

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

- 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.

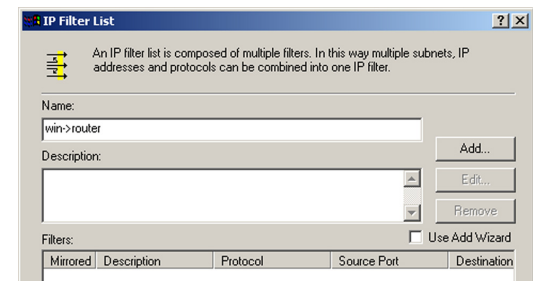


Figure C-4: IP Filter List

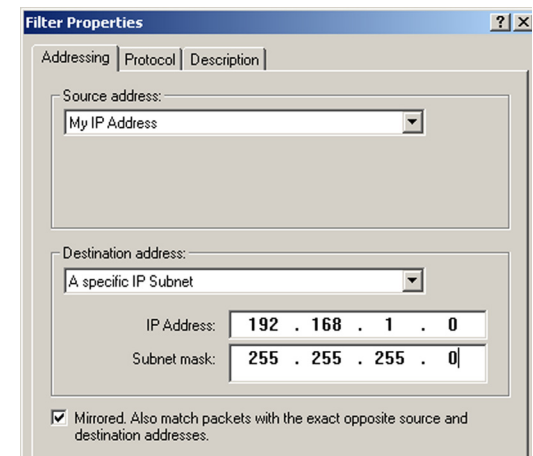


Figure C-5: Filters Properties

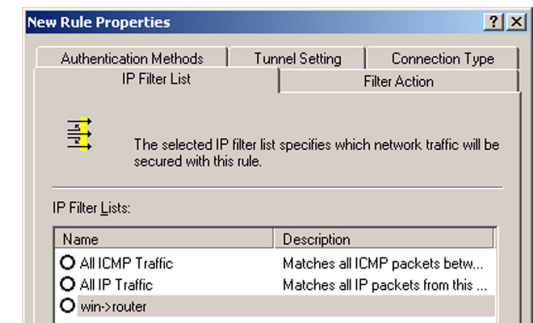


Figure C-6: New Rule Properties

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.
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.
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.

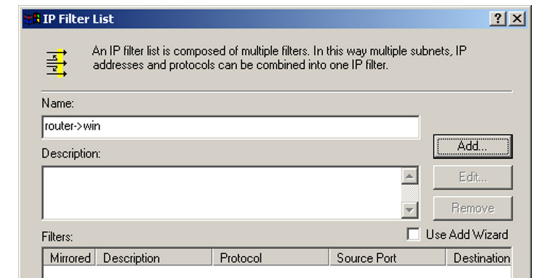


Figure C-7: IP Filter List

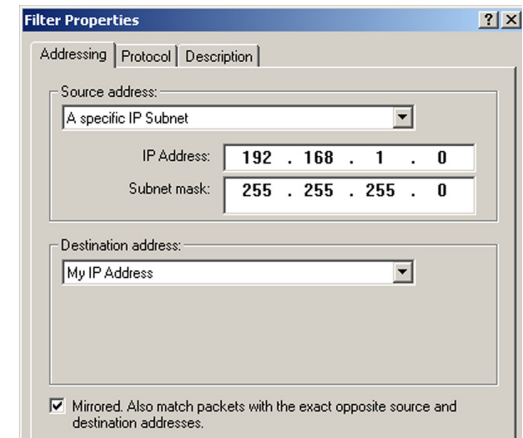


Figure C-8: Filters Properties

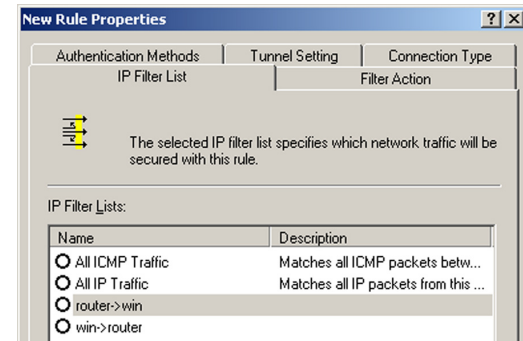


Figure C-9: New Rule Properties

Step 3: 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.
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.
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.

