую маску подсети.



Шаг 5 В поля Remote Subnet и Remote Netmask введите идентификатор удаленной сети DI-804HV (локальной сети DFL-300) и соответствующую маску подсети.



Часто задаваемые вопросы (продолжение)

Как настроить маршрутизатор на работу с межсетевым экраном DFL-300? (продолжение)

Шаг 11 Выберите 1 из выпадающего меню Proposal ID и нажмите кнопку Add To. Только что настроенная схема IKE будет добавлена в индекс IKE Proposal Index. Нажмите Apply и затем Back.

Шаг 12 Нажмите Select IPsec Proposal...

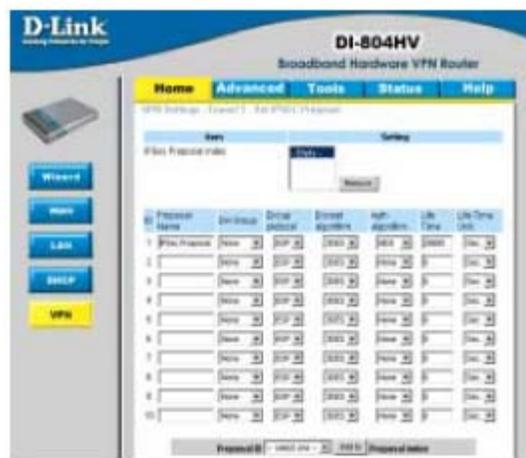
Шаг 13 Введите имя для схемы с ID, равным 1, и выберите None из выпадающего меню DH Group.



Шаг 14 Выберите ESP в качестве протокола инкапсуляции в поле Encapsulation Protocol.

Шаг 15 Выберите 3DES в качестве алгоритма шифрования в поле Encryption Algorithm и MD5 в качестве алгоритма аутентификации в поле Authentication Algorithm.

Шаг 16 Введите 28800 в качестве времени жизни схемы в поле Lifetime и затем выберите Sec. (секунды) в качестве единицы измерения времени жизни.



Часто задаваемые вопросы (продолжение)

Как настроить маршрутизатор на работу с межсетевым экраном DFL-300? (продолжение)

Шаг 4 Нажмите Policy и проверьте, настроены правила обработки исходящего трафика (Outgoing). Если не настроены, нажмите New Entry, примите значения по умолчанию и нажмите OK.



Шаг 5 Нажмите VPN и затем нажмите New Entry.

Шаг 6 Введите имя VPN-соединения без пробелов.

Шаг 7 Введите идентификатор сети и маску подсети внутренней сети.

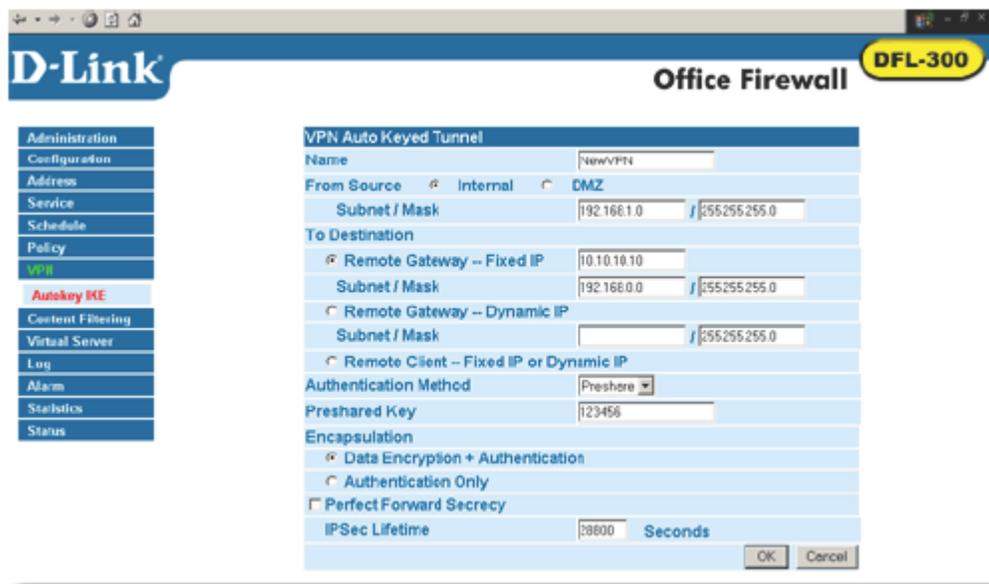
Шаг 8 В разделе To Destination выберите или Remote Gateway—Fixed IP или Remote Gateway—Dynamic IP. Введите IP-адрес интерфейса WAN DI-804HV, если выбрано Remote Gateway—Fixed IP.

