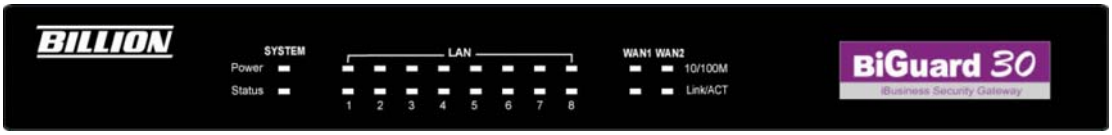
BiGuard 30

iBusiness Security Gateway SMB



www.billion.uk.com

User's Manual

Version Release 5.00 (FW:1.03)

BiGuard 30 User's Manual

(Updated July 4, 2007)

Copyright Information

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 30 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 30.
- Your BiGuard 30 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 30 in environments with high humidity or high temperatures.
- DO NOT use the same power source for BiGuard 30 as other equipment.
- DO NOT use your BiGuard 30 and any accessories outdoors.
- If you wall mount your BiGuard 30, make sure that no electrical, water or gas pipes will be damaged during installation.
- DO NOT install or use your BiGuard 30 during a thunderstorm.
- DO NOT expose your BiGuard 30 to dampness, dust, or corrosive liquids.
- DO NOT use your BiGuard 30 near water.
- Be sure to connect the cables to the correct ports.
- DO NOT obstruct the ventilation slots on your BiGuard 30 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 30.
- Only connect suitable accessories to your BiGuard 30.
- 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 3: Getting Started

Chapter 4: Router Configuration

4.3 Quick Start

4.4 Configuration

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

Appendix A: 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 Why use a Router?

D.2.2 What is a Router?

D.2.3 Routing Information Protocol (RIP)

D.3 Firewall Basics

D.3.1 What is a Firewall?

D.3.2.1 Stateful Packet Inspection

D.3.2.2 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)

Chapter 1: Introduction

1.1 Overview

Congratulations on purchasing BiGuard 30 Router from Billion. Combining a router with an Ethernet network switch, BiGuard 30 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 Load Balancing features grant advanced users total control over their network and Internet connection.

This manual illustrates the many features and functions of BiGuard 30, 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 30.

1.2 Product Highlights

1.2.1 Increased Bandwidth, Scalability and Resilience

With integrated Dual WAN ports, BiGuard 30 combines two broadband lines such as DSL or Cable into one Internet connection, providing optimal bandwidth sharing for multiple PCs on your network, or allowing maximum reliability with network redundancy. Load Balancing enables BiGuard 30 to efficiently balance network traffic across two connections, ideal for small-to-medium businesses that require increased bandwidth, network scalability, and resilience for mission-critical network and Internet applications. Auto failover can also be configured to ensure smooth, continuous service should one connection fail, providing maximum business uptime and productivity, plus uninterrupted service for you and your customers.

1.2.2 Virtual Private Network Support

BiGuard 30 supports comprehensive IPSec & PPTP 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. IPSec VPN is up to 30 simultaneous IPSec VPN connections are possible on BiGuard 30, with performance of up to 30Mbps. PPTP VPN is up to 4 simultaneous PPTP VPN

connections are possible on BiGuard 30, with performance of up to 10Mbps.

1.2.3 Advanced Firewall Security

Aside from intelligent broadband sharing, BiGuard 30 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 30 firewall can be configured to alert you via email should your network come under fire, offering both tight network security and peace of mind.

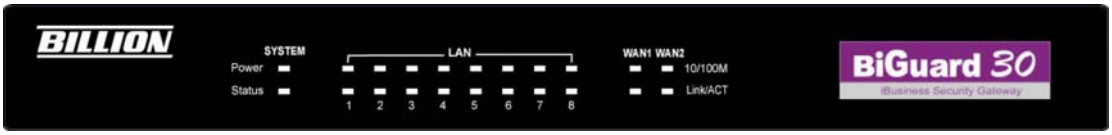
1.2.4 Intelligent Bandwidth Management

BiGuard 30 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 30 to automatically sort out actual speeds for unmatched convenience.

1.3 Package Contents

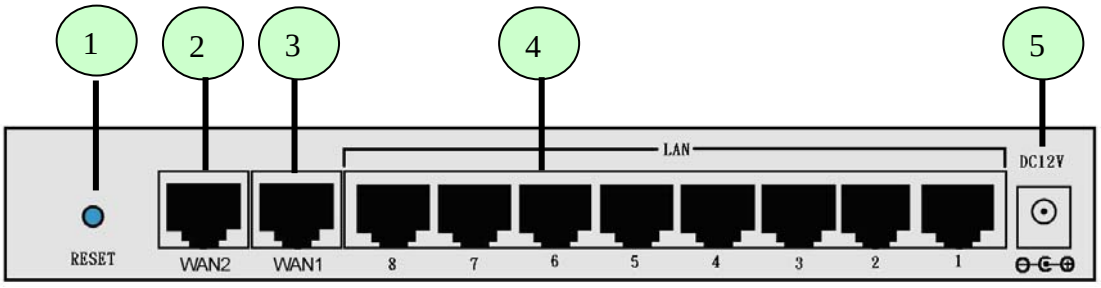
BiGuard 30 iBusiness Security Gateway SMB
Bracket x 2 (for rack-mounting)
Screw x 4 (for rack-mounting)
Getting Started CD-ROM
Quick Start Guide x 2
AC-DC Power Adapter (12VDC, 1A)

1.3.1 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.
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.
WAN1	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.
WAN2	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 Rear Panel



Port		Function
1	RESET	To reset the device and restore factory default settings, after the device is fully booted, press and hold RESET until the Status LED begins to blink.
2	WAN2	WAN2 10/100M Ethernet port (with auto crossover support); connect xDSL/Cable modem here.
3	WAN1	WAN1 10/100M Ethernet port (with auto crossover support); connect xDSL/Cable modem here.
4	LAN 1 — 8	Connect a UTP Ethernet cable (Cat-5 or Cat-5e) to one of the eight LAN ports when connecting a PC to the network.
5	DC12V	Connect DC Power Adapter here. (12VDC)

1.3.3 Rack Mounting

To rack mount BiGuard 30, 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.

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 30, 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 30 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) and both Inbound and Outbound Load Balancing. Alternatively, BiGuard 30 can also be set to redirect incoming and outgoing network traffic with the Fail Over capability, ensuring minimal downtime and increased reliability.

The following chapter describes how BiGuard 30 can work for you.

