Instant Broadband® Series

EtherFast® Cable/DSL Firewall Router with 4-Port Switch/VPN Endpoint

Use this guide to install:

BEFSX41

User Guide

LINKSYS®

COPYRIGHT & TRADEMARKS

Copyright © 2003 Linksys, All Rights Reserved. Linksys, EtherFast, and Instant Broadband are registered trademarks of Linksys. Microsoft, Windows, and the Windows logo are registered trademarks of Microsoft Corporation. All other trademarks and brand names are the property of their respective proprietors.

FCC STATEMENT

The Instant Broadband EtherFast Cable/DSL Firewall Router with 4-Port Switch/VPN Endpoint has been tested and complies with the specifications for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used according to the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which is found by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment or devices
- Connect the equipment to an outlet other than the receiver's
- Consult a dealer or an experienced radio/TV technician for assistance

EC Declaration of Conformity (Europe)

In compliance with the EMC Directive 89/336/EEC, Low Voltage Directive 73/23/EEC, and Amendment Directive 93/68/EEC, this product meets the requirements of the following standards:

- EN55022 Emission
- EN55024 Immunity

For product support and product registration, contact us at the addresses below:

E-mail	europe-support@linksys.com latan-soporte@linksys.com
Web	http://www.linksys.com/international

Table of Contents

Chapter 1: Introduction 1
The Linksys EtherFast Cable/DSL Firewall Router with 4-Port Switch/VPN Endpoint 1
Features 1
An Introduction to LANs and WANs 2
IP Addresses 2
Network Setup Overview 4

Chapter 2: Your Virtual Private Network (VPN) 5
Why Do I Need a VPN? 5
What is a Virtual Private Network? 6

Chapter 3: Getting to Know the EtherFast Cable/DSL Firewall Router 9
The Router’s Back Panel 9
The Router’s Front Panel LEDs 10

Chapter 4: Connect the Router 11
Overview 11
Connecting Your Hardware Together and Booting Up 11

Chapter 5: Configure the PCs 14
Overview 14
Configuring Windows 95, 98, and Millennium PCs 15
Configuring Windows 2000 PCs 17
Configuring Windows XP PCs 19

Chapter 6: Configure the Router 21

Chapter 7: The Cable/DSL Firewall Router’s Web-based Utility 27
Overview 27
Quick and Easy Router Administration 27
Setup 28
Firewall 35
VPN 38
Password 51
Status 53
DHCP 55
Log 57
Help 59
Advanced 60
Filters 61
Forwarding 65
Dynamic Routing 70
Static Routing 71
DMZ Host 73
MAC Address Clone 75

Appendix A: Troubleshooting 76
Common Problems and Solutions 76
Frequently Asked Questions 89

Appendix B: Maximizing VPN Security 93

Appendix C: Configuring IPSec between a Windows 2000 or XP PC and the Firewall Router 95
Introduction 95
Environment 95
Step One: Create an IPSec Policy 96
Step Two: Build Filter Lists 97
Step Three: Configure Individual Tunnel Rules 102
Step Four: Assign New IPSec Policy 110
Step Five: Create a Tunnel Through the Web-based Utility 111

Appendix D: SNMP Functions 113

Appendix E: How to Ping Your ISP's E-mail & Web Addresses 114

Appendix F: Installing the TCP/IP Protocol 117

Appendix G: Finding the MAC Address and IP Address for Your Ethernet Adapter 119

Appendix H: Glossary 123

Appendix I: Specifications 135

Environmental 135

Appendix J: Warranty Information 136

Appendix K: Contact Information 137

Chapter 1: Introduction

The Linksys EtherFast Cable/DSL Firewall Router with 4-Port Switch/VPN Endpoint

The Linksys Instant Broadband™ EtherFast® Cable/DSL Firewall Router with 4-Port Switch/VPN Endpoint is the perfect solution for connecting a small group of PCs to a high-speed broadband Internet connection or a 10/100 Ethernet backbone. The Router can be configured to limit internal users' Internet access based on URLs and/or time periods—URL filtering and time filtering. For enhanced protection against intruders from the Internet, the Router features an advanced Stateful Packet Inspection firewall.

Use the Cable/DSL Firewall Router with 4-Port Switch/VPN Endpoint to create up to two IPSec VPN tunnels, so you can securely connect to the corporate server from your home office—or any location when you're on the road. The Router provides a dedicated port for DMZ hosting and acts as the only externally recognized Internet gateway on your local area network (LAN). With the performance and security features of the Cable/DSL Firewall Router with 4-Port Switch/VPN Endpoint, your network will take advantage of the Internet while keeping its data secure.

Features

- Supports Universal Plug-and-Play
- Protects PCs from Ping of Death, SYN Flood, Land Attacks, IP Spoofing, and Other DoS (Denial of Service) Attacks
- Supports Up to Two IPSec Virtual Private Network (VPN) Tunnels
- Supports URL Filtering and Time Filtering
- Blocks Proxy, Java, ActiveX, and Cookies
- Easily Configurable through a Web Browser from Any Networked PC
- Supports IPSec and PPTP Pass-Through
- Administer and Upgrade Your Router Remotely over the Internet
- Supports Traffic and Event Logging
- Configurable as a DHCP Server on Your Network
- Administers Can Block Specific Internal Users' Internet Access with Filtering
- Supports SNMP ver. 2.0 and SNMP MIB I and II
- Supports NTP (Network Time Protocol) for Synchronization with Real-Time Server
- Support for PPPoE Connection
- Dedicated Port for DMZ

An Introduction to LANs and WANs

Simply put, a **router** is a network device that connects two networks together.

In this instance, the Router connects your **Local Area Network (LAN)**, or the group of PCs in your home or office, to the **Wide Area Network (WAN)**, that is, the Internet. The Router processes and regulates the data that travels between these two networks.

Think of the Router as a network device with two sides: the first side is made up of your private **Local Area Network (LAN)** of PCs. The other, public side is the Internet, or the **Wide Area Network (WAN)**, outside of your home or office.

The Router's firewall (NAT) protects your network of PCs so users on the public, Internet side cannot "see" your PCs. This is how your LAN, or network, remains private. The Router protects your network by inspecting the first packet coming in through the WAN port before delivery to the final destination on the LAN port. The Router inspects Internet port services like the web server, ftp server, or other Internet applications, and, if allowed, it will forward the packet to the appropriate PC on the LAN side.

Remember that the Router's ports connect to two sides: your 10/100 **LAN** ports and the Internet **WAN** port. The WAN and LAN ports transmit data at 10 Mbps or 100 Mbps.

IP Addresses

What's an IP Address?

IP stands for Internet Protocol. Every device on an IP-based network, including PCs, print servers, and routers, requires an **IP address** to identify its "location," or address, on the network. This applies to both the WAN and LAN connections. There are two ways of assigning an IP address to your network devices.

Static IP Addresses

A **static IP address** is a fixed IP address that you assign manually to a PC or other device on the network. Since a static IP address remains valid until you disable it, **static IP addressing** ensures that the device assigned it will always have that same IP address until you change it. Static IP addresses are commonly used with network devices such as server PCs or print servers.

If you use the Router to share your cable or DSL Internet connection, contact your ISP to find out if they have assigned a static IP address to your account. If so, you will need that static IP address when configuring the Router. You can get the information from your ISP.

Note: Since the Router is a device that connects two networks, it needs two IP addresses—one for the LAN side, and one for the WAN side. In this User Guide, you'll see references to the "WAN IP address" and the "LAN IP address."

Since the Router has firewall security, the only IP address that can be seen from the Internet for your network is the Router's WAN IP address.

However, even this WAN IP address for the Router can be blocked, so that the Router and network seem invisible to the Internet—see the Blocking WAN Requests description under Filters in "Chapter 7: The Cable/DSL Firewall Router's Web-based Utility."

Dynamic IP Addresses

A **dynamic IP address** is automatically assigned to a device on the network, such as PCs and print servers. These IP addresses are called "dynamic" because they are only *temporarily* assigned to the PC or device. After a certain time period, they expire and may change. If a PC logs onto the network (or the Internet) and its dynamic IP address has expired, the **DHCP server** will assign it a new dynamic IP address.

For DSL users, many ISPs may require you to log on with a user name and password to gain access to the Internet. This is a dedicated, high-speed connection type called Point to Point Protocol over Ethernet (PPPoE). PPPoE is similar to a dial-up connection, but PPPoE does not dial a phone number when establishing a connection. PPPoE also will provide the Router with a dynamic IP address to establish a connection to the Internet.

DHCP (Dynamic Host Configuration Protocol) Servers

PCs and other network devices using dynamic IP addressing are assigned a new IP address by a **DHCP server**. The PC or network device obtaining an IP address is called the DHCP client. DHCP frees you from having to assign IP addresses manually every time a new user is added to your network.

A DHCP server can either be a designated PC on the network or another network device, such as the Router. By default, the Router's WAN setting is DHCP client.

By default, a DHCP server (LAN side) is enabled on the Router. If you already have a DHCP server running on your network, you *must* disable one of the two DHCP servers. If you run more than one DHCP server on your network, you will experience network errors, such as conflicting IP addresses. To disable DHCP on the Router, see the DHCP section in "Chapter 7: The Cable/DSL Firewall Router's Web-based Utility."

> **Note:** Even if you assign a static IP address to a PC, other PCs can still use DHCP's dynamic IP addressing, as long as the static IP address is not within the DHCP range of the LAN IP Address.
>
> If the dynamic IP addressing fails to provide a dynamic IP address, refer to "Appendix A: Troubleshooting."

Network Setup Overview

This user guide covers the basic steps for setting up a network with a router. After going through "Chapter 3: Getting to Know the EtherFast Cable/DSL Firewall Router," most users will only need to use the following chapters:

- Chapter 4: Connect the Router
  This chapter instructs you on how to connect the cable or DSL modem to the Router and connect the PC(s) to the Router.

- Chapter 5: Configure the PCs
  This chapter instructs you on how to configure your PC(s) for a DHCP connection, if the network settings are not already set to DHCP.

- Chapter 6: Configure the Router
  This chapter explains how to configure the Router using your web browser and the Router's web-based utility. You will configure the Router using the settings provided by your ISP.

When you're finished with the basic steps, then you are ready to connect to the Internet. After the PC(s) can access the Internet through the Router, you can alter the Router's settings further; for example, you can adjust security features and other settings to enable online gaming.

Chapter 2: Your Virtual Private Network (VPN)

Why Do I Need a VPN?

Computer networking provides a flexibility not available when using an archaic, paper-based system. With this flexibility, however, comes an increased risk in security. This is why firewalls were first introduced. Firewalls help to protect data inside of a local network. But what do you do once information is sent outside of your local network, when emails are sent to their destination, or when you have to connect to your company's network when you are out on the road? How is your data protected?

That is when a VPN can help. VPNs are called Virtual Private Networks because they secure data moving outside of your network as if it were still within that network.

When data is sent out across the Internet from your computer, it is always open to attacks. You may already have a firewall, which will help protect data moving around or held within your network from being corrupted or intercepted by entities outside of your network, but once data moves outside of your network - when you send data to someone via email or communicate with an individual over the Internet - the firewall will no longer protect that data.

At this point, your data becomes open to hackers using a variety of methods to steal not only the data you are transmitting but also your network login and security data. Some of the most common methods are as follows:

1) MAC Address Spoofing

Packets transmitted over a network, either your local network or the Internet, are preceded by a packet header. These packet headers contain both the source and destination information for that packet to transmit efficiently. A hacker can use this information to spoof (or fake) a MAC address allowed on the network. With this spoofed MAC address, the hacker can also intercept information meant for another user.

2) Data Sniffing

Data "sniffing" is a method used by hackers to obtain network data as it travels through unsecured networks, such as the Internet. Tools for just this kind of activity, such as protocol analyzers and network diagnostic tools, are often built into operating systems and allow the data to be viewed in clear text.

3) Man in the middle attacks

Once the hacker has either sniffed or spoofed enough information, he can now perform a "man in the middle" attack. This attack is performed, when data is being transmitted from one network to another, by rerouting the data to a new destination. Even though the data is not received by its intended recipient, it appears that way to the person sending the data.

These are only a few of the methods hackers use and they are always developing more. Without the security of your VPN, your data is constantly open to such attacks as it travels over the Internet. Data travelling over the Internet will often pass through many different servers around the world before reaching its final destination. That's a long way to go for unsecured data and this is when a VPN serves its purpose.

What is a Virtual Private Network?

A VPN, or Virtual Private Network, is a connection between two endpoints - a VPN Router, for instance - in different networks that allows private data to be sent securely over a shared or public network, such as the Internet. This establishes a private network that can send data securely between these two locations or networks.

This is done by creating a "tunnel". A VPN tunnel connects the two PCs or networks and allows data to be transmitted over the Internet as if it were still within those networks. Not a literal tunnel, it is a connection secured by encrypting the data sent between the two networks.

VPN was created as a cost-effective alternative to using a private, dedicated, leased line for a private network. Using industry standard encryption and authentication techniques - IPSec, short for IP Security - the VPN creates a secure connection that, in effect, operates as if you were directly connected to your local network. Virtual Private Networking can be used to create secure networks linking a central office with branch offices, telecommuters, and/or professionals on the road (travelers can connect to a VPN Router using any computer with VPN client software that supports IPSec, such as SSH Sentinel.)

There are two basic ways to create a VPN connection:

- Firewall Router to Firewall Router
- Computer (using VPN client software that supports IPSec) to Firewall Router

The Firewall Router creates a “tunnel” or channel between two endpoints, so that data transmissions between them are secure. A computer with VPN client software that supports IPSec can be one of the two endpoints. Any computer with the built-in IPSec Security Manager (Microsoft 2000 and XP) allows the Firewall Router to create a VPN tunnel using IPSec (refer to “Appendix C: Configuring IPSec between a Microsoft Windows 2000 or XP PC and the Firewall Router”). Other versions of Microsoft operating systems require additional, third-party VPN client software applications that support IPSec to be installed.

Firewall Router to Firewall Router

An example of a Firewall Router-to- Firewall Router VPN would be as follows. (See Figure 2-1.) At home, a telecommuter uses his Firewall Router for his always-on Internet connection. His router is configured with his office's VPN settings. When he connects to his office's router, the two routers create a VPN tunnel, encrypting and decrypting data. As VPNs utilize the Internet, distance is not a factor. Using the VPN, the telecommuter now has a secure connection to the central office's network, as if he were physically connected.

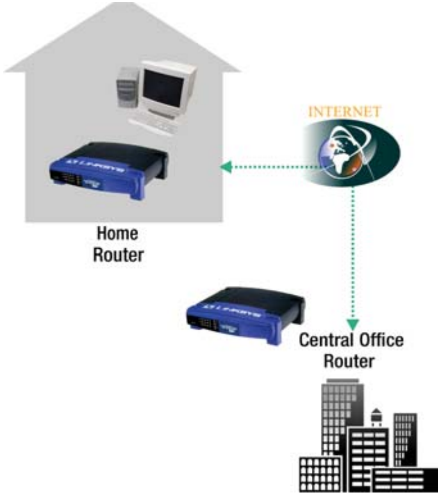


Figure 2-1

Important: You must have at least one Firewall Router on one end of the VPN tunnel. At the other end of the VPN tunnel, you must have a second Firewall Router or a computer with VPN client software that supports IPSec.

Computer (using VPN client software that supports IPSec) to Firewall Router

The following is an example of a computer-to-Firewall Router VPN. (See Figure 2-2.) In her hotel room, a traveling businesswoman dials up her ISP. Her notebook computer has VPN client software that is configured with her office's VPN settings. She accesses the VPN client software that supports IPSec and connects to the Firewall Router at the central office. As VPNs utilize the Internet, distance is not a factor. Using the VPN, the businesswoman now has a secure connection to the central office's network, as if she were physically connected.

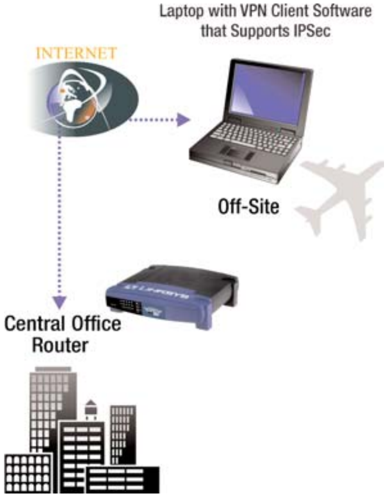


Figure 2-2

For additional information and instructions about creating your own VPN, please visit Linksys's website at *www.linksys.com* or refer to “Appendix C: Configuring IPSec between a Microsoft Windows 2000 or XP PC and the Firewall Router.”

Chapter 3: Getting to Know the EtherFast Cable/DSL Firewall Router

The Router’s Back Panel

The Router’s ports, shown in Figure 3-1, are where network cables are connected

WAN The **WAN** (Wide Area Network) port is where you connect your cable or DSL modem through an Ethernet cable. **Your modem connection will not work from any other port.**

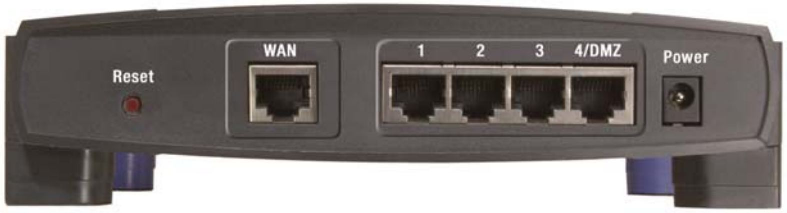


Figure 3-1

Ports 1-3 These three LAN (Local Area Network) ports are where you will connect networked devices, such as PCs, print servers, switches, and anything else you want to put on your network. (These ports auto-detect crossover and straight-through cables.)

Port 4/DMZ **Port 4/DMZ** operates like a regular LAN port to connect with network devices, unless DMZ is enabled through the Cable/DSL Firewall Router’s web-based utility. Once DMZ is enabled, this port will be accessible with NO PROTECTION from the firewall. Be sure to disable the DMZ function through the web-based utility if you want this port shielded by the Cable/DSL Firewall Router’s firewall. (This port auto-detects crossover and straight-through cables.)

Power The **Power** port is where you will connect the power adapter.

The Reset Button*

Briefly pressing the Reset Button will refresh the Cable/DSL Firewall Router's connections, potentially clearing any jammed links.

Pressing the Reset Button and holding it in for a few seconds will clear all of the Cable/DSL Firewall Router's data. This should be done only if you are experiencing heavy routing problems, and only after you have exhausted all of the other troubleshooting options. By resetting the Cable/DSL Firewall Router, you run the risk of creating conflicts between your PCs' actual IP Addresses and what the Cable/DSL Firewall Router thinks their IP Addresses should be. You may be forced to reboot the entire system(s).

If the Cable/DSL Firewall Router locks up, simply power it down for three to five seconds by removing the power cable from the Cable/DSL Firewall Router's Power Port. Leaving the power off for too long could result in the loss of network connections.

The Router's Front Panel LEDs

The Router's LEDs, shown in Figure 3-2, provide a graphic display of activity.

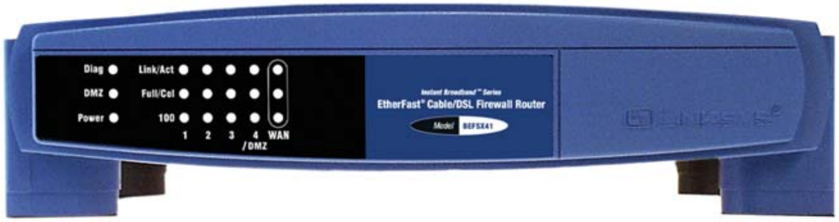

Diag
DMZ
Power
Link/Act
Full/Col
100
1
2
3
4
/DMZ
WAN
Instant Broadband™ Series
EtherFast® Cable/DSL Firewall Router
Model BEFSX41

Figure 3-2

Diag *Red*. The **Diag** LED lights up when the Router goes through its self-diagnosis mode during every boot-up. It will turn off upon successful completion of the diagnosis.

If this LED stays on for an abnormally long period of time, see "Appendix A: Troubleshooting."

DMZ *Green*. The DMZ LED lights up when the Cable/DSL Firewall Router's DMZ function is enabled. Enabling this function will remove firewall protection from Port 4/DMZ.

Power *Green*. The **Power** LED lights up when the Router is powered on.

WAN and LAN LEDs

Link/Act *Green*. The **Link/Act** LED serves two purposes. If the LED is continuously lit, the Router is successfully connected to a device through the corresponding port (1, 2, 3 or 4/DMZ). If the LED is flickering, the Router is actively sending or receiving data over that port.

Full/Col *Green*. The **Full/Col** LED also serves two purposes. If this LED is lit up continuously, the connection made through the corresponding port is running in Full Duplex mode. If the LED flickers, the connection is experiencing collisions. Infrequent collisions are normal.

If this LED flickers too often, there may be a problem with your connection. See "Appendix A: Troubleshooting" if you encounter this problem.

100 *Orange*. The **100** LED lights up when a successful 100Mbps connection is made through the corresponding port.

If this LED does not light up, then your connection speed is 10 Mbps.

Proceed to "Chapter 4: Connect the Router."

Chapter 4: Connect the Router

Overview

Unlike a hub or a switch, the Router's setup consists of more than simply plugging hardware together. You will have to configure your networked PCs to accept the IP addresses that the Router assigns them (if applicable), and you will also have to configure the Router with setting(s) provided by your Internet Service Provider (ISP).

The installation technician from your ISP should have left the setup information with you after installing your broadband connection. If not, you can call your ISP to request the data.

Once you have the setup information you need for your specific type of Internet connection, you can begin installation and setup of the Router.

The diagram in Figure 4-1 shows a typical configuration.

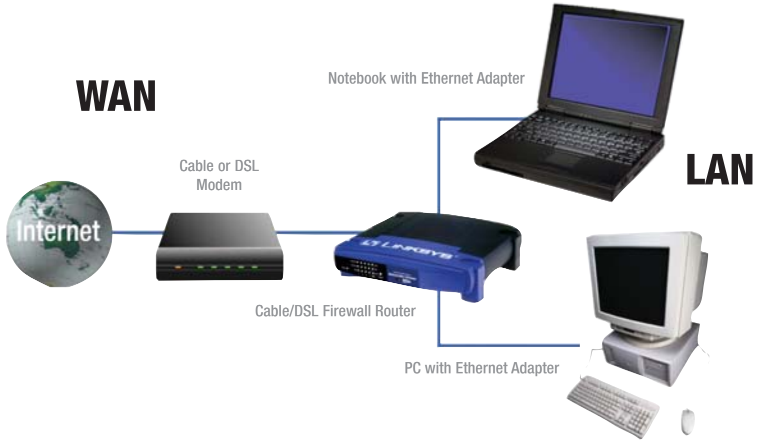


Figure 4-1

Connecting Your Hardware Together and Booting Up

1. Before you begin, make sure that all of your hardware is powered off, including the Router, PCs, hubs, switches, and cable or DSL modem.

2. Connect one end of an Ethernet cable to one of the LAN ports (labeled **1**, **2**, **3**, or **4/DMZ**) on the back of the Router, and the other end to a standard port on a network device, e.g., a PC, print server, hub, or switch (see Figure 4-2).

Repeat the above step to connect more PCs or network devices to the Router.

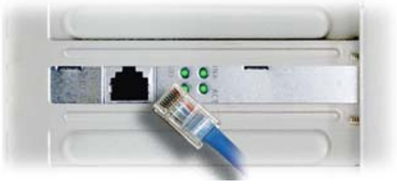


Figure 4-2

3. Connect the Ethernet cable from your cable or DSL modem to the **WAN** port on the Router's back panel, as shown in Figure 4-3. This is the only port that will work for your modem connection.

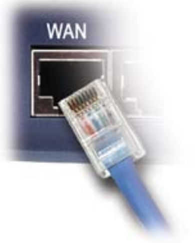


Figure 4-3

4. As shown in Figure 4-4, connect the power adapter to the Power port on the back panel of the Router, and then plug the power adapter into a power outlet.

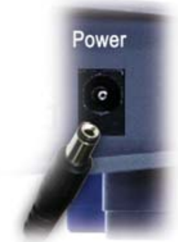


Figure 4-4

- The **Power** LED on the front panel will light up green as soon as the power adapter is connected properly. (The LEDs are shown in Figure 4-5.)

- The **Diag** LED will light up red for a few seconds when the Router goes through its self-diagnostic test. This LED will turn off when the self-test is complete.

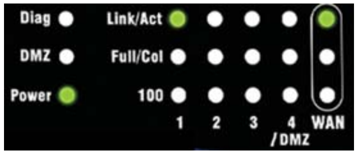


Figure 4-5

5. Turn on the cable or DSL modem and PCs.

The Router's hardware installation is now complete.

Chapter 5: Configure the PCs

Overview

The instructions in this chapter will help you configure each of your computers to be able to communicate with the Router.

To do this, you need to configure your PC's network settings to obtain an IP (or TCP/IP) address automatically (called DHCP). Computers use IP addresses to communicate with each other across a network or the Internet.

Find out which operating system your computer is running, such as Windows 95, 98, Millennium, NT 4.0, 2000, or XP. You will need to know which operating system your computer is running. You can find out by clicking the **Start** button and then going to the **Settings** option. Then click **Control Panel**, and then double-click the **System** icon. If your Start menu doesn't have a Settings option, you're running Windows XP. Click the **Cancel** button when done.

You may need to do this for each computer you are connecting to the Router.

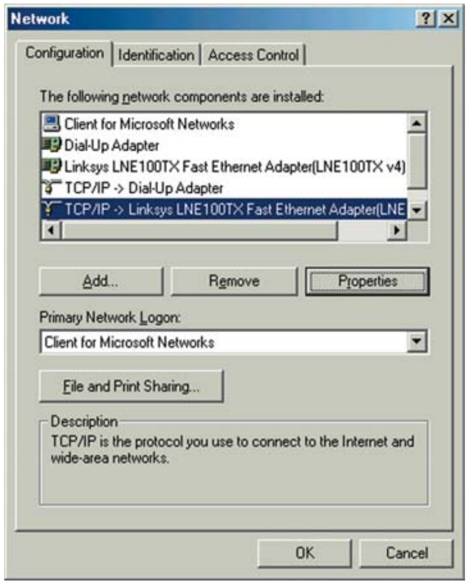
Important: These instructions apply only to Windows 95, Windows 98, Windows Millennium, Windows 2000, or Windows XP machines. For TCP/IP setup under Windows NT, see your Windows manual. By default Windows 98, 2000, Me, and XP has TCP/IP installed and set to obtain an IP address automatically.

The next few pages tell you, step by step, how to configure your network settings based on the type of Windows operating system you are using. Make sure that an Ethernet card or adapter has been successfully installed in each PC you will configure. Once you've configured your computers, continue to "Chapter 6: Configure the Router."

Configuring Windows 95, 98, and Millennium PCs

1. Go to the Network screen by clicking the **Start** button. Click **Settings** and then **Control Panel**. From there, double-click the **Network** icon.

2. On the Configuration tab, shown in Figure 5-1, select the **TCP/IP line** for the applicable Ethernet adapter. Do not choose a TCP/IP entry whose name mentions DUN, PPPoE, VPN, or AOL. If the word **TCP/IP** appears by itself, select that line. (If there is no TCP/IP line listed, refer to "Appendix F: Installing the TCP/IP Protocol" or your Ethernet adapter's user guide to install TCP/IP now.) Click the **Properties** button.



The following network components are installed:

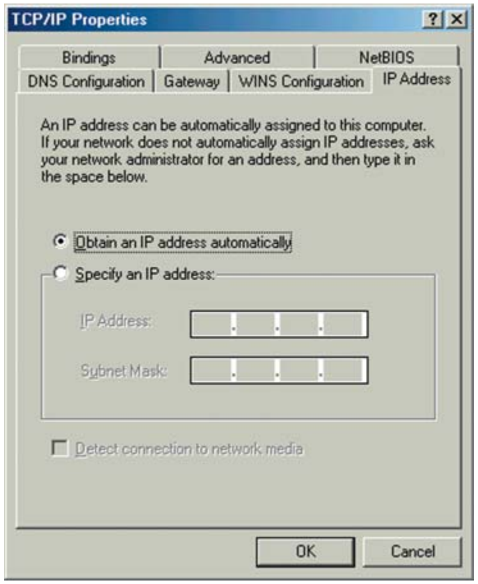
Client for Microsoft Networks
Dial-Up Adapter
Linksys LNE100TX Fast Ethernet Adapter(LNE100TX v4)
TCP/IP -> Dial-Up Adapter
TCP/IP -> Linksys LNE100TX Fast Ethernet Adapter(LNE

Primary Network Logon:
Client for Microsoft Networks

Description
TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

Figure 5-1

3. Click the **IP Address** tab and select **Obtain an IP address automatically**, as shown in Figure 5-2.



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

○ Specify an IP address:

IP Address: . . .

Subnet Mask: . . .

□ Detect connection to network media

Figure 5-2

4. Now click the **Gateway** tab to ensure that the Installed Gateway field is left blank. Click the **OK** button.

5. Click the **OK** button again. Windows may ask you for the original Windows installation disk or additional files. Supply them by pointing to the correct file location, e.g., D:\win98, D:\win9x, c:\windows\options\cabs, etc. (if "D" is the letter of your CD-ROM drive).

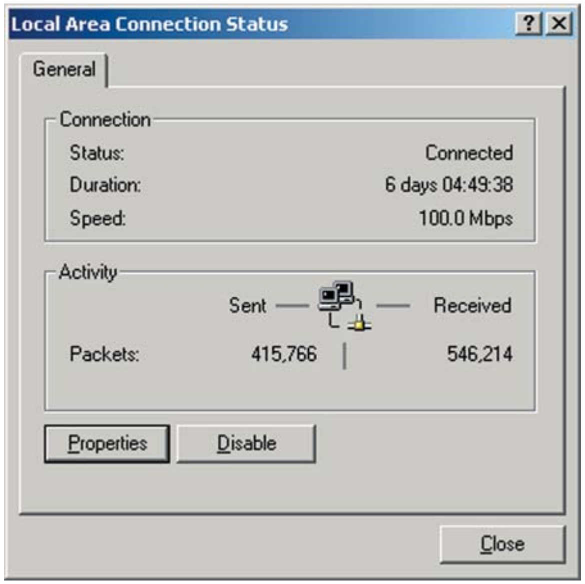
6. Windows may ask you to restart your PC. Click the **Yes** button. If Windows does not ask you to restart, restart your computer anyway.

Go to "Chapter 6: Configure the Router."

Configuring Windows 2000 PCs

1. Go to the Network screen by clicking the **Start** button. Click **Settings** and then **Control Panel**. From there, double-click the **Network and Dial-up Connections** icon.

2. Select the **Local Area Connection** icon for the applicable Ethernet adapter (usually it is the first Local Area Connection listed). Double-click the **Local Area Connection**. (See Figure 5-3.) Click the **Properties** button.



Status: Connected

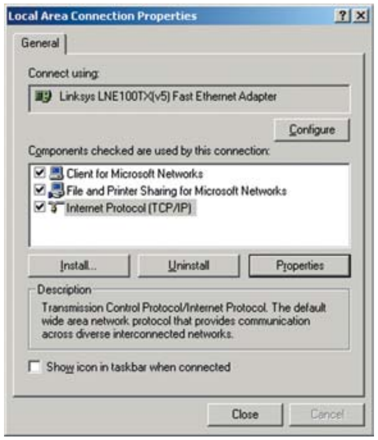
Duration: 6 days 04:49:38

Speed: 100.0 Mbps

Packets: 415,766 546,214

Figure 5-3

3. Select **Internet Protocol (TCP/IP)**, shown in Figure 5-4, and click the **Properties** button.



Local Area Connection Properties

General

Connect using:

Linksys LNE100TX(v5) Fast Ethernet Adapter

Configure

Components checked are used by this connection:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol (TCP/IP)

Install... | Uninstall | Properties

Description

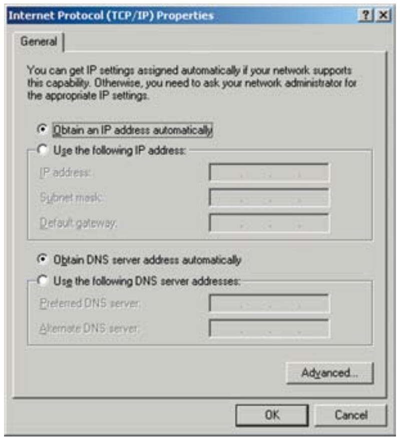
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ Show icon in taskbar when connected

Close | Cancel

Figure 5-4

4. Select **Obtain an IP address automatically** in both places, as shown in Figure 5-5, and click the **OK** button. Click the **OK** button again to complete the PC configuration.



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:

IP address:
Subnet mask:
Default gateway:

● Obtain DNS server address automatically
○ Use the following DNS server addresses:

Preferred DNS server:
Alternate DNS server:

Advanced...

OK | Cancel

Figure 5-5

5. Restart your computer.

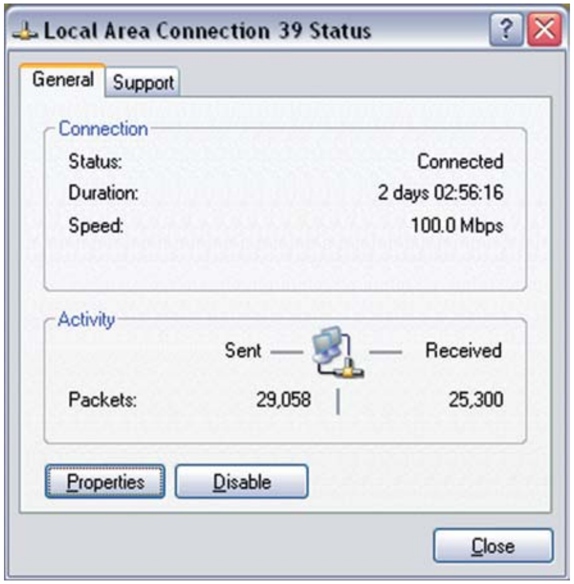
Go to "Chapter 6: Configure the Router."

Configuring Windows XP PCs

The following instructions assume you are running Windows XP with the default interface. If you are using the Classic interface (where the icons and menus look like previous Windows versions), please follow the instructions for Windows 2000.

1. Click to the Network screen by clicking the **Start** button and then **Control Panel**. From there, click the **Network and Internet Connections** icon and then the **Network Connections** icon.

2. Select the **Local Area Connection** icon for the applicable Ethernet adapter (usually it is the first Local Area Connection listed). Double-click the **Local Area Connection**. (See Figure 5-6.) Click the **Properties** button.



Local Area Connection 39 Status

General | Support

Connection

Status: Connected
Duration: 2 days 02:56:16
Speed: 100.0 Mbps

Activity

Sent — Received

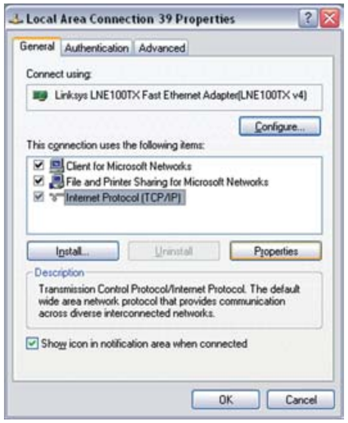
Packets: 29,058 | 25,300

Properties | Disable

Close

Figure 5-6

3. Select **Internet Protocol (TCP/IP)**, as shown in Figure 5-7, and click the **Properties** button.



Local Area Connection 39 Properties

Connect using:

Linksys LNE100TX Fast Ethernet Adapter(LNE100TX v4)

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol (TCP/IP)

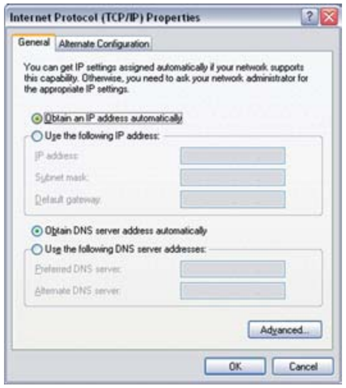
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in notification area when connected

Figure 5-7

4. Select **Obtain an IP address automatically**. Once the new window Select **Obtain an IP address automatically** in both places, as shown in Figure 5-8, and click the **OK** button. Click the **OK** button again to complete the PC configuration.



Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:
IP address:
Subnet mask:
Default gateway:

● Obtain DNS server address automatically
○ Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:

Figure 5-8

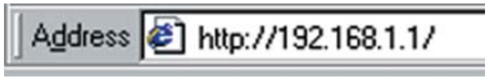
5. Restart your computer.

Go to "Chapter 6: Configure the Router."

Chapter 6: Configure the Router

This chapter will show you how to configure the Router to function in your network and gain access to the Internet through your Internet Service Provider (ISP). Detailed description of the Router's Web-based Utility can be found in "Chapter 7: The Cable/DSL Firewall Router's Web-based Utility." Your ISP may require the use of a Host Name and Domain Name. Further, you will set the WAN Connection Type on the Router's Setup tab based on the information provided by your ISP. *You will need the setup information from your ISP.* If you do not have this information, please contact your ISP before proceeding.

The instructions from your ISP will tell you how to set up your PC for Internet access. Because you are now using the Router to share Internet access among several computers, you will use the setup information to configure the Router instead of your PC. You only need to configure the Router once using the first computer you set up.

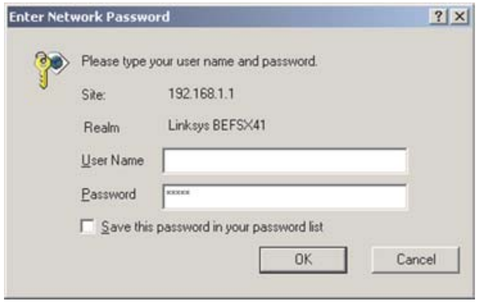


Address http://192.168.1.1/

Figure 6-1

1. Open your web browser. (It is all right if you get an error message at this point. Continue following these directions.) Enter **http://192.168.1.1** in the web browser's Address field, as shown in Figure 6-1. Press the **Enter** key.