Шаг 9 Введите идентификатор сети и соответствующую маску подсети локальной сети DI-804HV.

Шаг 10 Введите ключ Preshared Key. Ключ Preshared Key должен совпадать с аналогичным ключом, указанным на DI-804HV.

Шаг 11 Выберите Data Encryption + Authentication в разделе Encapsulation и нажмите OK.

Как настроить маршрутизатор на работу с межсетевым экраном DFL-300? (продолжение)



После настройки маршрутизатора и межсетевого экрана, необходимо установить соединение.

Шаг 1 Откройте командную строку на компьютере, находящемся во внутренней сети DFL-300, и выполните ping-тест IP-адреса компьютера, находящегося во внутренней сети DI-804HV, или наоборот.

```
D:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection 10:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.1.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

D:\>ping 192.168.0.100

Pinging 192.168.0.100 with 32 bytes of data:

Reply from 192.168.0.100: bytes=32 time<10ms TTL=126

Ping statistics for 192.168.0.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 2ms
```

Шаг 2 Как только компьютер начал отвечать на ping-тест, туннель установлен.

Часто задаваемые вопросы (продолжение)

Как открыть порты на маршрутизаторе?

Для разрешения входящего трафика в локальную сеть, необходимо открыть порты, иначе маршрутизатор будет блокировать запросы.

Шаг 1 Откройте web-браузер и введите IP-адрес маршрутизатора D-Link (192.168.0.1). Введите имя пользователя (admin) и пароль (по умолчанию не задан).

Шаг 2 Выберите вкладку **Advanced** и затем нажмите слева кнопку **Virtual Server**.

Шаг 3 Выберите **Enabled** для активации записи.

Шаг 4 Введите имя создаваемого виртуального сервера.

Шаг 5 В поле **Private IP** введите IP-адрес компьютера в локальной сети, на который будут перенаправляться запросы к виртуальному серверу.

Шаг 6 Выберите тип протокола в поле **Protocol Type** - TCP, UDP или оба. Если Вы не уверены, выберите оба.

Шаг 7 Введите номер частного порта в поле **Private Port** и номер публичного порта в поле **Public Port**. Частный и публичный номера портов обычно совпадают. Публичный порт – это порт, который виден со стороны WAN, а частный порт – это порт, используемый приложением на компьютере в локальной сети.

Шаг 8 Укажите расписание работы виртуального сервера в поле **Schedule**.

Шаг 9 Нажмите **Apply** и затем нажмите **Continue**.

Примечание: Убедитесь, что узел DMZ отключен. В противном случае, DMZ отключит все виртуальные серверы.

Поскольку наши маршрутизаторы используют NAT (Network Address Translation, трансляция сетевых адресов), то в один момент времени можно открыть определенный порт только для одного компьютера. Например: Если в локальной сети работают 2 web-сервера, нельзя открыть порт 80 для обоих компьютеров. Необходимо настроить один из web-серверов на порт 81. Таким образом, можно открыть порт 80 для первого компьютера и порт 81 для второго.



Часто задаваемые вопросы (продолжение)

Что такое DMZ?

Demilitarized Zone (незащищенная зона):

В компьютерных сетях зона DMZ (demilitarized zone, незащищенная зона) – это компьютер или небольшая сеть, находящаяся между частной сетью компании и внешней общедоступной сетью. Это не позволяет внешним пользователям получать доступ к серверам, которые хранят корпоративные данные. (Термин образовался от названия географической буферной зоны, созданной между Северной и Южной Кореей по эгидой ООН в начале 1950.) DMZ является дополнительной функцией и обеспечивает более надежную защиту при работе через межсетевой экран и работает так же эффективно, как и прокси-сервер.

