SOHOware®

BroadGuard™

Secure Cable/DSL Router

User's Guide

Model No. NBG800

Rev: A2

May 2001

SOHOware Inc.
Tel: +1 (408) 565-9888
Fax: +1 (408) 565-9889

SOHOware Europe
Tel: +44 1489 611-788
Fax: +44 1489 611-787

SOHOware Website
www.sohoware.com

Technical Support

E-mail: support@sohoware.com
Toll-Free Technical Support (US only): (800) 632-1118 ext: 2828
Technical Support Call Center (24hrs): +1 (888) 785-8222
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 Quick Guide
- One CD-ROM with manual in PDF format
- 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 years on the BroadGuard device, 1 year on the power adapter)
  - Information on upcoming product releases and special product offers
  - Free technical support and firmware upgrades

Table of Contents

List of Figures

Chapter 1: Introduction

The SOHOware 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.

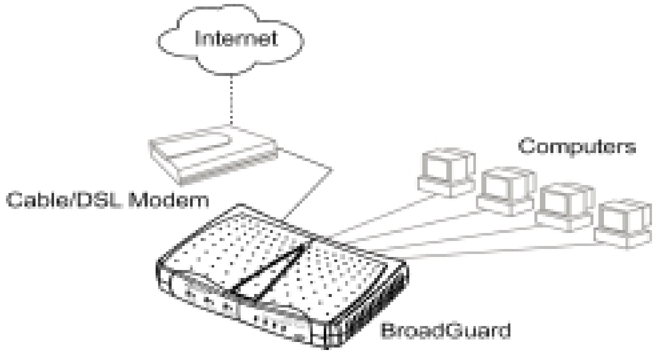


Figure 1. BroadGuard Connections

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 and outgoing data packets and filter requests from local computers. 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 algorithm (Denial of Service & Stateful Packet Inspection) protect your PCs from hacker attacks.

- **Multi-DMZ** – This feature places multiple PCs on your network outside the protection of the firewall and allows them to respond to requests from the Internet, e.g. for multiple simultaneous connections to a PPTP server.
- **Port Forwarding** – Provides enhanced security. The firewall accepts IP packets addressed to a specific port number. Port Forwarding then re-writes the header information on the packets and forwards them to the internal server providing the actual service. The reply packets from the internal server are re-written to make it appear that they came from the firewall.
- **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 SOHOware 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**).

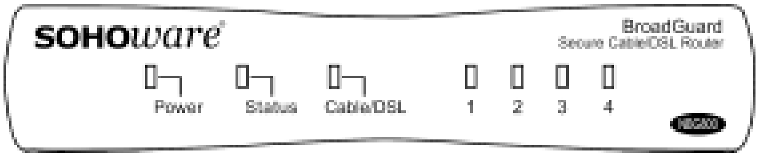


Figure 2. Front Panel

LED Indicators

LED	Color	Function
Power	Green	Lit: Power ON Unlit: Power OFF
Status	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 47
Cable/DSL	Orange	Lit: Indicates a good connection to a cable/DSL modem Blinking: Data is being transmitted/received to/from a cable/DSL modem
LAN Ports 1~4	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**)

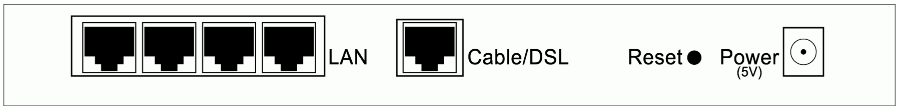


Figure 3. Rear Panel

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.

Chapter 2: Installation

What You Need

Before installing the SOHOware 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 BSP 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 cable service (formerly MediaOne), 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 should 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 BSP

- The assigned Gateway IP address
- Domain Name Server's IP address
- Subnet Mask

Hardware Installation

All the connection ports are on the rear panel of the BroadGuard. Two cables are supplied. Most Cable and DSL modems use straight-through Ethernet cable so first use the WHITE cable unless you know you need a crossover cable (the Green cable).
Follow the steps below to complete the hardware installation.

step1. Connect one end of the cable to the port marked *Cable/DSL* on the BroadGuard.

step2. Connect the other end of the cable to the Ethernet or Output port of your cable or DSL Modem.

step3. Turn ON both the modem and BroadGuard. Observe the Link indicator on the modem and the indicator marked *Cable/DSL* on the front of the BroadGuard. If the indicators are lit, you have a good connection.
If the indicators are not lit, then your modem requires a crossover cable - this is the GREEN cable provided with the BroadGuard. Disconnect the white cable and replace it with the green cable.

step4. Use standard RJ-45 Ethernet cables (not provided) to connect your computers to the BroadGuard LAN ports.

step5. 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.

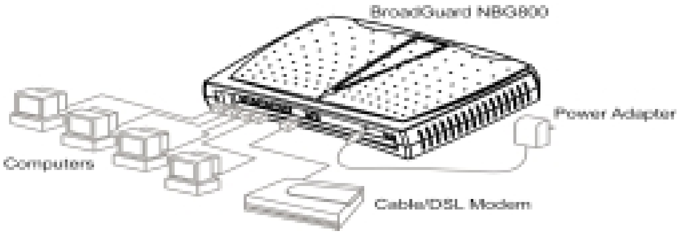


Figure 4. Connecting the BroadGuard

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

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 (see MAC Address Clone, *page 25).*

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 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

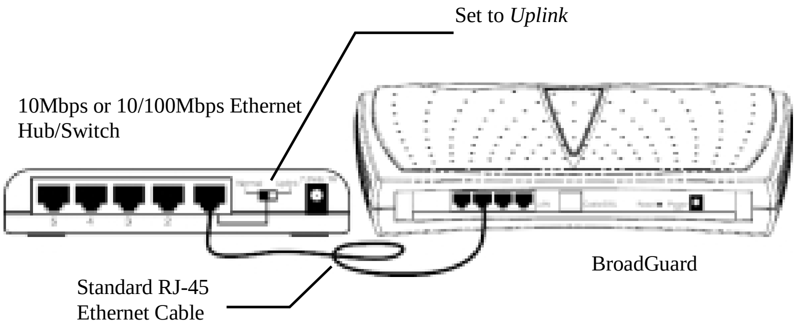

Set to *Uplink*
10Mbps or 10/100Mbps Ethernet Hub/Switch
BroadGuard
Standard RJ-45 Ethernet Cable

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).

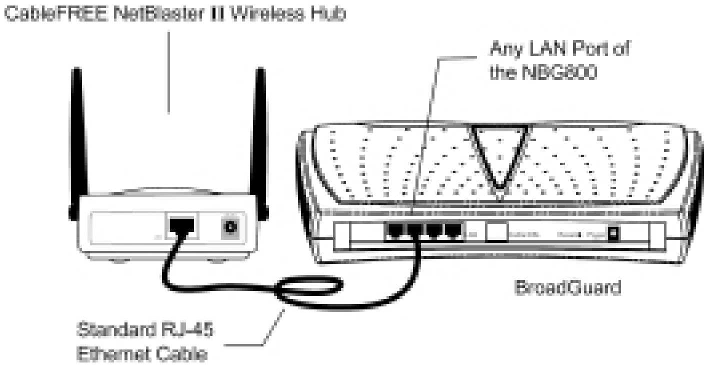

CableFREE NetBlaster II Wireless Hub
Any LAN Port of the NBG800
BroadGuard
Standard RJ-45 Ethernet Cable

Figure 6.   Wireless LAN Extension

TCP/IP Settings

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**)

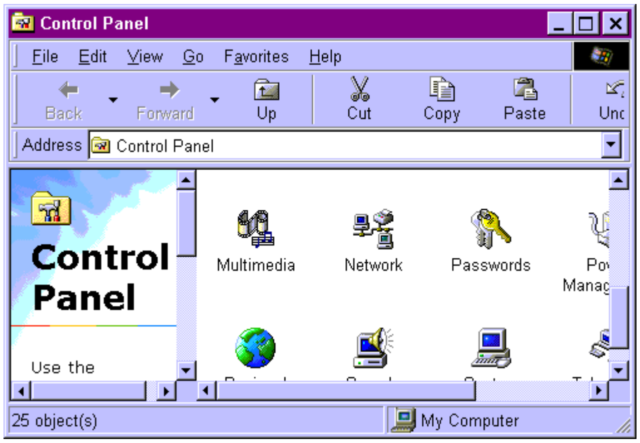
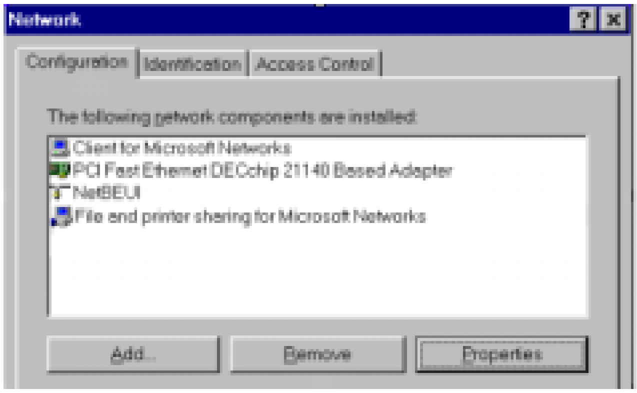


Figure 7. Control Panel

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

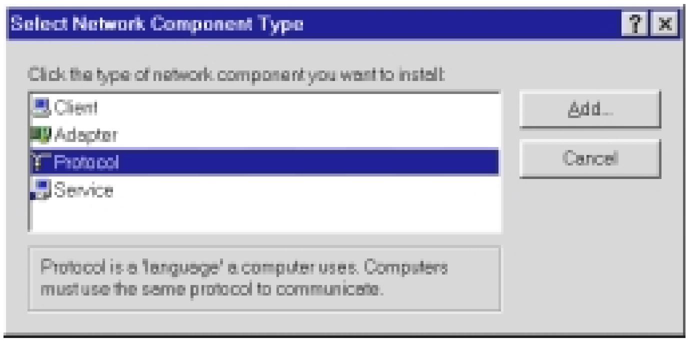


The following network components are installed:

Client for Microsoft Networks
PCI Fast Ethernet DECchip 21140 Based Adapter
NetBEUI
File and printer sharing for Microsoft Networks

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**)



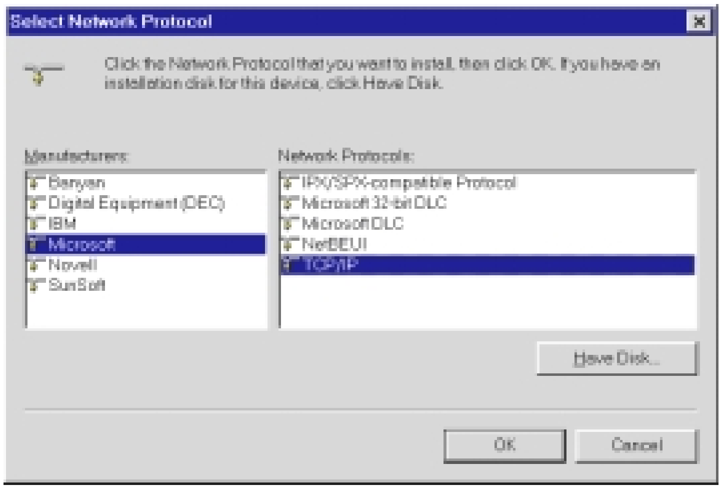
Select Network Component Type

Click the type of network component you want to install:

Protocol is a 'language' a computer uses. Computers must use the same protocol to communicate.

Figure 9. Select Network Component Type

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

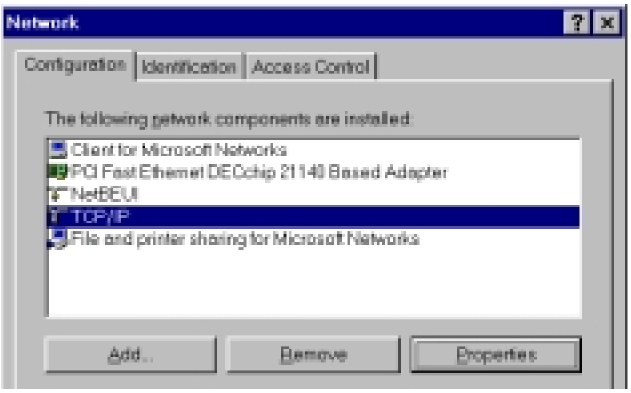


Select Network Protocol

Click the Network Protocol that you want to install, then click OK. If you have an installation disk for this device, click Have Disk.

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

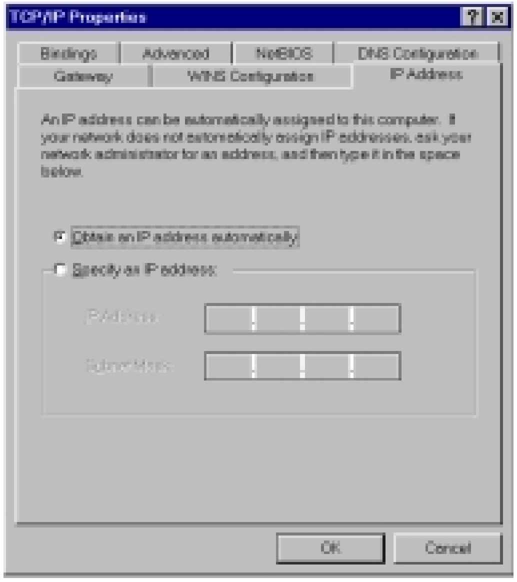


The following network components are installed:

- Client for Microsoft Networks
- PCI Fast Ethernet DECchip 21140 Based Adapter
- NetBEUI
- TCP/IP
- File and printer sharing for Microsoft Networks

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**)



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

● Obtain an IP address automatically

○ Specify an IP address:

IP Address: . . .

Subnet Mask: . . .

