

BiGuard 10

iBusiness Security Gateway Small-Office



BiGuard 2

iBusiness Security Gateway Home-Office



www.billion.uk.com

User's Manual

Version Release 3.00 (FW:1.03)

BiGuard 2/10 User's Manual

(Updated January 4, 2007)

Copyright Information

© 2007 Billion Electric Corporation, Ltd.

The contents of this publication may not be reproduced in whole or in part, transcribed, stored, translated, or transmitted in any form or any means, without the prior written consent of Billion Electric Corporation.

Published by Billion Electric Corporation. All rights reserved.

Disclaimer

Billion does not assume any liability arising out of the application of use of any products or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. Billion reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

Mac OS is a registered trademark of Apple Computer, Inc.

Windows 98, Windows NT, Windows 2000, Windows Me and Windows XP are registered trademarks of Microsoft Corporation.

Safety Warnings



Your BiGuard 2/10 is built for reliability and long service life. For your safety, be sure to read and follow the following safety warnings.

- Read this installation guide thoroughly before attempting to set up your BiGuard 2/10.
- Your BiGuard 2/10 is a complex electronic device. DO NOT open or attempt to repair it yourself. Opening or removing the covers can expose you to high voltage and other risks. In the case of malfunction, turn off the power immediately and have it repaired at a qualified service center. Contact your vendor for details.
- Connect the power cord to the correct supply voltage.
- Carefully place connecting cables to avoid people from stepping or tripping on them. DO NOT allow anything to rest on the power cord and DO NOT place the power cord in an area where it can be stepped on.
- DO NOT use BiGuard 2/10 in environments with high humidity or high temperatures.
- DO NOT use the same power source for BiGuard 2/10 as other equipment.
- DO NOT use your BiGuard 2/10 and any accessories outdoors.
- If you mount your BiGuard 2/10, make sure that no electrical, water or gas pipes will be damaged during installation.
- DO NOT install or use your BiGuard 2/10 during a thunderstorm.
- DO NOT expose your BiGuard 2/10 to dampness, dust, or corrosive liquids.
- DO NOT use your BiGuard 2/10 near water.
- Be sure to connect the cables to the correct ports.
- DO NOT obstruct the ventilation slots on your BiGuard 2/10 or expose it to direct sunlight or other heat sources. Excessive temperatures may damage your device.
- DO NOT store anything on top of your BiGuard 2/10.
- Only connect suitable accessories to your BiGuard 2/10.
- Keep packaging out of the reach of children.
- If disposing of the device, please follow your local regulations for the safe disposal of electronic products to protect the environment.

Table of Contents

Chapter 1: Introduction

- 1.1 Overview**
- 1.2 Product Highlights**
 - 1.2.1 Virtual Private Network Support**
 - 1.2.2 Advanced Firewall Security**
 - 1.2.3 Intelligent Bandwidth Management**
- 1.3 Package Contents**
 - 1.3.1 BiGuard 10**
 - 1.3.1.1 Front Panel**
 - 1.3.1.2 Rear Panel**
 - 1.3.1.3 Rack Mounting**
 - 1.3.1.4 Cabling**
 - 1.3.2 BiGuard 2**
 - 1.3.2.1 Front Panel**
 - 1.3.2.2 Rear Panel**
 - 1.3.2.3 Cabling**

Chapter 2: Router Applications

- 2.1 Overview**
- 2.2 Bandwidth Management with QoS**
 - 2.2.1 QoS Technology**
 - 2.2.2 QoS Policies for Different Applications**
 - 2.2.3 Guaranteed / Maximum Bandwidth**
 - 2.2.4 Policy Based Traffic Shaping**
 - 2.2.5 Priority Bandwidth Utilization**
 - 2.2.6 Management by IP or MAC address**
 - 2.2.7 DiffServ (DSCP Marking)**
- 2.3 Virtual Private Networking**
 - 2.3.1 General VPN Setup**
 - 2.3.2 Concentrator**

Chapter 3: Getting Started

- 3.1 Overview**
- 3.2 Before You Begin**
- 3.3 Connecting Your Router**
- 3.4 Configuring PCs for TCP/IP Networking**
 - 3.4.1 Overview – *see CD provided for 3.4.1-3.4.4**
 - 3.4.2 Windows XP**
 - 3.4.2.1 Configuring**
 - 3.4.2.2 Verifying Settings**
 - 3.4.3 Windows 2000**
 - 3.4.3.1 Configuring**
 - 3.4.3.2 Verifying Settings**
 - 3.4.4 Windows 98 / ME**
 - 3.4.4.1 Installing Components**
 - 3.4.4.2 Configuring**
 - 3.4.4.3 Verifying Settings**
- 3.5 Factory Default Settings**
 - 3.5.1 Username and Password**
 - 3.5.2 LAN and WAN Port Addresses**
- 3.6 Information From Your ISP**
 - 3.6.1 Protocols**
 - 3.6.2 Configuration Information**
- 3.7 Web Configuration Interface**

Chapter 4: Router Configuration

4.1 Overview

4.2 Status & Support - *see CD provided for 4.2.1-4.6

4.2.1 ARP Table

4.2.2 Routing Table

4.2.3 Session Table

4.2.4 DHCP Table

4.2.5 IPSec Status

4.2.6 PPTP Status

4.2.7 System Log

4.2.8 IPSec Log

4.3 Quick Start

4.3.1 DHCP

4.3.2 Static IP

4.3.3 PPPoE

4.3.4 PPTP

4.3.5 Big Pond

4.4 Configuration

4.4.1 LAN

4.4.1.1 Ethernet

4.4.1.2 DHCP Server

4.4.2 WAN

4.4.2.1 DHCP

4.4.2.2 Static IP

4.4.2.3 PPPoE

4.4.2.4 PPTP

4.4.2.5 Big Pond

4.4.3 Bandwidth Settings

4.4.4 System

4.4.4.1 Time Zone

4.4.4.2 Remote Access

4.4.4.3 Firmware Upgrade

4.4.4.4 Backup / Restore

4.4.4.5 Restart

4.4.4.6 Password

4.4.4.7 System Log Server

4.4.4.8 E-mail Alert

4.4.5 Firewall

- 4.4.5.1 Packet Filter**
- 4.4.5.2 URL Filter**
- 4.4.5.3 LAN MAC Filter**
- 4.4.5.4 Block WAN Request**
- 4.4.5.5 Intrusion Detection**

4.4.6 VPN

- 4.4.6.1 IPsec**
 - 4.4.6.1.1 IPsec Wizard**
 - 4.4.6.1.2 IPsec Policy**
- 4.4.6.2 PPTP**

4.4.7 QoS

4.4.8 Virtual Server

- 4.4.8.1 DMZ**
- 4.4.8.2 Port Forwarding**

4.4.9 Advanced

- 4.4.9.1 Static Route**
- 4.4.9.2 Dynamic DNS**
- 4.4.9.3 Device Management**

4.5 Save Configuration To Flash

4.6 Logout

Chapter 5: Troubleshooting - *see CD provided

5.1 Basic Functionality

- 5.1.1 Router Won't Turn On**
- 5.1.2 LEDs Never Turn Off**
- 5.1.3 LAN or Internet Port Not On**
- 5.1.4 Forgot My Password**

5.2 LAN Interface

- 5.2.1 Can't Access BiGuard 2/10 from the LAN**
- 5.2.2 Can't Ping Any PC on the LAN**
- 5.2.3 Can't Access Web Configuration Interface**
 - 5.2.3.1 Pop-up Windows**
 - 5.2.3.2 Javascripts**
 - 5.2.3.3 Java Permissions**

5.3 WAN Interface

5.3.1 Can't Get WAN IP Address from the ISP

5.4 ISP Connection

5.5 Problems with Date and Time

5.6 Restoring Factory Defaults

***For Appendix A-H please consult the CD provided**

Appendix A: Product Specifications

A.1 BiGuard 10 Product Specifications

A.2 BiGuard 2 Product Specifications

Appendix B: Customer Support

Appendix C: FCC Interference Statement

Appendix D: Network, Routing, and Firewall Basics

D.1 Network Basics

D.1.1 IP Addresses

D.1.1.1 Netmask

D.1.1.2 Subnet Addressing

D.1.1.3 Private IP Addresses

D.1.2 Network Address Translation (NAT)

D.1.3 Dynamic Host Configuration Protocol (DHCP)

D.2 Router Basics

D.2.1 What is a Router?