В типичной конфигурации DMZ для небольшой компании отдельный компьютер (или узел в сетевых терминах) принимает запросы от пользователей частной сети на доступ к Web-сайтам или другим компаниям, доступным в публичной сети. Узел DMZ затем инициирует сессии для этих запросов в публичной сети. Однако, узел DMZ не имеет возможности инициировать сессию назад в частную сеть. Он может только передавать пакеты, которые уже были запрошены.

Пользователи публичной сети вне компании могут получать доступ только к узлу DMZ. Кроме того, DMZ обычно может содержать Web-страницы компании, поэтому их можно запрашивать из публичной сети. Однако, DMZ не обеспечивает доступ к остальным корпоративным данным. В случае если внешний пользователь прорвется сквозь защиту узла DMZ, Web-страницы могут быть повреждены, но другая информация не будет затронута. D-Link, лидирующий производитель маршрутизаторов, входит в число компаний, продающих настраиваемые на DMZ устройства.

Как настроить DMZ?

Функция DMZ позволяет перенаправлять все входящие порты на один компьютер в локальной сети. DMZ (Demilitarized Zone, незащищенная зона) позволит выбрать компьютер, который будет открыт для Интернет. DMZ полезно использовать, когда конкретное приложение или игра не работают через межсетевой экран. Компьютер, настроенный на работу в качестве узла DMZ будет полностью уязвим в Интернет, поэтому настоятельно рекомендуется попытаться открыть порты, настроив виртуальный сервер или параметры межсетевого экрана, прежде чем использовать DMZ.

Шаг 1 Определите IP-адрес компьютера, который должен будет работать как узел DMZ.

За информацией о том, как нас определить IP-адрес компьютера в ОС Windows XP/2000/ME/9x или Macintosh, пожалуйста, обращайтесь к Шагу 4 первого вопроса в данном разделе (Часто задаваемые вопросы).

Часто задаваемые вопросы (продолжение)

Как настроить DMZ? (продолжение)

Шаг 2 Подключитесь к Web-интерфейсу управления, введя IP-адрес (по умолчанию: 192.168.0.1) маршрутизатора в адресной строке браузера. Имя пользователя (User Name) - **admin** (все буквы в нижнем регистре), пароль (Password) не задан (оставьте поле пустым).



Шаг 3 Выберите вкладку **Advanced** и затем нажмите кнопку **DMZ**. Выберите **Enable** и введите IP-адрес компьютера, определенный на шаге 1.

Шаг 4 Нажмите **Apply** и затем **Continue** для сохранения изменений.

Примечание: Когда DMZ включен, параметры виртуального сервера все еще остаются в силе. Помните, что нельзя передавать пакеты, идущие на один и тот же порт, на множество IP-адресов, поэтому параметры виртуального сервера будут иметь приоритет над параметрами DMZ.



Часто задаваемые вопросы (продолжение)

Как открыть диапазон портов на DI-804HV, используя правила межсетевого экрана?

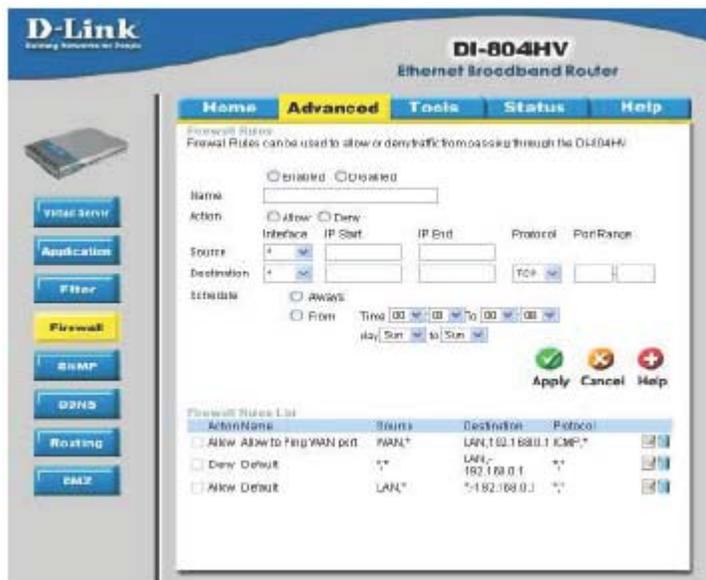
Шаг 1 Подключитесь к Web-интерфейсу управления маршрутизатора, введя его IP-адрес в web-браузере. По умолчанию его IP-адрес равен **192.168.0.1**. Для регистрации используйте свой пароль. По умолчанию имя пользователя **“admin”**, пароль не задан.