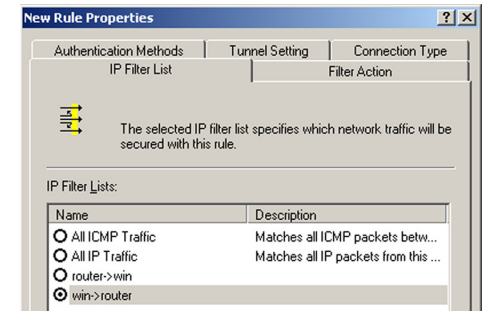


Figure C-10: IP Filter List Tab

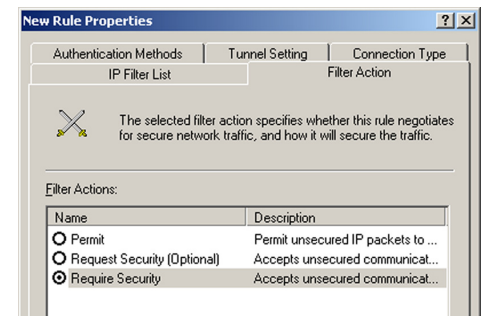


Figure C-11: Filter Action Tab

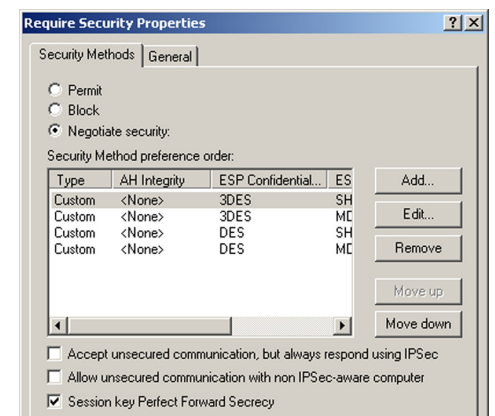


Figure C-12: Security Methods Tab

4. Select the **Authentication Methods** tab, shown in Figure C-13, and click the **Edit** button.
5. Change the authentication method to **Use this string to protect the key exchange (preshared key)**, as shown in Figure C-14, and enter the preshared key string, such as XYZ12345. Click the **OK** button.
6. This new Preshared key will be displayed in Figure C-15. Click the **OK** or **Close** button to continue.

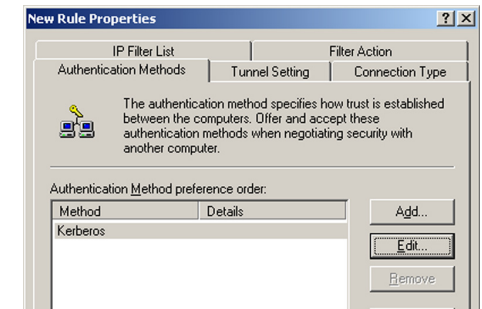


Figure C-13: Authentication Methods

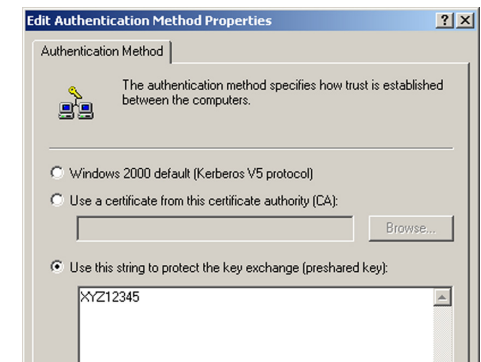


Figure C-14: Preshared Key

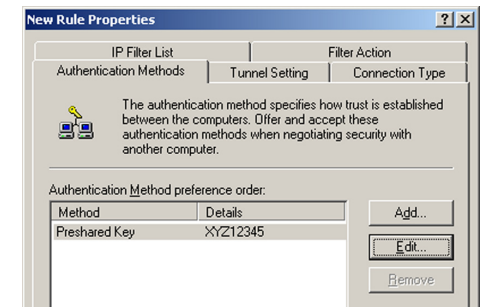


Figure C-15: New Preshared Key

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.
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.