D.2.2 Why use a Router?

D.2.3 Routing Information Protocol (RIP)

D.3 Firewall Basics

D.3.1 What is a Firewall?

D.3.1.1 Stateful Packet Inspection

D.3.1.2 Denial of Service (DoS) Attack

D.3.2 Why Use a Firewall?

Appendix E: Virtual Private Networking

E.1 What is a VPN?

E.1.1 VPN Applications

E.2 What is IPSec?

E.2.1 IPSec Security Components

E.2.1.1 Authentication Header (AH)

E.2.1.2 Encapsulating Security Payload (ESP)

E.2.1.3 Security Associations (SA)

E.2.2 IPSec Modes

E.2.3 Tunnel Mode AH

E.2.4 Tunnel Mode ESP

E.2.5 Internet Key Exchange (IKE)

Appendix F: IPSec Logs and Events

F.1 IPSec Log Event Categories

F.2 IPSec Log Event Table

Appendix G: Bandwidth Management with QoS

G.1 Overview

G.2 What is Quality of Service?

G.3 How Does QoS Work?

G.4 Who Needs QoS?

G.4.1 Home Users

G.4.2 Office Users

Appendix H: Router Setup Examples

H.1 VPN Configuration

H.1.1 LAN to LAN

H.1.2 Host to LAN

H.2 VPN Concentrator

H.3 Intrusion Detection

H.4 PPTP Remote Access by Windows XP

H.5 PPTP Remote Access by BiGuard

Chapter 1: Introduction

1.1 Overview

Congratulations on purchasing BiGuard 2/10 Router from Billion. Combining a router with an Ethernet network switch, BiGuard 2/10 is a state-of-the-art device that provides everything you need to get your network connected to the Internet over your Cable or DSL connection quickly and easily. The Quick Start Wizard and DHCP Server will get first-time users up and running with minimal fuss and configuration, while sophisticated Quality of Service (QoS) and traffic management features grant advanced users total control over their network and Internet connection.

This manual illustrates the many features and functions of BiGuard 2/10, and even takes you through the various ways you can apply this versatile device to your home or office. Take the time now to familiarize yourself with BiGuard 2/10.

1.2 Product Highlights

1.2.1 Virtual Private Network Support

BiGuard 2/10 supports comprehensive IPsec VPN protocols for businesses to establish private encrypted tunnels over the Internet to ensure data transmission security among multiple sites, such as a branch office or dial-up connection. Up to 2 simultaneous IPsec VPN connections are possible on BiGuard 2/10, with performance of up to 4Mbps.

1.2.2 Advanced Firewall Security

Aside from intelligent broadband sharing, BiGuard 2/10 offers integrated firewall protection with advanced features to secure your network from outside attacks. Stateful Packet Inspection (SPI) determines if a data packet is permitted to enter the private LAN. Denial of Service (DoS) prevents hackers from interrupting network services via malicious attacks. In addition, BiGuard 2/10 firewall can be configured to alert you via email should your network come under fire, offering both tight network security and peace of mind.

1.2.3 Intelligent Bandwidth Management

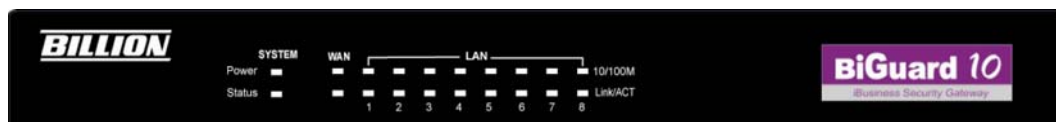
BiGuard 2/10 utilizes Quality of Service (QoS) to give you full control over the priority of both incoming and outgoing data, ensuring that critical data such as customer information moves through your network, even while under a heavy load. Transmission speeds can be throttled to make sure users are not saturating bandwidth required for mission-critical data transfers. Priority types of upload data can also be changed, allowing BiGuard 2/10 to automatically sort out actual speeds for unmatched convenience.

1.3 Package Contents

BiGuard 10

- BiGuard 10 iBusiness Security Gateway Small-Office
- Bracket x 2 (for rack-mounting)
- Screw x 4 (for rack-mounting)
- Getting Started CD-ROM
- Quick Start Guide x 2
- AC-DC Power Adapter (12VDC, 1A)

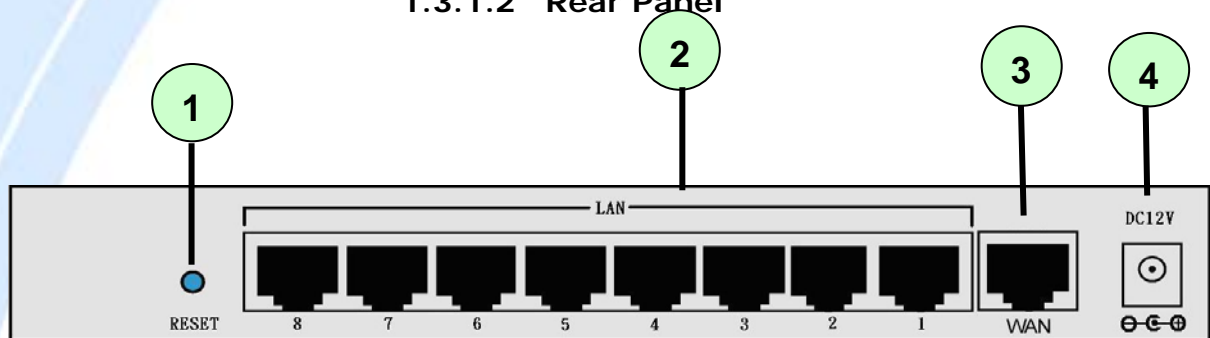
1.3.1.1 Front Panel



LED	Function
Power	A solid light indicates a steady connection to a power source.
Status	A blinking light indicates the device is writing to flash memory.
WAN	Lit when connected to an Ethernet device. 10/100M : Lit green when connected at 100Mbps. Not lit when connected at 10Mbps.

	<p>Link/ACT: Lit when device is connected. Blinking when data is transmitting/receiving.</p>
<p>LAN 1 – 8</p>	<p>Lit when connected to an Ethernet device.</p> <p>10/100M : Lit green when connected at 100Mbps. Not lit when connected at 10Mbps.</p> <p>Link/ACT: Lit when device is connected. Blinking when data is transmitting/receiving.</p>

1.3.1.2 Rear Panel



Port		Meaning
1	RESET	After the device is powered on, press it to reset the device or restore to factory default settings. 0-3 seconds: The Status LED will light 6 seconds above: restore to factory default settings (this is used when you cannot login to the router. E.g. forgot the password)
2	LAN 1X – 8X (RJ-45 connector)	Connect a UTP Ethernet cable (Cat-5 or Cat-5e) to one of the eight LAN ports when connecting to a PC or an office/home network of 10Mbps or 100Mbps.
3	WAN	WAN 10/100M Ethernet port (with auto crossover support); connect xDSL/Cable modem here.
4	DC12V	Connect DC power adapter here.(DC12V Power)

1.3.1.3 Rack Mounting

To rack mount BiGuard 10, carefully secure the device to your rack on both sides using the included brackets and screws. See the diagram below for a more detailed explanation.



1.3.1.4 Cabling

Most Ethernet networks currently use unshielded twisted pair (UTP) cabling. The UTP cable contains eight conductors, arranged in four twisted pairs, and terminated with an RJ45 type connector.

One of the most common causes of networking problems is bad cabling. Make sure that all connected devices are turned on. On the front panel of BiGuard 10, verify that the LAN link and WAN line LEDs are lit. If they are not, check to see that you are using the proper cabling.