2. An Enter Network Password window, shown in Figure 6-2, will appear (Windows XP users will see a Connect to 192.168.1.1 window, shown in Figure 6-3). Windows XP, the screen may look different.) Leave the User Name field empty, and enter **admin** in lowercase letters in the Password field (**admin** is the default password). Then, click the **OK** button.



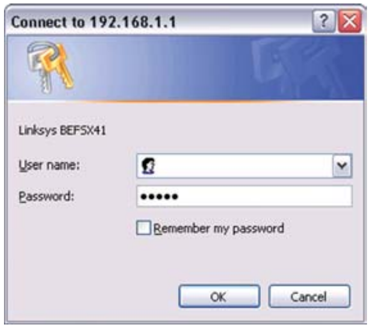
Enter Network Password

Please type your user name and password.

Site: 192.168.1.1
Realm Linksys BEFSX41
User Name
Password *****

☐ Save this password in your password list

Figure 6-2



Connect to 192.168.1.1

Linksys BEFSX41

User name:
Password: •••••

☐ Remember my password

Figure 6-3

3. The Router configuration screen will appear with the Setup tab selected. Based on the setup instructions from your ISP, you may need to provide the following information.

   Host Name and **Domain Name**: These fields allow you to provide a host name and domain name for the Router. These fields are usually left blank. If requested by your ISP (usually cable ISPs), complete these two fields.

   Device IP Address and **Subnet Mask**: The values for the Router's IP Address and Subnet Mask are shown on the Setup screen. The default value is 192.168.1.1 for the IP Address and 255.255.255.0 for the Subnet Mask. Leave these settings alone.

4. The Router supports six connection types: Obtain an IP Address Automatically, Static IP Address, PPPoE, RAS, PPTP, and HBS. These types are listed in the drop-down menu for the **WAN Connection Type** setting. Each Setup screen and available features will differ depending on what kind of connection type you select. Proceed to the instructions for the connection type you are using. When you are finished with the Setup tab, proceed to step 5.

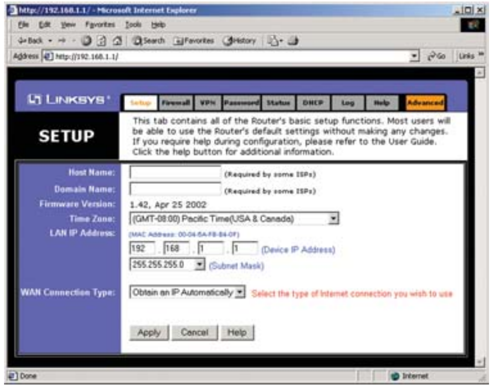
> **IMPORTANT:** If you have previously enabled any **Internet-sharing proxy server software** on any of your PCs, you must disable it now.
>
> Some examples of Internet-sharing software are Internet LanBridge, Wingate, ICS, and Sygate. To disable your Internet-sharing software:
>
> - If you are running Netscape Navigator, click **Edit** >> **Preferences** >> **Advanced** >> **Proxies**. Click **Direct Connection to the Internet**.
> - If you are running Internet Explorer 5.x or higher, click **Start** >> **Settings** >> **Control Panel** >> **Internet Options** >> **Connections** >> **LAN Settings**. Remove checkmarks from all three boxes. Click the **OK** button to continue.
>
> Also, you must disable any **Internet log-on software** (such as Ivasion Winpoet or Enternet 300) and any **firewall software** (such as ZoneAlarm and Watchdog) on all of your PCs.

Obtain an IP Address Automatically

If your ISP says that you are connecting through DHCP or a dynamic IP address from your ISP, perform these steps:

A. Select **Obtain an IP Automatically** as the WAN Connection Type. (Shown in Figure 6-4.)

B. Click the **Apply** and **Continue** buttons to save the setting, or click the **Cancel** button to clear the setting and start over. When you are finished, then proceed to step 5.


http://192.168.1.1/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.1.1/
Go Links
LINKSYS
Setup Firewall VPN Password Status DHCP Log Help Advanced
SETUP
Apply Cancel Help
Done
Internet

This tab contains all of the Router's basic setup functions. Most users will be able to use the Router's default settings without making any changes. If you require help during configuration, please refer to the User Guide. Click the help button for additional information.

Host Name: (Required by some ISPs)
Domain Name: (Required by some ISPs)
Firmware Version: 1.42, Apr 25 2002
Time Zone: (GMT-08:00) Pacific Time(USA & Canada)
LAN IP Address: (MAC Address: 00-04-5A-F8-B4-0F)
192 . 168 . 1 . 1 (Device IP Address)
255.255.255.0 (Subnet Mask)
WAN Connection Type: Obtain an IP Automatically Select the type of Internet connection you wish to use

Figure 6-4

Static IP Address

If your ISP says that you are connecting through a static or fixed IP address from your ISP, perform these steps:

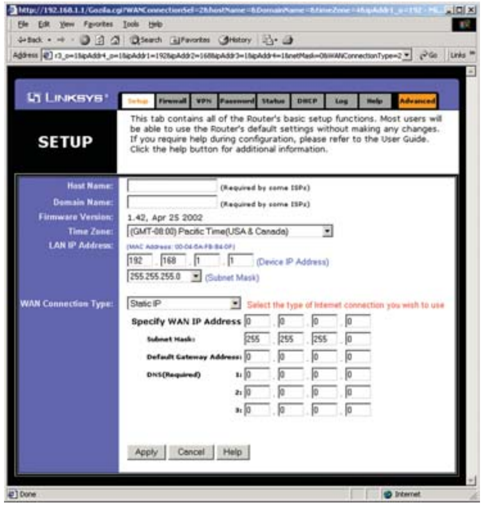
A. Select **Static IP** as the WAN Connection Type. (Shown in Figure 6-5.)

B. Enter the **IP Address**.

C. Enter the **Subnet Mask**.

D. Enter the **Gateway Address**.

E. Enter the **DNS** in the 1, 2, and/or 3 fields. You need to enter at least one DNS address.


http://192.168.1.1/Gozila.cgi?WANConnectionSel=2&hostName=&DomainName=&timeZone=4&ipAddr1_a=192
File Edit View Favorites Tools Help
Back Search Favorites History
Address r3_p=1&ipAddr4_p=1&ipAddr1=192&ipAddr2=168&ipAddr3=1&ipAddr4=1&netMask=0&WANConnectionType=2
Go Links
LINKSYS
Setup Firewall VPN Password Status DHCP Log Help Advanced
SETUP
Apply Cancel Help
Done
Internet

This tab contains all of the Router's basic setup functions. Most users will be able to use the Router's default settings without making any changes. If you require help during configuration, please refer to the User Guide. Click the help button for additional information.

Host Name: (Required by some ISPs)
Domain Name: (Required by some ISPs)
Firmware Version: 1.42, Apr 25 2002
Time Zone: (GMT-08:00) Pacific Time(USA & Canada)
LAN IP Address: (MAC Address: 00-04-5A-F8-B4-0F)
192 . 168 . 1 . 1 (Device IP Address)
255.255.255.0 (Subnet Mask)
WAN Connection Type: Static IP Select the type of Internet connection you wish to use
Specify WAN IP Address 0 . 0 . 0 . 0
Subnet Mask: 255 . 255 . 255 . 0
Default Gateway Address: 0 . 0 . 0 . 0
DNS(Required) 1: 0 . 0 . 0 . 0
2: 0 . 0 . 0 . 0
3: 0 . 0 . 0 . 0

Figure 6-5

F. Click the **Apply** and **Continue** buttons to save the settings, or click the **Cancel** button to clear the settings and start over. When you are finished, then proceed to step 5.

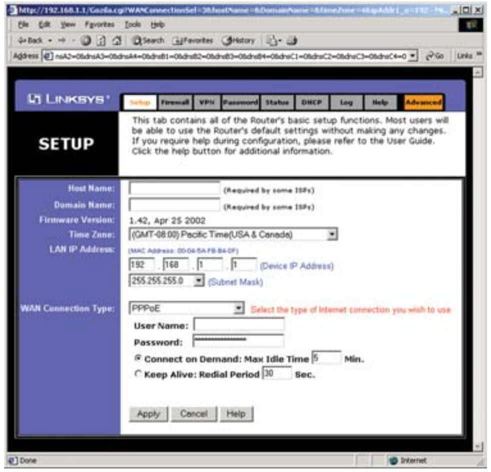
PPPoE

If your DSL provider says that you are connecting through PPPoE or if you normally enter a user name and password to access the Internet, perform these steps:

A. Select **PPPoE** as the WAN Connection Type. (Shown in Figure 6-6.)

B. Enter the **User Name**.

C. Enter the **Password**.



SETUP

This tab contains all of the Router's basic setup functions. Most users will be able to use the Router's default settings without making any changes. If you require help during configuration, please refer to the User Guide. Click the help button for additional information.

Host Name: (Required by some ISPs)
Domain Name: (Required by some ISPs)
Firmware Version: 1.42, Apr 25 2002
Time Zone: (GMT-08:00) Pacific Time(USA & Canada)
LAN IP Address: (MAC Address: 00-04-5A-F8-B4-0F)
192 . 168 . 1 . 1 (Device IP Address)
255.255.255.0 (Subnet Mask)
WAN Connection Type: PPPoE Select the type of Internet connection you wish to use
User Name:
Password: **************
● Connect on Demand: Max Idle Time 5 Min.
○ Keep Alive: Redial Period 30 Sec.

Figure 6-6

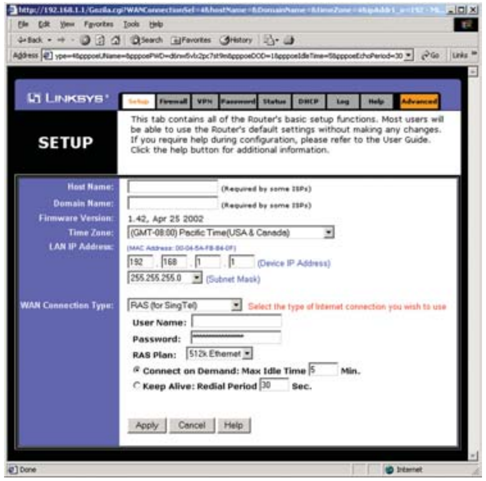
D. Click the **Apply** and **Continue** buttons to save the settings, or click the **Cancel** button to clear the settings and start over.

E. When you are finished, click the **Status** tab, and then click the **Connect** button to start the connection. Proceed to step 5.

RAS

RAS is a service used in Singapore only. (Shown in Figure 6-7.) If you are using a RAS connection, check with your ISP for the necessary setup information.

When you are finished with the Setup tab, proceed to step 5.



SETUP

This tab contains all of the Router's basic setup functions. Most users will be able to use the Router's default settings without making any changes. If you require help during configuration, please refer to the User Guide. Click the help button for additional information.

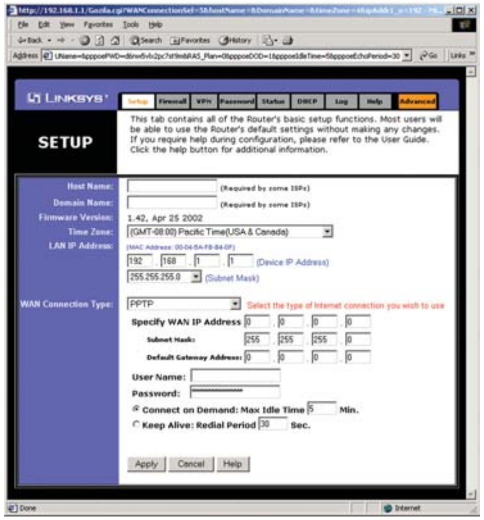
Host Name: (Required by some ISPs)
Domain Name: (Required by some ISPs)
Firmware Version: 1.42, Apr 25 2002
Time Zone: (GMT-08:00) Pacific Time(USA & Canada)
LAN IP Address: (MAC Address: 00-04-5A-F8-B4-0F)
192 . 168 . 1 . 1 (Device IP Address)
255.255.255.0 (Subnet Mask)
WAN Connection Type: RAS (for SingTel) Select the type of Internet connection you wish to use
User Name:
Password: **************
RAS Plan: 512k Ethernet
● Connect on Demand: Max Idle Time 5 Min.
○ Keep Alive: Redial Period 30 Sec.

Figure 6-7

PPTP

PPTP is a service used in Europe only. (Shown in Figure 6-8.) If you are using a PPTP connection, check with your ISP for the necessary setup information.

When you are finished with the Setup tab, proceed to step 5.



SETUP

This tab contains all of the Router's basic setup functions. Most users will be able to use the Router's default settings without making any changes. If you require help during configuration, please refer to the User Guide. Click the help button for additional information.

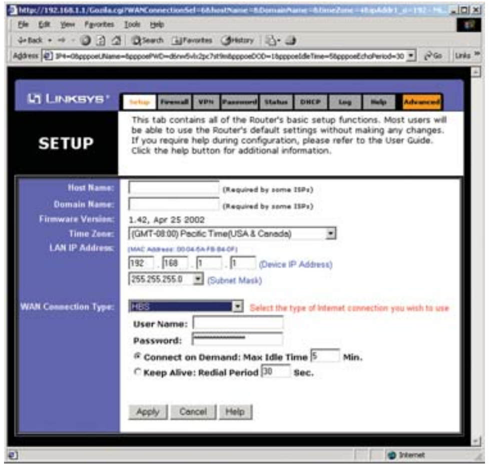
Host Name: (Required by some ISPs)
Domain Name: (Required by some ISPs)
Firmware Version: 1.42, Apr 25 2002
Time Zone: (GMT-08:00) Pacific Time(USA & Canada)
LAN IP Address: (MAC Address: 00-04-5A-F8-B4-0F)
192 . 168 . 1 . 1 (Device IP Address)
255.255.255.0 (Subnet Mask)
WAN Connection Type: PPTP Select the type of Internet connection you wish to use
Specify WAN IP Address 0 . 0 . 0 . 0
Subnet Mask: 255 . 255 . 255 . 0
Default Gateway Address: 0 . 0 . 0 . 0
User Name:
Password: **************
● Connect on Demand: Max Idle Time 5 Min.
○ Keep Alive: Redial Period 30 Sec.

Figure 6-8

HBS

HBS is a service used in Australia only. (Shown in Figure 6-9.) If you are using a HBS connection, check with your ISP for the necessary setup information.

When you are finished with the Setup tab, proceed to step 5.



SETUP

This tab contains all of the Router's basic setup functions. Most users will be able to use the Router's default settings without making any changes. If you require help during configuration, please refer to the User Guide. Click the help button for additional information.

Host Name: (Required by some ISPs)
Domain Name: (Required by some ISPs)
Firmware Version: 1.42, Apr 25 2002
Time Zone: (GMT-08:00) Pacific Time(USA & Canada)
LAN IP Address: (MAC Address: 00-04-5A-F8-B4-0F)
192 . 168 . 1 . 1 (Device IP Address)
255.255.255.0 (Subnet Mask)
WAN Connection Type: HBS Select the type of Internet connection you wish to use
User Name:
Password:
● Connect on Demand: Max Idle Time 5 Min.
○ Keep Alive: Redial Period 30 Sec.

Figure 6-9

5. If you haven't already done so, click the **Apply** button and then the **Continue** button to save your Setup settings. Close the web browser.

6. Reset the power on your cable or DSL modem.

7. Restart your computers so that they can obtain the Router's new settings.

   If you need advanced setting information, please refer to "Chapter 7: The Cable/DSL Firewall Router's Web-based Utility" or the Linksys support website at *support.linksys.com*.

   Congratulations! You've successfully configured the Router. Test the setup by opening your web browser from any computer and entering *www.linksys.com/registration*, as shown in Figure 6-10.

Address http://www.linksys.com/registration/

Figure 6-10

   If you are unable to reach our website, you may want to review what you did in this section or refer to "Appendix A: Troubleshooting."

Proceed to "Chapter 7: The Cable/DSL Firewall Router's Web-based Utility" for more details and advanced settings information.

Chapter 7: The Cable/DSL Firewall Router's Web-based Utility

Overview

For your convenience, use the Router's web-based utility to administer it. This chapter will explain all of the functions in this utility. The utility can be accessed via Microsoft Internet Explorer or Netscape Navigator through use of a computer connected with an Ethernet cable to the Router.

For a basic Router setup, most users only have to use the following screens of the utility:

- **Setup** Enter the settings provided by your ISP.

- **Password** The Router's default password is **admin**. To secure the Router, change the Password from its default.

The Status, Firewall, VPN, Password, Status, DHCP, Log, and Help tabs are also available for basic setup of the Router. For advanced setup of the Router, click the Advanced tab to access these screens: Filters, Forwarding, Dynamic Routing, Static Routing, DMZ Host, and MAC Address Clone.

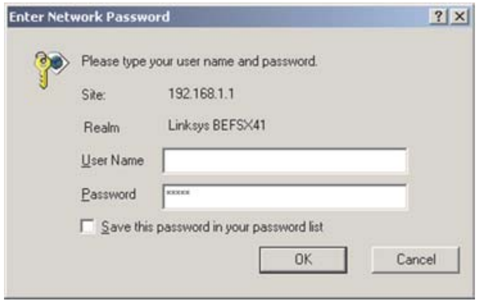
Quick and Easy Router Administration

To access the web-based utility of the Router, launch Internet Explorer or Netscape Navigator, and enter the Router's default IP address, **192.168.1.1**, in the Address field, as shown in Figure 7-1. Then, press **Enter**.

Address http://192.168.1.1/

Figure 7-1

An Enter Network Password window, shown in Figure 7-2, will appear (Windows XP users will see a Connect to 192.168.1.1 window, shown in Figure 7-3). Leave the User Name field blank, and enter **admin** in the Password field. Then click the **OK** button.



Please type your user name and password.

Site: 192.168.1.1

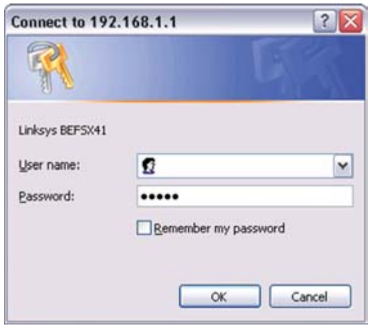
Realm: Linksys BEFSX41

User Name:

Password: *****

☐ Save this password in your password list

Figure 7-2



Linksys BEFSX41

User name:

Password: •••••

☐ Remember my password

Figure 7-3

In this section, you'll find brief descriptions of each web page in the Utility and each page's key functions.

To apply any of the settings you change on a page, click the **Apply** button, and then click the **Continue** button. To cancel any values you've entered on any page, click the **Cancel** button.

Setup

The Setup screen is the first screen you see when you access the web-based utility. If you have already installed and set up the Router, you have already seen this screen and properly configured all of the screen's values.

- **Host Name & Domain Name** These fields allow you to supply a host and domain name for the Router. Some ISPs require these names as identification. You may have to check with your ISP to see if your broadband Internet service has been configured with a host and domain name. In most cases, leaving these fields blank will work.

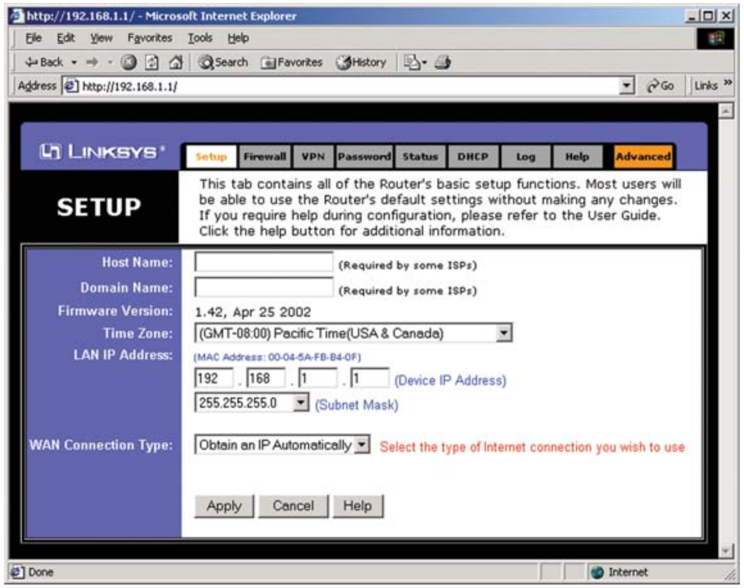
- **Firmware Version** This entry shows the version and date of the firmware you are using. Future versions of the Router's firmware will be posted and available for download on the Linksys website at *www.linksys.com*.

- **Time Zone** Set your local time zone here.

- **Device IP Address and Subnet Mask** The values for the Router's IP Address and Subnet Mask are shown here. The default values are 192.168.1.1 for the Device IP Address and 255.255.255.0 for the Subnet Mask.

- **WAN Connection Type** The Router supports six connection types: DHCP, PPPoE, Static IP, PPTP, RAS, and HBS. Each Setup screen and available features will differ depending on what kind of connection type you select.

Note: You can test and see if the settings are correct by successfully connecting to the Internet.



Address: http://192.168.1.1/

This tab contains all of the Router's basic setup functions. Most users will be able to use the Router's default settings without making any changes. If you require help during configuration, please refer to the User Guide. Click the help button for additional information.

Host Name: (Required by some ISPs)

Domain Name: (Required by some ISPs)

Firmware Version: 1.42, Apr 25 2002

Time Zone: (GMT-08:00) Pacific Time(USA & Canada)

LAN IP Address: (MAC Address: 00-04-5A-FB-B4-0F)
192 . 168 . 1 . 1 (Device IP Address)
255.255.255.0 (Subnet Mask)

WAN Connection Type: Obtain an IP Automatically — Select the type of Internet connection you wish to use

Figure 7-4

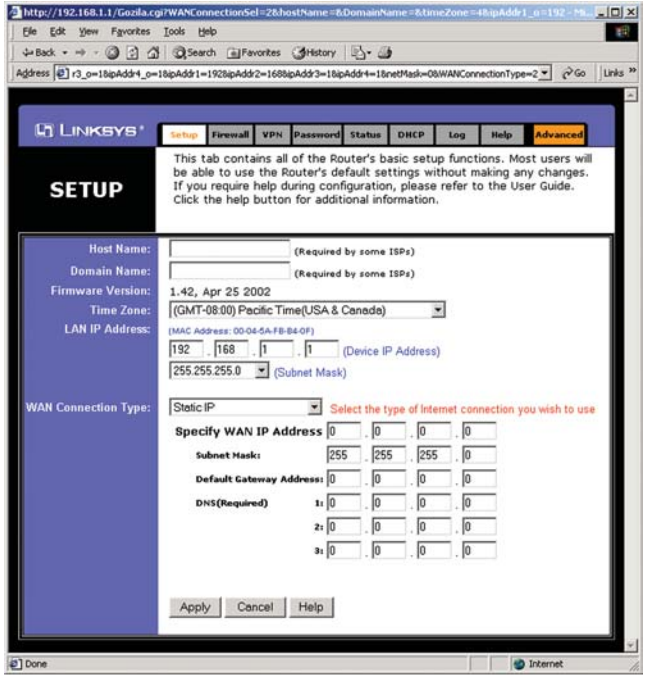
Obtain an IP Address Automatically

By default, the Router's WAN Connection Type is set to obtain an IP address automatically, shown in Figure 7-4, and it should be used only if your ISP supports DHCP.

To apply any of the settings you change on a page, click the **Apply** button, and then click the **Continue** button. To cancel any values you've entered on any page, click the **Cancel** button.

Static IP

If you are required to use a permanent IP address, then select **Static IP**, as shown in Figure 7-5.


http://192.168.1.1/Gozila.cgi?WANConnectionSel=2&hostName=&DomainName=&timeZone=4&ipAddr1_o=192 - Mi...
File Edit View Favorites Tools Help
Back Search Favorites History
Address r3_o=1&ipAddr4_o=1&ipAddr1=192&ipAddr2=168&ipAddr3=1&ipAddr4=1&netMask=0&WANConnectionType=2
Go Links
LINKSYS
Setup Firewall VPN Password Status DHCP Log Help Advanced
SETUP
Apply Cancel Help
Done Internet

This tab contains all of the Router's basic setup functions. Most users will be able to use the Router's default settings without making any changes. If you require help during configuration, please refer to the User Guide. Click the help button for additional information.

Host Name: (Required by some ISPs)
Domain Name: (Required by some ISPs)
Firmware Version: 1.42, Apr 25 2002
Time Zone: (GMT-08:00) Pacific Time(USA & Canada)
LAN IP Address: (MAC Address: 00-04-5A-FB-B4-0F)
192 . 168 . 1 . 1 (Device IP Address)
255.255.255.0 (Subnet Mask)
WAN Connection Type: Static IP Select the type of Internet connection you wish to use
Specify WAN IP Address 0 . 0 . 0 . 0
Subnet Mask: 255 . 255 . 255 . 0
Default Gateway Address: 0 . 0 . 0 . 0
DNS(Required) 1: 0 . 0 . 0 . 0
2: 0 . 0 . 0 . 0
3: 0 . 0 . 0 . 0

Figure 7-5

Specify WAN IP Address This is the IP address that the Router has, when seen from the WAN, or the Internet. Your ISP will provide you with the IP Address you need to specify here.

Subnet Mask This is the Router's Subnet Mask, as seen by external users on the Internet (including your ISP). Your ISP will provide you with the Subnet Mask.

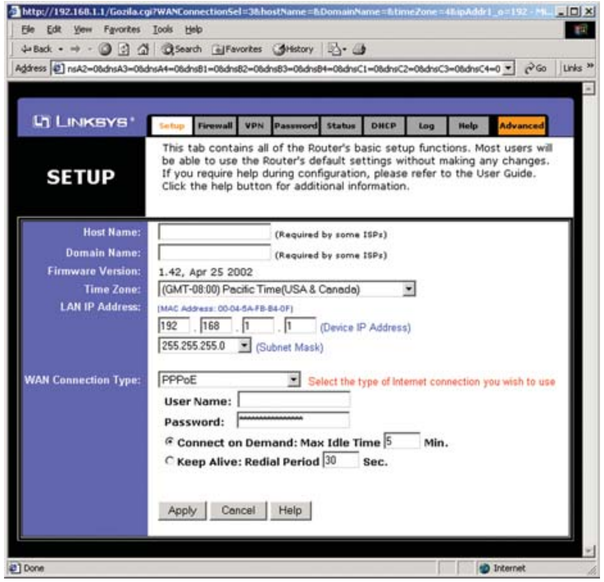
Default Gateway Address Your ISP will provide you with the Default Gateway Address.

DNS (Required) Your ISP will provide you with at least one DNS (Domain Name System) Server IP Address.

To apply any of the settings you change on a page, click the **Apply** button, and then click the **Continue** button. To cancel any values you've entered on any page, click the **Cancel** button.

PPPoE

Some DSL-based ISPs use PPPoE (Point-to-Point Protocol over Ethernet) to establish Internet connections for end-users. If you are connected to the Internet through a DSL line, check with your ISP to see if they use PPPoE. If they do, select the PPPoE connection type, as shown in Figure 7-6.


http://192.168.1.1/Gozila.cgi?WANConnectionSel=3&hostName=&DomainName=&timeZone=4&ipAddr1_o=192 - Mi...
File Edit View Favorites Tools Help
Back Search Favorites History
Address nsA2=0&dnsA3=0&dnsA4=0&dnsB1=0&dnsB2=0&dnsB3=0&dnsB4=0&dnsC1=0&dnsC2=0&dnsC3=0&dnsC4=0
Go Links
LINKSYS
Setup Firewall VPN Password Status DHCP Log Help Advanced
SETUP
Apply Cancel Help
Done Internet

This tab contains all of the Router's basic setup functions. Most users will be able to use the Router's default settings without making any changes. If you require help during configuration, please refer to the User Guide. Click the help button for additional information.

Host Name: (Required by some ISPs)
Domain Name: (Required by some ISPs)
Firmware Version: 1.42, Apr 25 2002
Time Zone: (GMT-08:00) Pacific Time(USA & Canada)
LAN IP Address: (MAC Address: 00-04-5A-FB-B4-0F)
192 . 168 . 1 . 1 (Device IP Address)
255.255.255.0 (Subnet Mask)
WAN Connection Type: PPPoE Select the type of Internet connection you wish to use
User Name:
Password: ***************
● Connect on Demand: Max Idle Time 5 Min.
○ Keep Alive: Redial Period 30 Sec.

Figure 7-6

User Name and Password Enter the **User Name** and **Password** provided by your ISP.

Connect on Demand and Max Idle Time You can configure the Router to cut your connection with your ISP after a specified period of time (Max Idle Time). If you have been disconnected due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, click the radio button. In the Max Idle Time field, enter the number of minutes you want to have elapsed before your Internet access disconnects.

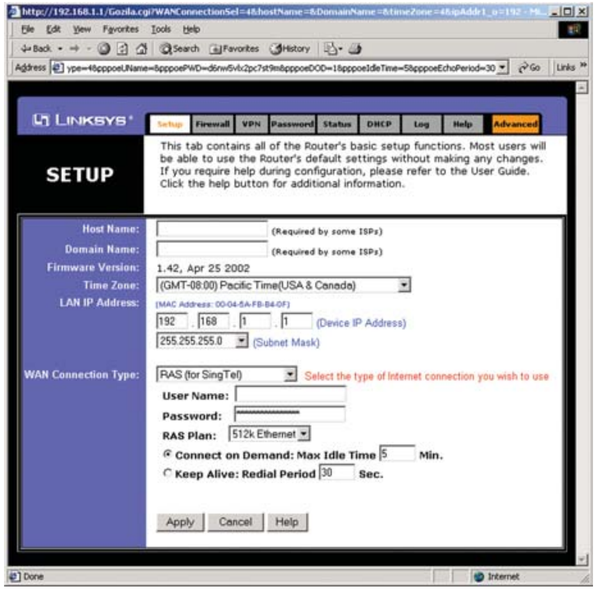
Keep Alive Option and Redial Period If you select this option, the Router will periodically check your Internet connection. If you are disconnected, then the Router will automatically re-establish your connection. To use this option, click the radio button next to **Keep Alive**. The default Redial Period is 30 seconds.

Important: For DSL users, if you need to enable PPPoE support, choose **PPPoE**. If you do enable PPPoE, remember to remove any PPPoE applications that are already installed on any of your PCs.

To apply any of the settings you change on a page, click the **Apply** button, and then click the **Continue** button. To cancel any values you've entered on any page, click the **Cancel** button.

RAS

Remote Access Service (RAS) is a service that applies to connections in Singapore only. (Shown in Figure 7-6.) For users in Singapore, check with Singtel for information on RAS.


File Edit View Favorites Tools Help
Back Search Favorites History
Go Links
LINKSYS
Setup Firewall VPN Password Status DHCP Log Help Advanced
Apply Cancel Help
Done
Internet

http://192.168.1.1/Gozila.cgi?WANConnectionSel=4&hostName=&DomainName=&timeZone=4&ipAddr1_o=192 - Mi...

Address: ype=4&pppoeUName=&pppoePWD=d6rw5vlx2pc7st9m&pppoeDOD=1&pppoeIdleTime=5&pppoeEchoPeriod=30

SETUP

This tab contains all of the Router's basic setup functions. Most users will be able to use the Router's default settings without making any changes. If you require help during configuration, please refer to the User Guide. Click the help button for additional information.

Host Name: (Required by some ISPs)
Domain Name: (Required by some ISPs)
Firmware Version: 1.42, Apr 25 2002
Time Zone: (GMT-08:00) Pacific Time(USA & Canada)
LAN IP Address: (MAC Address: 00-04-5A-FB-B4-0F)
192 . 168 . 1 . 1 (Device IP Address)
255.255.255.0 (Subnet Mask)
WAN Connection Type: RAS (for SingTel) Select the type of Internet connection you wish to use
User Name:
Password: ****************
RAS Plan: 512k Ethernet
● Connect on Demand: Max Idle Time 5 Min.
○ Keep Alive: Redial Period 30 Sec.

Figure 7-6

User Name and Password Enter the **User Name** and **Password** supplied by Singtel.

RAS Plan Select the type of plan you have.

Connect on Demand and Max Idle Time You can configure the Router to cut your connection with your ISP after a specified period of time (Max Idle Time). If you have been disconnected due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, click the radio button. In the Max Idle Time field, enter the number of minutes you want to have elapsed before your Internet access disconnects.

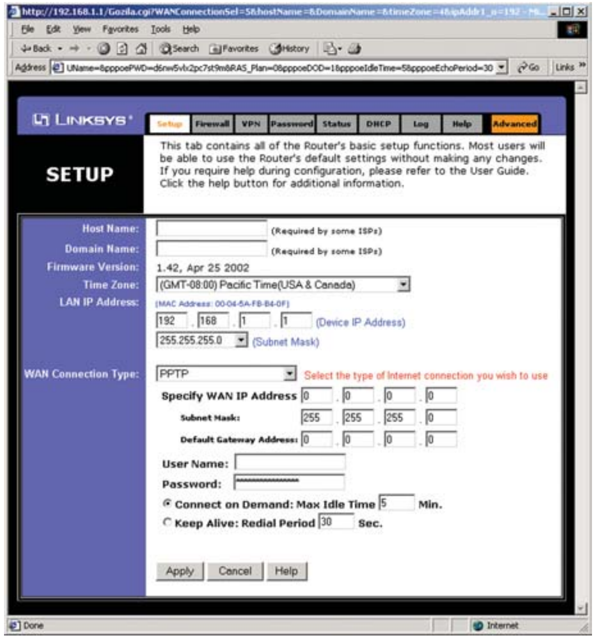
Keep Alive Option and Redial Period If you select this option, the Router will periodically check your Internet connection. If you are disconnected, then the Router will automatically re-establish your connection. To use this option, click the radio button next to **Keep Alive**. The default Redial Period is 30 seconds.

To apply any of the settings you change on a page, click the **Apply** button, and then click the **Continue** button. To cancel any values you've entered on any page, click the **Cancel** button.

PPTP

Point to Point Tunneling Protocol (PPTP) is a service that applies to connections in Europe only. Figure 7-8 shows a PPTP setup.

Specify WAN IP Address This is the IP address that the Router has, when seen from the WAN, or the Internet. Your ISP will provide you with the IP Address you need to specify here.


File Edit View Favorites Tools Help
Back Search Favorites History
Go Links
LINKSYS
Setup Firewall VPN Password Status DHCP Log Help Advanced
Apply Cancel Help
Done
Internet

http://192.168.1.1/Gozila.cgi?WANConnectionSel=5&hostName=&DomainName=&timeZone=4&ipAddr1_o=192 - Mi...

Address: UName=&pppoePWD=d6rw5vlx2pc7st9m&RAS_Plan=0&pppoeDOD=1&pppoeIdleTime=5&pppoeEchoPeriod=30

SETUP

This tab contains all of the Router's basic setup functions. Most users will be able to use the Router's default settings without making any changes. If you require help during configuration, please refer to the User Guide. Click the help button for additional information.

Host Name: (Required by some ISPs)
Domain Name: (Required by some ISPs)
Firmware Version: 1.42, Apr 25 2002
Time Zone: (GMT-08:00) Pacific Time(USA & Canada)
LAN IP Address: (MAC Address: 00-04-5A-FB-B4-0F)
192 . 168 . 1 . 1 (Device IP Address)
255.255.255.0 (Subnet Mask)
WAN Connection Type: PPTP Select the type of Internet connection you wish to use
Specify WAN IP Address 0 . 0 . 0 . 0
Subnet Mask: 255 . 255 . 255 . 0
Default Gateway Address: 0 . 0 . 0 . 0
User Name:
Password: ****************
● Connect on Demand: Max Idle Time 5 Min.
○ Keep Alive: Redial Period 30 Sec.

Figure 7-8

Subnet Mask This is the Router's Subnet Mask, as seen by external users on the Internet (including your ISP). Your ISP will provide you with the Subnet Mask.

Default Gateway Address Your ISP will provide you with the Default Gateway Address.

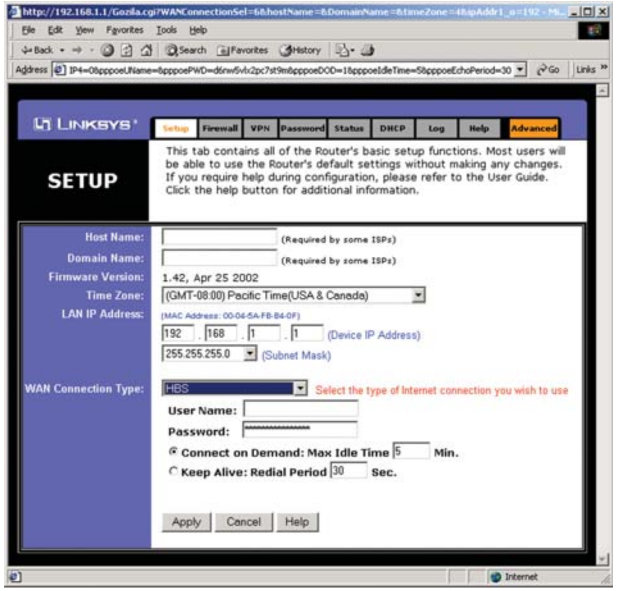
Connect on Demand and Max Idle Time You can configure the Router to cut your connection with your ISP after a specified period of time (Max Idle Time). If you have been disconnected due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, click the radio button. In the Max Idle Time field, enter the number of minutes you want to have elapsed before your Internet access disconnects.