Tunnel 2: router->win

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

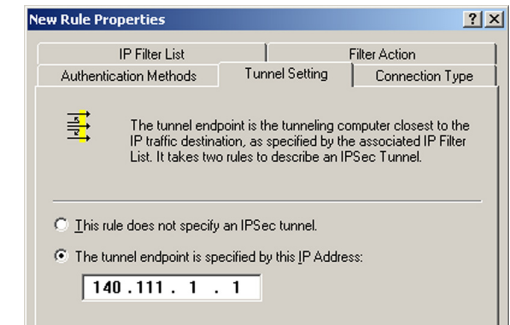


Figure C-16: Tunnel Setting Tab

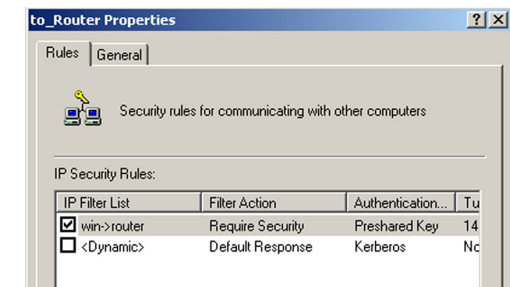


Figure C-17: Connectin Type Tab

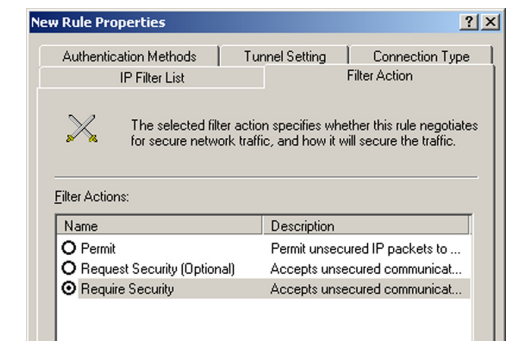


Figure C-18: Properties Screen

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

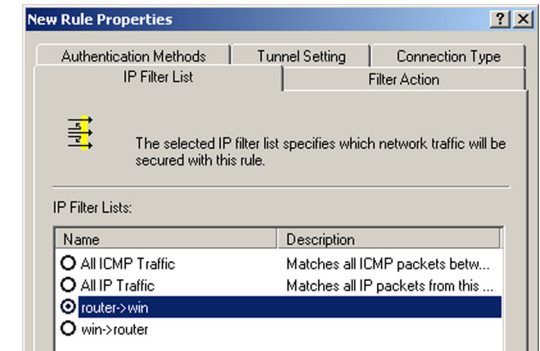


Figure C-19: IP Filter List Tab

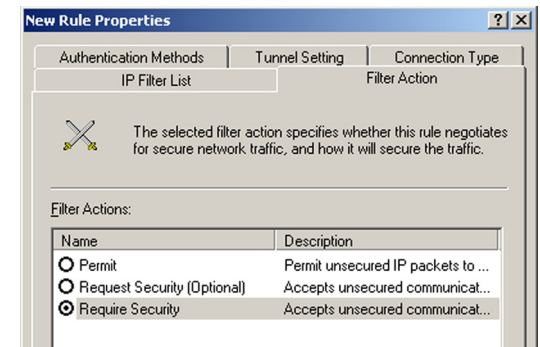


Figure C-20: Filter Action Tab

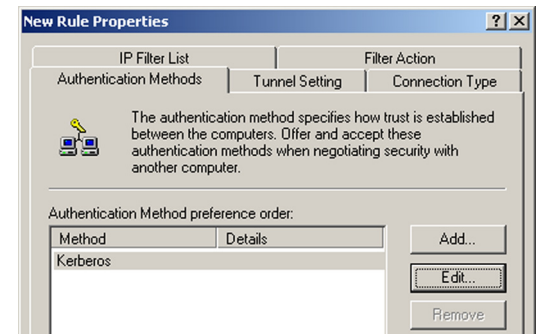


Figure C-21: Authentication Methods Tab

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

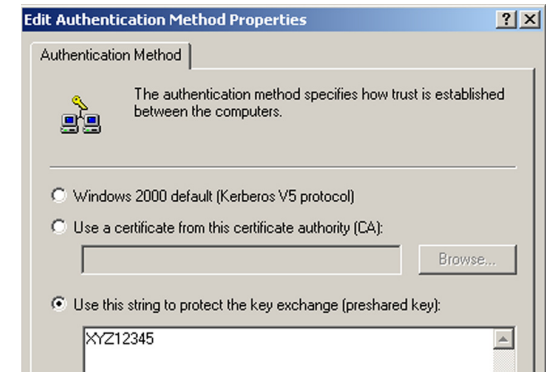


Figure C-22: Preshared Key

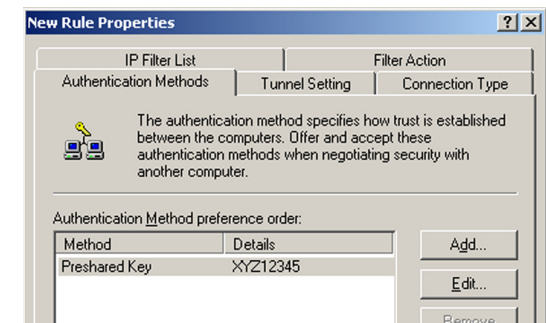


Figure C-23: New Preshared Key

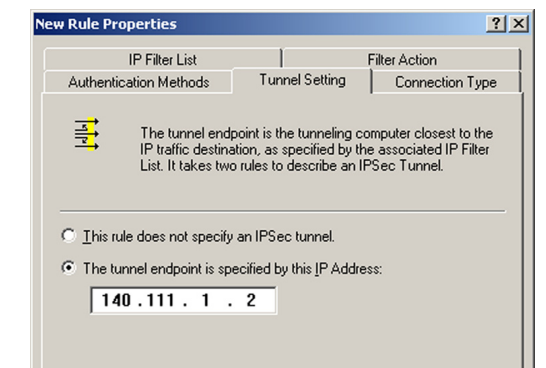


Figure C-24: Tunnel Setting Tab

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.

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

Step 4: 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.