Figure 12. TCP/IP Properties-1

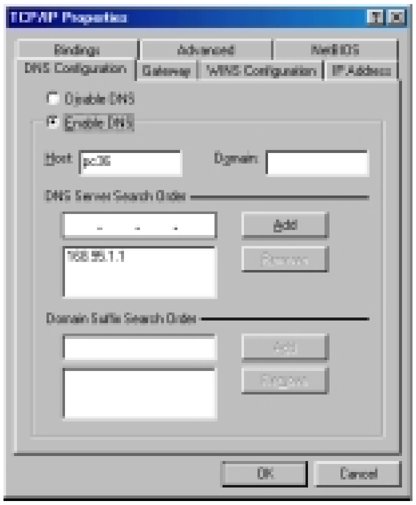
step7. On the *IP Address* page (**Figure 12**), check ***Obtain an IP address automatically***. Click ***OK*** and go to step 12. If you want to assign a static IP to a PC, go to step 8

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 will be running with Access Control enabled, assign an IP to the PC from the range *.2~.11*, i.e. *192.168.1.2 ~ 11*. The first three values must be the same as that of the BroadGuard IP address. The default BroadGuard IP is *192.168.1.1*.
If the PC is to be used as a DMZ/Port Forwarding PC, assign an address outside the *2~.11* range, i.e. *192.168.1.12 ~ 253*

step9. Enter the BroadGuard's subnet mask into the *Subnet Mask* field. The default value is *255.255.255.0*

step10. Click the *Gateway* tab and 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***



○ Disable DNS
● Enable DNS

Host: pc36 Domain:

DNS Server Search Order
168.95.1.1

Domain Suffix Search Order

Figure 13. TCP/IP Properties-2

step11. On the *DNS Configuration* page (**Figure 13**), check ***Enable DNS***. Enter your PC name into the *Host* field (see Finding your PC Host Name, page 26) 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

step12. 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***

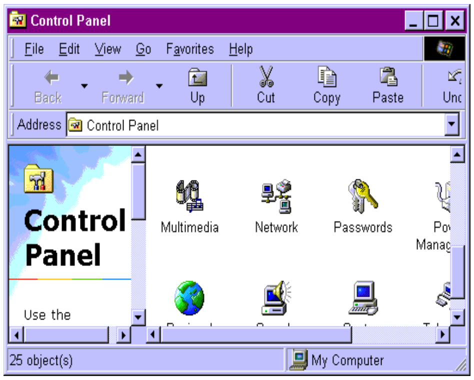
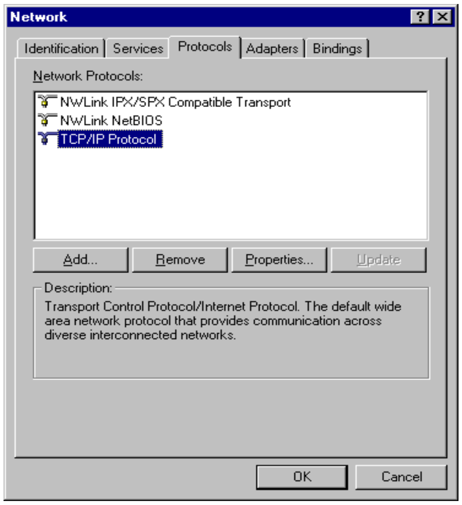


Figure 14. Control Panel

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


Network
Identification Services Protocols Adapters Bindings
Add... Remove Properties... Update
OK Cancel

Network Protocols:

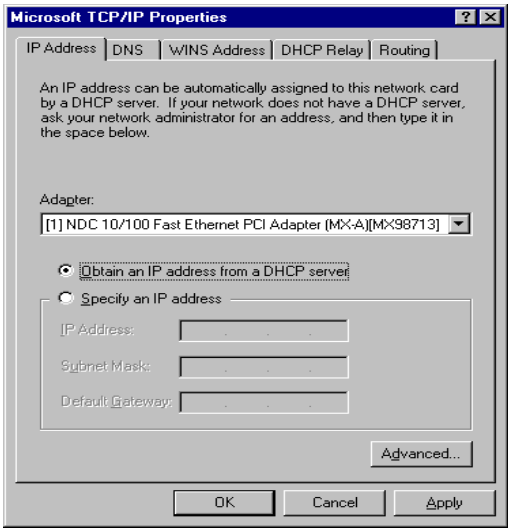
NWLink IPX/SPX Compatible Transport
NWLink NetBIOS
TCP/IP Protocol

Description:

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

Figure 15. Network

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



Microsoft TCP/IP Properties

An IP address can be automatically assigned to this network card by a DHCP server. If your network does not have a DHCP server, ask your network administrator for an address, and then type it in the space below.

Adapter: [1] NDC 10/100 Fast Ethernet PCI Adapter (MX-A)[MX98713]

● Obtain an IP address from a DHCP server

○ Specify an IP address

IP Address:

Subnet Mask:

Default Gateway:

Figure 16. Microsoft TCP/IP Properties-1

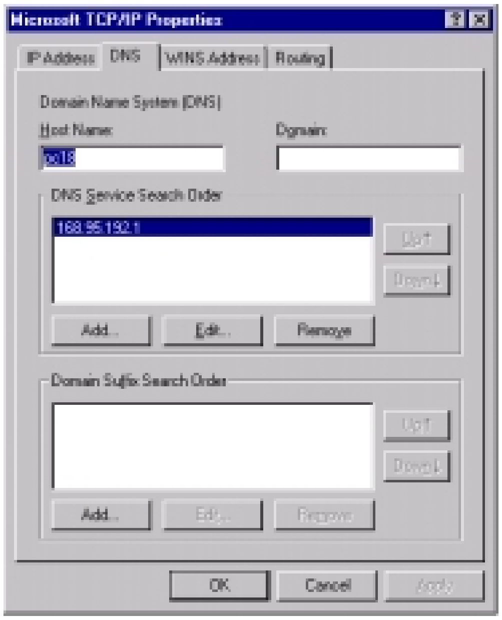
step4. On the *IP Address* page (**Figure 16**), check ***Obtain an IP address from a DHCP server***. Click ***OK*** and go to step 8. If you want to assign a static IP to a PC, go to step 5

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 will be running with Access Control enabled, assign an IP to the PC from the range *.2~.11*, i.e. *192.168.1.2 ~ 11*. The first three values must be the same as that of the BroadGuard IP address. The default BroadGuard IP is *192.168.1.1*.
If the PC is to be used as a DMZ/Port Forwarding PC, assign an address outside the *.2~.11* range, i.e. *192.168.1.12 ~ 253*

step6. Enter the BroadGuard's subnet mask into the *Subnet Mask* field. The default value is *255.255.255.0*. Enter the BroadGuard's IP address into the *Default Gateway* field (the default value is 192.168.1.1). Click ***OK***

step7. On the *DNS* page, enter your PC name into the *Host name* field (see Finding your PC Host Name, page 26) 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.



Host Name: pc18

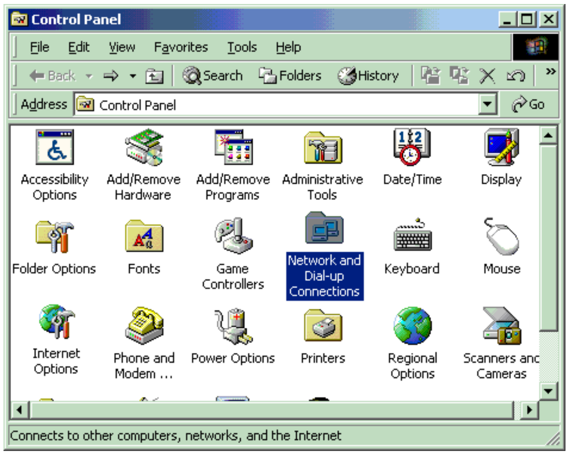
168.95.192.1

Figure 17. Microsoft TCP/IP Properties-2

step8. The system will ask you to restart the computer. Click ***Yes*** to complete the installation

Windows 2000

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

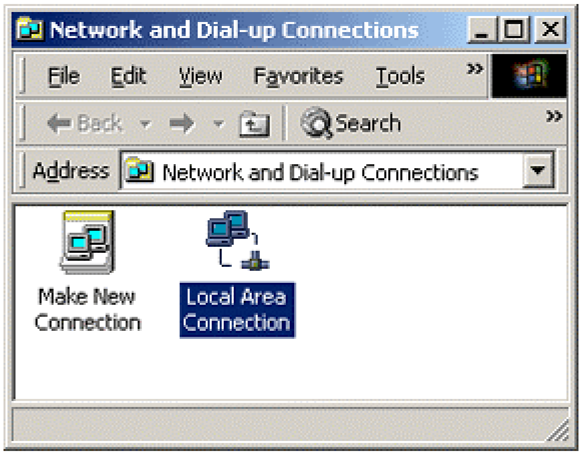


Address: Control Panel

Connects to other computers, networks, and the Internet

Figure 18. Control Panel

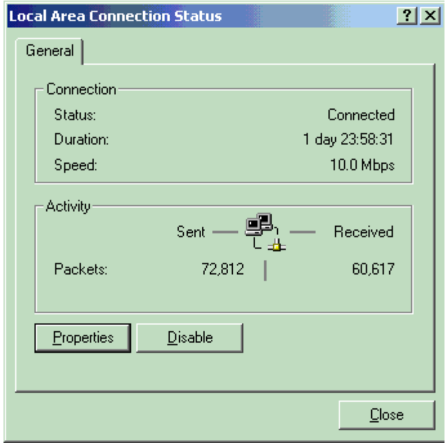
step2. Double-click the ***Network and Dial-up Connections*** icon (**Figure 18**). The *Network and Dial-up Connections* window will open (**Figure 19**)



Address: Network and Dial-up Connections

Figure 19. Network and Dial-up Connections

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



Connection

Status: Connected

Duration: 1 day 23:58:31

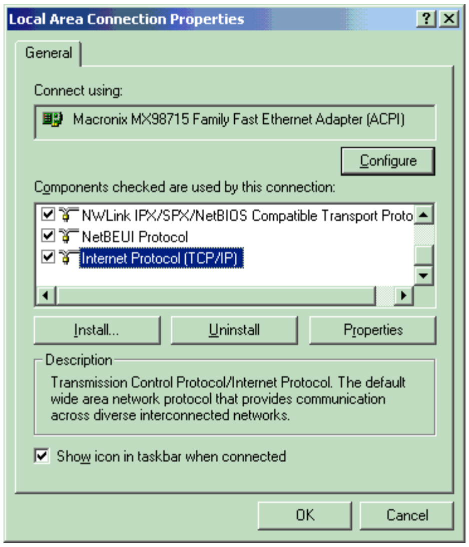
Speed: 10.0 Mbps

Activity

	Sent	Received
Packets:	72,812	60,617

Figure 20. Local Area Connection Status

step4. Click ***Properties***


Local Area Connection Properties

General

Connect using:

Macronix MX98715 Family Fast Ethernet Adapter (ACPI)

Configure

Components checked are used by this connection:

☑ NWLink IPX/SPX/NetBIOS Compatible Transport Proto
☑ NetBEUI Protocol
☑ Internet Protocol (TCP/IP)

Install... | Uninstall | Properties

Description

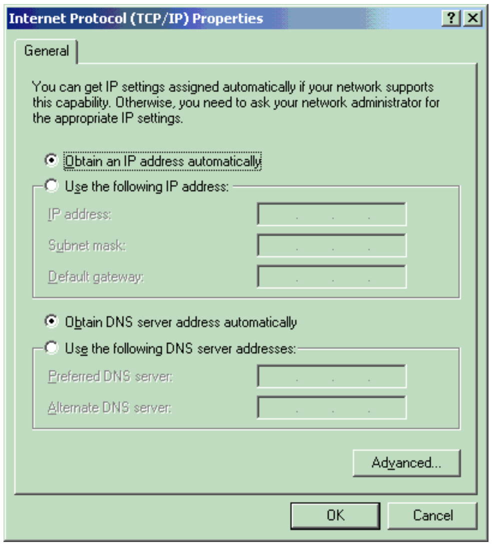
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in taskbar when connected

OK | Cancel

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**)


Internet Protocol (TCP/IP) Properties

General

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

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

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

Advanced...

OK | Cancel

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

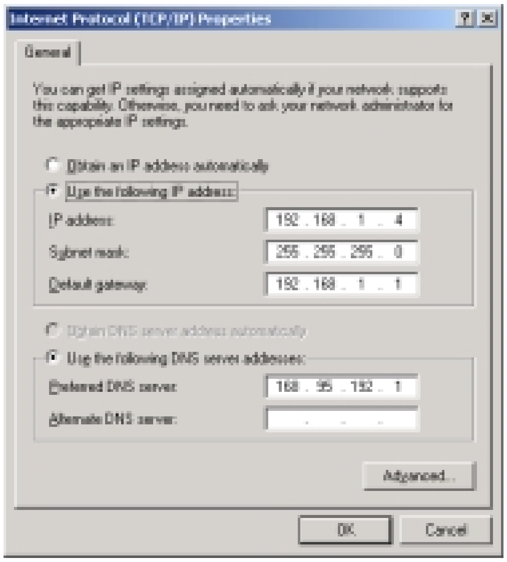
step6. Select *Obtain an IP address automatically* and *Obtain DNS server address automatically*. Click ***OK*** and go to step 10. If you want to assign a static IP to a PC, go to step 7

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 will be running with Access Control enabled, assign an IP to the PC from the range *.2~.11*, i.e. *192.168.1.2 ~ 11*. The first three values must be the same as that of the BroadGuard IP address. The default BroadGuard IP is *192.168.1.1*. If the PC is to be used as a DMZ/Port Forwarding PC, assign an address outside the *.2~ .11* range, i.e. *192.168.1.12 ~ 253*

step8. Enter the BroadGuard's subnet mask into the *Subnet Mask* field. The default value is *255.255.255.0*. Enter the BroadGuard's IP address into the *Default Gateway* field (the default value is 192.168.1.1). Click ***OK***

step9. 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



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

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 4

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 168 . 95 . 192 . 1

Alternate DNS server: . . .

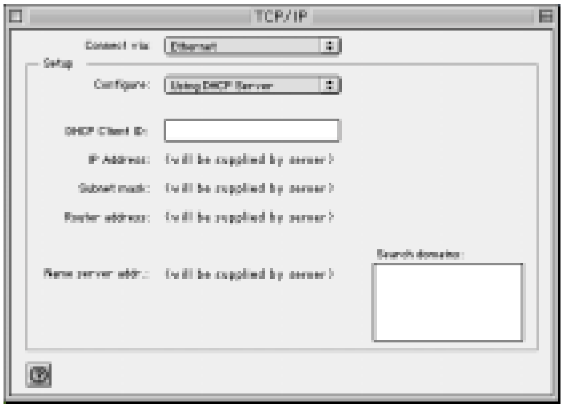
Figure 23. Internet Protocol (TCP/IP Properties-2

step10. 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**



Connect via: Ethernet

Configure: Using DHCP Server

DHCP Client ID:

IP Address: (will be supplied by server)

Subnet mask: (will be supplied by server)

Router address: (will be supplied by server)

Name server addr.: (will be supplied by server)

Search domains:

Figure 24. Using the DHCP Server

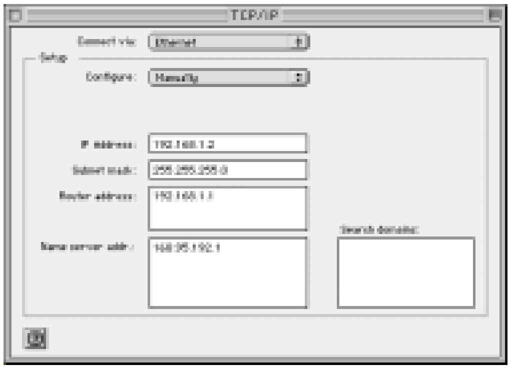
step2. From the *Connect Via* list box, choose ***Ethernet***

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**



TCP/IP

Connect via: Ethernet

Setup

Configure: Manually

IP Address: 192.168.1.2

Subnet mask: 255.255.255.0

Router address: 192.168.1.1

Name server addr.: 168.95.192.1

Search domains:

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: If the PC will be running with Access Control enabled, assign an IP to the PC from the range *.2~.11*, i.e. *192.168.1.2 ~ 11*. The first three values must be the same as that of the BroadGuard IP address. The default BroadGuard IP is *192.168.1.1*.
If the PC is to be used as a DMZ/Port Forwarding PC, assign an address outside the *.2~.11* range, i.e. *192.168.1.12 ~ 253*

step5. In the *Subnet mask* field, enter the BroadGuard's subnet mask. The default value is *255.255.255.0*

step6. In the *Router address* field, type the BroadGuard IP (the default value 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 the screen and save the configuration

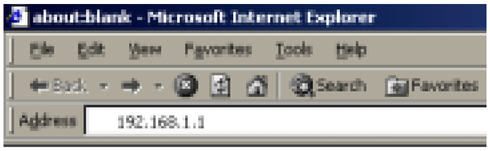
Chapter 3: Network Configuration

BroadGuard Configuration

Configuration is simple and easy via a standard web browser (Netscape Communicator 4.0/Microsoft Internet Explorer 3.0 or above).