Keep Alive Option and Redial Period If you select this option, the Router will periodically check your Internet connection. If you are disconnected, then the Router will automatically re-establish your connection. To use this option, click the radio button next to **Keep Alive**. The default Redial Period is 30 seconds.

To apply any of the settings you change on a page, click the **Apply** button, and then click the **Continue** button. To cancel any values you've entered on any page, click the **Cancel** button.

HBS

The HeartBeat Signal (HBS) is a service that applies to connections in Australia only. (Shown in Figure 7-9.) For users in Australia, check with your ISP for setup information.


http://192.168.1.1/Gozila.cgi?WANConnectionSel=6&hostName=&DomainName=&timeZone=4&ipAddr1_o=192 - Mi...
File Edit View Favorites Tools Help
Back Search Favorites History
Address IP4=0&pppoeUName=&pppoePWD=d6rw5vlx2pc7st9m&pppoeDOD=1&pppoeIdleTime=5&pppoeEchoPeriod=30
Go
Links
LINKSYS
Setup
Firewall
VPN
Password
Status
DHCP
Log
Help
Advanced
SETUP
Apply
Cancel
Help
Internet

This tab contains all of the Router's basic setup functions. Most users will be able to use the Router's default settings without making any changes. If you require help during configuration, please refer to the User Guide. Click the help button for additional information.

Host Name: (Required by some ISPs)
Domain Name: (Required by some ISPs)
Firmware Version: 1.42, Apr 25 2002
Time Zone: (GMT-08:00) Pacific Time(USA & Canada)
LAN IP Address: (MAC Address: 00-04-5A-FB-B4-0F)
192 . 168 . 1 . 1 (Device IP Address)
255.255.255.0 (Subnet Mask)
WAN Connection Type: HBS Select the type of Internet connection you wish to use
User Name:
Password: ****************
● Connect on Demand: Max Idle Time 5 Min.
○ Keep Alive: Redial Period 30 Sec.

Figure 7-9

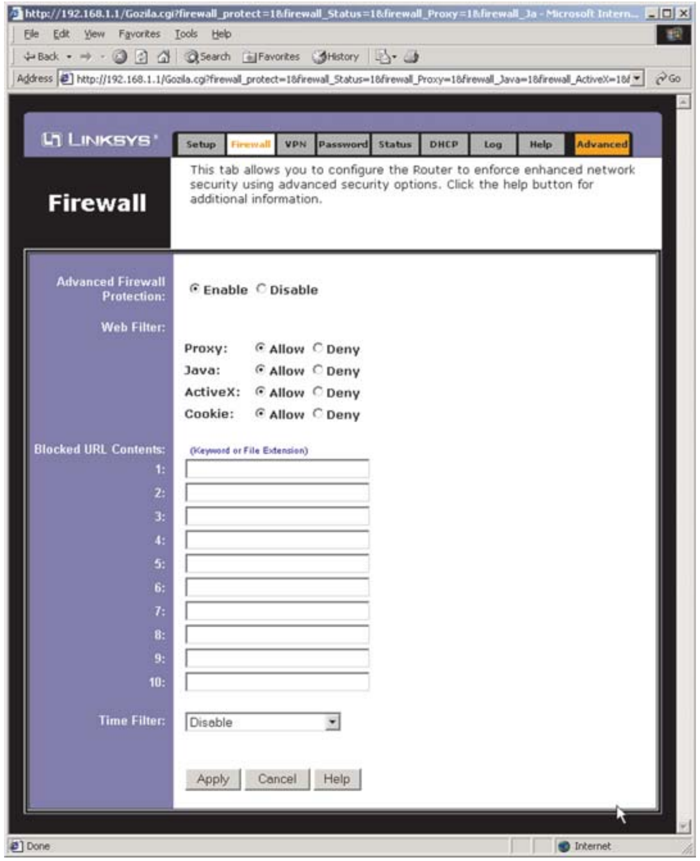
User Name and Password Enter the **User Name** and **Password** supplied by your ISP.

Connect on Demand and Max Idle Time You can configure the Router to cut your connection with your ISP after a specified period of time (Max Idle Time). If you have been disconnected due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate Connect on Demand, click the radio button. In the Max Idle Time field, enter the number of minutes you want to have elapsed before your Internet access disconnects.

Keep Alive Option and Redial Period If you select this option, the Router will periodically check your Internet connection. If you are disconnected, then the Router will automatically re-establish your connection. To use this option, click the radio button next to **Keep Alive**. The default Redial Period is 30 seconds.

To apply any of the settings you change on a page, click the **Apply** button, and then click the **Continue** button. To cancel any values you've entered on any page, click the **Cancel** button.

The Firewall Tab


http://192.168.1.1/Gozila.cgi?firewall_protect=1&firewall_Status=1&firewall_Proxy=1&firewall_Ja - Microsoft Intern...
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.1.1/Gozila.cgi?firewall_protect=1&firewall_Status=1&firewall_Proxy=1&firewall_Java=1&firewall_ActiveX=1&
Go
LINKSYS
Setup
Firewall
VPN
Password
Status
DHCP
Log
Help
Advanced
Firewall
Apply
Cancel
Help
Done
Internet

This tab allows you to configure the Router to enforce enhanced network security using advanced security options. Click the help button for additional information.

Advanced Firewall Protection: ● Enable ○ Disable
Web Filter:
Proxy: ● Allow ○ Deny
Java: ● Allow ○ Deny
ActiveX: ● Allow ○ Deny
Cookie: ● Allow ○ Deny
Blocked URL Contents: (Keyword or File Extension)
1:
2:
3:
4:
5:
6:
7:
8:
9:
10:
Time Filter: Disable

Figure 7-10

The Firewall Tab, shown in Figure 7-10, allows you to set the Cable/DSL Firewall Router's level of security. Some environments require greater security while some Internet applications work better with fewer restrictions. This tab allows you to customize these settings.

Advanced Firewall Protection Enable this option to employ SPI (Stateful Packet Inspection) and DoS (Denial of Service). These functions allow for more detailed review of data packets entering your network environment and prevention of Denial of Service attacks.

Web Filter You can either enable or disable these four filtering methods by selecting **Allow** or **Deny**.

- **Proxy** Use of WAN proxy servers may compromise the Router's security. Denying Proxy will disable access to any WAN proxy servers.

- **Java** Java is a programming language for websites. If you deny Java, you run the risk of not having access to Internet sites created using this programming language.

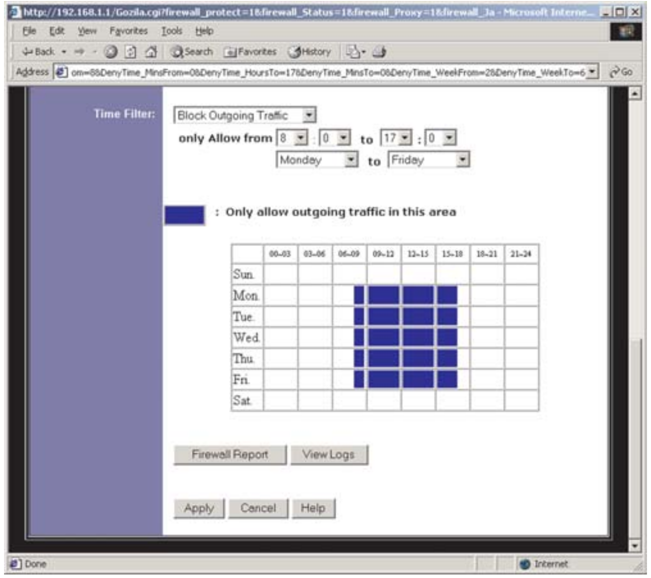
- **ActiveX** ActiveX is a programming language for websites. If you deny ActiveX, you run the risk of not having access to Internet sites created using this programming language.

- **Cookie** A cookie is data stored on your PC and used by Internet sites when you interact with them, so you may not want to deny cookies.

Blocked URL Contents These ten fields are for denying access to specific websites. Type the URL (or Internet address) of the site you wish to block or any text you wish the browser to discriminate against in one of the empty fields. You can also block specific files like JPEG or GIF files (e.g., files with the extension ".jpg" or ".gif").

Time Filter This option allows you to block access to your LAN or WAN, or both within a prescribed time period. Enabling Time Filter will display further options, as shown in Figure 7-11. Clicking **Block Incoming Traffic** will block access to your local area network. Clicking **Block Outgoing Traffic** will block access to your wide area network. To block access to both, click **Block Bi-Direction Traffic**. In choosing these options, you will be allowed to change the time when access is being filtered. This option is turned off by default with the **Disable** radio button selected. Next, click the drop-down windows to set the time and days when access will be filtered.

The Time Filter selection uses a 24-hour clock. In this method, every hour until noon is displayed as 1:00 through 12:00. Every hour after that is an hour added to 12. For example, 3:00 pm would be displayed as 15:00 and 9:45 pm would be displayed as 21:45.


http://192.168.1.1/Gozila.cgi?firewall_protect=1&firewall_Status=1&firewall_Proxy=1&firewall_Ja - Microsoft Interne...
File Edit View Favorites Tools Help
Back Search Favorites History
Address
om=8&DenyTime_MinsFrom=0&DenyTime_HoursTo=17&DenyTime_MinsTo=0&DenyTime_WeekFrom=2&DenyTime_WeekTo=6
Go
Done
Internet

Time Filter: Block Outgoing Traffic

only Allow from 8 : 0 to 17 : 0

Monday to Friday

■ : Only allow outgoing traffic in this area

	00~03	03~06	06~09	09~12	12~15	15~18	18~21	21~24
Sun.								
Mon.			■	■	■	■		
Tue.			■	■	■	■		
Wed.			■	■	■	■		
Thu.			■	■	■	■		
Fri.			■	■	■	■		
Sat.								

Firewall Report
View Logs
Apply
Cancel
Help

Figure 7-11

Click the **Firewall Report** button to view a status report on the firewall. (This is the same as the Firewall Log.)

Click the **View Logs** button to open a new window (which is the same as the Log tab). From the drop-down menu, select the log you wish to view: All (to view all logs), System Log, Access Log, Firewall Log, or VPN Log.

- **System Log** The System Log screen displays a list of cold and warm starts, web login successes and failures, and packet filtering policies.

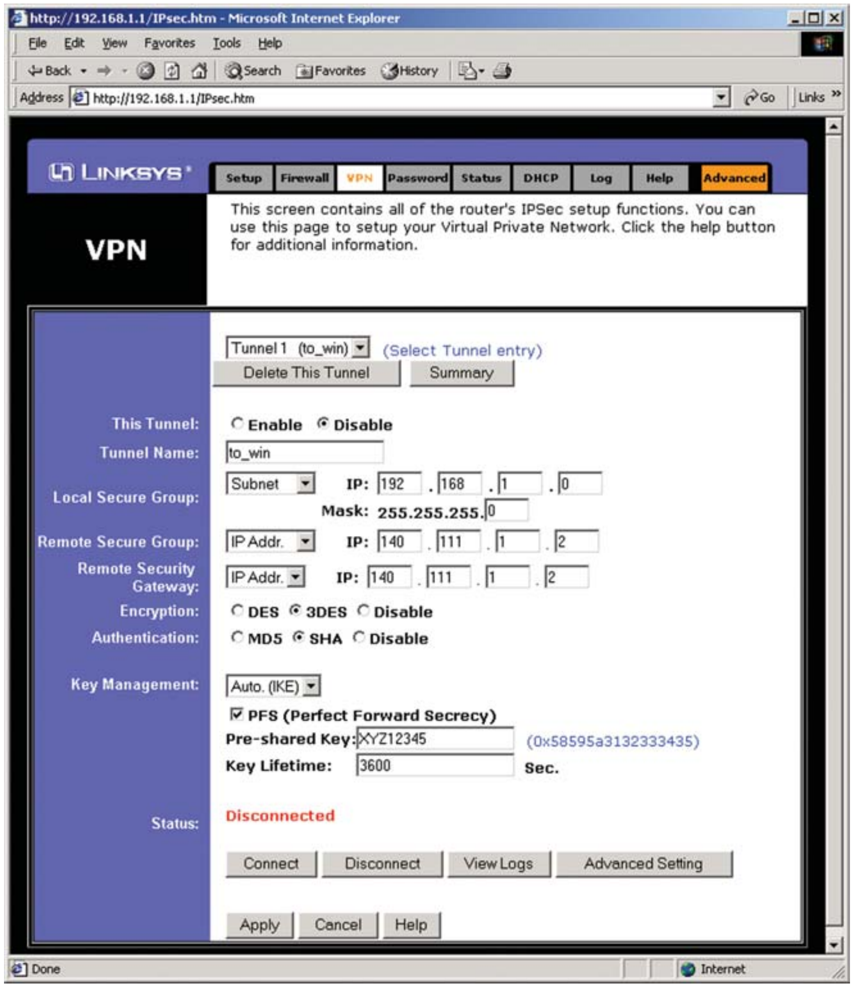
- **Access Log** The Access Log screen shows all incoming and outgoing traffic.

- **Firewall Log** The Firewall Log screen lists activities performed by the firewall to prevent DoS attacks, including URL filtering and time filtering.

- **VPN Log** The VPN Log screen displays successful connections, transmissions and receptions, and the types of encryption used.

To apply any of the settings you change on a page, click the **Apply** button, and then click the **Continue** button. To cancel any values you've entered on any page, click the **Cancel** button. For further help on this tab, click the **Help** button.

The VPN Tab


http://192.168.1.1/IPsec.htm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.1.1/IPsec.htm
Go Links
LINKSYS
Setup Firewall VPN Password Status DHCP Log Help Advanced
VPN
Done
Internet

This screen contains all of the router's IPSec setup functions. You can use this page to setup your Virtual Private Network. Click the help button for additional information.

Tunnel 1 (to_win) (Select Tunnel entry)
Delete This Tunnel | Summary

This Tunnel: ○ Enable ● Disable
Tunnel Name: to_win
Local Secure Group: Subnet IP: 192 . 168 . 1 . 0 Mask: 255.255.255. 0
Remote Secure Group: IP Addr. IP: 140 . 111 . 1 . 2
Remote Security Gateway: IP Addr. IP: 140 . 111 . 1 . 2
Encryption: ○ DES ● 3DES ○ Disable
Authentication: ○ MD5 ● SHA ○ Disable
Key Management: Auto. (IKE)
☑ PFS (Perfect Forward Secrecy)
Pre-shared Key: XYZ12345 (0x58595a3132333435)
Key Lifetime: 3600 Sec.
Status: Disconnected

Connect | Disconnect | View Logs | Advanced Setting

Apply | Cancel | Help

Figure 7-12

Virtual Private Networking (VPN) is a security measure that basically creates a secure connection between two remote locations. This connection is very specific as far as its settings are concerned; this is what creates the security. The VPN screen, shown in Figure 7-12, allows you to configure your VPN settings to make your network more secure.

Note: Network security, while a desirable and often necessary aspect of networking, is complex and requires a thorough understanding of networking principles.

Establishing a Tunnel

The Firewall Router creates a tunnel or channel between two endpoints, so that the data or information between these endpoints is secure. To establish this tunnel, select the tunnel you wish to create in the (**Select Tunnel Entry)** drop-down box. It is possible to create up to two simultaneous tunnels.

Then check the box next to **Enable** to enable the tunnel.

Once the tunnel is enabled, enter the name of the tunnel in the **Tunnel Name** field. This is to allow you to identify multiple tunnels and does not have to match the name used at the other end of the tunnel.

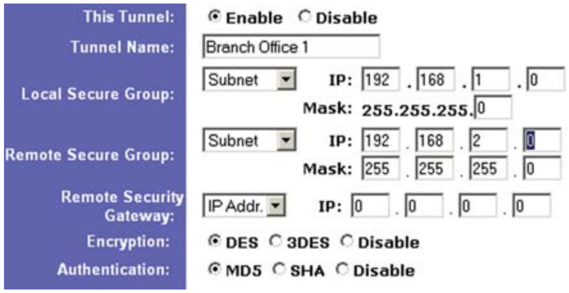
Click the **Delete This Tunnel** button to delete any tunnel entry. Click the **Summary** button to view information about the selected tunnel, after the tunnel has been connected.

Local Secure Group and Remote Secure Group

The **Local Secure Group** is the computer(s) on your LAN that can access the tunnel. The **Remote Secure Group** is the computer (s) on the remote end of the tunnel that can access the tunnel. Under Local Secure Group and Remote Secure Group, you may choose one of three options: Subnet, IP Address, and IP Range. Under Remote Secure Group, you have two additional options: Host and Any.

> **Note:** The IP Addresses and Subnet Mask values used here are for example only. ***Do not try to use them for your actual setup.*** Obtain the relevant information from your own network to accurately configure your Firewall Router.

- **Subnet -** If you select **Subnet** (which is the default), this will allow all computers on the local subnet to access the tunnel. In the example shown in Figure 7-13, all Local Secure Group computers with IP Addresses 192.168.1.xxx will be able to access the tunnel. All Remote Secure Group computers with IP Addresses 192.168.2.xxx will be able to access the tunnel (in your settings, use the IP Addresses appropriate for your VPN). When using the Subnet setting, the default values of **0** should remain in the last fields of the **IP** and **Mask** settings.

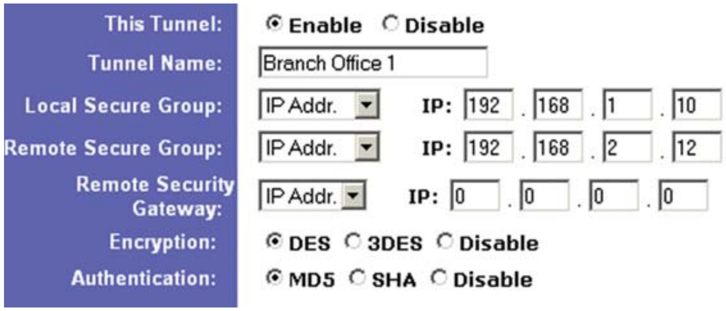


This Tunnel: ● Enable ○ Disable
Tunnel Name: Branch Office 1
Local Secure Group: Subnet IP: 192 . 168 . 1 . 0 Mask: 255.255.255.0
Remote Secure Group: Subnet IP: 192 . 168 . 2 . 0 Mask: 255 . 255 . 255 . 0
Remote Security Gateway: IP Addr. IP: 0 . 0 . 0 . 0
Encryption: ● DES ○ 3DES ○ Disable
Authentication: ● MD5 ○ SHA ○ Disable

Figure 7-13

> **Note:** It is possible to set up your Firewall Router using any combination of the three settings under Local Secure Group and the five settings under Remote Secure Group. For instance, when Subnet is chosen on the local end of the tunnel, Subnet does not have to be chosen at the remote end. So a single IP Address could be chosen to access the tunnel on the local end and a range of IP Addresses could be set at the remote end of the tunnel.

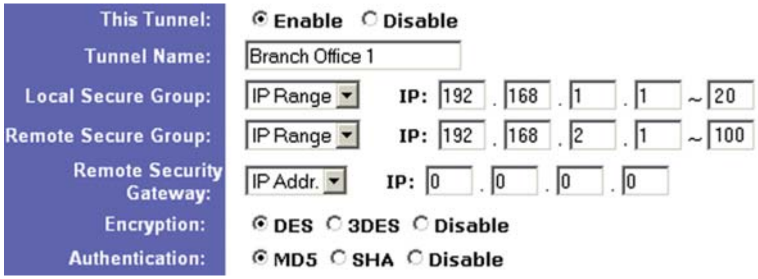
- **IP Address -** If you select **IP Address**, only the computer with the specific IP Address that you enter will be able to access the tunnel. In the example shown in Figure 7-14, only the computer with IP Address 192.168.1.10 can access the tunnel from this end. Only the computer with IP Address 192.168.2.12 can access the tunnel from the remote end (in your settings, use the IP Addresses appropriate for your VPN).



This Tunnel: ● Enable ○ Disable
Tunnel Name: Branch Office 1
Local Secure Group: IP Addr. IP: 192 . 168 . 1 . 10
Remote Secure Group: IP Addr. IP: 192 . 168 . 2 . 12
Remote Security Gateway: IP Addr. IP: 0 . 0 . 0 . 0
Encryption: ● DES ○ 3DES ○ Disable
Authentication: ● MD5 ○ SHA ○ Disable

Figure 7-14

- **IP Range -** If you select IP Range, it will be a combination of Subnet and IP Address. You can specify a range of IP Addresses within the Subnet which will have access to the tunnel. In the example shown in Figure 7-15, all computers on this end of the tunnel with IP Addresses between 192.168.1.1 and 192.168.1.20 can access the tunnel from the local end. Only computers assigned an IP Address between 192.168.2.1 and 192.168.2.100 can access the tunnel from the remote end (in your settings, use the IP Ranges appropriate for your VPN).

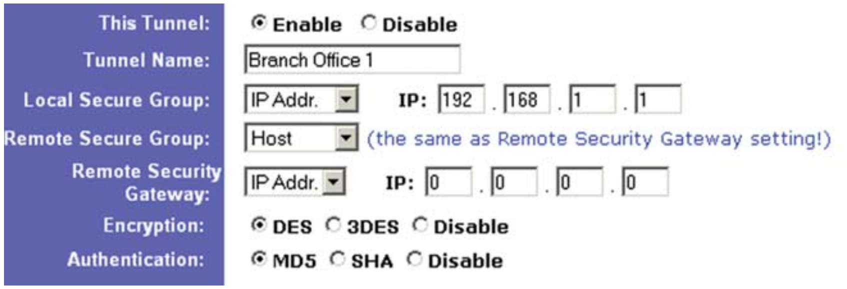


This Tunnel: ● Enable ○ Disable
Tunnel Name: Branch Office 1
Local Secure Group: IP Range IP: 192 . 168 . 1 . 1 ~ 20
Remote Secure Group: IP Range IP: 192 . 168 . 2 . 1 ~ 100
Remote Security Gateway: IP Addr. IP: 0 . 0 . 0 . 0
Encryption: ● DES ○ 3DES ○ Disable
Authentication: ● MD5 ○ SHA ○ Disable

Figure 7-15

Under **Remote Secure Group**, you have two additional options: Host and Any.

- **Host -** If you select Host for the Remote Secure Group, then the Remote Secure Group will be the same as the Remote Security Gateway setting: IP Address, FQDN (Fully Qualified Domain Name), or Any. (Remote Security Gateway settings are explained on the following page.) In the example shown in Figure 7-16, the Remote Secure Group is the same as the Remote Security Gateway, set to a specific IP Address.



This Tunnel: ● Enable ○ Disable

Tunnel Name: Branch Office 1

Local Secure Group: IP Addr. IP: 192 . 168 . 1 . 1

Remote Secure Group: Host (the same as Remote Security Gateway setting!)

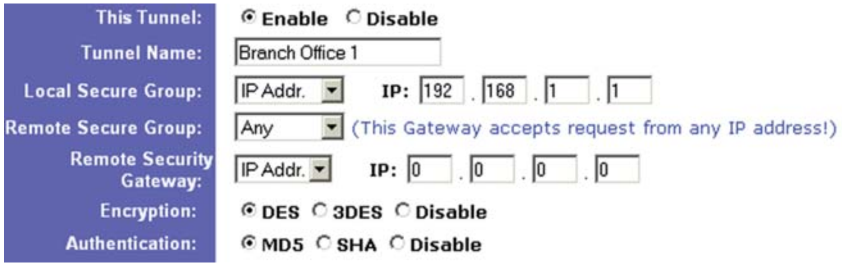
Remote Security Gateway: IP Addr. IP: 0 . 0 . 0 . 0

Encryption: ● DES ○ 3DES ○ Disable

Authentication: ● MD5 ○ SHA ○ Disable

Figure 7-16

- **Any -** If you select Any for the Remote Security Group, as shown in Figure 7-17, the local Firewall Router will accept a request from any IP address. This setting should be chosen when the other endpoint is using DHCP or PPPoE on the WAN side.



This Tunnel: ● Enable ○ Disable

Tunnel Name: Branch Office 1

Local Secure Group: IP Addr. IP: 192 . 168 . 1 . 1

Remote Secure Group: Any (This Gateway accepts request from any IP address!)

Remote Security Gateway: IP Addr. IP: 0 . 0 . 0 . 0

Encryption: ● DES ○ 3DES ○ Disable

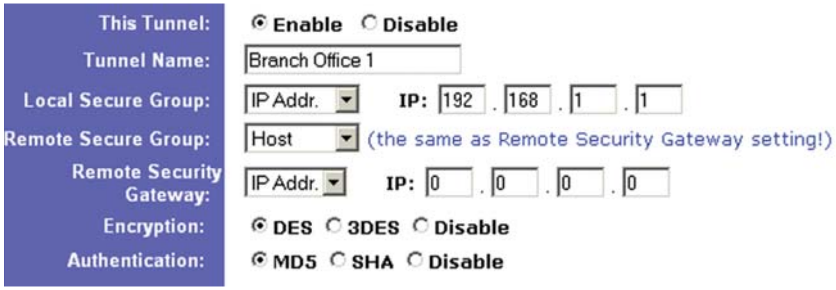
Authentication: ● MD5 ○ SHA ○ Disable

Figure 7-17

Remote Security Gateway

The Remote Security Gateway is the VPN device, such as a second Firewall Router, on the remote end of the VPN tunnel. Under **Remote Security Gateway**, you have three options: IP Address, FQDN, and Any.

- **IP Address -** If you select IP Address, as shown in Figure 7-18, enter the IP Address of the VPN device at the other end of the tunnel. The remote VPN device can be another Firewall Router, a VPN Server, or a computer with VPN client software that supports IPSec. The IP Address may either be static (permanent) or dynamic (changing), depending on the settings of the remote VPN device. Make sure that you have entered the IP Address correctly, or the connection cannot be made. Remember, this is NOT the IP Address of the local Firewall Router, but the IP Address of the remote Firewall Router or device with which you wish to communicate.



This Tunnel: ● Enable ○ Disable

Tunnel Name: Branch Office 1

Local Secure Group: IP Addr. IP: 192 . 168 . 1 . 1

Remote Secure Group: Host (the same as Remote Security Gateway setting!)

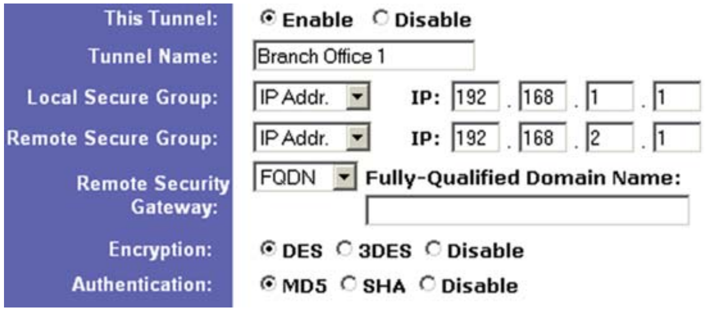
Remote Security Gateway: IP Addr. IP: 0 . 0 . 0 . 0

Encryption: ● DES ○ 3DES ○ Disable

Authentication: ● MD5 ○ SHA ○ Disable

Figure 7-18

- **FQDN** (Fully Qualified Domain Name) **-** If you select FQDN, as shown in Figure 7-19, enter the FQDN of the VPN device at the other end of the tunnel. The remote VPN device can be another Firewall Router, a VPN Server, or a computer with VPN client software that supports IPSec. The FQDN is the host name and domain name for a specific computer on the Internet, for example, *vpn.myvpnserver.com*.



This Tunnel: ● Enable ○ Disable

Tunnel Name: Branch Office 1

Local Secure Group: IP Addr. IP: 192 . 168 . 1 . 1

Remote Secure Group: IP Addr. IP: 192 . 168 . 2 . 1

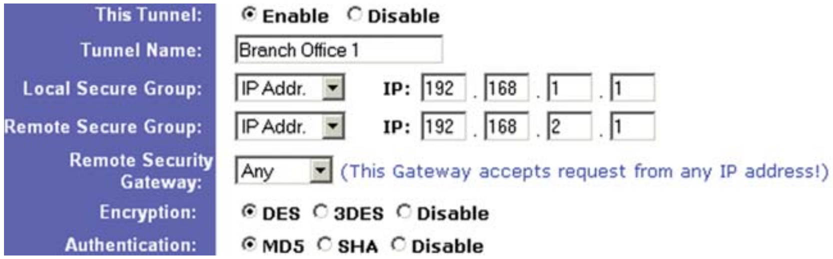
Remote Security Gateway: FQDN Fully-Qualified Domain Name:

Encryption: ● DES ○ 3DES ○ Disable

Authentication: ● MD5 ○ SHA ○ Disable

Figure 7-19

- **Any -** If you select Any for the Remote Security Gateway, as shown in Figure 7-20, the VPN device at the other end of the tunnel will accept a request from any IP address. The remote VPN device can be another Firewall Router, a VPN Server, or a computer with VPN client software that supports IPSec. If the remote user has an unknown or dynamic IP address (such as a professional on the road or a telecommuter using DHCP or PPPoE), then Any should be selected.



This Tunnel: ● Enable ○ Disable
Tunnel Name: Branch Office 1
Local Secure Group: IP Addr. IP: 192 . 168 . 1 . 1
Remote Secure Group: IP Addr. IP: 192 . 168 . 2 . 1
Remote Security Gateway: Any (This Gateway accepts request from any IP address!)
Encryption: ● DES ○ 3DES ○ Disable
Authentication: ● MD5 ○ SHA ○ Disable

Figure 7-20

Encryption

Using **Encryption** also helps make your connection more secure. There are two different types of encryption: **DES** or **3DES** (3DES is recommended because it is more secure). You may choose either of these, but it must be the same type of encryption that is being used by the VPN device at the other end of the tunnel. Or, you may choose not to encrypt by selecting **Disable**.

Authentication

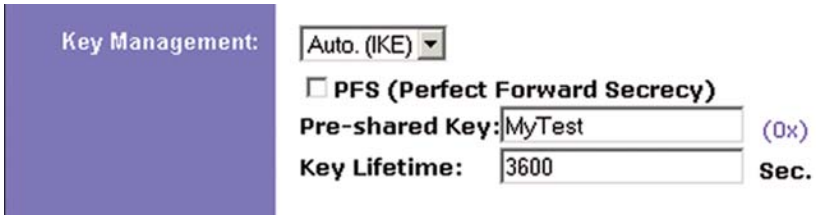
Authentication acts as another level of security. There are two types of authentication: **MD5** and **SHA** (SHA is recommended because it is more secure). As with encryption, either of these may be selected, provided that the VPN device at the other end of the tunnel is using the same type of authentication. Or, both ends of the tunnel may choose to **Disable** authentication.

Key Management

In order for any encryption to occur, the two ends of the tunnel must agree on the type of encryption and the way the data will be decrypted. This is done by sharing a "key" to the encryption code. Under **Key Management**, you may choose automatic or manual key management.

Automatic Key Management

Select **Auto (IKE)** and enter a series of numbers or letters in the Pre-shared Key field. Check the box next to **PFS (Perfect Forward Secrecy)** to ensure that the initial key exchange and IKE proposals are secure. In the example shown in Figure 7-21, the word **MyTest** is used. Based on this word, which MUST be entered at both ends of the tunnel if this method is used, a key is generated to scramble (encrypt) the data being transmitted over the tunnel, where it is unscrambled (decrypted). You may use any combination of up to 24 numbers or letters in this field. No special characters or spaces are allowed. In the Key Lifetime field, you may optionally select to have the key expire at the end of a time period of your choosing. Enter the number of seconds you'd like the key to be useful, or leave it blank for the key to last indefinitely.



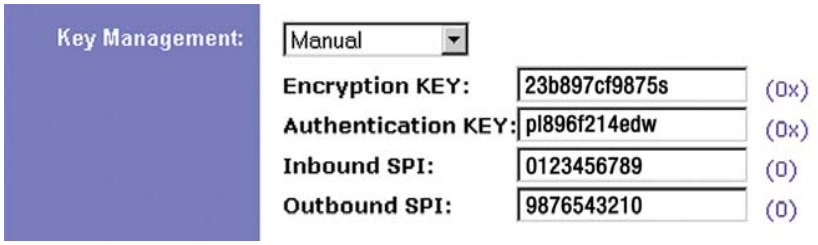
Key Management: Auto. (IKE)
☐ PFS (Perfect Forward Secrecy)
Pre-shared Key: MyTest (0x)
Key Lifetime: 3600 Sec.

Figure 7-21

Manual Key Management

Similarly, you may choose **Manual** keying, which allows you to generate the key yourself. Enter your **key** into the Encryption KEY field. Then enter an **Authentication KEY** into that field. These fields must both match the information that is being entered in the fields at the other end of the tunnel. The example in Figure 7-22 shows some sample entries for both the Encryption and Authentication Key fields. Up to 24 alphanumeric characters are allowed to create the Encryption Key. Up to 20 alphanumeric characters are allowed to create the Authentication Key.

The **Inbound SPI** and **Outbound SPI** fields are different, however. The Inbound SPI value set here must match the *Outbound SPI* value at the other end of the tunnel. The Outbound SPI here must match the *Inbound SPI* value at the other end of the tunnel. In the example (see Figure7-22), the Inbound SPI and Outbound SPI values shown would be opposite on the other end of the tunnel. Only numbers can be used in these fields. After you click the Apply button, hexadecimal characters (series of letters and numbers) are displayed in the Inbound SPI and Outbound SPI fields.

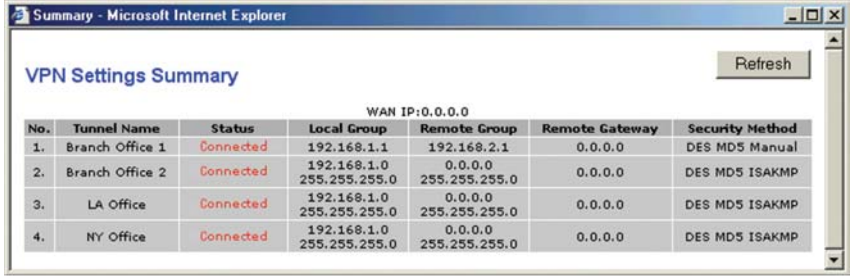


Key Management: Manual
Encryption KEY: 23b897cf9875s (0x)
Authentication KEY: pl896f214edw (0x)
Inbound SPI: 0123456789 (0)
Outbound SPI: 9876543210 (0)

Figure 7-22

Once you are satisfied with all your settings, click the **Apply** button. If you make any mistakes, clicking the **Cancel** button will exit the screen without saving any changes, provided that you have not already clicked the Apply button.

After the VPN device is set up at the other end of the tunnel, you may click the **Connect** button to use the tunnel. This assumes that both ends of the tunnel have a physical connection to each other (e.g., over the Internet, physical wiring, etc.). After clicking the Connect button, click the **Summary** button. If the connection is made, the screen shown in Figure 7-23 will appear:

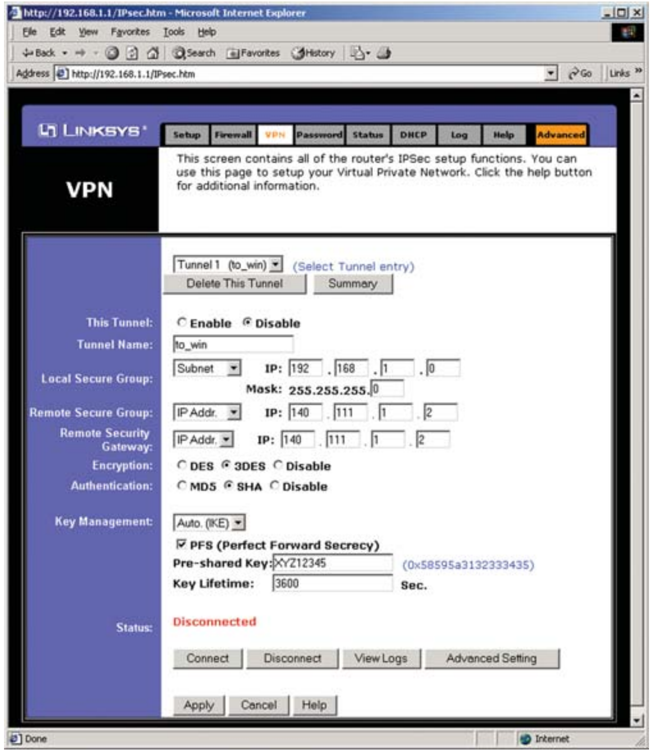


VPN Settings Summary

WAN IP:0.0.0.0

No.	Tunnel Name	Status	Local Group	Remote Group	Remote Gateway	Security Method
1.	Branch Office 1	Connected	192.168.1.1	192.168.2.1	0.0.0.0	DES MD5 Manual
2.	Branch Office 2	Connected	192.168.1.0 255.255.255.0	0.0.0.0 255.255.255.0	0.0.0.0	DES MD5 ISAKMP
3.	LA Office	Connected	192.168.1.0 255.255.255.0	0.0.0.0 255.255.255.0	0.0.0.0	DES MD5 ISAKMP
4.	NY Office	Connected	192.168.1.0 255.255.255.0	0.0.0.0 255.255.255.0	0.0.0.0	DES MD5 ISAKMP

Figure 7-23


http://192.168.1.1/IPsec.htm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.1.1/IPsec.htm Go Links
LINKSYS
Setup Firewall VPN Password Status DHCP Log Help Advanced
VPN
Delete This Tunnel
Summary
Connect
Disconnect
View Logs
Advanced Setting
Apply
Cancel
Help
Done
Internet

This screen contains all of the router's IPSec setup functions. You can use this page to setup your Virtual Private Network. Click the help button for additional information.