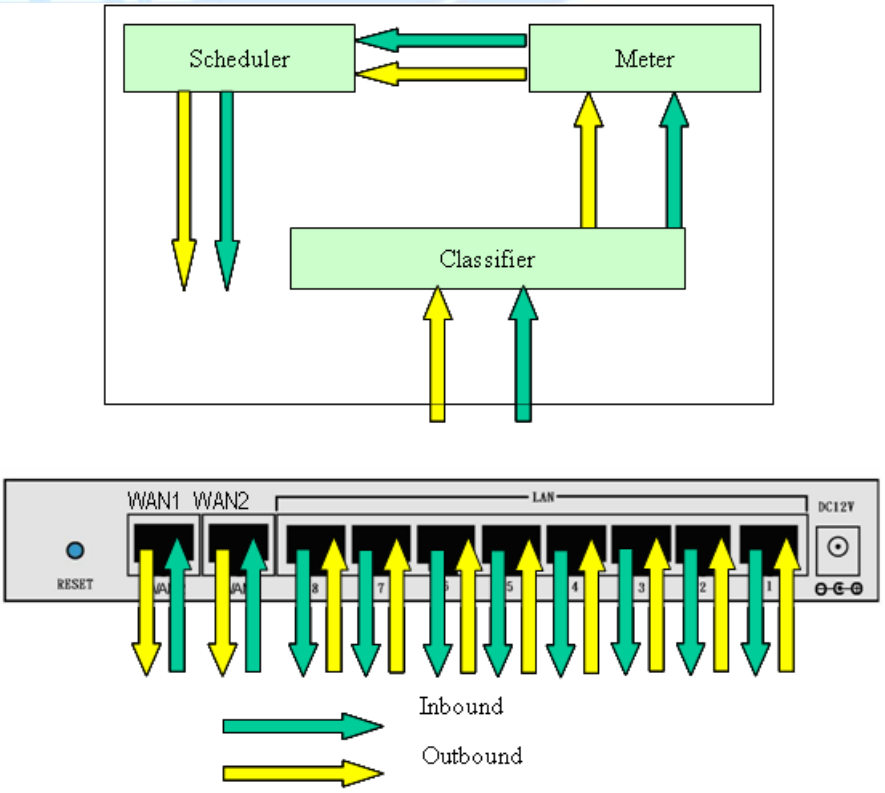
2.2 Bandwidth Management with QoS

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

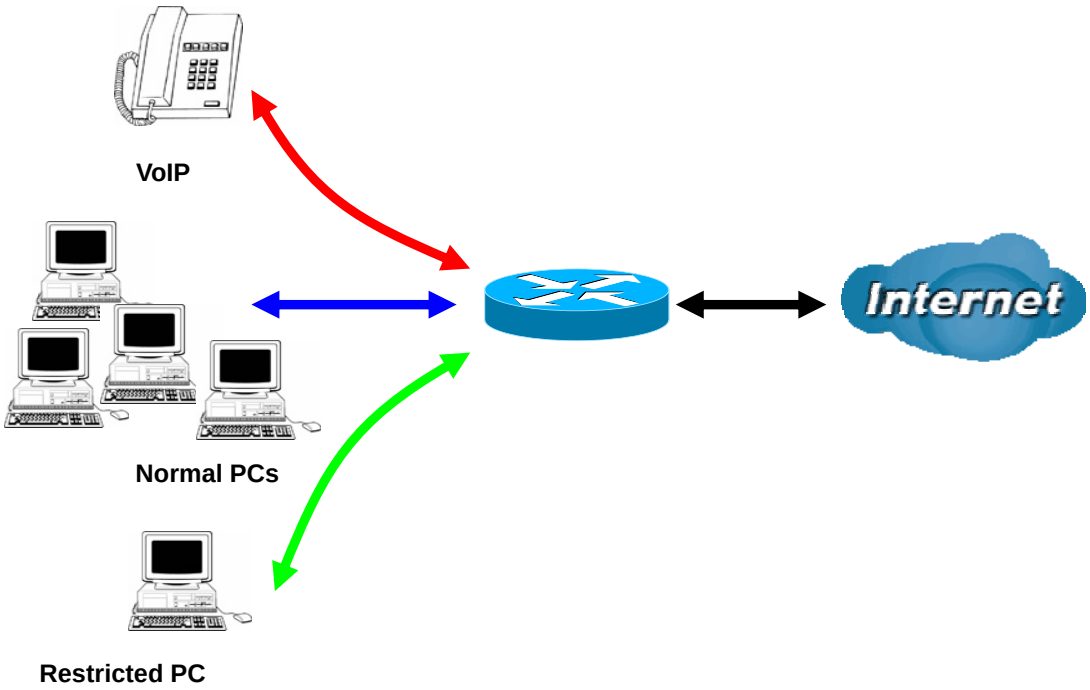
QoS generally involves the prioritization of network traffic. QoS is comprised of three major components: Classifier, Meter, and Scheduler. Each of these components has a distinct role in ensuring that incoming and outgoing data is managed according to user specifications.

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 30 to optimize the bandwidth that is being used on your network.



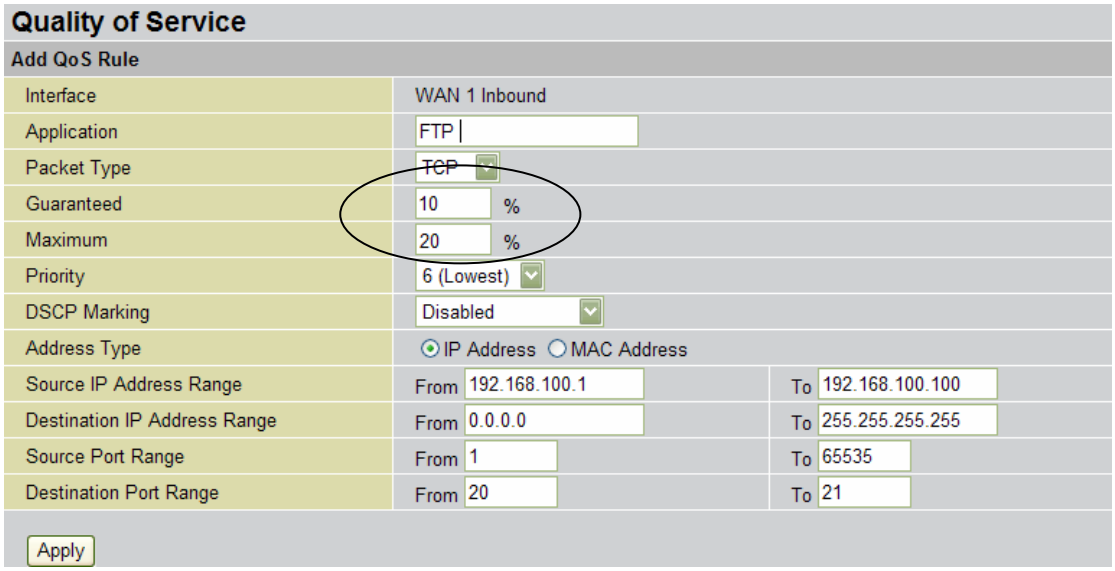
As illustrated in the diagram above, applications such as Voiceover IP (VoIP) require

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 30 to reserve 10% of the available bandwidth for a particular computer on the network to transfer files.

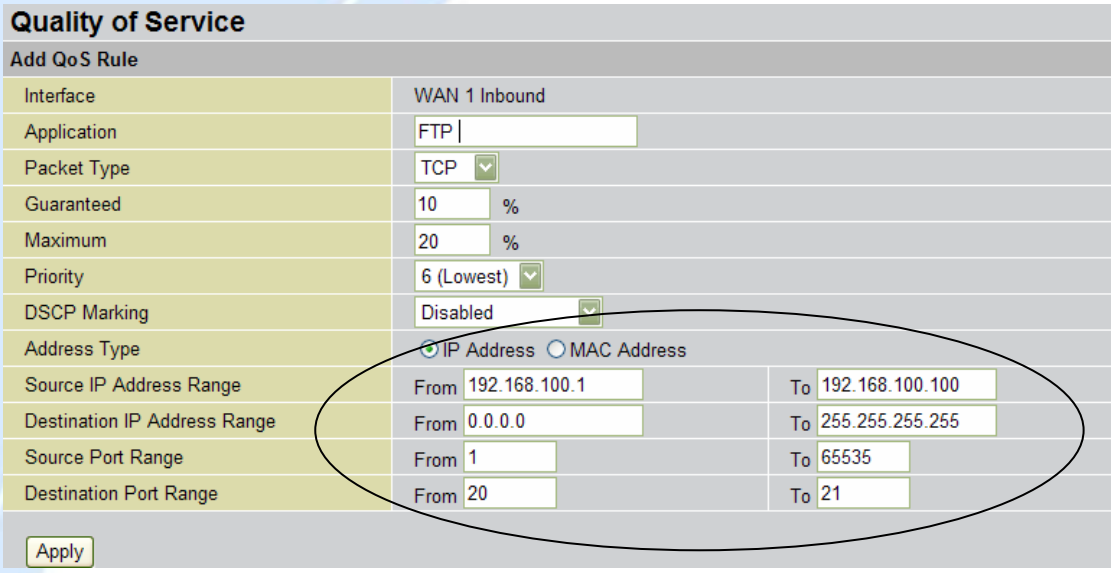
Alternatively you can set a Maximum Bandwidth to restrict a particular application to a fixed percentage of the total throughput. Setting a Maximum Bandwidth of 20% for a file sharing program will ensure that no more than 20% of the available bandwidth will be used for file sharing.



2.2.4 Policy Based Traffic Shaping

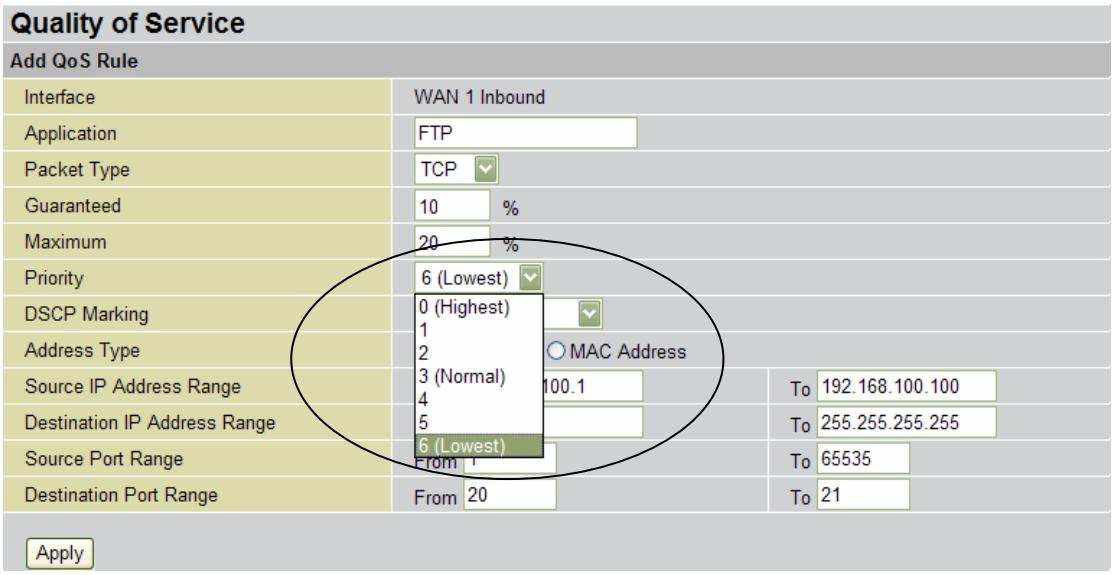
Policy Based Traffic Shaping allows you to apply specific traffic policies across a range of IP addresses or ports. This is particularly useful for assigning different policies for different PCs on the network. Policy based traffic shaping lets you better

manage your bandwidth, providing reliable Internet and network service to your organization.