Entering the BroadGuard Setup Home Page

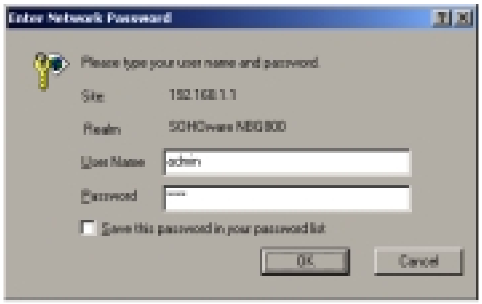
step1. Start the web browser and type 192.168.1.1 in the address field (**Figure 26**). Press *Enter*



Address 192.168.1.1

Figure 26. Entering the Setup Wizard

step2. The *Enter Network Password* window will open (**Figure 27**)



Please type your user name and password.

Site 192.168.1.1

Realm SOHOware NBG800

User Name admin

Password ****

□ Save this password in your password list

Figure 27. Enter Network Password

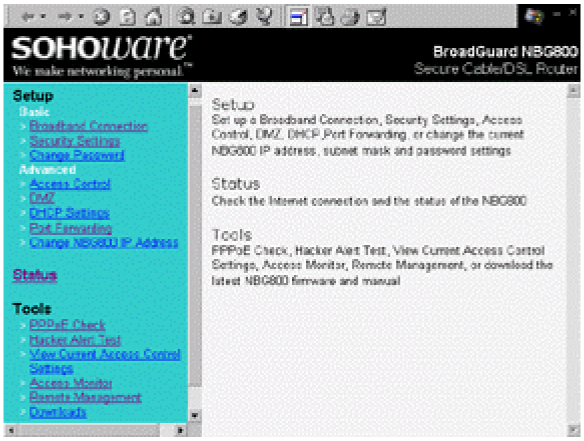
step3. Enter the factory default user name ***admin***

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



Setup

Set up a Broadband Connection, Security Settings, Access Control, DMZ, DHCP,Port Forwarding, or change the current NBG800 IP address, subnet mask and password settings

Status

Check the Internet connection and the status of the NBG800

Tools

PPPoE Check, Hacker Alert Test, View Current Access Control Settings, Access Monitor, Remote Management, or download the latest NBG800 firmware and manual

Figure 28. Setup Start Page

There are three sections on the home page:

Setup (Basic)

Broadband Connection	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.
Security Settings	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. If you disable firewall protection, *Hacker Attack E-mail Alerts* are also disabled.
Change Password	Changes the security password.

Setup (Advanced)

Access Control	The Access Control section allows you to control Internet use in your home/office.
DMZ	Use this function to expose multiple PCs to the Internet for playing interactive Internet games, video conferencing, as VPN servers/clients through the BroadGuard. To use the DMZ, you must set a static IP address for a DMZ PC and set that PC to use the selected IP address.
DHCP Setting	Enable/Disable the BroadGuard's DHCP server. Use to set the dynamic IP address range.
Port Forwarding	Forward packets sent to the BroadGuard from the external network to specified ports on the internal computers.
Change NBG800 IP Address	Change the BroadGuard's default IP address (192.168.1.1) and subnet mask (255.255.255.0).

Status

View WAN connection status and Internet Network settings
View LAN Network Settings
View Firewall Status

Tools

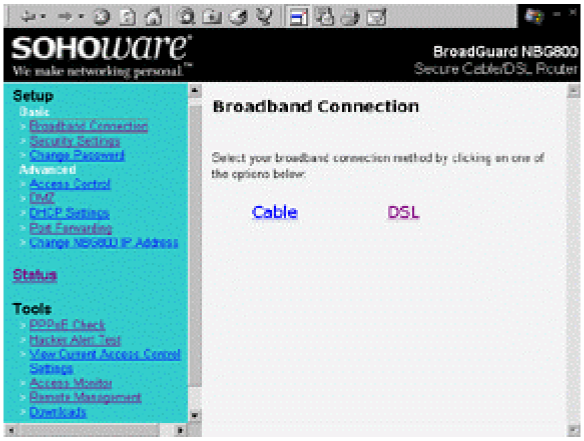
PPPoE Check	Checks PPPoE is functioning correctly.
Hacker Alert Test	Sends a test Hacker Alert E-mail.
View Current Access Control Settings	The PCs in the list have been denied access to the services shown.
Access Monitor	Shows the current Internet activities of monitored users.

Remote Management	Offers the capability to ping and configure your BroadGuard from a remote host.
Downloads	Download the latest BroadGuard firmware and manual.

Click the ***Broadband Connection*** link to begin setup of your broadband connection.

Basic

Broadband Connection



Broadband Connection

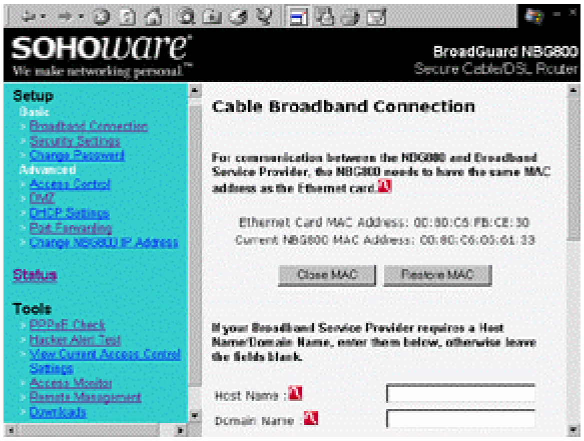
Select your broadband connection method by clicking on one of the options below:

Figure 29. 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 29**) 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



Cable Broadband Connection

For communication between the NBG800 and Broadband Service Provider, the NBG800 needs to have the same MAC address as the Ethernet card.

Ethernet Card MAC Address: 00:80:C6:FB:CE:30
Current NBG800 MAC Address: 00:80:C6:05:61:33

If your Broadband Service Provider requires a Host Name/Domain Name, enter them below, otherwise leave the fields blank.

Host Name :
Domain Name :

Figure 30. 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.

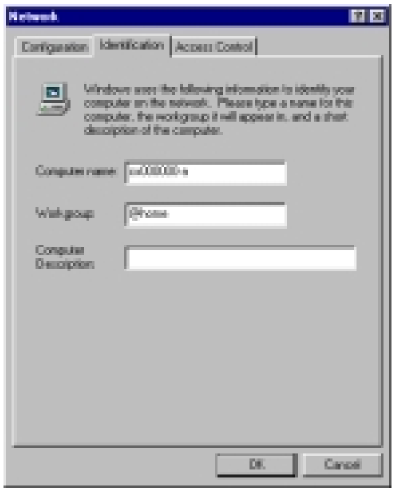
Note: After saving the settings and restarting the BroadGuard, you MUST turn your cable/DSL modem off and on.

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



Windows uses the following information to identify your computer on the network. Please type a name for this computer, the workgroup it will appear in, and a short description of the computer.

Computer name: cc000000-a

Workgroup: @home

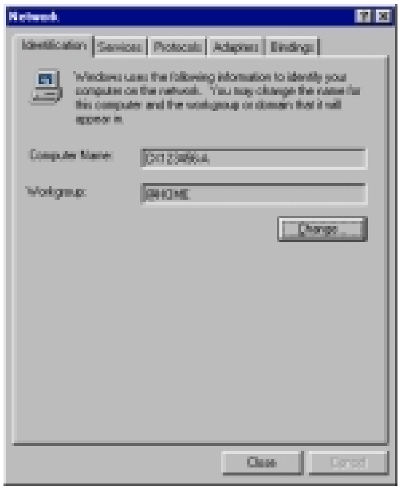
Computer Description:

Figure 31. Network-1

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



Windows uses the following information to identify your computer on the network. You may change the name for this computer and the workgroup or domain that it will appear in.

Computer Name: CX123456A

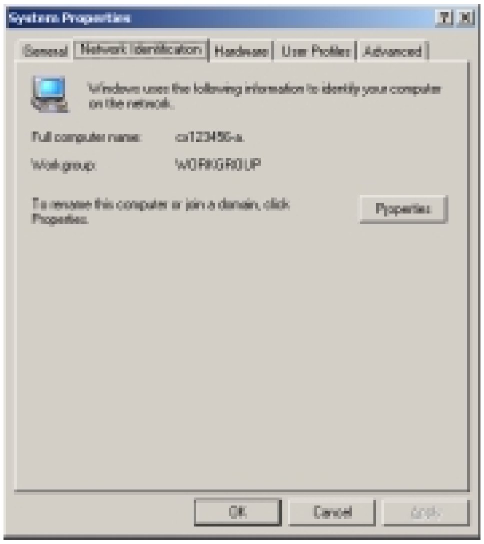
Workgroup: BHOME

Figure 32. Network-2

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



Windows uses the following information to identify your computer on the network.

Full computer name: cx123456-a.

Workgroup: WORKGROUP

To rename this computer or join a domain, click Properties.

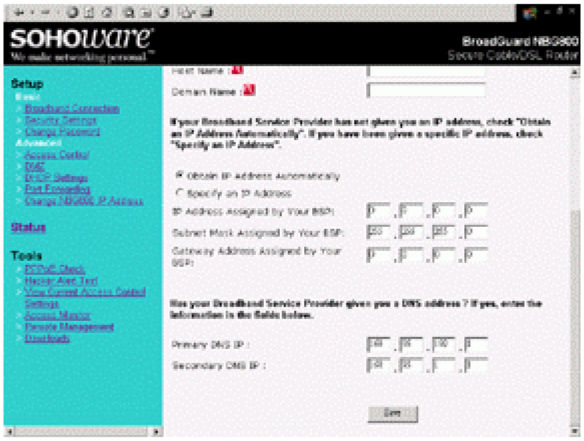
Figure 33. System Properties

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 that this field be filled 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.

Click ***Save*** and restart the BroadGuard. Go to the *Status* page to check whether your BroadGuard has received all necessary IP address information from your BSP. Restart the PC used to configure your BroadGuard.

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 34**). If not, you can skip this step.



Host Name :

Domain Name :

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 :

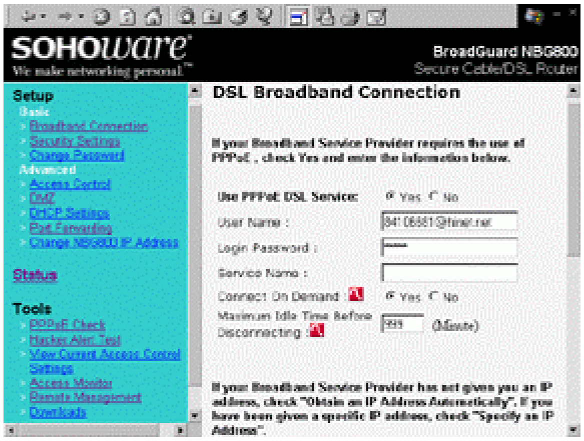
Figure 34. Cable Broadband Connection

If you do not wish to accept the NBG800 default IP address (192.168.1.1), go to the *Change NBG800 IP Address* page to change it.

Note: If you use an IP address other than the default (192.168.1.1), you will need to configure TCP/IP settings (see page 9) and related network settings.

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

DSL Setup



DSL Broadband Connection

If your Broadband Service Provider requires the use of PPPoE , check Yes and enter the information below.

Use PPPoE DSL Service: ● Yes ○ No

User Name : 84106881@timer.net

Login Password : *****

Service Name :

Connect On Demand : ● Yes ○ No

Maximum Idle Time Before Disconnecting : 999 (Minute)

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".

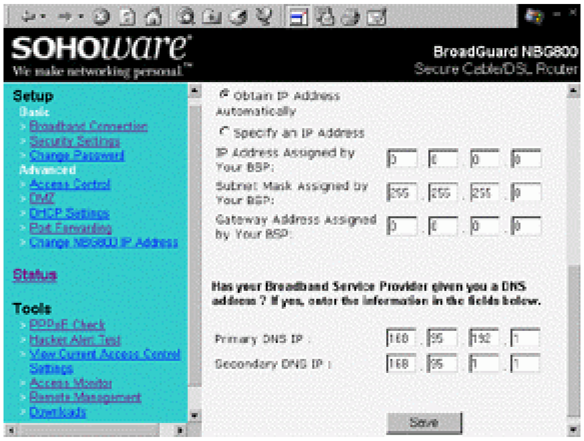
Figure 35. DSL Broadband Connection-1

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 within the time set here, the connection will 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.



● Obtain IP Address Automatically

○ Specify an IP Address

IP Address Assigned by Your BSP: 0 . 0 . 0 . 0

Subnet Mask Assigned by Your BSP: 255 . 255 . 255 . 0

Gateway Address Assigned by Your BSP: 0 . 0 . 0 . 0

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

Primary DNS IP : 168 . 95 . 192 . 1

Secondary DNS IP : 168 . 95 . 1 . 1

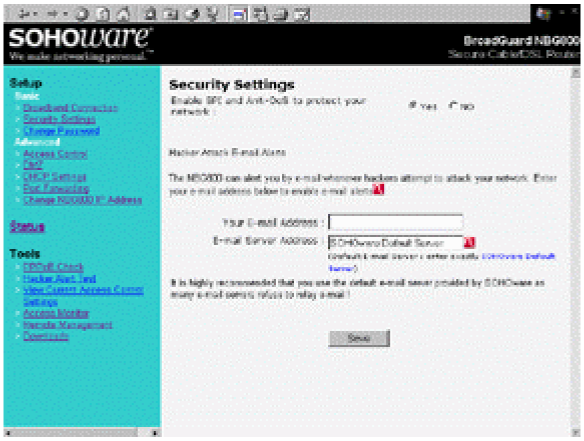
Figure 36. DSL Broadband Connection-2

If you do not wish to accept the NBG800 default IP address (192.168.1.1), go to the *Change NBG800 IP Address* page to change it.

Note: If you use an IP address other than the default (192.168.1.1), you will need to configure TCP/IP settings (see page 9) and related network settings.

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

Security Settings



Security Settings

Enable SPI and Anti-DoS to protect your network : ● Yes ○ No

Hacker Attack E-mail Alerts

The NBG800 can alert you by e-mail whenever hackers attempt to attack your network. Enter your e-mail address below to enable e-mail alerts.

