

Gaming

Movies

Education

Communication

Business

Music



Billion 400G User Manual



Modem Support
0860 110 041

Telkom ADSL Support
0800 375 375

BILLION™

www.dobroadband.co.za
www.sizwebroadband.co.za



Table of Contents

CHAPTER 1: INTRODUCTION	1
<i>INTRODUCTION TO YOUR ROUTER</i>	1
<i>FEATURES</i>	1
CHAPTER 2: INSTALLING THE ROUTER	3
<i>IMPORTANT NOTE FOR USING THIS ROUTER</i>	3
<i>PACKAGE CONTENTS</i>	3
<i>THE FRONT LEDS</i>	4
<i>THE REAR PORTS</i>	5
<i>CABLING</i>	6
CHAPTER 3: BASIC INSTALLATION	7
<i>CONNECTING YOUR ROUTER</i>	8
<i>FACTORY DEFAULT SETTINGS</i>	13
<i>Web Interface (Username and Password)</i>	13
<i>Device LAN IP settings</i>	13
<i>ISP setting in WAN site</i>	13
<i>DHCP server</i>	13
<i>LAN and WAN Port Addresses</i>	13
<i>INFORMATION FROM YOUR ISP</i>	14
<i>CONFIGURING WITH YOUR WEB BROWSER</i>	15
CHAPTER 4: CONFIGURATION	16
<i>STATUS</i>	17
<i>ADSL Status</i>	17
<i>ARP Table</i>	17
<i>DHCP Table</i>	18
<i>Routing Table</i>	18
<i>NAT Sessions</i>	19
<i>UPnP Portmap</i>	19
<i>Email Status</i>	19
<i>Event Log</i>	20
<i>Error Log</i>	20
<i>Diagnostic</i>	20
<i>QUICK START</i>	21
<i>CONFIGURATION</i>	24
<i>LAN - Local Area Network</i>	24
Bridge Interface	24
Ethernet.....	25
IP Alias.....	25
Ethernet Client Filter	26
Wireless	27
Wireless Security	29
Wireless Client / MAC Address Filter	31
WPS	32
Port Setting	32
DHCP Server	33
<i>WAN - Wide Area Network</i>	34
WAN Profile	34
ADSL Mode.....	40
<i>System</i>	41
Time Zone.....	41
Remote Access.....	42
Firmware Upgrade	42


Backup / Restore	43
Restart Router	44
User Management	44
<i>Firewall and Access Control</i>	46
General Settings.....	47
(Changed the format only.)	47
Packet Filter	48
Intrusion Detection	55
URL Filter.....	58
IM / P2P Blocking	60
Firewall Log.....	61
<i>QoS - Quality of Service</i>	61
Prioritization	61
Outbound IP Throttling (LAN to WAN)	63
Inbound IP Throttling (WAN to LAN).....	64
<i>Virtual Server (known as Port Forwarding)</i>	69
Add Virtual Server	69
Edit DMZ Host	71
Edit DMZ Host	72
Edit One-to-One NAT (Network Address Translation).....	73
<i>Time Schedule</i>	75
Configuration of Time Schedule	76
<i>Advanced</i>	77
Static Route.....	77
Dynamic DNS.....	78
Check Email.....	79
Device Management	80
IGMP	83
VLAN Bridge	83
<i>LOGOUT</i>	83
CHAPTER 5: TROUBLESHOOTING	84
<i>PROBLEMS STARTING UP THE ROUTER</i>	84
<i>PROBLEMS WITH THE WAN INTERFACE</i>	84
<i>PROBLEMS WITH THE LAN INTERFACE</i>	84
<i>CONTACT TELKOM ADSL SUPPORT</i>	85
<i>CONTACT SIZWEBBROADBAND FOR ROUTER SUPPORT</i>	85


Chapter 1: Introduction


Introduction to your Router


Your Billion 400G router is an “all-in-one” ADSL router, combining an ADSL 2/2+ modem/router and network switch, providing everything you need to you connected to the Internet using your ADSL connection.


Features


-  **Express Internet Access**


The router complies with ADSL worldwide standards. It supports downstream rate up to 12/24 Mbps with ADSL2/2+, 8Mbps with ADSL. Users enjoy not only high-speed ADSL services but also broadband multimedia applications such as interactive gaming, video streaming and real-time audio much easier and faster than ever. It is compliant with Multi-Mode standard (ANSI T1.413, Issue 2; G.dmt (ITU G.992.1); G.lite (ITU G.992.2); G.hs (ITU G994.1); G.dmt.bis (ITU G.992.3); G.dmt.bis.plus (ITU G.992.5)).
-  **802.11g Wireless AP with WPA Support**


With integrated 802.11g Wireless Access Point in the router, the device offers a quick and easy access among wired network, wireless network and broadband connection (ADSL) with single device simplicity, and as a result, mobility to the users. In addition to 54 Mbps 802.11g data rate, it also interoperates backward with existing 802.11b equipment. The Wireless Protected Access (WPA1 and WPA2) and Wireless Encryption Protocol (WEP) supported features enhance the security level of data protection and access control via Wireless LAN.
-  **Fast Ethernet Switch**

A 4-port 10/100Mbps fast Ethernet switch is built in with automatic switching between MDI and MDI-X for 10Base-T and 100Base-TX ports. An Ethernet straight or crossover cable can be used directly for auto detection.
-  **Multi-Protocol to Establish a Connection**

It supports PPPoA, RFC 1483 encapsulation over ATM (bridged or routed), PPP over Ethernet (RFC 2516), and IPoA to establish a connection with the ISP. The product also supports VC-based and LLC-based multiplexing. Furthermore the device supports multiple PPPoE connections on the same PVC to allow for smart traffic separation.
-  **Quick Installation Wizard**

The router can be setup and managed by using the easy setup wizard software included on the CD or the GUI (Graphical User Interface) imbedded on the router accessed using the router’s LAN IP address and a standard web-browser application like Internet Explorer.
-  **Universal Plug and Play (UPnP) and UPnP NAT Traversal**

This protocol is used to enable simple and robust connectivity among stand-alone devices and PCs from many different vendors. It makes network simple and affordable for users. UPnP architecture leverages TCP/IP and the Web to enable seamless proximity networking in addition to control and data transfer among networked devices. With this feature enabled, users can now connect to Net meeting or MSN Messenger seamlessly.
-  **Network Address Translation (NAT)**

Allows multi-users to access outside resources such as the Internet simultaneously with one IP address/one Internet access account. Many application layer gateways (ALG) are supported such as web browser, ICQ, FTP, Telnet, E-mail, News, Net2phone, Ping, NetMeeting, IP phone and others.
-  **SOHO Firewall Security with DoS and SPI**

Along with the built-in NAT natural firewall feature, the router also provides advanced hacker pattern-filtering protection. It can automatically detect and block Denial of Service (DoS) attacks. The router is built with Stateful Packet Inspection (SPI) to determine if a data packet is allowed through the firewall to the private LAN.

- **Domain Name System (DNS) Relay**

It provides an easy way to map the domain name (a friendly name for users such as www.yahoo.com) and IP address. When a local machine sets its DNS server with this router's IP address, every DNS conversion request packet from the PC to this router will be forwarded to the real DNS in the outside network.
- **Dynamic Domain Name System (DDNS)**

The Dynamic DNS service allows you to alias a dynamic WAN IP address to a static hostname. For example, to use the service, you must first apply for an account from a DDNS service like <http://www.dyndns.org/>. More than 5 DDNS servers are supported.
- **Quality of Service (QoS)**

QoS gives you full control over which types of outgoing data traffic should be given priority by the router, ensuring important data like gaming packets, customer information, or management information move through the router at lightning speed, even under heavy load. The QoS features are configurable by source IP address, destination IP address, protocol, and port. You can throttle the speed at which different types of outgoing data pass through the router, to ensure P2P users don't saturate upload bandwidth, or office browsing doesn't bring client web serving to a halt. In addition, or alternatively, you can simply change the priority of different types of upload data and let the router sort out the actual speeds.
- **Virtual Server ("port forwarding")**

Users can specify some services to be visible from outside users. The router can detect incoming service requests and forward either a single port or a range of ports to the specific local computer to handle it. For example, a user can assign a PC in the LAN acting as a WEB server inside and expose it to the outside network. Outside users can browse inside web servers directly while it is protected by NAT. A DMZ host setting is also provided to a local computer exposed to the outside network, Internet.
- **Rich Packet Filtering**

Not only filters the packet based on IP address, but also based on Port numbers. It will filter packets from and to the Internet, and also provides a higher level of security control.
- **Dynamic Host Configuration Protocol (DHCP) Client and Server**

In the WAN site, the DHCP client can get an IP address from the Internet Service Provider (ISP) automatically. In the LAN site, the DHCP server can allocate a range of client IP addresses and distribute them including IP address, subnet mask as well as DNS IP address to local computers. It provides an easy way to manage the local IP network.
- **Static and RIP1/2 Routing**

It has routing capability and supports easy static routing table or RIP1/2 routing protocol.
- **Simple Network Management Protocol (SNMP)**

It is an easy way to remotely manage the router via SNMP.
- **Web based GUI**

The routers' web based GUI is used for configuration and management. It is user-friendly and comes with on-line help. It also supports remote management capability for remote users to configure and manage the router.
- **Firmware Upgradeable**

Device can be upgraded to the latest firmware through the WEB based GUI.
- **Rich Management Interfaces**

It supports flexible management interfaces with local console port, LAN port, and WAN port. Users can use terminal applications through the console port to configure and manage the device, or Telnet, WEB GUI, and SNMP through LAN or WAN ports to configure and manage the device. TR-069 management is also supported, but is normally implemented by Telkom or your ISP.

Chapter 2: Installing the Router

Important note for using this router



Warning

- ✓ Do not use this router under high humidity or high temperatures.
- ✓ Do not use the same power source for this router as other equipment.
- ✓ Do not open or repair the case by yourself. If this router is too hot, turn off the power immediately and have it repaired at a qualified service center.
- ✓ Avoid using this product and all accessories outdoors.



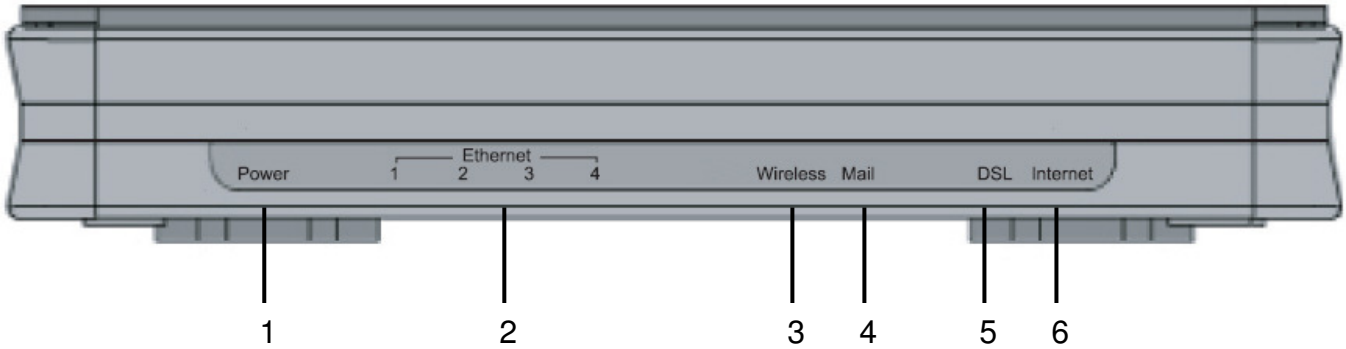
Attention

- ✓ Place this router on a stable surface.
- ✓ Only use the power adapter that comes with the package.
Using a different voltage rating power adaptor may damage this router.