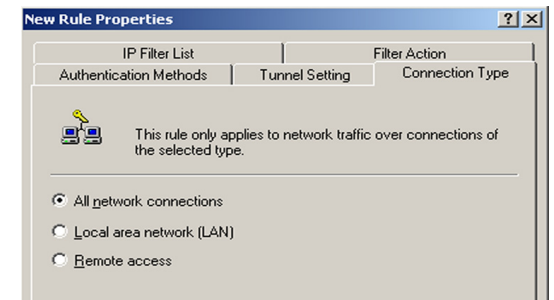


Figure C-25: Connection Type

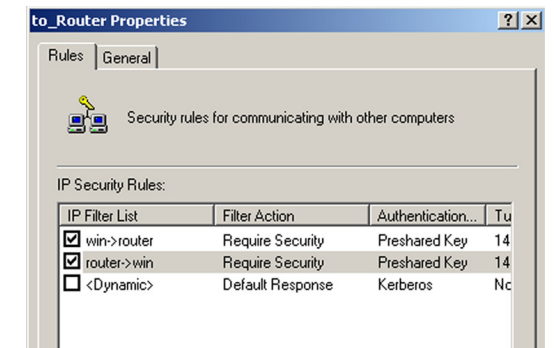


Figure C-26: Rules

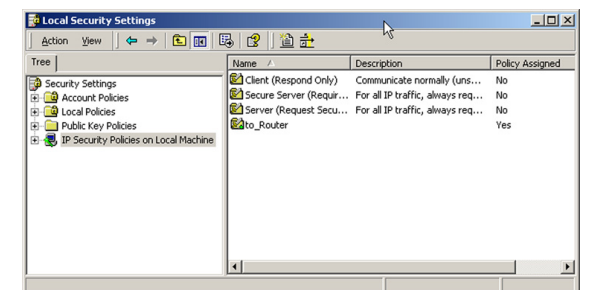


Figure C-27: Local Computer

Step 5: Create a Tunnel Through the 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, enter the default the user name and password **admin**. Press the **Enter** key.
3. From the Setup tab, click the **VPN** tab.
4. From the VPN tab, shown in Figure C-28, select the tunnel you wish to create in the Select Tunnel Entry drop-down box. Then click **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.
5. Enter the IP Address and Subnet Mask of the local VPN Router in the Local Secure Group fields. To allow access to the entire IP subnet, enter 0 for the last set of IP Addresses. (e.g. 192.168.1.0).
6. Enter the IP Address and Subnet Mask of the VPN device at the other end of the tunnel (the remote VPN Router or device with which you wish to communicate) in the Remote Security Gateway fields.
7. Select from 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.
8. Select from 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.
9. Select the 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. 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.
10. Click the **Save Settings** button to save these changes.

Your tunnel should now be established.

The screenshot displays the 'Security' configuration page with the 'VPN' tab selected. The left sidebar contains links for 'VPN Passthrough', 'VPN Tunnel', 'Local Secure Group', 'Remote Secure Group', 'Remote Security Gateway', 'Key Management', and 'Status'. The main content area is titled 'VPN Tunnel' and shows 'Tunnel 1' selected in a dropdown menu. The 'VPN Tunnel' status is 'Enabled'. Below this, there are input fields for 'Tunnel Name', 'P Address', and 'Mask' for both the 'Local Secure Group' and 'Remote Security Gateway'. The 'Encryption' is set to 'DES' and 'Authentication' is set to 'MD5'. Under 'Key Management', 'Key Exchange Method' is 'Auto(IKE)', 'PFS' is 'Enabled', and 'Pre-Shared Key' is 'Please enter shared secret'. The 'Key Lifetime' is set to '3600'. At the bottom, there is an 'Advanced VPN Tunnel Setup' button and 'Save Settings' and 'Cancel Changes' buttons.

Figure C-28: VPN Tab

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

This section describes how to find the MAC address for your computer's Ethernet adapter so you can use the MAC filtering and/or MAC address cloning feature of the Router. You can also find the IP address of your computer's Ethernet adapter. This IP address is used for the Router's filtering, forwarding, and/or DMZ features. Follow the steps in this appendix to find the adapter's MAC or IP address in Windows 98, Me, 2000, or XP.

Windows 98 or Me Instructions

1. Click **Start** and **Run**. In the *Open* field, enter **winipcfg**. Then press the **Enter** key or the **OK** button.
2. When the *IP Configuration* screen appears, select the Ethernet adapter you have connected to the Router via a CAT 5 Ethernet network cable. See Figure E-1.
3. Write down the Adapter Address as shown on your computer screen (see Figure E-2). This is the MAC address for your Ethernet adapter and is shown as a series of numbers and letters.

The MAC address/Adapter Address is what you will use for MAC address cloning or MAC filtering.

The example in Figure E-3 shows the Ethernet adapter's IP address as 192.168.1.100. Your computer may show something different.



Note: The MAC address is also called the Adapter Address.