Tunnel 1 (to_win) (Select Tunnel entry)
This Tunnel: ○ Enable ● Disable
Tunnel Name: to_win
Local Secure Group: Subnet IP: 192 . 168 . 1 . 0
Mask: 255.255.255.0
Remote Secure Group: IP Addr. IP: 140 . 111 . 1 . 2
Remote Security Gateway: IP Addr. IP: 140 . 111 . 1 . 2
Encryption: ○ DES ● 3DES ○ Disable
Authentication: ○ MD5 ● SHA ○ Disable
Key Management: Auto. (IKE)
☑ PFS (Perfect Forward Secrecy)
Pre-shared Key: XYZ12345 (0x58595a3132333435)
Key Lifetime: 3600 Sec.
Status: Disconnected

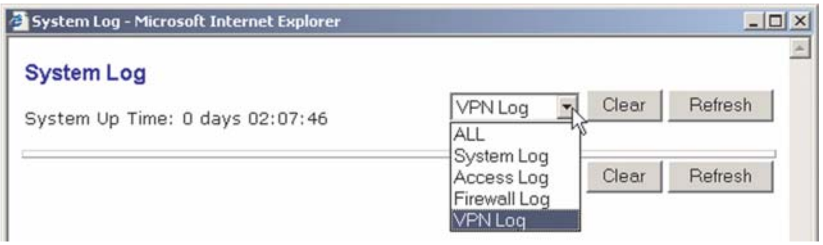
Figure 7-24

On the VPN screen, the word **Connected** should appear beside Status if the connection is successful. The other fields reflect the information that you entered on the VPN screen to make the connection.

If **Disconnected** appears under Status, as shown in Figure 7-24, some problem exists that prevents the creation of the tunnel. Make sure that all of your wiring is securely connected. Double-check all the values you entered on the VPN screen to make sure they are correct. If the other end of the tunnel is some distance from you (e.g., in another city, etc.), call to make sure that the settings on that end of the tunnel are correct as well.

If, for any reason, you experience a temporary disconnection, the connection will be re-established as long as the settings on both ends of the tunnel stay the same.

To get more details concerning your tunnel connection, click the **View Logs** button. The screen in Figure 7-25 will appear:



System Log - Microsoft Internet Explorer

System Log

System Up Time: 0 days 02:07:46

Figure 7-25

Select the log you wish to view: All (to view all logs), System Log, Access Log, Firewall Log, or VPN Log. The System Log screen displays a list of cold and warm starts, web login successes and failures, and packet filtering policies. The Access Log shows all incoming and outgoing traffic. The Firewall Log lists activities performed by the firewall to prevent DoS attacks, including URL filtering and time filtering. The VPN Log screen displays successful connections, transmissions and receptions, and the types of encryption used.

Once you no longer have need of the tunnel, simply click the **Disconnect** button on the bottom of the VPN page.

To change advanced settings, select the **tunnel** whose advanced settings you wish to change. Then, click the **Advanced Setting** button to change the Advanced Settings for a specific VPN tunnel.

Advanced Settings for Selected IPSec Tunnel

From the Advanced Settings screen, shown in Figure 7-26, you can adjust the settings for specific VPN tunnels.

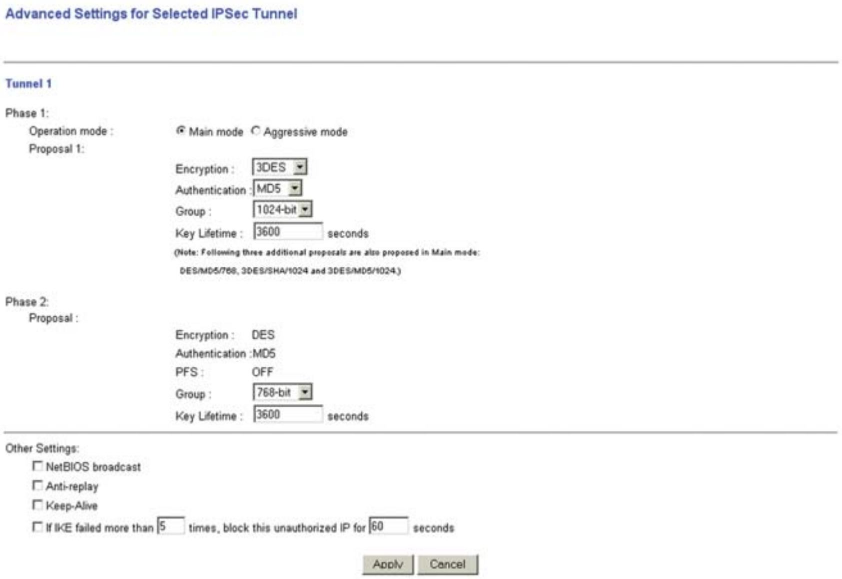
Phase 1

Phase 1 is used to create a security association (SA), often called the IKE SA. After Phase 1 is completed, Phase 2 is used to create one or more IPSec SAs, which are then used to key IPSec sessions.

Operation Mode

There are two modes: Main and Aggressive, and they exchange the same IKE payloads in different sequences. Main mode is more common; however, some people prefer Aggressive mode because it is faster. Main mode is for normal usage and includes more authentication requirements than Aggressive mode. Main mode is recommended because it is more secure. No matter which mode is selected, the VPN Router will accept both Main and Aggressive requests from the remote VPN device.

Encryption



Advanced Settings for Selected IPSec Tunnel

Tunnel 1

Phase 1:
Operation mode : ● Main mode ○ Aggressive mode
Proposal 1:
Encryption : 3DES
Authentication : MD5
Group : 1024-bit
Key Lifetime : 3600 seconds
(Note: Following three additional proposals are also proposed in Main mode: DES/MD5/768, 3DES/SHA/1024 and 3DES/MD5/1024.)

Phase 2:
Proposal :
Encryption : DES
Authentication : MD5
PFS : OFF
Group : 768-bit
Key Lifetime : 3600 seconds

Other Settings:
□ NetBIOS broadcast
□ Anti-replay
□ Keep-Alive
□ If IKE failed more than 5 times, block this unauthorized IP for 60 seconds

Figure 7-26

Select the length of the key used to encrypt/decrypt ESP packets. There are two choices: DES and 3DES. 3DES is recommended because it is more secure.

Authentication

Select the method used to authenticate ESP packets. There are two choices: MD5 and SHA. SHA is recommended because it is more secure.

Group

There are two Diffie-Hellman Groups to choose from: 768-bit and 1024-bit. Diffie-Hellman refers to a cryptographic technique that uses public and private keys for encryption and decryption.

Key Lifetime

In the Key Lifetime field, you may optionally select to have the key expire at the end of a time period of your choosing. Enter the number of seconds you'd like the key to be used until a re-key negotiation between each endpoint is completed.

Phase 2

Group

There are two Diffie-Hellman Groups to choose from: 768-bit and 1024-bit. Diffie-Hellman refers to a cryptographic technique that uses public and private keys for encryption and decryption.

Key Lifetime

In the Key Lifetime field, you may optionally select to have the key expire at the end of a time period of your choosing. Enter the number of seconds you'd like the key to be used until a re-key negotiation between each endpoint is completed.

Other Settings

NetBIOS broadcast

Check the box next to NetBIOS broadcast to enable NetBIOS traffic to pass through the VPN tunnel.

Anti-replay

Check the box next to Anti-replay to enable the Anti-replay protection. This feature keeps track of sequence numbers as packets arrive, ensuring security at the IP packet-level.

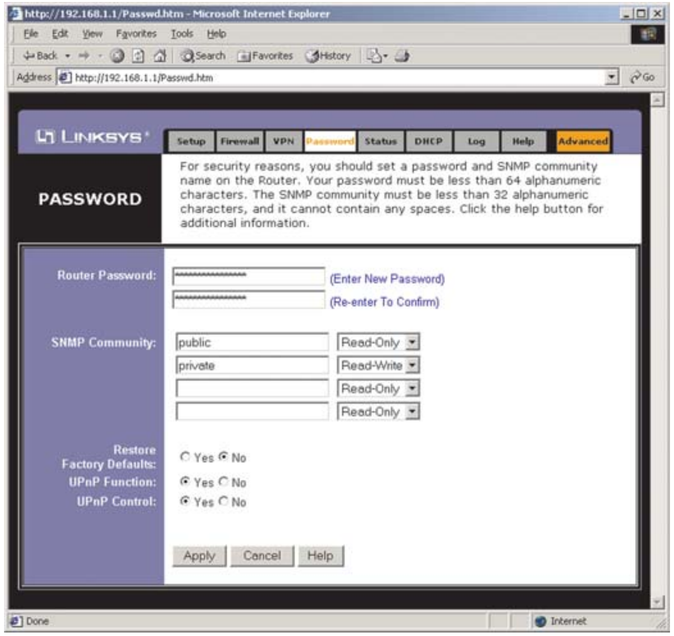
Keep-Alive

Check the box next to Keep-Alive to re-establish the VPN tunnel connection whenever it is dropped. Once the tunnel is initialized, this feature will keep the tunnel connected for the specified amount of idle time.

Unauthorized IP Blocking

Check this box to block unauthorized IP addresses. Complete the on-screen sentence to specify how many times IKE must fail before blocking that unauthorized IP address for a length of time that you specify (in seconds).

Password


http://192.168.1.1/Passwd.htm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.1.1/Passwd.htm
Go
LINKSYS
Setup Firewall VPN Password Status DHCP Log Help Advanced
Apply Cancel Help
Done
Internet

PASSWORD

For security reasons, you should set a password and SNMP community name on the Router. Your password must be less than 64 alphanumeric characters. The SNMP community must be less than 32 alphanumeric characters, and it cannot contain any spaces. Click the help button for additional information.

Router Password: **************** (Enter New Password)
**************** (Re-enter To Confirm)

SNMP Community: public Read-Only
private Read-Write
Read-Only
Read-Only

Restore Factory Defaults: ○ Yes ● No
UPnP Function: ● Yes ○ No
UPnP Control: ● Yes ○ No

Figure 7-27

The Password screen, shown in Figure 7-27, allows you to change the password, set SNMP Community names, enable UPnP Services, and restore default settings on the Router.

Router Password It is *strongly* recommended that you set a password for the Router. The default password is **admin**. If you don't change the password, all users on your network will be able to access the Router using the default password **admin**.

SNMP Community Each SNMP Community field allows a name to be assigned to any SNMP community that has been set up in the network. Four different communities can be defined, including the two default communities, public and private. For each SNMP Community name, you can configure each community's accessibility, making it either **Read-Only** or **Read-Write**.

Restore Factory Defaults If you select the **Restore Factory Defaults** option and click the **Apply** button, you will clear all of the Router's settings.

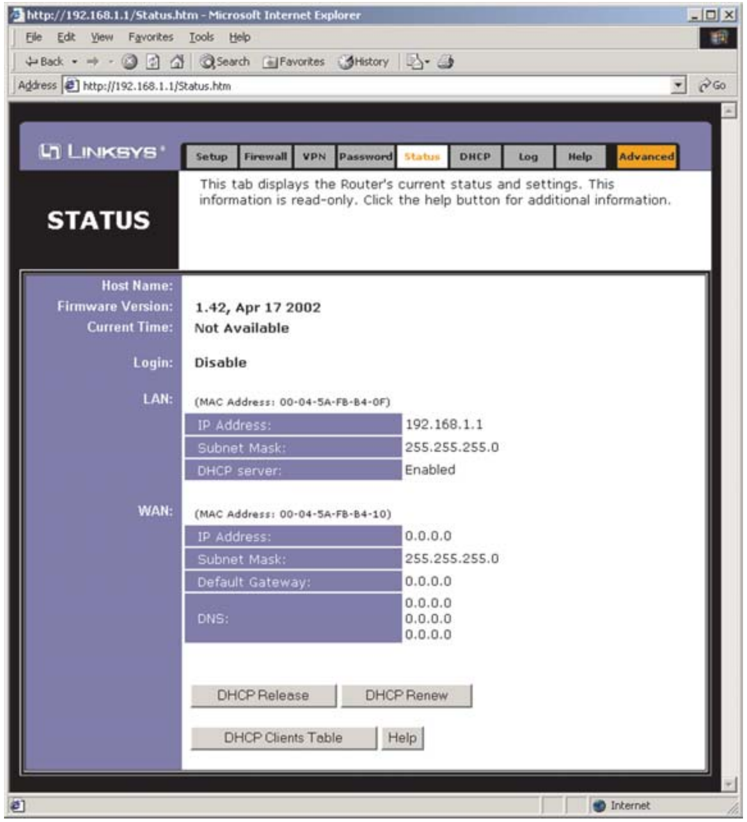
Do not restore the factory defaults unless you are having difficulties with the Router and have exhausted all other troubleshooting measures. Once the Router is reset, you will have to re-enter all of your configuration data.

UPnP Function Universal Plug and Play (UPnP) allows Windows XP to automatically configure the Router for various Internet applications, such as gaming and videoconferencing. To enable the use of UPnP, click the **Yes** radio button next to UPnP Function, or click the **No** radio button to disable the use of UPnP.

UPnP Control This feature allows Windows XP to read and write UPnP Forwarding using UPnP. To enable this feature, click the **Yes** radio button next to UPnP Control, or click the **No** radio button to disable this feature. If disabled, UPnP Forwarding can only be read.

To apply any of the settings you change on a page, click the **Apply** button, and then click the **Continue** button. To cancel any values you've entered on any page, click the **Cancel** button.

Status


http://192.168.1.1/Status.htm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.1.1/Status.htm
Go
LINKSYS
Setup
Firewall
VPN
Password
Status
DHCP
Log
Help
Advanced
STATUS
DHCP Release
DHCP Renew
DHCP Clients Table
Help
Internet

This tab displays the Router's current status and settings. This information is read-only. Click the help button for additional information.

Host Name:
Firmware Version: 1.42, Apr 17 2002
Current Time: Not Available

Login: Disable

LAN: (MAC Address: 00-04-5A-FB-B4-0F)

IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
DHCP server:	Enabled

WAN: (MAC Address: 00-04-5A-FB-B4-10)

IP Address:	0.0.0.0
Subnet Mask:	255.255.255.0
Default Gateway:	0.0.0.0
DNS:	0.0.0.0 0.0.0.0 0.0.0.0

Figure 7-28

The Status screen, shown in Figure 7-29, displays the Router's current status and reflects the data and selections you've entered using the Setup screen.

> **Note:** The information provided and buttons available may vary depending on the Router's settings.

All of the information provided on this screen is read-only. To make changes, select the Setup tab.

Host Name This field shows the name of the Router. This entry is necessary for some ISPs.

Firmware Version This field shows the installed version and date of the firmware. Version dates are slightly more accurate than version numbers.

Current Time Based upon the time zone selection made on the Setup tab, this field will display the current time.

Login This indicates if you are using a dial-up style connection like PPPoE, RAS, PPTP, or HBS. For PPPoE, RAS, PPTP, or HBS only, there is a **Connect** button to click if you are disconnected and want to re-establish a connection.

LAN These fields display the current IP Address and Subnet Mask of the Router, as seen by users on your local area network. The DHCP Server field shows the status of the Router's DHCP server function, which is either enabled or disabled.

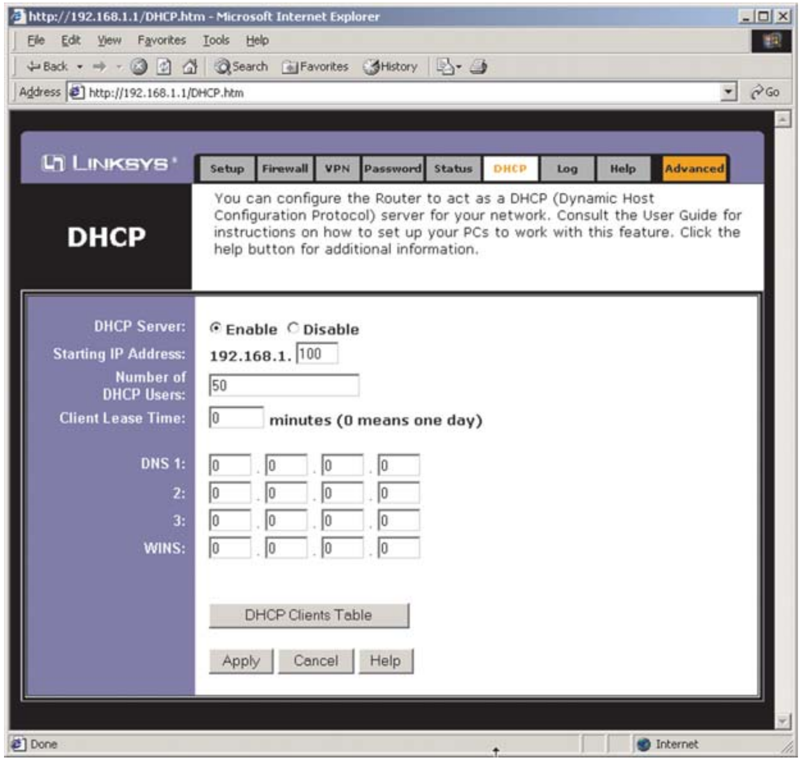
WAN These fields display the WAN IP Address, WAN Subnet Mask, and WAN Default Gateway IP Address of the Router, as seen by external users on the Internet. The DNS (Domain Name System) IP Address fields show the IP address(es) of the DNS currently used by the Router. Multiple DNS IP settings are common. In most cases, the first available DNS entry is used.

DHCP Release Click the **DHCP Release** button to release the current IP address of the device connected to the Router's WAN port.

DHCP Renew Click the **DHCP Renew** button to replace the current IP address—of the device connected to the Router's WAN port—with a new IP address.

DHCP Clients Table Click the **DHCP Clients Table** button to view the list of PCs that were given IP addresses by the Router.

DHCP


http://192.168.1.1/DHCP.htm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.1.1/DHCP.htm
Go
LINKSYS
Setup Firewall VPN Password Status DHCP Log Help Advanced
DHCP
DHCP Clients Table
Apply Cancel Help
Done
Internet

You can configure the Router to act as a DHCP (Dynamic Host Configuration Protocol) server for your network. Consult the User Guide for instructions on how to set up your PCs to work with this feature. Click the help button for additional information.

DHCP Server: ● Enable ○ Disable

Starting IP Address: 192.168.1. 100

Number of DHCP Users: 50

Client Lease Time: 0 minutes (0 means one day)

DNS 1: 0 . 0 . 0 . 0

2: 0 . 0 . 0 . 0

3: 0 . 0 . 0 . 0

WINS: 0 . 0 . 0 . 0

Figure 7-29

From the DHCP screen, shown in Figure 7-29, you can configure the Router as a DHCP Server.

A Dynamic Host Configuration Protocol (DHCP) server automatically assigns an IP address to each PC on your network for you. Unless you already have one, it is highly recommended that you leave the Router enabled as a DHCP server.

DHCP Server DHCP is already enabled by factory default. If you already have a DHCP server on your network, set the Router's DHCP option to **Disable**. Click the **Apply** button and then the **Continue** button. If you disable DHCP, remember to assign a static IP address to the Router.

Starting IP Address Enter a value for the DHCP server to start with when issuing IP addresses. This value must be 192.168.1.2 or greater, because the default IP address for the Router is **192.168.1.1**.

Number of DHCP Users (Optional) Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. This number cannot be greater than 253. In order to determine the DHCP IP Address range, add the starting IP address (e.g., 100) to the number of DHCP users. By default, as shown in Figure 7-28, add 100 to 50, and the range is 192.168.1.100 to 192.168.1.149.

Client Lease Time The Client Lease Time is the amount of time a network user will be allowed connection to the Router with their current dynamic IP address. Enter the amount of time, in minutes, that the user will be "leased" this dynamic IP address.

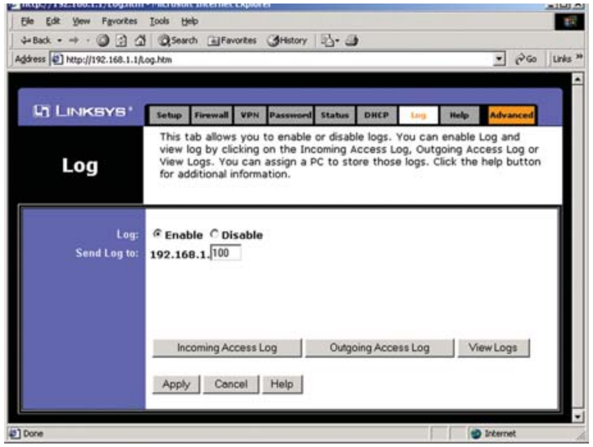
DNS The Domain Name System (DNS) is how the Internet translates domain or website names into Internet addresses or URLs. Your ISP will provide you with at least one DNS Server IP Address. If you wish to use another, type that **IP Address** in one of these fields. You can type up to three DNS Server IP Addresses here. The Router will use these for quicker access to functioning DNS servers. Otherwise, leave this blank.

WINS The Windows Internet Naming Service (WINS) manages each PC's interaction with the Internet. If you use a WINS server, enter that **server's IP Address** here. Otherwise, leave this blank.

DHCP Clients Table Click the **DHCP Clients Table** button to show the current DHCP Client data. (This data is stored in temporary memory and changes periodically.)

To apply any of the settings you change on a page, click the **Apply** button, and then click the **Continue** button. To cancel any values you've entered on any page, click the **Cancel** button.

Log


File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.1.1/Log.htm
Go Links
LINKSYS
Setup Firewall VPN Password Status DHCP Log Help Advanced
Log
Done
Internet

This tab allows you to enable or disable logs. You can enable Log and view log by clicking on the Incoming Access Log, Outgoing Access Log or View Logs. You can assign a PC to store those logs. Click the help button for additional information.

Log: ● Enable ○ Disable

Send Log to: 192.168.1.100

Incoming Access Log | Outgoing Access Log | View Logs

Apply | Cancel | Help

Figure 7-30

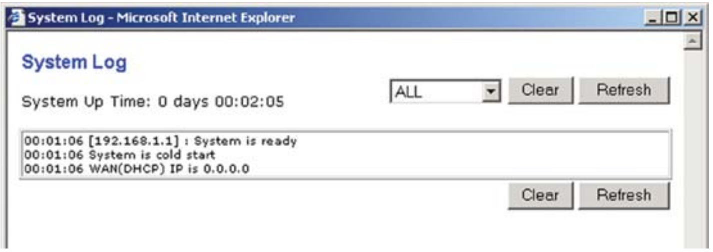
The Log tab, shown in Figure 7-30, provides you with a log of all incoming and outgoing URLs or IP addresses for your Internet connection.

To access activity logs, select the **Enable** option next to Log. This function can be disabled by clicking the **Disable** radio button.

With logging enabled, you can choose to view temporary logs or have a permanent record, using the Logviewer software. Temporary logs can be accessed from the Log screen by clicking either the **Incoming Access Log** or **Outgoing Access Log** button. The Incoming Access Log gives you a log of all the incoming Internet traffic while the Outgoing Access Log lists all the URLs and IP addresses of Internet sites that users on your network have accessed.

For a permanent record of these logs, Logviewer software must be used. This software is downloadable from the Linksys website, *www.linksys.com*. The Logviewer saves all incoming and outgoing activity as a permanent file on your PC's hard drive. In the *Send Log to* field, enter the fixed IP address of the PC running the Logviewer software. The Router will now send updated logs to that PC.

Click the **View Logs** button for a selection of logs to view (see Figure 7-31).



System Up Time: 0 days 00:02:05

```
00:01:06 [192.168.1.1] : System is ready
00:01:06 System is cold start
00:01:06 WAN(DHCP) IP is 0.0.0.0
```

Figure 7-31

From the drop-down menu, select the log you wish to view: All (to view all logs), System Log, Access Log, Firewall Log, or VPN Log.

- **System Log** The System Log screen displays a list of cold and warm starts, web login successes and failures, and packet filtering policies.
- **Access Log** The Access Log screen shows all incoming and outgoing traffic.
- **Firewall Log** The Firewall Log screen lists activities performed by the firewall to prevent DoS attacks, including URL filtering and time filtering.
- **VPN Log** The VPN Log screen displays successful connections, transmissions and receptions, and the types of encryption used.

To clear a log, click the **Clear** button. To refresh a log, click the **Refresh** button. To return to the Log screen, close this window.

To clear any values you've entered on any page, click **Cancel** and re-enter information. To apply any settings you've altered on any page, click the **Apply** button. Once all settings are correct, click **Continue**.

Help

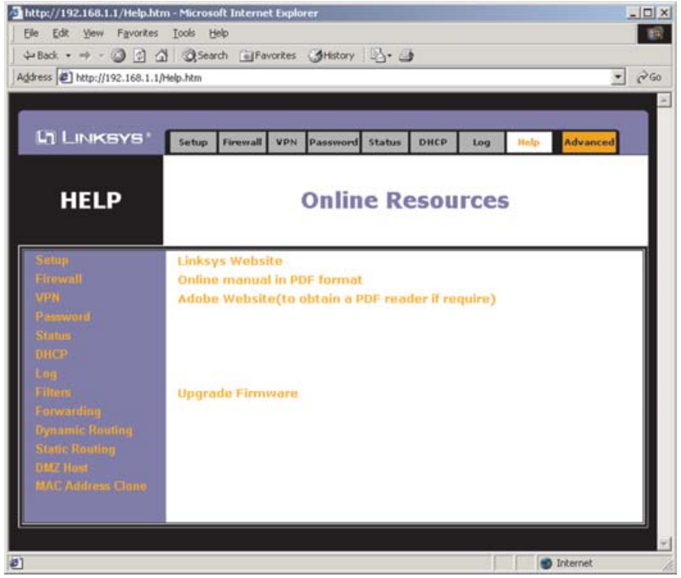

http://192.168.1.1/Help.htm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.1.1/Help.htm
Go
LINKSYS
Setup
Firewall
VPN
Password
Status
DHCP
Log
Help
Advanced
HELP
Online Resources
Setup
Firewall
VPN
Password
Status
DHCP
Log
Filters
Forwarding
Dynamic Routing
Static Routing
DMZ Host
MAC Address Clone
Linksys Website
Online manual in PDF format
Adobe Website(to obtain a PDF reader if require)
Upgrade Firmware
Internet

Figure 7-32

Under the Help tab, shown in Figure 7-32, you'll find links to all of the Utility's internal support documentation, including the application that upgrades the Router's firmware.

Clicking on any of the topics in the bar on the left will give you help information about that topic.

Clicking the Linksys Website link will take you to Linksys's website, *www.linksys.com*, provided you are connected to the Internet.

Clicking the Online manual in PDF format link will take you to the latest version of the user guide for this Router. The guide will be in Adobe Acrobat Portable Document File (.pdf) format. You will need the Adobe Acrobat Reader to view this pdf. If you do not have the Acrobat Reader, click the Adobe Website link to download it.

New firmware versions are posted at *www.linksys.com* and can be downloaded for free. If the Router can access the Internet already, there's no need to download a newer firmware version, unless that version has a new feature that you want to use. Loading new firmware onto the Router does not always enhance the speed or the quality of your connection.

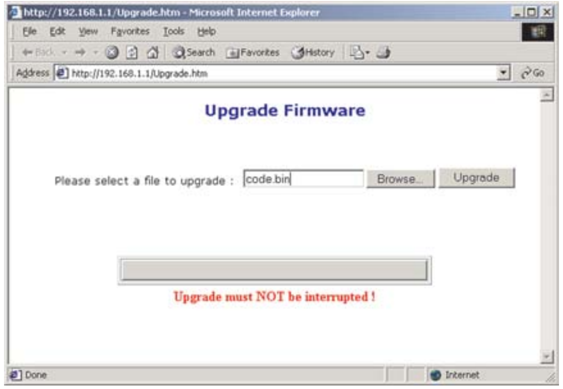
To upgrade the Router’s firmware:

Note: By upgrading the Router’s firmware, you may lose the Router’s configuration settings.

1. Select the **Help** tab (see Figure 7-32).

2. Click **Upgrade Firmware** to display the windo shown in Figure 7-33.

3. Click the **Browse** button to find the firmware upgrade file that you downloaded from the Linksys website and then extracted.


http://192.168.1.1/Upgrade.htm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.1.1/Upgrade.htm
Go
Browse...
Upgrade
Done
Internet

Upgrade Firmware

Please select a file to upgrade : code.bin

Upgrade must NOT be interrupted !

Figure 7-33

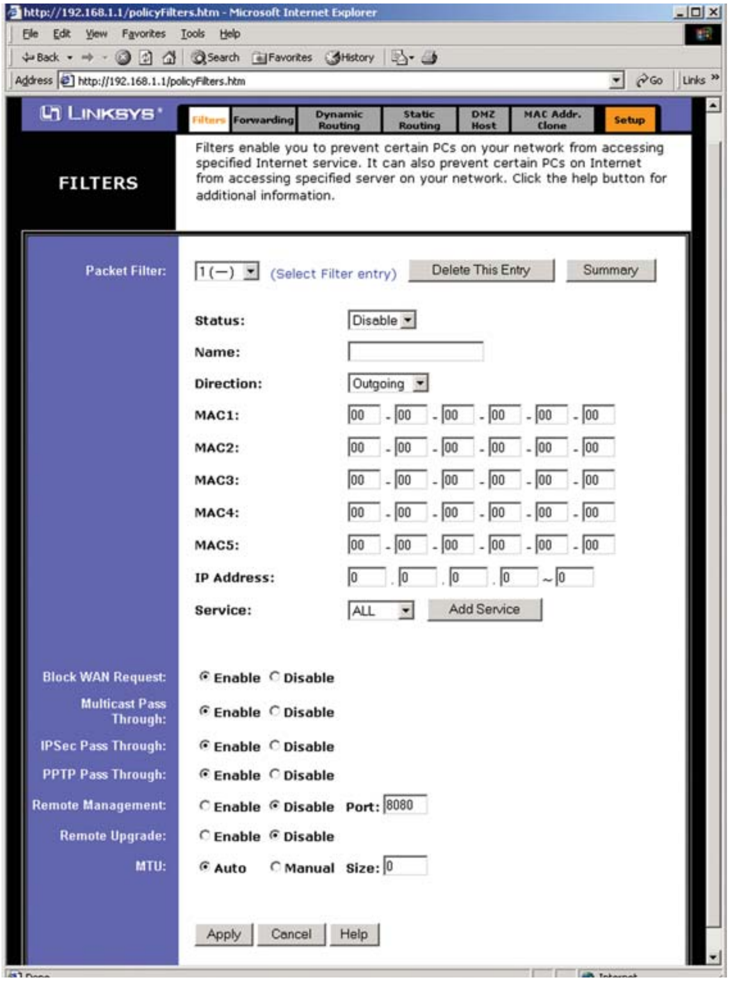
4. Double-click the **firmware file** you downloaded and extracted. Click the **Upgrade** button, and follow the instructions there.

Advanced

The following tabs are for advanced users or users whose setup needs require special configuration. When you click the Advanced tab, you will be able to set up these features. There are six additional tabs available.

- Filters - Allows you to set up packet filters and enable/disable IPSec or PPTP Pass-Through for Virtual Private Network (VPN) tunnels.
- Forwarding - Sets up public services on your network.
- Dynamic Routing - Sets up the Router so it will automatically adjust to physical changes in the network’s layout.
- Static Routing - Sets up static routes as needed when network information must travel to a specific host or network.
- DMZ Host - Allows one local user to be exposed to the Internet for use of special-purpose services such as online gaming or videoconferencing.
- MAC Address Cloning - Allows you to “clone” your Ethernet adapter’s MAC address onto the Router.

Filters


http://192.168.1.1/policyFilters.htm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.1.1/policyFilters.htm
Go
Links
LINKSYS
Filters
Forwarding
Dynamic Routing
Static Routing
DMZ Host
MAC Addr. Clone
Setup
FILTERS
Delete This Entry
Summary
Add Service
Apply
Cancel
Help
Done
Internet

Filters enable you to prevent certain PCs on your network from accessing specified Internet service. It can also prevent certain PCs on Internet from accessing specified server on your network. Click the help button for additional information.

Packet Filter: 1 (—) (Select Filter entry)

Status: Disable

Name:

Direction: Outgoing

MAC1: 00 - 00 - 00 - 00 - 00 - 00

MAC2: 00 - 00 - 00 - 00 - 00 - 00

MAC3: 00 - 00 - 00 - 00 - 00 - 00

MAC4: 00 - 00 - 00 - 00 - 00 - 00

MAC5: 00 - 00 - 00 - 00 - 00 - 00

IP Address: 0 . 0 . 0 . 0 ~ 0

Service: ALL

Block WAN Request: ● Enable ○ Disable

Multicast Pass Through: ● Enable ○ Disable

IPSec Pass Through: ● Enable ○ Disable

PPTP Pass Through: ● Enable ○ Disable

Remote Management: ○ Enable ● Disable Port: 8080

Remote Upgrade: ○ Enable ● Disable

MTU: ● Auto ○ Manual Size: 0

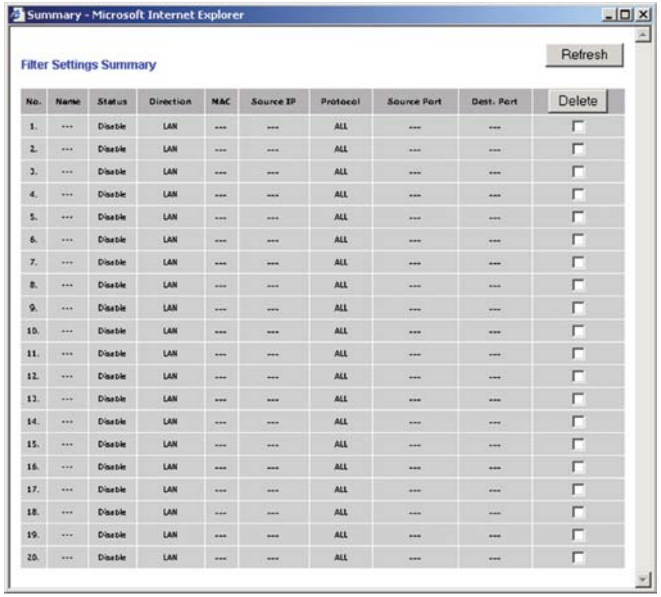
Figure 7-34

The Filters screen, shown in Figure 7-34, allows you to set up packet filters and enable/disable IPSec or PPTP Pass-Through for Virtual Private Network (VPN) tunnels. You can set up to 20 packet filters.

Packet Filter Select the number you wish to assign to a specific filter entry from the drop-down menu. Up to 20 packet filtering “rules” can be established.

Delete This Entry To delete a current packet filtering rule, select that rule from the Packet Filter Entry drop-down menu, and click this button.

Summary Clicking this button shows a summary of the settings and status of all packet rules, shown in Figure 7-35.



Summary - Microsoft Internet Explorer

Filter Settings Summary

Refresh

No.	Name	Status	Direction	MAC	Source IP	Protocol	Source Port	Dest. Port	Delete
1.	---	Disable	LAN	---	---	ALL	---	---	□
2.	---	Disable	LAN	---	---	ALL	---	---	□
3.	---	Disable	LAN	---	---	ALL	---	---	□
4.	---	Disable	LAN	---	---	ALL	---	---	□
5.	---	Disable	LAN	---	---	ALL	---	---	□
6.	---	Disable	LAN	---	---	ALL	---	---	□
7.	---	Disable	LAN	---	---	ALL	---	---	□
8.	---	Disable	LAN	---	---	ALL	---	---	□
9.	---	Disable	LAN	---	---	ALL	---	---	□
10.	---	Disable	LAN	---	---	ALL	---	---	□
11.	---	Disable	LAN	---	---	ALL	---	---	□
12.	---	Disable	LAN	---	---	ALL	---	---	□
13.	---	Disable	LAN	---	---	ALL	---	---	□
14.	---	Disable	LAN	---	---	ALL	---	---	□
15.	---	Disable	LAN	---	---	ALL	---	---	□
16.	---	Disable	LAN	---	---	ALL	---	---	□
17.	---	Disable	LAN	---	---	ALL	---	---	□
18.	---	Disable	LAN	---	---	ALL	---	---	□
19.	---	Disable	LAN	---	---	ALL	---	---	□
20.	---	Disable	LAN	---	---	ALL	---	---	□

Figure 7-35

Status Select **Allow** or **Deny** to restrict protocols to the users you specify in the Source MAC or Source IP fields. Select **Disable** to temporarily disable a specific packet filter.

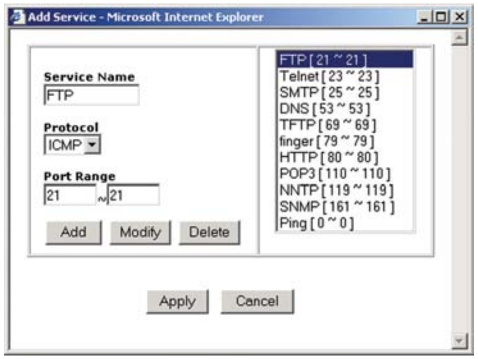
Name Enter a **name** for a specific packet filter entry. You can use up to 15 characters.

Direction Select **Incoming** or **Outgoing** to apply the packet filter rule to incoming or outgoing traffic.

MAC1-5 or IP Address In these fields, type the MAC Addresses or IP Address (or range of IP Addresses) of those PC(s) for which the rule will apply.

Service Select the service(s) to which the rule applies. Choices include All (all services), FTP, Telnet, SMTP, DNS, TFTP, HTTP, POP3, NNTP, SNMP, and Ping.

Click the **Add Service** button to add more services or edit the settings for a specific service. (Shown in Figure 7-36.) You can have up to 60 services, including default services such as FTP and Telnet.



Add Service - Microsoft Internet Explorer

Service Name: FTP

Protocol: ICMP

Port Range: 21 ~ 21

FTP [21 ~ 21]
Telnet [23 ~ 23]
SMTP [25 ~ 25]
DNS [53 ~ 53]
TFTP [69 ~ 69]
finger [79 ~ 79]
HTTP [80 ~ 80]
POP3 [110 ~ 110]
NNTP [119 ~ 119]
SNMP [161 ~ 161]
Ping [0 ~ 0]

Figure 7-36

Service Name Enter the name of the service in this field.