Package Contents

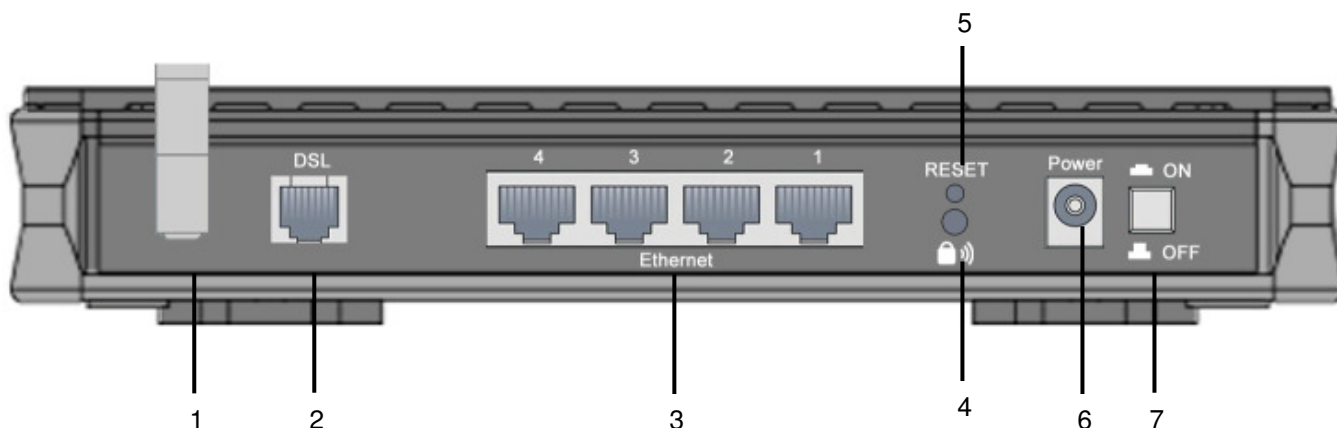
- Billion 400G Router
- CD-ROM containing this online manual
- 2 x RJ-11 ADSL/telephone Cable
- Ethernet (CAT-5 LAN) Cable
- Console tool kit
- Integrated surge and AC-DC power adapter (12VDC, 1.2A)
- A detachable antenna
- ADSL Micro filter
- ADSL Splitter
- Quick Start Guide

The Front LEDs



LED		Meaning
1	Power	Lit when power is ON. If lit red it means the system has failed to load. Restart the device or contact router support.
2	LAN Port 1X — 4X (RJ-45 connector)	Lit when connected to an Ethernet device. Green for 100Mbps; Orange for 10Mbps. Flashing when data is Transmitted / Received.
3	Wireless	Green when the wireless connection is established. Flashing when sending/receiving data.
4	Mail	Lit and flashing periodically when there are emails in the Inbox.
5	ADSL	Lit Green when the device is successfully connected to an ADSL DSLAM ("line synch").
6	Internet	Lit red when WAN port fails to get IP address. Lit green when WAN port gets IP address successfully.

The Rear Ports



NOTE:


The Ethernet Port # 4 can be used as a console port. You need a special console tool which already includes in the package to connect with LAN port 4 and PC's RS-232 port (9-pin serial port).

Port	Meaning
1	Antenna Connect the detachable antenna to this port.
2	ADSL Use the supplied RJ-11 ("telephone") cable to connect this port to the ADSL/telephone wall jack.
3	LAN 1X — 4X (RJ-45 connector) To connect your router to a PC or an office/home network of 10Mbps or 100Mbps use a UTP Ethernet cable (Cat-5 or Cat-5e) and connect to one of the LAN ports. Caution: Port 4 can be either a LAN or a Console port at any time but not simultaneously.
4	WPS Press the WPS button to trigger Wi-Fi Protected Setup function.
5	RESET When the router is turned on → the reset button is used to: Reset the router: press for 1-3 seconds . Restore factory default settings: press for 6 – 8 seconds, and power cycle the router : (useful if you cannot login to the router or have forgotten your Username/Password.) Caution: After pressing the RESET button for 6 - 8 seconds, be sure you power cycle the device. If the RESET button is pressed for more than 10 seconds, the device will need to be power cycled before normal operation can be resumed.
6	Power Connect the supplied power adapter to this jack.
7	Power Switch Power ON/OFF switch

Cabling

One of the most common causes of problems is the bad cabling or ADSL line(s). Make sure that all connected devices are turned on. On the front of the product is a bank of LEDs. Verify that the LAN Link and ADSL line LEDs are lit. If they are not, verify that you are using the proper cables.

Ensure that all other devices connected to the same telephone line as your router (e.g. telephones, fax machines, analogue modems) have a line filter connected between them and the wall socket (unless you are using a Central Splitter or Central Filter installed by a qualified and licensed electrician), and ensure that all line filters are correctly installed and the right way around. Missing line filters or line filters installed the wrong way around can cause problems with your ADSL connection, including causing frequent disconnections.

Chapter 3: Basic Installation

The router can be configured with your web browser. A web browser is included as a standard application in the following operating systems: Linux, Mac OS, Windows 98/NT/2000/XP/Me, etc. The product provides an easy and user-friendly interface for configuration.

Please check your PC's network components. The TCP/IP protocol stack and Ethernet network adapter must be installed. If not, please refer to your Windows-related or other operating system manuals.

You can connect your computer to the router either through an external hub/switch or directly. However, please ensure that your computer has a properly installed Ethernet interface prior to connecting it to the router. You ought to configure your Computers to obtain an IP address through a DHCP server or you can set them up with a fixed IP address that must be in the same subnet as the router. The default IP address of the router is **10.0.0.2** and the subnet mask is **255.255.255.0** (i.e. any attached Computer must be in the same subnet, and have an IP address in the range of 10.0.0.1 to 10.0.0.254). The best and easiest way is to configure the PC to get an IP address automatically from the router using DHCP. If you encounter any problem accessing the router's web interface it may also be advisable to temporarily remove any kind of software firewall on your Computer's as they can cause problems accessing the 10.0.0.2 IP address of the router. Users should always make their own decisions on how to best protect their network.

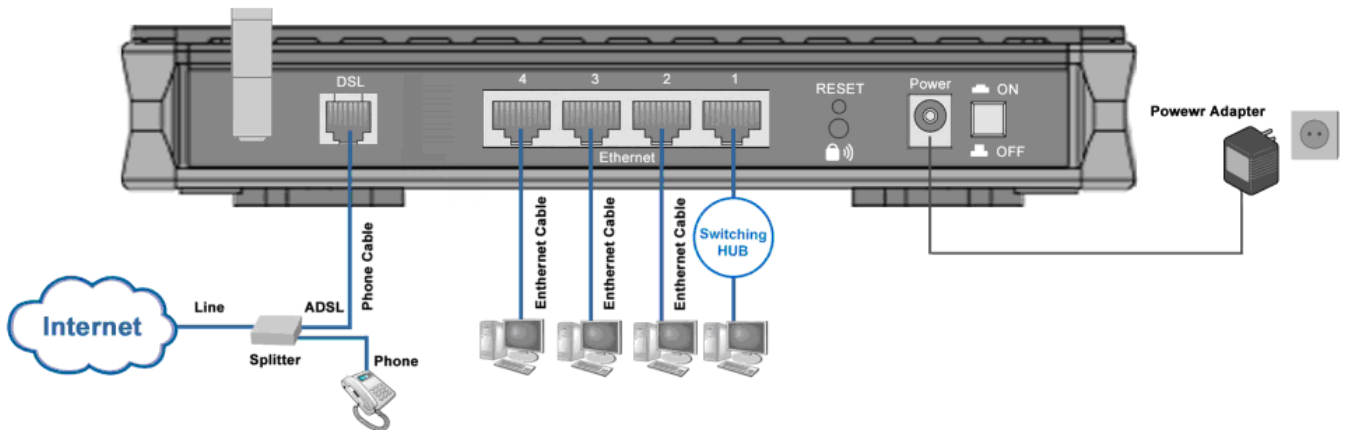
Please follow the steps below for your PC's network environment installation.



Any TCP/IP capable workstation can be used to communicate with or through the router. To configure other types of workstations, please consult the manufacturer's documentation.

Connecting Your Router

1. Connect the power adapter as illustrated below and power on the device, make sure that the PWR LED is lit steadily.
2. Connect your network or computer to the router using the **LAN** (Local Area Network) cable.
3. Connect the ADSL/telephone (**ADSL**) cable to the router's DSL port as illustrated below.



Configuring PCs in Windows in Window XP

1. Go to **Start / Control Panel** (in Classic View). In the Control Panel, double-click **Network Connections**.
2. Double-click **Local Area Connection**. (See Figure 3.1)

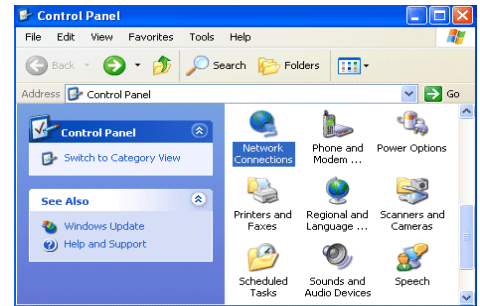


Figure 3.1: LAN Area Connection

3. In the **LAN Area Connection Status** window, click **Properties**. (See Figure 3.2)

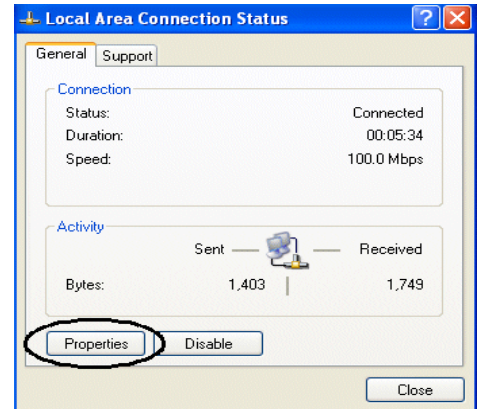


Figure 3.2: LAN Connection Status

4. Select **Internet Protocol (TCP/IP)** and click **Properties**. (See Figure 3.3)

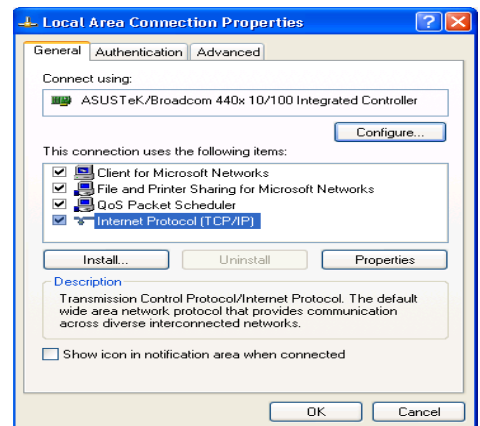


Figure 3.3: TCP / IP

5. Select the **Obtain an IP address automatically** and **Obtain DNS server address automatically** radio buttons. (See Figure 3.4)
6. Click **OK** to finish the configuration.