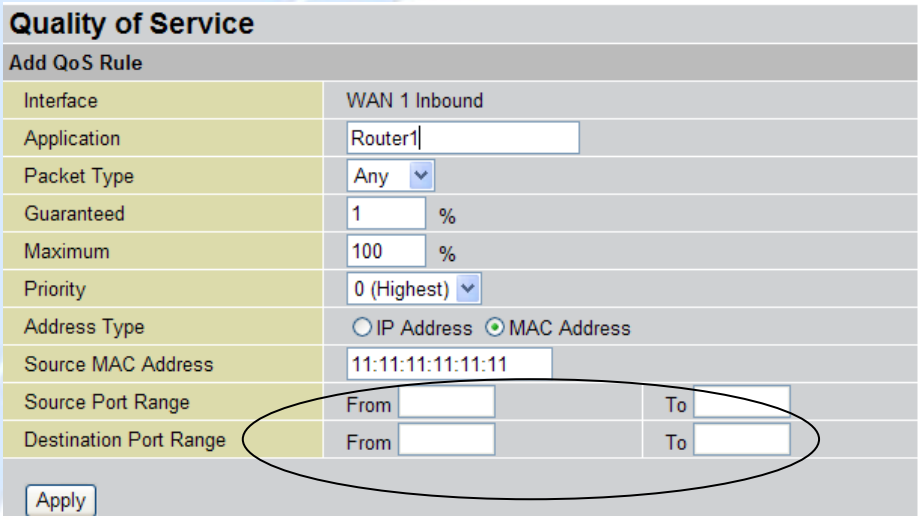
2.2.5 Priority Bandwidth Utilization

Assigning priority to a certain service allows BiGuard 30 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.



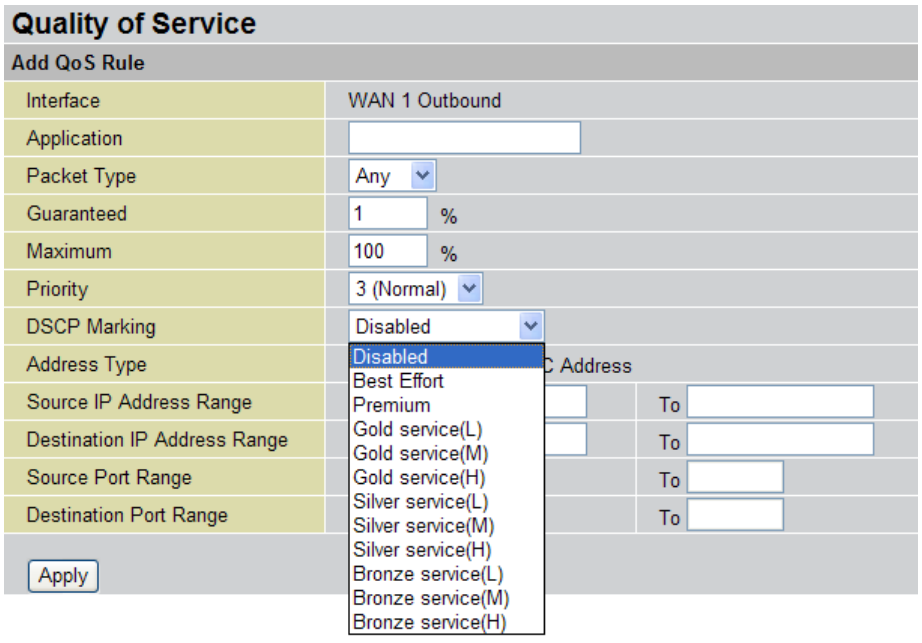
2.2.6 Management by IP or MAC address

BiGuard 30 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.



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.

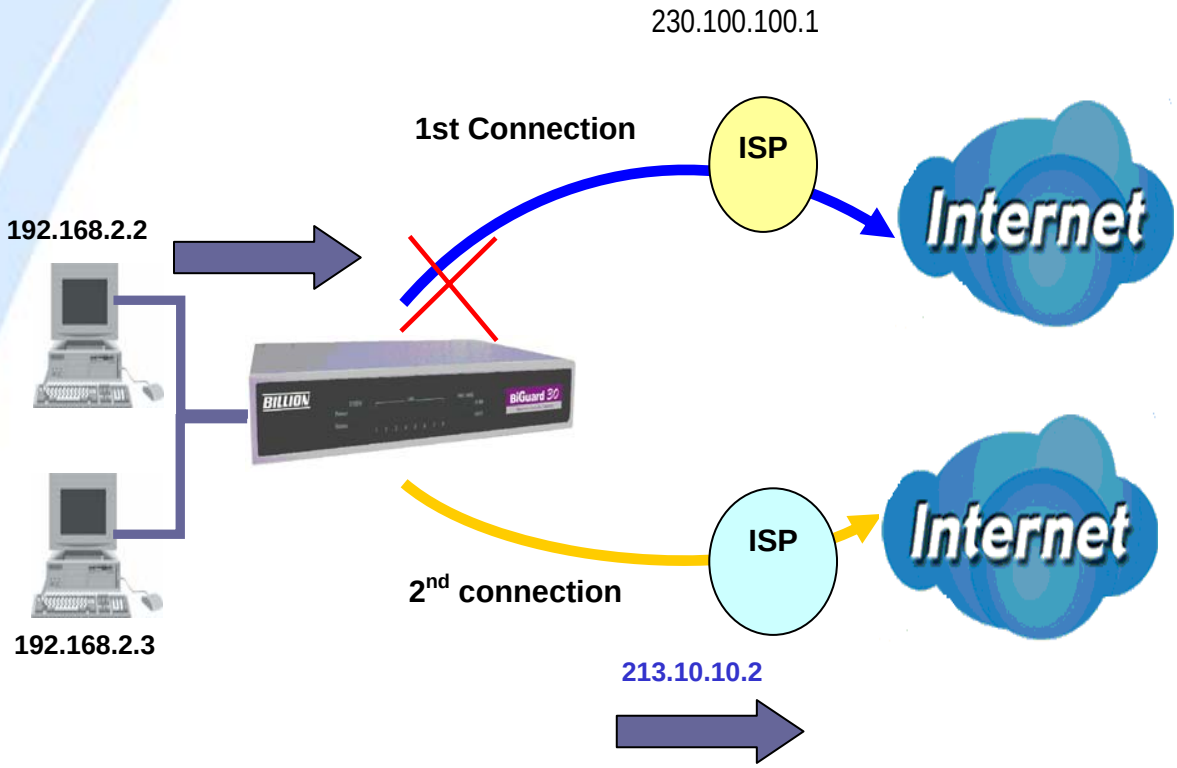


2.3 Outbound Traffic

This section outlines some of the ways you can use BiGuard 30 to manage outbound traffic.

2.3.1 Outbound Fail Over

Configuring BiGuard 30 for Outbound Fail Over allows you to ensure that outgoing traffic is uninterrupted by having BiGuard 30 default to WAN2 should WAN1 fail.

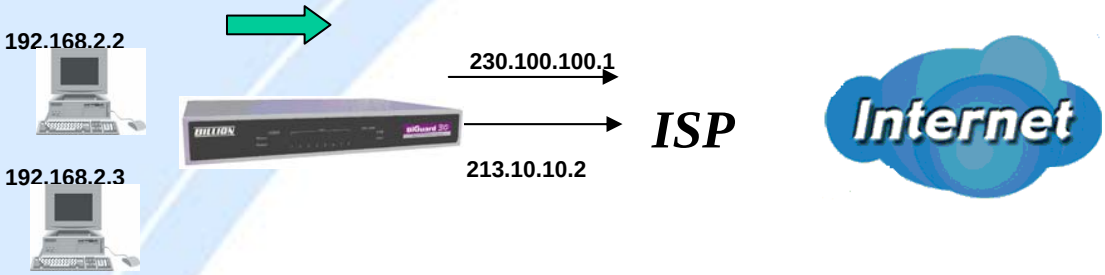


In the above example, PC 1 (IP_192.168.2.2) and PC 2 (IP_192.168.2.3) are connected to the Internet via WAN1 (IP_230.100.100.1) on BiGuard 30. Should WAN1 fail, Outbound Fail Over tells BiGuard 30 to reroute outgoing traffic to WAN2 (IP_213.10.10.2). Configuring your BiGuard 30 for Outbound Fail Over provides a more reliable connection for your outgoing traffic.

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

2.3.2 Outbound Load Balancing

Outbound Load Balancing allows BiGuard 30 to intelligently manage outbound traffic based on the amount of load of each WAN connection.



In the above example, PC 1 (IP_192.168.2.2) and PC 2 (IP_192.168.2.3) are connected to the Internet via WAN1 (IP_230.100.100.1) and WAN2 (IP_213.10.10.2) on BiGuard 30. You can configure BiGuard 30 to balance the load of each WAN port with one of two mechanisms:

1. Session (by session/by traffic/weight of link capability)
2. IP Hash (by traffic/weight of link capability)

The IP Hash mechanism will ensure that the traffic from the same source IP address and destination IP address will go through the same WAN port. This is useful for some server applications that need to identify the source IP address of the client.

By balancing the load between WAN1 and WAN2, your BiGuard 30 can ensure that outbound traffic is efficiently handled by making sure that both ports are equally sharing the load, preventing situations where one port is completely saturated by outbound traffic.