Protocol Select the protocol type for this rule from the drop-down menu, such as TCP, UDP, or ICMP.

Port Range Enter the range of ports for this entry.

Click the **Add** button to add a service. Click the **Modify** button to edit the settings for a service. Click the **Delete** button to delete a service.

Click the **Apply** button to make your changes. Click the **Cancel** button to undo your changes.

Blocking WAN Requests

- By enabling the Block WAN Request feature, you can prevent your network from being "pinged," or detected, by other Internet users. The Block WAN Request feature also reinforces your network security by hiding your network ports. Both functions of the Block WAN Request feature make it more difficult for outside users to work their way into your network.
- Click the **Apply** button and then the **Continue** button to save your changes.

Using Multicast Pass Through

- This feature allows for multiple transmissions to specific recipients at the same time. Select **Enable** to support the feature, or **Disable** to keep the Router from multicasting.

Using IPSec Pass Through

- This feature lets you use IPSec Pass Through. To use this feature, click the **Enable** button next to **IPSec Pass Through**, and then the **Apply** button. Click the **Continue** button.
- IPSec Pass Through is enabled by default. To disable IPSec Pass Through, click on **Disable** and then the **Apply** button. Click the **Continue** button.

Using PPTP Pass Through

- Point-to-Point Tunneling Protocol Pass Through is the method used to enable VPN sessions to a Windows NT 4.0 or 2000 server. To enable this feature, click the **Enable** button next to **PPTP Pass Through**, and click the **Apply** button. Then click the **Continue** button.
- PPTP Pass Through is enabled by default. To disable this feature, click on **Disable** next to **PPTP Pass Through**, and then the **Apply** button. Click the **Continue** button.

Using Remote Management

- This feature allows you to manage the Router from a remote location, via the Internet. To enable this feature, click on **Enable,** and enter the port number you want to use when accessing the Router remotely. Click the **Apply** button. Then click the **Continue** button. Remote Management must be activated before you can manage the Router from a remote location.
- To disable Remote Management, click on **Disable**, and click the **Apply** button. Then click the **Continue** button. If you wish to use this feature on the browser, enter **http:\\<WAN IP Address>: port.** (Enter your specific WAN IP Address in place of <WAN IP Address>, and enter the port number in place of the word port.)
- To disable this feature, click on **Disable**, and click the **Apply** button. Then click the **Continue** button.

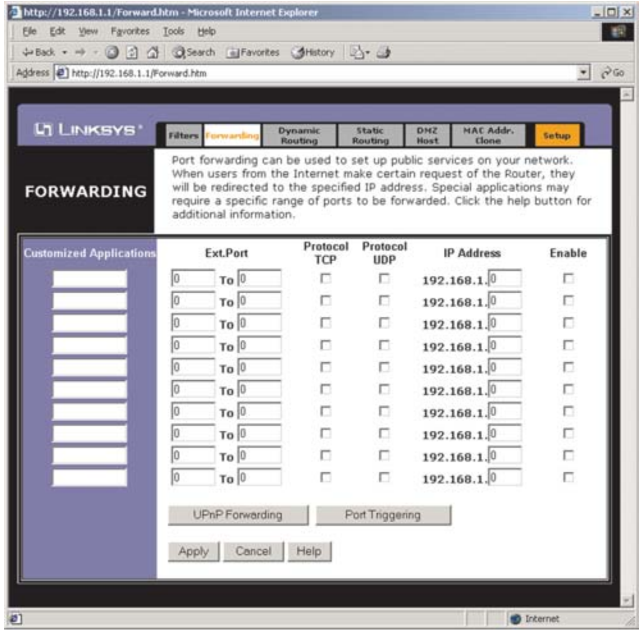
Using Remote Upgrade

- This feature allows you to upgrade the Router's firmware from a remote location. To enable Remote Upgrade, click on **Enable**, and then click the **Apply** button. Then click the **Continue** button. Remote Management must be activated before you can manage the Router from a remote location.

Using MTU (Maximum Transmission Unit)

- This feature specifies the largest packet size permitted for network transmission. Select **Auto** to leave the MTU at its factory default value. Select **Manual** to enable the MTU value you enter in the Size field. It is recommended that you keep this value in the 1200 to 1500 range. For most DSL users, it is recommended to use the value **1492**.

Forwarding


http://192.168.1.1/Forward.htm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.1.1/Forward.htm
Go
LINKSYS
Filters
Forwarding
Dynamic Routing
Static Routing
DMZ Host
MAC Addr. Clone
Setup
FORWARDING
UPnP Forwarding
Port Triggering
Apply
Cancel
Help
Internet

Port forwarding can be used to set up public services on your network. When users from the Internet make certain request of the Router, they will be redirected to the specified IP address. Special applications may require a specific range of ports to be forwarded. Click the help button for additional information.

Customized Applications	Ext.Port			Protocol TCP	Protocol UDP	IP Address	Enable
	0	To	0	□	□	192.168.1.0	□
	0	To	0	□	□	192.168.1.0	□
	0	To	0	□	□	192.168.1.0	□
	0	To	0	□	□	192.168.1.0	□
	0	To	0	□	□	192.168.1.0	□
	0	To	0	□	□	192.168.1.0	□
	0	To	0	□	□	192.168.1.0	□
	0	To	0	□	□	192.168.1.0	□
	0	To	0	□	□	192.168.1.0	□
	0	To	0	□	□	192.168.1.0	□

Figure 7-37

From the Forwarding tab, shown in Figure 7-37, you can set up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications. (Specialized Internet applications are any applications that use Internet access to perform functions such as videoconferencing or online gaming. Some Internet applications may not require any forwarding.) When users send this type of request to your network via the Internet, the Router will forward those requests to the appropriate PC. Before using Forwarding, the Router's DHCP function must be disabled under the DHCP tab and the computer must be assigned a new static LAN IP address because the IP address may change when using the DHCP server.

If you need to forward all ports to one PC, see the “DMZ Host” section.

To add a server using Forwarding:

1. Enter the **name** of the application in the appropriate Customized Applications field.

2. Next to the name of the application, enter the **number** or **range** of the external port(s) used by the server or Internet application in the Ext. Port column. Check with the Internet application software documentation for more information.

3. On the same line, select the protocol **UDP** or **TCP**, or select both protocols.

4. Enter the **IP address** of the server that you want the Internet users to be able to access. To find the IP address, go to “Appendix G: Finding the MAC Address and IP Address for Your Ethernet Adapter.”

5. Check the **Enable** box to enable the services you have defined. Port Range Forwarding will not function if the **Enable** button is left unchecked. This is disabled (unchecked) by default.

6. Configure as many entries as needed—the Router supports up to ten ranges of ports. Click the **Apply** button and **Continue** button when you are done.

UPnP Forwarding

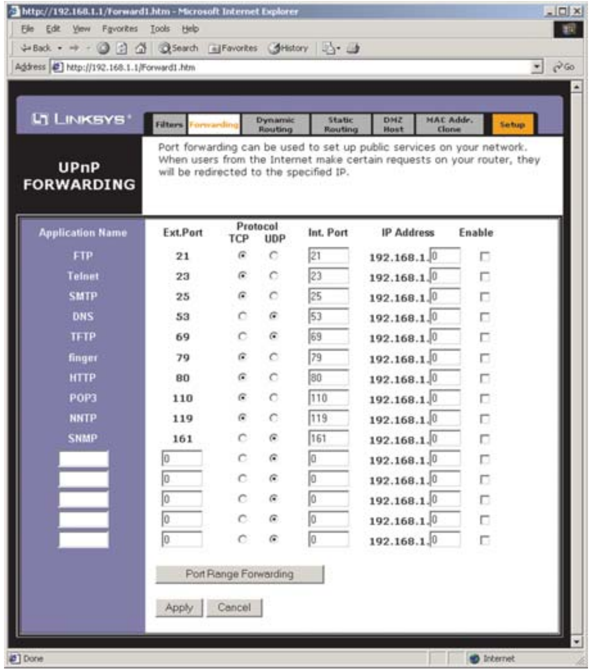
The UPnP Forwarding screen, shown in Figure 7-38, displays preset application settings as well as options for customization of port services for other applications.

The Preset Applications are among the most widely used Internet applications. They include the following:

- **FTP** (File Transfer Protocol) A protocol used to transfer files over a TCP/IP network (Internet, UNIX, etc.). For example, after developing the HTML pages for a website on a local machine, they are typically uploaded to the web server using FTP. FTP includes functions to log onto the network, list directories, and copy files. FTP operations can be performed by typing commands at a command prompt or via an FTP utility running under a graphical interface such as Windows. FTP transfers can also be initiated from within a web browser by entering the URL preceded by ftp://.

- **Telnet** A terminal emulation protocol commonly used on Internet and TCP/IP-based networks. It allows a user at a terminal or computer to log onto a remote device and run a program.

- **SMTP** (Simple Mail Transfer Protocol) The standard e-mail protocol on the Internet. It is a TCP/IP protocol that defines the message format and the message transfer agent (MTA), which stores and forwards the mail.


http://192.168.1.1/Forward1.htm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.1.1/Forward1.htm
Go
LINKSYS
Filters
Forwarding
Dynamic Routing
Static Routing
DMZ Host
MAC Addr. Clone
Setup
UPnP FORWARDING
Done
Internet

Port forwarding can be used to set up public services on your network. When users from the Internet make certain requests on your router, they will be redirected to the specified IP.

Application Name	Ext.Port	Protocol TCP	Protocol UDP	Int. Port	IP Address	Enable
FTP	21	●	○	21	192.168.1.0	□
Telnet	23	●	○	23	192.168.1.0	□
SMTP	25	●	○	25	192.168.1.0	□
DNS	53	○	●	53	192.168.1.0	□
TFTP	69	○	●	69	192.168.1.0	□
finger	79	●	○	79	192.168.1.0	□
HTTP	80	●	○	80	192.168.1.0	□
POP3	110	●	○	110	192.168.1.0	□
NNTP	119	●	○	119	192.168.1.0	□
SNMP	161	○	●	161	192.168.1.0	□
	0	○	●	0	192.168.1.0	□
	0	○	●	0	192.168.1.0	□
	0	○	●	0	192.168.1.0	□
	0	○	●	0	192.168.1.0	□
	0	○	●	0	192.168.1.0	□

Figure 7-38

- **DNS** (Domain Name System) The way that Internet domain names are located and translated into IP addresses. A domain name is a meaningful and easy-to-remember “handle” for an Internet address.

- **TFTP** (Trivial File Transfer Protocol) A version of the TCP/IP FTP protocol that has no directory or password capability.

- **Finger** A UNIX command widely used on the Internet to find out information about a particular user, such as a telephone number, whether the user is currently logged on, and the last time the user was logged on. The person being “fingered” must have placed his or her profile on the system in order for the information to be available. Fingering requires entering the full user@domain address.

- **HTTP** (HyperText Transport Protocol) The communications protocol used to connect to servers on the World Wide Web. Its primary function is to establish a connection with a web server and transmit HTML pages to the client web browser.

- **POP3** (Post Office Protocol 3) A standard mail server commonly used on the Internet. It provides a message store that holds incoming e-mail until users log on and download it. POP3 is a simple system with little selectivity. All pending messages and attachments are downloaded at the same time. POP3 uses the SMTP messaging protocol.

- **NNTP** (Network News Transfer Protocol) The protocol used to connect to Usenet groups on the Internet. Usenet newsreaders support the NNTP protocol.

- **SNMP** (Simple Network Management Protocol) A widely used network monitoring and control protocol. Data is passed from SNMP agents, which are hardware and/or software processes reporting activity in each network device (hub, router, bridge, etc.) to the workstation console used to oversee the network. The agents return information contained in a MIB (Management Information Base), which is a data structure that defines what is obtainable from the device and what can be controlled (turned off, on, etc.).

You must check the **Enable** box to enable the applications you have defined.

To add a server using UPnP Forwarding:

1. Enter the **name** of the application in the appropriate Application Name field.

2. Next to the name of the application, enter the **number** of the external port used by the server in the Ext. Port column. Check with the Internet application software documentation for more information.

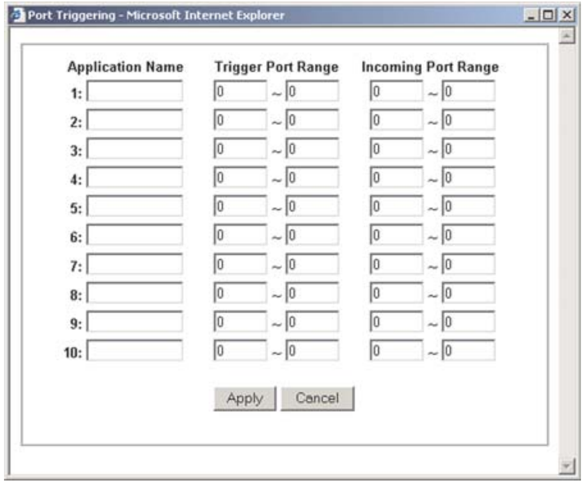
3. On the same line, select the protocol **UDP** or **TCP**.

4. Enter the **number** of the internal port used by the server in the Int. Port column. Check with the Internet application software documentation for more information.

5. Enter the IP address of the server that you want the Internet users to be able to access. To find the IP address, go to "Appendix G: Finding the MAC Address and IP Address for Your Ethernet Adapter."

6. Check the **Enable** box to enable the services you have defined. UPnP Forwarding will not function if the **Enable** button is left unchecked. This is disabled (unchecked) by default.

Port Triggering



	Application Name	Trigger Port Range	Incoming Port Range
1:		0 ~ 0	0 ~ 0
2:		0 ~ 0	0 ~ 0
3:		0 ~ 0	0 ~ 0
4:		0 ~ 0	0 ~ 0
5:		0 ~ 0	0 ~ 0
6:		0 ~ 0	0 ~ 0
7:		0 ~ 0	0 ~ 0
8:		0 ~ 0	0 ~ 0
9:		0 ~ 0	0 ~ 0
10:		0 ~ 0	0 ~ 0

Figure 7-39

From the Forwarding screen, click the **Port Triggering** button to open the Port Triggering screen, shown in Figure 7-39. From here, you can set the Router to watch outgoing data on assigned port numbers. The IP address of the computer that sends the matching data is remembered by the Router, so that when the requested data returns through the Router, the data is pulled back to the proper computer by way of IP address and port mapping rules.

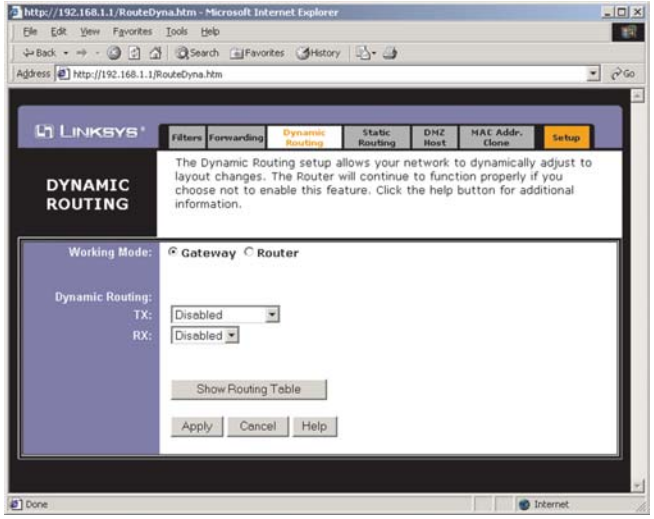
1. Enter the **Application Name** of the trigger.

2. Enter the **Trigger Port Range** used by the application. Check with the Internet application for the port number needed.

3. Enter the **Incoming Port Range** used by the application. Check with the Internet application for the port number needed.

4. Click the **Apply** button and then click the **Continue** button.

Dynamic Routing


http://192.168.1.1/RouteDyna.htm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.1.1/RouteDyna.htm
Go
LINKSYS
Filters
Forwarding
Dynamic Routing
Static Routing
DMZ Host
MAC Addr. Clone
Setup
Done
Internet

DYNAMIC ROUTING

The Dynamic Routing setup allows your network to dynamically adjust to layout changes. The Router will continue to function properly if you choose not to enable this feature. Click the help button for additional information.

Working Mode: ● Gateway ○ Router

Dynamic Routing:
TX: Disabled
RX: Disabled

Show Routing Table

Apply Cancel Help

Figure 7-40

From the Dynamic Routing screen, shown on Figure 7-40, you can enable the Router to automatically adjust to physical changes in the network's layout. The Router, using the RIP protocol, determines the network packets' route based on the fewest number of hops between the source and the destination. The RIP protocol regularly broadcasts routing information to other routers on the network. To set up Dynamic Routing:

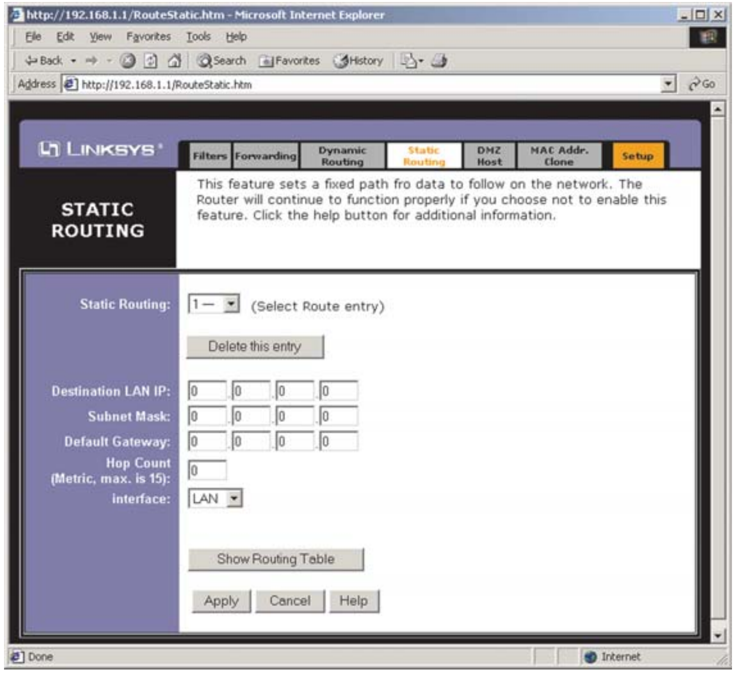
1. Choose the correct **Working Mode**. **Gateway Mode** should be used if the Router is hosting your network's connection to the Internet. **Router Mode** should be selected if the Router exists on a network with other routers. In Router Mode, any computer connected to the Router will not be able to connect to the Internet unless you have another router function as the Gateway.

2. Choose a **Dynamic Routing path protocol** for either transmission (TX) or reception (RX) of network data.

Click the **Show Routing Table** button to open a chart displaying how data is routed through your LAN.

When finished making your changes on this tab, click the **Apply** button followed by the **Continue** button to save these changes, or click the **Cancel** button to undo your changes. For further help on this tab, click the **Help** button.

Static Routing


http://192.168.1.1/RouteStatic.htm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.1.1/RouteStatic.htm
Go
LINKSYS
Filters
Forwarding
Dynamic Routing
Static Routing
DMZ Host
MAC Addr. Clone
Setup
Done
Internet

STATIC ROUTING

This feature sets a fixed path fro data to follow on the network. The Router will continue to function properly if you choose not to enable this feature. Click the help button for additional information.

Static Routing: 1 — (Select Route entry)

Delete this entry

Destination LAN IP: 0 . 0 . 0 . 0
Subnet Mask: 0 . 0 . 0 . 0
Default Gateway: 0 . 0 . 0 . 0
Hop Count (Metric, max. is 15): 0
interface: LAN

Show Routing Table

Apply Cancel Help

Figure 7-41

If the Router is connected to more than one network, it may be necessary to set up a static route between them. This can be done from the Static Routing screen, shown in Figure 7-41. A static route is a pre-determined pathway that network information must travel to reach a specific host or network. From the Static Routing tab, click the **Show Routing Table** button to view the current static routing configuration.

To create a static route entry:

1. Select a **Static Route Entry** from the drop-down list. The Router supports up to 20 static route entries.

   To delete a Static Routing entry, select an **entry**, and click the **Delete this entry** button.

2. Enter the following data to create a new static route.

   Destination LAN IP: The Destination LAN IP is the address of the remote network or host to which you want to assign a static route. Enter the **IP address** of the host for which you wish to create a static route here. If you are building a route to an entire network, be sure that the network portion of the IP address is set to 0. For example, the Router's standard IP address is 192.168.1.1. Based on this address, the address of the routed network is 192.168.1, with the last digit determining the Router's place on the network. Therefore you would enter the IP address 192.168.1.0 if you wanted to route to the Router's entire network, rather than just to the Router.

   Subnet Mask: The Subnet Mask (also known as the Network Mask) determines which portion of an IP address is the network portion, and which portion is the host portion. Take, for example, a network in which the Subnet Mask is 255.255.255.0. This determines (by using the values 255) that the first three numbers of a network IP address identify this particular network, while the last digit (from 1 to 254) identifies the specific host.

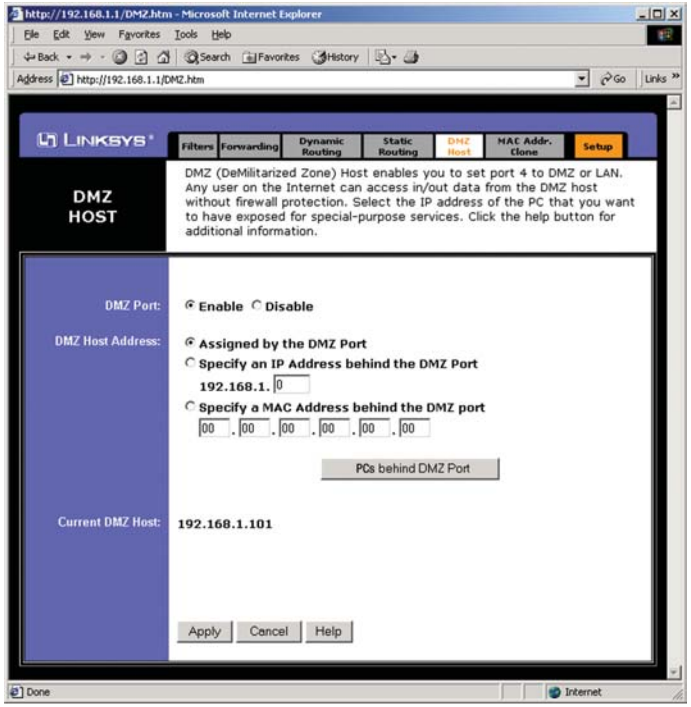
   Default Gateway: This IP address should be the IP address of the gateway device that allows for contact between the Router and the remote network or host.

   Hop Count: This determines the maximum number of steps between network nodes that data packets will travel. A node is any device on the network, such as PCs, print servers, routers, etc.

   interface: Select **LAN** or **WAN**, depending on the location of the static route's final destination.

3. When finished making your changes on this tab, click the **Apply** button and then the **Continue** button to save these changes, or click the **Cancel** button to undo your changes.

DMZ Host


http://192.168.1.1/DMZ.htm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.1.1/DMZ.htm
Go
Links
LINKSYS
Filters
Forwarding
Dynamic Routing
Static Routing
DMZ Host
MAC Addr. Clone
Setup
DMZ HOST
PCs behind DMZ Port
Apply
Cancel
Help
Done
Internet

DMZ (DeMilitarized Zone) Host enables you to set port 4 to DMZ or LAN. Any user on the Internet can access in/out data from the DMZ host without firewall protection. Select the IP address of the PC that you want to have exposed for special-purpose services. Click the help button for additional information.

DMZ Port: ● Enable ○ Disable

DMZ Host Address: ● Assigned by the DMZ Port
○ Specify an IP Address behind the DMZ Port
192.168.1. 0
○ Specify a MAC Address behind the DMZ port
00 . 00 . 00 . 00 . 00 . 00

Current DMZ Host: 192.168.1.101

Figure 7-42

From the DMZ Host tab, shown in Figure 7-42, you can set Port 4/DMZ to DMZ or LAN connection. Any user on the Internet can access incoming or outgoing data from the DMZ host without the use of firewall protection. This feature is used for special-purpose services such as Internet gaming and videoconferencing. Port 4 is the only port used for DMZ, and only one computer can be in DMZ mode.

DMZ Port

To enable or disable the DMZ port, click the **Enable** radio button or **Disable** radio button.

DMZ Host Address

Assigned by the DMZ Port: The DMZ host is the first PC connected to Port 4/DMZ of the Router, either directly or through a hub or switch. The Router will only allow one PC to be the DMZ host.

Specify an IP Address behind the DMZ Port: If you have multiple PCs connected to Port 4/DMZ via a hub or switch, you can specify which PC is the DMZ host. To expose a computer with a specific IP address, enter that computer's IP address in this field. To get the IP address of a computer, refer to "Appendix G: Finding the MAC Address and IP Address for Your Ethernet Adapter."

Specify a MAC Address behind the DMZ Port: If you have multiple PCs connected to Port 4/DMZ via a hub or switch, you can specify which PC is the DMZ host. To expose a PC with a specific MAC address, enter that computer's MAC address in this field. To get the MAC address of a computer, refer to "Appendix G: Finding the MAC Address and IP Address for Your Ethernet Adapter."

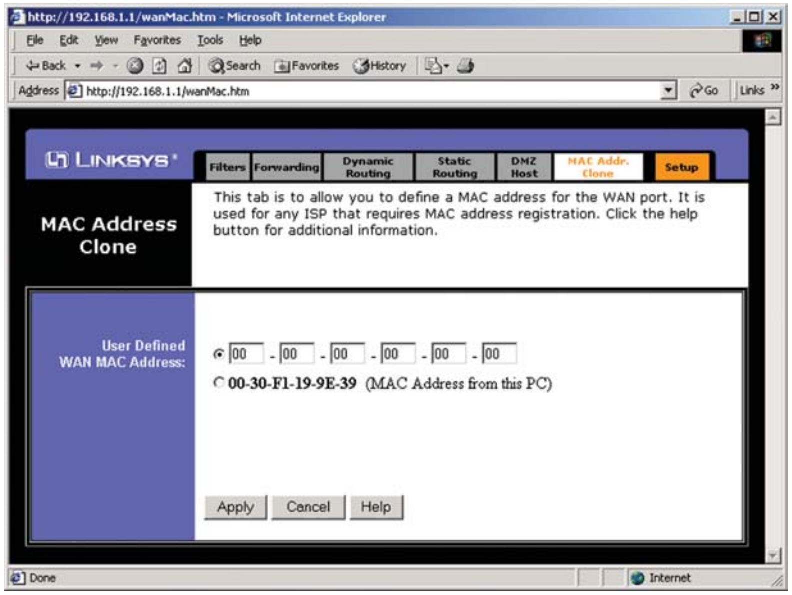
Click the **PCs behind DMZ Port** button to view all computers connected on Port 4/DMZ (multiple computers can be connected via a hub or switch).

Current DMZ Host

The IP address of the current DMZ host is displayed here.

When finished, click the **Apply** button and click the **Continue** button to save the settings. Otherwise, click the **Cancel** button to undo changes made on this screen.

MAC Address Clone


http://192.168.1.1/wanMac.htm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.1.1/wanMac.htm
Go Links
LINKSYS
Filters
Forwarding
Dynamic Routing
Static Routing
DMZ Host
MAC Addr. Clone
Setup
Apply
Cancel
Help
Done
Internet

MAC Address Clone

This tab is to allow you to define a MAC address for the WAN port. It is used for any ISP that requires MAC address registration. Click the help button for additional information.

User Defined WAN MAC Address: ● 00 - 00 - 00 - 00 - 00 - 00

○ 00-30-F1-19-9E-39 (MAC Address from this PC)

Figure 7-43

From the MAC Address Clone screen, shown in Figure 7-43, you can change the Router's WAN Mac Address.

The Router's **MAC address** is a 12-digit code assigned to a unique piece of hardware for identification, like a social security number. If your ISP requires MAC address registration, find your adapter's MAC address by following the instructions in "Appendix G: Finding the MAC Address and IP Address for Your Ethernet Adapter."

To define a MAC address for the WAN port, click the first radio button next to **User Defined WAN MAC Address**, and enter the 12 digits of your adapter's MAC address in the on-screen fields. This "clones" your network adapter's MAC address onto the Router, so you do NOT have to call your ISP to change the registered MAC address to the Router's MAC address.

If you want to clone the MAC address of the PC you are CURRENTLY using to configure the Router, then click the second radio button. The Router will automatically detect your PC's MAC address. It is recommended that the PC registered with the ISP is used to open the MAC Address Clone page.

When finished making your changes on this tab, click the **Apply** button and then the **Continue** button to save these changes, or click the **Cancel** button to undo your changes.

Appendix A: Troubleshooting

Common Problems and Solutions

This appendix consists of two parts: "Common Problems and Solutions" and "Frequently Asked Questions." Provided are possible solutions to problems regarding the installation and operation of the Router. If your situation is described here, the problem should be solved by applying the corresponding solution. If you can't find an answer here, check the Linksys website at *www.linksys.com*.

1. I need to set a static IP address on a PC.

The Router, by default, assigns an IP address range of 192.168.1.100 to 192.168.1.150 using the DHCP server on the Router. To set a static IP address, you can only use the ranges 192.168.1.2 to 192.168.1.99 and 192.168.1.151 to 192.168.1.254. Each PC or network device that uses TCP/IP must have a unique address to identify itself in a network. If the IP address is not unique to a network, Windows will generate an IP conflict error message. You can assign a static IP address to a PC by performing the following steps:

For Windows 95, 98, and Me:

A. Click **Start**, **Settings**, and **Control Panel**. Double-click **Network**.

B. In *The following network components are installed* box, select the **TCP/IP->** associated with your Ethernet adapter. If you only have one Ethernet adapter installed, you will only see one TCP/IP line with no association to an Ethernet adapter. Highlight it and click the **Properties** button.

C. In the *TCP/IP properties* window, select the **IP address** tab, and select **Specify an IP address**. Enter a unique **IP address** that is not used by any other computer on the network connected to the Router. You can only use an IP address in the ranges 192.168.1.2 to 192.168.1.99 and 192.168.1.151 to 192.168.1.254. Make sure that each IP address is unique for each PC or network device.

D. Click the **Gateway** tab, and in the *New Gateway* prompt, enter **192.168.1.1**, which is the default IP address of the Router. Click the **Add** button to accept the entry.

E. Click the **DNS** tab, and make sure the **DNS Enabled** option is selected. Enter the **Host** and **Domain** names (e.g., John for Host and home for Domain). Enter the **DNS entry** provided by your ISP. If your ISP has not provided the DNS IP address, contact your ISP to get that information or go to its website for the information.

F. Click the **OK** button in the *TCP/IP properties* window, and click **Close** or the **OK** button for the Network window.

G. Restart the computer when asked.

For Windows 2000:

A. Click **Start**, **Settings**, and **Control Panel**. Double-click **Network and Dial-Up Connections**.

B. Right-click the **Local Area Connection** that is associated with the Ethernet adapter you are using, and select the **Properties** option.

C. In the *Components checked are used by this connection* box, highlight **Internet Protocol (TCP/IP)**, and click the **Properties** button. Select **Use the following IP address** option.

D. Enter a unique **IP address** that is not used by any other computer on the network connected to the Router. You can only use an IP address in the ranges 192.168.1.2 to 192.168.1.99 and 192.168.1.151 to 192.168.1.254.

E. Enter the Subnet Mask, **255.255.255.0**.

F. Enter the Default Gateway, **192.168.1.1** (Router's default IP address).

G. Toward the bottom of the window, select **Use the following DNS server addresses**, and enter the **Preferred DNS server** and **Alternative DNS server** (provided by your ISP). Contact your ISP or go on its website to find the information.

H. Click the **OK** button in the *Internet Protocol (TCP/IP) Properties* window, and click the **OK** button in the *Local Area Connection Properties* window.

I. Restart the computer if asked.

For Windows NT 4.0:

A. Click **Start**, **Settings**, and **Control Panel**. Double-click the **Network** icon.

B. Click the **Protocol** tab, and double-click **TCP/IP Protocol**.

C. When the window appears, make sure you have selected the correct **Adapter** for your Ethernet adapter.

D. Select **Specify an IP address**, and enter a unique **IP address** that is not used by any other computer on the network connected to the Router. You can only use an IP address in the ranges 192.168.1.2 to 192.168.1.99 and 192.168.1.151 to 192.168.1.254.

E. Enter the Subnet Mask, **255.255.255.0**.

F. Enter the Default Gateway, **192.168.1.1** (Router's default IP address).

G. Click the **DNS** tab, and enter the **Host** and **Domain** names (e.g., John for Host and home for Domain). Under DNS Service Search Order, click the **Add** button. Enter the **DNS IP address** in the DNS Server field, and click the **Add** button. Repeat this action for all DNS IP addresses given by your ISP.

H. Click the **OK** button in the *TCP/IP Protocol Properties* window, and click the **Close** button in the *Network* window.

I. Restart the computer if asked.

For Windows XP:

The following instructions assume you are running Windows XP with the default interface. If you are using the Classic interface (where the icons and menus look like previous Windows versions), please follow the instructions for Windows 2000.

A. Click **Start** and **Control Panel**.
B. Click the **Network and Internet Connections** icon and then the **Network Connections** icon.
C. Right-click the **Local Area Connection** that is associated with the Ethernet adapter you are using, and select the **Properties** option.
D. In the *This connection uses the following items* box, highlight **Internet Protocol (TCP/IP)**. Click the **Properties** button.
E. Click the *use the following IP address* radio button. Enter a unique **IP address** that is not used by any other computer on the network connected to the Router. You can only use an IP address in the ranges 192.168.1.2 to 192.168.1.99 and 192.168.1.151 to 192.168.1.254.
F. Enter the Subnet Mask, **255.255.255.0**.
G. Enter the Default Gateway, **192.168.1.1** (Router's default IP address).
H. Toward the bottom of the window, select **Use the following DNS server addresses**, and enter the **Preferred DNS server** and **Alternative DNS server** (provided by your ISP). Contact your ISP or go on its website to find the information.
I. Click the **OK** button in the *Internet Protocol (TCP/IP) Properties* window. Click the **OK** button in the *Local Area Connection Properties* window.

2. I want to test my Internet connection.

A. Check your TCP/IP settings.

For Windows 95, 98, and Me:

- Refer to "Appendix F: Installing the TCP/IP Protocol" and "Chapter 5: Configure the PCs" for details. Make sure **Obtain IP address automatically** is selected in the settings.

For Windows 2000:

- Click **Start**, **Settings**, and **Control Panel**. Double-click **Network and Dial-Up Connections**.
- Right-click the **Local Area Connection** that is associated with the Ethernet adapter you are using, and select the **Properties** option.
- In the *Components checked are used by this connection* box, highlight **Internet Protocol (TCP/IP)**, and click the **Properties** button. Make sure that **Obtain an IP address automatically** and **Obtain DNS server address automatically** are selected.
- Click the **OK** button in the *Internet Protocol (TCP/IP) Properties* window, and click the **OK** button in the Local Area Connection Properties window.
- Restart the computer if asked.

For Windows XP:

The following instructions assume you are running Windows XP with the default interface. If you are using the Classic interface (where the icons and menus look like previous Windows versions), please follow the instructions for Windows 2000.

- Click **Start** and **Control Panel**.
- Click the **Network and Internet Connections** icon and then the **Network Connections** icon.
- Right-click the **Local Area Connection** that is associated with the Ethernet adapter you are using, and select the **Properties** option.
- In the *This connection uses the following items* box, highlight **Internet Protocol (TCP/IP)**, and click the **Properties** button. Make sure that **Obtain an IP address automatically** and **Obtain DNS server address automatically** are selected.
- Click the **OK** button in the *Internet Protocol (TCP/IP) Properties* window, and click the **OK** button in the *Local Area Connection Properties* window.
- Restart the computer if asked.

For Windows NT 4.0:

- Click **Start**, **Settings**, and **Control Panel**. Double-click the **Network** icon.
- Click the **Protocol** tab, and double-click on **TCP/IP Protocol**.
- When the window appears, make sure you have selected the correct **Adapter** for your Ethernet adapter and set it for **Obtain an IP address from a DHCP server**.
- Click the **OK** button in the *TCP/IP Protocol Properties* window, and click the **Close** button in the *Network* window.
- Restart the computer if asked.

B. Open a command prompt.

- For **Windows 95, 98,** and **Me**, please click **Start** and **Run**. In the Open field, type in **command**. Press the **Enter** key or click the **OK** button.
- For **Windows NT, 2000,** and **XP**, please click **Start** and **Run**. In the Open field, type **cmd**. Press the **Enter** key or click the **OK** button.

C. In the command prompt, type **ping 192.168.1.1** and press the **Enter** key.
- If you get a reply, the computer is communicating with the Router.
- If you do NOT get a reply, please check the cable, and make sure **Obtain an IP address automatically** is selected in the TCP/IP settings for your Ethernet adapter.

D. In the command prompt, type **ping** *followed by your WAN IP address* and press the **Enter** key. The WAN IP Address can be found in the web interface of the Router. For example, if your WAN IP address is 1.2.3.4, you would enter **ping 1.2.3.4** and press the **Enter** key.
- If you get a reply, the computer is connected to the Router.
- If you do NOT get a reply, try the ping command from a different computer to verify that your original computer is not the cause of the problem.

E. In the command prompt, type **ping www.yahoo.com** and press the **Enter** key.
- If you get a reply, the computer is connected to the Internet. If you cannot open a webpage, try the ping command from a different computer to verify that your original computer is not the cause of the problem.
- If you do NOT get a reply, there may be a problem with the connection. Try the ping command from a different computer to verify that your original computer is not the cause of the problem.

