



BroadGuard™
Secure Cable/DSL Router

User's Guide

Model No. NBG800

P/N: 85-500600-02

Rev: A1

January 2001

SOHware Inc.

Tel: +1 (408) 565-9888

Fax: +1 (408) 565-9889

SOHware Europe

Tel: +44 1489 611 788

Fax: +44 1489 611 787

Technical Support

E-mail: support@sohware.com

Technical Support Call Center (24hrs): +1 (888) 785-8222

Toll-Free Customer Service (US only): (800) 632-1118 ext: 2801

Fax: +1 (408) 565-9889

TRADEMARKS

SOHOware is a trademark of SOHOware Inc. All other names mentioned in this document are trademarks/registered trademarks of their respective owners. SOHOware provides this document “as is,” without warranty of any kind, neither expressed nor implied, including, but not limited to, the particular purpose. We may make improvements and/or changes in this manual or in the product(s) and/or the program(s) described in this manual at any time. This document could include technical inaccuracies or typographical errors.

FCC WARNING

This equipment has been tested and found to comply with the limits 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 in accordance with 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 can be determined by turning the equipment on and off, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Relocate the equipment with respect to the receiver
- Plug the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult your dealer or an experienced radio/TV technician for help

You are cautioned that changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the 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

Packing List

Check the contents of your package to ensure that they match the packing list below. If anything is missing or damaged, contact the store where you purchased the product.

The BroadGuard pack comes with the following:

- One BroadGuard Device
- One Power Adapter
- One User's Guide and Quick Guide
- Two Color-coded RJ-45 UTP cables
- Registration card (or go to www.sohoware.com for on-line registration)
Register to receive free:
 - Warranty protection (3 year on BroadGuard device, 1 year on power adapter)
 - Information on upcoming product releases and special product offers
 - Free technical support and firmware upgrades

Table of Contents

CHAPTER 1: INTRODUCTION.....	1
FEATURES AND BENEFITS.....	1
GETTING TO KNOW YOUR BROADGUARD.....	2
<i>Front Panel.....</i>	<i>2</i>
<i>LED Indicators.....</i>	<i>3</i>
<i>Rear Panel.....</i>	<i>3</i>
CHAPTER 2: INSTALLATION.....	5
WHAT YOU NEED.....	5
<i>Broadband Internet Account.....</i>	<i>5</i>
MAKING A CONNECTION.....	6
NETWORK EXTENSION.....	7
<i>Wired LAN Extension.....</i>	<i>7</i>
<i>Wireless LAN Extension.....</i>	<i>8</i>
NETWORK CONFIGURATION.....	9
<i>Windows 95/98/Me.....</i>	<i>9</i>
<i>Windows NT 4.0.....</i>	<i>13</i>
<i>Windows 2000.....</i>	<i>15</i>
<i>Mac OS.....</i>	<i>19</i>
CHAPTER 3: NETWORK CONFIGURATION.....	21
BROADGUARD NETWORK CONFIGURATION.....	21
ENTERING THE BROADGUARD SETUP HOME PAGE.....	21
SETUP HOME PAGE.....	22
BASIC.....	24
<i>Broadband Connection.....</i>	<i>24</i>
<i>Hacker Attack E-mail Alerts.....</i>	<i>30</i>
<i>Change Password.....</i>	<i>31</i>
ADVANCED.....	32

<i>Access Control</i>	32
<i>DMZ Host</i>	34
<i>DMZ Host Disable</i>	34
<i>DHCP Settings</i>	35
<i>Status</i>	36
TOOLS	37
<i>PPPoE Check (DSL Users Only)</i>	37
<i>View Current Access Control Settings</i>	40
<i>Access Monitor</i>	41
CHAPTER 4: TROUBLESHOOTING	43
CHAPTER 5: FAQs	49
APPENDIX A: VPN REMOTE ACCESS	52
BROADGUARD VPN SERVER CONFIGURATION.....	52
CLIENT CONFIGURATION (E.G. MICROSOFT PPTP)	52
<i>Windows 98/98/SE/Me VPN Client Setup</i>	52
<i>Windows 2000 VPN Server Setup</i>	58
APPENDIX B: GLOSSARY	68
TECHNICAL SPECIFICATIONS	71
TECHNICAL SUPPORT	72
SOHOWARE LIMITED WARRANTY	73

List of Figures

Figure 1. BroadGuard Connections.....	1
Figure 2. Front Panel.....	2
Figure 3. Rear Panel.....	3
Figure 4. Connecting the BroadGuard.....	6
Figure 5. Wired LAN Extension	7
Figure 6. Wireless LAN Extension	8
Figure 7. Control Panel	9
Figure 8. Network	9
Figure 9. Select Network Component Type	10
Figure 10. Select Network Protocol	10
Figure 11. Network	11
Figure 12. TCP/IP Properties-1	11
Figure 13. TCP/IP Properties-2.....	12
Figure 14. Control Panel	13
Figure 15. Network	13
Figure 16. Microsoft TCP/IP Properties-1	14
Figure 17. Microsoft TCP/IP Properties-2	15
Figure 18. Control Panel	15
Figure 19. Network and Dial-up Connections.....	16
Figure 20. Local Area Connection Status.....	16
Figure 21. Local Area Connection Properties	17
Figure 22. Internet Protocol (TCP/IP) Properties-1.....	17
Figure 23. Internet Protocol (TCP/IP Properties-2.....	18
Figure 24. Using the DHCP Server.....	19
Figure 25. Manual Configuration of IP Addresses.....	20
Figure 26. Saving the Configuration	20
Figure 27. Entering the Setup Wizard	21
Figure 28. Enter Network Password.....	21
Figure 29. Setup Start Page.....	23
Figure 30. Broadband Connection.....	24

Figure 31. Cable Broadband Connection	24
Figure 32. Network	26
Figure 33. Network	26
Figure 34. System Properties	27
Figure 35. Cable Broadband Connection	28
Figure 36. Broadband Connection.....	28
Figure 37. DSL Broadband Connection	29
Figure 38. Hacker Attack E-mail Alerts	30
Figure 39. Change Password	31
Figure 40. Access Control.....	32
Figure 41. Globally Disallowed Websites/Keywords.....	33
Figure 42. DMZ Host.....	34
Figure 43. DHCP Settings.....	35
Figure 44. DHCP IP Address Assignments.....	35
Figure 45. Status	36
Figure 46. PPPoE Check	37
Figure 47. PPPoE Service Running.....	38
Figure 48. PPPoE Check Successful	38
Figure 49. PPPoE Check Unsuccessful	39
Figure 50. Authentication Failed.....	39
Figure 51. Hacker Alert Test.....	40
Figure 52. View Current Access Control Settings.....	40
Figure 53. Access Monitor	41
Figure 54. Download Firmware	41
Figure 55. Status	44
Figure 56. Run.....	44
Figure 57. IP Configuration	45
Figure 58. Command Prompt-1.....	45
Figure 59. Command Prompt-2.....	46
Figure 60. Command Prompt-3.....	46
Figure 61. Command Prompt-4.....	47
Figure 62. Status	47

Figure 63. Control Panel	52
Figure 64. Network	53
Figure 65. Select Network Component Type	53
Figure 66. Select Network Adapters	53
Figure 67. Network	54
Figure 68. Welcome to Dial-Up Networking	55
Figure 69. Make New Connection-1	55
Figure 70. Make New Connection-2	56
Figure 71. Make New Connection-3	56
Figure 72. Dial-Up Networking	57
Figure 73. Connect To.....	57
Figure 74. Connection Established.....	58
Figure 75. Routing and Remote Access	58
Figure 76. Common Configurations.....	59
Figure 77. Remote Client Protocols	59
Figure 78. Internet Connection.....	60
Figure 79. IP Address Assignment.....	60
Figure 80. Address Range Assignment	61
Figure 81. New Address Range.....	61
Figure 82. Address Range Assignment	62
Figure 83. Managing Multiple Remote Access Servers	62
Figure 84. Routing and Remote Access	62
Figure 85. Routing and Remote Access	63
Figure 86. Local Area connection Properties	64
Figure 87. Administrative Tools	65
Figure 88. Computer Management.....	65
Figure 89. User Properties.....	66
Figure 90. Network and Dial-Up Connections.....	66

Chapter 1: Introduction

The SOHware BroadGuard Secure cable/DSL Router provides convenient Internet access to office/family users by sharing a single Broadband Service Provider (BSP) account. The BroadGuard functions with cable/DSL modems and allows up to 253 computers to share secure broadband Internet access simultaneously.

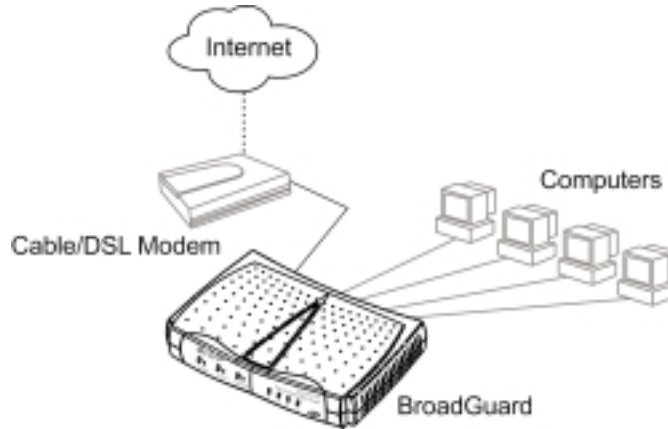


Figure 1. BroadGuard Connections

Embedded Network Address Translation (NAT) enables you to use a private set of IP addresses that the BroadGuard translates into a single public IP address. The BroadGuard can also act as a DHCP server by automatically allocating a dynamic IP address to each computer on the network.

An enhanced firewall and the Access Control feature monitor incoming data packets and filter server requests. Together they allow parents/employers to see how the network connection is being used, and protect all PCs behind the BroadGuard.

Features and Benefits

- **Share Your Internet Connection** – Built-in NAT, DHCP, and 10/100 Ethernet switch allow multiple users to share a single cable/DSL account simultaneously.
- **Easy-to-use** – No driver or software required. Easily configured and managed through a web browser (Netscape Communicator 4.0/Microsoft Internet Explorer 3.0 or above), from LAN-connected PCs.
- **Consumer-oriented Firewall** – Security via NAT (Network Address Translation) protects your network from intruders. Built in anti-attack

SOHware® Secure Cable/DSL Router 1

algorithm (Denial of Service & Stateful Packet Inspection) protect your PCs from hacker attacks.

- **Access Control** – Provides management/control of Internet application use. The feature allows parents/employers to monitor what their children are doing or to see how the network connection is being used.
- **Flexible and Expandable** – Connects directly to computers, to an Ethernet hub for network expansion, or to a SOHware NetBlaster for wireless network access.
- **Virtual Private Network (VPN)** – Allows Internet security protocol packets such as PPTP to pass through the BroadGuard so that a remote PC can securely access a server located on your network, or allows a PC behind the BroadGuard to remotely access a VPN server.
- **Multimedia Streaming Protocol** – Multimedia data is streamed at a constant rate for best enjoyment of Real Player, QuickTime, IP/TV, Video on Demand, and Video Phone.
- **Intelligent Routing** – Built in RIP I & II routing protocols. The BroadGuard automatically learns the outside Internet infrastructure and determines the most efficient data transfer route.
- **FCC Class B Certified** – Safe for use in residential environments.

Getting to Know Your BroadGuard

Front Panel

Users can monitor the status of the BroadGuard via the LEDs on the front panel (Figure 2).

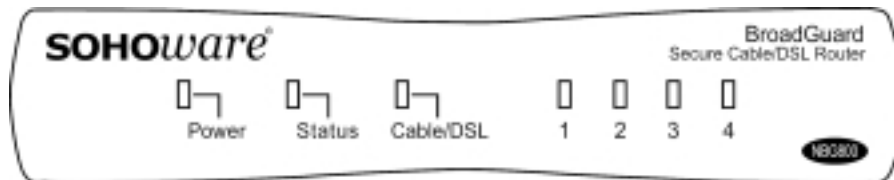


Figure 2. Front Panel

LED Indicators

LED	Color	Function
<i>Power</i>	Green	Lit: Power ON Unlit: Power OFF
<i>Status</i>	Red	Blinking: On power-up the BroadGuard checks for proper operation. The checking procedure takes only a few seconds Lit: If this LED is always lit, the device is not working properly. Go to Chapter 4: Troubleshooting, page 43
<i>Cable/DSL: Link/Activity</i>	Orange	Lit: Indicates a good connection to a cable/DSL modem Blinking: Data is being transmitted/received to/from a cable/DSL modem
<i>LAN: LAN Ports 1~4 Link/Activity</i>	Green Orange	Lit/Blinking: Indicates the link status and activity of 100Mbps Ethernet data Lit/Blinking: Indicates the link status and activity of 10Mbps Ethernet data

Rear Panel

Ports on the Rear Panel (Figure 3)



Figure 3. Rear Panel

LAN Ports There are four 10/100Base-T Switch ports for linking computers or other Ethernet devices, e.g. a hub/switch. When linking to other networking devices, we need a cross-over cable or an uplink port on that device

Cable/DSL port An Ethernet 10Base-T port is used for linking to the Ethernet

port of a cable/DSL modem

Reset

Re-start the BroadGuard by pressing the *Reset* button for longer than 5 seconds.

If you forget the password for the Setup Wizard, restore the default settings by pressing the reset button for longer than 13 seconds. Enter the default users name (admin) and password (1234) to regain access to the BroadGuard.

Power (5V)

Used to connect the external power adapter supplied with the BroadGuard. Note that only the supplied adapter should be used.

4 SOHware® Secure Cable/DSL Router

Chapter 2: Installation

What You Need

Before installing the SOHOfware BroadGuard you need the following:

Any Network Operating System with:

- TCP/IP installed
- Internet browser installed
- 10Mbps/100Mbps or 10/100Mbps Ethernet network adapters installed

Broadband Internet Account

You should be subscribed to a broadband Internet service and have a cable/DSL modem with a 10Base-T interface. Know whether your Public IP address is fixed or is dynamically assigned (ask your Broadband Service Provider).

1. If your IP address is dynamically assigned (most common), the BroadGuard will automatically get a public IP address from your ISP through the modem. You will not need to do any IP address configuration.
There is no need to enter any information in *Broadband Connection* unless your BSP has assigned you specific Internet connection information (Host Name, Domain Name, MAC address authentication, PPPoE, or a static IP address).
To do a manual setup, type **192.168.1.1** into the web address location on a web browser on any connected PC. Enter the factory default user name **admin** and password **1234**. After clicking **OK** you will enter the setup home page. Click the **Broadband Connection** link to begin setup of the broadband connection.
2. If you have an AT&T (formerly MediaOne) cable service, or any service that requires a Media Access Control (MAC) address for authentication, when you are setting up the BroadGuard for first use, only the PC with the registered Ethernet card's MAC address can be connected to the BroadGuard.
3. If you have a DSL service with PPPoE, obtain the following information from your BSP:
 - The user login name
 - The login password
 - Service name (some BSPs may not require you to use this)

4. If you have a fixed public IP address, obtain the following information from your ISP
 - The assigned Gateway IP address
 - Domain Name Server's IP address
 - Subnet Mask

Making a Connection

All the connection ports are on the rear panel of the BroadGuard. Follow the steps below to complete the hardware installation.