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

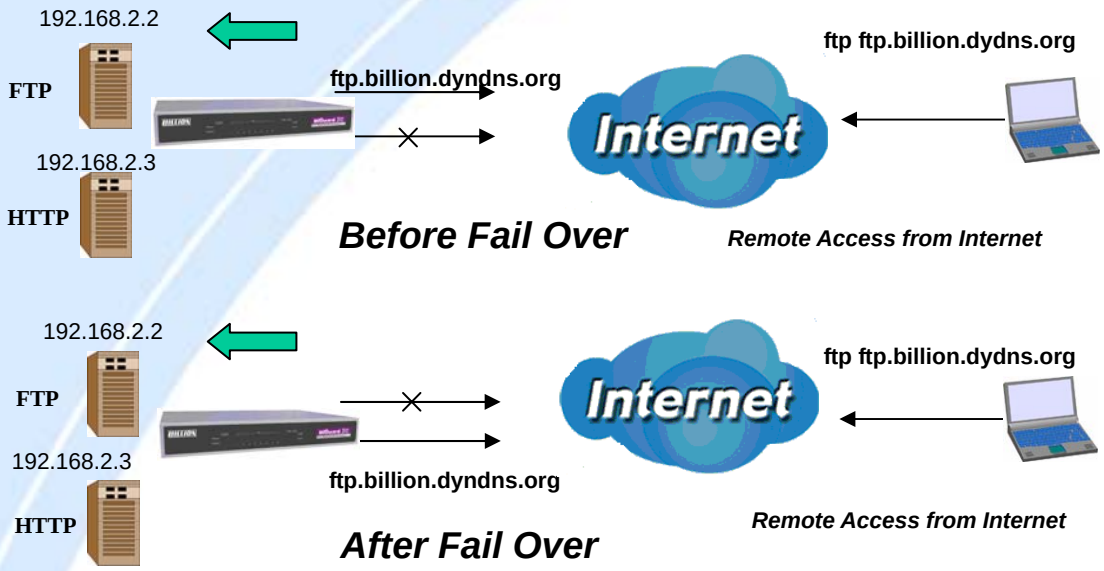
2.4 Inbound Traffic

Learn how BiGuard 30 can handle inbound traffic in the following section.

2.4.1 Inbound Fail Over

Configuring BiGuard 30 for Inbound Fail Over allows you to ensure that incoming

traffic is uninterrupted by having BiGuard 30 default to WAN2 should WAN1 fail.



In the above example, an FTP Server (IP_192.168.2.2) and an HTTP Server (IP_192.168.2.3) are connected to the Internet via WAN1 (ftp.billion.dyndns.org) on BiGuard 30. A remote computer is trying to access these servers via the Internet. Under normal circumstances, the remote computer will gain access to the network via WAN1. Should WAN1 fail, Inbound Fail Over tells BiGuard 30 to reroute incoming traffic to WAN2 by using the Dynamic DNS mechanism. Configuring your BiGuard 30 for Inbound Fail Over provides a more reliable connection for your incoming traffic.

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

2.4.2 Inbound Load Balancing

Inbound Load Balancing allows BiGuard 30 to intelligently manage inbound traffic based on the amount of load of each WAN connection.

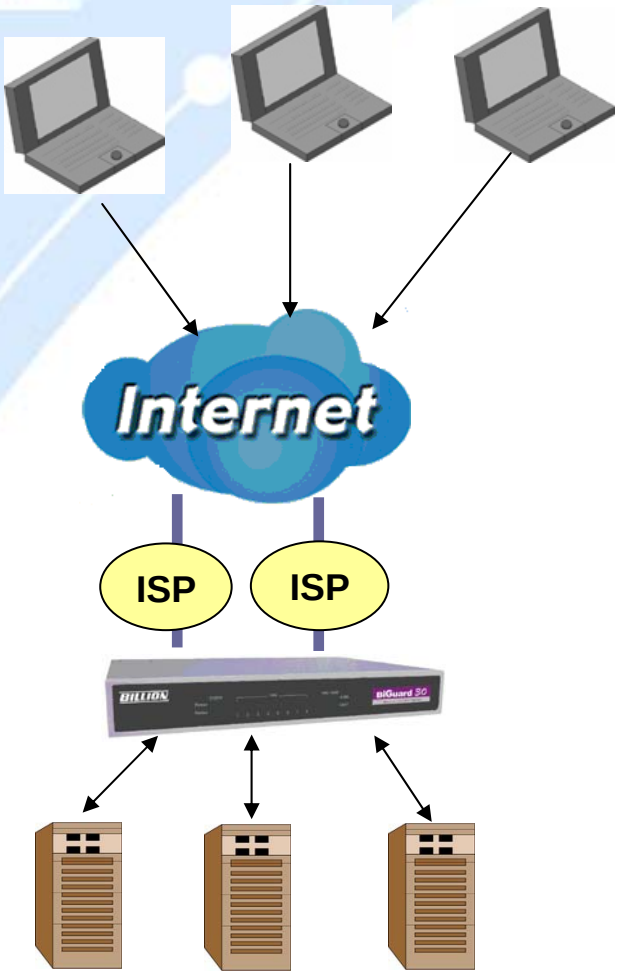
Remote Access from Internet

In the above example, an FTP server (IP_192.168.2.2) and an HTTP server (IP_192.168.2.3) are connected to the Internet via WAN1 (www.billion2.dyndns.org) and WAN2 (www.billion3.dyndns.org) on BiGuard 30. Remote PCs are attempting to access the servers via the Internet. Using Inbound Load Balancing, BiGuard 30 can direct incoming requests to the correct WAN port based on group assignment. For example, a sales force can be directed to www.billion2.dyndns.org, while the R&D group can access www.billion3.dyndns.org. By balancing the load between WAN1 and WAN2, your BiGuard 30 can ensure that inbound traffic is efficiently handled with both ports equally sharing the load, preventing situations where service is slow because one port is completely saturated by inbound traffic.

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

2.5 DNS Inbound

Using DNS Inbound is a great way to intelligently direct network traffic.

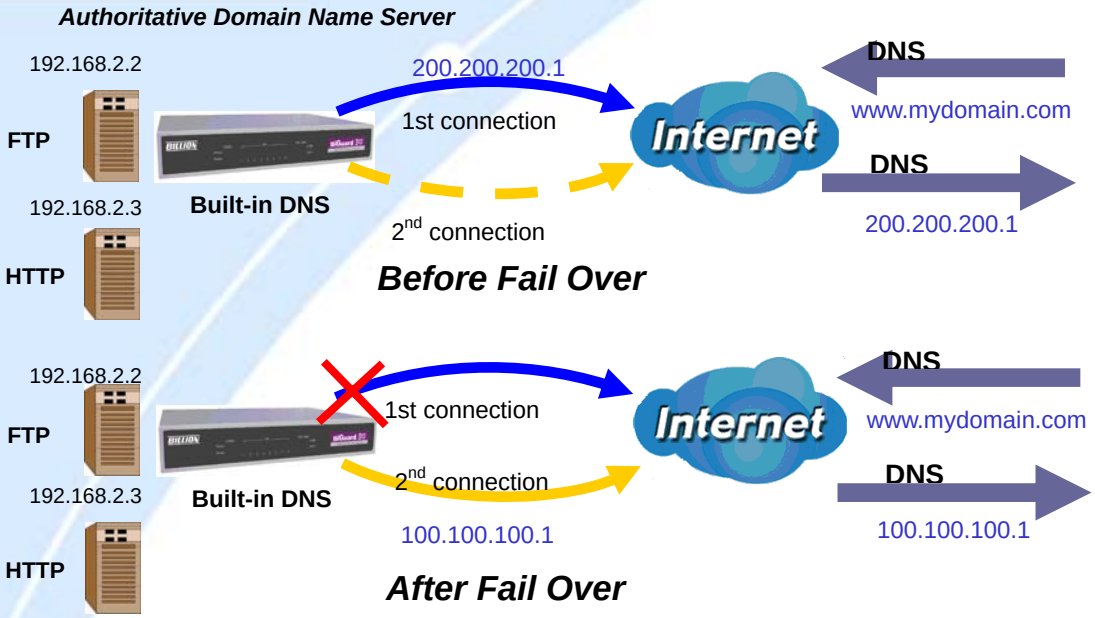


DNS Inbound is a three step process. First, a DNS request is made to the router via a remote PC. BiGuard 30, based on settings specified by the user, will direct the requesting PC to the correct WAN port by replying the selected WAN IP address through the built-in DNS server. The remote PC then accesses the network via the specified WAN port. How BiGuard 30 directs this traffic through the built-in DNS server depends on whether it is configured for Fail Over or Load Balancing.

Learn how to make DNS Inbound on BiGuard 30 work for you in the following section.

2.5.1 DNS Inbound Fail Over

BiGuard 30 can be configured to reply the WAN2 IP address for the DNS domain name request should WAN1 fail.