3. I am not getting an IP address on the WAN with my Internet connection.

A. Refer to “Problem #2, I want to test my Internet connection” to verify that you have connectivity.
B. If you need to register the MAC address of your Ethernet adapter with your ISP, please see “Appendix G: Finding the MAC address and IP Address for Your Ethernet Adapter.” If you need to clone the MAC address of your Ethernet adapter onto the Router, see the MAC Address Clone section of “Chapter 7: The Cable/DSL Firewall Router’s Web-based Utility” for details.
C. Make sure you are using the right WAN settings. Contact your ISP to see if your WAN connection type is DHCP, Static IP Address, or PPPoE (commonly used by DSL consumers). Please refer to the Setup section of “Chapter 7: The Cable/DSL Firewall Router’s Web-based Utility” for details on WAN settings.
D. Make sure you have the right cable. Check to see if the WAN column has a solidly lit Link LED.
E. Make sure the cable connecting from your cable or DSL modem is connected to the Router’s WAN port. Verify that the Status page of the Router’s web interface shows a valid IP address from your ISP.

F. Turn off the computer, Router, and cable/DSL modem. Wait 30 seconds, and then turn on the Router, cable/DSL modem, and computer. Check the Status tab of the Router’s web-based utility to see if you get an IP address.

4. I am not able to access the Router’s web interface Setup page.

A. Refer to “Problem #2, I want to test my Internet connection” to verify that your computer is properly connected to the Router.
B. Refer to “Appendix G: Finding the MAC Address and IP address for Your Ethernet Adapter” to verify that your computer has an IP Address, Subnet Mask, Gateway, and DNS.
C. Set a static IP address on your system; refer to “Problem #1: I need to set a static IP address.”
D. Refer to “Problem #10: I need to remove the proxy settings or the dial-up pop-up window (for PPPoE users).”

5. I can’t get my Virtual Private Network (VPN) Pass-Through working through the Router (not a VPN tunnel).

Access the Router’s web interface by going to **http://192.168.1.1** or the **IP address** of the Router, and go to the **Advanced => Filter** tab. Make sure you have IPsec pass-through and/or PPTP pass-through enabled.

VPNs that use IPSec with the ESP (Encapsulation Security Payload known as protocol 50) authentication will work fine. At least one IPSec session will work through the Router; however, simultaneous IPSec sessions *may* be possible, depending on the specifics of your VPNs.

VPNs that use IPSec and AH (Authentication Header known as protocol 51) are incompatible with the Router. AH has limitations due to occasional incompatibility with the NAT standard.

Change the IP address for the Router to another subnet to avoid a conflict between the VPN IP address and your local IP address. For example, if your VPN server assigns an IP address 192.168.1.X (X is a number from 1 to 254) and your local LAN IP address is 192.168.1.X (X is the same number used in the VPN IP address), the Router will have difficulties routing information to the right location. If you change the Router’s IP address to 192.168.2.1, that should solve the problem. Change the Router’s IP address through the Setup tab of the web interface. If you assigned a static IP address to any computer or network device on the network, you need to change its IP address accordingly to 192.168.2.Y (Y being any number from 1 to 254). Note that each IP address must be unique within the network.

Your VPN may require port 500/UDP packets to be passed to the computer that is connecting to the IPSec server. Refer to "Problem #7, I need to set up online game hosting or use other Internet applications" for details.

Check the Linksys website for more information at *www.linksys.com*.

6. I need to set up a server behind my Router.

To use a server like a web, ftp, or mail server, you need to know the respective port numbers they are using. For example, port 80 (HTTP) is used for web; port 21 (FTP) is used for FTP, and port 25 (SMTP outgoing) and port 110 (POP3 incoming) are used for the mail server. You can get more information by viewing the documentation provided with the server you installed. Follow these steps to set up port forwarding through the Router's web-based utility. We will be setting up web, ftp, and mail servers.

A. Access the Router's web-based utility by going to **http://192.168.1.1** or the **IP address** of the Router. Go to the **Advanced => Forwarding** tab.
B. Enter any **name** you want to use for the Customized Application.
C. Enter the **Ext. Port range** of the service you are using. For example, if you have a web server, you would enter the range 80 to 80.
D. Check the **protocol** you will be using, TCP and/or UDP.
E. Enter the **IP address** of the PC or network device that you want the port server to go to. For example, if the web server's Ethernet adapter IP address is 192.168.1.100, you would enter 100 in the field provided. Check "Appendix G: Finding the MAC Address and IP Address for Your Ethernet Adapter" for details on getting an IP address.
F. Check the **Enable** option for the port services you want to use. Consider the example below:

Customized Application	Ext. Port	TCP	UDP	IP Address	Enable
Web server	80 to 80	X	X	192.168.1.100	X
FTP server	21 to 21	X		192.168.1.101	X
SMTP (outgoing)	25 to 25	X	X	192.168.1.102	X
POP3 (incoming)	110 to 110	X	X	192.168.1.102	X

When you have completed the configuration, click the **Apply** button and then the **Continue** button.

7. I need to set up online game hosting or use other Internet applications.

If you want to play online games or use Internet applications, most will work without doing any port forwarding or DMZ hosting. There may be cases when you want to host an online game or Internet application. This would require you to set up the Router to deliver incoming packets or data to a specific computer. This also applies to the Internet applications you are using. The best way to get the information on what port services to use is to go to the website of the online game or application you want to use. Follow these steps to set up online game hosting or use a certain Internet application:

A. Access the Router's web interface by going to **http://192.168.1.1** or the **IP address** of the Router. Go to the **Advanced => Forwarding** tab.
B. Enter any **name** you want to use for the Customized Application.
C. Enter the **Ext. Port range** of the service you are using. For example, if you want to host Unreal Tournament (UT), you would enter the range 7777 to 27900.
D. Check the **protocol** you will be using, TCP and/or UDP.
E. Enter the **IP address** of the PC or network device that you want the port server to go to. For example, if the web server's Ethernet adapter IP address is 192.168.1.100, you would enter 100 in the field provided. Check "Appendix G: Finding the MAC Address and IP Address for Your Ethernet Adapter" for details on getting an IP address.
F. Check the **Enable** option for the port services you want to use. Consider the example below:

Customized Application	Ext. Port	TCP	UDP	IP Address	Enable
UT	7777 to 27900	X	X	192.168.1.100	X
Halflife	27015 to 27015	X	X	192.168.1.105	X
PC Anywhere	5631 to 5631		X	192.168.1.102	X
VPN IPSEC	500 to 500		X	192.168.1.100	X

When you have completed the configuration, click the **Apply** button and then the **Continue** button.

8. I can't get the Internet game, server, or application to work.

If you are having difficulties getting any Internet game, server, or application to function properly, consider exposing one PC to the Internet using DeMilitarized Zone (DMZ) hosting. This option is available when an application requires too many ports or when you are not sure which port services to use. Make sure you disable all the forwarding entries if you want to successfully use DMZ hosting, since forwarding has priority over DMZ hosting. (In other words, data that enters the Router will be checked first by the forwarding settings. If the port number that the data enters from does not have port forwarding, then the Router will send the data to whichever PC or network device you set for DMZ hosting.) Follow these steps to set DMZ hosting:

A. Access the Router's web-based utility by going to **http://192.168.1.1** or the **IP address** of the Router. Go to the **Advanced => Forwarding** tab.
B. Disable or remove the entries you have entered for forwarding. Keep this information in case you want to use it at a later time.
C. Click the **DMZ Host** tab.
D. Enter the Ethernet adapter's **IP address** of the computer you want exposed to the Internet. This will bypass the NAT firewall for that computer. Please refer to "Appendix G: Finding the MAC Address and IP Address for Your Ethernet Adapter" for details on getting an IP address.

Once completed with the configuration, click the **Apply** button and then the **Continue** button.

9. I forgot my password, or the password prompt always appears when saving settings to the Router.

Reset the Router to factory default by pressing the **Reset** button for 30 seconds and then releasing it. If you are still getting prompted for a password when saving settings, then perform the following steps:

A. Access the Router's web interface by going to **http://192.168.1.1** or the **IP address** of the Router. Enter the default password **admin**, and click the **Password** tab.
B. Enter a **different password** in the Router Password field, and enter the same password in the second field to confirm the password.
C. Click the **Apply** and **Continue** buttons.

10. I am a PPPoE user, and I need to remove the proxy settings or the dial-up pop-up window.

If you have proxy settings, you need to disable these on your computer. Because the Router is the gateway for the Internet connection, the computer does not need any proxy settings to gain access. Please follow these directions to verify that you do not have any proxy settings and that the browser you use is set to connect directly to the LAN.

For Microsoft Internet Explorer 5.0 or higher:
A. Click **Start**, **Settings**, and **Control Panel**. Double-click **Internet Options**.
B. Click the **Connections** tab.
C. Click the **LAN settings** button and remove anything that is checked.
D. Click the **OK** button to go back to the previous screen.
E. Click the option **Never dial a connection**. This will remove any dial-up pop-ups for PPPoE users.

For Netscape 4.7 or higher:
A. Start **Netscape Navigator**, and click **Edit**, **Preferences**, **Advanced**, and **Proxies**.
B. Make sure you have **Direct connection to the Internet** selected on this screen.
C. Close all the windows to finish.

11. To start over, I need to set the Router to factory default.

Hold the **Reset** button for up to 30 seconds and then release it. This will return the password, forwarding, and other settings on the Router to the factory default settings. In other words, the Router will revert to its original factory configuration.

12. I need to upgrade the firmware.

In order to upgrade the firmware with the latest features, you need to go to the Linksys website and download the latest firmware at *www.linksys.com*. Follow these steps:

A. Go to the Linksys website at **http://www.linksys.com** and download the latest firmware.
B. To upgrade the firmware, follow the steps in the Help section found in "Chapter 7: The Cable/DSL Firewall Router's Web-based Utility."

13. The firmware upgrade failed, and/or the Diag LED is flashing.

The upgrade could have failed for a number of reasons. Follow these steps to upgrade the firmware and/or make the Diag LED stop flashing:

A. If the firmware upgrade failed, use the **TFTP** program (it was downloaded along with the firmware). Open the pdf that was downloaded along with the firmware and TFTP program, and follow the pdf's instructions.

B. Set a **static IP address** on the PC; refer to "Problem #1, I need to set a static IP address." Use the following IP address settings for the computer you are using:

IP Address: 192.168.1.50
Subnet Mask: 255.255.255.0
Gateway: 192.168.1.1

C. Perform the upgrade using the TFTP program or the Router's web-based utility through its Help tab.

14. My DSL service's PPPoE is always disconnecting.

PPPoE is not actually a dedicated or always-on connection. The DSL ISP can disconnect the service after a period of inactivity, just like a normal phone dial-up connection to the Internet. There is a setup option to "keep alive" the connection. This may not always work, so you may need to re-establish connection periodically.

A. To connect to the Router, go to the web browser, and enter **http://192.168.1.1** or the **IP address** of the Router.
B. Enter the **password**, if asked. (The default password is **admin**.)
C. In the Setup tab, select the option **Keep Alive**, and set the **Redial Period** option at **20** (seconds).
D. Click the **Apply** and **Continue** buttons.
E. Click the **Status** tab, and click the **Connect** button.
F. You may see the login status display as **Connecting**. Press the **F5** key to refresh the screen, until you see the login status display as **Connected**.
G. Click the **Apply** and **Continue** buttons to continue.

If the connection is lost again, follow steps E to G to re-establish connection.

15. I can't access my email, web, or VPN, or I am getting corrupted data from the Internet.

The Maximum Transmission Unit (MTU) setting may need to be adjusted. By default, the MTU is set at 1500. For most DSL users, it is strongly recommended to use MTU 1492. If you are having some difficulties, perform the following steps:

A. To connect to the Router, go to the web browser, and enter **http://192.168.1.1** or the **IP address** of the Router.
B. Enter the password, if asked. (The default password is **admin**.)
C. Click the **Advanced => Filter** tab.
D. Look for the MTU option, and select **Manual**. In the Size field, enter **1492**.
E. Click the **Apply** and **Continue** buttons to continue.

If your difficulties continue, change the **Size** to different values. Try this list of values, one value at a time, in this order, until your problem is solved:

1462
1400
1362
1300

16. I need to use port triggering.

Port triggering looks at the outgoing port services used and will trigger the Router to open a specific port, depending on which port an Internet application uses. Follow these steps:

A. To connect to the Router, go to the web browser, and enter **http://192.168.1.1** or the **IP address** of the Router.
B. Enter the password, if asked. (The default password is **admin**.)
C. Click the **Advanced => Forwarding** tab, and click the **Port Triggering** button.
D. Enter any **name** you want to use for the Application Name.
E. Enter the **Triggered Port Range**. Check with your Internet application provider for more information on which outgoing port services it is using.
F. Enter the **Incoming Port Range**. Check with your Internet Application provider for more information on which incoming port services are required by the Internet application.

17. The Diag LED stays lit continuously.

The Diag LED lights up when the device is first powered up. Meantime, the system will boot up itself and check for proper operation. After finishing the checking procedure, the LED turns off to show that the system is working fine. If the LED remains lit after this time, the device is not working properly. Try to flash the firmware by assigning a static IP address to the computer, and then upgrade the firmware. Try using the following settings, IP Address: 192.168.1.50 and Subnet Mask: 255.255.255.0. To set a static IP address, refer to “Problem #1: I need to set a static IP address.”

18. When I enter a URL or IP address, I get a time-out error or am prompted to retry.

- Check if other PCs work. If they do, ensure that your workstation’s IP settings are correct (IP Address, Subnet Mask, Default Gateway, and DNS). Restart the computer that is having a problem.
- If the PCs are configured correctly, but still not working, check the Router. Ensure that it is connected and ON. Connect to it and check its settings. (If you cannot connect to it, check the LAN and power connections.)
- If the Router is configured correctly, check your Internet connection (DSL/cable modem, etc.) to see if it is working correctly. You can remove the Router to verify a direct connection.
- Manually configure the TCP/IP with a DNS address provided by your ISP.
- Make sure that your browser is set to connect directly and that any dial-up is disabled. For Internet Explorer, click **Tools**, **Internet Options**, and then the **Connection** tab. Make sure that Internet Explorer is set to **Never dial a connection**. For Netscape Navigator, click **Edit**, **Preferences**, **Advanced**, and **Proxy**. Make sure that Netscape Navigator is set to **Direct connection to the Internet**.

19. The Full/Col LED keeps flickering continuously.

- Check the Category 5 Ethernet cable and its RJ-45 connectors.
- There may be interference with other network devices. Try removing other PCs or network devices to see if the problem persists. Eliminate each network device one at a time to determine the cause.

Frequently Asked Questions

What is the maximum number of IP addresses that the Router will support? The Router will support up to 253 IP addresses.

Is IPSec Pass-Through supported by the Router? Yes, it is a built-in feature that the Router automatically enables.

Where is the Router installed on the network? In a typical environment, the Router is installed between the cable/DSL modem and the LAN. Plug the Router into the cable/DSL modem’s Ethernet port.

Does the Router support IPX or AppleTalk? No. TCP/IP is the only protocol standard for the Internet and has become the global standard for communications. IPX, a NetWare communications protocol used only to route messages from one node to another, and AppleTalk, a communications protocol used on Apple and Macintosh networks, can be used for LAN to LAN connections, but those protocols cannot connect from WAN to LAN.

Does the WAN connection of the Router support 100 Mbps Ethernet? Yes, and it does, of course, support 100 Mbps over the auto-sensing Fast Ethernet 10/100 switch on the LAN side of the Router.

What is Network Address Translation and what is it used for? Network Address Translation (NAT) translates multiple IP addresses on the private LAN to one public address that is sent out to the Internet. This adds a level of security since the address of a PC connected to the private LAN is never transmitted on the Internet. Furthermore, NAT allows the Router to be used with low cost Internet accounts, such as DSL or cable modems, when only one TCP/IP address is provided by the ISP. The user may have many private addresses behind this single address provided by the ISP.

Does the Router support any operating system other than Windows 95, Windows 98, Windows 2000, Windows NT, or Windows XP? Yes, but Linksys does not, at this time, provide technical support for setup, configuration or troubleshooting of any non-Windows operating systems.

Does the Router support ICQ send file? Yes, with the following fix: click **ICQ menu -> preference -> connections tab->**, and check **I am behind a firewall or proxy**. Then set the firewall time-out to **80** seconds in the firewall setting. The Internet user can then send a file to a user behind the Router.

I set up an Unreal Tournament Server, but others on the LAN cannot join. What do I need to do? If you have a dedicated Unreal Tournament server running, you need to create a static IP for each of the LAN computers and forward ports 7777, 7778, 7779, 7780, 7781, and 27900 to the IP address of the server. You can also use a port forwarding range of 7777 ~ 27900. If you want to use the UT Server Admin, forward another port (8080 usually works well but is used for remote admin. You may have to disable this.), and then in the [UWeb.WebServer] section of the server.ini file, set the ListenPort to 8080 (to match the mapped port above) and ServerName to the IP assigned to the Router from your ISP.

Can multiple gamers on the LAN get on one game server and play simultaneously with just one public IP address? It depends on which network game or what kind of game server you are using. For example, Unreal Tournament supports multi-login with one public IP.

How do I get *Half-Life: Team Fortress* to work with the Router? The default client port for Half-Life is 27005. The computers on your LAN need to have "+clientport 2700x" added to the HL shortcut command line; the x would be 6, 7, 8, and on up. This lets multiple computers connect to the same server. *One problem:* Version 1.0.1.6 won't let multiple computers with the same CD key connect at the same time, even if on the same LAN (not a problem with 1.0.1.3). As far as hosting games, the HL server does not need to be in the DMZ. Just forward port 27015 to the local IP address of the server computer.

How can I block corrupted FTP downloads? If you are experiencing corrupted files when you download a file with your FTP client, try using another FTP program.

The web page hangs; downloads are corrupt, or nothing but junk characters are being displayed on the screen. What do I need to do? Force your Ethernet adapter to 10Mbps or half duplex mode, and turn off the "Auto-negotiate" feature of your Ethernet adapter as a temporary measure. (Please look at the Network Control Panel in your Ethernet adapter's Advanced Properties tab.) Make sure that your proxy setting is disabled in the browser. Check our website at *www.linksys.com* for more information.

If all else fails in the installation, what can I do? Reset the Router by holding down the reset button until the Diag LED fully turns on and off. Reset your cable or DSL modem by powering the unit off and then on. Obtain and flash

the latest firmware release that is readily available on the Linksys website, *www.linksys.com*.

How will I be notified of new Router firmware upgrades? All Linksys firmware upgrades are posted on the Linksys website at *www.linksys.com*, where they can be downloaded for free. The Router's firmware can be upgraded with TFTP programs. If the Router's Internet connection is working well, there is no need to download a newer firmware version, unless that version contains new features that you would like to use. Downloading a more current version of Router firmware will not always enhance the quality or speed of your Internet connection, and may disrupt your current connection stability.

Will the Router function in a Macintosh environment? Yes, but the Router's setup pages are accessible only through Internet Explorer 4.0 or Netscape Navigator 4.0 or higher for Macintosh.

I am not able to get the web configuration screen for the Router. What can I do? You may have to remove the proxy settings on your Internet browser, e.g., Netscape Navigator or Internet Explorer. Or remove the dial-up settings on your browser. Check with your browser documentation, and make sure that your browser is set to connect directly and that any dial-up is disabled. Make sure that your browser is set to connect directly and that any dial-up is disabled. For Internet Explorer, click **Tools**, **Internet Options**, and then the **Connection** tab. Make sure that Internet Explorer is set to **Never dial a connection**. For Netscape Navigator, click **Edit**, **Preferences**, **Advanced**, and **Proxy**. Make sure that Netscape Navigator is set to **Direct connection to the Internet**.

What is DMZ Hosting? Demilitarized Zone (DMZ) allows one IP address (computer) to be exposed to the Internet. Some applications require multiple TCP/IP ports to be open. It is recommended that you set your computer with a static IP if you want to use DMZ Hosting. To get the LAN IP address, see "Appendix G: Finding the MAC Address and IP Address for Your Ethernet Adapter," or use the web-based utility to determine the MAC address of the computer accessing the Router's web-based utility.

If DMZ Hosting is used, does the exposed user share the public IP with the Router? No.

Is the Router cross-platform compatible? Any platform that supports Ethernet and TCP/IP is compatible with the Router.

How many ports can be simultaneously forwarded? Theoretically, the Router can establish 520 sessions at the same time, but you can only forward 10 ranges of ports.

Does the Router replace a modem? Is there a cable or DSL modem in the Router? No, this version of the Router must work in conjunction with a cable or DSL modem.

Which modems are compatible with the Router? The Router is compatible with virtually any cable or DSL modem that supports Ethernet.

What are the advanced features of the Router? The Router's advanced features include Filters, Forwarding, Dynamic Routing, Static Routing, DMZ Hosting, and MAC Address Cloning.

What is the maximum number of VPN tunnels allowed by the Router? The Router supports up to two simultaneous IPSec VPN tunnels.

How big is the memory buffer on the Router? 8MB buffer and 2MB flash.

How can I check whether I have static or DHCP IP Addresses? Consult your ISP to obtain this information.

How do I get mIRC to work with the Router? Under the Port Range Forwarding tab, set port forwarding to 113 for the PC on which you are using mIRC.

If your questions are not addressed here, refer to the Linksys website, *www.linksys.com*.

Appendix B: Maximizing VPN Security

Just as you maximized your network security with a firewall, you should also maximize security for your data with the Firewall Router.

IPSec is compatible with most VPN endpoints and ensures privacy and authentication for data, while authenticating user identification. With IPSec, authentication is based upon the PC's IP Address. This not only confirms the user's identity but also establishes the secure tunnel at the network layer, protecting all data that passes through.

By operating at the network layer, IPSec is independent of any applications running on the network. This way, it doesn't harm your PC's performance and still allows you to do more with greater security. Still, it is important to note that IPSec encryption does create a slight slowdown in network throughput, due to encrypting and decrypting data.

A method of securing data transmission is by using key exchange with a VPN tunnel. Securing the key exchange without compromising earlier sessions is by using PFS (Perfect Forward Secrecy). PFS protects by authenticating the key exchange between two VPN endpoints. This is done by sending one key to the other endpoint and then then creating a new key to be passed back to the the original sender of the data exchange.

All of this protection actually comes at a lower cost than most VPN endpoint software packages. The Firewall Router will allow the users on your network to secure their data over the Internet without having to purchase the extra client licenses that other VPN hardware manufacturers and software packages will require. With VPN functions handled by the router, rather than your PC (which software packages would require), this frees up your PCs to perform more functions, more efficiently. An additional benefit is that you aren't required to reconfigure any of your network PCs.

As secure as the Firewall Router makes your data, there are still more ways to maximize security. The following are a few suggestions on how to increase data security beyond the Firewall Router.

1) Maximize security on your other networks. Install firewall routers for your Internet connections, and use the most up-to-date security measures for wireless networking.

2) Narrow the scope of your VPN tunnel as much as possible. Rather than allowing a range of IP Addresses, use the addresses specific to the end-points required.

3) Do not set the Remote Security Group to Any, as this will open the VPN to any IP Address. Host a specific IP address.

4) Maximize encryption and authentication. Use 3DES encryption and SHA authentication whenever possible.

5) Manage your pre-shared keys. Change pre-shared keys regularly.

Data transmission over the Internet is a hole in network security that is often overlooked. With VPN maximized, along with the use of a firewall router and wireless security, you can secure your data even when it leaves your network.

Appendix C: Configuring IPSec between a Windows 2000 or XP PC and the Firewall Router

Introduction

This document demonstrates how to establish a secure IPSec tunnel using pre-shared keys to join a private network inside the Firewall Router and a Microsoft Windows 2000 or XP PC. You can find detailed information on configuring the Microsoft Windows 2000 server at the Microsoft website:

Microsoft KB Q252735 - How to Configure IPSec Tunneling in Windows 2000
http://support.microsoft.com/support/kb/articles/Q252/7/35.asp

Microsoft KB Q257225 - Basic IPSec Troubleshooting in Windows 2000
http://support.microsoft.com/support/kb/articles/Q257/2/25.asp

Environment

The IP addresses and other specifics mentioned in this appendix are for illustration purposes only.

Windows 2000 or Windows XP
IP Address: 140.111.1.2 <= User ISP provides IP Address; this is only an example.

Subnet Mask: 255.255.255.0

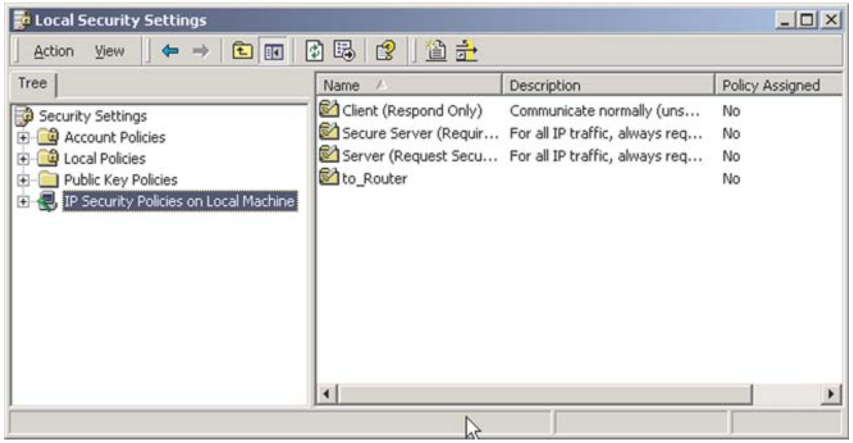
BEFSX41
WAN IP Address: 140.111.1.1 <= User ISP provides IP Address; this is only an example.

Subnet Mask: 255.255.255.0
LAN IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0

Note: Keep a record of any changes you make. Those changes will be identical in the Windows "secpol" application and the Router's Web-Based Utility.

Step One: Create an IPSec Policy

1. Click the **Start** button, select **Run**, and type **secpol.msc** in the Open field. The Local Security Setting screen will appear as shown in Figure C-1.



- Security Settings
  - Account Policies
  - Local Policies
  - Public Key Policies
  - IP Security Policies on Local Machine

Name	Description	Policy Assigned
Client (Respond Only)	Communicate normally (uns...	No
Secure Server (Requir...	For all IP traffic, always req...	No
Server (Request Secu...	For all IP traffic, always req...	No
to_Router		No

Figure C-1

2. Right-click **IP Security Policies on Local Computer**, and click **Create IP Security Policy**.

3. Click the **Next** button, and then enter a name for your policy (for example, **to_router**). Then, click **Next**.

4. Deselect the **Activate the default response rule** check box, and then click the **Next** button.

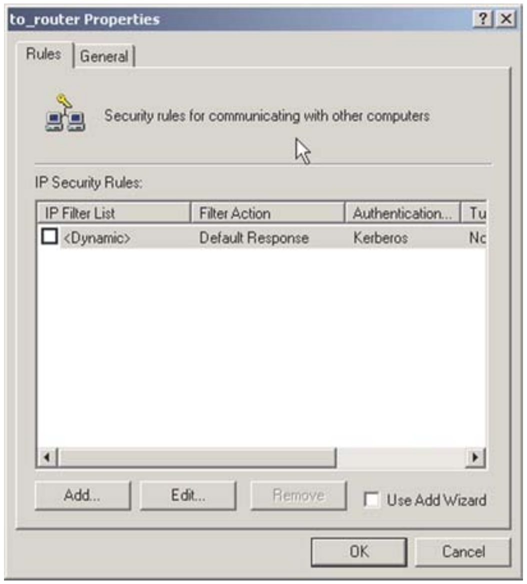
5. Click the **Finish** button, making sure the **Edit** check box is checked.

Step Two: Build Filter Lists

Filter List 1: win->router

Note: The references in this section to "win" are references to Windows 2000 and XP.

1. In the new policy's properties screen, verify that the **Rules** tab is selected, as shown in Figure C-2. Deselect the **Use Add Wizard** check box, and click the **Add** button to create a new rule.



Security rules for communicating with other computers

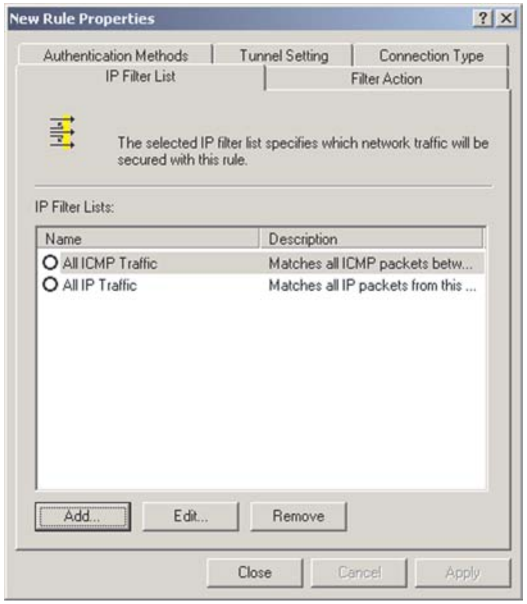
IP Security Rules:

IP Filter List	Filter Action	Authentication...	Tu
☐ <Dynamic>	Default Response	Kerberos	Nc

☐ Use Add Wizard

Figure C-2

2. Make sure the **IP Filter List** tab is selected, and click the **Add** button.



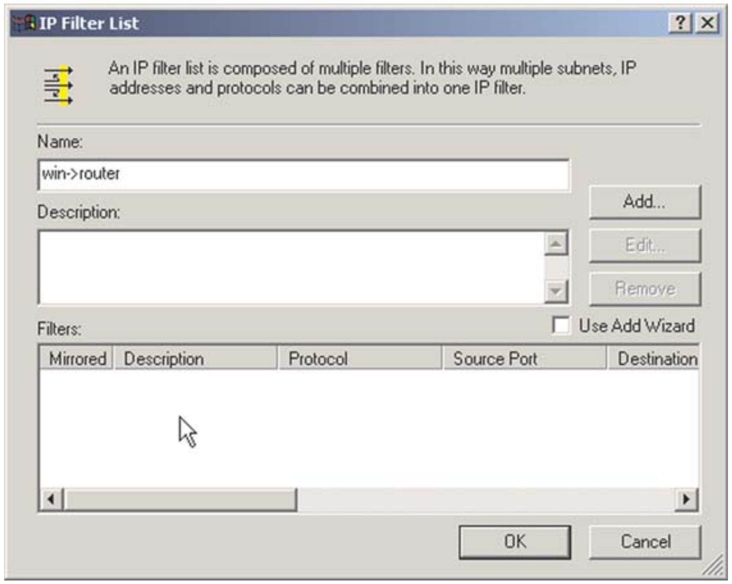
The selected IP filter list specifies which network traffic will be secured with this rule.

IP Filter Lists:

Name	Description
○ All ICMP Traffic	Matches all ICMP packets betw...
○ All IP Traffic	Matches all IP packets from this ...

Figure C-3

3. The *IP Filter List* screen should appear, as shown in Figure C-4. Enter an appropriate name, such as **win->router**, for the filter list, and de-select the **Use Add Wizard** check box. Then, click the **Add** button.



IP Filter List

An IP filter list is composed of multiple filters. In this way multiple subnets, IP addresses and protocols can be combined into one IP filter.

Name: win->router

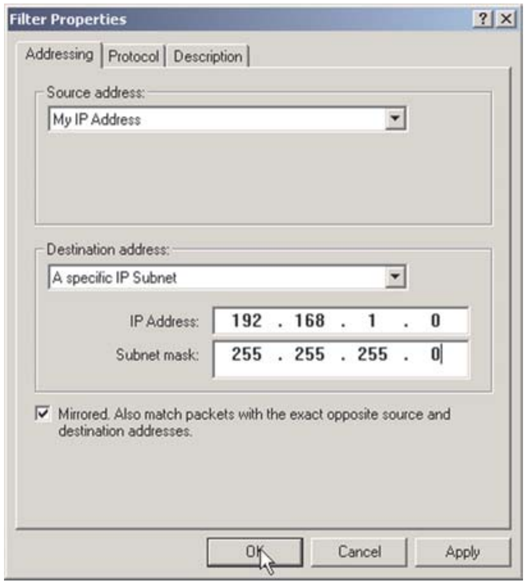
Description:

Filters: □ Use Add Wizard

Mirrored	Description	Protocol	Source Port	Destination

Figure C-4

4. The *Filters Properties* screen will appear, as shown in Figure C-5. Select the **Addressing** tab. In the Source address field, select **My IP Address**. In the Destination address field, select **A specific IP Subnet**, and fill in the IP Address: **192.168.1.0** and Subnet mask: **255.255.255.0**. (These are the Router's default settings. If you have changed these settings, enter your new values.)



Filter Properties

Source address: My IP Address

Destination address: A specific IP Subnet

IP Address: 192 . 168 . 1 . 0

Subnet mask: 255 . 255 . 255 . 0

☑ Mirrored. Also match packets with the exact opposite source and destination addresses.

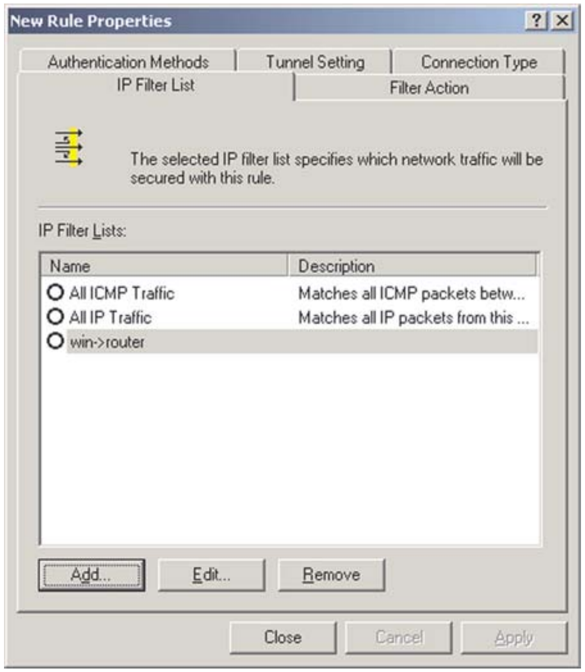
Figure C-5

5. If you want to enter a description for your filter, click the **Description** tab and enter the description there.

6. Click the **OK** button. Then, click the **OK** (for Windows XP) or **Close** (for Windows 2000) button on the *IP Filter List* window.

Filter List 2: router=>win

7. The *New Rule Properties* screen will appear, as shown in Figure C-6. Select the **IP Filter List** tab, and make sure that **win -> router** is highlighted. Then, click the **Add** button.



New Rule Properties

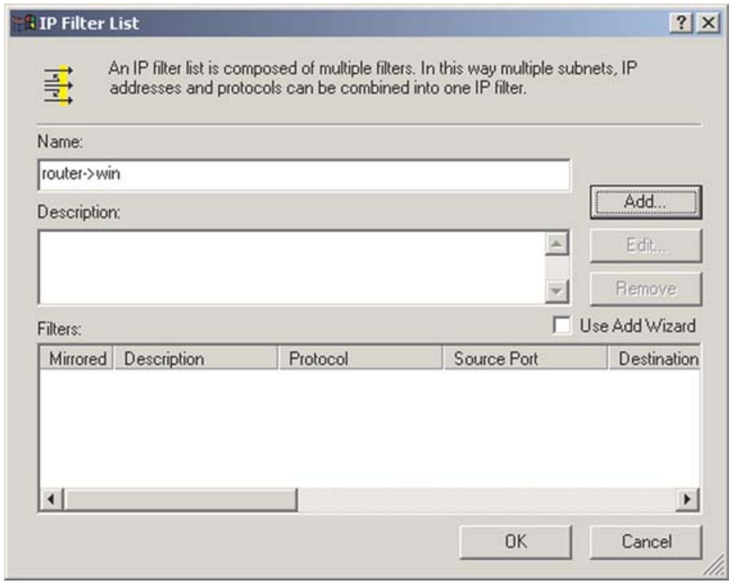
The selected IP filter list specifies which network traffic will be secured with this rule.

IP Filter Lists:

Name	Description
○ All ICMP Traffic	Matches all ICMP packets betw...
○ All IP Traffic	Matches all IP packets from this ...
○ win->router	

Figure C-6

8. The *IP Filter List* screen should appear, as shown in Figure C-7. Enter an appropriate name, such as **router->win** for the filter list, and de-select the **Use Add Wizard** check box. Click the **Add** button.



IP Filter List

An IP filter list is composed of multiple filters. In this way multiple subnets, IP addresses and protocols can be combined into one IP filter.

Name: router->win

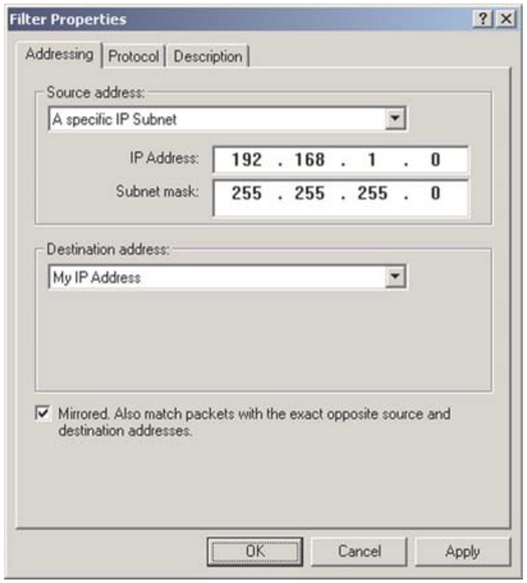
Description:

Filters: □ Use Add Wizard

Mirrored	Description	Protocol	Source Port	Destination

Figure C-7

9. The *Filters Properties* screen will appear, as shown in Figure C-8. Select the **Addressing** tab. In the Source address field, select **A specific IP Subnet**, and enter the IP Address: **192.168.1.0** and Subnet mask: **255.255.255.0**. (Enter your new values if you have changed the default settings.) In the Destination address field, select **My IP Address**.