Если при получении доступа к web-интерфейсу управления возникли проблемы, пожалуйста, смотрите первый вопрос в данном разделе.

Шаг 2 На странице Home выберите вкладку **Advanced** и затем нажмите кнопку **Firewall**.

Шаг 3 Нажмите **Enabled** и введите имя нового правила.

Шаг 4 Выберите **WAN** в поле **Source** и введите диапазон IP-адресов из Интернет, к которым необходимо применить данное правило. Если Вы хотите позволить всем пользователям Интернет получать доступ к этим портам, введите «звездочку» (*) в первом поле и оставьте второе поле пустым.



Шаг 5 Выберите **LAN** в поле **Destination** и введите IP-адрес компьютера в локальной сети, к которому будет разрешен доступ по открытым портам. Нельзя указывать диапазон IP-адресов.

Шаг 6 Введите порт или диапазон портов, которые требуется открыть для входящего трафика.

Шаг 7 Нажмите **Apply** и затем нажмите **Continue**.

Примечание: Убедитесь, что узел DMZ отключен.

Поскольку наши маршрутизаторы используют NAT (Network Address Translation, трансляция сетевых адресов), то в один момент времени можно открыть определенный порт только для одного компьютера. Например: Если в локальной сети работают 2 web-сервера, нельзя открыть порт 80 для обоих компьютеров. Необходимо настроить один из web-серверов на порт 81. Таким образом, можно открыть порт 80 для первого компьютера и порт 81 для второго.

Часто задаваемые вопросы (продолжение)

Как использовать PC Anywhere с маршрутизатором DI-804HV?

Шаг 6 Создайте вторую запись, как показано здесь:

Шаг 7 Нажмите **Apply** и затем **Continue**.



Шаг 8 Создайте третью и последнюю запись, как показано здесь:



Шаг 9 Нажмите **Apply** и затем **Continue**.

Шаг 10 Запустите *PCAnywhere* с удаленного компьютера и используйте IP-адрес интерфейса WAN маршрутизатора, а не IP-адрес компьютера.

Часто задаваемые вопросы (продолжение)

Как использовать eDonkey за маршрутизатором D-Link?

Необходимо открыть порты на маршрутизаторе, что разрешить входящий трафик при использовании eDonkey. eDonkey использует три порта (4 при использовании CLI):

4661 (TCP) Для подключения к серверу

4662 (TCP) Для подключения к другим клиентам

4665 (UDP) Для взаимодействия с серверами, к которым Вы не подключены.

4663 (TCP) *Используется для клиента командной строки (CLI) при настройке на разрешение удаленных подключений. Это случай, когда используется графический интерфейс (такой как Java-интерфейс) с клиентом.

Шаг 1 Откройте web-браузер и введите IP-адрес маршрутизатора (192.168.0.1). Введите имя пользователя (admin) и пароль (оставьте пустым).

Шаг 2 Нажмите **Advanced** и затем нажмите **Firewall**.

Шаг 3 Создайте новое правило: Нажмите **Enabled**. Введите имя (edonkey). Нажмите **Allow**. Далее в поле Source выберите интерфейс **WAN**. В первом поле диапазона IP-адресов введите *. Оставьте второе поле пустым. В поле Destination выберите интерфейс **LAN**. Далее введите IP-адрес компьютера, на котором работает eDonkey. Оставьте второе поле диапазона IP-адресов пустым. Под заголовком Protocol выберите *. В полях Port range введите **4661** в первом поле и **4665** во втором поле. Нажмите **Always** или укажите расписание применения правила.

Шаг 4 Нажмите **Apply** и затем **Continue**.



Часто задаваемые вопросы (продолжение)

Как настроить маршрутизатор для работы SOCOM на Playstation 2?

Чтобы разрешить использование SOCOM и слушать аудио, необходимо загрузить последнюю версию ПО на маршрутизатор (если требуется), включить игровой режим (Game Mode) и открыть порт 6869 на IP-адрес Playstation.

Шаг 1 Обновите ПО (по приведенной ранее ссылке).