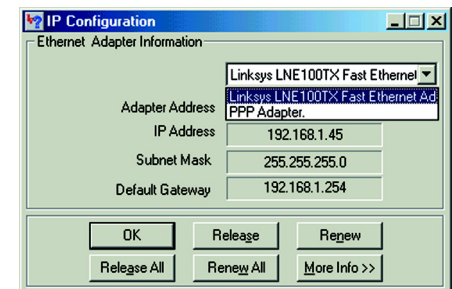


Figure D-1: IP Configuration Screen

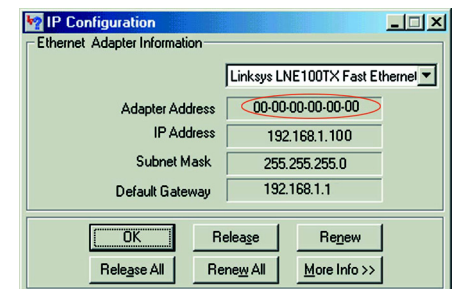


Figure D-2: MAC Address/Adapter Address

Windows 2000 or XP Instructions

1. Click **Start** and **Run**. In the *Open* field, enter **cmd**. Press the **Enter** key or click the **OK** button.



Note: The MAC address is also called the Physical Address.

2. At the command prompt, enter **ipconfig /all**. Then press the **Enter** key.
3. Write down the Physical Address as shown on your computer screen (Figure E-3); it is the MAC address for your Ethernet adapter. This appears as a series of numbers and letters.

The MAC address/Physical Address is what you will use for MAC address cloning or MAC filtering.