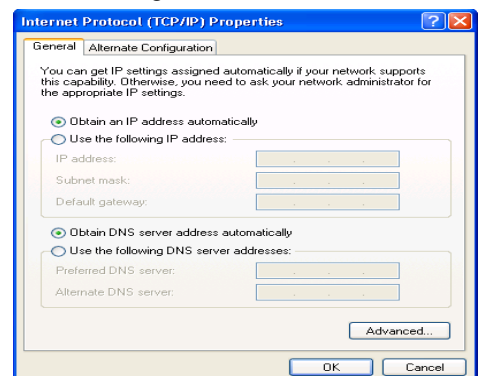


Figure 3.4: IP Address & DNS Configuration

Configuring PCs in Windows 2000

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click **Network and Dial-up Connections**.
2. Double-click **Local Area (“LAN”) Connection**. (See Figure 3.5)



Figure 3.5: LAN Area Connection

3. In the **LAN Area Connection Status** window, click **Properties**. (See Figure 3.6)

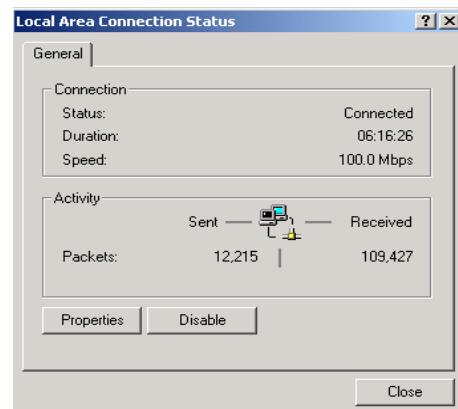


Figure 3.6: LAN Connection Status

4. Select **Internet Protocol (TCP/IP)** and click **Properties**. (See Figure 3.7)

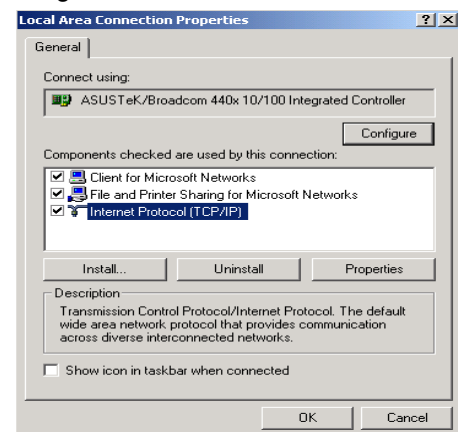


Figure 3.7: TCP / IP

5. Select the **Obtain an IP address automatically** and **Obtain DNS server address automatically** radio buttons. (See Figure 3.8)
6. Click **OK** to finish the configuration.

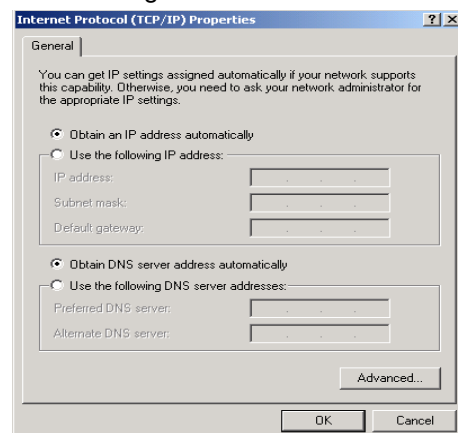


Figure 3.8: IP Address & DNS Configuration

Configuring PC in Windows 95/98/ME

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click **Network** and choose the **Configuration** tab.
2. Select **TCP / IP -> NE2000 Compatible**, or the name of any Network Interface Card (NIC) in your PC. (See Figure 3.9)
3. Click **Properties**.

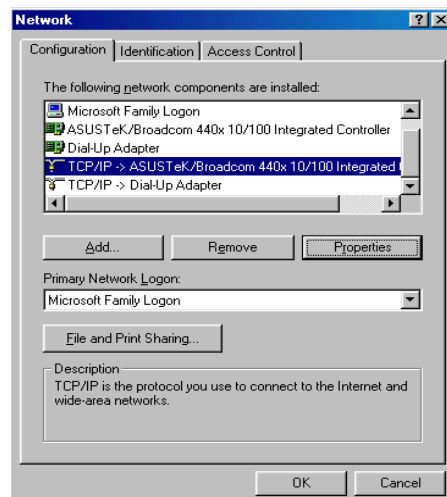


Figure 3.9: TCP / IP

4. Select the **IP Address** tab. In this page, click the Obtain an IP address automatically radio button. (See Figure 3.10)

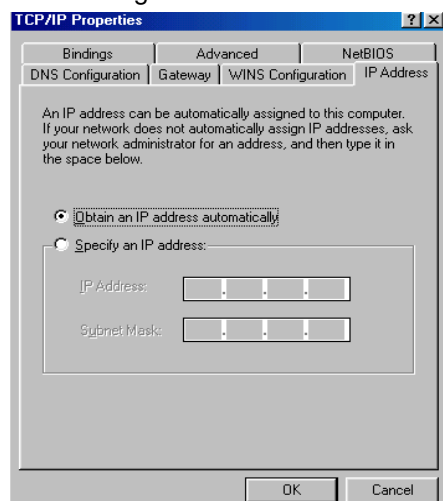


Figure 3.10: IP Address

5. Then select the **DNS Configuration** tab. (See Figure 3.11)
6. Select the **Disable DNS** radio button and click **OK** to finish the configuration.

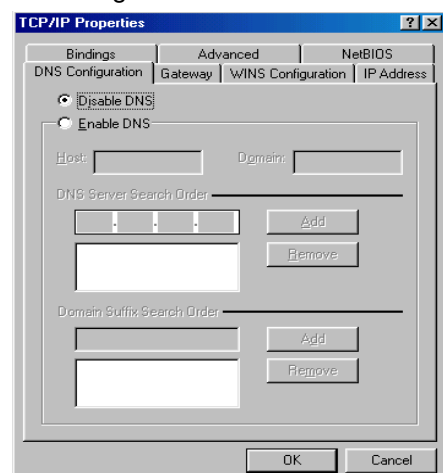


Figure 3.11: DNS Configuration

Configuring PC in Windows NT4.0

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click **Network** and choose the **Protocols** tab.

2. Select **TCP/IP Protocol** and click **Properties**. (See Figure 3.12)

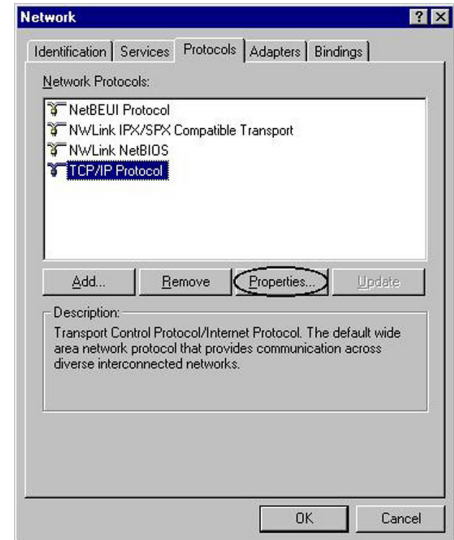


Figure 3.12: TCP / IP

3. Select the **Obtain an IP address from a DHCP server** radio button and click **OK**. (See Figure 3.13)

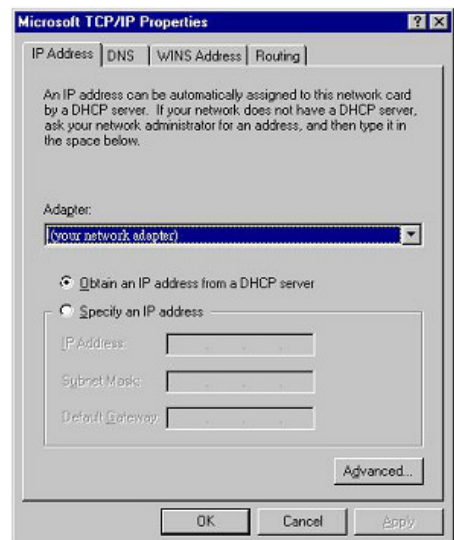


Figure 3.13: IP Address

Factory Default Settings

Before configuring your, you need to know the following default settings.

Web Interface (Username and Password)

- ▶ Username: admin
- ▶ Password: admin

The default username and password are “**admin**” and “**admin**” respectively.



Attention

If you ever forget the username/password to login to the router, you may press the RESET button for 6 – 8 seconds to restore the factory default settings.

Caution: After pressing the RESET button for more than 6 seconds, to be sure you power cycle the device again.

Device LAN IP settings

- ▶ IP Address: 10.0.0.2
- ▶ Subnet Mask: 255.255.255.0

ISP setting in WAN site

- ▶ PPPoE

DHCP server

- ▶ DHCP server is enabled.
- ▶ Start IP Address: 10.0.0.100
- ▶ IP pool counts: 100

LAN and WAN Port Addresses

The parameters of LAN and WAN ports are pre-set in the factory. The default values are shown below.

LAN Port		WAN Port
IP address	10.0.0.2	The WAN protocol has been pre-selected and set by Telkom for automated service deployment and delivery.
Subnet Mask	255.255.255.0	
DHCP server function	Enabled	
IP addresses for distribution to PCs	100 IP addresses continuing from 10.0.0.100 through 10.0.0.199	

Information from your ISP

Telkom ADSL connections use PPPoE, and automatically assign a WAN IP address to your router. The following information is provided should you wish to connect to an alternative ISP.

Gather the information as illustrated in the following table and keep it for reference.

PPPoE	VPI/VCI, VC / LLC-based multiplexing, Username, Password, Service Name, and Domain Name System (DNS) IP address (this is automatically set by the Telkom network but be set manually should this be required).
PPPoE (Multisession)	VPI/VCI, VC / LLC-based multiplexing, Username, Password, Service Name, Domain Name System (DNS) IP address and multiple-sessions on the same PVC.
PPPoE / PPPoE with Pass-through	VPI/VCI, VC / LLC-based multiplexing, Username, Password, Service Name, and Domain Name System (DNS) IP address (this is automatically set by the Telkom network but be set manually should this be required). In addition, additional WAN address can be assigned using PPPoE dialer.
PPPoA	VPI/VCI, VC / LLC-based multiplexing, Username, Password and Domain Name System (DNS) IP address (it can be automatically assigned by your ISP when you connect or be set manually).
RFC 1483 Bridged	VPI/VCI, VC / LLC-based multiplexing to use Bridged Mode.
RFC 1483 Routed	VPI/VCI, VC / LLC-based multiplexing, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is a fixed IP address).
IPoA Routed (IP over ATM)	VPI/VCI, VC / LLC-based multiplexing, IP address, Subnet mask, Gateway address, and Domain Name System (DNS) IP address (it is a fixed IP address).