Шаг 2 Откройте web-браузер и введите IP-адрес маршрутизатора (192.168.0.1). Введите имя пользователя (admin) и пароль (оставьте пустым).

Шаг 3 Выберите вкладку **Advanced** и затем нажмите слева **Virtual Server**.

Шаг 4 Теперь необходимо создать новый виртуальный сервер. Нажмите **Enabled** и введите имя записи (socom). Введите IP-адрес Playstation в поле **Private IP**.

Шаг 5 В поле **Protocol Type** выберите Both. Введите **6869** и в поле **Private Port**, и в поле **Public Port**. Нажмите **Always**. Нажмите **Apply** для сохранения изменений и затем **Continue**



Шаг 6 Выберите вкладку **Tools** и слева затем **Misc**.

Шаг 7 Убедитесь, что включен режим **Gaming Mode**. Иначе, нажмите **Enabled**. Нажмите **Apply** и затем **Continue**.

Часто задаваемые вопросы (продолжение)

Как использовать Gamespy за маршрутизатором D-Link?

Шаг 1 Откройте web-браузер и введите IP-адрес маршрутизатора (192.168.0.1). Введите имя пользователя (admin) и пароль (оставьте пустым).

Шаг 2 Выберите вкладку **Advanced** и затем нажмите слева **Virtual Server**.

Шаг 3 Необходимо создать 2 записи.

Шаг 4 Нажмите Enabled и введите следующие значения:

NAME - Gamespy1

PRIVATE IP – IP-адрес компьютера, на котором работает Gamespy.

PROTOCOL TYPE - Both

PRIVATE PORT - 3783

PUBLIC PORT - 3783

SCHEDULE - Always.

Нажмите **Apply** и затем **Continue**.



Шаг 5 Создайте вторую запись:

Нажмите Enabled

NAME - Gamespy2

PRIVATE IP – IP-адрес компьютера, на котором работает Gamespy.

PROTOCOL TYPE - Both

PRIVATE PORT - 6500

PUBLIC PORT - 6500

SCHEDULE - Always.

Нажмите **Apply** и затем **Continue**.



Часто задаваемые вопросы (продолжение)

Как настроить маршрутизатор для работы KaZaA и Grokster?

Следующие шаги нужно выполнить для разрешения работы KaZaA, Grokster и других файлообменных сетей, использующих систему FastTrack P2P.

В большинстве случаев не требуется каким-либо образом настраивать маршрутизатор или ПО Kazaa. Если возникли проблемы, пожалуйста, выполните следующее:

Шаг 1 Откройте web-браузер и введите IP-адрес маршрутизатора (192.168.0.1). Введите имя пользователя (admin) и пароль (оставьте пустым).

Шаг 2 Введите имя пользователя (admin) и пароль (оставьте пустым).

Шаг 3 Выберите Advanced и затем нажмите Virtual Server.

Шаг 4 Нажмите Enabled и введите имя записи в поле Name (kazaa, например).

Шаг 5 Введите IP-адрес компьютера, на котором работает KaZaA, в поле Private IP. Выберите TCP в поле Protocol Type.

Шаг 6 Введите 1214 в полях Private Port и Public Port. Выберите Always под заголовком Schedule или укажите расписание применения правила. Нажмите Apply.



Убедитесь, что в ПО KaZaA не включено использование проски-сервера/межсетевого экрана.

Часто задаваемые вопросы (продолжение)

Как настроить маршрутизатор для игры в Warcraft 3?

Необходимо открыть порты на маршрутизаторе, чтобы разрешить входящий трафик при создании игрового сервера в Warcraft 3. Для простой игры не требуется настраивать маршрутизатор.

Warcraft 3 (Battlenet) использует порт 6112.

Для DI-804HV:

Шаг 1 Откройте web-браузер и введите IP-адрес маршрутизатора (192.168.0.1). Введите имя пользователя (admin) и пароль (оставьте пустым).

Шаг 2 Выберите вкладку **Advanced** и затем нажмите слева **Virtual Server**.

Шаг 3 Создайте новую запись: Нажмите **Enabled**. Введите имя записи (warcraft3). В поле Private IP введите IP-адрес компьютера, который будет работать в качестве игрового сервера. Выберите **Both** в поле Protocol Type. Введите **6112** и в поле Private Port, и в поле Public Port. Нажмите **Always** или укажите расписание применения правила.