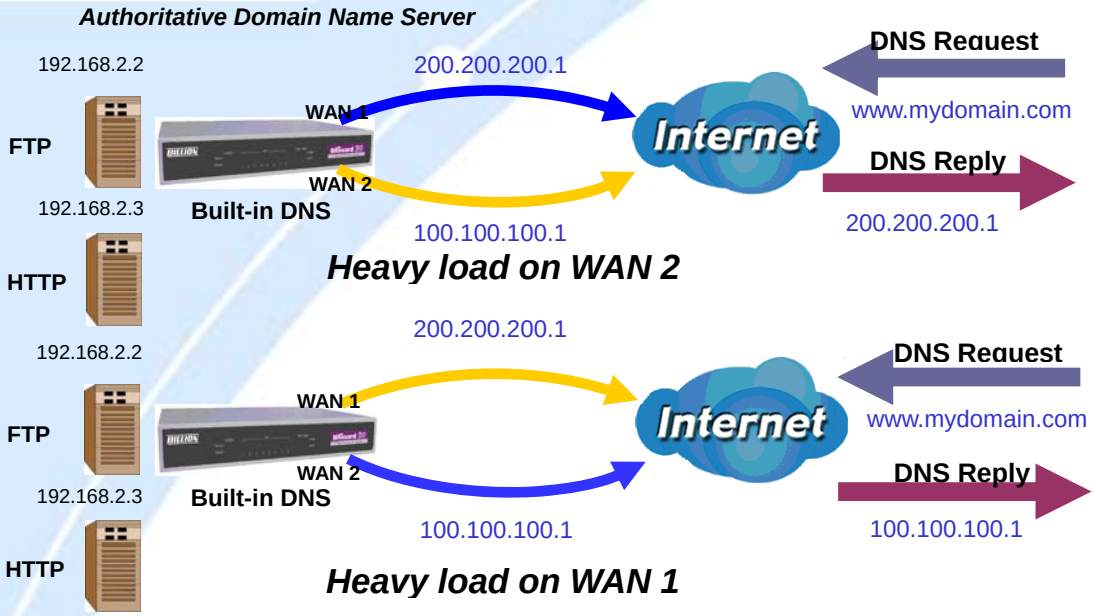


In the above example, an FTP Server (IP_192.168.2.2) and an HTTP Server (IP_192.168.2.3) are connected to the Internet via WAN1 (IP_200.200.200.1) on BiGuard 30. A remote computer is trying to access these servers via the Internet, and makes a DNS request. The DNS request (www.mydomain.com) will be sent through WAN1 (200.200.200.1) to the built-in DNS server. The DNS server will reply 200.200.200.1 because this is the only active WAN port. Should WAN1 fail, BiGuard 30 will instead reply with WAN2's IP address (100.100.100.1), and the remote PC will gain access to the network via WAN2. By configuring BiGuard 30 for DNS Inbound Fail Over, incoming requests will enjoy increased reliability when accessing your network.

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

2.5.2 DNS Inbound Load Balancing

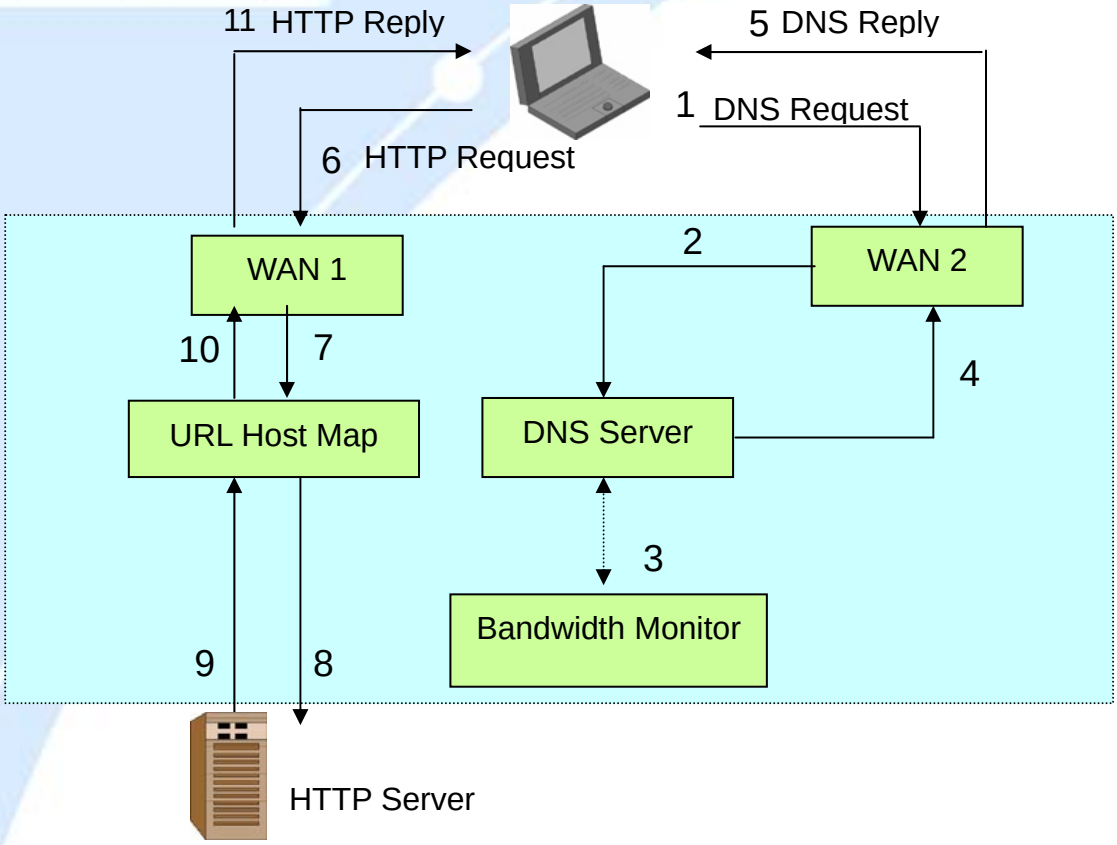
DNS Inbound Load Balancing allows BiGuard 30 to intelligently manage inbound traffic based on the amount of load of each WAN connection by assigning the IP address with the lowest traffic load to incoming requests.



In the above example, an FTP server (IP_192.168.2.2) and an HTTP server (IP_192.168.2.3) are connected to the Internet via WAN1 (IP_200.200.200.1) and WAN2 (IP_100.100.100.1) on BiGuard 30. Remote PCs are attempting to access the servers via the Internet by making a DNS request, entering a URL (www.mydomain.com). Using a load balancing algorithm, BiGuard 30 can direct incoming requests to either WAN port based on the amount of load each WAN port is currently experiencing. If WAN2 is experiencing a heavy load, BiGuard 30 responds to incoming DNS requests with WAN1. By balancing the load between WAN1 and WAN2, your BiGuard 30 can ensure that inbound traffic is efficiently handled, making sure that both ports are equally sharing the load and preventing situations where service is slow because one port is completely saturated by inbound traffic.

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

A typical scenario of how traffic is directed with DNS Inbound Load Balancing is illustrated below:



In the example above, the client is making a DNS request. The request is sent to the DNS server of BiGuard 30 through WAN2 (1). WAN2 will route this request to the embedded DNS server of BiGuard 30 (2). BiGuard 30 will analyze the bandwidth of both WAN1 and WAN2 and decide which WAN IP to reply to the request (3). After the decision is made, BiGuard 30 will route the DNS reply to the user through WAN2 (4). The user will receive the DNS reply with the IP address of WAN1 (5). The browser will initiate an HTTP request to the WAN1 IP address (6). The HTTP request will be send to BiGuard 30's URL Host Map (7). The Host Map will then redirect the HTTP request to the HTTP server (8). The HTTP server will reply (9). The URL Host Map will route the packet through WAN1 to the user (10). Finally, the client will receive an HTTP reply packet (11).

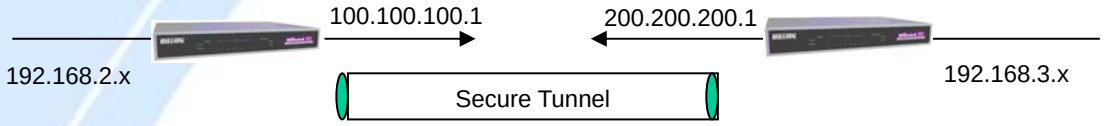
2.6 Virtual Private Networking

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 headquarters across the Internet in a secure fashion.

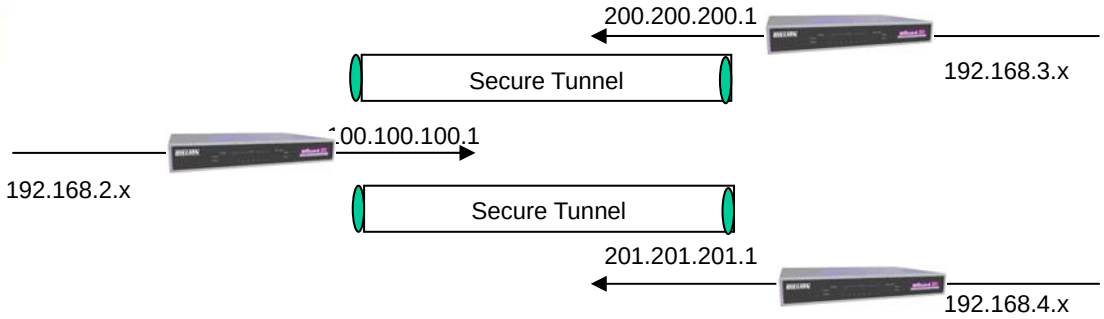
The following section discusses Virtual Private Networking with BiGuard 30.

2.6.1 General VPN Setup

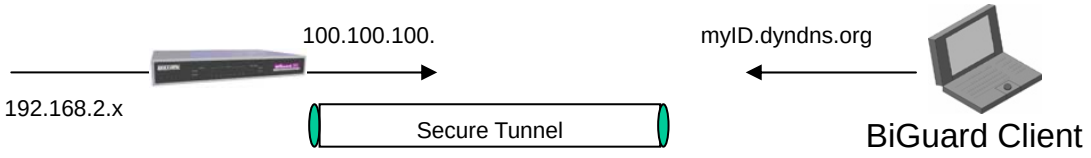
There are typically three different VPN scenarios. The first is a **Gateway to Gateway** setup, where two remote gateways communicate over the Internet via a secure tunnel.