BiGuard 2

BiGuard 2 iBusiness Security Gateway Home-Office

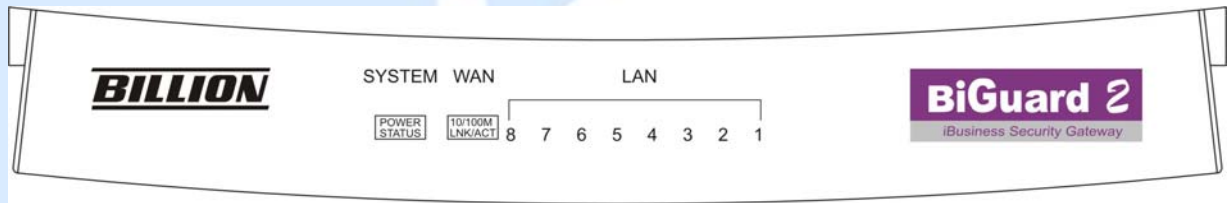
Getting Started CD-ROM

Quick Start Guide x 2

Ethernet (CAT-5 LAN) Cable

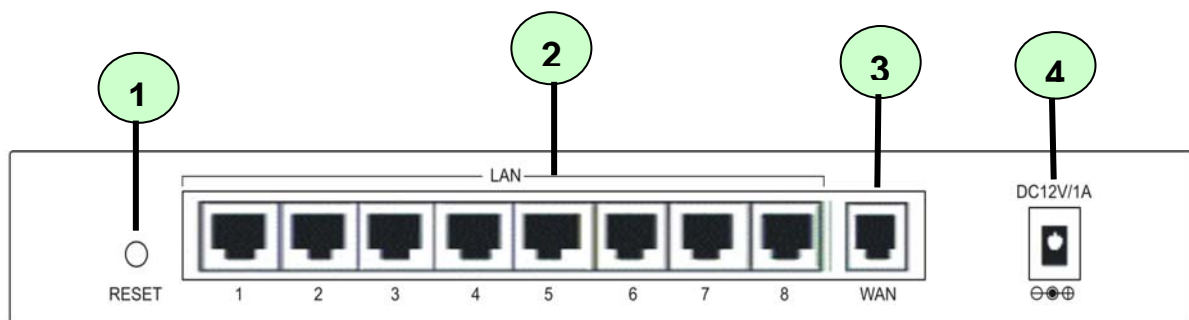
AC-DC Power Adapter (12VDC, 1A)

1.3.2.1 Front Panel



LED	Function
POWER	A solid light indicates a steady connection to a power source.
STATUS	A blinking light indicates the device is writing to flash memory.
WAN	Lit when connected to an Ethernet device. 10/100M : Lit green when connected at 100Mbps. Not lit when connected at 10Mbps. Link/ACT: Lit when device is connected. Blinking when data is transmitting/receiving.
LAN 1 – 8	Lit when connected to an Ethernet device. 10/100M : Lit green when connected at 100Mbps. Not lit when connected at 10Mbps. Link/ACT: Lit when device is connected. Blinking when data is transmitting/receiving.

1.3.2.2 Rear Panel



Port		Meaning
1	RESET	After the device is powered on, press it to reset the device or restore to factory default settings. 0-3 seconds: The Status LED will light 6 seconds above: restore to factory default settings (this is used when you cannot login to the router. E.g. forgot the password)
2	LAN 1X — 8X (RJ-45 connector)	Connect a UTP Ethernet cable (Cat-5 or Cat-5e) to one of the eight LAN ports when connecting to a PC or an office/home network of 10Mbps or 100Mbps.
3	WAN	WAN 10/100M Ethernet port (with auto crossover support); connect xDSL/Cable modem here.
4	DC12V	Connect DC power adapter here.(DC12V Power)

1.3.2.3 Cabling

Most Ethernet networks currently use unshielded twisted pair (UTP) cabling. The UTP cable contains eight conductors, arranged in four twisted pairs, and terminated with an RJ45 type connector.

One of the most common causes of networking problems is bad cabling. Make sure that all connected devices are turned on. On the front panel of BiGuard 2, verify that the LAN link and WAN line LEDs are lit. If they are not, check to see that you are using the proper cabling.

Chapter 2: Router Applications

2.1 Overview

Your BiGuard 2/10 Router is a versatile device that can be configured to not only protect your network from malicious attackers, but also ensure optimal usage of available bandwidth with Quality of Service (QoS). Alternatively, BiGuard 2/10 can also be set to handle secure connections with Virtual Private Networking (VPN).

The following chapter describes how BiGuard 2/10 can work for you.

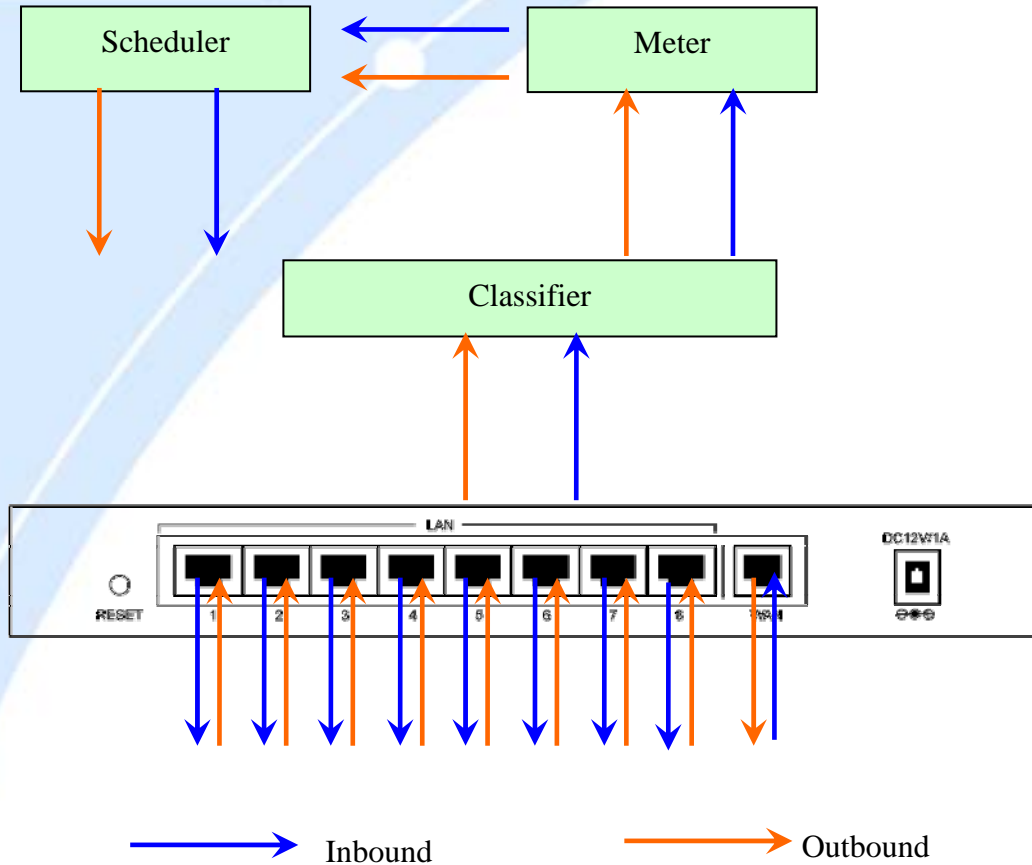
2.2 Bandwidth Management with QoS

Quality of Service (QoS) gives you full control over which types of outgoing data traffic should be given priority by the router. By doing so, the router can ensure that latency-sensitive applications like voice, bandwidth-consuming data like gaming packets, or even mission critical files efficiently move through the router even under a heavy load. You can throttle the speed at which different types of outgoing data pass through the router. In addition, you can simply change the priority of different types of upload data and let the router sort out the actual speeds.