Шаг 4 Нажмите **Apply** и затем **Continue**.

Примечание: Если необходимо, чтобы несколько компьютеров в локальной сети могли играть в одну и ту же игру, для которой создается игровой сервер, повторите приведенные выше шаги и введите IP-адреса других компьютеров. Нужно изменить порты. Компьютер 2 может использовать порт 6113, компьютер 3 – порт 6114 и так далее. Кроме того, нужно изменить порт в игре Warcraft3 на компьютере 2, компьютере 3 и так далее.

Настройте игровой порт на каждом компьютере:

Запустите Warcraft 3 на каждом компьютере, нажмите **Options > Gameplay**. Прокрутите страницу вниз до параметра **Game Port**. Введите номер порта, указанный ранее при настройке маршрутизатора.

Часто задаваемые вопросы (продолжение)

Как использовать Netmeeting за маршрутизатором D-Link?

В отличие от большинства приложений TCP/IP, NetMeeting использует **ДИНАМИЧЕСКИ ПОРТЫ** вместо **СТАТИЧЕСКИХ ПОРТОВ**. Это означает, что каждое новое соединение NetMeeting отличается от предыдущего. К примеру, HTTP web-сайт использует порт 80. NetMeeting может использовать любой из более чем 60,000 различных портов.

Все широкополосные маршрутизаторы, использующие (только) стандартный NAT и все программы совместного доступа в Интернет, такие как Microsoft ICS, которые используют (только) стандартный NAT, НЕ БУДУТ работать с NetMeeting или иными пакетами программ H.323.

Решением является перемещение маршрутизатора в зону DMZ.

Примечание: Некоторые производители аппаратного обеспечения фактически предоставляют совместимость с H.323. Это непростая задача, поскольку маршрутизатор должен проверять, не является ли каждый входящий пакет пакетом Netmeeting. Это намного большая работа, чем обычно выполняет маршрутизатор, и может в действительности стать **слабым местом межсетевое экрана**. D-Link не относится к таким производителям. За более подробной информацией обращайтесь на <http://www.HomenetHelp.com>.

Как настроить маршрутизатор для работы iChat? -для пользователей Macintosh-

iChat использует следующие порты: 5060 (UDP), 5190 (TCP), файлообменные 16384-16403 (UDP) для видеоконференций с другими пользователями.

Шаг 1 Откройте web-браузер и введите IP-адрес маршрутизатора (192.168.0.1). Введите имя пользователя (admin) и пароль (оставьте пустым).

Шаг 2 Выберите вкладку **Advanced** и затем нажмите **Firewall**.

Часто задаваемые вопросы (продолжение)

Как настроить маршрутизатор для работы iChat? -для пользователей Macintosh-

Шаг 3 Создайте новое правило:

Нажмите **Enabled**. Введите имя (ichat1). Нажмите **Allow**. Далее в поле Source под заголовком Interface выберите **WAN**. В первом поле диапазона IP-адресов введите *. Второе поле оставьте пустым. Далее в поле Destination под заголовком Interface выберите **LAN**. В первом поле диапазона IP-адресов введите IP-адрес компьютера, на котором работает iChat. Оставьте второе поле пустым. В поле Protocol выберите **UDP**. В полях Port range введите **5060** в первое поле и оставьте второе поле пустым. Выберите **Always** или укажите расписание применения правила.



Шаг 4 Нажмите **Apply** и затем **Continue**.

Шаг 5 Повторите шаги 3 и 4. Введите имя правила **ichat2** и откройте порты **16384-16403** (UDP).



Часто задаваемые вопросы (продолжение)

Как настроить маршрутизатор для работы iChat? -для пользователей Macintosh-

Для обмена файлами:

Шаг 1 Нажмите **Advanced** и затем **Virtual Server**.

Шаг 2 Выберите **Enabled** для активации записи.

Шаг 3 Введите имя виртуального сервера (ichat3).

Шаг 4 Далее в поле Private IP введите IP-адрес компьютера локальной сети, к которому нужно разрешить входящий трафик.

Шаг 5 Выберите **TCP** в поле Protocol Type.

Шаг 6 Введите **5190** в поля Private Port и Public Port.

Шаг 7 Нажмите **Always** или укажите расписание применения правила.