The example in Figure E-3 shows the Ethernet adapter's IP address as 192.168.1.100. Your computer may show something different.

```

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 D-3: MAC Address/Physical Address

Appendix E: SNMP Functions

SNMP (Simple Network Management Protocol) is a widely-used network monitoring and control protocol. Data is passed from a SNMP agent, such as the VPN Router, 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 Router is compatible with all HP Openview compliant software.

Appendix F: Upgrading Firmware

The Router's firmware is upgraded through the Web-Utility's Firmware Upgrade tab from the Administration tab. Follow these instructions:

1. Click the Browse button to find the firmware upgrade file that you downloaded from the Linksys website and then extracted.
2. Double-click the firmware file you downloaded and extracted. Click the Upgrade button, and follow the instructions there.

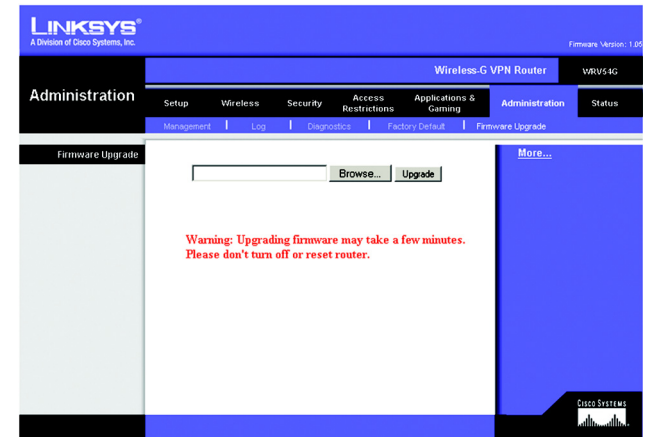


Figure F-1: Upgrade Firmware

Appendix G: Windows Help

All wireless products require Microsoft Windows. Windows is the most used operating system in the world and comes with many features that help make networking easier. These features can be accessed through Windows Help and are described in this appendix.

TCP/IP

Before a computer can communicate with the Access Point, TCP/IP must be enabled. TCP/IP is a set of instructions, or protocol, all PCs follow to communicate over a network. This is true for wireless networks as well. Your PCs will not be able to utilize wireless networking without having TCP/IP enabled. Windows Help provides complete instructions on enabling TCP/IP.

Shared Resources

If you wish to share printers, folder, or files over your network, Windows Help provides complete instructions on utilizing shared resources.

Network Neighborhood/My Network Places

Other PCs on your network will appear under Network Neighborhood or My Network Places (depending upon the version of Windows you're running). Windows Help provides complete instructions on adding PCs to your network.

Appendix H: Glossary

802.11a - An IEEE wireless networking standard that specifies a maximum data transfer rate of 54Mbps and an operating frequency of 5GHz.

802.11b - An IEEE wireless networking standard that specifies a maximum data transfer rate of 11Mbps and an operating frequency of 2.4GHz.

802.11g - An IEEE wireless networking standard that specifies a maximum data transfer rate of 54Mbps, an operating frequency of 2.4GHz, and backward compatibility with 802.11b devices.

Access Point - Device that allows wireless-equipped computers and other devices to communicate with a wired network. Also used to expand the range of a wireless network.

Adapter - This is a device that adds network functionality to your PC.

Ad-hoc - A group of wireless devices communicating directly with each other (peer-to-peer) without the use of an access point.

Backbone - The part of a network that connects most of the systems and networks together, and handles the most data.

Bandwidth - The transmission capacity of a given device or network.

Beacon Interval - The frequency interval of the beacon, which is a packet broadcast by a router to synchronize a wireless network.

Bit - A binary digit.

Boot - To start a device and cause it to start executing instructions.

Bridge - A device that connects two different kinds of local networks, such as a wireless network to a wired Ethernet network.

Broadband - An always-on, fast Internet connection.

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.

Buffer - A block of memory that temporarily holds data to be worked on later when a device is currently too busy to accept the data.

Cable Modem - A device that connects a computer to the cable television network, which in turn connects to the Internet.

CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) - A method of data transfer that is used to prevent data loss in a network.

CTS (Clear To Send) - A signal sent by a device to indicate that it is ready to receive data.

Daisy Chain - A method used to connect devices in a series, one after the other.

Database - A collection of data that is organized so that its contents can easily be accessed, managed, and updated.

DDNS (Dynamic Domain Name System) - The capability of having a website, FTP, or e-mail server-with a dynamic IP address-use a fixed domain name.

Default Gateway - A device that forwards Internet traffic from your local area network.

DHCP (Dynamic Host Configuration Protocol) - A protocol that lets one device on a local network, known as a DHCP server, assign temporary IP addresses to the other network devices, typically computers.

DMZ (Demilitarized Zone) - Removes the Router's firewall protection from one PC, allowing it to be "seen" from the Internet.

DNS (Domain Name Server) - The IP address of your ISP's server, which translates the names of websites into IP addresses.

Domain - A specific name for a network of computers.

Download - To receive a file transmitted over a network.

DSL (Digital Subscriber Line) - An always-on broadband connection over traditional phone lines.

DSSS (Direct-Sequence Spread-Spectrum) - A type of radio transmission technology that includes a redundant bit pattern to lessen the probability of data lost during transmission. Used in 802.11b networking.

DTIM (Delivery Traffic Indication Message) - A message included in data packets that can increase wireless efficiency.

Dynamic IP Address - A temporary IP address assigned by a DHCP server.

Encryption - Encoding data to prevent it from being read by unauthorized people.

Ethernet - An IEEE standard network protocol that specifies how data is placed on and retrieved from a common transmission medium.

Finger - A program that tells you the name associated with an e-mail address.

Firewall - Security measures that protect the resources of a local network from intruders.

Firmware - 1. In network devices, the programming that runs the device. 2. Programming loaded into read-only memory (ROM) or programmable read-only memory (PROM) that cannot be altered by end-users.

Fragmentation - Breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.

FTP (File Transfer Protocol) - A standard protocol for sending files between computers over a TCP/IP network and the Internet.

Full Duplex - The ability of a networking device to receive and transmit data simultaneously.

Gateway - A system that interconnects networks.

Half Duplex - Data transmission that can occur in two directions over a single line, but only one direction at a time.

Hardware - The physical aspect of computers, telecommunications, and other information technology devices.

HTTP (HyperText Transport Protocol) - The communications protocol used to connect to servers on the World Wide Web.

IEEE (The Institute of Electrical and Electronics Engineers) - An independent institute that develops networking standards.