Filter Properties

Addressing | Protocol | Description

Source address: A specific IP Subnet

IP Address: 192 . 168 . 1 . 0

Subnet mask: 255 . 255 . 255 . 0

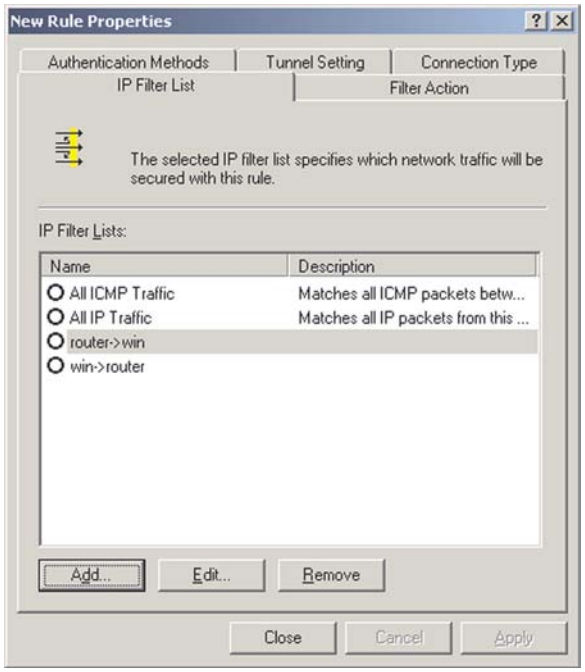
Destination address: My IP Address

☑ Mirrored. Also match packets with the exact opposite source and destination addresses.

Figure C-8

10. If you want to enter a description for your filter, click the **Description** tab and enter the description there.

11. Click the **OK** button and the *New Rule Properties* screen should appear with the IP Filer List tab selected, as shown in Figure C-9. There should now be a listing for “router -> win” and “win -> router”. Click the **OK** (for WinXP) or **Close** (for Win2000) button on the *IP Filter List* window.



New Rule Properties

Authentication Methods | Tunnel Setting | Connection Type | IP Filter List | Filter Action

The selected IP filter list specifies which network traffic will be secured with this rule.

IP Filter Lists:

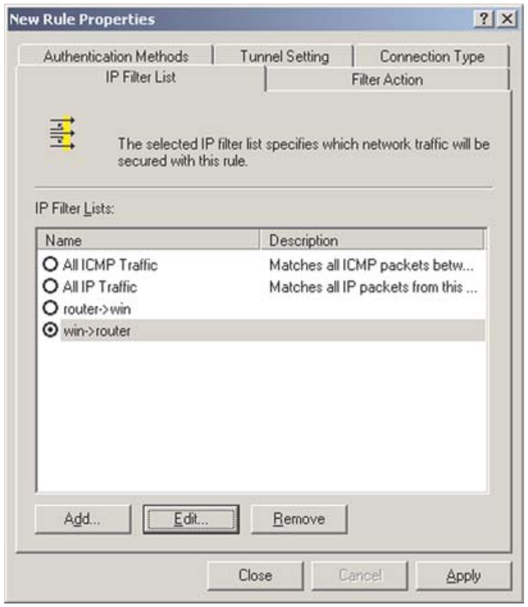
Name	Description
○ All ICMP Traffic	Matches all ICMP packets betw...
○ All IP Traffic	Matches all IP packets from this ...
○ router->win	
○ win->router	

Figure C-9

Step Three: Configure Individual Tunnel Rules

Tunnel 1: win->router

1. From the *IP Filter List* tab, shown in Figure C-10, click the filter list **win->router**.



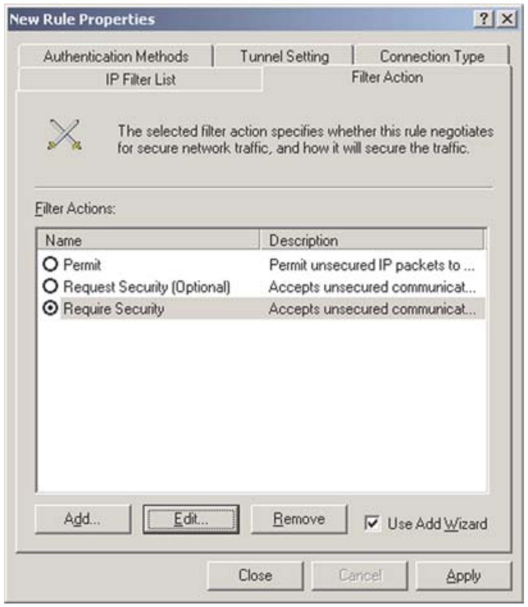
The selected IP filter list specifies which network traffic will be secured with this rule.

IP Filter Lists:

Name	Description
○ All ICMP Traffic	Matches all ICMP packets betw...
○ All IP Traffic	Matches all IP packets from this ...
○ router->win	
● win->router	

Figure C-10

2. Click the **Filter Action** tab (as in Figure C-11), and click the filter action **Require Security** radio button. Then, click the **Edit** button.



The selected filter action specifies whether this rule negotiates for secure network traffic, and how it will secure the traffic.

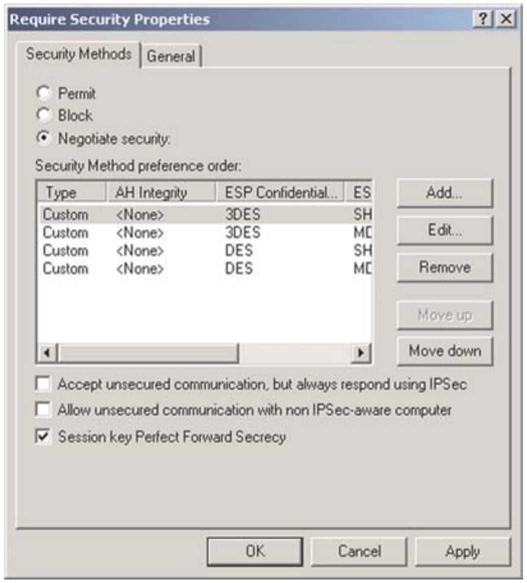
Filter Actions:

Name	Description
○ Permit	Permit unsecured IP packets to ...
○ Request Security (Optional)	Accepts unsecured communicat...
● Require Security	Accepts unsecured communicat...

☑ Use Add Wizard

Figure C-11

3. From the *Security Methods* tab, shown in Figure C-12, verify that the **Negotiate security** option is enabled, and deselect the **Accept unsecured communication, but always respond using IPSec** check box. Select **Session key Perfect Forward Secrecy**, and click the **OK** button.



○ Permit
○ Block
● Negotiate security:

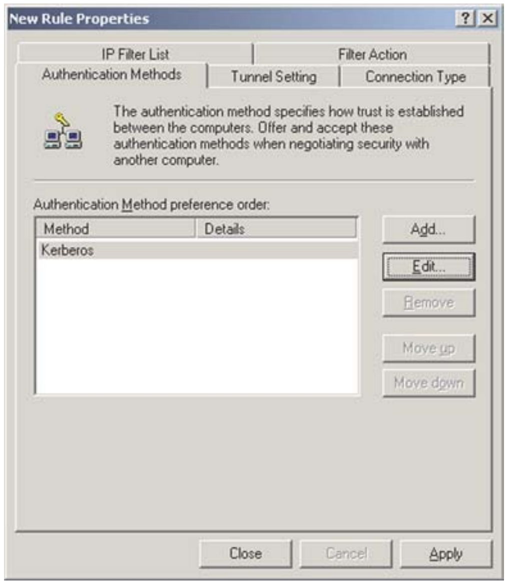
Security Method preference order:

Type	AH Integrity	ESP Confidential...	ES
Custom	<None>	3DES	SH
Custom	<None>	3DES	MD
Custom	<None>	DES	SH
Custom	<None>	DES	MD

□ Accept unsecured communication, but always respond using IPSec
□ Allow unsecured communication with non IPSec-aware computer
☑ Session key Perfect Forward Secrecy

Figure C-12

4. Select the **Authentication Methods** tab, shown in Figure C-13, and click the **Edit** button.



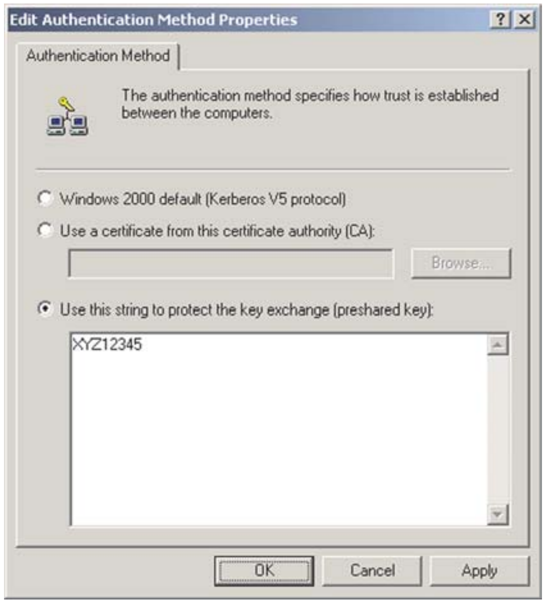
The authentication method specifies how trust is established between the computers. Offer and accept these authentication methods when negotiating security with another computer.

Authentication Method preference order:

Method	Details
Kerberos	

Figure C-13

5. Change the authentication method to **Use this string to protect the key exchange (pre-shared key)**, as shown in Figure C-14, and enter the preshared key string, such as **XYZ12345**. Click the **OK** button.



The authentication method specifies how trust is established between the computers.

○ Windows 2000 default (Kerberos V5 protocol)

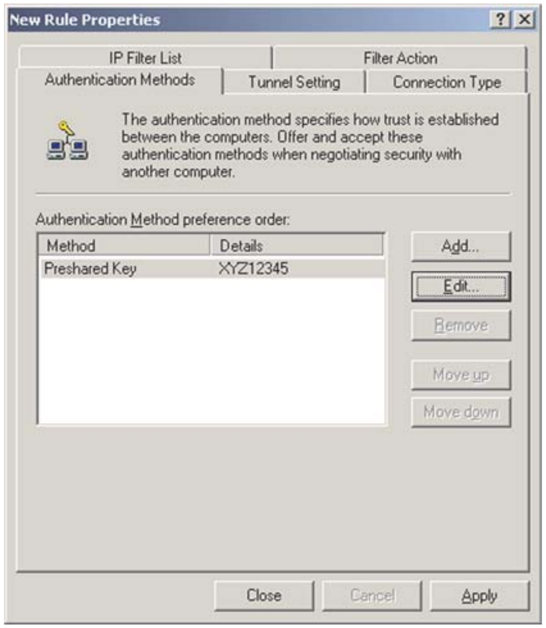
○ Use a certificate from this certificate authority (CA):

● Use this string to protect the key exchange (preshared key):

XYZ12345

Figure C-14

6. This new Preshared key will be displayed in Figure C-15. Click the **OK** or **Close** button to continue.



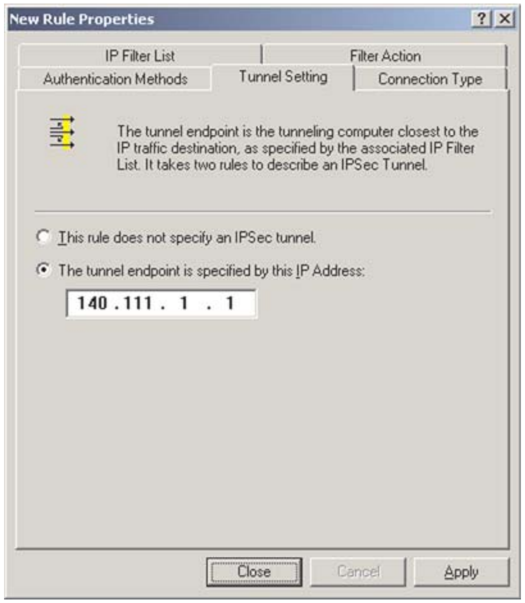
The authentication method specifies how trust is established between the computers. Offer and accept these authentication methods when negotiating security with another computer.

Authentication Method preference order:

Method	Details
Preshared Key	XYZ12345

Figure C-15

7. Select the **Tunnel Setting** tab, shown in Figure C-16, and click **The tunnel endpoint is specified by this IP Address** radio button. Then, enter the Router's **WAN IP Address**.



The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the associated IP Filter List. It takes two rules to describe an IPSec Tunnel.

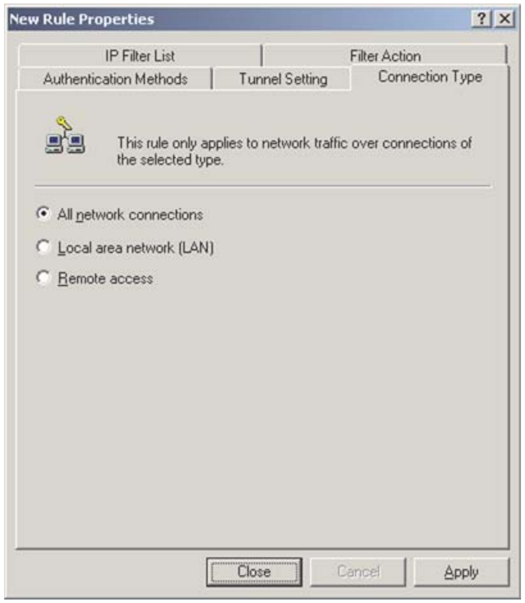
○ This rule does not specify an IPSec tunnel.

● The tunnel endpoint is specified by this IP Address:

140 .111 . 1 . 1

Figure C-16

8. Select the **Connection Type** tab, as shown in Figure C-17, and click **All network connections**. Then, click the **OK** or **Close** button to finish this rule.



This rule only applies to network traffic over connections of the selected type.

● All network connections

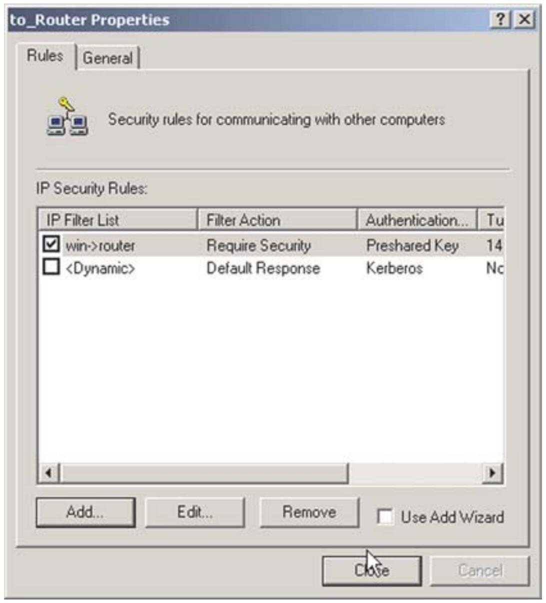
○ Local area network (LAN)

○ Remote access

Figure C-17

Tunnel 2: router->win

9. In the screen, shown in Figure C-18, make sure that "win -> router" is select and deselect the **Use Add Wizard** check box. Then, click the **Add** button to create the second IP filter.



Security rules for communicating with other computers

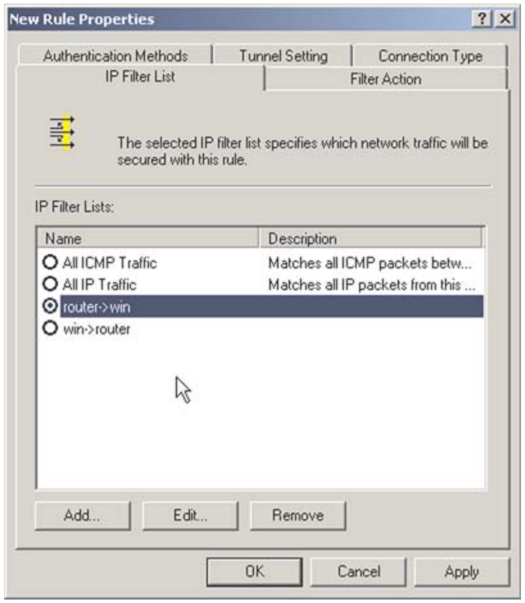
IP Security Rules:

IP Filter List	Filter Action	Authentication...	Tu
☑ win->router	Require Security	Preshared Key	14
☐ <Dynamic>	Default Response	Kerberos	Nc

☐ Use Add Wizard

Figure C-18

10. Go to the **IP Filter List** tab, and click the filter list **router->win**, as shown in Figure C-19



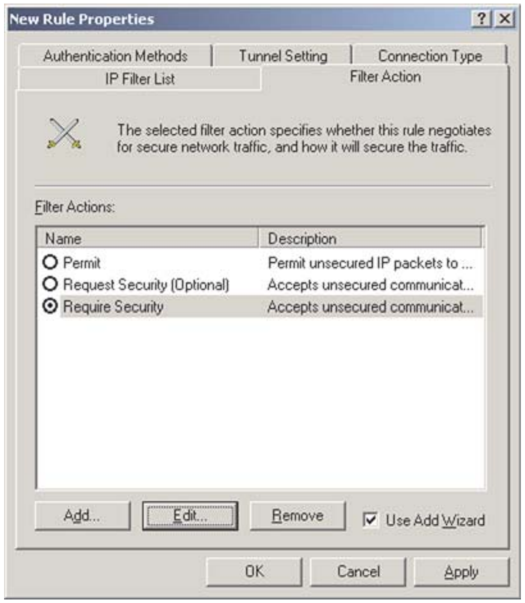
The selected IP filter list specifies which network traffic will be secured with this rule.

IP Filter Lists:

Name	Description
○ All ICMP Traffic	Matches all ICMP packets betw...
○ All IP Traffic	Matches all IP packets from this ...
● router->win	
○ win->router	

Figure C-19

11. Click the **Filter Action** tab, and select the filter action **Require Security**, as shown in Figure C-20. Then, click the **Edit** button.



The selected filter action specifies whether this rule negotiates for secure network traffic, and how it will secure the traffic.

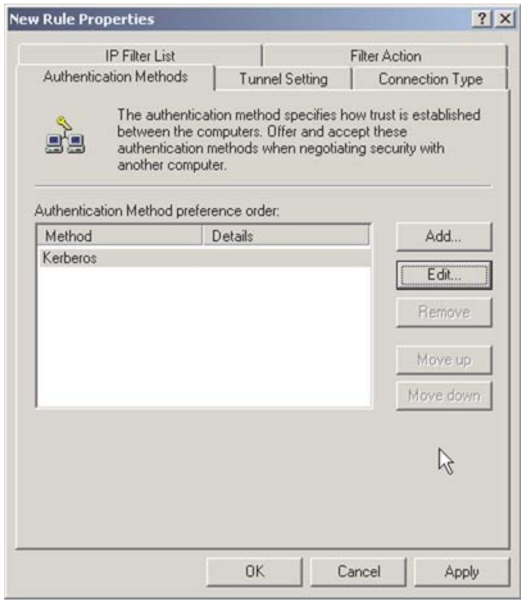
Filter Actions:

Name	Description
○ Permit	Permit unsecured IP packets to ...
○ Request Security (Optional)	Accepts unsecured communicat...
● Require Security	Accepts unsecured communicat...

☑ Use Add Wizard

Figure C-20

12. Click the **Authentication Methods** tab, and verify that the authentication method *Kerberos* is selected, as shown in Figure C-21. Then, click the **Edit** button.



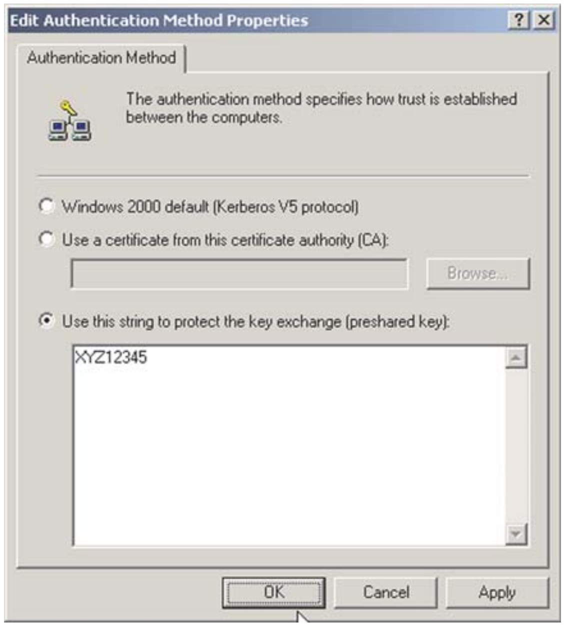
The authentication method specifies how trust is established between the computers. Offer and accept these authentication methods when negotiating security with another computer.

Authentication Method preference order:

Method	Details
Kerberos	

Figure C-21

13. Change the authentication method to **Use this string to protect the key exchange (preshared key)**, and enter the preshared key string, such as **XYZ12345**, as shown in Figure C-22. (This is a sample key string. Yours should be a key that is unique but easy to remember.) Then click the **OK** button.


Edit Authentication Method Properties

The authentication method specifies how trust is established between the computers.

○ Windows 2000 default (Kerberos V5 protocol)

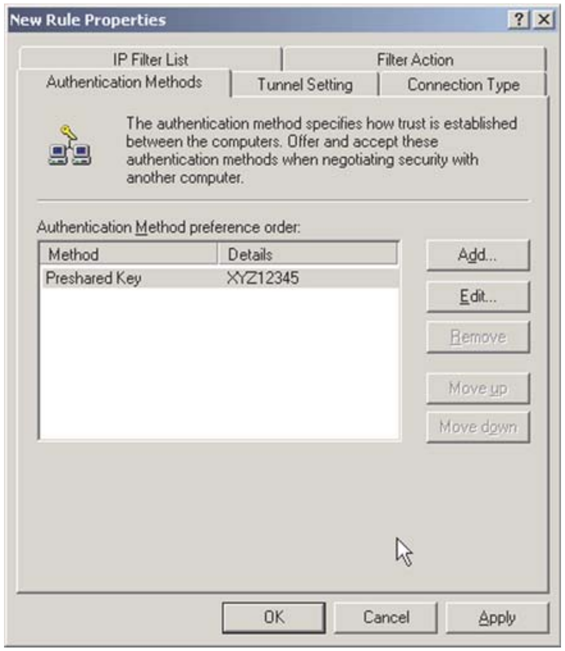
○ Use a certificate from this certificate authority (CA):

● Use this string to protect the key exchange (preshared key):

XYZ12345

Figure C-22

14. This new Preshared key will be displayed in Figure C-23. Click the **OK** button to continue.


New Rule Properties

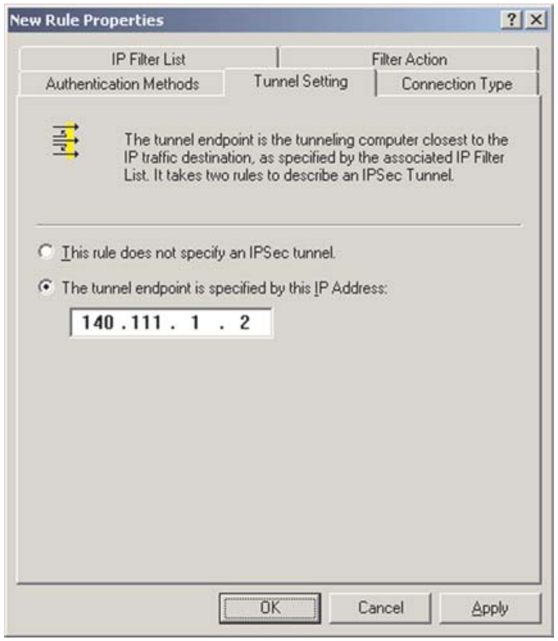
The authentication method specifies how trust is established between the computers. Offer and accept these authentication methods when negotiating security with another computer.

Authentication Method preference order:

Method	Details
Preshared Key	XYZ12345

Figure C-23

15. From the Tunnel Setting tab, shown in Figure C-24, click the radio button for **The tunnel endpoint is specified by this IP Address**, and enter the Windows 2000/XP computer's IP Address.


New Rule Properties

The tunnel endpoint is the tunneling computer closest to the IP traffic destination, as specified by the associated IP Filter List. It takes two rules to describe an IPSec Tunnel.

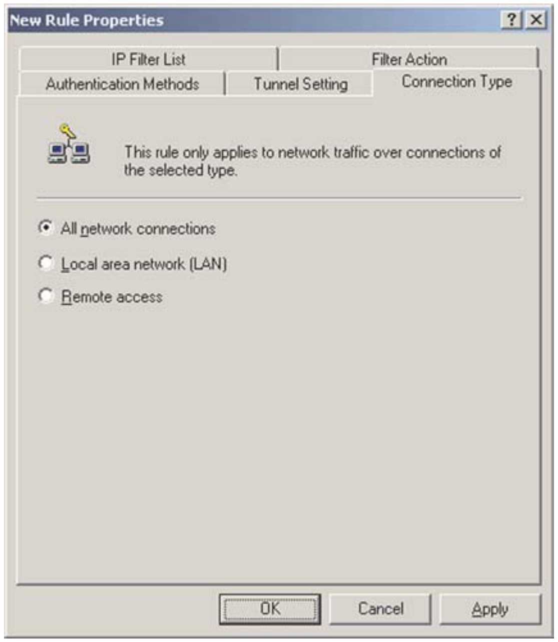
○ This rule does not specify an IPSec tunnel.

● The tunnel endpoint is specified by this IP Address:

140 . 111 . 1 . 2

Figure C-24

16. Click the **Connection Type** tab, shown in Figure C-25, and select **All network connections**. Then click the **OK** (for Windows XP) or **Close** (for Windows 2000) button to finish.


New Rule Properties

This rule only applies to network traffic over connections of the selected type.

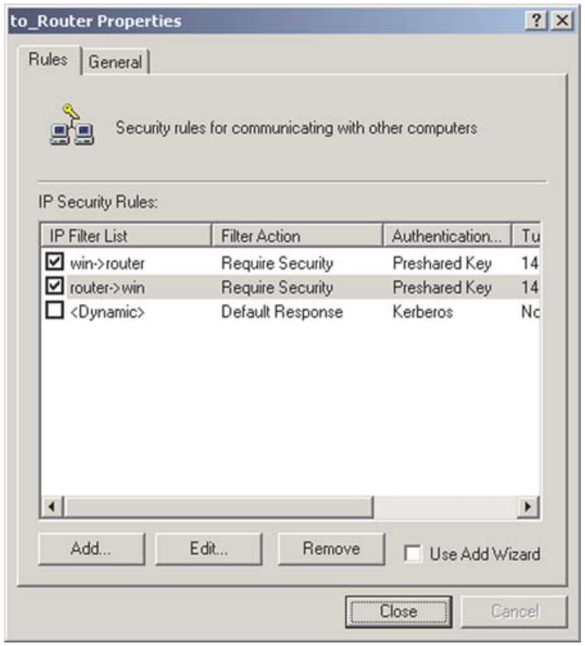
● All network connections

○ Local area network (LAN)

○ Remote access

Figure C-25

17. From the Rules tab, shown in Figure C-26, click the **Close** button to return to the secpol screen.



to_Router Properties

Rules | General

Security rules for communicating with other computers

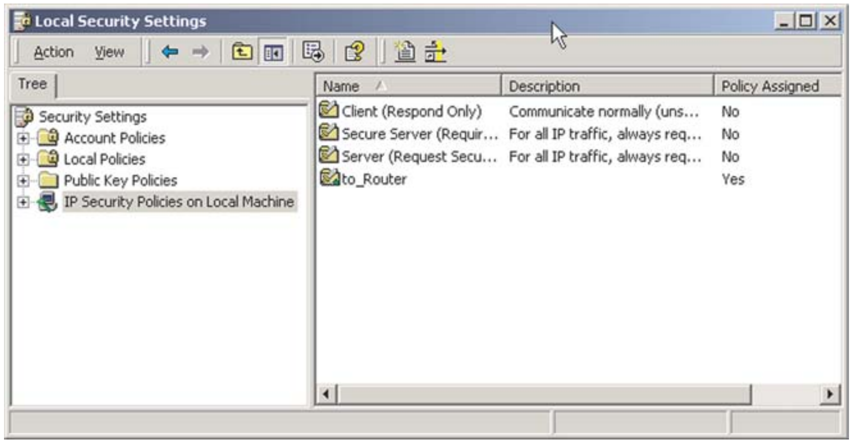
IP Security Rules:

	IP Filter List	Filter Action	Authentication...	Tu
☑	win->router	Require Security	Preshared Key	14
☑	router->win	Require Security	Preshared Key	14
☐	<Dynamic>	Default Response	Kerberos	Nc

Figure C-26

Step Four: Assign New IPSec Policy

In the **IP Security Policies on Local Computer** window, shown in Figure C-27, right-click the policy named **to_router**, and click **Assign**. A green arrow appears in the folder icon.



Local Security Settings

- Security Settings
  - Account Policies
  - Local Policies
  - Public Key Policies
  - IP Security Policies on Local Machine

Name	Description	Policy Assigned
Client (Respond Only)	Communicate normally (uns...	No
Secure Server (Requir...	For all IP traffic, always req...	No
Server (Request Secu...	For all IP traffic, always req...	No
to_Router		Yes

Figure C-27

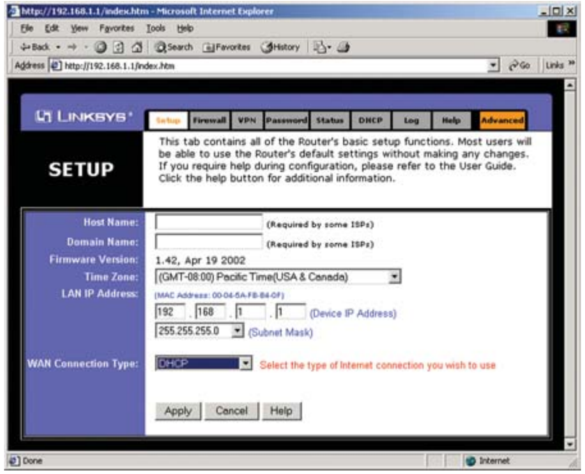
Step Five: Create a Tunnel Through the Web-Based Utility

> **Note:** Further details on this step can be found in the VPN Tab section in “Chapter 7: The Cable/DSL Firewall Router’s Web-Based Utility”.

1. Open your web browser, and enter **192.168.1.1** in the Address field. Press the **Enter** key.

2. When the User name and Password field appears, skip the user name and enter the default password **admin**. Press the **Enter** key.

3. From the Setup tab, shown in Figure C-28, click the **VPN** tab.



http://192.168.1.1/index.htm - Microsoft Internet Explorer

Address: http://192.168.1.1/index.htm

This tab contains all of the Router's basic setup functions. Most users will be able to use the Router's default settings without making any changes. If you require help during configuration, please refer to the User Guide. Click the help button for additional information.

Host Name: (Required by some ISPs)

Domain Name: (Required by some ISPs)

Firmware Version: 1.42, Apr 19 2002

Time Zone: (GMT-08:00) Pacific Time(USA & Canada)

LAN IP Address: (MAC Address: 00-04-5A-FB-84-0F)

192 . 168 . 1 . 1 (Device IP Address)

255.255.255.0 (Subnet Mask)

WAN Connection Type: DHCP Select the type of Internet connection you wish to use

Figure C-28

4. From the VPN tab, shown in Figure C-29, select **Enable** beside This Tunnel.

5. Enter a **Tunnel Name**. This name should be unique for this particular tunnel.

6. Select **Subnet** from the pull-down menu beside Local Secure Group. Then, enter the **IP Address** for this group. This would be the IP Address of the local endpoint, your endpoint.

7. Select **IP Addr.** from the pull-down menu beside Remote Secure Group. Then, enter the **IP Address** for this group. This would be the IP Address of the remote endpoint, the endpoint on the other side of the tunnel.

8. Select **IP Addr.** from the pull-down menu beside Remote Security Gateway. This would be the IP Address of your Internet connection as seen from the Internet. Enter this **IP Address** here.

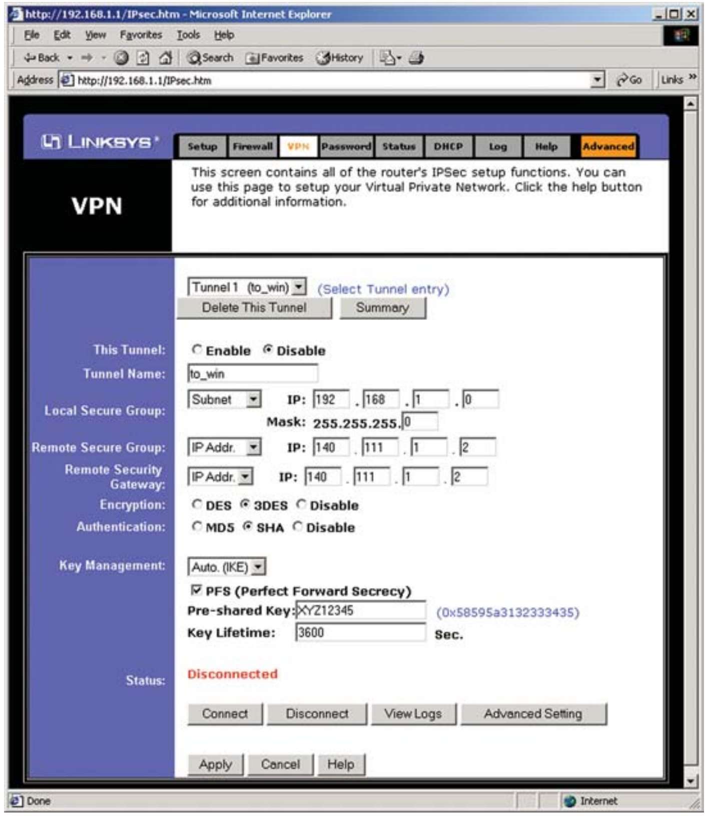
9. Select a type of **encryption** and **authentication** for the tunnel your are establishing.

10. Check **PFS (Perfect Forward Secrecy)** and enter the **Pre-Shared Key** and **Key Lifetime**.

11. Click the **Apply** button followed by the **Continue** button.

12. Click the **Connect** button.

Your tunnel should now be established.


http://192.168.1.1/IPsec.htm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.1.1/IPsec.htm
Go Links
LINKSYS
Setup Firewall VPN Password Status DHCP Log Help Advanced
VPN
Delete This Tunnel
Summary
Connect Disconnect View Logs Advanced Setting
Apply Cancel Help
Done
Internet

This screen contains all of the router's IPSec setup functions. You can use this page to setup your Virtual Private Network. Click the help button for additional information.

Tunnel 1 (to_win) (Select Tunnel entry)

This Tunnel: ○ Enable ● Disable

Tunnel Name: to_win

Local Secure Group: Subnet IP: 192 . 168 . 1 . 0 Mask: 255.255.255.0

Remote Secure Group: IP Addr. IP: 140 . 111 . 1 . 2

Remote Security Gateway: IP Addr. IP: 140 . 111 . 1 . 2

Encryption: ○ DES ● 3DES ○ Disable

Authentication: ○ MD5 ● SHA ○ Disable

Key Management: Auto. (IKE)

☑ PFS (Perfect Forward Secrecy)

Pre-shared Key: XYZ12345 (0x58595a3132333435)

Key Lifetime: 3600 Sec.

Status: Disconnected

Figure C-29

Appendix D: SNMP Functions

SNMP (**S**imple **N**etwork **M**anagement **P**rotocol) is a widely-used network monitoring and control protocol. Data is passed from a SNMP agent, such as the EtherFast Cable/DSL Firewall Router with 4-Port 10/100 Switch/VPN Endpoint to the workstation console used to oversee the network. The Router then returns information contained in a MIB (Management Information Base), which is a data structure that defines what is obtainable from the device and what can be controlled (turned off, on, etc.).

SNMP functions, such as statistics, configuration, and device information, are not available without third-party Management Software. The EtherFast Cable/DSL Firewall Router with 4-Port Switch/VPN Endpoint is compatible with all HP Openview compliant software.

Appendix E: How to Ping Your ISP's E-mail & Web Addresses

Virtually all Internet addresses are configured with words or characters (e.g., *www.linksys.com*, *www.yahoo.com*, etc.) In actuality, however, these Internet addresses are assigned to IP addresses, which are the true addresses on the Internet. For example, *www.linksys.com* is actually 216.23.162.142. Type it into your web browser and you will wind up at the Linksys home page every time. There are servers that translate the URL to an IP address; this is called Domain Name System (DNS).

IP and web addresses, however, can sometimes be long and hard to remember. Because of this, certain ISPs will shorten their server addresses to single words or codes on their users' web browser or e-mail configurations. If your ISP's e-mail and web server addresses are configured with single words (*www*, *e-mail*, *home*, *pop3*, etc.) rather than whole Internet addresses or IP addresses, the Router may have problems sending or receiving mail and accessing the Internet. This happens because the Router has not been configured by your ISP to accept their abbreviated server addresses.

The solution is to determine the true web addresses behind your ISPs code words. You can determine the IP and web addresses of your ISP's servers by "pinging" them.

Important: If you don't have your ISP's web and e-mail IP addresses, you *must* either get them from your ISP or follow these steps *prior* to connecting your Router to your network.

Step One: Pinging an IP Address

The first step to determining your ISP's web and e-mail server address is to ping its IP address.

1. **Power on the computer and the cable or DSL modem**, and restore the network configuration set by your ISP if you have since changed it.