The next type of VPN setup is the **Gateway to Multiple Gateway** setup, where one gateway (Headquarters) 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.

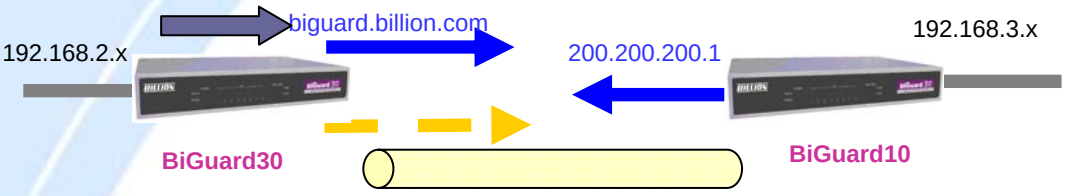


VPN provides a flexible, cost-efficient, and reliable way for companies of all sizes to stay connected. One of the most important steps in setting up a VPN is proper

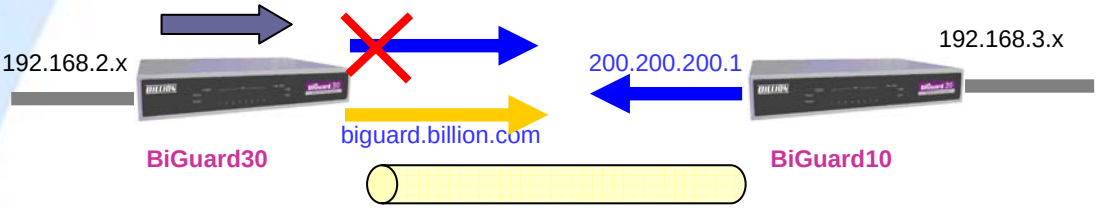
planning. The following sections demonstrate the various ways of using BiGuard 30 to setup your VPN.

2.6.2 VPN Planning - Fail Over

Configuring your VPN with Fail Over allows BiGuard 30 to automatically default to WAN2 should WAN1 fail.



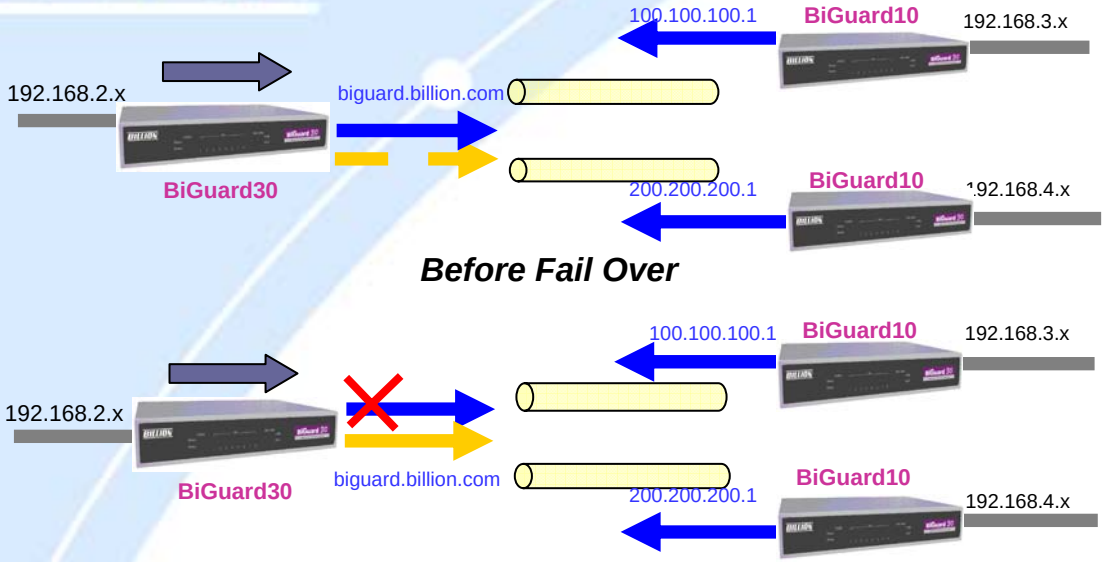
Before Fail Over



After Fail Over

Because the dynamic domain name biguard.billion.com is configured for both WAN1 and WAN2, the active WAN port will announce the domain name through the WAN IP address. The remote gateway will then be able to connect to the VPN through the domain name.

In this Gateway to Gateway example, BiGuard 30 is communicating to a remote gateway using WAN1 through a secure VPN tunnel. Should WAN1 fail, outbound traffic from BiGuard 30 will automatically be redirected to WAN2. This process is completely transparent to the remote gateway, as BiGuard 30 will automatically update the domain name (biguard.billion.com) with the WAN2 IP address. Configuring a Gateway to Multiple Gateway setup with Fail Over is similar, as shown below:

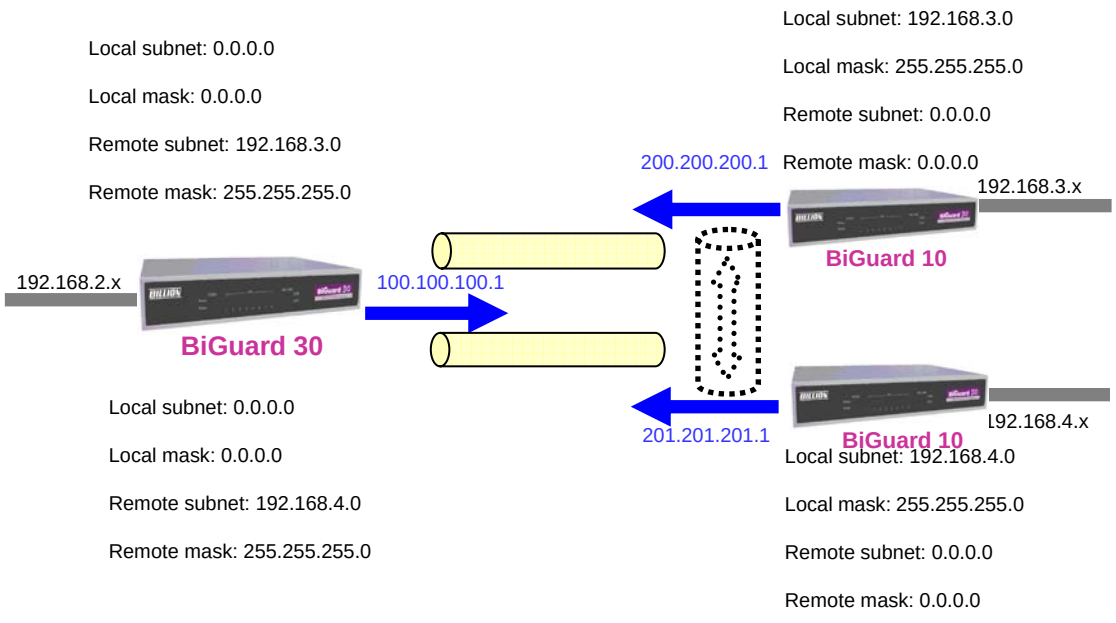


Configuring BiGuard 30 for Fail Over provides added reliability to your VPN.

2.6.3 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 30 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 30 is designed to be a powerful and flexible network device that is also easy to use. With an intuitive web-based configuration, BiGuard 30 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 30. Take a look and see how easy it is to get your network up and running.

3.2 Before You Begin

BiGuard 30 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
Decide whether you are going to use one or both WAN ports. For one WAN port, you may need a fully qualified domain name either for convenience or if you have a dynamic IP address. If you are going to use both WAN ports, determine whether you are going to use them in fail over mode for increased network reliability or load balancing mode for maximum bandwidth efficiency. 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. Each BiGuard 30 WAN port must be configured separately, whether you are using a separate ISP for each WAN port or are having the traffic of both WAN ports routed through the same ISP.

3. Determine your network management approach
BiGuard 30 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 for security reason.

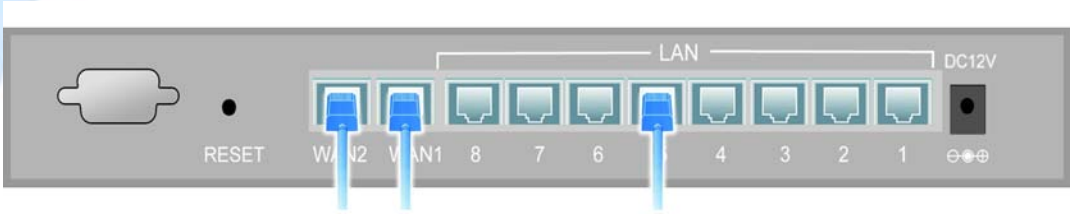
4. Prepare to physically connect BiGuard 30 to Cable or DSL modems and a computer.

Be sure to also review the **Safety Warnings** located in the preface of this manual before working with your BiGuard 30.

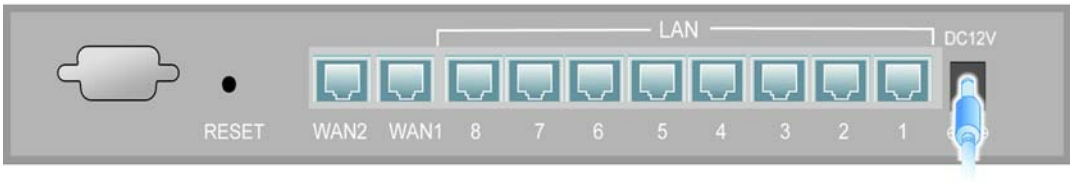
3.3 Connecting Your Router

Connecting BiGuard 30 is an easy three-step process:

1. Connect BiGuard 30 to your LAN by connecting Ethernet cables from your networked PCs to the LAN ports on the router. Connect BiGuard 30 to your broadband Internet connection via router's WAN port.