Infrastructure - Currently installed computing and networking equipment.

Infrastructure Mode - Configuration in which a wireless network is bridged to a wired network via an access point.

IP (Internet Protocol) - A protocol used to send data over a network.

IP Address - The address used to identify a computer or device on a network.

IPCONFIG - A Windows 2000 and XP utility that displays the IP address for a particular networking device.

IPSec (Internet Protocol Security) - A VPN protocol used to implement secure exchange of packets at the IP layer.

ISM band - Radio band used in wireless networking transmissions.

ISP (Internet Service Provider) - A company that provides access to the Internet.

LAN (Local Area Network) - The computers and networking products that make up the network in your home or office.

MAC (Media Access Control) Address - The unique address that a manufacturer assigns to each networking device.

Mbps (Megabits Per Second) - One million bits per second; a unit of measurement for data transmission.

Multicasting - Sending data to a group of destinations at once.

NAT (Network Address Translation) - NAT technology translates IP addresses of a local area network to a different IP address for the Internet.

Network - A series of computers or devices connected for the purpose of data sharing, storage, and/or transmission between users.

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

Node - A network junction or connection point, typically a computer or work station.

OFDM (Orthogonal Frequency Division Multiplexing) - A type of modulation technology that separates the data stream into a number of lower-speed data streams, which are then transmitted in parallel. Used in 802.11a, 802.11g, and powerline networking.

Packet - A unit of data sent over a network.

Passphrase - Used much like a password, a passphrase simplifies the WEP encryption process by automatically generating the WEP encryption keys for Linksys products.

Ping (Packet INternet Groper) - An Internet utility used to determine whether a particular IP address is online.

POP3 (Post Office Protocol 3) - A standard protocol used to retrieve e-mail stored on a mail server.

Port - 1. The connection point on a computer or networking device used for plugging in a cable or an adapter. 2. The virtual connection point through which a computer uses a specific application on a server.

Wireless-G VPN Broadband Router

PPPoE (Point to Point Protocol over Ethernet) - A type of broadband connection that provides authentication (username and password) in addition to data transport.

PPTP (Point-to-Point Tunneling Protocol) - A VPN protocol that allows the Point to Point Protocol (PPP) to be tunneled through an IP network. This protocol is also used as a type of broadband connection in Europe.

Preamble - Part of the wireless signal that synchronizes network traffic.

RJ-45 (Registered Jack-45) - An Ethernet connector that holds up to eight wires.

Roaming - The ability to take a wireless device from one access point's range to another without losing the connection.

Router - A networking device that connects multiple networks together, such as a local network and the Internet.

RTS (Request To Send) - A packet sent when a computer has data to transmit. The computer will wait for a CTS (Clear To Send) message before sending data.

Server - Any computer whose function in a network is to provide user access to files, printing, communications, and other services.

SMTP (Simple Mail Transfer Protocol) - The standard e-mail protocol on the Internet.

SNMP (Simple Network Management Protocol) - A widely used network monitoring and control protocol.

Software - Instructions for the computer. A series of instructions that performs a particular task is called a "program".

Spread Spectrum - Wideband radio frequency technique used for more reliable and secure data transmission.

SSID (Service Set Identifier) - Your wireless network's name.

Static IP Address - A fixed address assigned to a computer or device that is connected to a network.

Static Routing - Forwarding data in a network via a fixed path.

Subnet Mask - An address code that determines the size of the network.

Switch - 1. Device that is the central point of connection for computers and other devices in a network, so data can be shared at full transmission speeds. 2. A device for making, breaking, or changing the connections in an electrical circuit.

Wireless-G VPN Broadband Router

TCP/IP (Transmission Control Protocol/Internet Protocol) - A network protocol for transmitting data that requires acknowledgement from the recipient of data sent.

Telnet - A user command and TCP/IP protocol used for accessing remote PCs.

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

Throughput - The amount of data moved successfully from one node to another in a given time period.

Topology - The physical layout of a network.

TX Rate - Transmission Rate.

UDP (User Datagram Protocol) - A network protocol for transmitting data that does not require acknowledgement from the recipient of the data that is sent.

Upgrade - To replace existing software or firmware with a newer version.

Upload - To transmit a file over a network.

URL (Uniform Resource Locator) - The address of a file located on the Internet.

VPN (Virtual Private Network) - A security measure to protect data as it leaves one network and goes to another over the Internet.

WAN (Wide Area Network) - The Internet.

WEP (Wired Equivalent Privacy) - A method of encrypting data transmitted on a wireless network for greater security.

WINIPCFG - A Windows 98 and Millennium utility that displays the IP address for a particular networking device.

WLAN (Wireless Local Area Network) - A group of computers and associated devices that communicate with each other wirelessly.

Appendix I: Specifications

Standards	IEEE 802.3, 802.11b and 802.11g
Ports	One Internet, Ethernet (1-4), Power
Buttons	One Reset Button, One Power Switch
Cabling Type	UTP CAT 5 or better
Data Rate	Up to 54Mbps
Transmit Power	15dBm
LEDs	Power, Internet, Ethernet (1, 2, 3, 4), Wireless-G, DMZ
Security Features	WEP, 802.1x Authentication
WEP Key Bits	64, 128
Dimensions (W x H x D)	7.32" x 6.89" x 1.89" (186 mm x 175 mm x 48 mm)
Unit Weight	1.26 lb (0.57 kg)
Power	External, 5V DC, 2.5A
Certifications	FCC, IC-03
Operating Temp.	0°C to 40°C (32°F to 104°F)
Storage Temp.	-20°C to 70°C (-4°F to 158°F)
Operating Humidity	10% to 85% Non-Condensing

Cisco-Linksys, LLC declares that WRV54G (FCC ID: Q87-HGA5S-3) is limited in CH1~CH11 by specified firmware controlled in U.S.A.

Wireless-G VPN Broadband Router

Storage Humidity 5% to 90% Non-Condensing

Appendix J: Warranty Information

LIMITED WARRANTY