Your E-mail Address :

E-mail Server Address : SOHOware Default Server

(Default E-mail Server : enter exactly SOHOware Default Server)

It is highly recommended that you use the default e-mail server provided by SOHOware as many e-mail servers refuse to relay e-mail !

Figure 37. Security Settings

Two anti-attack algorithm, anti-DoS (Denial of Service) and SPI (Stateful Packet Inspection), are built in to the BroadGuard so that it can protect client PCs from common hacker attacks (see page 55 for an explanation of these terms). With

BroadGuard, you have a professional firewall but without the need for specialized setup/configuration. BroadGuard gives your network protection from many kinds of hacker attacks. You can disable firewall protection by checking *No*. In most situations, we recommend you enable firewall protection.

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. in the log file 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 numbers 840, 546, and 544, they are the ports numbers that are being attacked.

Forward this e-mail to your BSP for analysis.

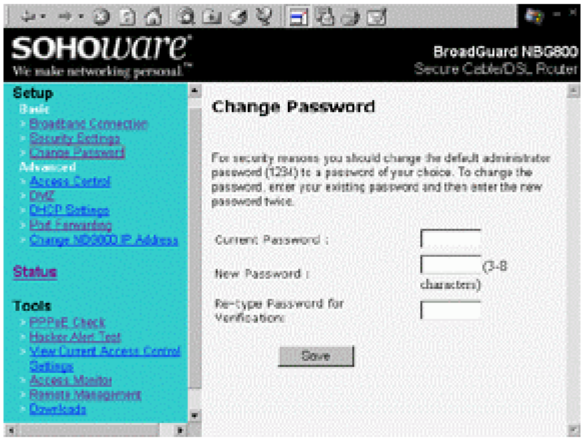
Note: The e-mail alert is sent at approximately the same time your computer is attacked.

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

It is highly recommended that you use the default e-mail server provided by SOHOware as many e-mail servers refuse to relay e-mail.

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

Change Password



Change Password

For security reasons you should change the default administrator password (1234) to a password of your choice. To change the password, enter your existing password and then enter the new password twice.

Current Password :

New Password : (3-8 characters)

Re-type Password for Verification:

Figure 38. 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

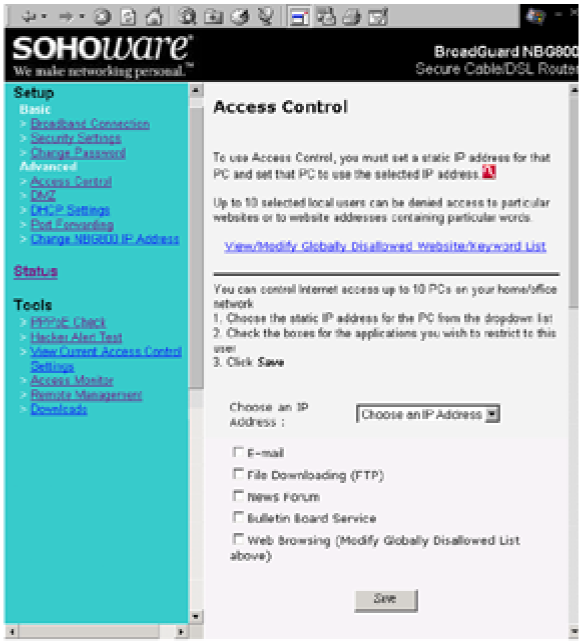
step2. The *Enter Network Password* dialog box will open

step3. Enter the username ***admin***, and key in the new password. Click ***OK*** and you will enter the BroadGuard Setup page again

Note: If you use an IP address other than the default (192.168.1.1), you will need to configure TCP/IP settings (see page 9) and related network settings.

Advanced

Access Control



Access Control

To use Access Control, you must set a static IP address for that PC and set that PC to use the selected IP address.

Up to 10 selected local users can be denied access to particular websites or to website addresses containing particular words.

View/Modify Globally Disallowed Website/Keyword List

You can control Internet access 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 restrict to this user
3. Click **Save**

Choose an IP Address : Choose an IP Address ▾

□ E-mail

□ File Downloading (FTP)

□ News Forum

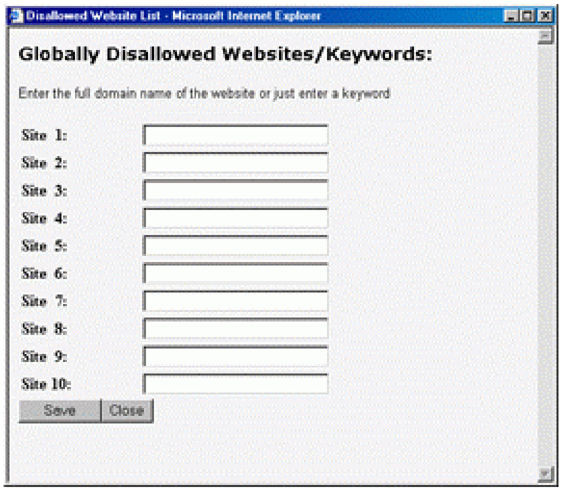
□ Bulletin Board Service

□ Web Browsing (Modify Globally Disallowed List above)

Figure 39. 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 must 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 websites list (**Figure 40**).



Disallowed Website List - Microsoft Internet Explorer

Globally Disallowed Websites/Keywords:

Enter the full domain name of the website or just enter a keyword

Site 1:

Site 2:

Site 3:

Site 4:

Site 5:

Site 6:

Site 7:

Site 8:

Site 9:

Site 10:

Figure 40. 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.

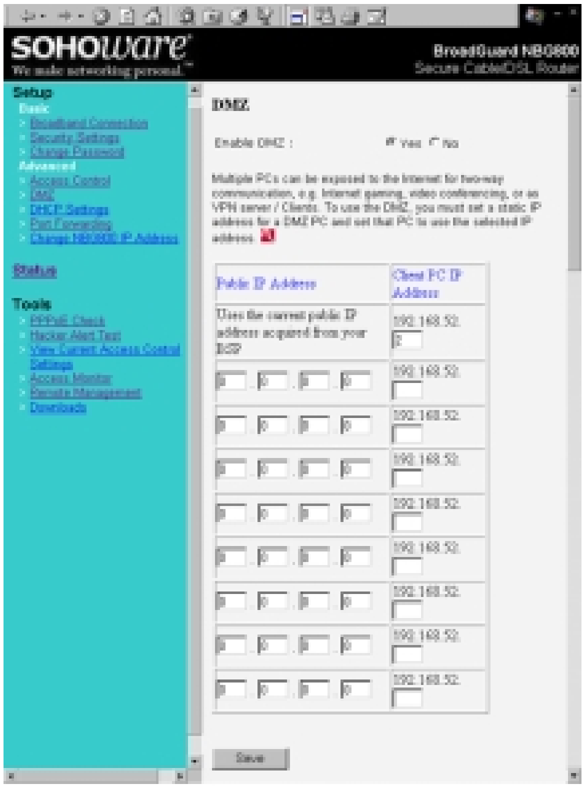
Access Control may be used to restrict use of the following Internet applications:

- 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



DMZ

Enable DMZ : ● Yes ○ No

Multiple PCs can be exposed to the Internet for two-way communication, e.g. Internet gaming, video conferencing, or as VPN server / Clients. To use the DMZ, you must set a static IP address for a DMZ PC and set that PC to use the selected IP address.

Public IP Address	Client PC IP Address
Uses the current public IP address acquired from your ISP	192.168.52. 2
0 . 0 . 0 . 0	192.168.52.
0 . 0 . 0 . 0	192.168.52.
0 . 0 . 0 . 0	192.168.52.
0 . 0 . 0 . 0	192.168.52.
0 . 0 . 0 . 0	192.168.52.
0 . 0 . 0 . 0	192.168.52.
0 . 0 . 0 . 0	192.168.52.
0 . 0 . 0 . 0	192.168.52.

Figure 41. DMZ

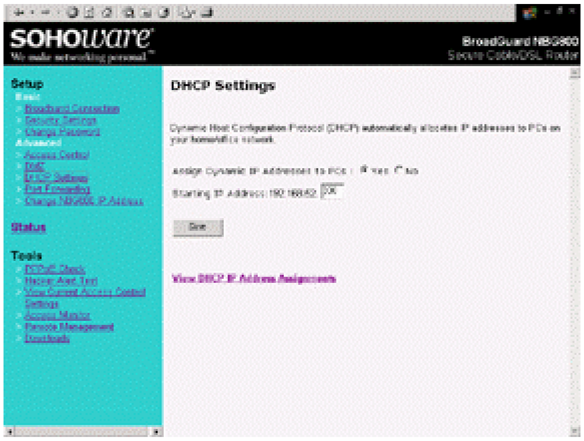
Usually all PCs connected to the BroadGuard are protected from Internet intruders by a built-in firewall. For some kinds of Internet applications, for example, Internet interactive games, video-conferencing, VPN (Virtual Private Networks), or as an e-mail server etc., computers must be exposed to the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

Note: One public IP address is mapped to one DMZ PC. IP addresses from .2 to .11.are reserved for Access Control. Do not assign an address in this range to DMZ PC's.

BroadGuard Setting: You must set a static IP address for a DMZ PC to be exposed to the Internet and set that PC to use the selected IP address. Then click ***Save*** to make the setting effective. Click ***Restart*** to initialize the BroadGuard with the updated settings.

DMZ opens all ports on a computer to requests for service from the Internet and exposes the computer to risk from hackers. “Open only the ports you need” is the most important rule for your broadband Internet security. Therefore, it is highly recommended that, unless you don’t know the ports used by the application, the Port Forwarding feature be used to support your Internet applications (see Port Forwarding, page 37).

DHCP Settings



DHCP Settings

Dynamic Host Configuration Protocol (DHCP) automatically allocates IP addresses to PCs on your home/office network.

Assign Dynamic IP addresses to PCs : ● Yes ○ No

Starting IP Address: 192.168.1. 100

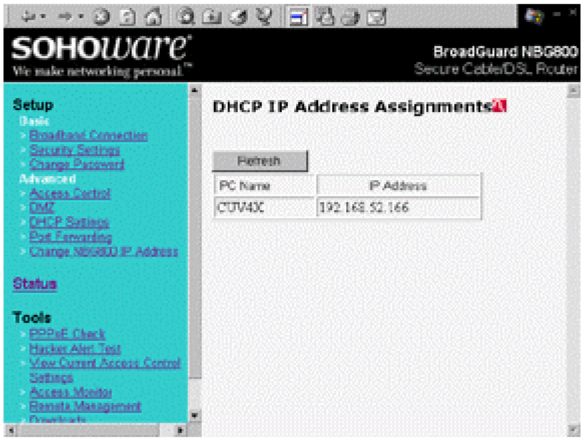
Figure 42. DHCP Settings

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, 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.



DHCP IP Address Assignments

PC Name	IP Address
CUV4X	192.168.52.166

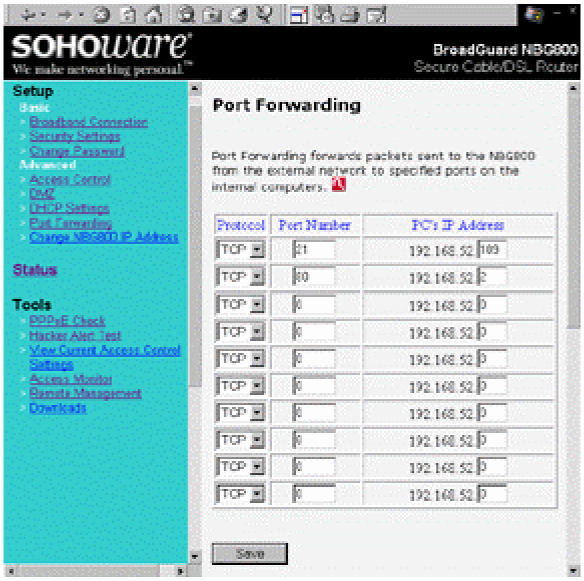
Figure 43. DHCP IP Address Assignments

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

When your PC asks the BroadGuard for an IP address, it issues an IP address with a validity period of three days. If you turn off the BroadGuard and turn it on within that three-day period, your PC will not attempt to renew the IP address. As the previous IP assignment table will be cleared when the BroadGuard was turned off, your IP address will not be shown in the table.

To renew the IP address: for Windows 95/98/Me go to page 48, for Windows NT 4.0 go to page 49, and for Windows 2000 go to page 50.

Port Forwarding



Port Forwarding

Port Forwarding forwards packets sent to the NBG800 from the external network to specified ports on the internal computers.

Protocol	Port Number	PC's IP Address
TCP	21	192.168.52. 100
TCP	80	192.168.52. 2
TCP	0	192.168.52. 0
TCP	0	192.168.52. 0
TCP	0	192.168.52. 0
TCP	0	192.168.52. 0
TCP	0	192.168.52. 0
TCP	0	192.168.52. 0
TCP	0	192.168.52. 0
TCP	0	192.168.52. 0

Figure 44. Port Forwarding

An increasing number of web applications, games, java applets, etc. need access to some service on your local computer in order to function properly. Since this access may pose a security problem, the machine providing the service should not be directly connected to the Internet.

Port Forwarding provides an almost ideal solution to this access problem. On the firewall, IP packets that come in to a specific port number are re-written and forwarded to the internal server providing the actual service. The reply packets from the internal server are re-written to make it appear that they came from the firewall.

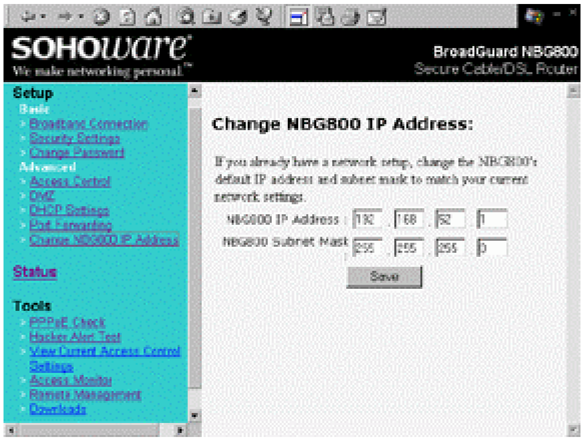
- Port forwarding routes all packets intended for one forwarding port on the gateway from the external networks, to a specified port on one of the internal machines (after a little re-writing of headers).
- In the *Protocol* column, choose either TCP or UDP from the drop-down list.
- Enter the port number you wish to open in the *Port Number* field. Well known ports include 7(Echo), 21(FTP), 23(TELNET), 25(SMTP), 53(DNS), 79(Finger), 80/8080(HTTP), 110(POP3), 113(Authentication Service), 119(NNTP), 161(SNMP), 162(SNMP Trap), 1723(PPTP).

- Enter the IP address of the PC you wish to map to the port number in the PC's IP Address field.

Note: IP addresses from .2 to .11 are reserved for Access Control. Do not assign an IP address from this range to Port Forwarding PCs.

- If you want to disable port forwarding, enter 0 (zero) in both the *IP Address* field and the *Port Number* field.