- step1.** Connect to a cable/DSL modem - Two cables are supplied with the SOHware NBG800. The white cable (straight-through) is for connecting a cable modem to the Cable/DSL port; the green one (cross-over) is for connecting a DSL modem to the cable/DSL port.

Plug one end of the cable into the cable/DSL port of the BroadGuard and the other end into the Ethernet port of the cable/DSL modem. If the cable is connected correctly, the Cable/DSL LED will remain lit (the cable/DSL modem must be turned on). If not, try switching the cables, green for white

- step2.** Connect to the PCs - Use a standard RJ-45 Ethernet cable (not provided) to connect the Ethernet LAN adapters in the computers to the BroadGuard LAN ports

- step3.** Install the power adapter - Plug the power adapter into an AC power outlet. Plug the other end into the BroadGuard. The Power LED should light immediately

Note: Use only the power adapter supplied with the BroadGuard

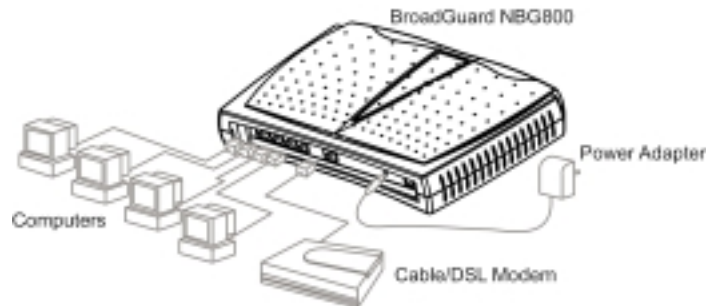


Figure 4. Connecting the BroadGuard

Note: Only one PC should be connected to the BroadGuard during setting up

6 SOHware® Secure Cable/DSL Router

Some BSPs use an Ethernet adapter's MAC address as an identifier to provide Internet service. In these cases you need to clone the Ethernet adapters MAC address to the BroadGuard. At the BroadGuard, disconnect the Ethernet cables from the other PCs on the network, leaving only the PC with the Ethernet adapter that you wish to register connected.

Note: If you previously used a registered MAC address to connect to your broadband service, you need to clone this Ethernet adapter's MAC address to the BroadGuard.

Network Extension

If you want to connect more users to your network, or use a wireless connection through the BroadGuard, refer to the following section:

Wired LAN Extension

This section describes how to extend your BroadGuard LAN using one of our SOHOware Home series products, e.g. a 10Mbps or 10/100Mbps Ethernet Hub/Switch.

Easy two-step installation procedure:

- step1.** Set the Uplink port of the external hub/switch to the *Uplink* position
- step2.** Use standard RJ-45 Ethernet cable to connect any BroadGuard LAN port to the *Uplink* port of the hub/switch. If the device does not feature an Uplink switch, use a cross-over cable

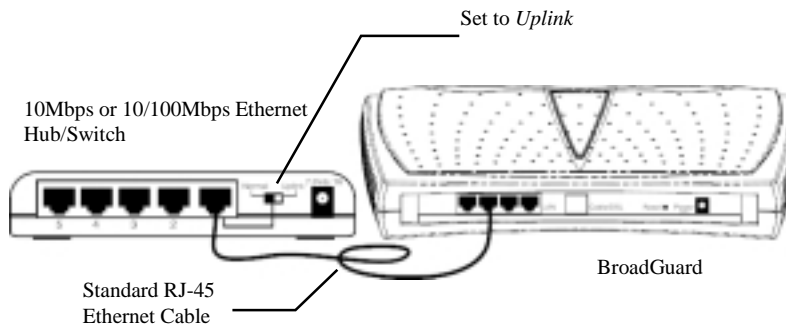


Figure 5. Wired LAN Extension

Wireless LAN Extension

This section describes how to extend your BroadGuard LAN to a CableFREE NetBlaster II Wireless hub. Just connect any normal port of the BroadGuard to the CableFREE NetBlaster II with standard RJ-45 Ethernet cable (for more SOHOware NetBlaster II information, visit www.sohoware.com).

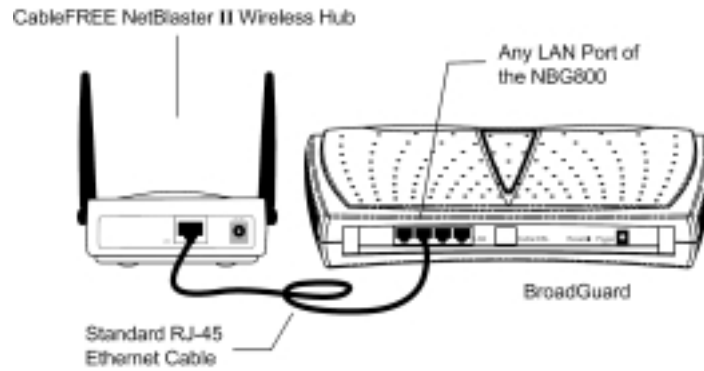


Figure 6. Wireless LAN Extension

Network Configuration

If your local network will access the Internet through a single IP, you need to configure the TCP/IP settings. For Windows 95/98/Me, see the following section, for Windows NT 4.0 go to page 13, and for Windows 2000 go to page 15. For Mac OS users, turn to page 19.

Windows 95/98/Me

step1. Click *Start/Settings/Control Panel* (**Figure 7**)

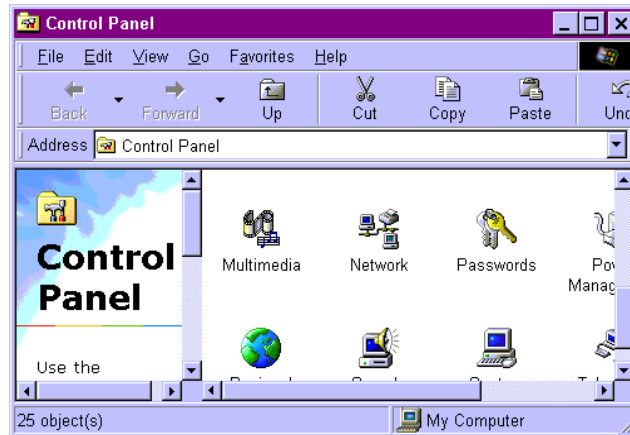


Figure 7. Control Panel

step2. In *Control Panel*, double-click the *Network* icon. The *Network* dialog box will open (**Figure 8**)

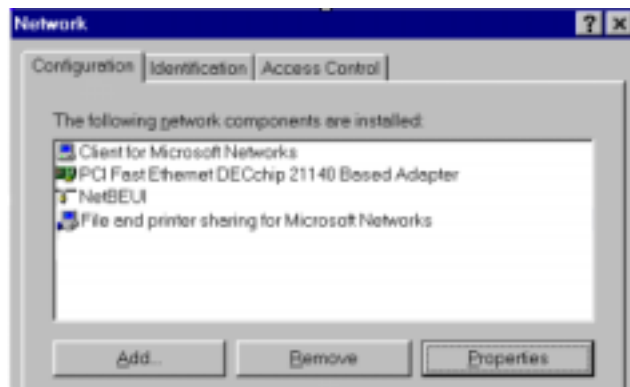


Figure 8. Network

- step3.** If TCP/IP is already shown in the list, go to Step 6. If not, click *Add*. The *Select Network Component Type* dialog box will open (**Figure 9**)



Figure 9. Select Network Component Type

- step4.** Double-click *Protocol*. The *Select Network Protocol* dialog box will open (**Figure 10**)

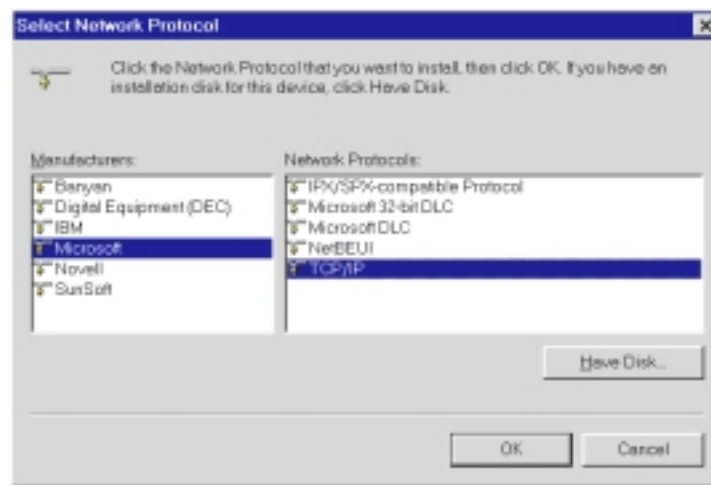


Figure 10. Select Network Protocol

- step5.** In the left window, choose *Microsoft*. In the right, select *TCP/IP*. After the TCP/IP component is completely installed, click *OK*. You will be returned to the *Network* menu (**Figure 11**). The *TCP/IP* item in the *Network* box indicates that TCP/IP has been installed

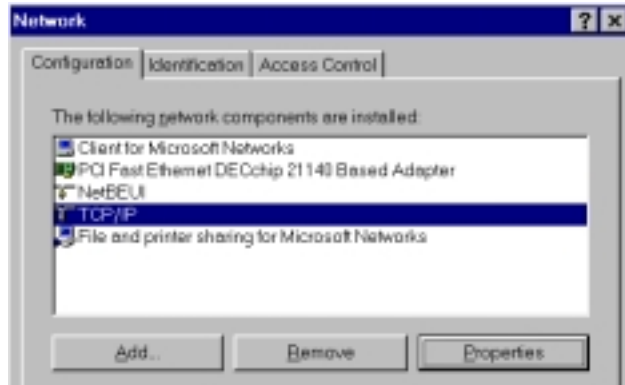


Figure 11. Network

- step6.** On the *Configuration* card (Figure 11), select *TCP/IP* and click *Properties*. The *TCP/IP Properties* dialog box will open (Figure 12)



Figure 12. TCP/IP Properties-1

- step7.** On the *IP Address* page (Figure 12), select *Obtain an IP address automatically*. Click *OK* and go to step 9. If you want to assign a static IP to a PC, go to step 8

Note: The BroadGuard operates as a DHCP server (it automatically assigns an IP address to connecting computers) and must be the only DHCP server on the network

- step8.** On the *IP Address* page (**Figure 12**), select *Specify an IP address* and assign an IP to your PC in the *IP Address* field. If the PC is to be used as a DMZ Host, or controlled by Access Control, assign an IP to the PC from the range *192.168.1.2~192.168.1.11*. Enter *255.255.255.0* into the *Subnet Mask* field. On the *Gateway* sheet, enter the BroadGuard's IP address into the *New Gateway* field (the default value is *192.168.1.1*). Click *Add* to add this value to the *Installed Gateway* list. Click *OK*



Figure 13. TCP/IP Properties-2

- step9.** On the *DNS Configuration* page, check *Enable DNS*. Enter your PC name into the *Host* field (see Finding your PC Host Name, page 25) and your BSP's domain name into the *Domain* field. Enter your BSP's domain name server's IP address into the *DNS Server Search Order* field and click *Add*. If you don't know your BSP's domain name and domain name server IP address, contact your BSP to get this information
- step10.** Click *OK*. The system will ask you to restart the computer. Click *Yes* to complete the installation

Windows NT 4.0

step1. Click *Start/Settings/Control Panel*



Figure 14. Control Panel

step2. Double-click the *Network* icon (Figure 14). The *Network* dialog box will open (Figure 15)

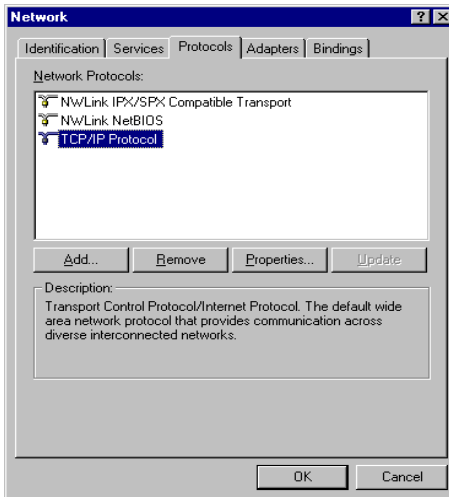


Figure 15. Network

step3. On the *Protocols* card, select *TCP/IP Protocol* and click *Properties* (Figure 15)

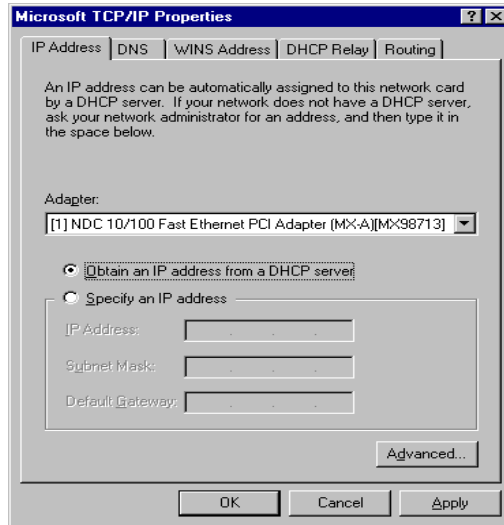


Figure 16. Microsoft TCP/IP Properties-1

- step4.** On the *IP Address* page (**Figure 16**), select *Obtain an IP address from a DHCP server* and click **OK** and go to step 6. If you want to assign a static IP to a PC, go to step 5

Note: The BroadGuard operates as a DHCP server (it automatically assigns an IP address to connecting computers) and must be the only DHCP server on the network

- step5.** On the *IP Address* page (**Figure 16**), select *Specify an IP address* and assign an IP address to your PC in the *IP Address* field. If the PC is to be used as a DMZ Host, or controlled by Access Control, assign an IP to the PC from the range 192.168.1.2~11. Enter 255.255.255.0 into the *Subnet Mask* field. On the *Gateway* sheet, enter the BroadGuard's IP address into the *Default Gateway* field (the default value is 192.168.1.1). Click **OK**
- step6.** On the *DNS* page, enter your PC name into the *Host name* field (see Finding your PC Host Name, page 25) and your BSP's domain name into the *Domain* field. Enter your BSP's domain name server's IP address into the *DNS Service Search Order* field and click **Add**. If you don't know your BSP's domain name and domain name server IP address, contact your BSP to get this information.