2.2.1 QoS Technology

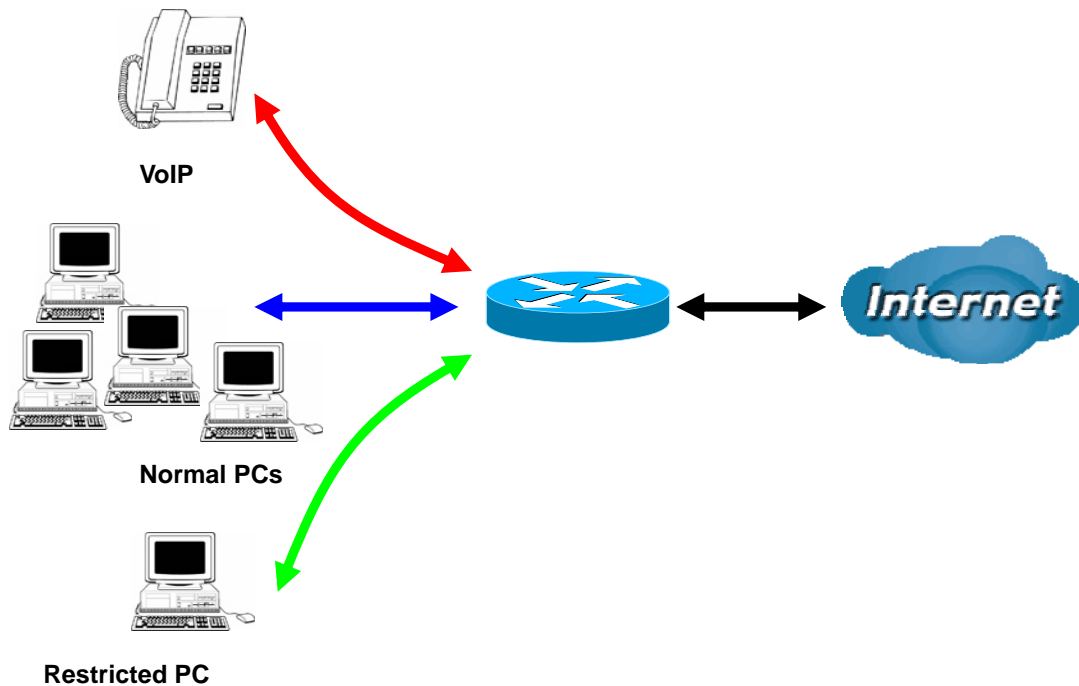
QoS generally involves the prioritization of network traffic. QoS is comprised of three major components: Classifier, Meter, and Scheduler. Each of these components has a distinct role in ensuring that incoming and outgoing data is managed according to user specifications.

The Classifier analyses incoming packets and marks each one according to configured parameters. The Meter communicates the drop priority to the Scheduler and measures the temporal priorities of the output stream against configured parameters. Finally, the Scheduler schedules each packet for transmission based on information from both the Classifier and the Meter.



2.2.2 QoS Policies for Different Applications

By setting different QoS policies according to the applications you are running, you can use BiGuard 2/10 to optimize the bandwidth that is being used on your network.



As illustrated in the diagram above, applications such as Voiceover IP (VoIP) require low network latencies to function properly. If bandwidth is being used by other applications such as an FTP server, users using VoIP will experience network lag and/or service interruptions during use. To avoid this scenario, this network has assigned VoIP with a guaranteed bandwidth and higher priority to ensure smooth communications. The FTP server, on the other hand, has been given a maximum bandwidth cap to make sure that regular service to both VoIP and normal Internet applications is uninterrupted.

2.2.3 Guaranteed / Maximum Bandwidth

Setting a Guaranteed Bandwidth ensures that a particular service receives a minimum percentage of bandwidth. For example, you can configure BiGuard 2/10 to reserve 10% of the available bandwidth for a particular computer on the network to transfer files.

Alternatively you can set a Maximum Bandwidth to restrict a particular application to a fixed percentage of the total throughput. Setting a Maximum Bandwidth of 20% for a file sharing program will ensure that no more than 20% of the available bandwidth will be used for file sharing.

Quality of Service		
Add QoS Rule		
Interface	WAN Outbound	
Application	FTP	
Packet Type	TCP	
Guaranteed	10 %	
Maximum	20 %	
Priority	6 (Lowest)	
DSCP Marking	Disabled	
Address Type	<input checked="" type="radio"/> IP Address <input type="radio"/> MAC Address	
Source IP Address Range	From 192.168.100.1	To 192.168.100.100
Destination IP Address Range	From 0.0.0.0	To 255.255.255.255
Source Port Range	From 1	To 65535
Destination Port Range	From 20	To 21
<input type="button" value="Apply"/>		

2.2.4 Policy Based Traffic Shaping

Policy Based Traffic Shaping allows you to apply specific traffic policies across a range of IP addresses or ports. This is particularly useful for assigning different policies for different PCs on the network. Policy based traffic shaping lets you better manage your bandwidth, providing reliable Internet and network service to your organization.

Quality of Service	
Add QoS Rule	
Interface	WAN Outbound
Application	FTP
Packet Type	TCP
Guaranteed	10 %
Maximum	20 %
Priority	6 (Lowest)
DSCP Marking	Disabled
Address Type	<input checked="" type="radio"/> IP Address <input type="radio"/> MAC Address
Source IP Address Range	From 192.168.100.1 To 192.168.100.100
Destination IP Address Range	From 0.0.0.0 To 255.255.255.255
Source Port Range	From 1 To 65535
Destination Port Range	From 20 To 21
<input type="button" value="Apply"/>	

2.2.5 Priority Bandwidth Utilization

Assigning priority to a certain service allows BiGuard 2/10 to give either a higher or lower priority to traffic from this particular service. Assigning a higher priority to an application ensures that it is processed ahead of applications with a lower priority and vice versa.

Quality of Service

Add QoS Rule

Interface	WAN Outbound		
Application	FTP		
Packet Type	TCP		
Guaranteed	1	%	
Maximum	5	%	
Priority	3 (Normal)		
DSCP Marking	<input type="checkbox"/> 0 (Highest) <input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 (Normal) <input type="checkbox"/> 4 <input checked="" type="checkbox"/> 5 <input type="checkbox"/> 6 (Lowest)		
Address Type	<input type="radio"/> IP Address <input type="radio"/> MAC Address		
Source IP Address Range	100/1	To	192.168.100.100
Destination IP Address Range		To	255.255.255.255
Source Port Range		To	65535
Destination Port Range	From 20	To	21

Apply

2.2.6 Management by IP or MAC address

BiGuard 2/10 can also be configured to apply traffic policies based on a particular IP or MAC address. This allows you to quickly assign different traffic policies to a specific computer on the network.

Quality of Service

Add QoS Rule

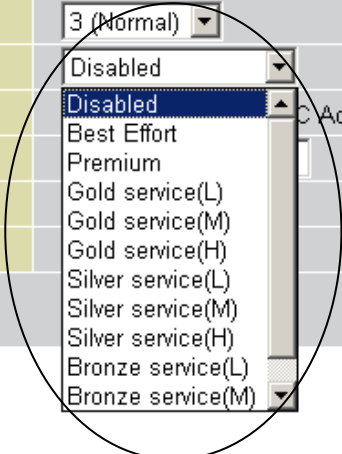
Interface	WAN Outbound		
Application			
Packet Type	Any		
Guaranteed	1	%	
Maximum	100	%	
Priority	0 (Highest)		
DSCP Marking	Disabled		
Address Type	<input type="radio"/> IP Address <input checked="" type="radio"/> MAC Address		
Source MAC Address	11:11:11:11:11:11		
Source Port Range	From	To	
Destination Port Range	From	To	

Apply

2.2.7 DiffServ (DSCP Marking)

DiffServ (a.k.a. DSCP Marking) allows you to classify traffic based on IP DSCP values. These markings can be used to identify traffic within the network. Other interfaces can match traffic based on the DSCP markings. DSCP markings are used to decide how packets should be treated, and is a useful tool to give precedence to varying types of data.

Quality of Service	
Add QoS Rule	
Interface	WAN Outbound
Application	<input type="text"/>
Packet Type	Any
Guaranteed	1 %
Maximum	100 %
Priority	3 (Normal)
DSCP Marking	Disabled
Address Type	<input type="text"/>
Source MAC Address	<input type="text"/>
Source Port Range	To <input type="text"/>
Destination Port Range	To <input type="text"/>
<input type="button" value="Apply"/>	



2.3 Virtual Private Networking

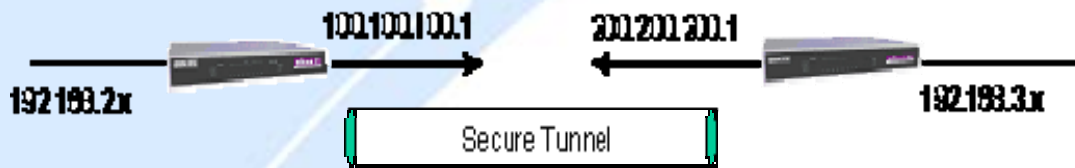
A Virtual Private Network (VPN) enables you to send data between two computers across a shared or public network in a manner that emulates the properties of a point-to-point private link. As such, it is perfect for connecting branch offices to headquarter across the Internet in a secure fashion.