2. Plug BiGuard 30 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 30 is ready.

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

3.4 Configuring PCs for TCP/IP Networking

Now that your BiGuard 30 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 30, 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 30 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 30.

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 30, 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 User Name 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 30 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 30 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 *enabled* to

Subnet Mask	255.255.255.0	automatically get the WAN port configuration from the ISP.
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 30. After the network and firewall are configured, BiGuard 30 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

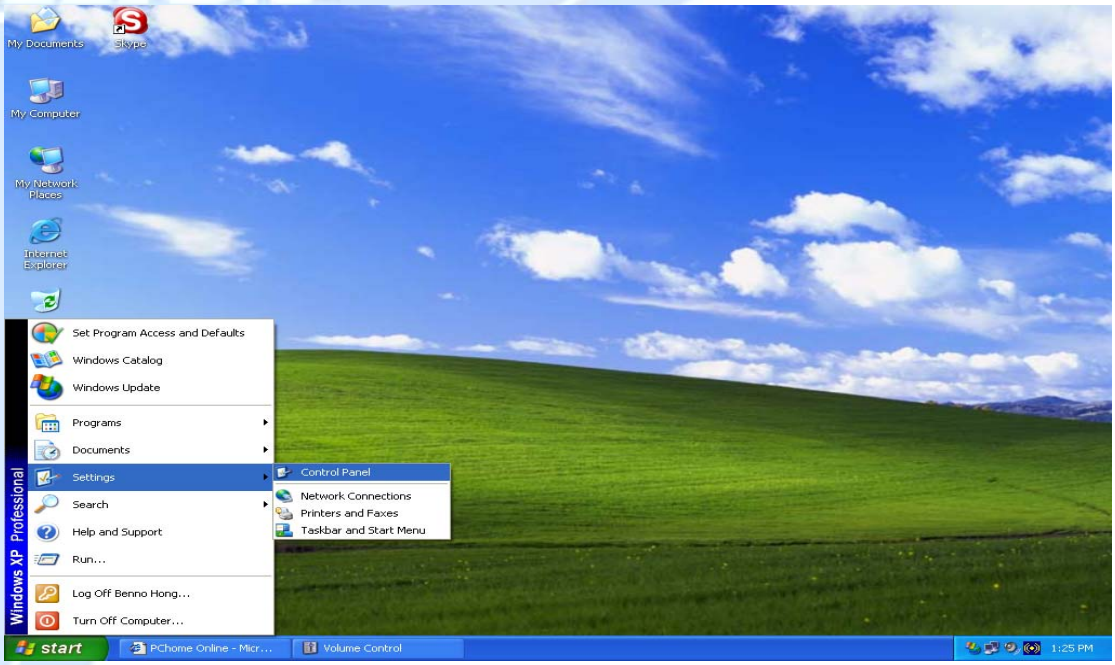
Depending on your ISP, a host name and domain suffix may also be provided. If any of these items are dynamically supplied by the ISP, your BiGuard 30 will automatically acquire them.

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 30. The following sections describe how you can obtain this information.

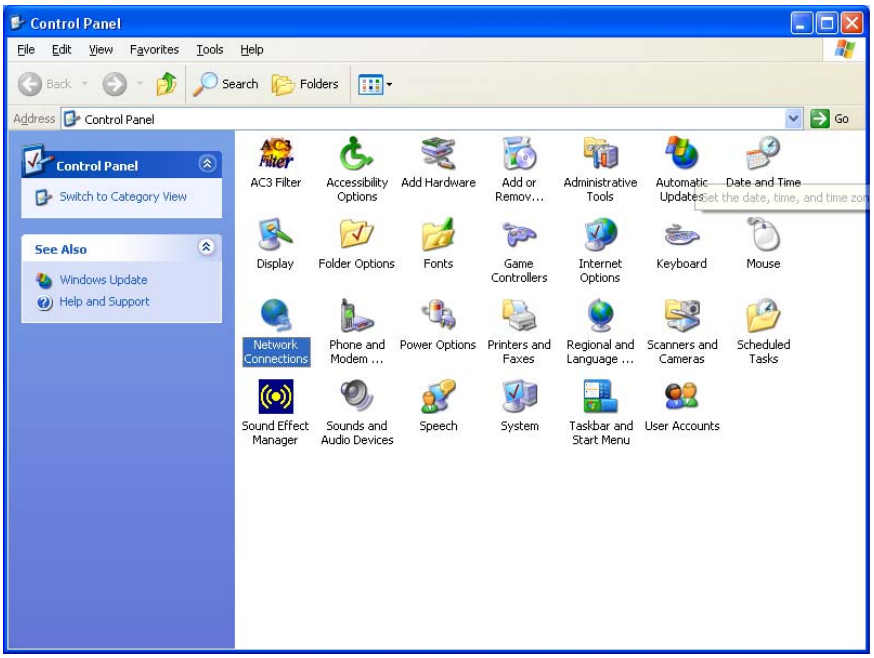
3.6.2.1 Windows

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.

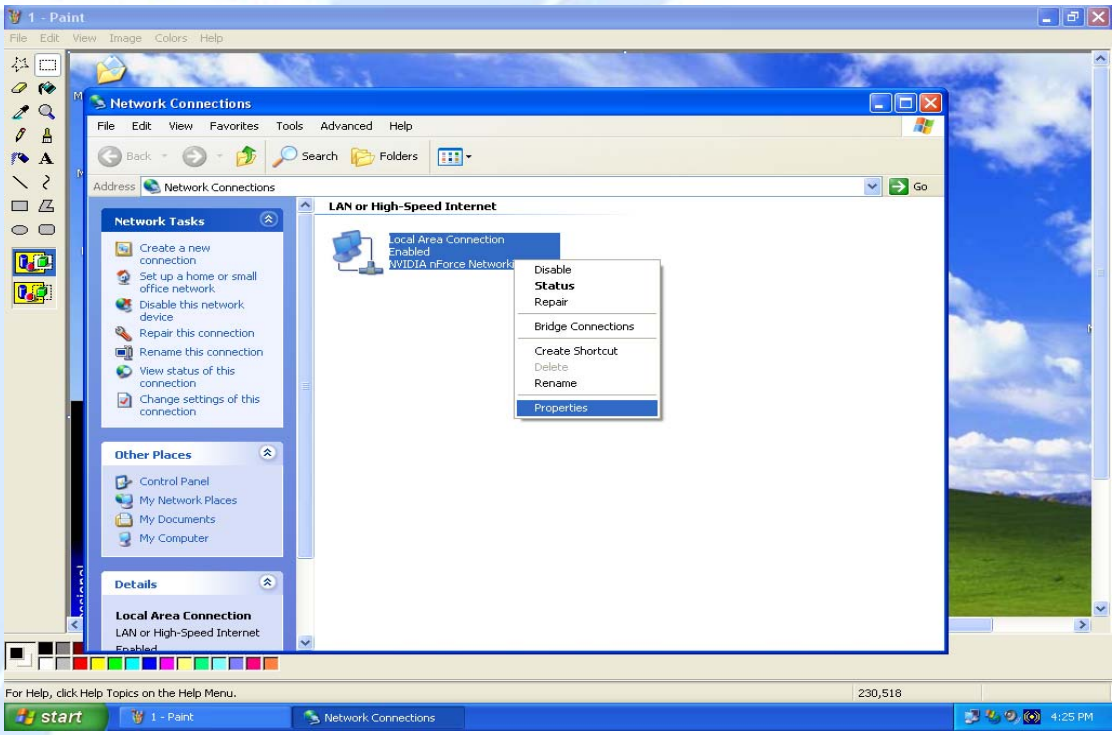
1. Select **Start** > **Settings** > **Control Panel**.



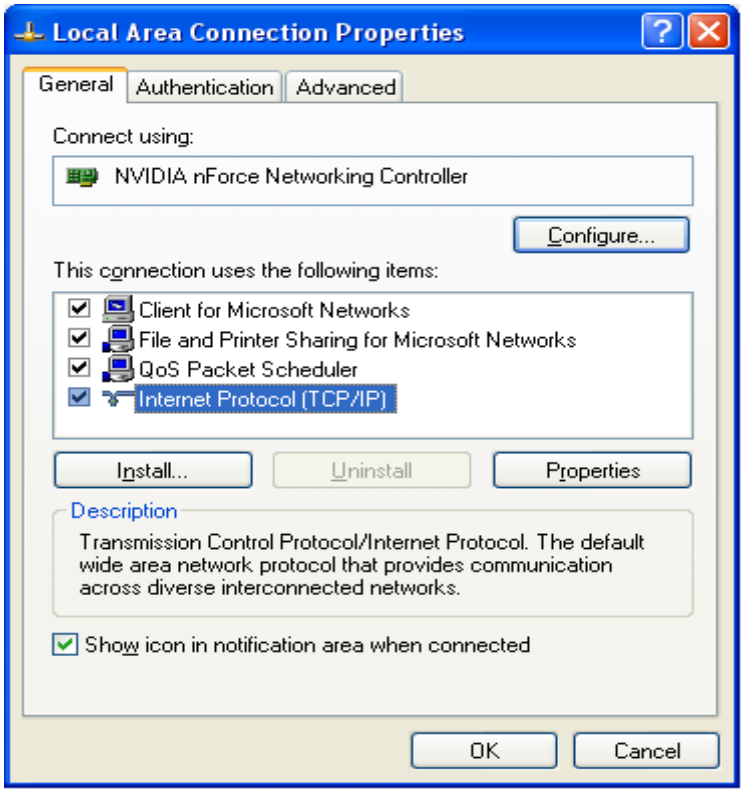
2. Double-click the **Network** icon.