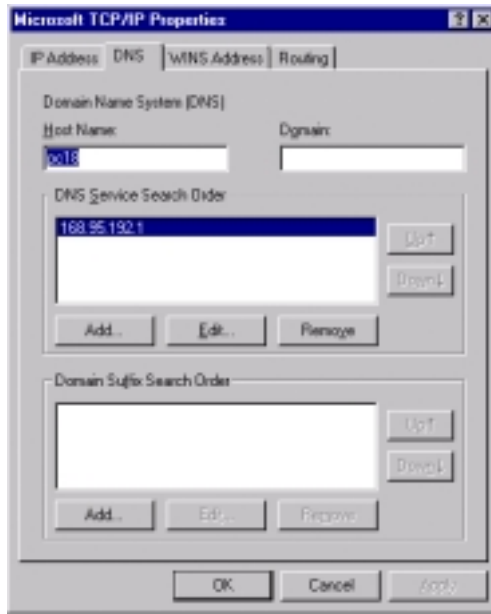


Figure 17. Microsoft TCP/IP Properties-2

step7. The system will ask you to restart the computer. Click *Yes* to complete the installation

Windows 2000

step1. Click *Start/Settings/Control Panel*



Figure 18. Control Panel

- step2.** Double-click the *Network and Dial-up Connections* icon (Figure 18). The *Network and Dial-up Connections* window will open (Figure 19)

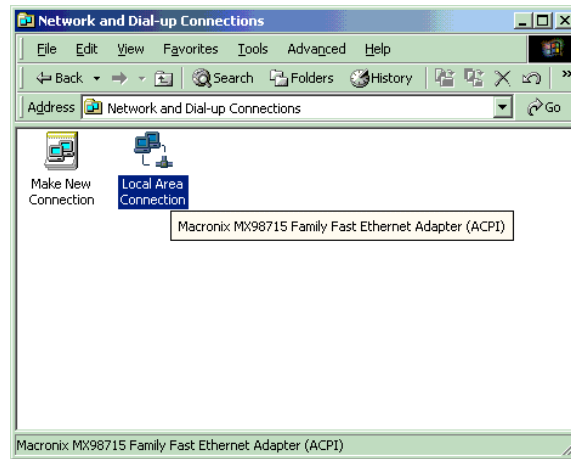


Figure 19. Network and Dial-up Connections

- step3.** Double-click *Local Area Connection*. The *Local Area Connection Status* dialog box will open (Figure 20)

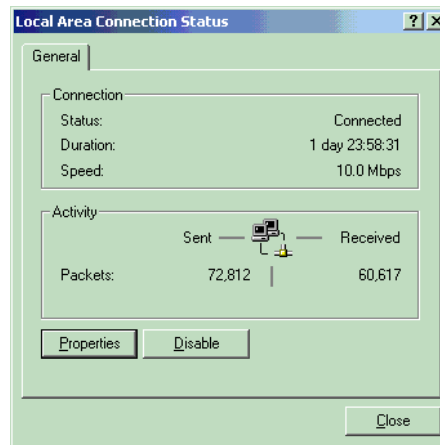


Figure 20. Local Area Connection Status

- step4.** Click *Properties*

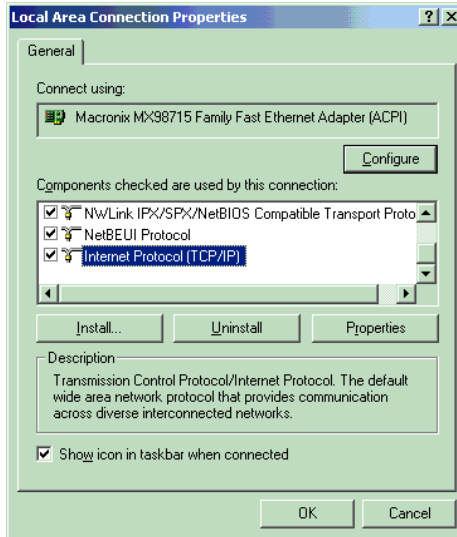


Figure 21. Local Area Connection Properties

- step5.** Select *Internet Protocol (TCP/IP)*, and click *Properties* (Figure 21). The *Internet Protocol (TCP/IP) Properties* window will open (Figure 22)

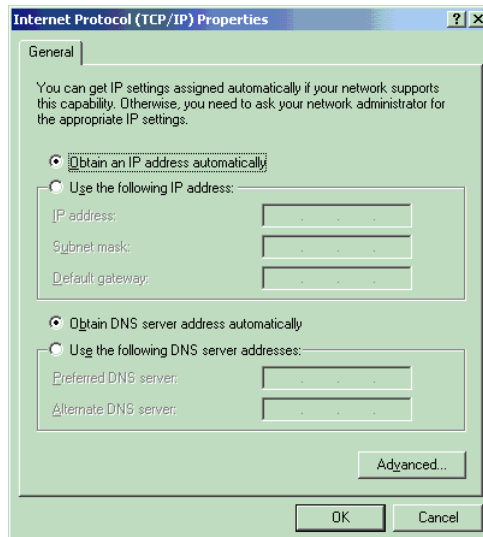


Figure 22. Internet Protocol (TCP/IP) Properties-1

- step6.** Select *Obtain an IP address automatically* and *Obtain DNS server address automatically*. Click **OK** and go to step 9. If you want to assign a static IP to a PC, go to step 7

Note: The BroadGuard operates as a DHCP server (it automatically assigns an IP address to connecting computers) and must be the only DHCP server on the network

- step7.** Check *Use the following IP address* (Figure 23) and enter an IP address for your PC in the *IP Address* field. If the PC is to be used as a DMZ Host, or controlled by Access Control, assign an IP to the PC from the range 192.168.1.2~192.168.1.11. Enter 255.255.255.0 into the *Subnet Mask* field. On the *Gateway* sheet, enter the BroadGuard's IP address into the *Default Gateway* field (the default value is 192.168.1.1). Click **OK**
- step8.** Check *Use the following DNS server addresses* (Figure 23) and enter a DNS IP address for your BSP in the *Preferred DNS server* field. If you don't know your BSP's domain name server IP address, contact your BSP to get this information

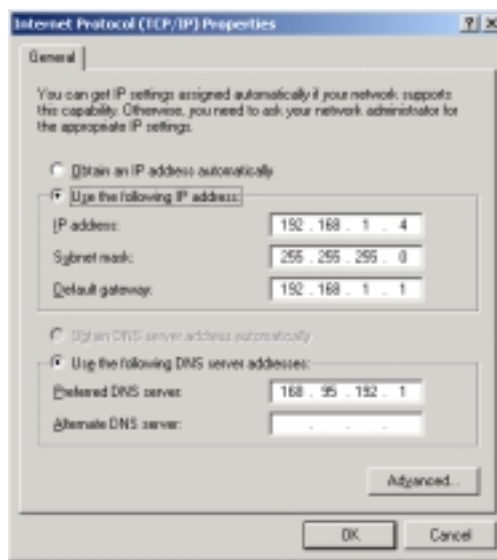


Figure 23. Internet Protocol (TCP/IP Properties-2

- step9.** Click **OK** to complete the installation

Mac OS

Using the DHCP server to assign an IP address

- step1.** Click the Apple icon in the upper left corner of the screen and select *Control Panel/TCP/IP*. The *TCP/IP (Setup Ethernet)* dialog box will appear as shown in **Figure 24**

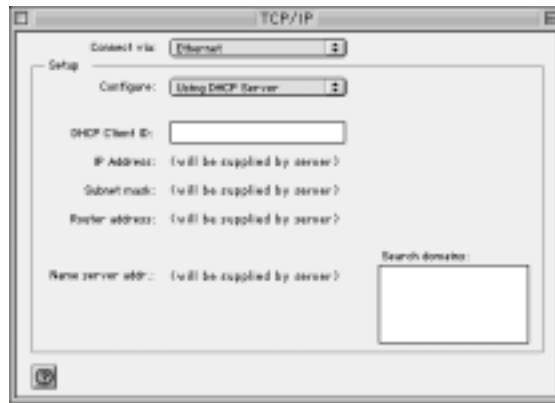


Figure 24. Using the DHCP Server

- step2.** From the *Connect Via* list box, choose *Ethernet*
- step3.** From the *Configure* list box, choose *Using DHCP Server*
- step4.** Leave the *DHCP Client ID* field blank

Manual Assignment of IP addresses

- step1.** Click the **Apple** icon in the upper left corner of the screen and select *Control Panel/TCP/IP*. The *TCP/IP (Setup Ethernet)* dialog box will appear as shown in **Figure 25**



Figure 25. Manual Configuration of IP Addresses

- step2.** From the *Connect Via* list box, choose *Ethernet*
- step3.** From the *Configure* list box, choose *Manually*
- step4.** In the *IP Address* field, type an IP address: 192.168.1.2 (or 192.168.1.3, 192.168.1.4, or 192.168.1.5)
- step5.** In the *Subnet mask* field, type 255.255.255.0
- step6.** In the *Router address* field, type the BroadGuard IP (default is 192.168.1.1)
- step7.** In the *Name server addr.* field, type the name server address(es) provided by your broadband service provider
- step8.** Close this screen and save the configuration as shown in **Figure 26**

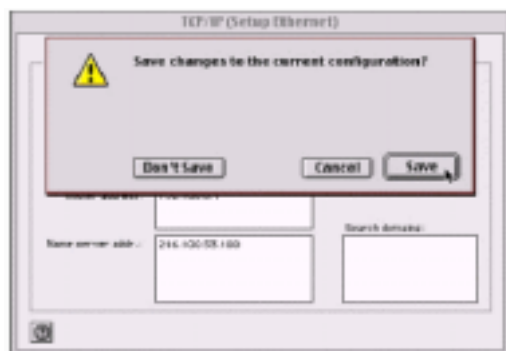


Figure 26. Saving the Configuration

- step9.** Restart your computer

Chapter 3: Network Configuration

BroadGuard Network Configuration

Network Configuration is easy to setup on the BroadGuard using a standard web browser (Netscape Communicator 4.0/Microsoft Internet Explorer 3.0 or above).

Entering the BroadGuard Setup Home Page

- step1.** Start the web browser and type 192.168.1.1 in the address field (**Figure 27**). Press *Enter*

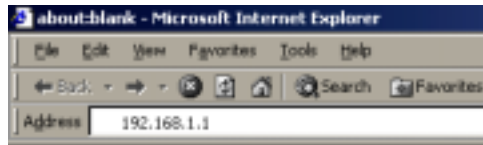


Figure 27. Entering the Setup Wizard

- step2.** The *Enter Network Password* window will open (**Figure 28**)



Figure 28. Enter Network Password

- step3.** Enter the factory default User Name *admin*
step4. Enter the factory default Password *1234*
step5. Click *OK*

Note: Refer to "Change Password" on page 31 if you wish to change the password

Setup Home Page

There are three sections on the home page:

Setup (Basic)	<i>Broadband Connection</i>	Use when your BSP (Broadband Service Provider) requests you to enter specific settings, e.g. MAC address authentication, PPPoE, host name/domain name, or specifies an IP address to make an Internet connection.
	<i>Hacker Attack E-mail Alerts</i>	An anti-attack algorithm is built into the BroadGuard to protect your network from conventional hacker attacks. If you enable e-mail alerts, whenever the BroadGuard detects an attack it will send a warning e-mail to the address entered here.
	<i>Change Password</i>	Changes the security password.
Setup (Advanced)		
	<i>Access Control</i>	The Access Control section allows you to control Internet use in your home/office.
	<i>DMZ Host</i>	Use this function to expose a PC to the Internet for playing Internet interactive games, video conferencing, as a VPN server, or as an e-mail server through the BroadGuard. A static IP address needs to be assigned to the DMZ Host PC.
	<i>DHCP Setting</i>	Enable/Disable the BroadGuard's DHCP server. Use to set the dynamic IP address range.
Status		<ul style="list-style-type: none"> • View WAN connection status and Internet Network settings • View LAN Network Settings • View Firewall Status
Tools		
	<i>PPPoE Check</i>	Checks PPPoE is functioning correctly

22 SOHOware® Secure Cable/DSL Router

	<i>Hacker Alert Test</i>	Sends a test Hacker Alert E-mail
	<i>View Current Access Control Settings</i>	The PCs in the list have been denied access to the services shown.
	<i>Access Monitor</i>	Shows the current Internet activities of monitored users.
	<i>Download Firmware</i>	Download the latest BroadGuard firmware.

After clicking **OK** you will enter the setup home page. Click the **Broadband Connection** link to begin setup of your broadband connection.

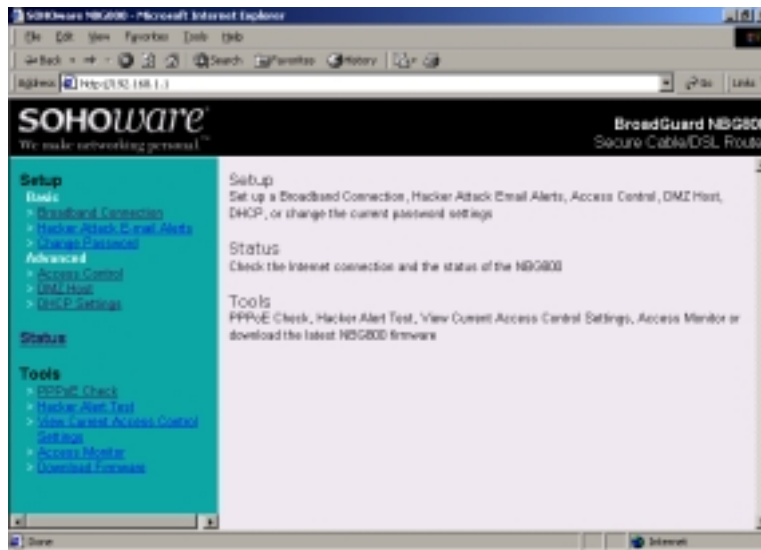


Figure 29. Setup Start Page

Basic

Broadband Connection

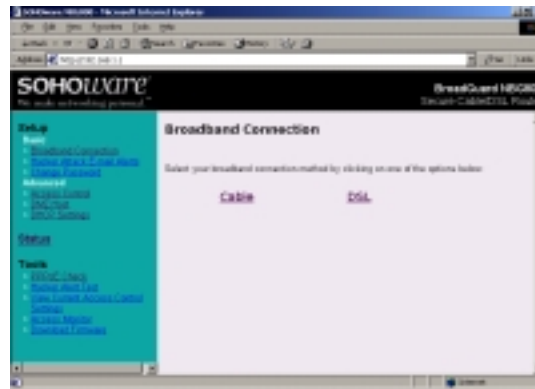


Figure 30. Broadband Connection

Select the type of Broadband service that you are subscribed to. Click either *Cable Modem* or *DSL* to set up the network properties.