The following section discusses Virtual Private Networking with BiGuard 2/10.

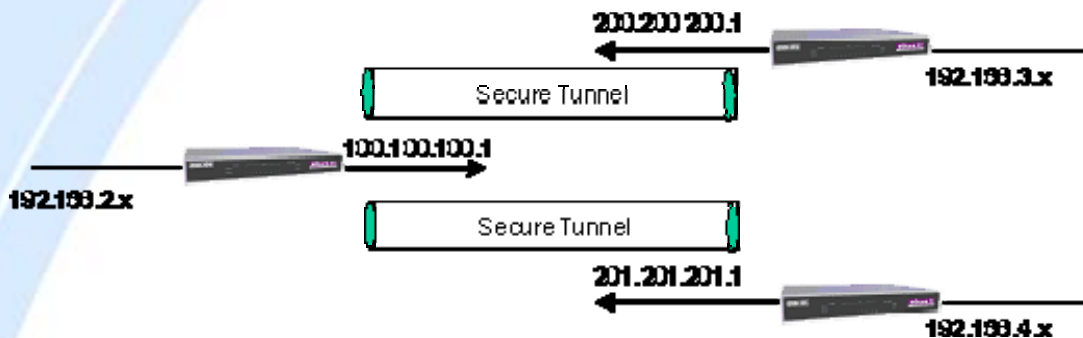
2.3.1 General VPN Setup

There are typically three different VPN scenarios. The first is a **Gateway to Gateway** setup, where two remote gateways communicate over the Internet via a

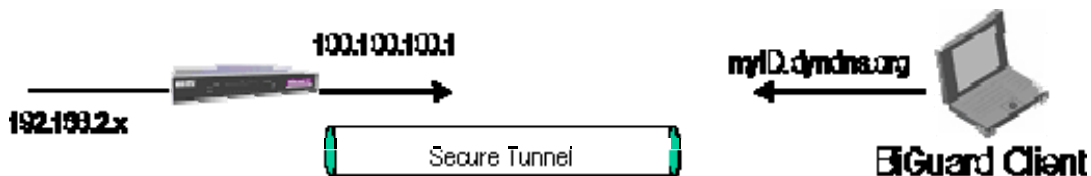
secure tunnel.



The next type of VPN setup is the **Gateway to Multiple Gateway** setup, where one gateway (Headquarter) is communicating with multiple gateways (Branch Offices) over the Internet. As with all VPNs, data is kept secure with secure tunnels.



The final type of VPN setup is the **Client to Gateway**. A good example of where this can be applied is when a remote sales person accesses the corporate network over a secure VPN tunnel.



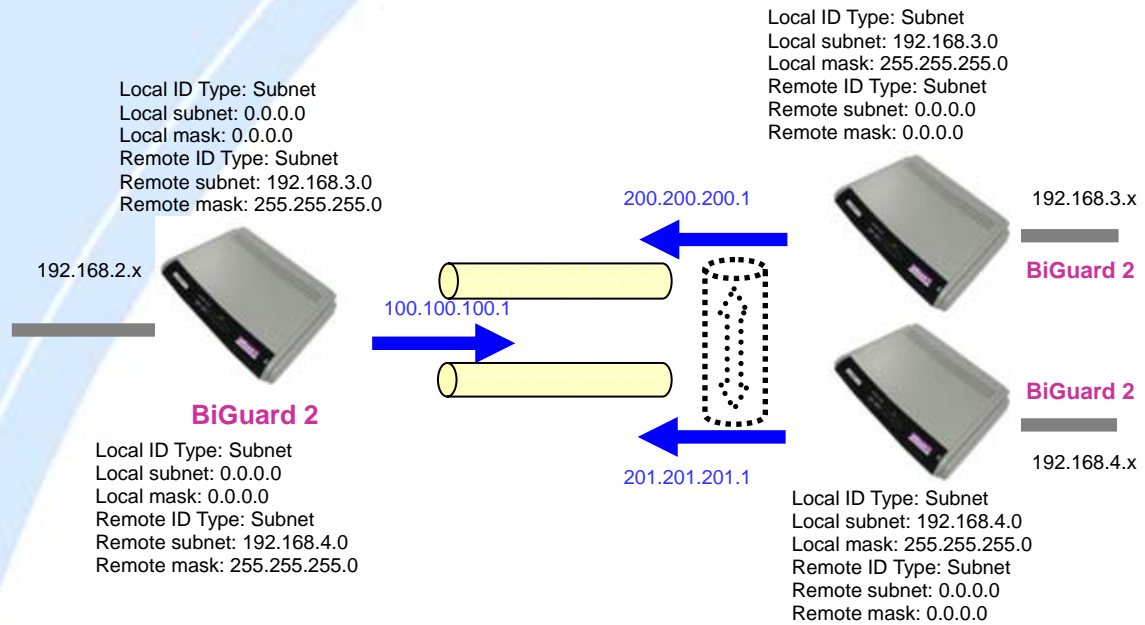
VPN provides a flexible, cost-efficient, and reliable way for companies of all sizes to stay connected. One of the most important steps in setting up a VPN is proper planning. The following sections demonstrate the various ways of using BiGuard 2/10 to setup your VPN.

2.3.2 Concentrator

The VPN Concentrator provides an easy way for branch offices to connect to headquarter through a VPN tunnel. All branch office traffic will be redirected to the VPN tunnel to headquarter with the exception of LAN-side traffic. This way, all branch offices can connect to each other through headquarter via the headquarter's firewall management. You can also configure BiGuard 2/10 to function as a VPN

Concentrator:

Please refer to appendix H for example settings. See CD provided.



Chapter 3: Getting Started

3.1 Overview

BiGuard 2/10 is designed to be a powerful and flexible network device that is also easy to use. With an intuitive web-based configuration, BiGuard 2/10 allows you to administer your network via virtually any Java-enabled web browser and is fully compatible with Linux, Mac OS, and Windows 98/Me/NT/2000/XP operating systems.

The following chapter takes you through the very first steps to configuring your network for BiGuard 2/10. Take a look and see how easy it is to get your network up and running.

3.2 Before You Begin

BiGuard 2/10 is a flexible and powerful networking device. To simplify the configuration process and increase the efficiency of your network, consider the following items before setting up your network for the first time:

1. Plan your network

You may need a fully qualified domain name either for convenience or if you have a dynamic IP address. See Chapter 2: Router Applications for more information.

2. Set up your accounts

Have access to the Internet and locate the Internet Service Provider (ISP) configuration information.

3. Determine your network management approach

BiGuard 2/10 is capable of remote management. However, this feature is not active by default. If you reset the device, remote administration must be enabled again. If you decide to manage your network remotely, be sure to change the default password to something more secure.

4. Prepare to physically connect BiGuard 2/10 to Cable or DSL modems and a computer.

Be sure to also review the Safety Warnings located in the preface of this manual before working with your BiGuard 2/10.

3.3 Connecting Your Router

Connecting BiGuard 2/10 is an easy three-step process:

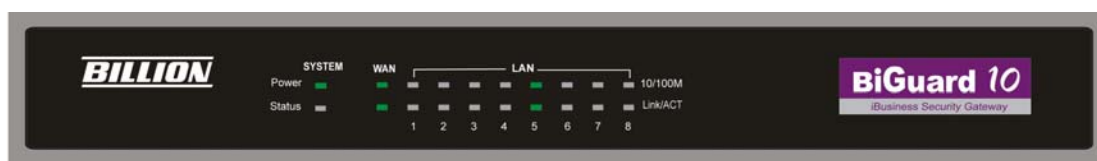
1. Connect BiGuard 2/10 to your LAN by connecting Ethernet cables from your networked PCs to the LAN ports on the router. Connect BiGuard 2/10 to your broadband Internet connection via router's WAN port.



2. Plug BiGuard 2/10 to an AC outlet with the included AC Power Adapter.



3. Ensure that the Power and WAN LEDs are solidly lit, and that on any LAN port that has an Ethernet cable plugged in the LED is also solidly lit. The Status LED will remain solid as the device boots. Once the boot sequence is complete, the LED will shut off, indicating that BiGuard 2/10 is ready.