Configuring with your Web Browser

Open your web browser, enter the IP address of your router, which by default is **10.0.0.2**, and click “Go”, a user name and password window prompt will appear. **The default username and password are “admin” and “admin” respectively. (See Figure 3.14)**

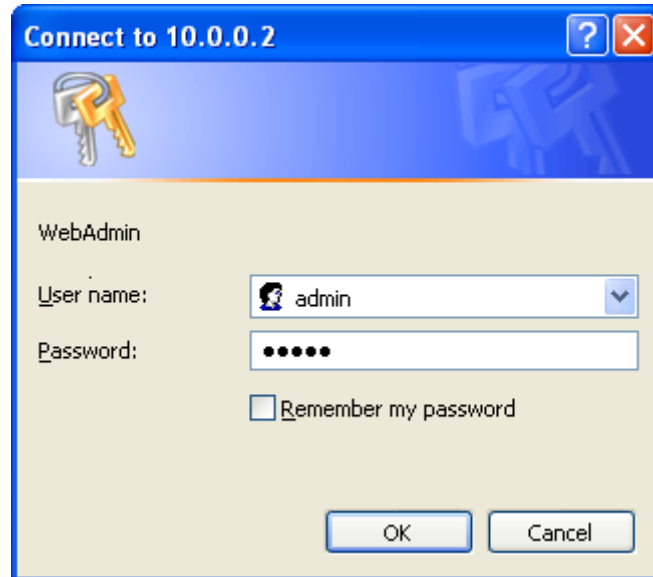


Figure 3.14: User name & Password Prompt Window

Congratulations! You are now successfully logged on to the Router!

Chapter 4: Configuration

At the configuration homepage, the left navigation pane where bookmarks are provided links you directly to the desired setup page, including:

- **Status**
 - ADSL Status
 - ARP Table
 - DHCP Table
 - Routing Table
 - NAT Sessions
 - UPnP Portmap
 - Email Status
 - Event Log
 - Error Log
 - Diagnostic
- **Quick Start**
- **Configuration**
 - LAN
 - WAN
 - System
 - Firewall
 - VPN
 - QoS
 - Virtual Server
 - Time Schedule
 - Advanced
- **Language** (provides user interface in English and French languages)

Status

ADSL Status

This section displays the ADSL overall status, which shows a number of helpful information such as DSP firmware version.

Status	
ADSL Status	
Parameters	
DSP Firmware Version	E.25.41.18 A
Connected	false
Operational Mode	Inactive
Annex Type	AnnexA
Upstream	0
Downstream	0
SNR Margin(Upstream)	0 dB
SNR Margin(Downstream)	0.0 dB
Line Attenuation(Upstream)	0.0 dB
Line Attenuation(Downstream)	0.0 dB
CRC Errors(Upstream)	0
CRC Errors(Downstream)	0
Latency(Upstream)	
Latency(Downstream)	

ARP Table

This section displays the router's ARP (Address Resolution Protocol) Table, which shows the mapping of Internet (IP) addresses to Ethernet (MAC) addresses. This is useful as a quick way of determining the MAC address of the network interface of your PCs to use with the router's **Firewall – MAC Address Filter** function. See the Firewall section of this manual for more information on this feature.

Status			
ARP Table			
Wired			
IP Address	MAC Address	Interface	Static
10.0.0.100	00:03:0d:3d:c0:fb	iplan	no
Wireless			
IP Address	MAC		

IP Address: A list of IP addresses of devices on your LAN (Local Area Network).

MAC Address: The MAC (Media Access Control) addresses for each device on your LAN.

Interface: The interface name (on the router) that this IP Address connects to.

Static: Static status of the ARP table entry:

- ⊙ “no” for dynamically-generated ARP table entries.
- ⊙ “yes” for static ARP table entries added by the user.

DHCP Table

Status			
<div style="border: 1px solid #ccc; padding: 5px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼ DHCP Table</div> <div style="background-color: #f0f0f0; padding: 2px;">Type</div> <div style="display: flex; justify-content: space-between; padding: 2px;"> Leased ▶ Expired ▶ Permanent ▶ </div> </div>			

Leased: The DHCP assigned IP addresses information.

Expired: The expired IP addresses information.

Permanent: The fixed host mapping information

Leased Table

Leased Table			
IP Address	MAC Address	Client Host Name	Expiry

IP Address: The IP address that assigned to client.

MAC Address: The MAC address of client.

Client Host Name: The Host Name (Computer Name) of client.

Expiry: The current lease time of client.

Routing Table

Status														
<div style="border: 1px solid #ccc; padding: 5px;"> <div style="background-color: #f0f0f0; padding: 2px;">▼ Routing Table</div> <div style="background-color: #f0f0f0; padding: 2px;">Routing Table</div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 10%;">Valid</th> <th style="width: 30%;">Destination</th> <th style="width: 20%;">Netmask</th> <th style="width: 30%;">Gateway/Interface</th> <th style="width: 10%;">Cost</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> <td> </td> <td> </td> <td> </td> </tr> </tbody> </table> </div>					Valid	Destination	Netmask	Gateway/Interface	Cost					
Valid	Destination	Netmask	Gateway/Interface	Cost										
<div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> <div style="background-color: #f0f0f0; padding: 2px;">RIP Routing Table</div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">Destination</th> <th style="width: 30%;">Netmask</th> <th style="width: 30%;">Gateway</th> <th style="width: 10%;">Cost</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> <td> </td> <td> </td> </tr> </tbody> </table> </div>					Destination	Netmask	Gateway	Cost						
Destination	Netmask	Gateway	Cost											

Routing Table

Valid: It indicates a successful routing status.

Destination: The IP address of the destination network.

Netmask: The destination Netmask address.

Gateway/Interface: The IP address of the gateway or existing interface that this route will use.

Cost: The number of hops counted as the cost of the route.

RIP Routing Table

Destination: The IP address of the destination network.


Netmask: The destination Netmask address.

Gateway: The IP address of the gateway that this route will use.

Cost: The number of hops counted as the cost of the route.

NAT Sessions

This section lists all current NAT sessions between interface of types external (WAN) and internal (LAN).

Status 


▼ NAT Sessions

No active NAT sessions between interfaces of types external and internal.

Refresh

UPnP Portmap

The section lists all port-mapping established using UPnP (Universal Plug and Play). See the **Advanced** section of this manual for more details on UPnP and the router's UPnP configuration options.

Status 


▼ UPnP Portmap

UPnP Portmap Table

Name	Protocol	External Port	Redirect Port	IP Address
------	----------	---------------	---------------	------------

Email Status

Details and status for the Email Account you have configured the router to check. Please see the **Advanced** section of this manual for details on this function.

Status 

▼ Email Status

Email Account

No accounts specified

Event Log

This page displays the router's Event Log entries. Major events are logged to this window, such as when the router's ADSL connection is disconnected, as well as Firewall events when you have enabled Intrusion or Blocking Logging in the **Configuration – Firewall** section of the interface. Please see the **Firewall** section of this manual for more details on how to enable Firewall logging.

Status

▼ Event Log

```

----- system log buffer head -----
Jan 01 00:00:00 home.gateway:ipsec:none: [INFO]Start IPSEC Initialize .....
Jan 01 00:00:00 home.gateway:ipsec:none: [INFO]Start IPSEC Initialize ..... Done
Jan 01 00:00:12 home.gateway:im:none: Changed iplan IP address to 192.168.1.254
Jan 01 00:00:21 home.gateway:im:none: Reset SNMP community to factory default
settings
----- system log buffer tail -----
                    
```

Error Log

Any errors encountered by the router (e.g. invalid names given to entries) are logged to this window.

Status

▼ Error Log

Error Log (times are in seconds since last reboot)

When	Process	Error Log

Diagnostic

It tests the connection to computer(s) which is connected to LAN ports and also the WAN Internet connection. If **PING www.google.com** is shows as FAIL and the rest show as PASS, you ought to check your PC's DNS settings is set correctly.

Status

▼ Diagnostic

LAN Connection

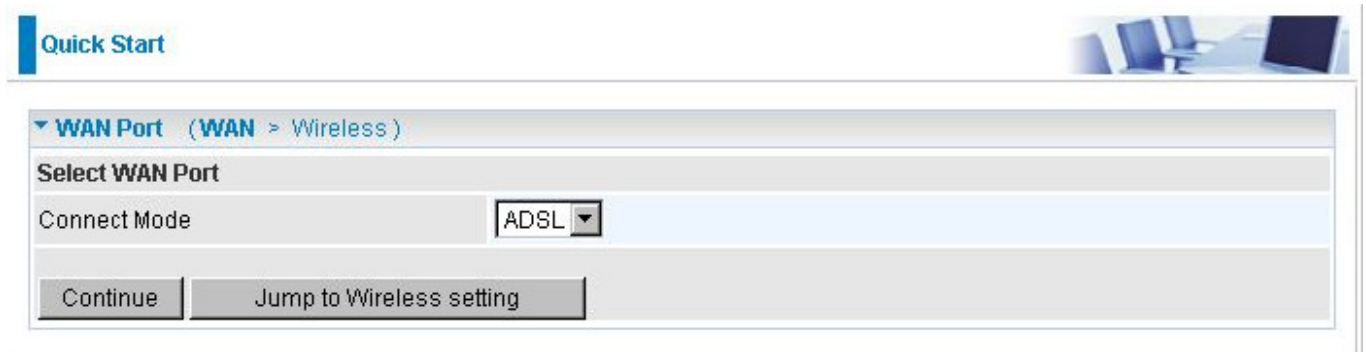
Testing Ethernet LAN connection	PASS
Testing Wireless LAN connection	PASS

WAN Connection

Testing ADSL Synchronization	FAIL
Testing WAN connection	FAIL
Ping Primary Domain Name Server	FAIL
PING www.google.com	FAIL

Quick Start

1. Click Quick Start. Select the connect mode you want. There are two options you can choose, **ADSL**. Select **ADSL** from Connect Mode drop-down menu, and click **Continue**.



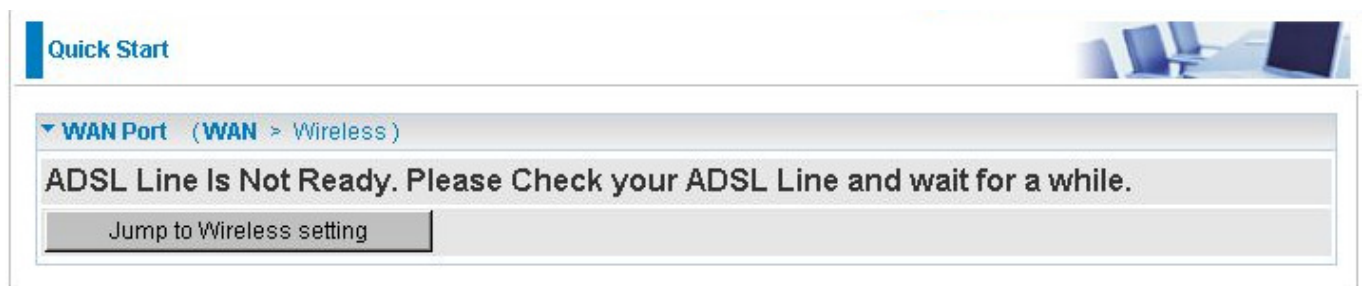
Quick Start

▼ WAN Port (WAN > Wireless)

Select WAN Port

Connect Mode

2. If your ADSL line is not ready, you need to check your ADSL line has been set or not.



Quick Start

▼ WAN Port (WAN > Wireless)

ADSL Line Is Not Ready. Please Check your ADSL Line and wait for a while.

3. If your ADSL line is ready, the screen appears ADSL Line is Ready. Choose **Auto** radio button and click **Apply**. It will automatically scan the recommended mode for you. Manually mode makes you to set the ADSL line by manual. (If you choose **Manually**, you will directly go to step 5.)