There is no need to enter any information in *Broadband Connection* (Figure 30) unless your BSP has assigned you specific Internet connection information (Host Name, Domain Name, MAC address authentication, PPPoE, or a static IP Address).

Cable Setup



Figure 31. Cable Broadband Connection

MAC Address Clone: Some BSPs use an Ethernet adapter's MAC address as an identifier to provide Internet service. In these cases, you need to clone the Ethernet adapter's MAC address to the BroadGuard. At the BroadGuard, disconnect the Ethernet cables from the other PCs on the network, leaving only the PC with the Ethernet adapter that you wish to register connected.

Note: If you previously used a registered MAC address to connect to your broadband service, you need to use the same Ethernet adapter and clone its MAC address to the BroadGuard.

There are two MAC addresses shown on the screen. One is the PC's Ethernet card's (this PC is connected to the BroadGuard via Ethernet), the other is the BroadGuard's. Click **Clone MAC** to change the IP address of the BroadGuard to that of the Ethernet card. Click **Restore MAC** to restore the original MAC address of the BroadGuard.

Note: After saving the settings and restarting the BroadGuard, you **MUST** turn your cable/DSL modem off and on.

Host Name: Some BSPs (e.g. Cox@Home) may ask their subscribers to enter information into this field in order to make a connection to their broadband service. Begin setting up the BroadGuard with the computer originally setup by the Cox@Home technician, or the computer that you registered with Cox@Home - this computer will already contain your Cox@Home Host Name. If you have not been given a specific name, leave this field blank.

Finding your PC Host Name

Windows 95/98/98SE/Me

step1. Right-click *Network Neighborhood*. Click **Properties**. The *Network* dialog box will open



Figure 32. Network

step2. Click on the *Identification* tab and write down the information contained in the *Computer Name* field – this is your Host Name

Windows NT 4.0

step1. Right-click *Network Neighborhood*. Click *Properties*. The *Network* dialog box will open



Figure 33. Network

- step2.** Write down the information contained in the *Computer Name* field – this is your Host Name

Windows 2000

- step1.** Right-click *My Computer*. Click *Properties*. The *System Properties* dialog box will open

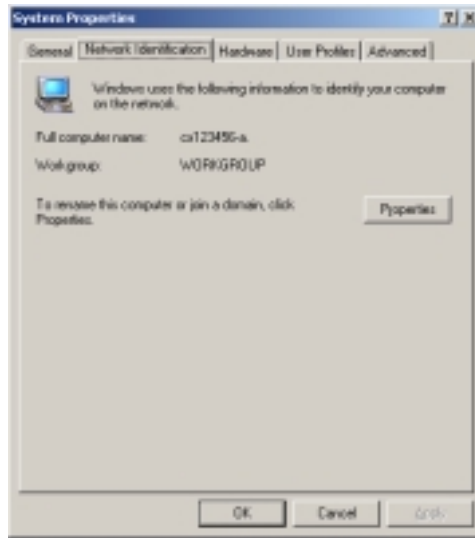


Figure 34. System Properties

- step2.** Click on the *Identification* tab and write down the information contained in the *Computer Name* field – this is your Host Name

Domain Name: Some BSPs (e.g. Cox@Home) may ask their subscribers to enter information into this field in order to make a connection to their broadband service. The BroadGuard will automatically get this information from the Cox@Home server. If you have not been given a specific name, leave this field blank.

Note: You must restart the PC after entering your Cox@Home Host Name as described above.

If your broadband service provider assigns you a static IP address, you must check **Specify an IP Address** and then enter all IP address information into all fields (**Figure 35**). If not, you can skip this step.

If your Broadband Service Provider has not given you an IP address, check "Obtain an IP Address Automatically". If you have been given a specific IP address, check "Specify an IP Address".

Obtain IP Address Automatically
 Specify an IP Address

IP Address Assigned by Your BSP:

Subnet Mask Assigned by Your BSP:

Gateway Address Assigned by Your BSP:

Has your Broadband Service Provider given you a DNS address? If yes, enter the information in the fields below.

Primary DNS IP :

Secondary DNS IP :

Figure 35. Cable Broadband Connection

Click *Save* and *Restart* to start sharing your broadband connection.

DSL Setup

The screenshot shows the SOHOware web interface for configuring a DSL connection. The page title is "DSL Broadband Connection". It includes a sidebar with navigation options like "Setup", "Status", and "Task". The main content area contains the following fields and options:

- Use PPPoE DSL Service:** No Yes
- User Name:**
- Login Password:**
- Service Name:**
- Connect On Demand:** Yes No
- Maximum Idle Time Before Disconnecting:** (Default)

Figure 36. Broadband Connection

Check *Yes* to enable PPPoE service. Several parameters are required to establish a DSL connection via PPPoE (User Name, Login Password, some broadband service providers also require a Service Name). Enter all information provided by your BSP into all required fields.

Connect-on-demand --- This setting allows the BroadGuard to automatically make a connection to your BSP whenever you launch an Internet application. The default setting is “Yes”.

Maximum Idle Time Before Disconnecting --- If there is no activity on the connection longer than the time set here, the connection will automatically be dropped.

If your Broadband service provider assigns you a static IP address, you must set *Use PPPoE DSL Service* to **NO**. Next check *Specify an IP Address* and enter all IP address information into all fields. If not, you can skip this step.

If your Broadband Service Provider has not given you an IP address, check "Obtain an IP Address Automatically". If you have been given a specific IP address, check "Specify an IP Address".

Obtain IP Address Automatically
 Specify an IP Address

IP Address Assigned by Your BSP:

Subnet Mask Assigned by Your BSP:

Gateway Address Assigned by Your BSP:

Has your Broadband Service Provider given you a DNS address? If yes, enter the information in the fields below.

Primary DNS IP :

Secondary DNS IP :

Figure 37. DSL Broadband Connection

Click *Save* and *Restart* to start sharing your broadband connection.

Hacker Attack E-mail Alerts

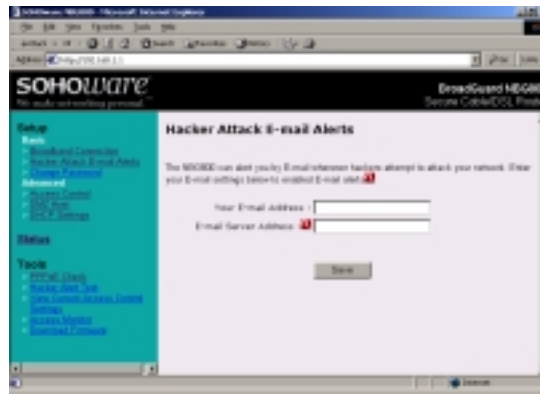


Figure 38. Hacker Attack E-mail Alerts

An anti-attack algorithm is built in to the BroadGuard so that it can protect client PCs from conventional attacks. With BroadGuard, you have a professional firewall but without any specialized setup/configuration. BroadGuard gives your network the capability to prevent many kinds of hackers' attacks.

If you turn on the e-mail alert function, whenever BroadGuard detects an Internet attack it will automatically send an e-mail with an attached log file to you.

The info. will look something like the following:

```
udp -(203.69.97.139 ,211.55.79.155 )-840 -port scan attack-forward  
udp -(203.69.97.139 ,211.55.79.155 )-546 -port scan attack-forward  
udp -(203.69.97.139 ,211.55.79.155 )-544 -port scan attack-forward
```

In the example above, the first IP address (203.69.97.139) on each line indicates the address the hacker is using. The second (211.55.79.155) is the user's Internet IP address. As for ports 840, 546, and 544, they are the numbers of ports that are being attacked.

Forward this e-mail to your BSP for analysis.

Note: The e-mail alert is sent at approximately the same time your computer is attacked.

Enter the e-mail address that the warnings should be sent to.

The e-mail server address can be obtained from your broadband service provider.

Click **Save** to store the settings. Click **Restart** to initialize the BroadGuard with the new settings.

Change Password

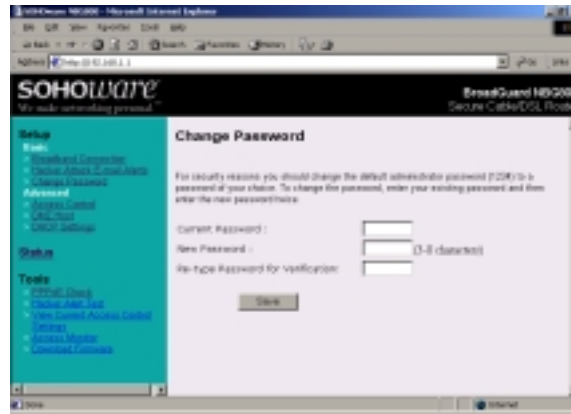


Figure 39. Change Password

For security reasons you should change the default administrator password (1234) to a password of your choice.

- step1.** Enter the current password, the new password, and then retype it for verification. Click **Save**. Click **Restart** to initialize the BroadGuard with the new password
- step2.** The *Enter Network Password* dialog box will open
- step3.** Enter the username **admin**, and key in the new password. Click **OK** and you will enter the BroadGuard Setup page again

Advanced

Access Control

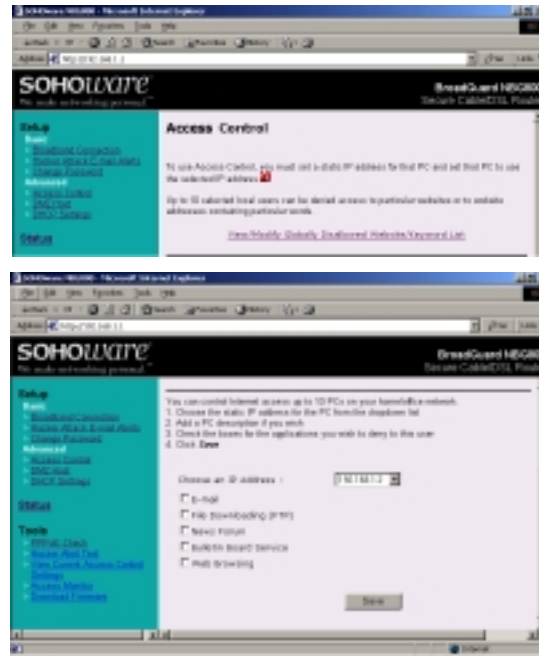


Figure 40. Access Control

This feature prevents users (or children) from running disallowed Internet applications or accessing unsuitable websites (maximum 10 websites). In order to achieve this functionality, a static IP should be assigned to users who will be restricted.

Up to 10 local users can be denied access to particular websites or to website addresses containing particular words. Click *View/Modify Globally Disallowed Website/Keyword List* to open the limited web sites list (Figure 41).



Figure 41. Globally Disallowed Websites/Keywords

This list will be applied to all restricted users. Enter the full domain name of the website or just enter a keyword. Click **Save** to save the new list.

Access Control may be used to restrict use of the following Internet applications:

- E-mail
- File Downloading
Checking *File downloading* stops use of the FTP protocol and prevents users from downloading files from an FTP site (but they will still be able to download files from a website)
- News Forum
- Bulletin Board Service
- Web Surfing

You may control Internet access of up to 10 PCs on your home/office network.

1. Choose the static IP address for the PC from the dropdown list
2. Check the boxes for the applications you wish to deny to this IP address
3. Click **Save**

DMZ Host

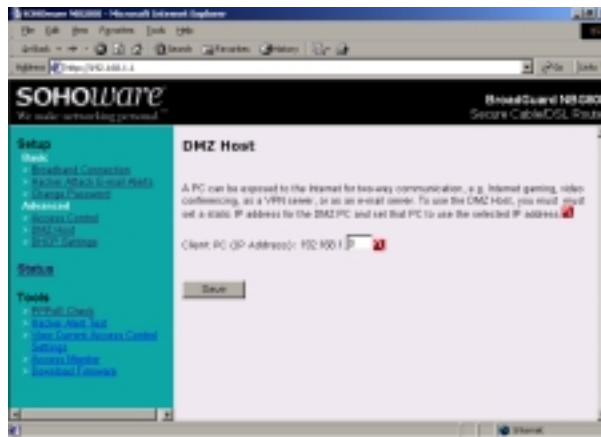


Figure 42. DMZ Host

Usually all PCs connected to the BroadGuard are protected from Internet intruders by a built-in firewall. For some kinds of Internet applications, for example, Internet interactive games, video-conferencing, VPN (Virtual Private Networks), or as an e-mail server etc., computers must be exposed to the Internet. The DMZ Host function assigns one of the client computers to be exposed.

BroadGuard setting: You must assign a static IP address to the Client PC to be exposed to the Internet, then click **Save** to make the setting effective. Click **Restart** to initialize the BroadGuard with the updated settings.

Once the static IP address is assigned to a specific client PC, you **MUST** specify the PC as the DMZ Host.

DMZ Host Disable

For extra security, when you do not require the DMZ Host to be exposed to the Internet, you should disable this function by entering a 0 (zero) in the Client PC (IP Address) box.

Note: The DMZ PC operates outside the protection of the BroadGuard's built-in firewall. If the DMZ PC is not operating in the DMZ role, but is still powered-on for local use, you should disable DMZ Host to prevent hackers from accessing the PC.

DHCP Settings



Figure 43. DHCP Settings

Under normal operation, all client PCs' IP addresses are automatically assigned by the BroadGuard's DHCP server.

The IP address range runs from 192.168.1.1 to 192.168.1.254. Up to 253 IP addresses may be assigned to client PCs. The IP address 192.168.1.1 is reserved for the BroadGuard. The other IP addresses are divided into two IP groups. One is the dynamic IP group, the other is the static IP group.

The dynamic IP start address may be specified by the user, e.g. 192.168.1.100 (default value). Once this start IP address has been assigned by you, all IP addresses running from 192.168.1.100 to 192.168.1.254 will be part of the dynamic IP address pool. IP addresses from 192.168.1.2 to 192.168.1.99 will be available as static IP addresses.

You can see the client PC's information on the *DHCP IP Address Assignments* screen

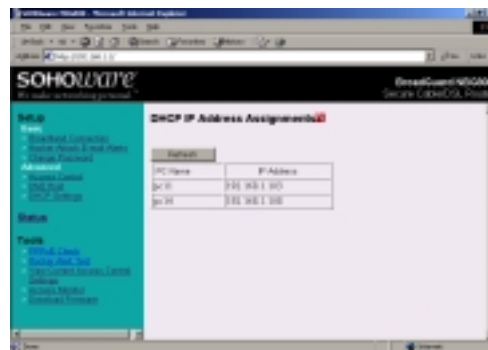


Figure 44. DHCP IP Address Assignments

Note: IP information of statically assigned IP PCs is not shown here.

Each time the BroadGuard is powered-off, the *DHCP IP Address Assignments* information will be cleared, even though your computer may still be switched on. To prevent this problem:

- step1.** Shut down your PC
- step2.** Power your BroadGuard on
- step3.** Turn your PCs on

Status

The *Status* section contains; Internet information, the BroadGuard LAN IP address assignment, and the Public IP Address assignments (**Figure 45**). This information is useful in resolving a connection problem.