If the router does not power on, please refer to **Chapter 5: Troubleshooting** on the CD provided for possible solutions.

3.4 Configuring PCs for TCP/IP Networking

Now that your BiGuard 2/10 is connected properly to your network, it's time to configure your networked PCs for TCP/IP networking.

In order for your networked PCs to communicate with your router, they must have the following characteristics:

1. Have a properly installed and functioning Ethernet Network Interface Card (NIC).
2. Be connected to BiGuard 2/10, either directly or through an external repeater hub via an Ethernet cable.
3. Have TCP/IP installed and configured with an IP address.

The IP address for each PC may be a fixed IP address or one that is obtained from a DHCP server. If using a fixed IP address, it is important to remember that it must be in the same subnet as the router. The default IP address of BiGuard 2/10 is 192.168.1.254 with a subnet mask of 255.255.255.0. Using the default configuration, networked PCs must reside in the same subnet, and have an IP address in the range of 192.168.1.1 to 192.168.1.253. However, you'll find that the quickest and easiest way to configure the IP addresses for your PCs is to obtain the IP addresses automatically by using the router as a DHCP server.

If you are unable to access the web configuration interface, check to see if you have any software-based firewalls installed on your PCs, as they can cause problems accessing the 192.168.1.254 IP address of BiGuard 2/10.

The sections 3.4.1 – 3.4.4 outline how to set up your PCs for TCP/IP networking. Please consult 3.4.1 – 3.4.4 in the full manual on the CD provided if necessary and refer to the applicable section for your PC's operating system.

3.5 Factory Default Settings

Before configuring your BiGuard 2/10, you need to know the following default settings:

Web Interface:

Username: admin

Password: admin

LAN Device IP Settings:

IP Address: 192.168.1.254

Subnet Mask: 255.255.255.0

ISP setting in WAN site:

Obtain an IP Address automatically (DHCP Client)

DHCP server:

DHCP server is enabled.

Start IP Address: 192.168.1.100

End IP Address: 192.168.1.199

3.5.1 Username and Password

The default user name and password are "admin" and "admin" respectively.

If you ever forget your user name and/or password, you can restore your BiGuard 2/10 to its factory settings by holding the Reset button on the back of your router until the Status LED begins to blink. Please note that doing this will also erase any previous router settings that you have made. The Status LED will remain solid as the device boots. Once the boot sequence is complete, the LED will shut off, indicating that BiGuard 2/10 is ready.

3.5.2 LAN and WAN Port Addresses

The default values for LAN and WAN ports are shown below:

LAN Port	WAN Port
----------	----------

IP address	192.168.1.254	The DHCP Client is <i>enabled</i> to automatically get the WAN port configuration from the ISP.
Subnet Mask	255.255.255.0	
DHCP server function	Enabled	
IP addresses for distribution to PCs	100 IP addresses continuing from 192.168.1.100 through 192.168.1.199	

3.6 Information From Your ISP

3.6.1 Protocols

Before configuring this device, you have to check with your ISP (Internet Service Provider) to find out what kind of service is provided such as DHCP, Static IP, PPPoE, or PPTP. The following table outlines each of these protocols:

DHCP	Configure this WAN interface to use DHCP client protocol to get an IP address from your ISP automatically. Your ISP provides an IP address to the router dynamically when logging in.
Static IP	Configure this WAN interface with a specific IP address. This IP address should be provided by your ISP.
PPPoE	PPPoE (PPP over Ethernet) is known as a dial-up DSL or cable service. It is designed to integrate the broadband services into the current widely deployed, easy-to-use, and low-cost dial-up-access networking infrastructure.
PPTP	If your ISP provides a PPTP connection, you can use the PPTP protocol to establish a connection to your ISP.
Big Pond	The Big Pond login for Telstra cable in Australia.

If your account uses PPP over Ethernet (PPPoE), you will need to enter your login name and password when configuring your BiGuard 2/10. After the network and

firewall are configured, BiGuard 2/10 will login automatically, and you will no longer need to run the login program from your PC.

3.6.2 Configuration Information

If your ISP does not dynamically assign configuration information but instead uses fixed configurations, you will need the following basic information from your ISP:

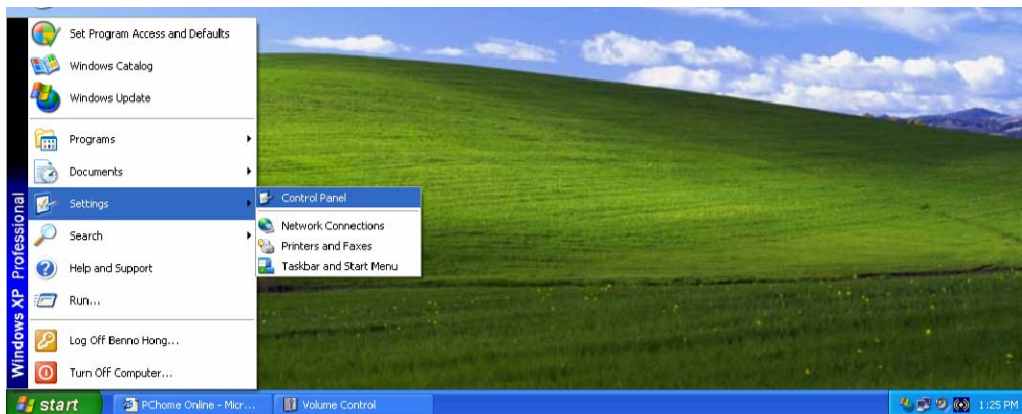
- An IP address and subnet mask
- A gateway IP address
- One or more domain name server (DNS) IP addresses

Depending on your ISP, a host name and domain suffix may also be provided. If any of these items are dynamically supplied by the ISP, your BiGuard 2/10 will automatically acquire them.

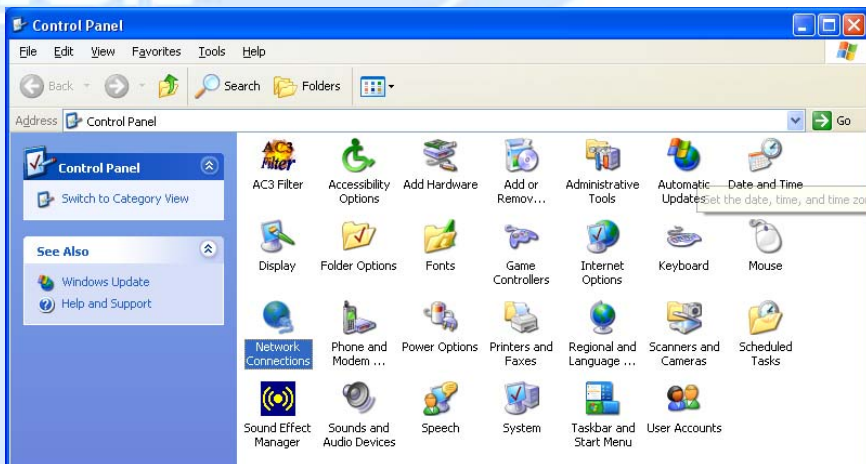
If an ISP technician configured your computer or if you configured it using instructions provided by your ISP, you need to copy the configuration information from your PC's Network TCP/IP Properties window before reconfiguring your computer for use with BiGuard 2/10. The following sections describe how you can obtain this information.

This section uses illustrations from Windows XP. However, other versions of Windows will follow a similar procedure. Have your Windows CD handy, as it may be required during the configuration process.