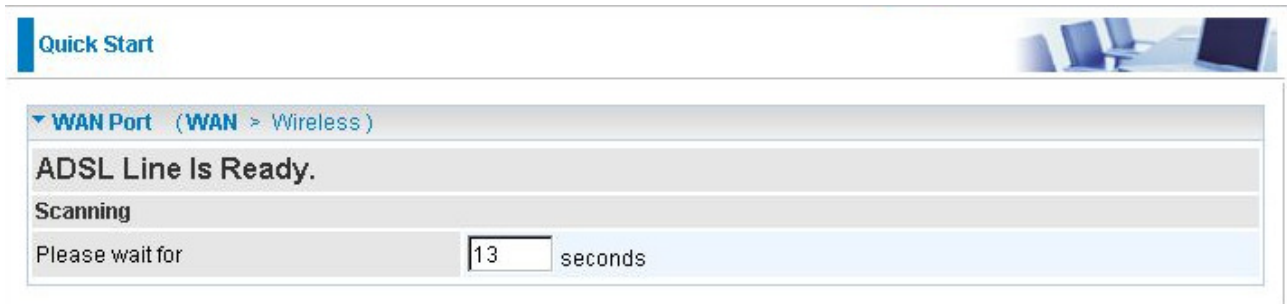


Quick Start

▼ WAN Port (WAN > Wireless)

ADSL Line Is Ready.

Auto scan Auto Manually



Quick Start

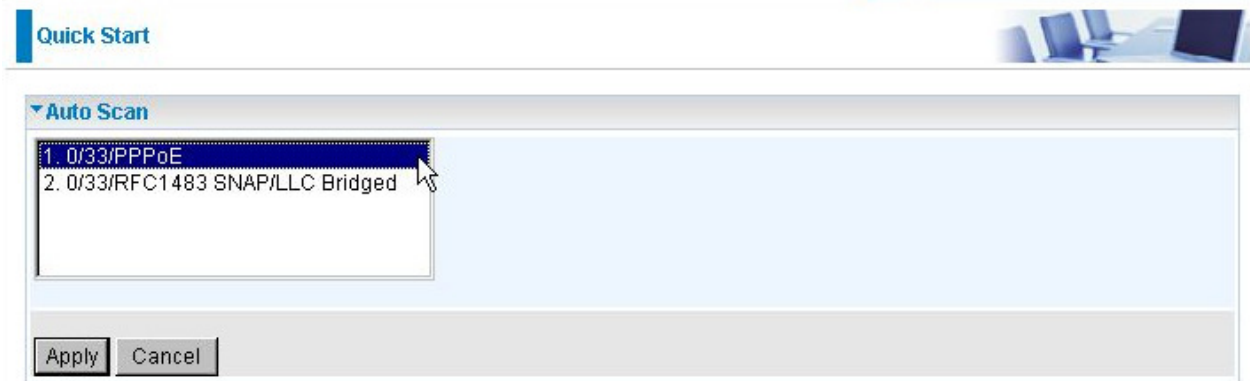
▼ WAN Port (WAN > Wireless)

ADSL Line Is Ready.

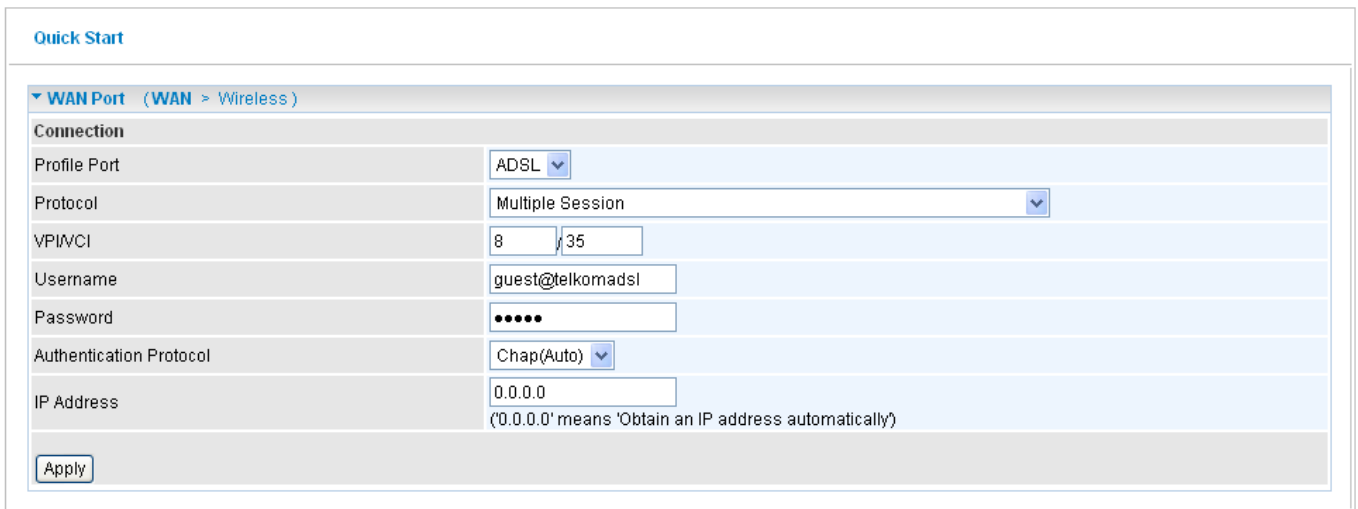
Scanning

Please wait for seconds

4. The list below has different mode applied for your choice. Choose **0/33/PPPoE(Recommended)** and click **Apply**.



5. Please enter “**Username**” and “**Password**” as supplied by your ISP(Internet Service Provider) and click **Apply** to continue.



Profile Port: Select the connection mode. There isADSL.

Encapsulation: Select the encapsulation mode. The default mode is PPPoE.

VPI/VCI: Enter the VPI and VCI information provided by your ISP.

Username: Enter the username provided by your ISP.

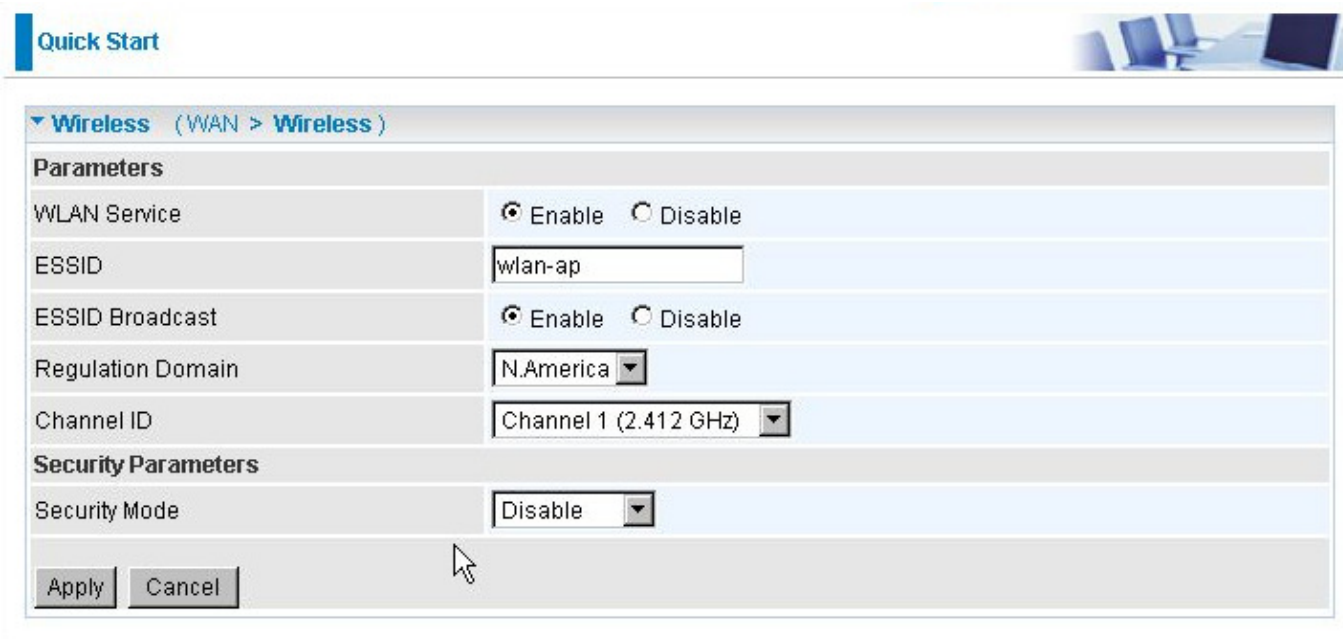
Password: Enter the password provided by your ISP.

Service Name: This item is for identification purposes. If it is required, your ISP provides you the information.

Authentication Protocol: Default is **Auto**. Your ISP advises on using **Chap** or **Pap**.

IP Address: Your WAN IP address. Leave this at 0.0.0.0 to obtain automatically an IP address from your ISP.

6. Configure the Wireless LAN setting.



Quick Start

▼ **Wireless** (WAN > Wireless)

Parameters

WLAN Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
ESSID	wlan-ap
ESSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Regulation Domain	N.America
Channel ID	Channel 1 (2.412 GHz)

Security Parameters

Security Mode	Disable
---------------	---------

Apply Cancel

WLAN Service: Default setting is set to **Enable**. If you want to use wireless, both 802.11g and 802.11b device in your network, you can select **Enable**.

ESSID: The ESSID is the unique name of a wireless access point (AP) to be distinguished from another. For security propose, change to a unique ID name to the AP which is already built-in to the router's wireless interface. It is case sensitive and must not excess 32 characters. Make sure your wireless clients have exactly the ESSID as the device, in order to get connected to your network.

ESSID Broadcast: It is function in which transmits its ESSID to the air so that when wireless client searches for a network, router can then be discovered and recognized. Default setting is **Enable**.

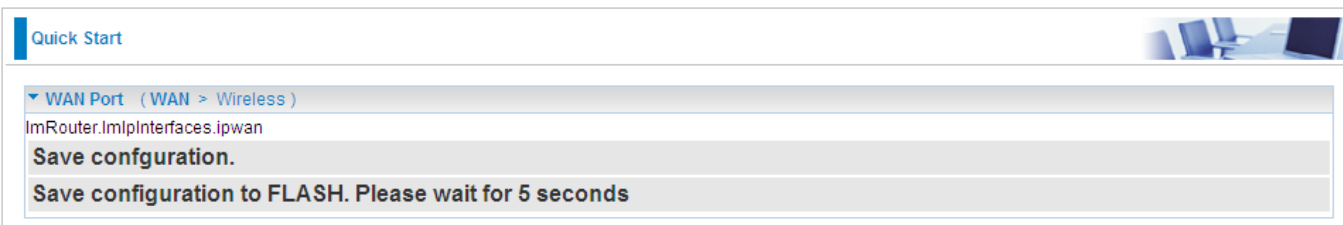
Enable: When Enable is selected, you can allow anybody with a wireless client to be able to locate the Access Point (AP) of your router.

Disable: Select Disable if you do not want broadcast your ESSID. When select Disable, no one will be able to locate the Access Point (AP) of your router.

Channel ID: Select the ID channel that you would like to use.

Security Mode: You can disable or enable with WPA or WEP for protecting wireless network. The default mode of wireless security is **Disable**.