Change NBG800 IP Address



Change NBG800 IP Address:

If you already have a network setup, change the NBG800's default IP address and subnet mask to match your current network settings.

NBG800 IP Address : 192 . 168 . 52 . 1

NBG800 Subnet Mask 255 . 255 . 255 . 0

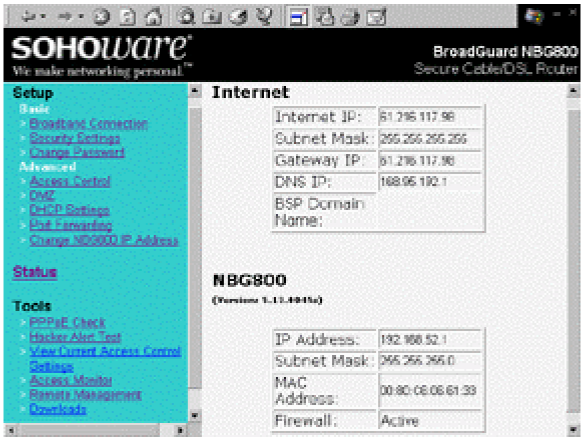
Figure 45. Change NBG800 IP Address

If you do not wish to accept the NBG800 default IP address (192.168.1.1) and subnet mask (255.255.255.0), change them to a setting of your choice.

Click ***Save*** and ***Restart*** to restart your BroadGuard. Close your browser. Release and renew your PC's IP address in order to get the new BroadGuard IP address (For Windows 95/98/Me go to page 48, for Windows NT 4.0 go to page 49, and for Windows 2000 go to page 50).

Status

The *Status* section contains; Internet information, the Public IP Address assignment, and the BroadGuard LAN IP address assignments (**Figure 46**). This information is useful in resolving a connection problem.



Internet

Internet IP:	61.216.117.98
Subnet Mask:	255.255.255.255
Gateway IP:	61.216.117.98
DNS IP:	168.95.192.1
BSP Domain Name:	

NBG800

(Version 1.11.4045a)

IP Address:	192.168.52.1
Subnet Mask:	255.255.255.0
MAC Address:	00:80:C6:06:61:33
Firewall:	Active

Figure 46. Status

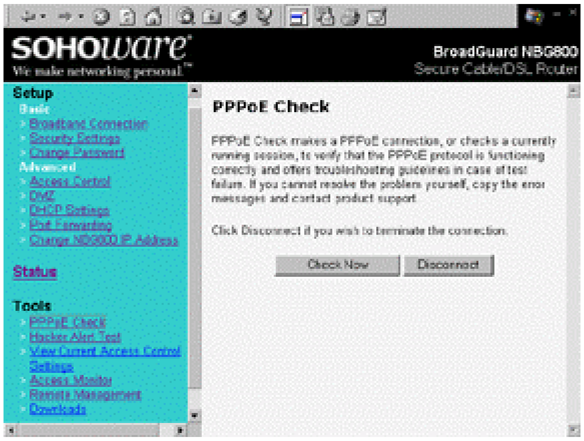
Internet	Internet IP address assigned by your BSP Subnet Mask: 255.255.255.0 is the default setting Gateway IP: The IP address of the BSP's Internet Network Gateway DNS IP: The IP address of the BSP's Domain Name Server BSP Domain Name: The BSP's Domain Name Server (this field may be blank depending on your BSP)
NBG800	IP Address: The IP address of the NGB800 Subnet Mask: 255.255.255.0 is the default setting MAC Address: The MAC address of the NGB800 Firewall: The NGB800 firewall status

Tools

Six useful tools are provided: PPPoE Check, Hacker Alert Test, View Current Access Control Settings, Access Monitor, Remote Management, and Downloads.

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***. You may click ***Disconnect*** to terminate your DSL connection.



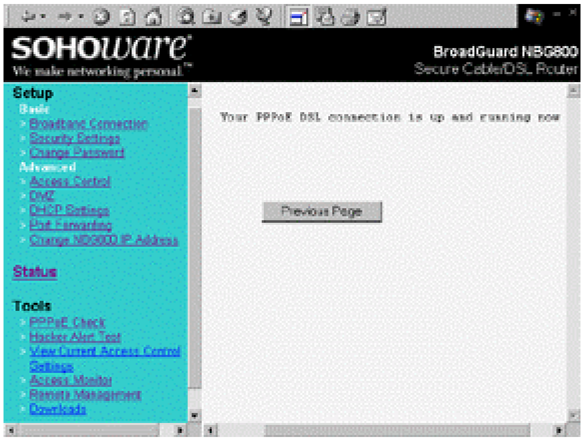
PPPoE Check

PPPoE Check makes a PPPoE connection, or checks a currently running session, to verify that the PPPoE protocol is functioning correctly and offers troubleshooting guidelines in case of test failure. If you cannot resolve the problem yourself, copy the error messages and contact product support.

Click Disconnect if you wish to terminate the connection.

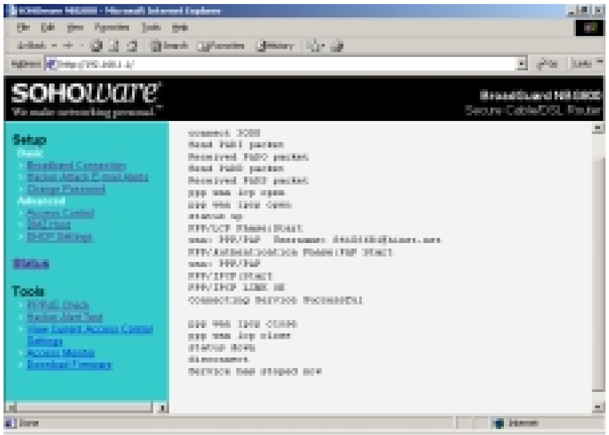
Figure 47. PPPoE Check

Either of the following screens (**Figure 48** or **Figure 49**) indicate that PPPoE is operating correctly.



```
Your PPPoE DSL connection is up and running now
```

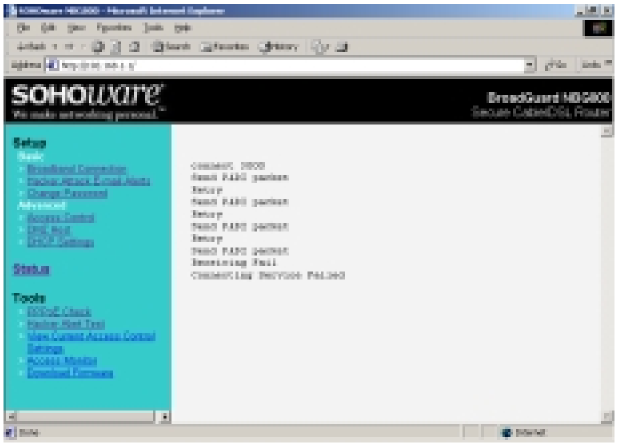
Figure 48. PPPoE Service Running



```
connect [illegible]
Send PADI packet
Received PADO packet
Send PADR packet
Received PADS packet
ppp wan lcp open
ppp wan ipcp open
status up
PPP/LCP Phase:Start
wan: PPP/PAP  Username: [illegible]
PPP/Authentication Phase:PAP Start
wan: PPP/PAP
PPP/IPCP Start
PPP/IPCP LINK UP
Connecting Service Successful

ppp wan ipcp close
ppp wan lcp close
status down
disconnect
Service has stoped now
```

Figure 49. PPPoE Check Successful

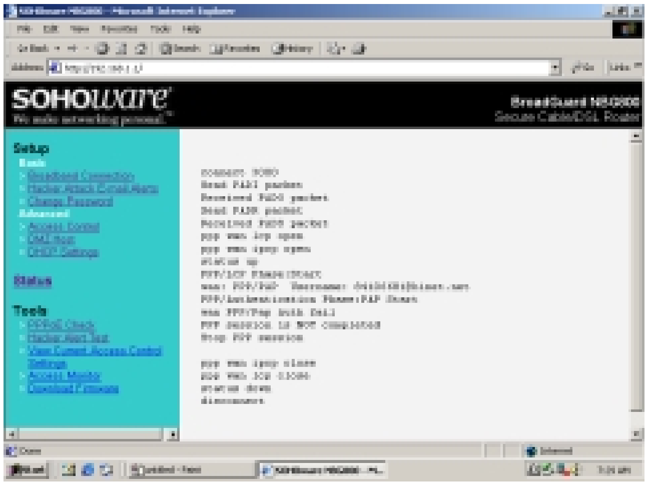
If you see a screen similar to the following (**Figure 50**), it means that your BSP's server may not be operating, or something could be wrong with your DSL modem, e.g. a loose cable either on the DSL modem or the BroadGuard port.



```
connect [illegible]
Send PADI packet
Retry
Send PADI packet
Retry
Send PADI packet
Retry
Send PADI packet
Receiving Fail
Connecting Service Failed
```

Figure 50. PPPoE Check Unsuccessful

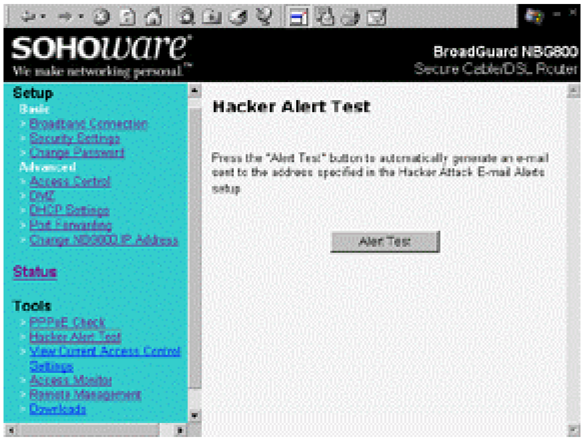
A screen such as that shown in Figure 51 indicates that you entered a wrong username, login password, or service name. Go to the DSL broadband connection setup page to check them again.



```
connect SOHO
Send PADI packet
Received PADO packet
Send PADR packet
Received PADS packet
ppp wan lcp open
ppp wan ipcp open
status up
PPP/LCP Phase:Start
wan: PPP/PAP  Username: [illegible]
PPP/Authentication Phase:PAP Start
wan PPP/Pap Auth fail
PPP session is NOT completed
Stop PPP session

ppp wan ipcp close
ppp wan lcp close
status down
disconnect
```

Figure 51. Authentication Failed

Hacker Alert Test



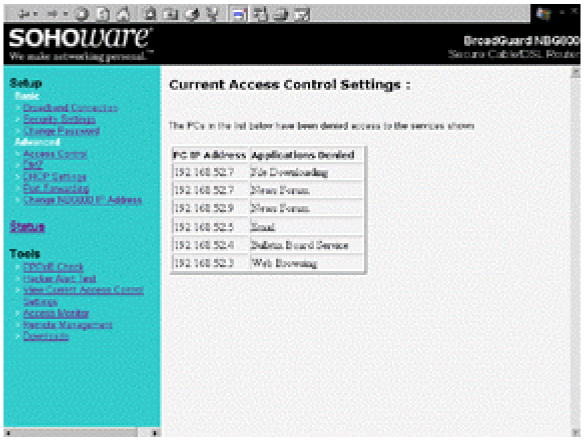
Hacker Alert Test

Press the "Alert Test" button to automatically generate an e-mail sent to the address specified in the Hacker Attack E-mail Alerts setup

Figure 52. Hacker Alert Test

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

View Current Access Control Settings



Current Access Control Settings :

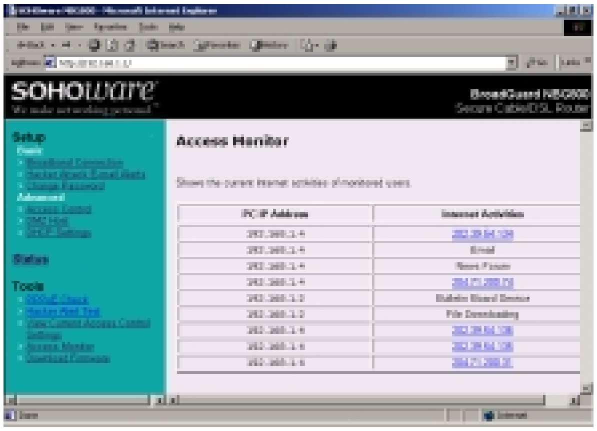
The PCs in the list below have been denied access to the services shown

PC IP Address	Applications Denied
192.168.52.7	File Downloading
192.168.52.7	News Forum
192.168.52.9	News Forum
192.168.52.5	Email
192.168.52.4	Bulletin Board Service
192.168.52.3	Web Browsing

Figure 53. 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



Access Monitor

Shows the current Internet activities of monitored users.

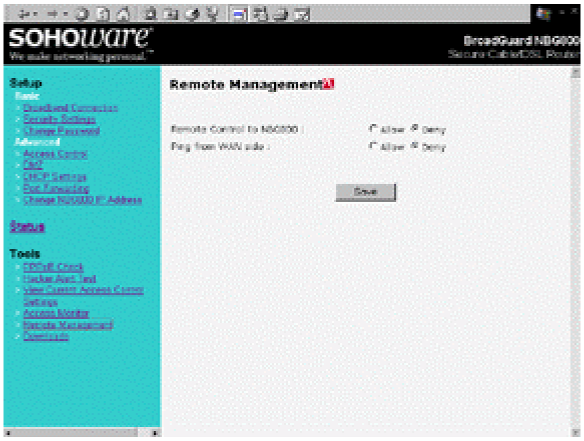
PC IP Address	Internet Activities
192.168.1.4	[illegible]
192.168.1.4	Email
192.168.1.4	News Forum
192.168.1.4	[illegible]
192.168.1.2	Bulletin Board Service
192.168.1.2	File Downloading
192.168.1.4	[illegible]
192.168.1.4	[illegible]
192.168.1.6	[illegible]

Figure 54. 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.

Click ***Refresh*** to display the latest Internet activities. Click any website's hypertext address to go to that website.

Remote Management



Remote Management

Remote Control to NBG800 : ○ Allow ● Deny

Ping from WAN side : ○ Allow ● Deny

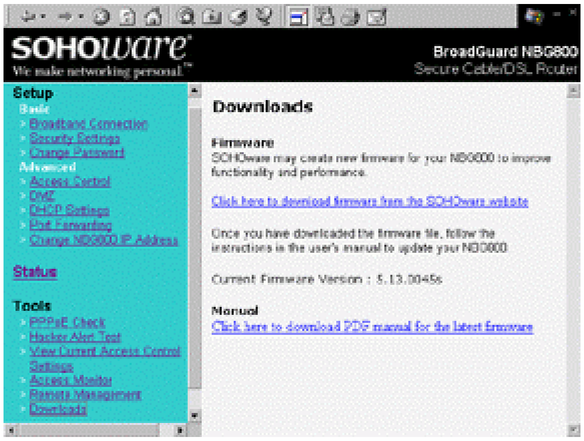
Figure 55. Remote Management

Remote Management allows you to remotely configure your BroadGuard. For the security of your network, the default setting is *Deny*.
We recommend that you enable the NBG800's Remote Management function only when necessary. Be sure to change the default admin password (1234) before using this feature. If you set "Enable SPI & Anti-DoS to protect your network" to ***No*** (see Security Settings, page 30) then remote management will always be available no matter whether you check ***Allow*** or ***Deny***.