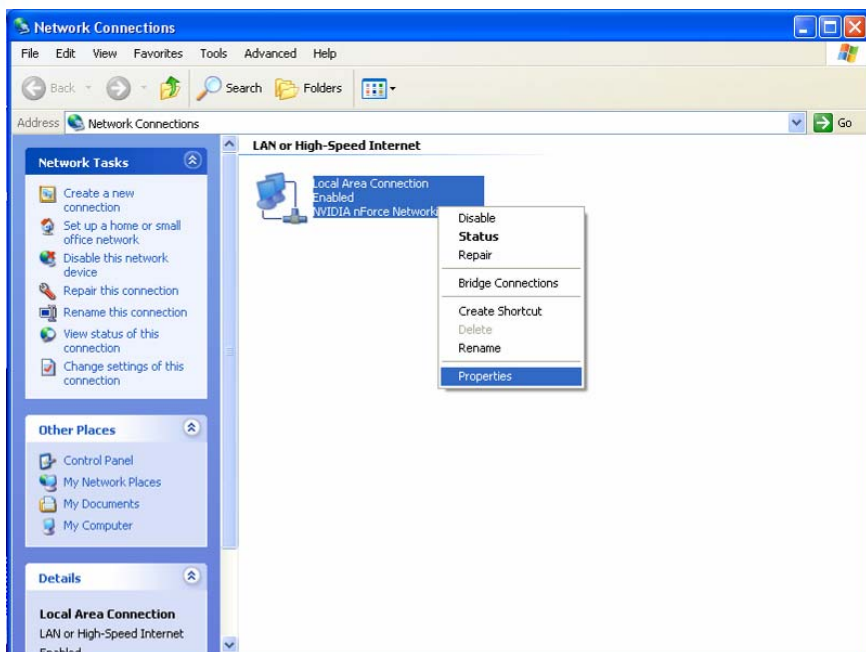
1. Select **Start > Settings > Control Panel**.



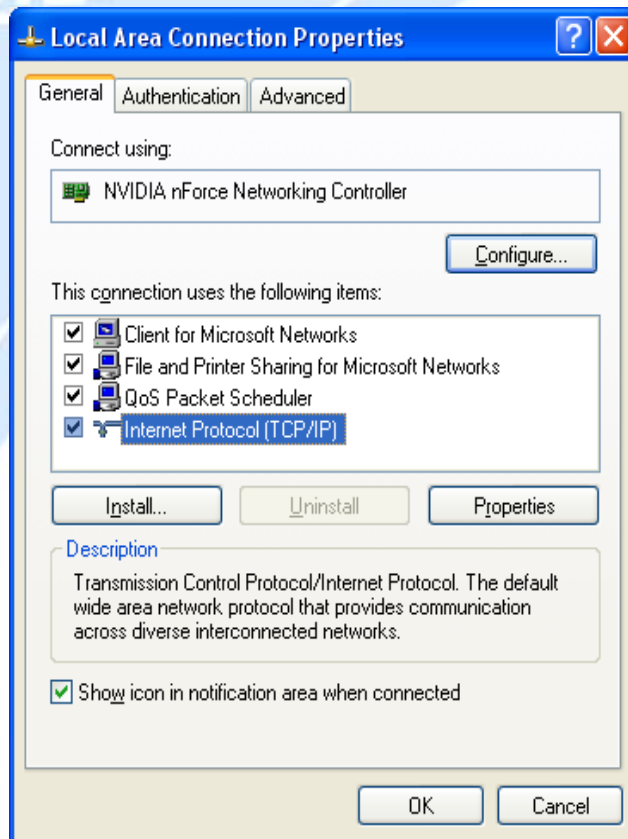
2. Double-click the **Network** icon.



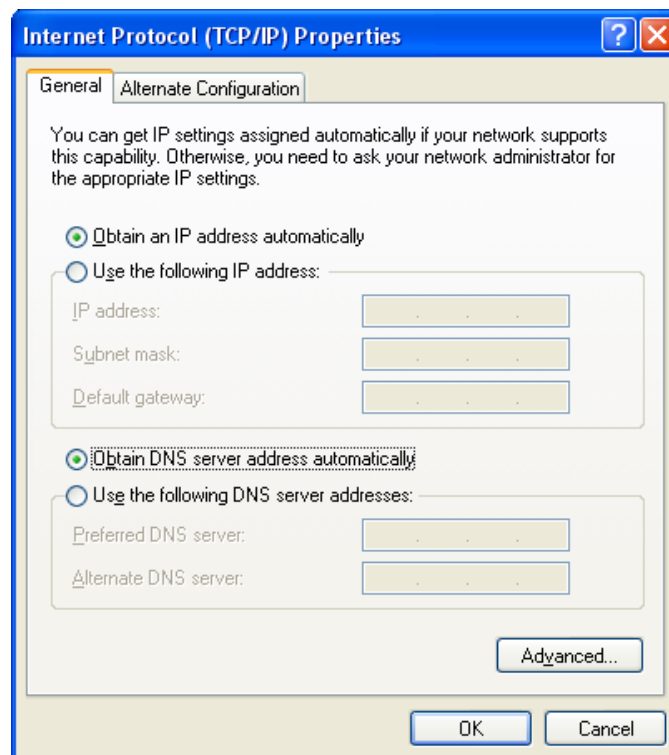
3. In the **Network Connections** window, right-click **Local Area Connection** and select **Properties**.



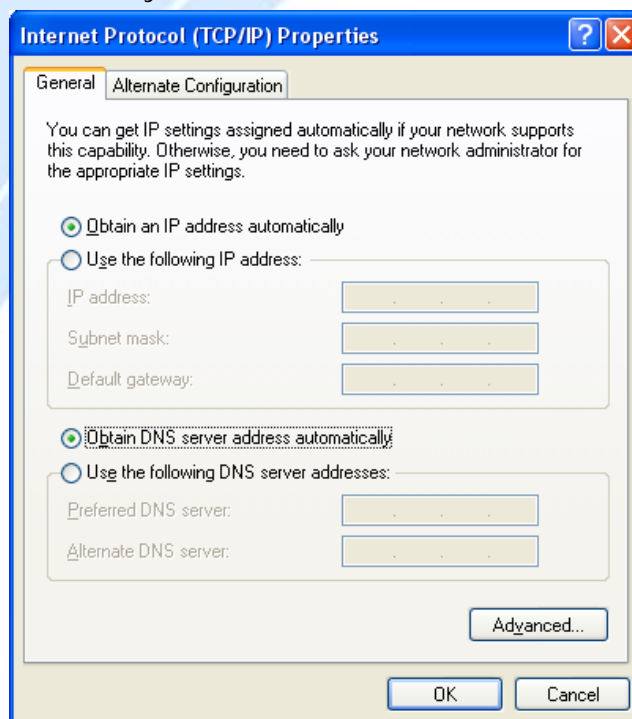
4. Select **Internet Protocol (TCP/IP)** and click **Properties**.



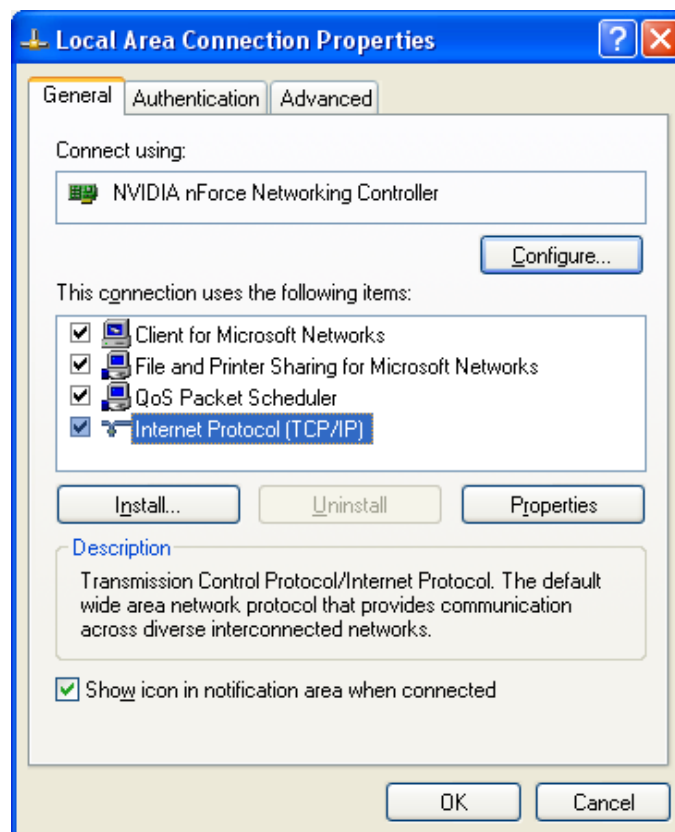
5. If an **IP address**, **subnet mask** and a **Default gateway** are shown, write down the information. If no address is present, your account's IP address is dynamically assigned. **Click the Obtain an IP address automatically** radio button.



6. If any DNS server addresses are shown, write them down. Click the Obtain DNS server address automatically radio button.