7. Wait for the configuration.



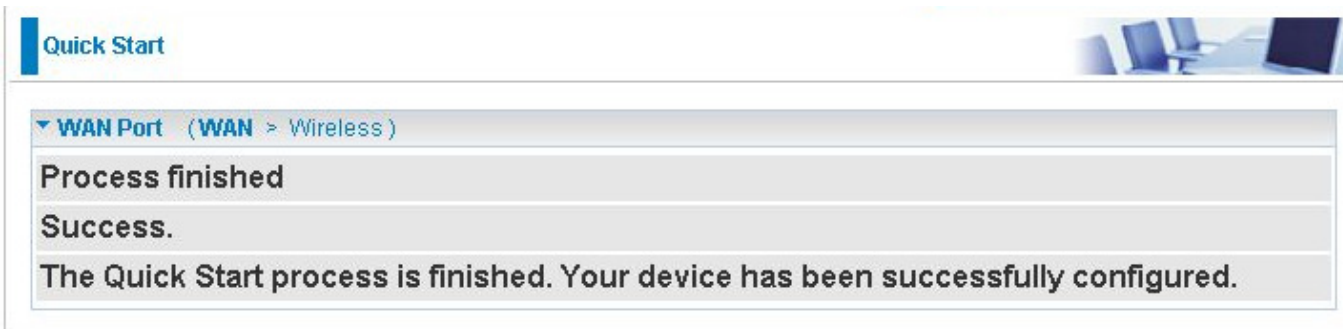
Quick Start

▼ **WAN Port** (WAN > Wireless)

ImRouter.ImlInterfaces.ipwan

Save configuration.

Save configuration to FLASH. Please wait for 5 seconds



Quick Start

▼ **WAN Port** (WAN > Wireless)

Process finished

Success.

The Quick Start process is finished. Your device has been successfully configured.

8. When ADSL is synchronic, it will appear “check”.

Status

Device Information

Model Name	Billion 400G
Host Name	home.gateway
System Up-Time	00:43:31s
Current Time	Fri, 04 Jul 2008 - 13:47:52 Sync Now
Hardware Version	Solos-W ADSL-MMWG v1.00
Software Version	5.53.s3.dh2.069
MAC Address	00:04:ED:12:40:91

Port Status

Ethernet	✓
ADSL	✓
Wireless	✓

WAN

Port	Protocol	VPI/VCI	Connection	IP Address	Subnet Mask	Default Gateway	Primary DNS
ADSL	PPPoE	8 /35	Connection established Disconnect	41.221.227.151	255.255.255.255	0.0.0.0 (Interface:ipwan)	41.223.60.26

Configuration

When you click this item, you get following sub-items to configure the ADSL router.

- LAN, WAN, System, Firewall, VPN, QoS, Virtual Server, Time Schedule and Advanced

These functions are described below in the following sections.

LAN - Local Area Network

Here are the items within the LAN section:

- Bridge Interface
- Ethernet
- IP Alias
- Ethernet Client Filter
- Wireless
- Wireless Security
- Wireless Client Filter
- WPS
- Port Settings
- DHCP Server

Bridge Interface

Configuration

Bridge Interface

Parameters

Bridge Interface	VLAN Port
ethernet	<input checked="" type="checkbox"/> P1 <input checked="" type="checkbox"/> P2 <input checked="" type="checkbox"/> P3 <input checked="" type="checkbox"/> P4
ethernet1	<input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
ethernet2	<input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4
ethernet3	<input type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> P3 <input type="checkbox"/> P4

Device Management

Management Interface	<input checked="" type="radio"/> ethernet
----------------------	---

Apply

Billion 400G Router

You can setup member ports for each VLAN group under Bridge Interface section. From the example, two VLAN groups need to be created.

Ethernet: P1 (Port 1)

Ethernet1: P2, P3 and P4 (Port 2, 3, 4). Uncheck P2, P3, P4 from Ethernet VLAN port first.

Note: You should setup each VLAN group with caution. Each Bridge Interface is arranged in this order.

Bridge Interface	VLAN Port (Always starts with)
ethernet	P1 / P2 / P3 / P4
ethernet1	P2 / P3 / P4
ethernet2	P3 / P4
ethernet3	P4

Management Interface: To specify which VLAN group has possibility to do device management, like doing web management.

Note: NAT/NAPT can be applied to management interface only.

Ethernet

Configuration

▼ Ethernet

Primary IP Address

IP Address:

Subnet Mask:

RIP: RIP v1 RIP v2 RIP v2 Multicast

Primary IP Address

IP Address: The default IP on this router.

Subnet Mask: The default subnet mask on this router.

RIP: RIP v1, RIP v2, and RIP v2 Multicast. Check to enable RIP function.

IP Alias

This function creates multiple virtual IP interfaces on this router. It helps to connect two or more local networks to the ISP or remote node. In this case, an internal router is not required.

Configuration

► IP Alias

Parameters

IP Address:

Netmask:

Security Interface: Internal ▼

Edit	IP Address	Subnet Mask	Security Interface	Delete
------	------------	-------------	--------------------	--------

IP Address: Specify an IP address on this virtual interface.

SubNetmask: Specify a subnet mask on this virtual interface.

Security Interface: Specify the firewall setting on this virtual interface.

Internal: The network is behind NAT. All traffic will do network address translation when sending out to Internet if NAT is enabled.

External: There is no NAT on this IP interface and connected to the Internet directly. Mostly it will be used when providing multiple public IP addresses by ISP. In this case, you can use public IP address in local network which gateway IP address point to the IP address on this interface.

DMZ: Specify this network to DMZ area. There is no NAT on this interface.

Ethernet Client Filter

The Ethernet Client Filter supports up to 16 Ethernet network machines that helps you to manage your network control to accept traffic from specific authorized machines or can restrict unwanted machine(s) to access your LAN.

There are no pre-define Ethernet MAC address filter rules; you can add the filter rules to meet your requirements.

The screenshot shows the 'Ethernet Client Filter' configuration page. It includes a 'Filtering Rules' table with columns for 'Ethernet Client Filter', 'Disable', 'Allowed', and 'Blocked'. The 'Disable' radio button is selected. Below the table, there is a 'MAC Address List' section with a 'Candidates' button and a note: '(MAC Address Format is 'xxxxxxxxxxxx')'. An 'Apply' button is at the bottom left.

Ethernet Client Filter: Default setting is set **Disable**.

Allowed: check to authorize specific device accessing your LAN by insert the MAC Address in the space provided or click [Candidates](#). Make sure your PC's MAC is listed.

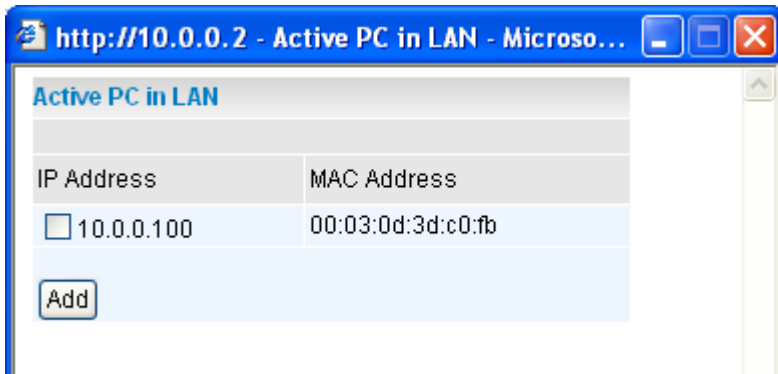
Blocked: To prevent unwanted device accessing your LAN, insert the MAC Address in the space provided or click [Candidates](#). Make sure your PC's MAC is not listed.

The maximum client is 16. The MAC addresses are 6 bytes long; they are presented only in hexadecimal characters. The number **0 - 9** and letters **a - f** are acceptable.

Note: Follow the MAC Address Format **xx:xx:xx:xx:xx:xx**. Semicolon (**:**) must be included.

Candidates: automatically detects devices connected to the router through the Ethernet. .

[Candidates](#) → **Active PC in LAN**



Active PC in LAN displays a list of individual Ethernet device's IP Address & MAC Address which connecting to the router.

You can easily by checking the box next to the IP address to be blocked or allowed. Then, **Add** to insert to the Ethernet Client Filter table. The maximum Ethernet client is 16.

Wireless

Configuration

Wireless

Parameters

WLAN Service	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Mode	802.11b + g
ESSID	wlan-ap
ESSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Regulation Domain	N.America
Channel ID	Channel 1 (2.412 GHz)
Tx PowerLevel	127 (1 ~ 127)
Connected	true
AP MAC address	00:04:ed:00:00:01
AP Firmware Version	2.17.24.0 Private

Wireless Distribution System (WDS)

WDS Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
1.Peer WDS MAC address	00:00:00:00:00:00
2.Peer WDS MAC address	00:00:00:00:00:00
3.Peer WDS MAC address	00:00:00:00:00:00
4.Peer WDS MAC address	00:00:00:00:00:00

Apply Cancel

Parameters

WLAN Service: Default setting is set to **Enable**. If you do not have any wireless devices (802.11g or 802.11b) on your network, select **Disable**.

Mode: The default setting is **802.11b+g** (Mixed mode). If you do not know what type of wireless devices you have, or have both 11g and 11b devices in your network, then keep the default setting (**mixed mode**). From the drop-down menu, you can select **802.11g** if you have only 11g clients on your network or if you have only 11b clients on your network, then select **802.11b**.

ESSID: The ESSID is the unique name of a wireless access point (AP) used to distinguish it from other AP's. For security purposes, change the default AP ID (**wlan-ap**) to a unique ID name. The ESSID is case sensitive and must not exceed 32 characters. Make sure your wireless clients have exactly the same ESSID as the AP so that you will be able to connect to it .

Billion 400G Router

ESSID Broadcast: ESSID Broadcast is the function that controls the Router's transmission of its ESSID. This transmission enables wireless clients to detect the presence of the AP when they search for AP's to connect to. The default setting is **Enabled**.

⊙ **Disable:** If you do not want broadcast your ESSID. Any client uses "any" wireless setting cannot discover the Access Point (AP) of your router.

⊙ **Enable:** Any client using the "any" setting can discover the Access Point (AP).

Regulation Domain: There are seven Regulation Domains for you to choose from, including North America (N.America), Europe, France, etc. The Channel ID will be different based on this setting.

Channel ID: Select the wireless connection ID channel that you would like to use. Use the *Scan Channel Usage* to help to select non-occupied wireless channel.

⊙ **Scan Channel Usage:** Wireless channel scan takes up to 14 seconds to survey the wireless channels in the surrounding area. The result will show which of the wireless channels are already being used, and which are available for use.

Note: Wireless performance may degrade if select ID channel is already being occupied by other AP(s).

TX PowerLevel: This function enhances the wireless transmitting signal strength. Users may adjust this power level from minimum 0 up to maximum 255.

Note: Maximum power Level is not necessarily the best choice in all cases. Choose the most suitable level for your network and environment.

Connected: Representing in **true** or **false**. That it is the connection status between the system and the build-in wireless card.

AP MAC Address: It is a unique hardware address of the Access Point.

AP Firmware Version: The Access Point firmware version.

Wireless Distribution System (WDS)

This is a wireless access point mode that enables wireless linking and communication with other access points. It is easy to install - simply define the peer AP's MAC address. The WDS system gives a cost saving and flexible method of extending wireless range, since no extra wireless client device is required to bridge between two access points. Using WDS, the user can extend an existing wired or wireless infrastructure network to create a larger network.