Note1: If you have forwarded incoming packets to a web server located on your local network, the local web server should be set to listen on port 8080.

Note2: You cannot remotely upgrade the BroadGuard, even when remote control is enabled.

Downloads



Downloads

Firmware
SOHOware may create new firmware for your NBG800 to improve functionality and performance.

Click here to download firmware from the SOHOware website

Once you have downloaded the firmware file, follow the instructions in the user's manual to update your NBG800

Current Firmware Version : 5.13.0045s

Manual
Click here to download PDF manual for the latest firmware

Figure 56. Downloads

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

Windows Users
Download the firmware from the SOHOware 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 press the *Reset* button on the rear of the BroadGuard to make your new firmware effective.

Mac & Linux Users

For Mac and Linux users we currently offer the firmware binary file only. Linux has a built-in TFTP program, Mac users need a third-party TFTP program.

After the upgrade process is complete, you must press the *Reset* button on the rear of the BroadGuard to make your new firmware effective.

Chapter 4: Troubleshooting

If you cannot find your problem listed below, see Chapter 5: FAQs, page 54, 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*.

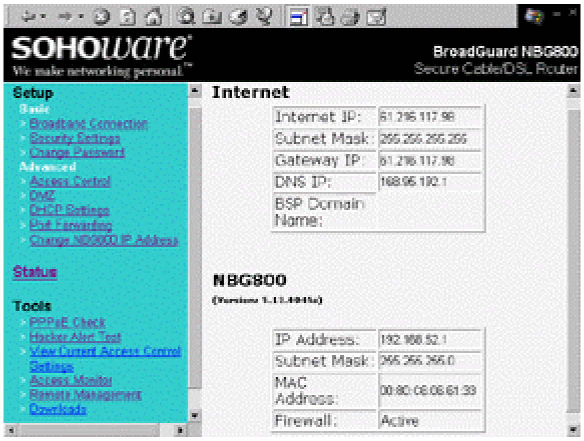
- The Subnet Mask should be set to *255.255.255.0* to match the BroadGuard. On the client PC, you can check these settings by using *Control Panel/Network* to check the properties for the TCP/IP protocols.

2. The Status LED stays lit when it should not.

The Status LED lights when the device is powered up and checks for proper operation. After finishing the checking procedure, the LED should turn 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 57**) 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.



Internet

Internet IP:	61.216.117.98
Subnet Mask:	255.255.255.255
Gateway IP:	61.216.117.98
DNS IP:	168.95.192.1
BSP Domain Name:	

NBG800

(Version: 1.11.4045a)

IP Address:	192.168.52.1
Subnet Mask:	255.255.255.0
MAC Address:	00:80:C6:06:61:33
Firewall:	Active

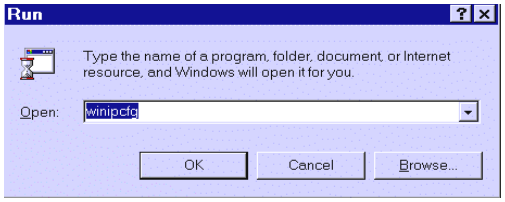
Figure 57. Status

- Check that the PC got an IP address assigned to it automatically (for Windows 95/98/Me see the following section. For Windows NT 4.0, see page 49. For Windows 2000 see page 50.

- 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 58**)

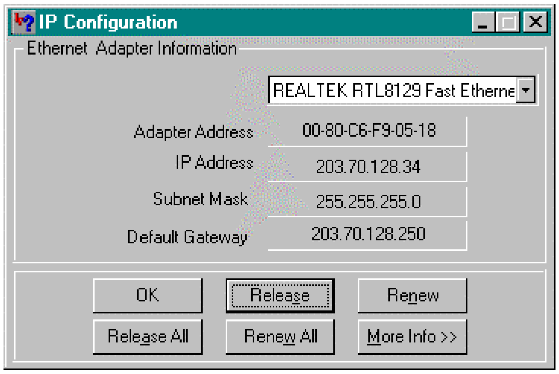


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: winipcfg

Figure 58. Run

step2. The *IP Configuration* dialog box will open (**Figure 59**)



IP Configuration

Ethernet Adapter Information

REALTEK RTL8129 Fast Etherne

Adapter Address 00-80-C6-F9-05-18

IP Address 203.70.128.34

Subnet Mask 255.255.255.0

Default Gateway 203.70.128.250

Figure 59. IP Configuration

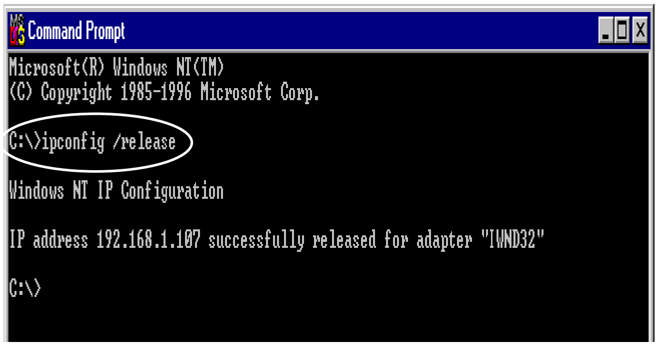
step3. Select the network adapter you use to connect to the BroadGuard. Click ***Release***

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 43, page 36). Click ***Refresh***

Windows NT 4.0

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

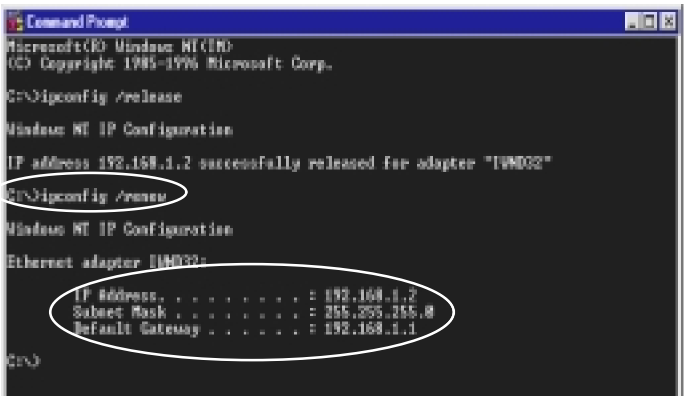


```
Microsoft(R) Windows NT(TM)
(C) Copyright 1985-1996 Microsoft Corp.

C:\>ipconfig /release

Windows NT IP Configuration

IP address 192.168.1.107 successfully released for adapter "IWND32"

C:\>
```

Figure 60. Command Prompt-1

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**)



```
Microsoft(R) Windows NT(TM)
(C) Copyright 1985-1996 Microsoft Corp.

C:\>ipconfig /release

Windows NT IP Configuration

IP address 192.168.1.2 successfully released for adapter "IWND32"

C:\>ipconfig /renew

Windows NT IP Configuration

Ethernet adapter IWND32:

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

C:\>
```

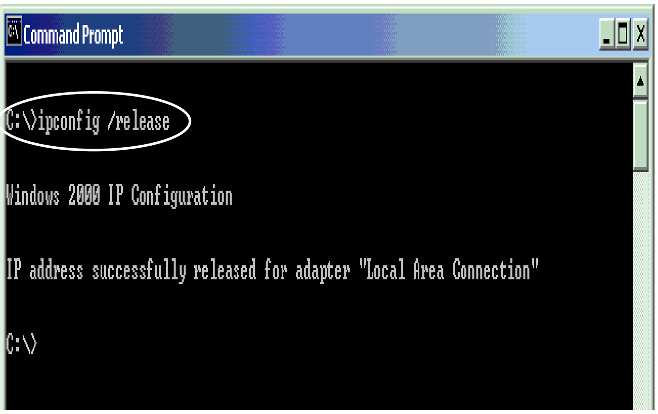
Figure 61. Command Prompt-2

step4. Type ***Exit***

step6. Go to *DHCP IP Address Assignments* (see Figure 43, page 36). Click ***Refresh***

Windows 2000

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

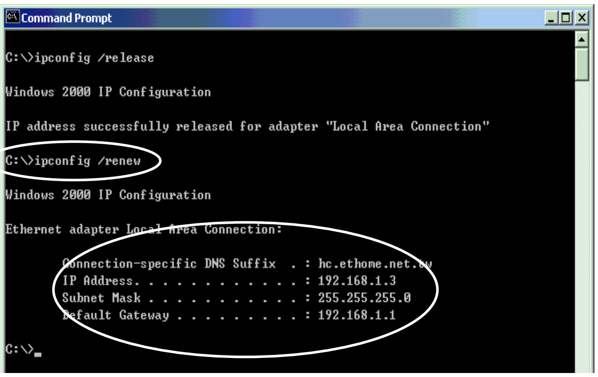


```
C:\>ipconfig /release

Windows 2000 IP Configuration

IP address successfully released for adapter "Local Area Connection"

C:\>
```

Figure 62. Command Prompt-3

step2. Type "*ipconfig /release*" (**Figure 62**) 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 63**)



```
C:\>ipconfig /release

Windows 2000 IP Configuration

IP address successfully released for adapter "Local Area Connection"

C:\>ipconfig /renew

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : hc.ethome.net.tw
        IP Address. . . . . . . . . . . . : 192.168.1.3
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1

C:\>_
```

Figure 63. Command Prompt-4

step4. Type ***Exit***.

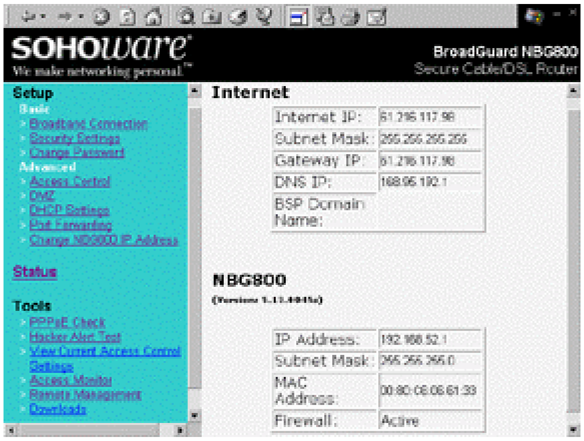
step5. Go to *DHCP IP Address Assignments* (see Figure 43, page 36). Click ***Refresh***

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 64**). If there is no information shown on the screen, it means that your BSP has a problem



Internet

Internet IP:	61.216.117.98
Subnet Mask:	255.255.255.255
Gateway IP:	61.216.117.98
DNS IP:	168.95.192.1
BSP Domain Name:	

NBG800

(Version: 1.13.4045a)

IP Address:	192.168.52.1
Subnet Mask:	255.255.255.0
MAC Address:	00:80:06:06:61:33
Firewall:	Active

Figure 64. Status

5. I 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.

When your PC asks the BroadGuard for an IP address, it issues an IP address with a validity period of three days. If you turn off the BroadGuard and turn it on within that three day period, your PC will not attempt to renew the IP address. As the previous IP assignment table will be cleared when the BroadGuard was turned off, your IP address will not be shown in the table.

To renew the IP address: for Windows 95/98/Me go to page 48, for Windows NT 4.0 go to page 49, and for Windows 2000 go to page 50.

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.

7. My computer was originally connected to the Internet via PPPoE without any problem. When I install a BroadGuard into the network, all LEDs light correctly but I cannot get a connection. When I switch back to my original network setup (without a BroadGuard), the network connection operates normally. What should I do?

Completely remove the PPPoE software from all your PCs. The PPPoE software supplied by Broadband Service Providers causes many conflicts, including one with the BroadGuard’s PPPoE program.

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 setting: ICQ menu-> Preferences -> 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 SOHOware website at

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

- **Does the BroadGuard pass PPTP packets?**
  Yes.

- **What is the recommended maximum number of VPN sessions I can run on the BroadGuard?**
  If you setup a VPN server inside the BroadGuard, and users from the Internet want to access the VPN server, we recommend the number of sessions is five or less to prevent influencing the throughput of the BroadGuard.
  If multiple PCs inside the BroadGuard want to simultaneously access the same VPN server located on the Internet, you must have multiple public IP addresses and enable DMZ. Otherwise only one session can be created.

- **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 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 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 34, page 28. For DSL users, see Figure 36, page 30.

- **Is there an internal cable or DSL modem in the BroadGuard?**
  No, the BroadGuard only operates 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 (see DMZ, page 34) or Port Forwarding (see Port Forwarding, page 37). 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 (see DMZ, page 34) or Port Forwarding (see Port Forwarding, page 37).

- **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 (Virtual Private Network) server from your home office, or build a VPN server for mobile sales people to access. 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 using DMZ (see DMZ, page 34) or Port Forwarding (see Port Forwarding, page 37). Only one PC can be used as a VPN server as only one PC may be set as a DMZ Host or Port Forwarding machine.

step1. See Broadband Connection, 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 or Port Forwarding machine

VPN Client Configuration (e.g. Microsoft PPTP)

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 98/98SE/Me VPN Client Setup

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

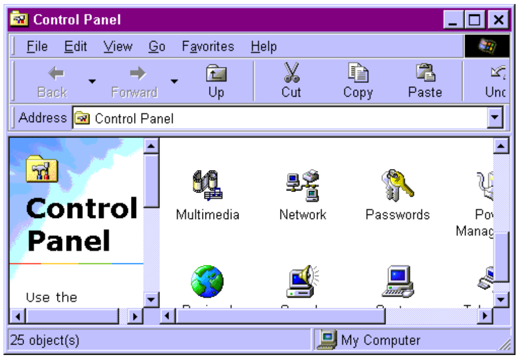
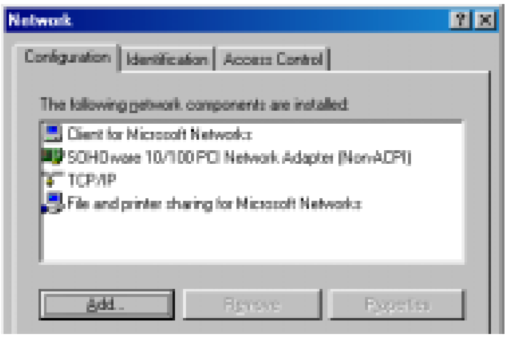


Figure 65. Control Panel

step2. In *Control Panel*, double-click the ***Network*** icon. The *Network* dialog box will open (**Figure 66**)

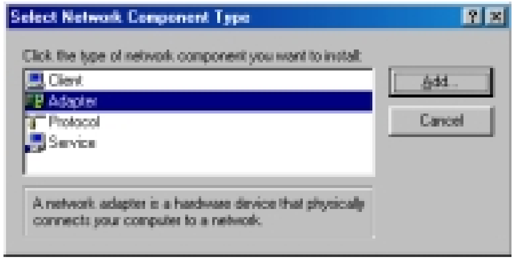


The following network components are installed:

- Client for Microsoft Networks
- SOHOware 10/100 PCI Network Adapter (NonACPI)
- TCP/IP
- File and printer sharing for Microsoft Networks

Figure 66. Network

step3. Click ***Add***. The *Select Network Component Type* dialog box will open (**Figure 67**)



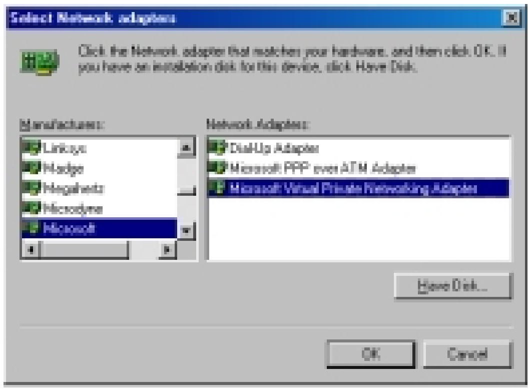
Click the type of network component you want to install:

- Client
- Adapter
- Protocol
- Service

A network adapter is a hardware device that physically connects your computer to a network.