Шаг 8 Нажмите **Apply** и затем **Continue**.



При использовании встроенного в Mac OS X межсетевого экрана, необходимо временно отключить межсетевой экран на панели Sharing preference на обоих компьютерах.

При использовании встроенного в Mac OS X межсетевого экрана необходимо открыть те же самые порты, что открыты на маршрутизаторе:

Шаг 1 Выберите **Apple menu > System Preferences**.

Шаг 2 Выберите **View > Sharing**.

Шаг 3 Выберите вкладку **Firewall**.

Шаг 4 Нажмите **New**.

Шаг 5 Выберите **Other** из выпадающего меню.

Шаг 6 В полях Port Number, Range или Series введите: **5060, 16384-16403**.

Шаг 7 В поле Description введите: **iChat AV**

Шаг 8 Нажмите **OK**.

Часто задаваемые вопросы (продолжение)

Как отправить или принять файл через iChat, когда межсетевой экран MAC OS X включен? -для пользователей Macintosh- Mac OS X 10.2 или выше

Следующая информация взята из онлайн базы знаний Macintosh AppleCare:

iChat не может отправить или принять файл, когда межсетевой экран Mac OS X работает в установленном по умолчанию режиме. Если открыть порт AIM, появится возможность принимать файлы, но отправлять. По умолчанию межсетевой экран Mac OS X блокирует передачу файлов через iChat или ПО America Online AIM. Если или отправитель, или получатель включит межсетевой экран Mac OS X, передача может быть заблокирована.

Простейший способ обойти эту проблему – временно отключить межсетевой экран на панели Sharing preference на обоих компьютерах. Это требуется для отправителя. Однако, получатель может оставить межсетевой экран включенным, если порт AIM открыт. Чтобы открыть порт AIM:

Шаг 1 Выберите **Apple menu > System Preferences**.

Шаг 2 Выберите **View > Sharing**.

Шаг 3 Выберите вкладку **Firewall**.

Шаг 4 Нажмите **New**.

Шаг 5 Выберите AOL IM из выпадающего меню Port Name. В поле должен появиться номер порта 5190.

Шаг 6 Нажмите **OK**.

Если Вы не хотите отключать межсетевой экран на отправителе, можно использовать другую файлообменную систему вместо iChat. Типы файлообменных систем для Mac OS X описаны в техническом документе 106461, "Mac OS X: File Sharing" в онлайн базе знаний AppleCare.

Примечание: Если Вы используете файлообменный сервис, когда межсетевой экран включен, не забудьте выбрать вкладку Firewall и выберите нужный сервис в списке "Allow". В противном случае межсетевой экран будет блокировать файлообменный сервис."

Часто задаваемые вопросы (продолжение)

Что такое NAT?

NAT расшифровывается как **Network Address Translator (Трансляция сетевых адресов)**. NAT описан в стандарте RFC-1631 и используется для решения проблемы нехватки IP-адресов. В основном, каждое устройство NAT содержит таблицу, состоящую из пар локальных IP-адресов и глобальных уникальных адресов, по которым устройство может «транслировать» локальные IP-адреса на глобальные и наоборот. Иными словами, этот метод позволяет подключить несколько компьютеров к Интернет (или любой другой сети IP), используя один IP-адрес.

Широкополосные маршрутизаторы D-Link (например: DI-604) поддерживают NAT. При правильной настройке множество пользователей может получить доступ в Интернет через устройство NAT, используя единственное подключение к Интернет.

Более подробную информацию смотрите в RFC-1631: The IP Network Address Translator (NAT), по адресу <http://www.faqs.org/rfcs/rfc1631.html>

Обращение в службу технической поддержки

Вы можете найти последнюю версию программного обеспечения и документацию по продуктам на сайте D-Link.

D-Link обеспечивает бесплатную техническую поддержку клиентов в течение гарантийного срока изделия. Клиенты могут связаться со службой технической поддержки D-Link через наш web-сайт или по телефону.

Телефоны службы технической поддержки D-Link:

+7 (095) 744 00 99

Техническая поддержка D-Link через Интернет:

support@dlink.ru

При обращении в службу технической поддержки, пожалуйста, предоставьте следующую информацию:

- Номер модели или имя продукта
- Серийный номер устройства
- Тип программного обеспечения и номер версии