In addition, WDS enhances its link connection security in WEP mode, WEP key encryption must be the same for both access points.

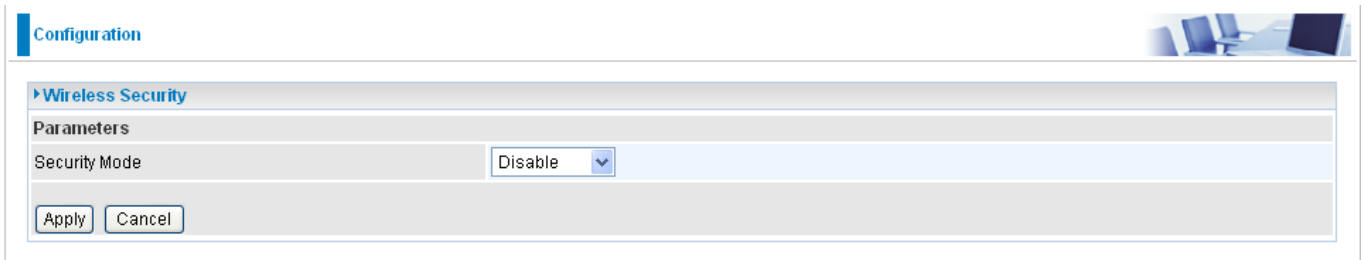
WDS Service: The default setting is **Disabled**. Check **Enable** radio button to activate this function.

Peer WDS MAC Address: this is the associated AP's MAC Address. It is important that your peer's AP must include your MAC address in order to allow the AP's to acknowledge and communicate with each other.

Note: For MAC Address, Semicolon (:) must be included.

Wireless Security

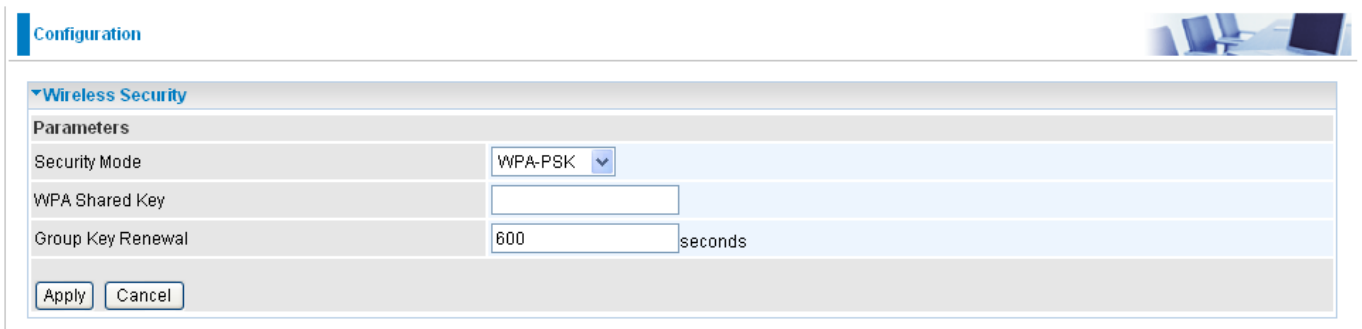
You can disable or enable WPA or WEP for protecting your wireless network. The default mode of wireless security is Enabled. And the default security mode is WPA.



The screenshot shows the 'Configuration' page for the Billion 400G Router. Under the 'Wireless Security' section, the 'Parameters' table is visible. The 'Security Mode' is set to 'Disable'. There are 'Apply' and 'Cancel' buttons at the bottom of the configuration area.

Parameters	
Security Mode	Disable

WPA-PSK / WPA2-PSK / WEP



The screenshot shows the 'Configuration' page for the Billion 400G Router. Under the 'Wireless Security' section, the 'Parameters' table is visible. The 'Security Mode' is set to 'WPA-PSK'. The 'WPA Shared Key' field is empty. The 'Group Key Renewal' is set to '600' seconds. There are 'Apply' and 'Cancel' buttons at the bottom of the configuration area.

Parameters	
Security Mode	WPA-PSK
WPA Shared Key	
Group Key Renewal	600 seconds

WPA Algorithms: There are two types of the WPA-PSK, WPA-PSK and WPA2-PSK. The WPA-PSK adapts the TKIP (Temporal Key Integrity Protocol) encrypted algorithms, which incorporates Message Integrity Code (MIC) to provide protection against hackers. The WPA2-PSK adapts CCMP (Cipher Block Chaining Message Authentication Code Protocol) of the AES (Advanced Encryption Security) algorithms.

WPA Shared Key: The key for network authentication. The input format is in character style and key size should be in the range between 8 and 63 characters. By default, your Router is provided with a unique Key. This key is also given on a label on the underside of your router.

Group Key Renewal: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). Default value is **3600** seconds.

Configuration



Wireless Security	
Parameters	
Security Mode	WEP
WEP Authentication	Open System
WEP Encryption	<input checked="" type="radio"/> WEP64 <input type="radio"/> WEP128 Hex
Passphrase	<input type="text"/> <input type="button" value="Generate"/>
Default Used WEP Key	1 (1~4)
Key 1	0000000000
Key 2	0000000000
Key 3	0000000000
Key 4	0000000000
HINT: Input 10 hexadecimal digits (0-9, a-f) in Key.	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

WEP Authentication: To prevent unauthorized wireless stations from accessing data transmitted over the network, the router offers secure data encryption, known as WEP. If you require high security for transmissions, there are two options to select from: **Open System, Share key**.

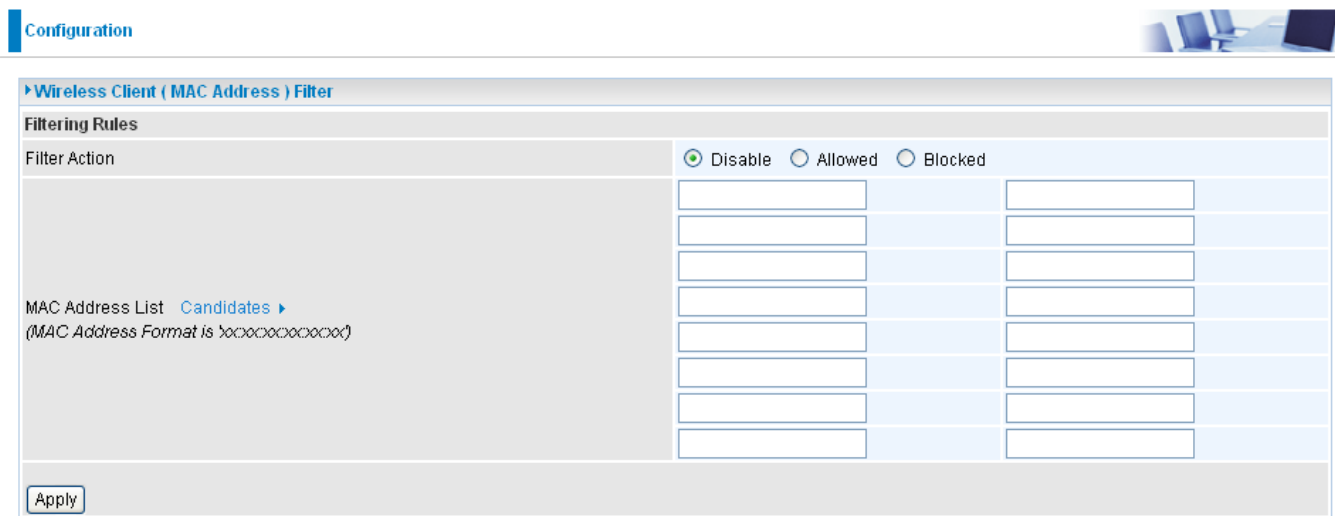
WEP Encryption: To prevent unauthorized wireless stations from accessing data transmitted over the network, the router offers highly secure data encryption, known as WEP. If you require high security for transmissions, there are two alternatives to select from: **WEP 64 and WEP 128**. WEP 128 will offer increased security over WEP 64.

Passphrase: This is used to generate WEP keys automatically based upon the input string and a pre-defined algorithm in WEP64 or WEP128. **Default Used WEP Key:** Select the encryption key ID; please refer to **Key (1~4)** below.

Key (1-4): Enter the key to encrypt wireless data. To allow encrypted data transmission, the WEP Encryption Key values on all wireless stations must be the same as the router. There are four keys for your selection. The input format is in HEX style, 5 and 13 HEX codes are required for WEP64 and WEP128 respectively, the separator is “-“. For example, using WEP64, 11-22-33-44-55 is a valid key, whilst 1122334455 is invalid.

Wireless Client / MAC Address Filter

The MAC Address supports up to 16 wireless network machines and helps you to manage your network control to accept traffic from specific authorized machines or to restrict unwanted machine(s) from accessing your LAN. There are no pre-define MAC Address filter rules; you can add the filter rules to meet your requirements.



Wireless Client Filter: Default setting is set to **Disable**.

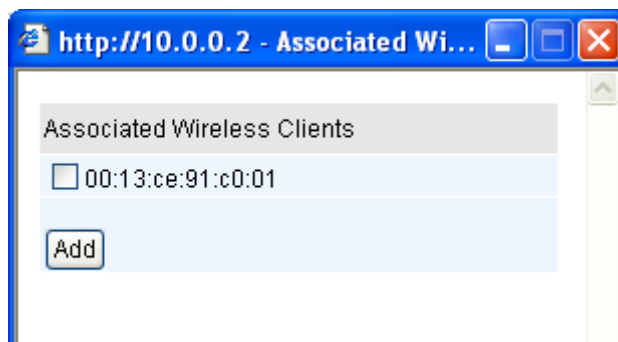
- ⊙ **Allowed:** To allow a specific device access to your LAN, insert the devices MAC Address in the space provided, or click [Candidates](#). Make sure your computer's MAC is listed.
- ⊙ **Blocked:** To prevent unwanted devices from accessing the LAN, insert the MAC Address of an unwanted computer into the space provided, or click [Candidates](#). Make sure your computer's MAC is not listed.

The maximum number of clients is 16. MAC addresses are 6 bytes long; they are presented only in hexadecimal format. The numbers **0 - 9** and letters **a - f** are acceptable. MAC addresses are 6 bytes long

Note: Follow the MAC Address Format **xx:xx:xx:xx:xx:xx**. Semicolon (:) must be included.

Candidates: This function automatically detects devices connected to the router through the Wireless AP.

[Candidates](#) → **Associated Wireless Clients**

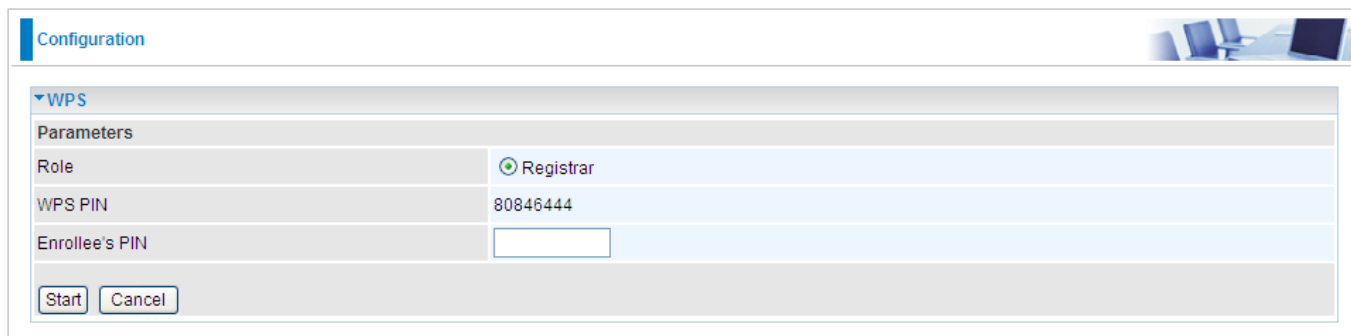


Associate Wireless Client displays a list of individual wireless device's MAC Address that are currently connected to the router.