Figure 67. Select Network Component Type

step4. Double-click ***Adapter***. The *Select Network adapters* dialog box will open (**Figure 68**)



Click the Network adapter that matches your hardware, and then click OK. If you have an installation disk for this device, click Have Disk.

Manufacturers:

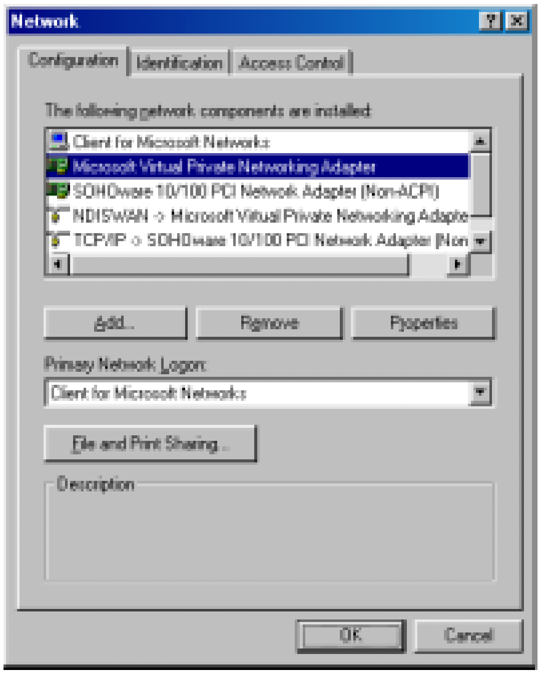
- Linksys
- Madge
- Megahertz
- Microdyne
- Microsoft

Network Adapters:

- Dial-Up Adapter
- Microsoft PPP over ATM Adapter
- Microsoft Virtual Private Networking Adapter

Figure 68. 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* dialog box (**Figure 69**). The *Microsoft Virtual Private Networking Adapter* item in the *Network* box indicates that it has been successfully installed.



The following network components are installed:

- Client for Microsoft Networks
- Microsoft Virtual Private Networking Adapter
- SOHOware 10/100 PCI Network Adapter (Non-ACPI)
- NDISWAN -> Microsoft Virtual Private Networking Adapte
- TCP/IP -> SOHOware 10/100 PCI Network Adapter (Non

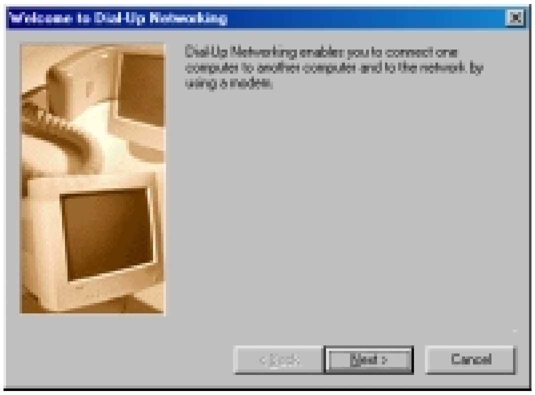
Primary Network Logon:
Client for Microsoft Networks

Figure 69. 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. Remove the CD and 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 70**)

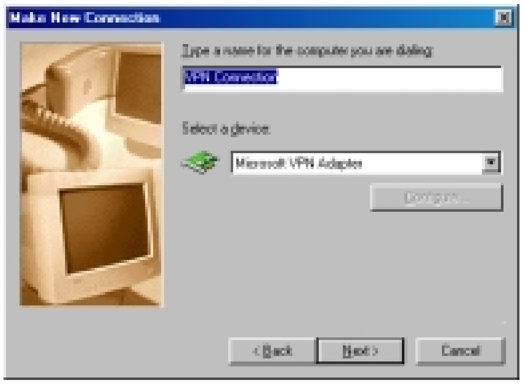


Welcome to Dial-Up Networking

Dial-Up Networking enables you to connect one computer to another computer and to the network by using a modem.

Figure 70. Welcome to Dial-Up Networking

step9. Click ***Next***. The *Make New Connection* dialog box will open (**Figure 71**)



Make New Connection

Type a name for the computer you are dialing:

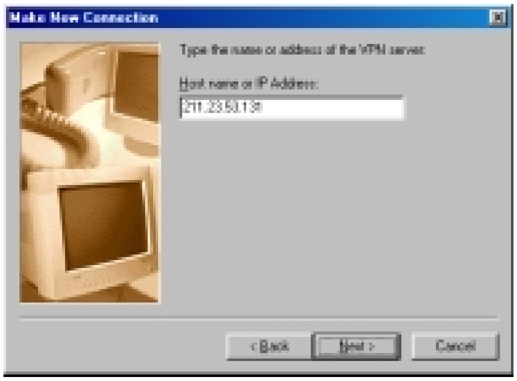
VPN Connection

Select a device:

Microsoft VPN Adapter

Figure 71. 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***



Make New Connection

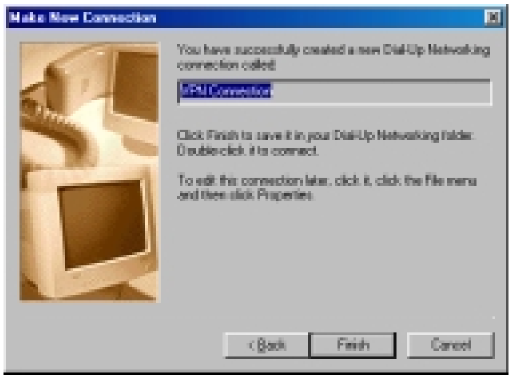
Type the name or address of the VPN server:

Host name or IP Address:

211.23.53.131

Figure 72. Make New Connection-2

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



Make New Connection

You have successfully created a new Dial-Up Networking connection called:

VPN Connection

Click Finish to save it in your Dial-Up Networking folder. Double-click it to connect.

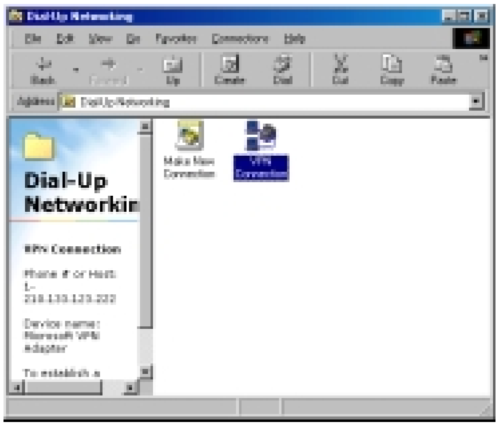
To edit this connection later, click it, click the File menu and then click Properties.

Figure 73. 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 74**), you should have a new VPN connection


Dial-Up Networking
File Edit View Go Favorites Connections Help
Back Forward Up Create Dial Cut Copy Paste
Address Dial-Up Networking
Make New Connection
VPN Connection

Dial-Up Networking

VPN Connection

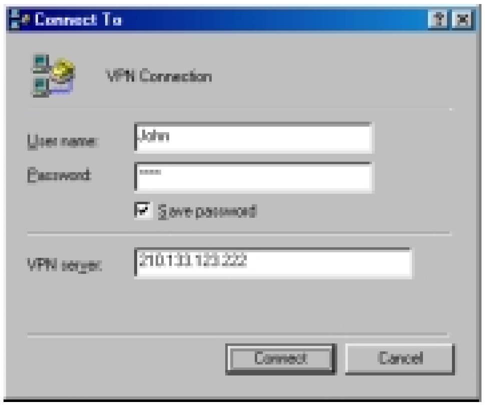
Phone # or Host: 1-210.133.123.222

Device name: Microsoft VPN Adapter

To establish a

Figure 74. Dial-Up Networking

step15. Double-click the newly-created icon. The *Connect To* dialog box will open (**Figure 75**)



VPN Connection

User name: John

Password: ****

☑ Save password

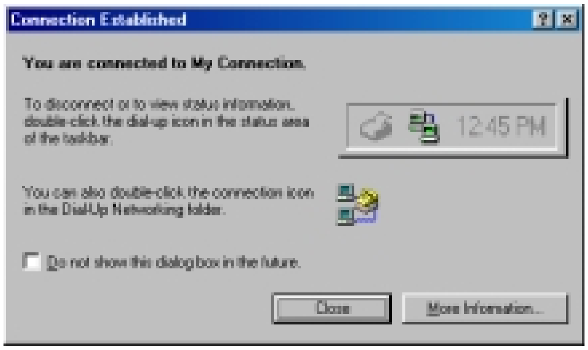
VPN server: 210.133.123.222

Figure 75. 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 76**)



Connection Established

You are connected to My Connection.

To disconnect or to view status information, double-click the dial-up icon in the status area of the taskbar.

You can also double-click the connection icon in the Dial-Up Networking folder.

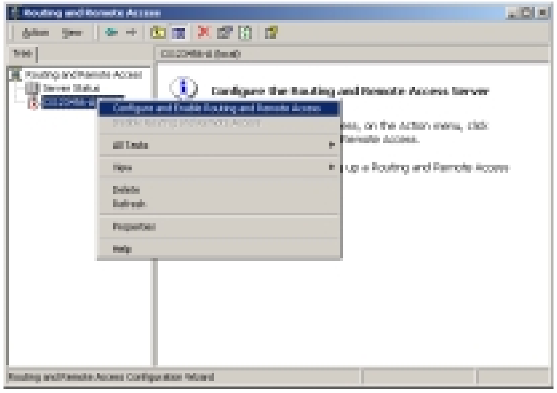
□ Do not show this dialog box in the future.

Figure 76. Connection Established

Windows 2000 VPN Server Setup

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

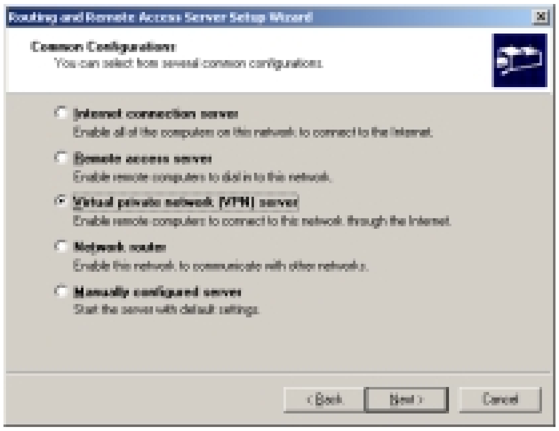
step1. Click ***Start/Programs/Administrative Tools/Routing and Remote Access***



Routing and Remote Access
Action
View
Tree
Routing and Remote Access
Server Status
Configure the Routing and Remote Access Server
Configure and Enable Routing and Remote Access
All Tasks
View
Delete
Refresh
Properties
Help
Routing and Remote Access Configuration Wizard

Figure 77. Routing and Remote Access

step2. In the *Routing and Remote Access* box (**Figure 77**), 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 78**)



Routing and Remote Access Server Setup Wizard

Common Configurations
You can select from several common configurations.

○ **Internet connection server**
Enable all of the computers on this network to connect to the Internet.

○ **Remote access server**
Enable remote computers to dial in to this network.

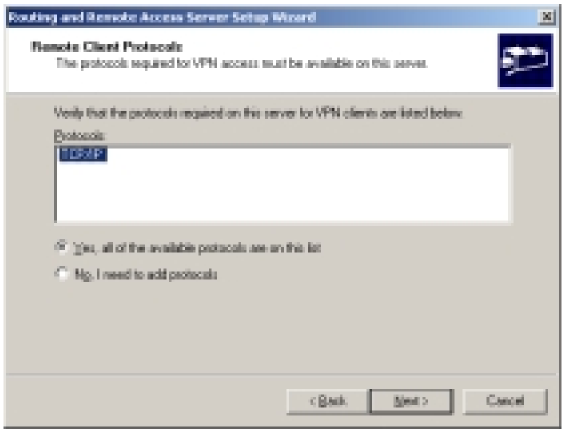
● **Virtual private network (VPN) server**
Enable remote computers to connect to this network through the Internet.

○ **Network router**
Enable this network to communicate with other networks.

○ **Manually configured server**
Start the server with default settings.

Figure 78. Common Configurations

step3. Check *Virtual private network (VPN) server* and click ***Next***. The *Remote Client Protocols* dialog box will open (**Figure 79**)



Routing and Remote Access Server Setup Wizard

Remote Client Protocols
The protocols required for VPN access must be available on this server.

Verify that the protocols required on this server for VPN clients are listed below.

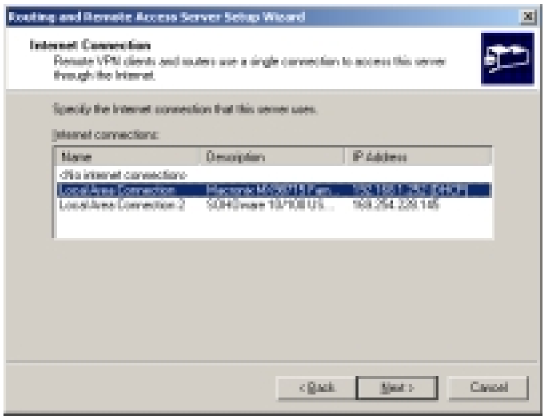
Protocols:
TCP/IP

● Yes, all of the available protocols are on this list

○ No, I need to add protocols

Figure 79. 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 80**)



Routing and Remote Access Server Setup Wizard

Internet Connection

Remote VPN clients and routers use a single connection to access this server through the Internet.

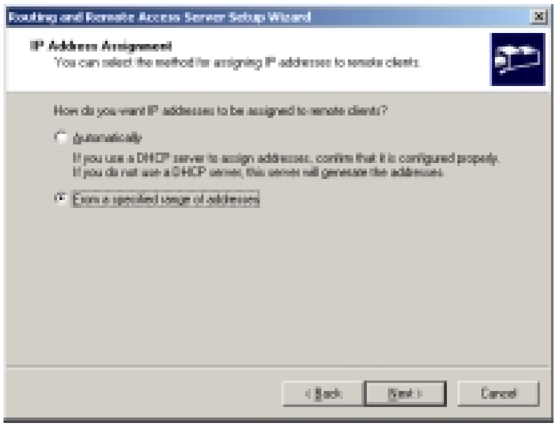
Specify the Internet connection that this server uses.