Linksys warrants to the original end user purchaser ("You") that, for a period of three years, (the "Warranty Period") Your Linksys product will be free of defects in materials and workmanship under normal use. Your exclusive remedy and Linksys's entire liability under this warranty will be for Linksys at its option to repair or replace the product or refund Your purchase price less any rebates.

If the product proves defective during the Warranty Period call Linksys Technical Support in order to obtain a Return Authorization Number. BE SURE TO HAVE YOUR PROOF OF PURCHASE ON HAND WHEN CALLING. When returning a product, mark the Return Authorization Number clearly on the outside of the package and include a copy of your original proof of purchase. RETURN REQUESTS CANNOT BE PROCESSED WITHOUT PROOF OF PURCHASE. You are responsible for shipping defective products to Linksys. Linksys pays for UPS Ground shipping from Linksys back to You only. Customers located outside of the United States of America and Canada are responsible for all shipping and handling charges.

ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE ARE LIMITED TO THE DURATION OF THE WARRANTY PERIOD. ALL OTHER EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF NON-INFRINGEMENT, ARE DISCLAIMED. Some jurisdictions do not allow limitations on how long an implied warranty lasts, so the above limitation may not apply to You. This warranty gives You specific legal rights, and You may also have other rights which vary by jurisdiction.

TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL LINKSYS BE LIABLE FOR ANY LOST DATA, REVENUE OR PROFIT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE THE PRODUCT, EVEN IF LINKSYS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL LINKSYS' LIABILITY EXCEED THE AMOUNT PAID BY YOU FOR THE PRODUCT.

The foregoing limitations will apply even if any warranty or remedy provided under this Section fails of its essential purpose. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to You.

Please direct all inquiries to: Linksys, P.O. Box 18558, Irvine, CA 92623 USA.

Appendix K: Regulatory Information

FCC STATEMENT

This product 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

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body.

INDUSTRY CANADA (CANADA)

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

The use of this device in a system operating either partially or completely outdoors may require the user to obtain a license for the system according to the Canadian regulations.

EC DECLARATION OF CONFORMITY (EUROPE)

Linksys Group declares that the Instant Wireless™ Series products included in the Instant Wireless™ Series conform to the specifications listed below, following the provisions of the EMC Directive 89/336/EEC and Low Voltage Directive 73/23/EEC:

ETS 300-826, 301 489-1 General EMC requirements for Radio equipment.

EN 609 50 Safety

ETS 300-328-2 Technical requirements for Radio equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Wireless-G VPN Broadband Router

Note: This equipment is intended to be used in all EU and EFTA countries. Outdoor use may be restricted to certain frequencies and/or may require a license for operation. For more details, contact Linksys Corporate Compliance.

Note: Combinations of power levels and antennas resulting in a radiated power level of above 100 mW are considered as not compliant with the above mentioned directive and are not allowed for use within the European community and countries that have adopted the European R&TTE directive 1999/5/EC and/or the CEPT recommendation Rec 70.03. For more details on legal combinations of power levels and antennas, contact Linksys Corporate Compliance.

Linksys Group™ vakuuttaa täten että Instant Wireless IEEE 802.11 PC Card tyyppinen laite on direktiivin 1999/5/EY, direktiivin 89/336/EEC ja direktiivin 73/23/EEC oleellisten vaatimusten ja sitä koskevien näiden direktiivien muiden ehtojen mukainen.

Linksys Group™ déclare que la carte PC Instant Wireless IEEE 802.11 est conforme aux conditions essentielles et aux dispositions relatives à la directive 1999/5/EC, la directive 89/336/EEC, et à la directive 73/23/EEC.

Belgique B L'utilisation en extérieur est autorisé sur le canal 11 (2462 MHz), 12 (2467 MHz), et 13 (2472 MHz).

Dans le cas d'une utilisation privée, à l'extérieur d'un bâtiment, au-dessus d'un espace public, aucun enregistrement n'est nécessaire pour une distance de moins de 300m. Pour une distance supérieure à 300m un enregistrement auprès de l'IBPT est requise. Pour une utilisation publique à l'extérieur de bâtiments, une licence de l'IBPT est requise. Pour les enregistrements et licences, veuillez contacter l'IBPT.

France F: Bande de fréquence restreinte: seuls les canaux 10, 11, 12, 13 (2457, 2462, 2467, et 2472 MHz respectivement) doivent être utilisés en France.

Toute utilisation, qu'elle soit intérieure ou extérieure, est soumise à autorisation. Vous pouvez contacter l'Autorité de Régulation des Télécommunications

(<<http://www.art-telecom.fr>>) pour la procédure à suivre.

France F: Restricted frequency band: only channels 10, 11, 12, 13 (2457, 2462, 2467, and 2472 MHz respectively) may be used in France. License required for every indoor and outdoor installations. Please contact ART for procedure to follow.

Deutschland D: Anmeldung im Outdoor-Bereich notwendig, aber nicht genehmigungspflichtig. Bitte mit Händler die Vorgehensweise abstimmen.

Germany D: License required for outdoor installations. Check with reseller for procedure to follow

Italia I: E' necessaria la concessione ministeriale anche per l'uso interno. Verificare con i rivenditori la procedura da seguire. L'uso per installazione in esterni non e' permessa.

Italy I: License required for indoor use. Use with outdoor installations not allowed.

the Netherlands NL License required for outdoor installations. Check with reseller for procedure to follow.

Nederlands NL Licentie verplicht voor gebruik met buitenantennes. Neem contact op met verkoper voor juiste procedure.

Appendix L: Contact Information

Need to contact Linksys?

Visit us online for information on the latest products and updates to your existing products at:

<http://www.linksys.com> or
<ftp.linksys.com>

Can't find information about a product you want to buy on the web? Do you want to know more about networking with Linksys products? Give our advice line a call at:
Or fax your request in to:

800-546-5797 (LINKSYS)
949-261-8868

If you experience problems with any Linksys product, you can call us at:

800-326-7114
support@linksys.com

Don't wish to call? You can e-mail us at:

If any Linksys product proves defective during its warranty period, you can call the Linksys Return Merchandise Authorization department for obtaining a Return Authorization Number at:
(Details on Warranty and RMA issues can be found in the Warranty Information section in this Guide.)

949-261-1288

Also Available:

- **Linksys High Gain Antenna for SMA Connectors (HGA5S)**