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

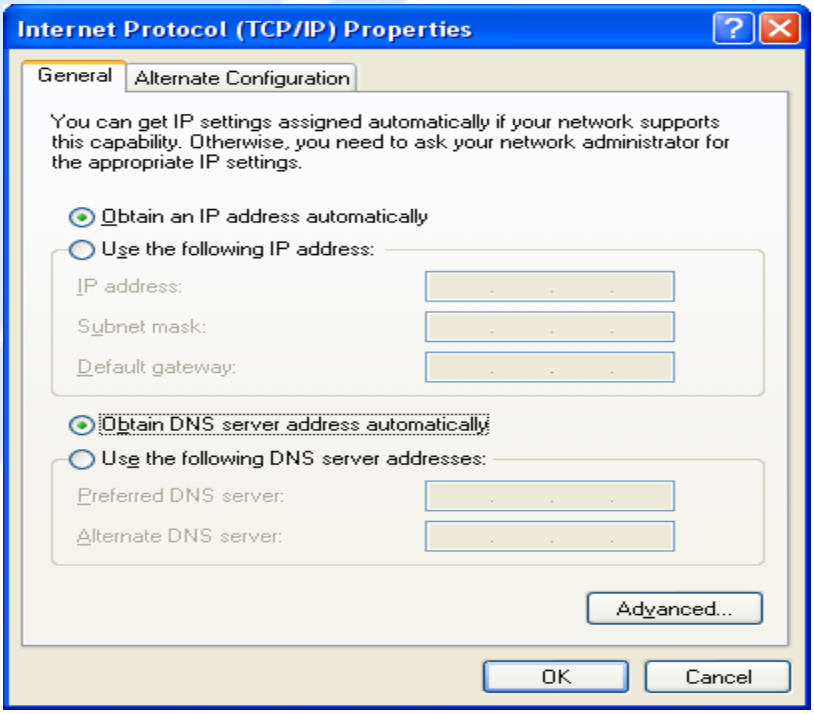


4. Select **Internet Protocol (TCP/IP)** and click **Properties**.

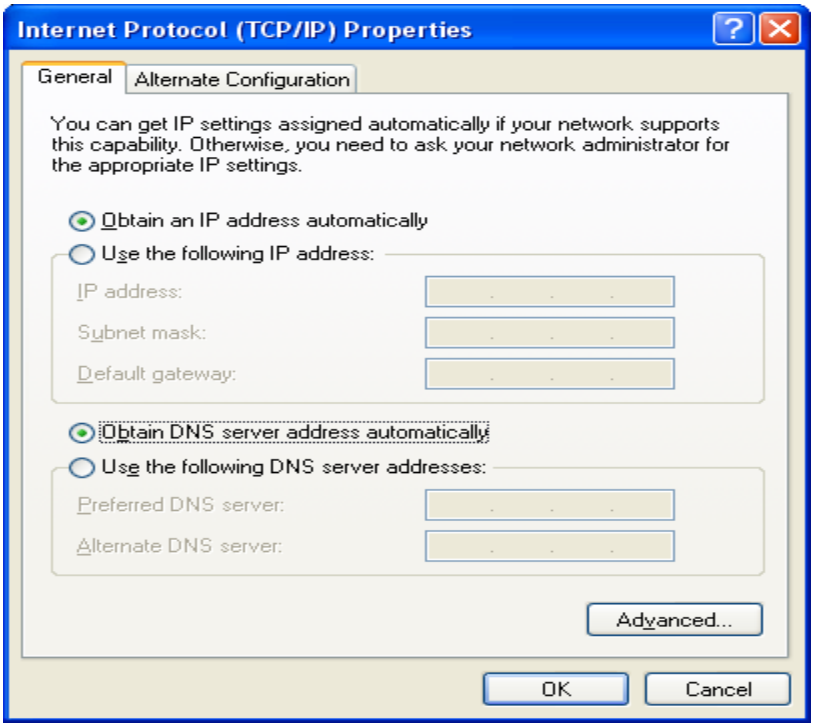


5. If an **IP address**, **subnet mask** and a **Default gateway** are shown, write down the information. If no address is present, your account's IP address is dynamically

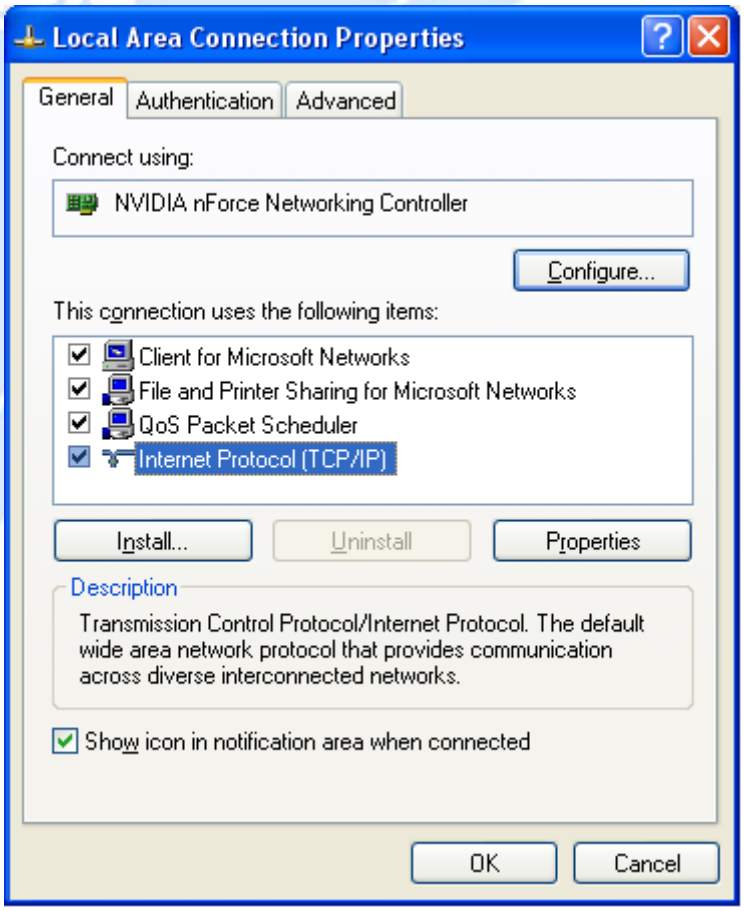
assigned. **Click the Obtain an IP address automatically** radio button.



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

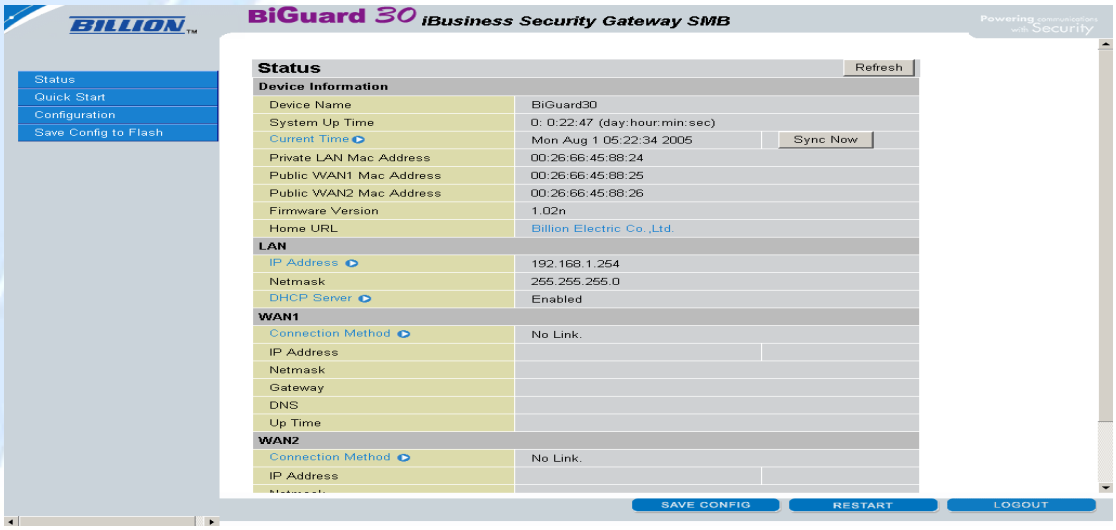
BiGuard 30 includes a Web Configuration Interface for easy administration via virtually any browser on your network. To access this interface, open your web browser, enter the IP address of your router, which by default is 192.168.1.254, and click **Go**. A user name and password window prompt will appear. Enter your user name and password (the default user name and password are "admin" and "admin") to access the Web Configuration Interface.

If the Web Configuration Interface appears, congratulations! You are now ready to configure your BiGuard 30. 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.



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 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 30. 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
- Traffic Statistics
- System Log
- IPSec Log

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.