Figure 45. Status

Internet	<p>Internet IP address assigned by your BSP</p> <p>Subnet Mask: 255.255.255.0 is the default setting</p> <p>Gateway IP: The IP address of the BSP's Internet Network Gateway</p> <p>DNS Server IP: The IP address of the BSP's Domain Name Server</p>
-----------------	---

BroadGuard	<p>IP Address: The IP address of the NGB800</p> <p>Subnet Mask: 255.255.255.0 is the default setting</p> <p>MAC Address: The MAC address of the BroadGuard</p> <p>Firewall: The NGB800 firewall status</p>
-------------------	--

Tools

Five useful tools are provided: PPPoE Check, Hacker Alert Test, View Current Access Control Settings, Access Monitor, and Download Firmware.

PPPoE Check (DSL Users Only)

If you are a DSL user, this page will help you to check whether your settings for PPPoE work or not. After making the PPPoE settings on the broadband connection, save and restart your BroadGuard. Then open the PPPoE Check page and click ***Check Now***.

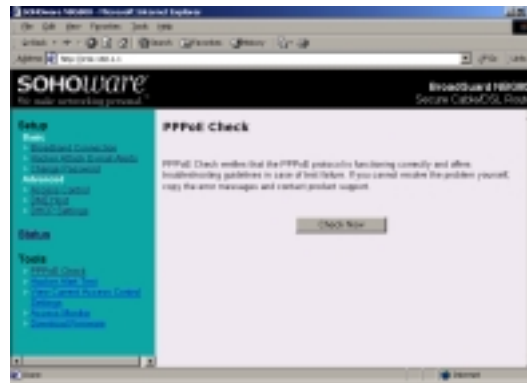


Figure 46. PPPoE Check

Either of the following screens (**Figure 47** or **Figure 48**) indicate that your PPPoE has worked well.

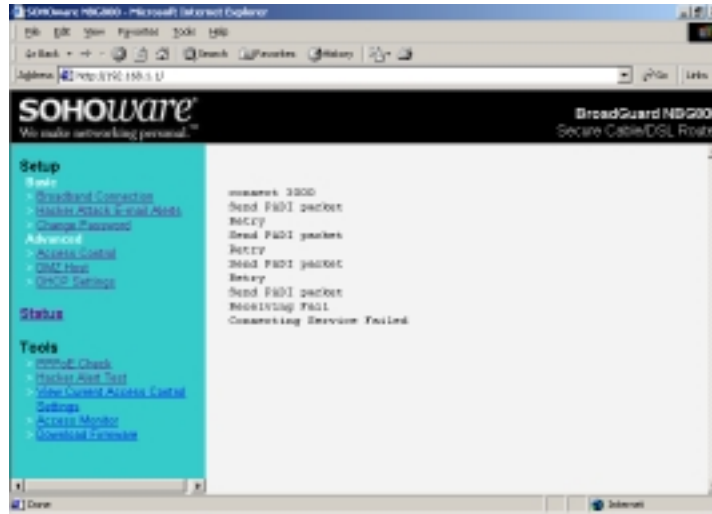


Figure 49. PPPoE Check Unsuccessful

A screen such as that shown in Figure 50 indicates that you entered a wrong username, login password, or service name. Go to the DSL broadband connection setup page to check them again.

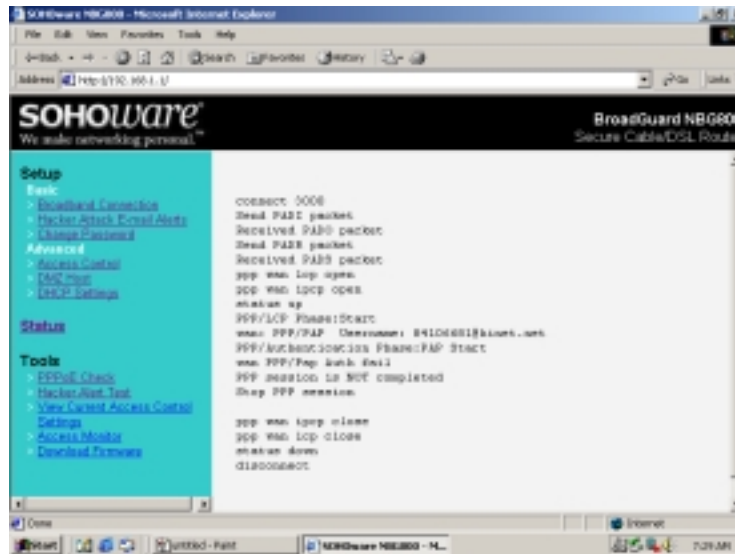


Figure 50. Authentication Failed

Hacker Alert Test

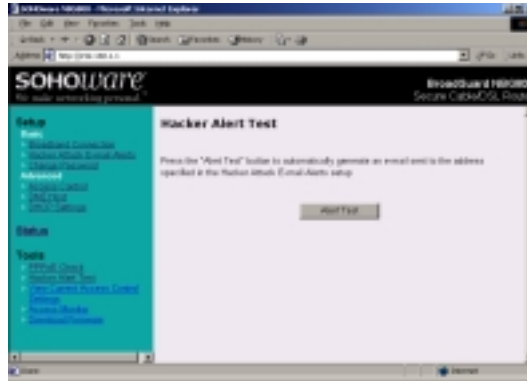


Figure 51. Hacker Alert Test

Click the *Alert Test* button to automatically generate an email sent to the address specified in Hacker Attack E-mail Alerts, page 30. The subject line will read “NBG800 Hacker Alert Test”.

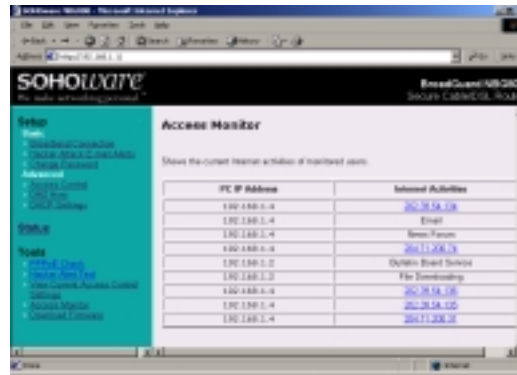
View Current Access Control Settings

IP Address	Applications Denied
192.168.1.2	Email
192.168.1.2	File Downloading
192.168.1.3	Email
192.168.1.3	File Downloading
192.168.1.3	Stream P2P
192.168.1.4	Email
192.168.1.4	File Downloading
192.168.1.4	Stream P2P
192.168.1.4	Instant Board Service
192.168.1.5	Email
192.168.1.5	File Downloading
192.168.1.5	Stream P2P
192.168.1.5	Instant Board Service
192.168.1.7	Web Browsing

Figure 52. View Current Access Control Settings

On this page you can view access control settings of PCs restricted by you. You will see each PC’s manually assigned IP address, and a list of the denied Internet applications for each restricted PC.

Access Monitor



PC IP Address	Internet Activities
192.168.1.4	201.38.58.106
192.168.1.4	Email
192.168.1.4	New Forum
192.168.1.4	2011.008.19
192.168.1.0	D/Win Board Service
192.168.1.0	File Downloading
192.168.1.4	201.38.58.106
192.168.1.4	201.38.58.100
192.168.1.4	201.71.206.37

Figure 53. Access Monitor

Access Monitor shows the current Internet activities of monitored users. The table shows the PC's IP address, and its Internet activities. Easily monitor Internet activity flow through the BroadGuard to see whether there is any improper Internet activity on your home/office network.

The information shown is automatically updated every 5 seconds. Click any website's hypertext address to go to that website.

Download Firmware

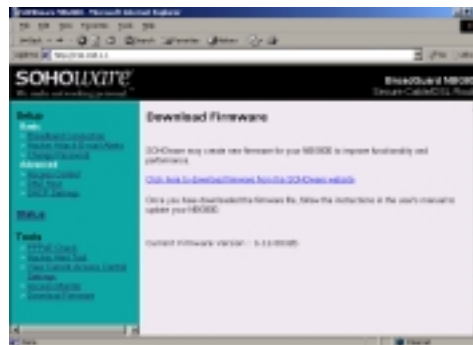


Figure 54. Download Firmware

This tool permits easy downloading of the latest BroadGuard firmware. The SOHware website provides two different files depending on whether you are using a Windows, Mac, or Linux computer.

Windows Users

Download the firmware from the SOHOfware web site and save the file on your local hard drive. Double-click the file and follow the on-screen instructions to run the firmware upgrade.

After the upgrade process is complete, you must turn off and turn on your BroadGuard to make your new firmware effective.

Mac & Linux Users

For Mac and Linux users we currently offer the firmware binary file only. These users will require a third-party TFTP program to complete the firmware upgrade.

After the upgrade process is complete, you must turn off and turn on your BroadGuard to make your new firmware effective.

Chapter 4: Troubleshooting

If you cannot find your problem listed below, see Chapter 5: FAQs, page 49, or see the BroadGuard FAQ at the SOHOware website.

1. I can't connect to the BroadGuard. The BroadGuard is properly installed, LAN connections are OK, and it is powered ON.

- Ensure that your PC and the BroadGuard are on the same network segment. If you are not sure, restart the BroadGuard, let the PC get the IP address automatically.
- Ensure that your PC is using a static IP Address within the default range of 192.168.1.2 to 192.168.1.254 and is thus compatible with the BroadGuard default IP Address of 192.168.1.1.
- The Subnet Mask should be set to 255.255.255.0 to match the BroadGuard. On the client PC, you can check these settings by using *Control Panel/Network* to check the properties for the TCP/IP protocols.

2. The Status LED stays lit when it shouldn't.

The Status LED lights when the device is powered up and checks for proper operation. After finishing the checking procedure, the LED turns off to show the system is working fine.

If the LED remains lit after this time, the BroadGuard is not working properly. Contact your dealer.

3. I can't browse through the BroadGuard.

- Check that both ends of the network cable and power adapter are properly connected. Check that all LEDs on the front panel are functioning properly. Use *Status (Figure 55)* to check that your BroadGuard is still connected to your BSP. If there is no public IP address shown on the screen, the problem lies with the BSP.



Figure 55. Status

- Check that the PC got an IP address assigned to it automatically (for Windows 95/98/Me see Figure 12, page 11. For Windows NT 4.0, see Figure 16, page 14. For Windows 2000 see Figure 22, page 17. For Mac users, see Figure 24, page 19.
- Make sure that TCP/IP is setup on the client PCs and that the IP addresses are in the range 192.168.1.x (x is from 2 to 254). Check the IP Address via the *View DHCP IP Address Assignments* page. If the IP address assignments are not within the stated range, follow the steps below to rebuild the setup.

Windows 95/98/Me

step1. Click *Start/Run*, type *winipcfg*, and click *OK* (Figure 56)

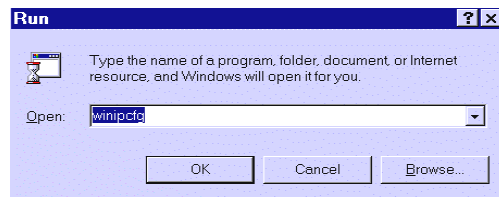


Figure 56. Run

step2. The *IP Configuration* dialog box will open (Figure 57)

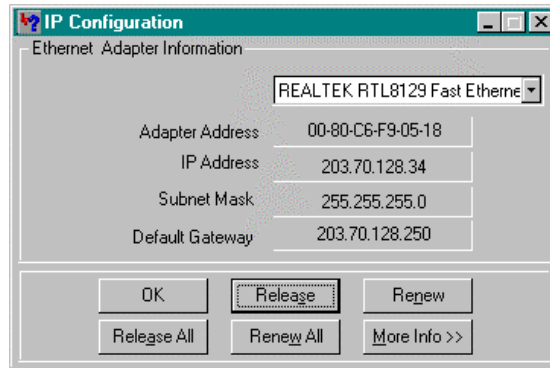


Figure 57. IP Configuration

- step3.** Select the network adapter you use to connect to the BroadGuard. Click **Release**
- step4.** Click **Renew** to retrieve new information (IP address, subnet mask, and default gateway address) from the BroadGuard. Click **OK** to save the changes and exit the program
- step5.** Go to **DHCP IP Address Assignments** (see Figure 44, page 35). Click **Refresh**

Windows NT 4.0

- step1.** Click **Start/Programs/Command Prompt**

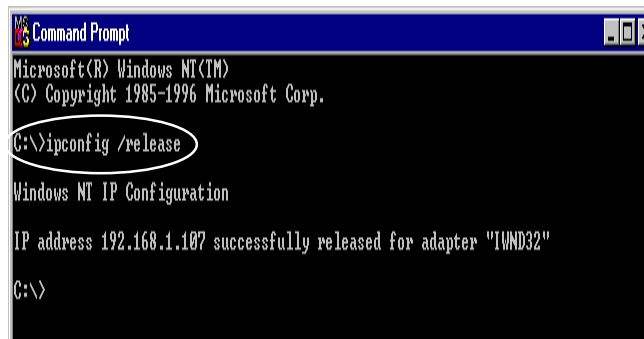


Figure 58. Command Prompt-1

- step2.** Type "**ipconfig /release**" (**Figure 58**) and press **Enter**
- step3.** Type "**ipconfig /renew**", and press **Enter** to retrieve new information (IP address, subnet mask, and default gateway address) from the BroadGuard (**Figure 59**)

```
Microsoft Windows NT [RM]
(C) Copyright 1985-1996 Microsoft Corp.

C:\>ipconfig /release

Windows NT IP Configuration

IP address 192.168.1.2 successfully released for adapter "TND02"

C:\>ipconfig /renew

Windows NT IP Configuration

Ethernet adapter TND02:

    IP Address. . . . . : 192.168.1.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

C:\>
```

Figure 59. Command Prompt-2

- step4. Type *Exit*
- step6. Go to *DHCP IP Address Assignments* (see Figure 44, page 35). Click *Refresh*

Windows 2000

- step1. Click *Start/Programs/Accessories/Command Prompt*

```
Command Prompt

C:\>ipconfig /release

Windows 2000 IP Configuration

IP address successfully released for adapter "Local Area Connection"

C:\>
```

Figure 60. Command Prompt-3

- step2. Type "*ipconfig /release*" (Figure 60) and press *Enter*
- step3. Type "*ipconfig /renew*", and press *Enter* to retrieve new information (IP address, subnet mask, and default gateway address) from the BroadGuard (Figure 61)

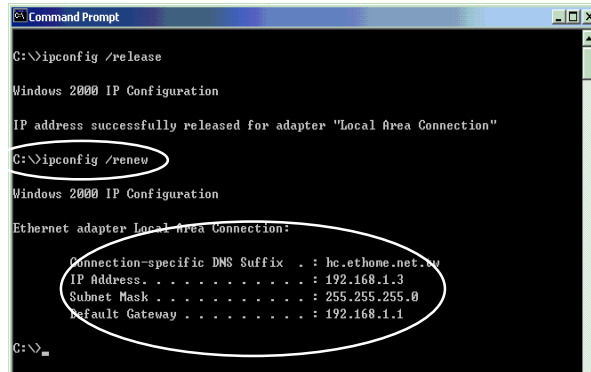


Figure 61. Command Prompt-4

- step4.** Type *Exit*.
- step5.** Go to *DHCP IP Address Assignments* (see Figure 44, page 35). Click *Refresh*

4. Entering a URL or IP address results in a timeout error.

Follow the steps below to solve this problem:

- step1.** Check if other PCs can connect to the network without problems. If they can, ensure the problem PC's IP settings are correct (IP address, subnet mask, default gateway, and DNS)
- step2.** Check the BroadGuard Internet settings (IP address, subnet mask, default gateway, and DNS) in *Status* (**Figure 62**). If there is no information shown on the screen, it means that your BSP has a problem



Figure 62. Status

5. You can't view a PC's name or its IP address in the *DHCP IP Address Assignments* page, though it can still access the Internet.