Internet connections:

Name	Description	IP Address
<No internet connections>		
Local Area Connection	Macronix MX98715 Fam...	192.168.1.252 (DHCP)
Local Area Connection 2	SOHOware 10/100 US...	169.254.228.145

Figure 80. 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 81**)



Routing and Remote Access Server Setup Wizard

IP Address Assignment

You can select the method for assigning IP addresses to remote clients.

How do you want IP addresses to be assigned to remote clients?

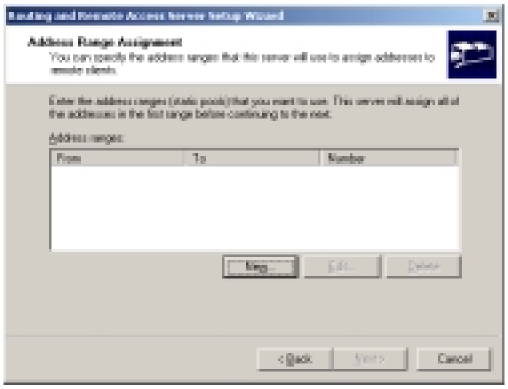
○ Automatically

If you use a DHCP server to assign addresses, confirm that it is configured properly. If you do not use a DHCP server, this server will generate the addresses.

● From a specified range of addresses

Figure 81. IP Address Assignment

step6. Check *From a specified range of addresses*. Click ***Next***. The *Address Range Assignment* box will open (**Figure 82**)



Address Range Assignment

You can specify the address ranges that this server will use to assign addresses to remote clients.

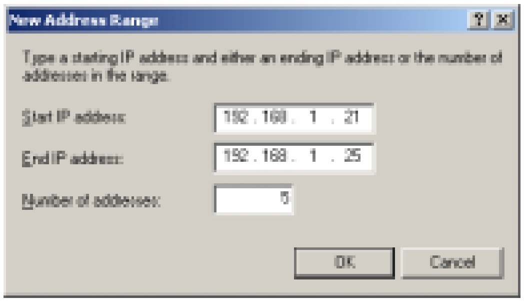
Enter the address ranges (static pools) that you want to use. This server will assign all of the addresses in the first range before continuing to the next.

Address ranges:

From	To	Number

Figure 82. Address Range Assignment

step7. Click ***Next***. The *New Address Range* box will open (**Figure 83**)



Type a starting IP address and either an ending IP address or the number of addresses in the range.

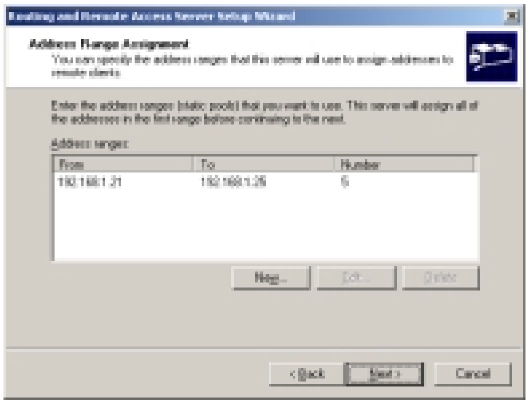
Start IP address: 192 . 168 . 1 . 21

End IP address: 192 . 168 . 1 . 25

Number of addresses: 5

Figure 83. 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 83, 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 84**)



Address Range Assignment

You can specify the address ranges that this server will use to assign addresses to remote clients.

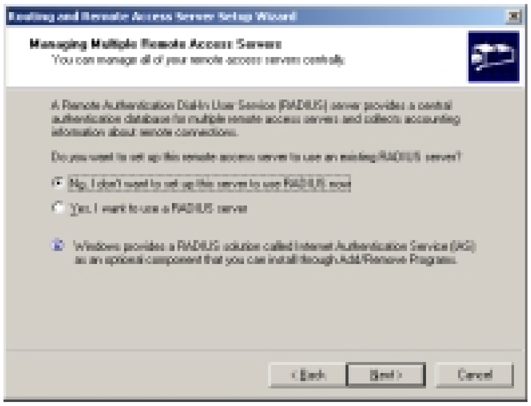
Enter the address ranges (static pools) that you want to use. This server will assign all of the addresses in the first range before continuing to the next.

Address ranges:

From	To	Number
192.168.1.21	192.168.1.25	5

Figure 84. Address Range Assignment

step9. Click ***Next***. The *Managing Multiple Remote Access Servers* dialog box will open (**Figure 85**)



Managing Multiple Remote Access Servers

You can manage all of your remote access servers centrally.

A Remote Authentication Dial-In User Service (RADIUS) server provides a central authentication database for multiple remote access servers and collects accounting information about remote connections.

Do you want to set up this remote access server to use an existing RADIUS server?

● No, I don't want to set up this server to use RADIUS now

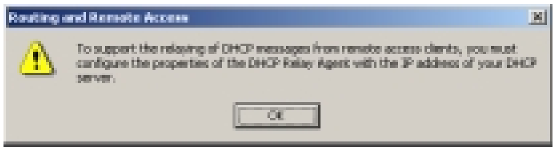
○ Yes, I want to use a RADIUS server

Windows provides a RADIUS solution called Internet Authentication Service (IAS) as an optional component that you can install through Add/Remove Programs.

Figure 85. Managing Multiple Remote Access Servers

step10. Check *No, I don't want…* then click ***Next***

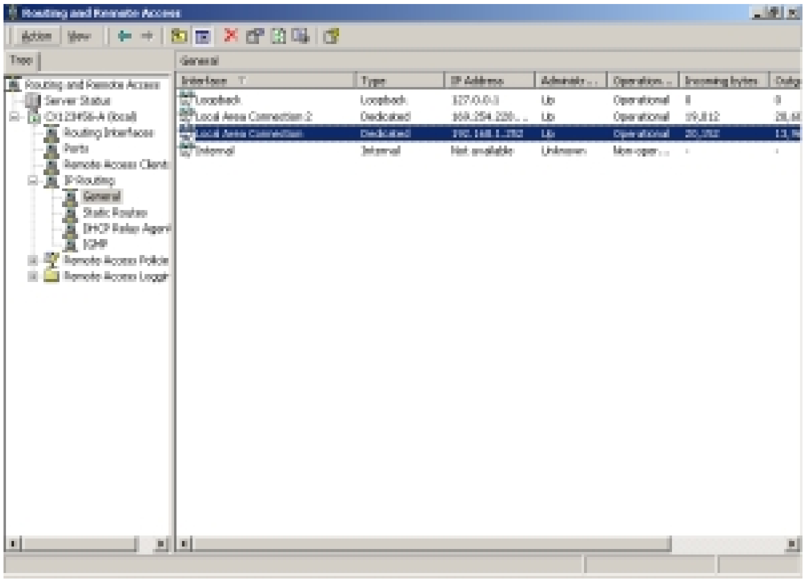
step11. Click ***Finish.*** A *Routing and Remote Access* warning screen will open (**Figure 86**)



To support the relaying of DHCP messages from remote access clients, you must configure the properties of the DHCP Relay Agent with the IP address of your DHCP server.

Figure 86. Routing and Remote Access-1

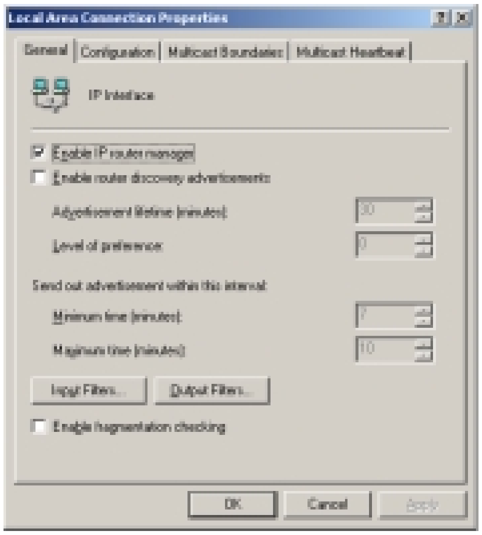
step12. Click ***OK*** to return to the *Routing and Remote Access* main screen (**Figure 87**)



Interface	Type	IP Address	Administr...	Operation...	Incoming bytes	Outg
Loopback	Loopback	127.0.0.1	Up	Operational	8	0
Local Area Connection 2	Dedicated	169.254.220...	Up	Operational	19,812	28,6
Local Area Connection	Dedicated	192.168.1.252	Up	Operational	20,152	13,9
Internal	Internal	Not available	Unknown	Non-oper...	-	-

Figure 87. Routing and Remote Access-2

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 88**)



☑ Enable IP router manager

□ Enable router discovery advertisements

Advertisement lifetime (minutes): 30

Level of preference: 0

Send out advertisement within this interval:

Minimum time (minutes): 7

Maximum time (minutes): 10

□ Enable fragmentation checking

Figure 88. 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 user access permissions.

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 89**)

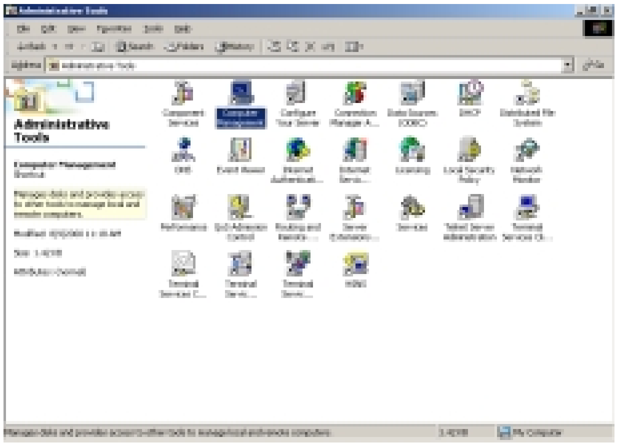


Figure 89. Administrative Tools

step2. Double-click ***Computer Management.*** Expand *System Tools/Local Users and Groups.* Click ***Users*** to show all users lists in *Computer Management* (**Figure 90**)

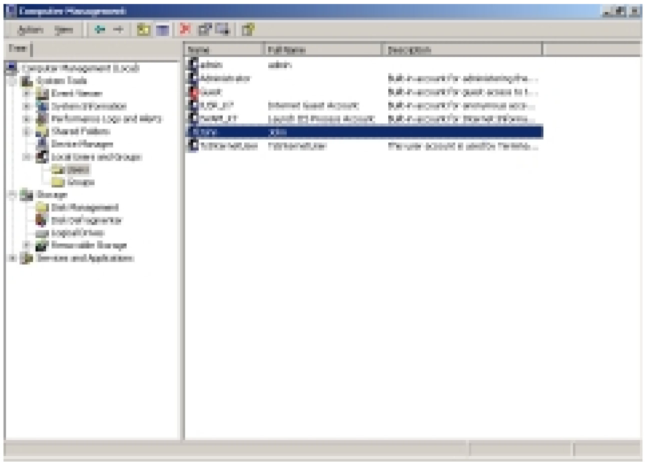
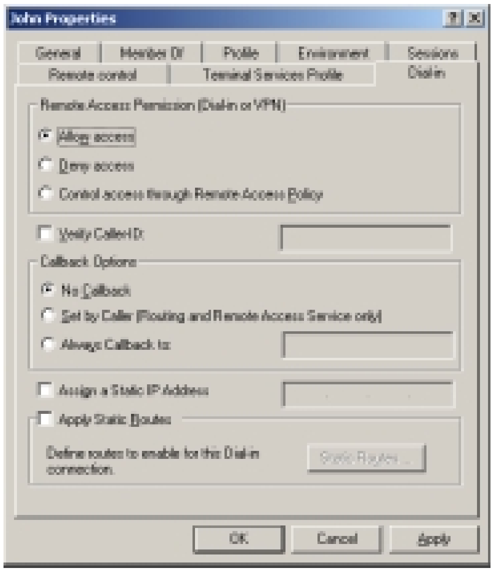


Figure 90. Computer Management

step3. Double-click the name of the user you want to set permissions for. The *Properties* box will open (**Figure 91**)



John Properties

General | Member Of | Profile | Environment | Sessions
Remote control | Terminal Services Profile | Dial-in

Remote Access Permission (Dial-in or VPN)

● Allow access
○ Deny access
○ Control access through Remote Access Policy

□ Verify Caller-ID:

Callback Options

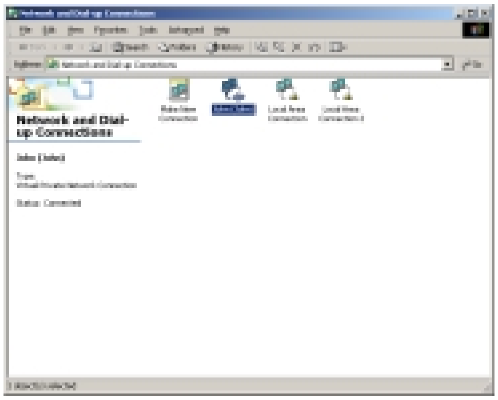
● No Callback
○ Set by Caller (Routing and Remote Access Service only)
○ Always Callback to:

□ Assign a Static IP Address
□ Apply Static Routes

Define routes to enable for this Dial-in connection.

Figure 91. 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 92**)



Network and Dial-up Connections

John (John)

Type:
Virtual Private Network Connection

Status: Connected

Figure 92. Network and Dial-Up Connections

step5. When there is a live connection from a remote user, the icon will show activity (**Figure 92**)

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 ten 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 sohoware.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 solutions.

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 provides an electronic message database where people can login 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.

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 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 a cable/DSL modem
User Interface	Browser-based Management
Maximum Number of PCs	253
Firewall Security	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 Cable/DSL 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 g (27.2 oz.)
Power Consumption	AC 5V/1A
Warranty	BroadGuard Unit: Three-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

Telephone	:	408-565-9888
Toll Free Technical Support	:	800 632-1118 ext: 2828
Technical Support 24hrs	:	888 785-8222
FAX	:	408-565-9889
E-mail	:	support@sohoware.com

Europe and Asia Pacific

Telephone	:	+886-3-578-3966
FAX	:	+886-3-577-7989
E-mail	:	techsupt@ndc.com.tw

For more information on networking, please visit us at:

www.sohoware.com

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 SOHOware. 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 SOHOware. If returned by another carrier, the purchaser will pay the difference. A return freight and handling fee will be charged to the purchaser if SOHOware determines that there was "No Problem Found" or that the damage was caused by the user

Warning

SOHOware 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 SOHOware 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 SOHOware be liable for any incidental, consequential, special, or indirect damages resulting from loss of data, loss of profits, or loss of use, even if SOHOware or an authorized SOHOware 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	**:**	**NDC Europe**
Company Address	**:**	**1, Earlsfort Centre,** **Hatch Street,** **Dublin 2, Ireland.**

Person authorized to make this declaration:

Name	**:**	**Changhua Chiang**
Position/Title	**:**	**President & CEO**

March 15, 2001

Date

Legal Signature

Index