2. **Click Start**, then **Run,** and type **command**. This will bring up the DOS window.

3. **At the DOS command prompt**, type **ping mail** (assuming that the location for which you're trying to find an IP address is configured as *mail*). Press **Enter**. Information such as the following data, taken from a ping of Microsoft Network's e-mail server, will be displayed.

```
C:\>ping mail

Pinging mail [24.53.32.4] with 32 bytes of data:

Reply from 24.53.32.4: bytes=32 time<10ms TTL=128
Reply from 24.53.32.4: bytes=32 time<10ms TTL=128
Reply from 24.53.32.4: bytes=32 time<10ms TTL=128
Reply from 24.53.32.4: bytes=32 time<10ms TTL=128

Ping statistics for 24.53.32.4:
     Packets: Sent = 4, Received = 4, Lost = 0 (0%
   loss),
Approximate round trip times in milli-seconds:
     Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

Figure E-1

4. **Write down the IP address returned by the ping command**. (In the example above: 24.53.32.4.) This IP address is the actual IP address of the server *mail*, or any other word or value you have pinged.

Step Two: Pinging for a Web Address

While the IP address returned above would work as your e-mail server address, it may not be permanent. IP addresses change all the time. Web addresses, however, usually don't. Because of this, you're likely to have fewer problems by configuring your system with web addresses rather than IP addresses. Follow the instructions below to find the web address assigned to the IP address you just pinged.

1. **At the DOS command prompt**, type **ping -a 24.53.32.4**, where 24.53.32.4 is the IP address you just pinged. Information such as the following data will be displayed.

```
C:\>ping -a 24.53.32.4

Pinging mail.msnv3.occa.home.com [24.53.32.4] with
   32 bytes of data:

Reply from 24.53.32.4: bytes=32 time<10ms TTL=127
Reply from 24.53.32.4: bytes=32 time<10ms TTL=127
Reply from 24.53.32.4: bytes=32 time<10ms TTL=127
Reply from 24.53.32.4: bytes=32 time<10ms TTL=127

Ping statistics for 24.53.32.4:
     Packets: Sent = 4, Received = 4, Lost = 0 (0%
   loss),
Approximate round trip times in milli-seconds:
     Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

Figure E-2

2. **Write down the web address returned by the ping command** (In the example in Figure C-2: *mail.msnv3.occa.home.com* is the web address). This web address is the web address assigned to the IP address you just pinged. While the IP address of *mail* could conceivably change, it is likely that this web address will not.

3. **Replace your ISP's abbreviated server address** with this extended web address in the corresponding Internet application (web browser, e-mail application, etc.).

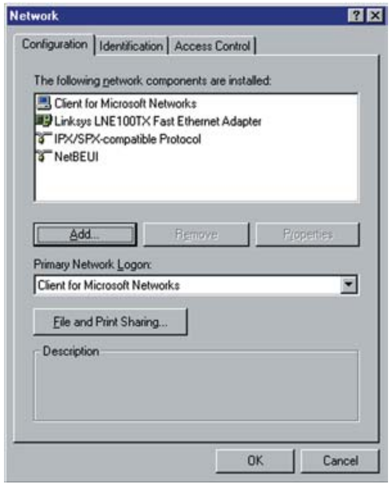
Once you have replaced the brief server address with the true server address, the Router should have no problem accessing the Internet through that Internet application.

Appendix F: Installing the TCP/IP Protocol

Follow these instructions to install the TCP/IP protocol on one of your PCs *only* after a network card has been successfully installed inside the PC. These instructions are for Windows 95, Windows 98, and Windows Me. For TCP/IP setup under Windows NT, 2000, and XP, see your Windows documentation or the Help feature.

1. Click the **Start** button. Choose **Settings** and then **Control Panel**.

2. Double-click on the **Network** icon to bring up your Network window. Select the **Configuration** tab.



The following network components are installed:

Client for Microsoft Networks
Linksys LNE100TX Fast Ethernet Adapter
IPX/SPX-compatible Protocol
NetBEUI

Primary Network Logon: Client for Microsoft Networks

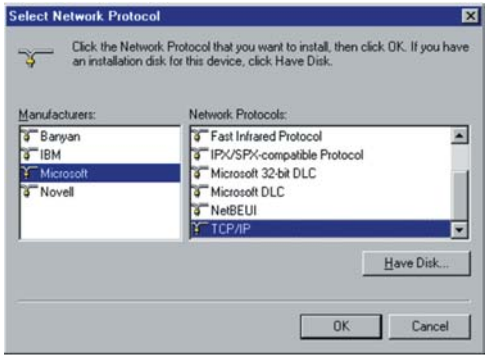
Figure F-1

3. Click the **Add** button**.**

4. Double-click on **Protocol**.

5. Highlight **Microsoft** under the list of manufacturers.

6. Find and double-click **TCP/IP** in the list to the right (see Figure F-2).



Select Network Protocol

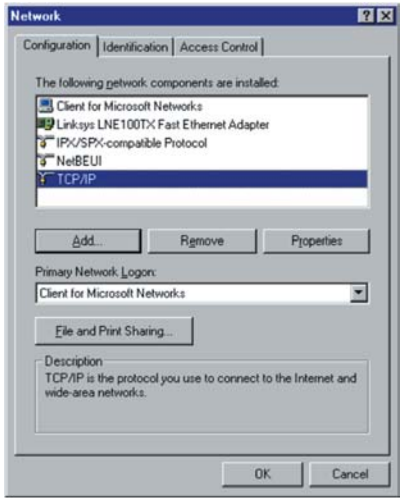
Click the Network Protocol that you want to install, then click OK. If you have an installation disk for this device, click Have Disk.

Manufacturers:
- Banyan
- IBM
- Microsoft
- Novell

Network Protocols:
- Fast Infrared Protocol
- IPX/SPX-compatible Protocol
- Microsoft 32-bit DLC
- Microsoft DLC
- NetBEUI
- TCP/IP

Figure F-2

7. After a few seconds, the main Network window will appear. The TCP/IP Protocol should now be listed.



Network

The following network components are installed:
- Client for Microsoft Networks
- Linksys LNE100TX Fast Ethernet Adapter
- IPX/SPX-compatible Protocol
- NetBEUI
- TCP/IP

Primary Network Logon: Client for Microsoft Networks

Description
TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

Figure F-3

8. Click the **OK** button. Windows may ask for original Windows installation files. Supply them as needed, e.g., c:\windows\options\cabs, D:\win98, D:\win95, D:\win9x.

9. Windows will ask you to restart the PC. Click the **Yes** button.

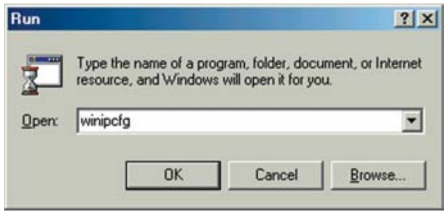
The TCP/IP installation is now complete.

Appendix G: Finding the MAC Address and IP Address for Your Ethernet Adapter

This section describes how to find the MAC address for your Ethernet adapter to do MAC Address Cloning for the Router and ISP. You can also find the IP address of your computer's Ethernet adapter. The IP address is used for filtering, forwarding, and DMZ. Follow the steps in this appendix to find the MAC address or IP address for your adapter in Windows 95, 98, Me, NT, 2000, and XP.

For Windows 95, 98, and Me:

1. Click on **Start** and **Run**. In the Open field, enter **winipcfg**. Then press the **Enter** key or the **OK** button.



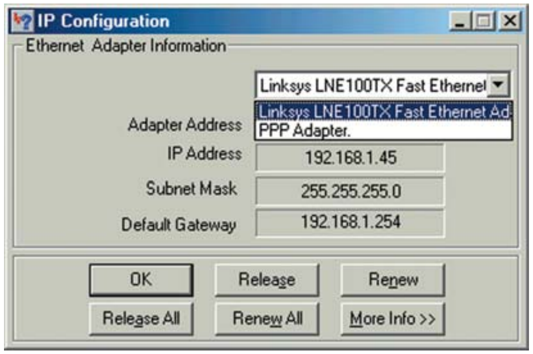
Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: winipcfg

Figure G-1

2. When the IP Configuration window appears, select the Ethernet adapter you are using to connect to the Router via a CAT 5 Ethernet cable.



IP Configuration

Ethernet Adapter Information

Linksys LNE100TX Fast Ethernet
- Linksys LNE100TX Fast Ethernet Ad
- PPP Adapter.

Adapter Address

IP Address 192.168.1.45

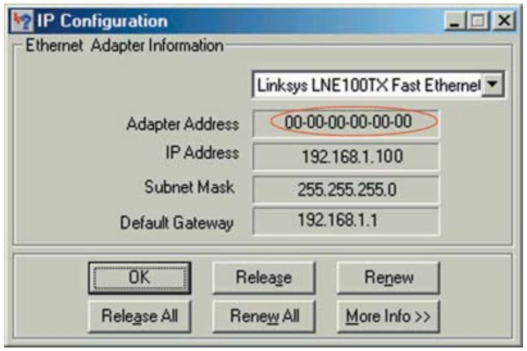
Subnet Mask 255.255.255.0

Default Gateway 192.168.1.254

Figure G-2

3. Write down the Adapter Address as shown on your computer screen (see Figure G-3). This is the MAC address for your Ethernet adapter and will be shown as a series of numbers and letters.

   The MAC address/Adapter Address is what you will use for MAC Address Cloning.



IP Configuration

Ethernet Adapter Information

Linksys LNE100TX Fast Ethernet

Adapter Address: 00-00-00-00-00-00

IP Address: 192.168.1.100

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

Figure G-3

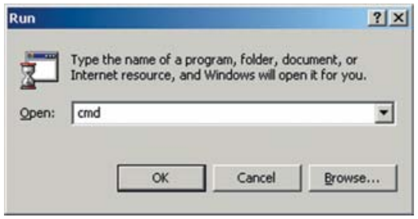
The example in Figure G-3 shows the IP address of your Ethernet adapter as 192.168.1.100. Your computer may show something different.

> **Note**: The MAC address is also called the Adapter Address.

For Windows NT, 2000, and XP:

The following steps show an alternative way of obtaining the MAC address and IP address for your Ethernet adapter.

1. Click on **Start** and **Run**. In the Open field, enter **cmd**. Press the **Enter** key or click the **OK** button.



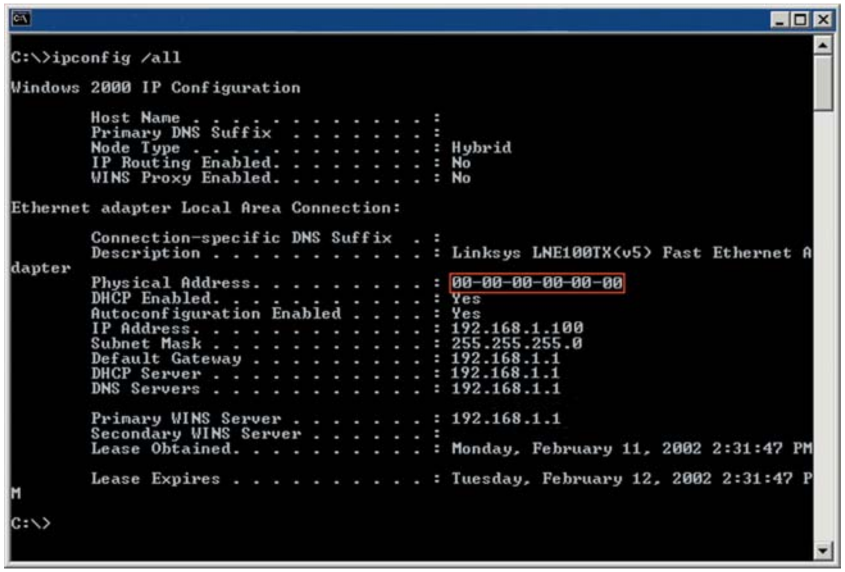
Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: cmd

Figure G-4

2. In the command prompt, enter **ipconfig /all**. Then press the **Enter** key.



```
C:\>ipconfig /all

Windows 2000 IP Configuration

        Host Name . . . . . . . . . . . . :
        Primary DNS Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Linksys LNE100TX(v5) Fast Ethernet A
dapter
        Physical Address. . . . . . . . . : 00-00-00-00-00-00
        DHCP Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.1.100
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1
        DHCP Server . . . . . . . . . . . : 192.168.1.1
        DNS Servers . . . . . . . . . . . : 192.168.1.1

        Primary WINS Server . . . . . . . : 192.168.1.1
        Secondary WINS Server . . . . . . :
        Lease Obtained. . . . . . . . . . : Monday, February 11, 2002 2:31:47 PM

        Lease Expires . . . . . . . . . . : Tuesday, February 12, 2002 2:31:47 P
M

C:\>
```

Figure G-5

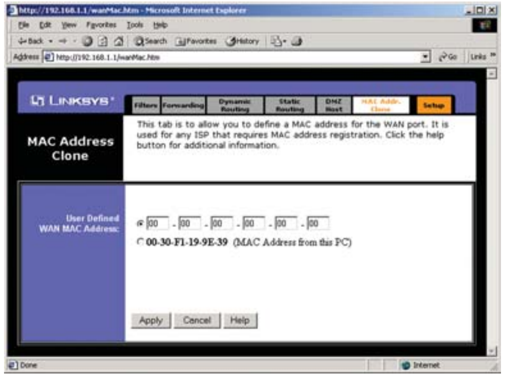
3. Write down the Physical Address as shown on your computer screen; it is the MAC address for your Ethernet adapter. This will appear as a series of letters and numbers.

   The MAC address/Physical Address is what you will use for MAC Address Cloning.

> **Note**: The MAC address is also called the Physical Address.

The example in Figure G-5 shows the IP address of your Ethernet adapter as 192.168.1.100. Your computer may show something different.

When entering information for MAC Address Cloning, type the **12-digit MAC address** (see Figure G-6).


http://192.168.1.1/wanMac.htm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.1.1/wanMac.htm
Go Links
LINKSYS
Filters
Forwarding
Dynamic Routing
Static Routing
DMZ Host
MAC Addr. Clone
Setup
MAC Address Clone
Apply
Cancel
Help
Done
Internet

This tab is to allow you to define a MAC address for the WAN port. It is used for any ISP that requires MAC address registration. Click the help button for additional information.

User Defined WAN MAC Address: ● 00 - 00 - 00 - 00 - 00 - 00

○ 00-30-F1-19-9E-39 (MAC Address from this PC)

Figure G-6

Appendix H: Glossary

3DES - 3DES is a variation on DES that uses a 168-bit key.

Adapter - Printed circuit board that plugs into a PC to add to capabilities or connectivity to a PC.

AppleTalk - An Apple Computer networking system that supports Apple's proprietary local talk.

Backbone - The part of a network that connects most of the systems and networks together and handles the most data.

Bit - A binary digit. The value - 0 or 1-used in the binary numbering system. Also, the smallest form of data.

Boot - To cause the computer to start executing instructions. Personal computers contain built-in instructions in a ROM chip that are automatically executed on startup. These instructions search for the operating system, load it and pass control to it.

Bridge - A device that interconnects different networks together.

Broadband - A data-transmission scheme in which multiple signals share the bandwidth of a medium. This allows the transmission of voice, data and video signals over a single medium. Cable television uses broadband techniques to deliver dozens of channels over one cable.

Browser - A browser is an application program that provides a way to look at and interact with all the information on the World Wide Web or PC. The word "browser" seems to have originated prior to the Web as a generic term for user interfaces that let you browse text files online.

Buffer - A buffer is a shared or assigned memory area used by hardware devices or program processes that operate at different speeds or with different sets of priorities. The buffer allows each device or process to operate without being held up by the other. In order for a buffer to be effective, the size of the buffer and the algorithms for moving data into and out of the buffer need to be considered by the buffer designer. Like a cache, a buffer is a "midpoint holding place" but exists not so much to accelerate the speed of an activity as to support the coordination of separate activities.

Cable Modem - A device that connects a computer to the cable television network, which in turn connects to the Internet. Once connected, cable modem users have a continuous connection to the Internet. Cable modems feature asymmetric transfer rates: around 36 Mbps downstream (from the Internet to the computer), and from 200 Kbps to 2 Mbps upstream (from the computer to the Internet).

CAT 5 - ANSI/EIA (American National Standards Institute/Electronic Industries Association) Standard 568 is one of several standards that specify "categories" (the singular is commonly referred to as "CAT") of twisted pair cabling systems (wires, junctions, and connectors) in terms of the data rates that they can sustain. CAT 5 cable has a maximum throughput of 100 Mbps and is usually utilized for 100BaseTX networks.

Cookie - Data created by a Web server that is stored on a user's computer. It provides a way for the Web site to keep track of a user's patterns and preferences and, with the cooperation of the Web browser, to store them on the user's own hard disk.

Data Packet - One frame in a packet-switched message. Most data communications is based on dividing the transmitted message into packets. For example, an Ethernet packet can be from 64 to 1518 bytes in length.

Default Gateway - The routing device used to forward all traffic that is not addressed to a station within the local subnet.

Denial of Service - A protocol that directs the network to no longer respond to requests that might arise as the result of a Denial of Service attack.

Denial of Service Attack - An assault on a network that floods it with so many additional requests that regular traffic is either slowed or completely interrupted.

DES (**D**igital **E**ncryption **S**tandard) **-** Encryption used for data communication where both the sender and receiver must know the same secret key, used to encrypt and decrypt the data, or to generate and verify a message authentication code. Linksys DES encryption uses a 56-bit key.

DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol) **-** A protocol that lets network administrators manage centrally and automate the assignment of Internet Protocol (IP) addresses in an organization's network. Using the Internet's set of protocol (TCP/IP), each machine that can connect to the Internet needs a unique IP address. When an organization sets up its computer users with a connection to the Internet, an IP address must be assigned to each machine. Without DHCP, the IP address must be entered manually at each computer and, if computers move to another location in another part of the network, a new IP address must be entered. DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically sends a new IP address when a computer is plugged into a different place in the network.

DHCP uses the concept of a "lease" or amount of time that a given IP address will be valid for a computer. The lease time can vary depending on how long a user is likely to require the Internet connection at a particular location. It's especially useful in education and other environments where users change frequently. Using very short leases, DHCP can dynamically reconfigure networks in which there are more computers than there are available IP addresses.

DHCP supports static addresses for computers containing Web servers that need a permanent IP address.

DMZ (**Dem**ilitarized **Z**one) **-** Allows one IP address (or computer) to be exposed to the Internet. Some applications require multiple TCP/IP ports to be open. It is recommended that you set your computer with a static IP address if you want to use DMZ Hosting.

DNS - The domain name system (DNS) is the way that Internet domain name are located and translated into Internet Protocol (IP) addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address.

Domain - A subnetwork comprised of a group of clients and servers under the control of one security database. Dividing LANs into domains improves performance and security.

Download - To receive a file transmitted over a network. In a communications session, download means receive, upload means transmit.

DSL (**D**igital **S**ubscriber **L**ine) **-** A technology that dramatically increases the digital capacity of ordinary telephone lines into the home or office and, by employing unused bandwidth, still allows for normal phone usage. DSL provides "always-on" operation, eliminating the need to dial in to the service.

Dynamic IP Address - An IP address that is automatically assigned to a client station in a TCP/IP network, typically by a DHCP server. Network devices that serve multiple users, such as servers and printers, are usually assigned static IP addresses.

Dynamic Routing - The ability for a router to forward data via a different route based on the current conditions of the communications circuits. For example, it can adjust for overloaded traffic or failing lines and is much more flexible than static routing, which uses a fixed forwarding path.

Encryption - A security method that applies a specific algorithm to data in order to alter the data's appearance and prevent other devices from reading the information.

Ethernet - IEEE standard network protocol that specifies how data is placed on and retrieved from a common transmission medium. Has a transfer rate of 10 Mbps. Forms the underlying transport vehicle used by several upper-level protocols, including TCP/IP and XNS.

Fast Ethernet - A 100 Mbps technology based on the 10Base-T Ethernet CSMA/CD network access method.

Finger - A UNIX command widely used on the Internet to find out information about a particular user, such as telephone number, whether currently logged on or the last time logged on. The person being "fingered" must have placed his or her profile on the system. Fingering requires entering the full user@domain address.

Firewall - A firewall is a set of related programs, located at a network gateway server, that protects the resources of a network from users from other networks. (The term also implies the security policy that is used with the programs.) An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources and for controlling what outside resources to which its own users have access.

Basically, a firewall, working closely with a router, examines each network packet to determine whether to forward it toward its destination.

Firmware - Code that is written onto read-only memory (ROM) or programmable read-only memory (PROM). Once firmware has been written onto the ROM or PROM, it is retained even when the device is turned off.

FTP (**F**ile **T**ransfer **P**rotocol) **-** A protocol used to transfer files over a TCP/IP network (Internet, UNIX, etc.). For example, after developing the HTML pages for a Web site on a local machine, they are typically uploaded to the Web server using FTP.

FTP includes functions to log onto the network, list directories and copy files. It can also convert between the ASCII and EBCDIC character codes. FTP operations can be performed by typing commands at a command prompt or via an FTP utility running under a graphical interface such as Windows. FTP transfers can also be initiated from within a Web browser by entering the URL preceded with ftp://.

Unlike e-mail programs in which graphics and program files have to be "attached," FTP is designed to handle binary files directly and does not add the overhead of encoding and decoding the data.

Full Duplex - The ability of a device or line to transmit data simultaneously in both directions.

Gateway - A device that interconnects networks with different, incompatible communications protocols.

Half Duplex - Data transmission that can occur in two directions over a single line, but only one direction at a time.

Hardware - Hardware is the physical aspect of computers, telecommunications, and other information technology devices. The term arose as a way to distinguish the "box" and the electronic circuitry and components of a computer from the program you put in it to make it do things. The program came to be known as the software.

Hop - The link between two network nodes.

HTTP (**H**yper**T**ext **T**ransport **P**rotocol) **-** The communications protocol used to connect to servers on the World Wide Web. Its primary function is to establish a connection with a Web server and transmit HTML pages to the client browser.

Hub - The device that serves as the central location for attaching wires from workstations. Can be passive, where there is no amplification of the signals; or active, where the hubs are used like repeaters to provide an extension of the cable that connects to a workstation.

ICMP (**I**nternet **C**ontrol **M**essage **P**rotocol) **-** Part of the TCP/IP protocol. Network devices such as routers or servers use ICMP to transmit error messages and control messages. For example, the PING program uses ICMP.

ICQ - A conferencing program for the Internet that provides interactive chat, e-mail and file transfer and can alert you when someone on your predefined list has also come online.

IEEE (The **I**nstitute of **E**lectrical and **E**lectronics **E**ngineers) **-** The IEEE describes itself as "the world's largest technical professional society, promoting the development and application of electrotechnology and allied sciences for the benefit of humanity, the advancement of the profession, and the well-being of our members."

The IEEE fosters the development of standards that often become national and international standards. The organization publishes a number of journals, has many local chapters, and several large societies in special areas, such as the IEEE Computer Society.

IKE (**I**nternet **K**ey **E**xchange) **-** A negotiation and key exchange protocol specified by the Internet Engineering Task Force. An IKE security association (SA) automatically negotiates encryption and authentication keys. With IKE, an initial exchange authenticates the VPN session and automatically negotiates keys that will be used to pass encrypted data over the Internet or any other network.

IP (**I**nternet **P**rotocol) **-** The method or protocol by which data is sent from one computer to another on the Internet. It is a standard set of rules, procedures, or conventions relating to the format and timing of data transmission between two computers that they must accept and use to be able to understand each other.

IP Address - In the most widely installed level of the Internet Protocol (IP) today, an IP address is a 32-binary digit number that identifies each sender or receiver of information that is sent in packet across the Internet. When you request an HTML page or send e-mail, the Internet Protocol part of TCP/IP includes your IP address in the message (actually, in each of the packets if more than one is required) and sends it to the IP address that is obtained by looking up the domain name in the Uniform Resource Locator you requested or in the e-mail address you're sending a note to. At the other end, the recipient can see the IP address of the Web page requestor or the e-mail sender and can respond by sending another message using the IP address it received.

IPSec (**I**nternet **P**rotocol **Sec**urity) **-** A suite of protocols used to implement secure exchange of packets at the IP layer. IPSec supports two basic modes: Transport and Tunnel. Transport encrypts the payload of each packet, leaving the header untouched, while Tunnel mode encrypts both the header and the payload and is therefore more secure. IPSec must be supported on both transmitter and receiver and must share a public key. Tunnel mode is widely deployed in VPNs (Virtual Private Networks).

IPX (**I**nternetwork **P**acket E**X**change) **-** A NetWare communications protocol used to route messages from one node to another. IPX packets include network addresses and can be routed from one network to another.

ISP (**I**nternet **S**ervice **P**rovider) **-** A company that provides individuals and companies access to the Internet and other related services such as Web site building and virtual hosting.

LAN (**L**ocal **A**rea **N**etwork) **-** A group of computers and associated devices that share a common communications line and typically share the resources of a single processor or server within a small geographic area (for example, within an office building).

MAC (**M**edia **A**ccess **C**ontrol) **Address -** A unique number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level.

Mbps (**M**ega**b**its **p**er **s**econd) **-** One million bits per second; unit of measurement for data transmission.

MD5 - A type of one-way authentication method that uses passwords. MD5 authentication is not as secure as the EAP-TLS or EAP/TTLS authentication methods.

MIB (**M**anagement **I**nformation **B**ase) **-** A set of database objects. This set contains information about a specific device for utilizing SNMP.

mIRC - mIRC runs under Windows and provides a graphical interface for logging onto IRC servers and listing, joining and leaving channels.

Multicasting - Sending data to a group of nodes instead of a single destination.

NAT (**N**etwork **A**ddress **T**ranslation) **-** The translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network. One network is designated the inside network and the other is the outside.

NetBIOS - The native networking protocol in DOS and Windows networks. Although originally combined with its transport layer protocol (NetBEUI), NetBIOS today provides a programming interface for applications at the session layer (layer 5). NetBIOS can ride over NetBEUI, its native transport, which is not routable, or over TCP/IP and IPX/SPX, which are routable protocols.

NetBIOS computers are identified by a unique 15-character name, and Windows machines (NetBIOS machines) periodically broadcast their names over the network so that Network Neighborhood can catalog them. For TCP/IP networks, NetBIOS names are turned into IP addresses via manual configuration in an LMHOSTS file or a WINS server.

There are two NetBIOS modes. The Datagram mode is the fastest mode, but does not guarantee delivery. It uses a self-contained packet with send and receive name, usually limited to 512 bytes. If the recipient device is not listening for messages, the datagram is lost. The Session mode establishes a connection until broken. It guarantees delivery of messages up to 64KB long.

Network - A system that transmits any combination of voice, video and/or data between users.

Network Mask - Also known as the "Subnet Mask".

NNTP (**N**etwork **N**ews **T**ransfer **P**rotocol) **-** The protocol used to connect to Usenet groups on the Internet. Usenet newsreaders support the NNTP protocol.

Node - A network junction or connection point, typically a computer or work station.

Notebook (PC) **-** A notebook computer is a battery-powered personal computer generally smaller than a briefcase that can easily be transported and conveniently used in temporary spaces such as on airplanes, in libraries, temporary offices, and at meetings. A notebook computer, sometimes called a laptop computer, typically weighs less than five pounds and is three inches or less in thickness.

Packet - A unit of data routed between an origin and a destination in a network.

Packet Filtering - Discarding unwanted network traffic based on its originating address or range of addresses or its type (e-mail, file transfer, etc.).

Ping (**P**acket **IN**ternet **G**roper) **-** An Internet utility used to determine whether a particular IP address is online. It is used to test and debug a network by sending out a packet and waiting for a response.

Plug-and-Play - The ability of a computer system to configure expansion boards and other devices automatically without requiring the user to turn off the system during installation.

POP3 (**P**ost **O**ffice **P**rotocol **3**) **-** A standard mail server commonly used on the Internet. It provides a message store that holds incoming e-mail until users log on and download it. POP3 is a simple system with little selectivity. All pending messages and attachments are downloaded at the same time. POP3 uses the SMTP messaging protocol.

Port - A pathway into and out of the computer or a network device such as a switch or router. For example, the serial and parallel ports on a personal computer are external sockets for plugging in communications lines, modems and printers.

PPPoE (**P**oint to **P**oint **P**rotocol **o**ver **E**thernet) **-** PPPoE is a method for the encapsulation of PPP packets over Ethernet frames from the user to the ISP over the Internet. One reason PPPoE is preferred by ISPs is because it provides authentication (username and password) in addition to data transport. A PPPoE session can be initiated by either a client application residing on a PC, or by client firmware residing on a modem or router.

PPTP (**P**oint-to-**P**oint **T**unneling **P**rotocol) **-** A protocol which allows the Point to Point Protocol (PPP) to be tunneled through an IP network. PPTP does not specify any changes to the PPP protocol but rather describes a "tunneling service" for carrying PPP (a tunneling service is any network service enabled by tunneling protocols such as PPTP, L2F, L2TP, and IPSEC tunnel mode). One example of a tunneling service is secure access from a remote small office network to a headquarters corporate intranet via a Virtual Private Network (VPN) that traverses the Internet. However, tunneling services are not restricted to corporate environments and may also be used for personal (i.e., non-business) applications.

RIP (**R**outing **I**nformation **P**rotocol) **-** A simple routing protocol that is part of the TCP/IP protocol suite. It determines a route based on the smallest hop count between source and destination. RIP is a distance vector protocol that routinely broadcasts routing information to its neighboring routers.

RJ-45 (**R**egistered **J**ack-**45**) **-** A connector similar to a telephone connector that holds up to eight wires, used for connecting Ethernet devices.

Router - Protocol-dependent device that connects subnetworks together. Routers are useful in breaking down a very large network into smaller subnetworks; they introduce longer delays and typically have much lower throughput rates than bridges.

Security Association - A group of security settings related to a specific VPN tunnel.

Server - Any computer whose function in a network is to provide user access to files, printing, communications, and other services.

SMTP (**S**imple **M**ail **T**ransfer **P**rotocol) **-** The standard e-mail protocol on the Internet. It is a TCP/IP protocol that defines the message format and the message transfer agent (MTA), which stores and forwards the mail.

SNMP (**S**imple **N**etwork **M**anagement **P**rotocol) **-** A widely used network monitoring and control protocol. Data is passed from SNMP agents, which are hardware and/or software processes reporting activity in each network device (hub, router, bridge, etc.) to the workstation console used to oversee the network. The agents return information contained in a MIB (Management Information Base), which is a data structure that defines what is obtainable from the device and what can be controlled (turned off, on, etc.).

Software - Instructions for the computer. A series of instructions that performs a particular task is called a "program." The two major categories of software are "system software" and "application software." System software is made up of control programs such as the operating system and database management system (DBMS). Application software is any program that processes data for the user.

SPI (**S**tateful **P**acket **I**nspection) **-** A firewall technology that monitors the state of the transaction so that it can verify that the destination of an inbound packet matches the source of a previous outbound request. It examines not just the headers of the packet, but also the contents, to determine more about the packet than just its source and destination information. It is called "stateful" because verifies that the stated destination computer has previously requested the current communication. In this way, it verifies that all communications are initiated by the recipient computer and are taking place only with sources that are known and trusted from previous interactions. In addition to being a more rigorous inspection, stateful packet inspection closes off ports until connection to the specific port is requested. This allows an added layer of protection from the threat of port scanning.

Static IP Address - A permanent IP address that is assigned to a node in an IP or a TCP/IP network.

Static Routing - Forwarding data in a network via a fixed path. Static routing cannot adjust to changing line conditions as can dynamic routing.

Subnet Mask - The method used for splitting IP networks into a series of subgroups, or subnets. The mask is a binary pattern that is matched up with the IP address to turn part of the host ID address field into a field for subnets.

Switch - 1. A data switch connects computing devices to host computers, allowing a large number of devices to share a limited number of ports. 2. A device for making, breaking, or changing the connections in an electrical circuit.

TCP (**T**ransmission **C**ontrol **P**rotocol) **-** A method (protocol) used along with the IP (Internet Protocol) to send data in the form of message units (datagram) between network devices over a LAN or WAN. While IP takes care of handling the actual delivery of the data (routing), TCP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient delivery over the network. TCP is known as a "connection oriented" protocol due to requiring the receiver of a packet to return an acknowledgment of receipt to the sender of the packet resulting in transmission control.

TCP/IP (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol) **-** The basic communication language or set of protocols for communications over a network (developed specifically for the Internet). TCP/IP defines a suite or group of protocols and not only TCP and IP.

Telnet - A terminal emulation protocol commonly used on the Internet and TCP/IP-based networks. It allows a user at a terminal or computer to log onto a remote device and run a program.

TFTP (**T**rivial **F**ile **T**ransfer **P**rotocol) **-** A version of the TCP/IP FTP protocol that has no directory or password capability.

Throughput - The amount of data moved successfully from one place to another in a given time period.

UDP (**U**ser **D**atagram **P**rotocol) **-** A method (protocol) used along with the IP (Internet Protocol) to send data in the form of message units (datagram) between network devices over a LAN or WAN. While IP takes care of handling the actual delivery of the data (routing), UDP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient delivery over the network. UDP is known as a "connection-less" protocol due to NOT requiring the receiver of a packet to return an acknowledgment of receipt to the sender of the packet (as opposed to TCP).

Upgrade - To replace existing software or firmware with a newer version.

Upload - To transmit a file over a network. In a communications session, upload means transmit, download means receive.

URL (**U**niform **R**esource **L**ocator) **-** The address that defines the route to a file on the Web or any other Internet facility. URLs are typed into the browser to access Web pages, and URLs are embedded within the pages themselves to provide the hypertext links to other pages.

VPN (**V**irtual **P**rivate **N**etwork) **-** A technique that allows two or more LANs to be extended over public communication channels by creating private communication subchannels (tunnels). Effectively, these LANs can use a WAN as a single large "virtually private" LAN. This removes the need to use leased lines for WAN communications through secure use of a publicly available WAN (such as the Internet). Examples of VPN technology are: PPTP (Point to Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol), and IPSec (Internet Protocol Security).

VPN end point - VPN end point capability within a router provides the ability to initiate a VPN tunnel to some other location that supports either a VPN client or has VPN end point capability.

WAN (**W**ide **A**rea **N**etwork)**-** A communications network that covers a relatively large geographic area, consisting of two or more LANs. Broadband communication over the WAN is often through public networks such as the telephone (DSL) or cable systems, or through leased lines or satellites. In its most basic definition, the Internet could be considered a WAN.

WINIPCFG - Configuration utility based on the Win32 API for querying, defining and managing IP addresses within a network. A commonly used utility for configuring networks with static IP addresses.

Appendix I: Specifications

Model Number	BEFSX41
Standards	IEEE 802.3, IEEE 802.3u
Protocol	CSMA/CD
Ports	
WAN:	One 10/100 RJ-45 Port
LAN:	Four 10/100 RJ-45 Ports (One with DMZ Functionality)
Cabling Type	UTP Category 5 or Better
Topology	Star
Speed (Mbps)	
WAN:	10/100 (Half Duplex) 20/200 (Full Duplex)
LAN:	10/100 (Half Duplex) 20/200 (Full Duplex)
LED Indicators	Power, Diag, DMZ
WAN:	Link/Act, Full/Col, 10/100
LAN:	Link/Act, Full/Col, 10/100

Environmental

Dimensions	186 mm x 154 mm x 48 mm
Unit Weight	0.38 kg
Power Input	12V AC, 1000 mA
Certifications	FCC Class B, CE Mark
Operating Temperature	0°C to 40°C
Storage Temperature	-20°C to 70°C
Operating Humidity	10% to 85%, Non-condensing
Storage Humidity	5% to 90%, Non-condensing

Appendix J: Warranty Information

LIMITED WARRANTY
Linksys guarantees that every EtherFast® Cable/DSL Firewall Router with 4-Port Switch/VPN Endpoint is free from physical defects in material and workmanship for two years from the date of purchase (Africa, Europe and Latin America only, other regions may have a different warranty period), when used within the limits set forth in the Specifications section of this User Guide. If you suspect the product is defective during the warranty period, contact Linksys Technical Support in order to obtain a Return Merchandise Authorization (RMA) number or contact the location where the product was purchased (if applicable). BE SURE TO HAVE YOUR PROOF OF PURCHASE ON HAND WHEN CONTACTING TECHNICAL SUPPORT. RETURN REQUESTS CANNOT BE PROCESSED WITHOUT PROOF OF PURCHASE.

IN NO EVENT SHALL LINKSYS' LIABILITY EXCEED THE PRICE PAID FOR THE PRODUCT FROM DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE PRODUCT, ITS ACCOMPANYING SOFTWARE, OR ITS DOCUMENTATION. LINKSYS OFFERS NO REFUNDS FOR ITS PRODUCTS. Linksys makes no warranty or representation, expressed, implied, or statutory, with respect to its products or the contents or use of this documentation and all accompanying software, and specifically disclaims its quality, performance, merchantability, or fitness for any particular purpose. Linksys reserves the right to revise or update its products, software, or documentation without obligation to notify any individual or entity. Please direct all inquiries to the address listed below or contact Technical Support:

Linksys
P.O. Box 18558
Irvine, California 92623
U.S.A.

Appendix K: Contact Information

For help with the installation or operation of this product, contact Linksys Technical Support at one of the phone numbers listed on the Technical Support insert or one of the Internet addresses below:

E-mail	
Europe	europe-support@linksys.com
United Kingdom & Ireland	uks@linksys.com
Latin America	latam-soporte@linksys.com
U.S. and Canada	support@linksys.com

For unlisted regions or the most up-to-date contact information, please visit the website below:

Web	http://www.linksys.com/international

LINKSYS®

www.linksys.com

© Copyright 2003 Linksys, All Rights Reserved.