Each time the BroadGuard is powered-off, the *DHCP IP Address Assignments* information will be cleared, even though your computer may still be switched on. To prevent this problem:

- step1.** Shut down your PC
- step2.** Power your BroadGuard on
- step3.** Turn your PCs on

6. I can connect to the BroadGuard, but can't get outside connections

- Ensure that all of your cabling is properly connected and that all of the BroadGuard's cable/DSL and LAN LEDs are correctly illuminated.
- Power down your cable/DSL modem and BroadGuard for a few seconds. Then turn the cable/DSL modem on. After the modem goes through its self-test, turn the BroadGuard on. After the BroadGuard goes through its self-test, check whether you can get an outside connection.
- Ensure that your cable or DSL modem is DHCP-capable.
- Make sure all broadband connection setup is correct.
- The problem may be caused by your BSP (Broadband Service Provider) issuing a different IP address from time to time. The BroadGuard gets its public IP from the BSP's DHCP server automatically. The BroadGuard must renew the public IP if the BSP cancels the originally assigned IP address.

Chapter 5: FAQs

- **How many PCs simultaneously accessing the Internet can be supported by the BroadGuard?**
253 PCs may simultaneously access the Internet via the BroadGuard.
- **Where should we install the BroadGuard on our network?**
In a typical environment, the BroadGuard is installed between a cable/DSL modem and LAN. Connect the BroadGuard to the cable/DSL modem with Cat.5 RJ-45 cable.
Plug one end of the cable into the WAN port of the BroadGuard and the other end into the Ethernet port of the cable/DSL modem.
- **Does the BroadGuard support IPX or AppleTalk?**
No. TCP/IP is the 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.
- **I'm using Linux. Does the BroadGuard support this operating system?**
Yes. The BroadGuard is compatible with any operating system.
- **Does the BroadGuard support 100Mbps Fast Ethernet?**
Yes. Both 10 and 100Mbps Fast Ethernet are supported.
- **Does the BroadGuard support ICQ send file?**
Yes, with the following fix: ICQ menu-> preference -> connections tab-> check "I am behind a firewall or proxy", and set the firewall time-out to 80 seconds. An Internet user can then send a file to a user behind the BroadGuard.
- **How do I get Napster to work with the BroadGuard?**
Napster is fully compatible with the BroadGuard and requires no special settings.
- **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 can I avoid receiving corrupted FTP downloads?**
If you are experiencing corrupted files when you download a file with your FTP client, try using another FTP program.
- **How will I be notified of new BroadGuard firmware upgrades?**
All firmware upgrades are posted on the SOHOfware website at

www.sohoware.com, where they can be downloaded for free.

- **Does the BroadGuard pass PPTP packets?**
Yes.
- **Does the BroadGuard support IPSec?**
This function will be supported in later firmware upgrades.
- **What is the recommended maximum number of VPN sessions I can run on the BroadGuard?**
We recommend the number of sessions is five or less to prevent influencing the throughput of the BroadGuard.
- **Will the BroadGuard function in a Macintosh environment?**
Yes, but the BroadGuard's setup pages are accessible only through Internet Explorer v4.0 or Netscape Navigator v4.0 or higher for Macintosh.
- **With which type of firewall is the BroadGuard equipped?**
The BroadGuard uses NAT, anti-DoS (Denial of Service) and (SPI) Stateful Packet Inspection.
- **What is DoS (Denial of Service)?**
The goal of a Denial of Service (DoS) attack is not to steal information, but to disable a device or network so users no longer have access to network resources. For example, "TearDrop", a DoS hacker tool which is widely available on the Internet, allows users to remotely crash any unprotected Windows computer on the Internet. Most types of Internet attacks try to exploit the weaknesses in the TCP stacks of the operating systems of host machines. BroadGuard protects against the following types of DoS attacks:
 - SYN Flooding
 - Ping of Death
 - LAND attacks
 - Smurf attacks
 - IP Spoofing
 - TearDrop
 - WinNuke
- **What is Stateful Packet Inspection (SPI)?**
Stateful Packet Inspection is a technology similar to that used in enterprise-level firewall products. It is generally regarded as a "state of the art" firewall technology. With SPI, the BroadGuard makes security decisions based on the origination of Internet sessions. The BroadGuard will allow incoming data

from the Internet only if it is part of a session that was initiated by one of the users on the secure Local Area Network (LAN), but will block all communications that are initiated from the Internet. SPI has the added benefit of being easy to manage, making it ideal for those who don't have MIS people for networking maintenance.

- **Does the BroadGuard support routing protocols?**
Yes, it support both RIP I & RIP II.
- **I am not able to get the web configuration screen for the BroadGuard. 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.
- **Will the BroadGuard allow me to use my own public IP and Domain?**
The BroadGuard allows for customization of your public IP and Domain. If you use a cable connection see Figure 35, page 28. For DSL users, see Figure 37, page 29.
- **Is there an internal cable or DSL modem in the BroadGuard?**
No, the BroadGuard must work in conjunction with an external cable or DSL modem.
- **Which modems are compatible with the BroadGuard?**
The BroadGuard is compatible with virtually any cable or DSL modem that supports Ethernet.
- **How can I check whether I have static DHCP IP Addresses?**
Consult your BSP to confirm the information.
- **How do I get Half-Life: Team Fortress to Work with the BroadGuard?**
If you want to host a game, you must expose your PC to the Internet using DMZ Host (see DMZ Host, page 34). If you only want to join a game hosted by somebody else, then there is no need to set your machine as a DMZ Host.
- **How do I get mIRC to work with the BroadGuard?**
You must expose your PC to the Internet using DMZ Host (see DMZ Host, page 34).
- **How can I learn more about Internet safety issues?**
As parents, protecting children from accessing websites that contain improper content is critical. Many sites discuss this issue on the Internet. You can use a search engine (e.g. www.yahoo.com) to get those sites' addresses by entering the keywords "child safety". The www.getnetwise.org website is suggested for parents to obtain more information.

Appendix A: VPN REMOTE ACCESS

Thanks to advanced technology, you can use the BroadGuard to remotely access your office VPN server from your home office and you also can build a VPN server for mobile sales to access for urgent purposes. BroadGuard supports all PPTP packet based VPN software

BroadGuard VPN Server Configuration

To run a VPN server, you will find using a static IP will greatly simplify your system management (as the IP address never changes). The PC must be exposed to the Internet as a DMZ Host. Only one PC can be used as a VPN server as only one PC may be set as a DMZ Host.

- step1.** See Broadband , page 24, and check *Specify an IP Address* and then enter all IP address information into all fields
- step2.** The PC that you plan to make a VPN server must be assigned as the DMZ Host

Client Configuration (e.g. Microsoft PPTP)

Set up your Microsoft computer as a VPN Client

VPN is natively supported in Windows 98, 98SE, and Me. On a Windows 95 machine, you need to upgrade to Dial-Up Networking Version 1.3.

Windows 98/98/SE/Me VPN Client Setup

- step1.** Click *Start/Settings/Control Panel*

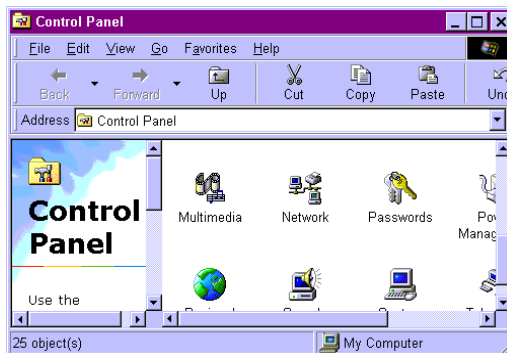


Figure 63. Control Panel

step2. In *Control Panel*, double-click the *Network* icon. The *Network* dialog box will open (**Figure 64**)

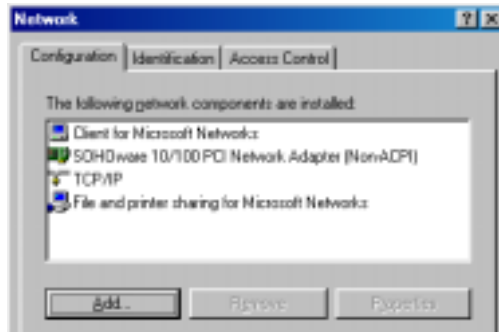


Figure 64. Network

step3. Click *Add*. The *Select Network Component Type* dialog box will open (**Figure 65**)



Figure 65. Select Network Component Type

step4. Double-click *Adapter*. The *Select Network adapters* dialog box will open (**Figure 66**)

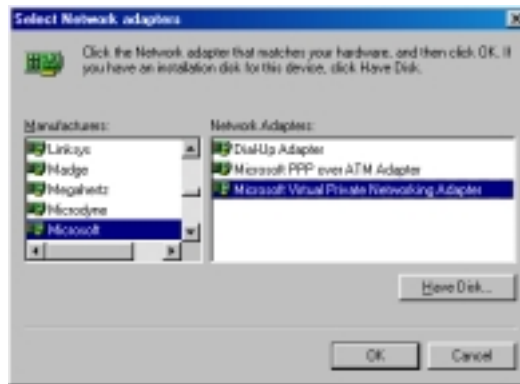


Figure 66. Select Network Adapters

- step5.** In the left window, choose *Microsoft*. In the right, select *Microsoft Virtual Private Networking Adapter*. After the Microsoft Virtual Private Networking Adapter component is completely installed, click **OK**. You will be returned to the *Network* menu (**Figure 67**). The *Microsoft Virtual Private Networking Adapter* item in the *Network* box indicates that it has been successfully installed.

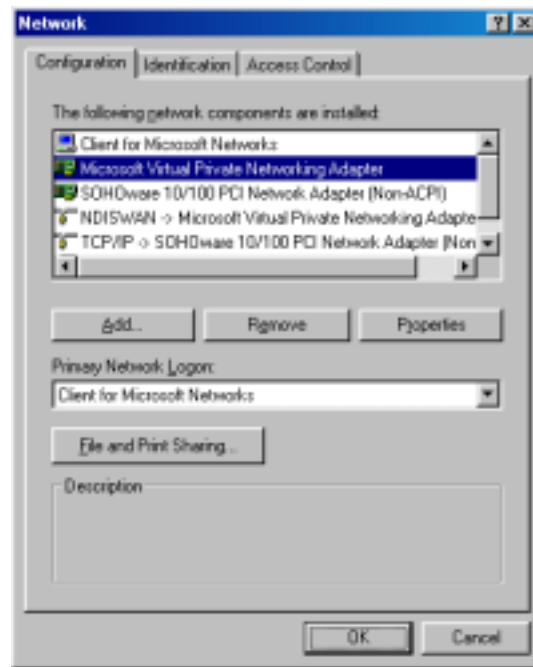


Figure 67. Network

- step6.** Windows may ask for the Windows CD-ROM. Insert the Windows CD and click **OK**
- step7.** The system will ask you to restart your computer. Click **Yes** to complete the installation
- step8.** After restarting, click *My Computer/Dial-Up Networking*. The *Welcome to Dial-Up Networking* dialog box will open (**Figure 68**)



Figure 68. Welcome to Dial-Up Networking

step9. Click *Next*. The *Make New Connection* dialog box will open (**Figure 69**)

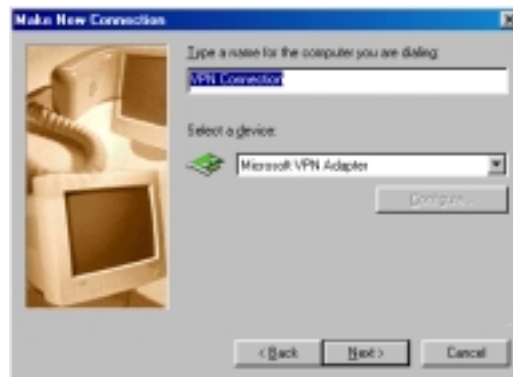


Figure 69. Make New Connection-1

step10. Type a descriptive name for the connection. Choose *Microsoft VPN Adapter* from the *Select a device* dropdown list. Click *Next*

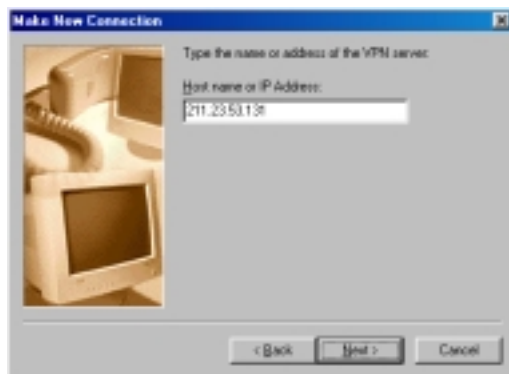


Figure 70. Make New Connection-2

- step11.** Enter the Internet IP Address of the VPN server you want to connect to and click *Next*



Figure 71. Make New Connection-3

- step12.** Click *Finish* to complete the settings. The system may ask you to install *Microsoft Dial-Up adapter*. Click *OK* to continue
- step13.** Windows may ask for the Windows CD-ROM. Insert your Windows CD and click *OK*
- step14.** In the *Dial-Up Networking* folder (**Figure 72**), you should have a new VPN connection

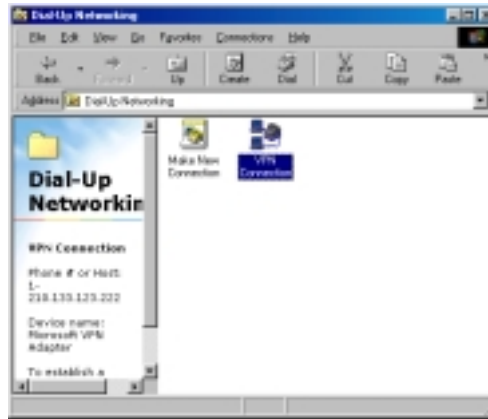


Figure 72. Dial-Up Networking

- step15.** Double-click the newly-created icon. The *Connect To* dialog box will open (**Figure 73**)

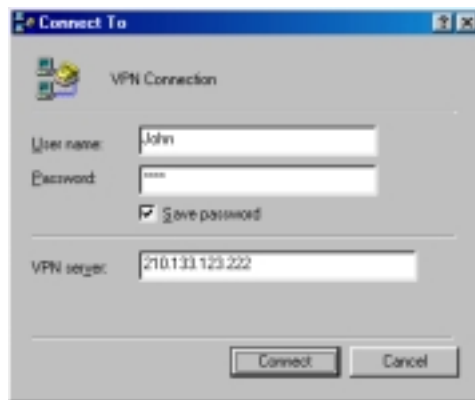


Figure 73. Connect To

- step16.** Enter your *User name*, *Password*, and the Internet IP address of the *VPN server*. Click **Connect**

Note: Connecting to the VPN server may take several attempts before a connection is established.