7. Click **OK** to save your changes.



3.7 Web Configuration Interface

BiGuard 2/10 includes a Web Configuration Interface for easy administration via virtually any browser on your network. To access this interface, open your web browser, enter the IP address of your router, which by default is 192.168.1.254, and click **Go**. A user name and password window prompt will appear. Enter your user name and password (the default user name and password are "admin" and "admin") to access the Web Configuration Interface.



Enter Network Password

Please type your user name and password.

Site: 192.168.1.254

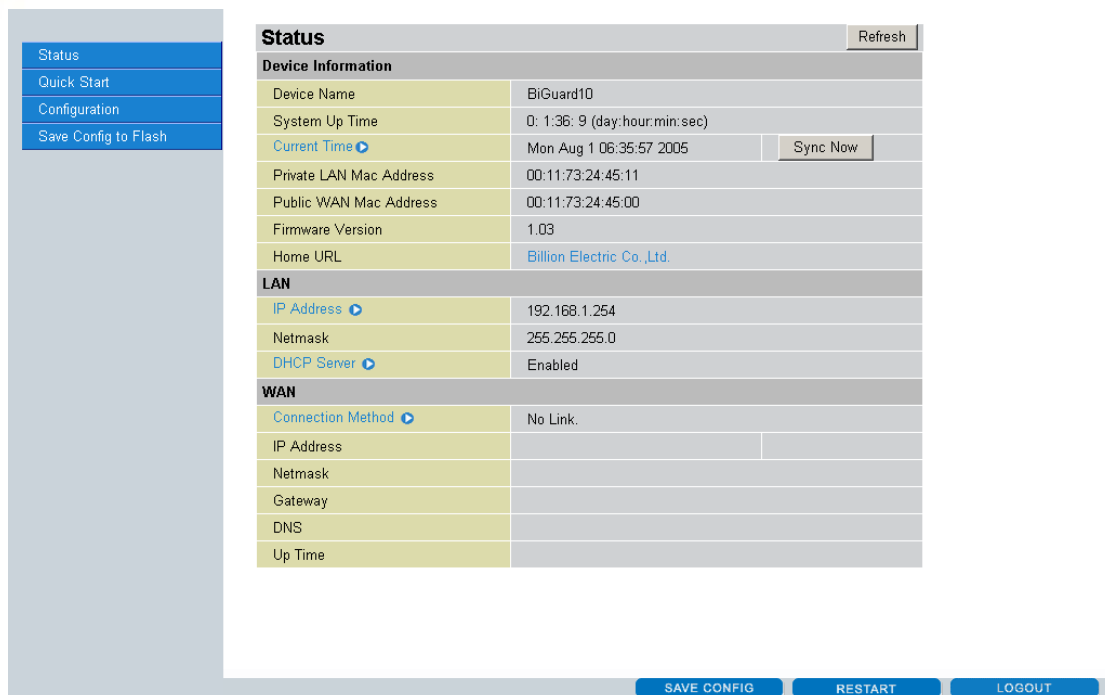
Realm: WebAdmin

User Name: admin

Password: [masked]

Save this password in your password list

OK Cancel



Status

Quick Start

Configuration

Save Config to Flash

Status Refresh

Device Information

Device Name	BiGuard10
System Up Time	0: 1:36: 9 (day:hour:min:sec)
Current Time	Mon Aug 1 06:35:57 2005 Sync Now
Private LAN Mac Address	00:11:73:24:45:11
Public WAN Mac Address	00:11:73:24:45:00
Firmware Version	1.03
Home URL	Billion Electric Co.,Ltd.

LAN

IP Address	192.168.1.254
Netmask	255.255.255.0
DHCP Server	Enabled

WAN

Connection Method	No Link.
IP Address	
Netmask	
Gateway	
DNS	
Up Time	

SAVE CONFIG RESTART LOGOUT

If the Web Configuration Interface appears, congratulations! You are now ready to configure your BiGuard 2/10. If you are having trouble accessing the interface, please refer to **Chapter 5: Troubleshooting** in the manual on the CD provided for possible resolutions.

Chapter 4: Router Configuration

4.1 Overview

The Web Configuration Interface makes it easy for you to manage your network via any PC connected to it. On the Web Configuration homepage, you will see the navigation pane located on the left hand side. From it, you will be able to select various options used to configure your router.

The screenshot displays the 'Status' page of the Billion router's Web Configuration Interface. On the left is a navigation pane with buttons for 'Status', 'Quick Start', 'Configuration', and 'Save Config to Flash'. The main content area is titled 'Status' and includes a 'Refresh' button. It is divided into three sections: 'Device Information', 'LAN', and 'WAN'. The 'Device Information' section lists fields such as Device Name (BiGuard10), System Up Time (0: 1:36: 9), Current Time (Mon Aug 1 06:35:57 2005), Private LAN Mac Address (00:11:73:24:45:11), Public WAN Mac Address (00:11:73:24:45:00), Firmware Version (1.03), and Home URL (Billion Electric Co.,Ltd.). The 'LAN' section shows IP Address (192.168.1.254), Netmask (255.255.255.0), and DHCP Server (Enabled). The 'WAN' section shows Connection Method (No Link) and other fields for IP Address, Netmask, Gateway, DNS, and Up Time. At the bottom of the interface are three buttons: 'SAVE CONFIG', 'RESTART', and 'LOGOUT'.

Status		Refresh
Device Information		
Device Name	BiGuard10	
System Up Time	0: 1:36: 9 (day:hour:min:sec)	
Current Time	Mon Aug 1 06:35:57 2005	Sync Now
Private LAN Mac Address	00:11:73:24:45:11	
Public WAN Mac Address	00:11:73:24:45:00	
Firmware Version	1.03	
Home URL	Billion Electric Co.,Ltd.	
LAN		
IP Address	192.168.1.254	
Netmask	255.255.255.0	
DHCP Server	Enabled	
WAN		
Connection Method	No Link.	
IP Address		
Netmask		
Gateway		
DNS		
Up Time		

1. Click **Apply** if you would like to apply the settings on the current screen to the device. The settings will be effective immediately, however the configuration is not saved yet and the settings will be erased if you power off or restart the device.
2. Click **SAVE CONFIG** to save the current settings permanently to the device.
3. Click **RESTART** to restart the device. There are two options to restart the device.
 - Select **Current Settings** if you would like to restart using the current configuration.
 - Select **Factory Default Settings** if you would like to restart using the factory default configuration.

4. To exit the router's web interface, click **LOGOUT**. Please ensure that you have saved your configuration settings before you logout. Be aware that the router is restricted to only one PC accessing the web configuration interface at a time. Once a PC has logged into the web interface, other PCs cannot gain access until the current PC has logged out. If the previous PC forgets to logout, the second PC can access the page after a user-defined period (5 minutes by default).

The following sections will show you how to configure your router using the Web Configuration Interface.

4.2 Status

The Status menu displays the various options that have been selected and a number of statistics about your BiGuard 2/10. In this menu, you will find the following sections. **Please consult the full manual on the CD provided for detailed configuration, 4.2.1-4.6.**

- ARP Table
- Routing Table
- Session Table
- DHCP Table
- IPSec Status
- PPTP Status
- System Log
- IPSec Log

Status		Refresh
Device Information		
Device Name	BiGuard10	
System Up Time	0: 1:36: 9 (day:hour:min:sec)	
Current Time	Mon Aug 1 06:35:57 2005	Sync Now
Private LAN Mac Address	00:11:73:24:45:11	
Public WAN Mac Address	00:11:73:24:45:00	
Firmware Version	1.03	
Home URL	Billion Electric Co.,Ltd.	
LAN		
IP Address	192.168.1.254	
Netmask	255.255.255.0	
DHCP Server	Enabled	
WAN		
Connection Method	No Link.	
IP Address		
Netmask		
Gateway		
DNS		
Up Time		

Support

Telephone Support for Internet Access **ONLY** is available during office hours from Mon-Fri 10am–5pm on 0870-8501528. If you are successfully connected to the Internet and have a support query please contact www.billion.uk.com/esupport and submit a ticket.



This symbol on the product or in the instructions means that your electrical and electronic equipment should be disposed at the end of its life separately from your household waste.

There are separate collection systems for recycling in the EU.

For more information please contact the local authority or your retailer where you purchased the product.

BILLION

BILLION