- step17.** The *Connection Established* dialog box will open (**Figure 74**)

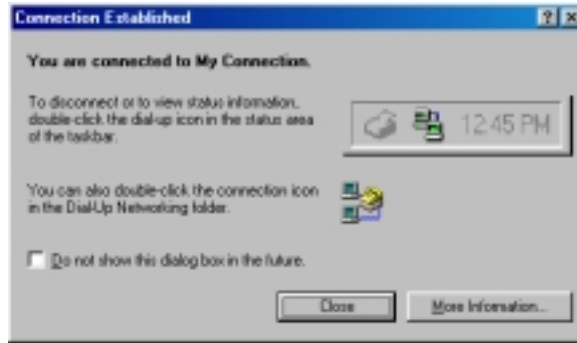


Figure 74. Connection Established

Windows 2000 VPN Server Setup

Note: You must have two Network Interface Cards installed in your Windows 2000 server.

- step1.** Click *Start/Programs/Administrative Tools/Routing and Remote Access*

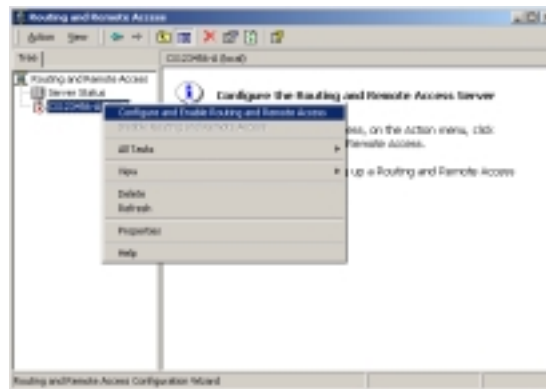


Figure 75. Routing and Remote Access

- step2.** In the *Routing and Remote Access* box (**Figure 75**), right-click the server name and choose ***Configure and Enable Routing and Remote Access***. The *Routing and Remote Access Server Setup Wizard* welcome screen will open. Click *Next* and the *Common Configurations* dialog box will open (**Figure 76**)

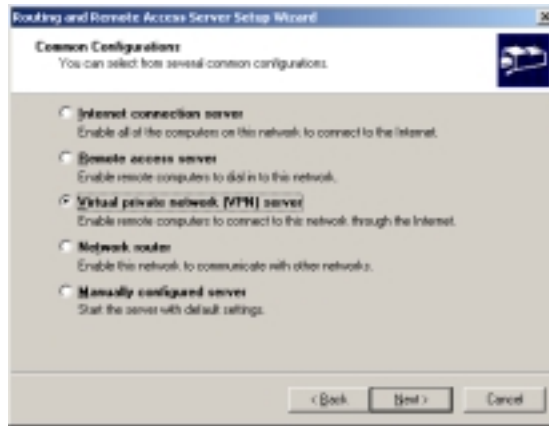


Figure 76. Common Configurations

- step3.** Check *Virtual private network (VPN) server* and click *Next*. The *Remote Client Protocols* dialog box will open (**Figure 77**)

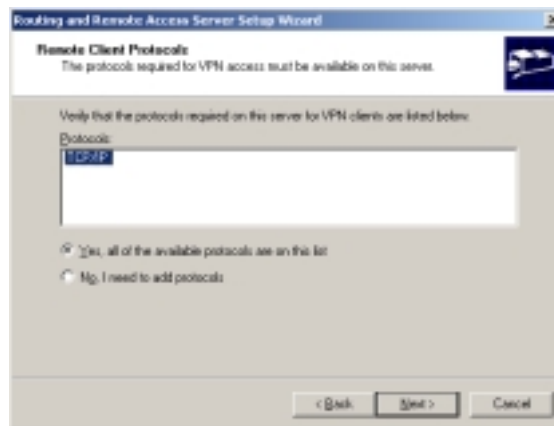


Figure 77. Remote Client Protocols

- step4.** Make sure TCP/IP is in the *Protocols* list, then check *Yes, all of the available protocols are on this list*. Click *Next* and the *Internet Connection* dialog box will open (**Figure 78**)

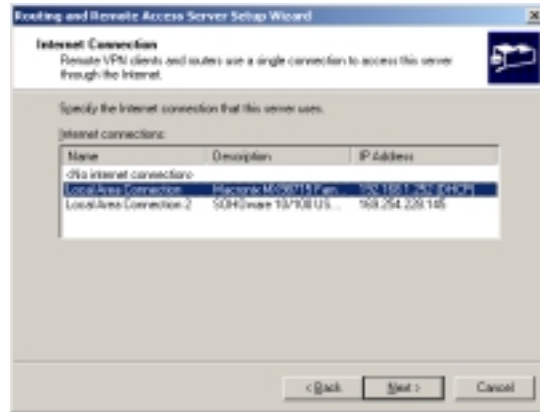


Figure 78. Internet Connection

- step5.** Highlight the *Local Area Connection* with the IP address in the 192.168.1.2 ~192.168.1.254 range. Click *Next*. The *IP Address Assignment* box will open (**Figure 79**)

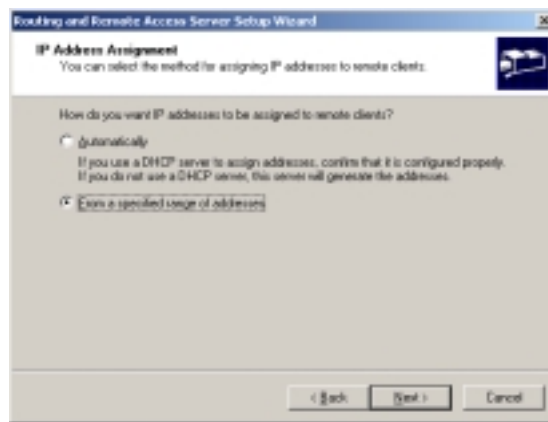


Figure 79. IP Address Assignment

- step6.** Check *From a specified range of addresses*. Click *Next*. The *Address Range Assignment* box will open (**Figure 80**)

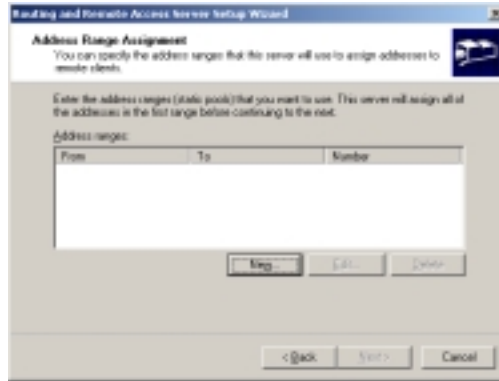


Figure 80. Address Range Assignment

step7. Click *Next*. The *New Address Range* box will open (**Figure 81**)

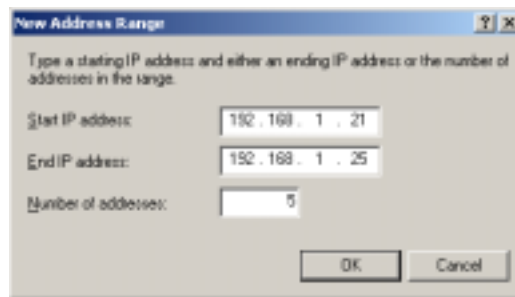


Figure 81. New Address Range

step8. In the *Start IP address* field, enter a start IP address in the range 192.168.1.2 ~ 192.168.1.254. Enter an end IP address in the same range. In the example in Figure 81, we allow five remote users to access the VPN server. We recommend the number of addresses is five or less to prevent influencing the throughput of the BroadGuard. Click **OK** to save the settings. You will be returned to the *Address Range Assignment* box (**Figure 82**)

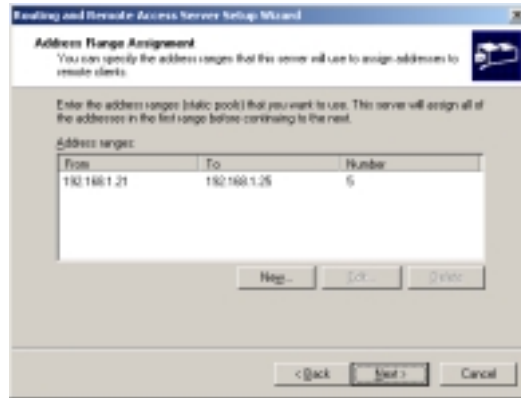


Figure 82. Address Range Assignment

- step9.** Click *Next*. The *Managing Multiple Remote Access Servers* dialog box will open (Figure 83)

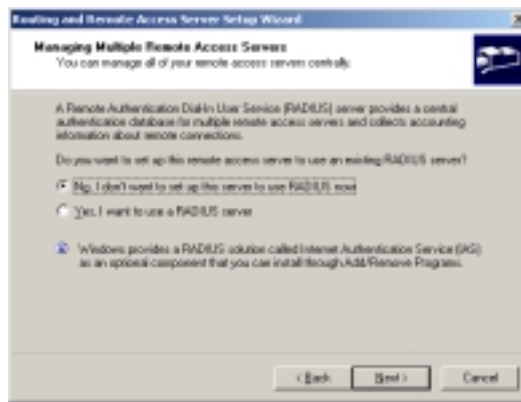


Figure 83. Managing Multiple Remote Access Servers

- step10.** Check *No, I don't want...* then click *Next*
- step11.** Click **Finish**. A *Routing and Remote Access* warning screen will open (Figure 84)



Figure 84. Routing and Remote Access

step12. Click **OK** to return to the *Routing and Remote Access* main screen (**Figure 85**)

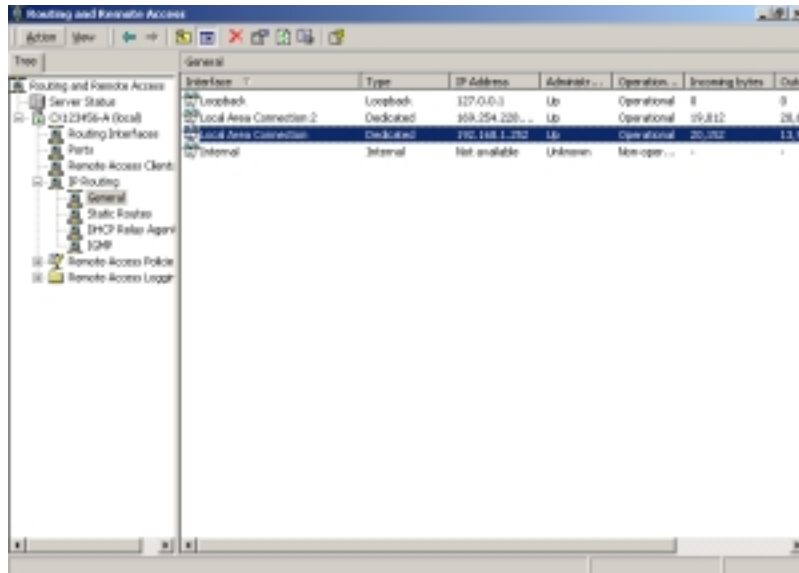


Figure 85. Routing and Remote Access

step13. In the left pane, double-click the server and double-click *IP Routing*. In the right, double-click the *Local Area Connection* with the IP address in the 192.168.1.2 ~192.168.1.254 range. The *Local Area connection Properties* box will open (**Figure 86**)

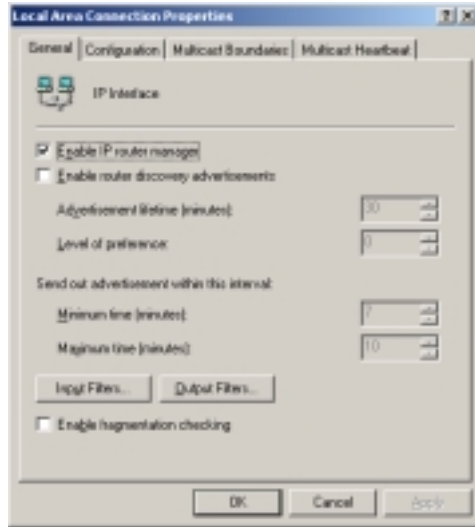


Figure 86. Local Area connection Properties

- step14.** On the *General* card, check *Enable IP Router Manager*. Click *Input Filters*. Remove all filters from the list, then click **OK**. Click *Output Filters*. Once again, remove all filters from the list, then click **OK**. Click **OK** to close the window and return to the *Routing and Remote Access* window. Click **OK** to save and close the *Routing and Remote Access* window.
- These changes make it possible to run any Internet application through this server

That completes the VPN server setup. The next stage is to set permissions for the users access the server

Set User Permissions

- step1.** Click *Start/Settings/Control Panel*. In *Control Panel*, double-click the *Administrative Tools* icon. The *Administrative Tools* window will open (**Figure 87**)

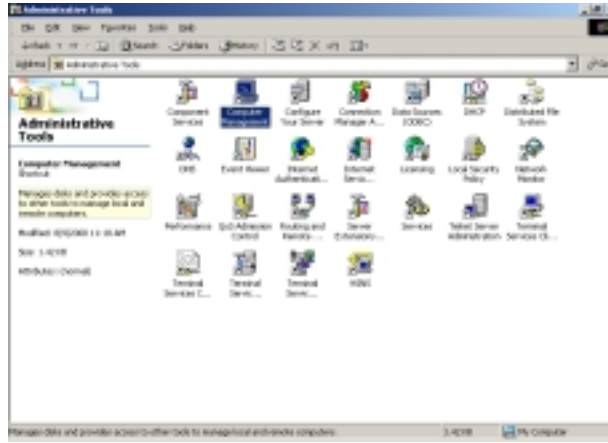


Figure 87. Administrative Tools

step2. Double-click *Computer Management*. Expand *System Tools/Local Users and Groups*. Click *Users* to show all users lists in *Computer Management* (Figure 88)

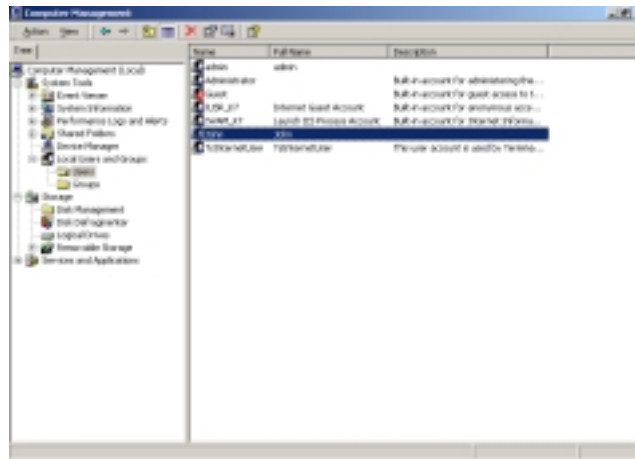


Figure 88. Computer Management

step3. Double-click the name of the user you want to set permissions for. The *Properties* box will open (Figure 89)

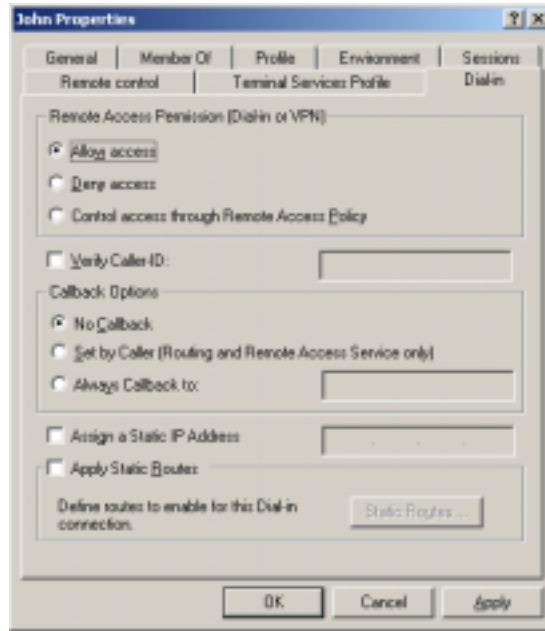


Figure 89. User Properties

- step4.** On the *Dial-in* card, check either *Allow access* or *Control access through Remote Access Policy* (which one you use depends on your security policy). Click **OK** to save and complete the setting. An icon will appear in the *Network and Dial-Up Connections* folder (**Figure 90**)

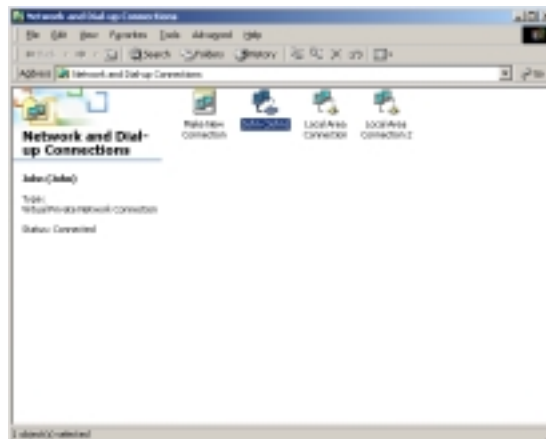


Figure 90. Network and Dial-Up Connections

step5. When there is a live connection from a remote user, the icon will show activity (**Figure 90**)

Note: Connections to the VPN server may take several attempts before a connection is established.

Appendix B: GLOSSARY

Ethernet

One of the most common Local Area Network (LAN) protocols. Ethernet uses a bus topology that supports a data transfer rate of 10Mbps.

Fast Ethernet

Much the same as Ethernet but 10 times faster; requires upgraded network cards and hubs.

Protocol

A protocol is a set of rules for communicating between computers.

10Base-T

A variant of Ethernet that allows computers to be networked at 10Mbps via twisted pair cable.

100Base-TX

A variant of Ethernet that allows computers to be networked at 100Mbps via twisted pair cable.

Browser

A software application used to locate and display Web pages, such as Netscape Navigator and Microsoft Internet Explorer.

DHCP (Dynamic Host Configuration Protocol)

DHCP is a protocol that assigns temporary IP addresses to PCs. Without DHCP the IP address must be entered manually at each computer.

Domain Name

The Domain Name identifies one or more IP addresses. For example, the domain name of sohware.com represents about a dozen IP addresses.

URL (Uniform Resource Locator)

A Uniform Resource Locator is a standard for specifying the location of an object on the Internet, such as a file or a newsgroup. URLs are used extensively on the World Wide Web. They are used in HTML documents to specify the target of a hyperlink, which is often another HTML document (possibly stored on another computer).

DNS (Domain Name Server)

A server used to translate a Domain Name to a numerical form IP address.

PPPoE

PPPoE supports reliable and straightforward end-user authentication with no security risk and can provide a range of operational benefits to both the subscriber as well as the service provider. Among these are network management and diagnostic capabilities that can identify operational problems and automatically offer resolutions.

Firewall

A security system used to enforce an access control policy between a LAN and the Internet.

Gateway

A device that links two different networks.

Internet

A global network that connects millions of computers for information exchange.

IP Address

The Internet Protocol (IP) is a set of basic rules for network communication. Each computer on the Internet has a unique IP address (e.g. 192.168.1.2) and its IP functions as an I.D. number/identifier/address.

BSP (Broadband Service Provider)

A BSP is a company that provides individuals or companies broadband access to the Internet and other related Internet services via cable or DSL.

Local Area Network (LAN)

A LAN is a network of interconnected workstations, sharing the resources of a single server or each other, within a relatively small geographic area.

LAN Adapter

A device that connects the computer to the network cable.

MAC Address

Short for Media Access Control Address, a hardware address that uniquely identifies each node on a network.

NAT (Network Address Translation)

A routing protocol that allows global IP addresses to be translated into multiple private IP addresses for use on internal LAN networks. The explosion in the use of the Internet has created a critical problem for the Internet Assigned Numbers Authority (IANA) which is charged with assigning IP addresses to Internet users, ISPs, etc. NAT is a technology that has been introduced to help maximize the utilization of assigned IANA or global IP addresses.

TCP/IP

TCP/IP protocols are used for Internet communications and consist of:

- TCP (Transmission Control Protocol), which uses a set of rules to exchange messages with other Internet points
- IP (Internet Protocol), which uses a set of rules to identify Internet addresses on the Internet. Every computer on the Internet has a unique IP address. The IP protocol helps Internet users to identify each sender or receiver of information that is sent across the Internet

VPN

Virtual Private Network: The use of encryption in the lower protocol layers to provide a secure connection through an otherwise insecure network, typically the Internet.

BBS (Bulletin Board Service)

A computer and associated software that typically provides an electronic message database where people can log in and leave messages. Apart from public message areas, a BBS may provide archives of files, personal electronic mail, and any other services or activities of interest to the bulletin board's system operator (the "sysop").

News Forum

An electronic meeting place where people can exchange news or discuss common interests.

Hacker

A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary. Recently misused to describe a Cracker. See the next item.

Cracker

An individual who attempts to gain unauthorized access to a computer system. These individuals are often malicious. Contrary to widespread myth, cracking does not usually involve some mysterious leap of hackerly brilliance, but rather persistence and the dogged repetition of a handful of fairly well-known tricks that exploit common weaknesses in the security of target systems.

Firmware

Software stored in read-only memory (ROM) or programmable ROM (PROM). Easier to change than hardware, but harder than software stored on disk. Firmware is often responsible for the behavior of a system when it is first switched on.

Technical Specifications

Standards Compliance	IEEE 802.3 10Base-T & 100Base-TX
Certifications	FCC Class B, VCCI, CE
Standards Compliance	Compression TCP/IP (RFC 1144), DHCP (1533,1541), DNS (1034,1035)
Network Interfaces	LAN: Four 10/100 Base-TX Switched Ethernet RJ-45 connectors Autosensing Switch (LAN ports Four RJ-45 10Base-T/100Base-TX Ethernet ports (for PCs, peripherals or a wireless LAN bridge) WAN: One 10Base-T Ethernet RJ-45 connector for cable/DSL modem
User Interface	Browser -based Management
Maximum Number of PCs	253
Firewall Security	NAT, DMZ, SPI, Prevention of DoS attacks
VPN Support	Client and server pass through (Microsoft PPTP)
Protocols	WAN: TCP/IP, DHCP client, IP Multicast, RTSP, PPTP, and PPPoE LAN: TCP/IP, DHCP server, NAT, RIP I & II
LED Indicators	Power Status Internet activity (WAN) Ethernet port activity (LAN)
Operating Environment	Operating Temperature: 0-50 deg C (32-122 deg F) Humidity 0 to 90%, (non-condensing)
Dimensions	258 x 168 x 45mm (10.2 x 6.6 x 1.8 in.)
Weight	770 gm (27.2 oz.)
Power Consumption	AC 5V/1A
Warranty	BroadGuard Unit: 3-year Limited Power Adapter: One year

Technical Support

Support from Your Network Supplier

If additional assistance is required, call your supplier for help. Have the following information ready before you make the call.

1. LED status
2. A list of the product hardware (including revision levels), and if possible, a brief description of the network structure
3. Details of recent configuration changes, if applicable

Support from SOHOware

If you have any problems that you cannot resolve with the information in troubleshooting, please note the following information and contact our technical support team.

- What you were doing when the error occurred
- What error messages you saw
- Whether the problem can be reproduced
- The serial number of your SOHOware product

USA & Europe

Telephone	:	+1-408-565-9888
Technical Support	:	+1 (888) 785-8222
Toll Free Customer Service (US only)	:	+1 (800) 632-1118 ext: 2801
FAX	:	+1-408-565-9889
E-mail	:	support@sohoware.com

Asia Pacific

Telephone	:	+886-3-5783966
FAX	:	+886-3-5777989
E-mail	:	techsupt@ndc.com.tw

For more information on networking, please visit us at:

<http://www.sohoware.com>

72 SOHOware® Secure Cable/DSL Router

SOHOware Limited Warranty

Hardware

SOHOware, Inc. warrants its products to be free of defects in workmanship and materials, under normal use and service, from the date of purchase from SOHOware or its Authorized Reseller and for the period of time specified in the documentation supplied with each product.

Should a product fail to be in good working order during the applicable warranty period, SOHOware will, at its option and expense, repair or replace it, or deliver to the purchaser an equivalent product or part at no additional charge except as set forth below. Repair parts and replacement products are furnished on an exchange basis and will be either reconditioned or new. All replaced products and parts will become the property of SOHOware. Any replaced or repaired product or part has a ninety (90) day warranty or the remainder of the initial warranty period, whichever is longer.

SOHOware shall not be liable under this warranty if its testing and examination disclose that the alleged defect in the product does not exist or was caused by the purchaser's, or any third party's misuse, neglect, improper installation or testing, unauthorized attempt to repair or modify, or any other cause beyond the range of the intended use, or by accident, fire, lightning, or other hazard.

Software

Software and documentation materials are supplied "as is" without warranty as to their performance, merchantability, or fitness for any particular purpose. However, the diskette media containing the software are covered by a 90-day warranty that protects the purchaser against failure within that period.

Limited Warranty Service Procedures

Any product (1) received in error, (2) in a defective or non-functioning condition, or (3) exhibiting a defect under normal working conditions, can be returned to SOHOware by following these steps:

You must prepare:

- dated proof of purchase
- product model number & quantity
- product serial number
- precise reason for return
- your name/address/e-mail address/telephone/fax

1. Inform the distributor or retailer
2. Ship the product back to the distributor/retailer with prepaid freight. The purchaser must pay the shipping freight from the distributor/retailer to SOHOfware. Any package sent C.O.D. (Cash On Delivery) will be refused
3. Charges: Usually RMA (Returned Material Authorization) items will be returned to the purchaser via Airmail, prepaid by SOHOfware. If returned by another carrier, the purchaser will pay the difference. A return freight and handling fee will be charged to the purchaser if SOHOfware determines that there was "No Problem Found" or that the damage was caused by the user

Warning

SOHOfware is not responsible for the integrity of any data on storage equipment (hard drives, tape drives, floppy diskettes, etc.). We strongly recommend that our customers backup their data before sending such equipment in for diagnosis or repair.

Services after Warranty Period

After the warranty period expires, all products can be repaired for a reasonable service charge. The shipping charges to and from the SOHOfware facility will be borne by the purchaser.

Return for Credit

In the case of a DOA (Dead on Arrival) or a shipping error, a return for credit will automatically be applied to the purchaser's account, unless otherwise requested.

Limitation of Liability

All expressed and implied warranties of a product's merchantability, or of its fitness for a particular purpose, are limited in duration to the applicable period as set forth in this limited warranty, and no warranty will be considered valid after its expiration date.

If this product does not function as warranted, your sole remedy shall be repair or replacement as provided for above. In no case shall SOHOfware be liable for any incidental, consequential, special, or indirect damages resulting from loss of data, loss of profits, or loss of use, even if SOHOfware or an authorized SOHOfware distributor/dealer has been advised of the possibility of such damages, or for any claim by any other party.

EC DECLARATION OF CONFORMITY

For the following equipment:

Product Name : BroadGuard™ - Secure Cable/DSL Router
Model Number : NBG800

Produced by:

Manufacturer's Name : NATIONAL DATACOMM CORPORATION
Manufacturer's Address : 4F, NO. 24-2, INDUSTRY EAST 4TH ROAD
SCIENCE PARK, HSIN-CHU
TAIWAN, R.O.C.

is hereby confirmed to comply with the requirements set out in the Council Directive on the Approximation of the Laws of the Member States relating to Electromagnetic Compatibility (89/ 336/ EEC).

The product meets or exceeds the following EMC standards:

EMI	EN50081-1:1992	EN55022(B)
EMS	EN50082-1:1997	

The manufacturer/importer is responsible for this declaration:

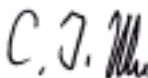
Company Name : SOHware Europe
Company Address : 1, EARLSFORT CENTRE,
HATCH STREET,
DUBLIN 2, IRELAND.

Person authorized to make this declaration:

Name : CHIN-TU WU
Position/Title : MANAGING DIRECTOR

15 January 2001

Date



Legal Signature

SOHware® Secure Cable/DSL Router 75

Free Manuals Download Website

<http://myh66.com>

<http://usermanuals.us>

<http://www.somanuals.com>

<http://www.4manuals.cc>

<http://www.manual-lib.com>

<http://www.404manual.com>

<http://www.luxmanual.com>

<http://aubethermostatmanual.com>

Golf course search by state

<http://golfingnear.com>

Email search by domain

<http://emailbydomain.com>

Auto manuals search

<http://auto.somanuals.com>

TV manuals search

<http://tv.somanuals.com>