You can easily add a particular client to the Allow or Block list by checking the box next to the MAC address and selecting Add to insert to the client into the Wireless Client (MAC Address) Filter table.

WPS

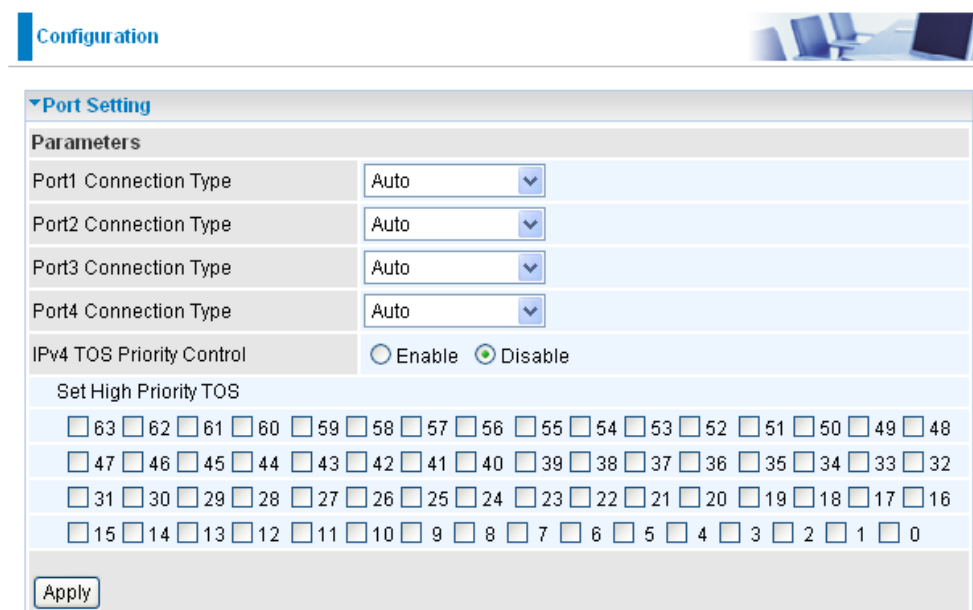
The WPS feature uses the Wi-Fi Alliance standard to allow easy set up of security-enabled Wi-Fi networks in the home and small office environments. WPS supports two connection methods (via the routers Web GUI and through the push button found on the rear panel) that will significantly reduce the number of steps required to set up the network.



Parameters	
Role	<input checked="" type="radio"/> Registrar
WPS PIN	80846444
Enrollee's PIN	<input type="text"/>

Port Setting

This section allows you to configure the settings for the router's Ethernet ports to solve some of the compatibility problems that may be encountered while connecting to the Internet, as well allowing users to tweak the performance of their network.



Parameters	
Port1 Connection Type	Auto
Port2 Connection Type	Auto
Port3 Connection Type	Auto
Port4 Connection Type	Auto
IPv4 TOS Priority Control	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Set High Priority TOS	
<input type="checkbox"/> 63	<input type="checkbox"/> 62 <input type="checkbox"/> 61 <input type="checkbox"/> 60 <input type="checkbox"/> 59 <input type="checkbox"/> 58 <input type="checkbox"/> 57 <input type="checkbox"/> 56 <input type="checkbox"/> 55 <input type="checkbox"/> 54 <input type="checkbox"/> 53 <input type="checkbox"/> 52 <input type="checkbox"/> 51 <input type="checkbox"/> 50 <input type="checkbox"/> 49 <input type="checkbox"/> 48
<input type="checkbox"/> 47	<input type="checkbox"/> 46 <input type="checkbox"/> 45 <input type="checkbox"/> 44 <input type="checkbox"/> 43 <input type="checkbox"/> 42 <input type="checkbox"/> 41 <input type="checkbox"/> 40 <input type="checkbox"/> 39 <input type="checkbox"/> 38 <input type="checkbox"/> 37 <input type="checkbox"/> 36 <input type="checkbox"/> 35 <input type="checkbox"/> 34 <input type="checkbox"/> 33 <input type="checkbox"/> 32
<input type="checkbox"/> 31	<input type="checkbox"/> 30 <input type="checkbox"/> 29 <input type="checkbox"/> 28 <input type="checkbox"/> 27 <input type="checkbox"/> 26 <input type="checkbox"/> 25 <input type="checkbox"/> 24 <input type="checkbox"/> 23 <input type="checkbox"/> 22 <input type="checkbox"/> 21 <input type="checkbox"/> 20 <input type="checkbox"/> 19 <input type="checkbox"/> 18 <input type="checkbox"/> 17 <input type="checkbox"/> 16
<input type="checkbox"/> 15	<input type="checkbox"/> 14 <input type="checkbox"/> 13 <input type="checkbox"/> 12 <input type="checkbox"/> 11 <input type="checkbox"/> 10 <input type="checkbox"/> 9 <input type="checkbox"/> 8 <input type="checkbox"/> 7 <input type="checkbox"/> 6 <input type="checkbox"/> 5 <input type="checkbox"/> 4 <input type="checkbox"/> 3 <input type="checkbox"/> 2 <input type="checkbox"/> 1 <input type="checkbox"/> 0

Port # Connection Type: this is where you can customize the connection type of each of the routers Ethernet ports. There are Six options to choose from: Auto, disable, 10M half-duplex, 10M full-duplex, 100M half-duplex, 100M full-duplex and Disable. Sometimes, there are Ethernet compatibility problems with legacy Ethernet devices, and you can configure a particular Ethernet port to one of the different types to solve compatibility issues. The default is **Auto**, which users should keep unless there are specific problems with computers not being able to access your LAN.

IPv4 TOS priority Control (Advanced users): TOS, Type of Services, is the 2nd octet of an IP packet. Bits 6-7 of this octet are reserved and bit 0-5 are used to specify the priority of the packet.

This feature uses bits 0-5 to classify the packet's priority. If the packet is high priority, it will flow first and will not be constrained by the Rate Limit. Therefore, when this feature is enabled, the router's Ethernet switch will check the 2nd octet of each IP packet. If the value in the TOS field matches the checked values in the table (0 to 63), this packet will be treated as high priority.

DHCP Server

You can disable or enable the DHCP (Dynamic Host Configuration Protocol) server or enable the router's DHCP relay functions. The DHCP protocol allows your router to dynamically assign IP addresses to PCs on your network if they are configured to obtain IP addresses automatically.

Configuration

▼ DHCP Server

Configuration

DHCP Server Mode	<input type="radio"/> Disable <input checked="" type="radio"/> DHCP Server <input type="radio"/> DHCP Relay Agent
------------------	---

DHCP Server Status

Allow Bootp	true
Allow Unknown Clients	true
Enable	true

Subnet Definitions

Subnet Value	10.0.0.0
Subnet Mask	255.255.255.0
Maximum Lease Time	86400 seconds
Default Lease Time	43200 seconds
Use local host address as DNS server	true
Use local host address as default gateway	true
Get subnet from IP interface	iplan
IP Range	10.0.0.100- 10.0.0.199
Option	domain-name-servers= 0.0.0.0

To disable the router's DHCP Server, check **Disabled** and click **Next**, then click **Apply**. When the DHCP Server is disabled you will need to manually assign a fixed IP address to each PCs on your network, and set the default gateway for each PCs to the IP address of the router (by default this is 10.0.0.2).

To configure the router's DHCP Server, check **DHCP Server** and click **Next**. You can then configure parameters of the DHCP Server including the IP pool (starting IP address and ending IP address to be allocated to PCs on your network), lease time for each assigned IP address (the period of time the IP address assigned will be valid), DNS IP address and the gateway IP address. These details are sent to the DHCP client (i.e. your PC) when it requests an IP address from the DHCP server. Click **Apply** to enable this function. If you check "**Use Router as a DNS Server**", the ADSL Router will perform the domain name lookup, find the IP address from the outside network automatically and forward it back to the requesting PC in the LAN (your Local Area Network).

If you check **DHCP Relay Agent** and click **Next**, then you will have to enter the IP address of the DHCP server which will assign an IP address back to the DHCP client in the LAN. Use this function only if advised to do so by your network administrator or ISP.

Click **Apply** to enable this function.

WAN - Wide Area Network

WAN refers to your Wide Area Network connection, i.e. your router's connection to your ISP and the Internet. Here are the items within the **WAN** section: [WAN Profile](#) and [ADSL Mode](#).

WAN Profile

PPPoE Connection

PPPoE (PPP over Ethernet) provides access control in a manner which is similar to dial-up services using PPP.

Configuration

WAN Connection

PPPoE Routed

Profile Port:

Protocol:

Description: VPI/VCI: / ATM Class:

Username: Password: Service Name:

NAT: Enable IP (0.0.0.0: Auto): Auth. Protocol:

Connection: Idle Timeout: min(s) MTU:

RIP: RIP v1 RIP v2 RIP v2 Multicast TCP MSS Clamp: Enable

MAC Spoofing: Enable : : : : :

Obtain DNS: Automatic Primary: Secondary:

Edit	Name	Description	Creator	VPI	VCI	Delete
<input checked="" type="radio"/>	wanlink	PPPoE Routed with Multiple Session	WebAdmin	8	35	

Profile Port: Select the profile port ADSL.

Protocol: The ATM protocol will be used in the device.

Description: A given name for the connection.

VPI/VCI: Enter the information provided by your ISP.

ATM Class: The Quality of Service for ATM layer.

Username: Enter the username provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive). This is in the format of "username@ispname".

Password: Enter the password provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive).

Service Name: This item is for identification purposes. If it is required, your ISP will provide you the information. Maximum input is **15** alphanumeric characters.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing the single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

IP (0.0.0.0:Auto): Specify IP addresses that are allowed to logon and access the router's web server.

Note: IP 0.0.0.0 indicates all users who are connected to this router are allowed to logon to the device and modify data.

Auth. Protocol: Default is Chap(Auto). Your ISP will advise you whether to use Chap or Pap.

Connection:

⊙ **Always on:** If you want the router to establish a PPPoE session when starting up and to automatically re-establish the PPPoE session when disconnected by the ISP.

⊙ **Connect on Demand:** If you want to establish a PPPoE session only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet).

Idle Timeout: Auto-disconnect the router when there is no activity on the line for a predetermined period of time.

⊙ **Detail:** You can define destination port and packet type (TCP/UDP) information that will not result in the router checking the timer. It allows you to set which outgoing traffic will not trigger and reset the idle timer.

MTU: Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

RIP: RIP v1, RIP v2, and RIP v2 Multicast. Check to enable RIP function.

TCP MSS Clamp: This option helps to discover the optimal MTU size automatically. Default is enabled.

MAC Spoofing: This option is required by some service providers. You must fill in the MAC address that has been specified by the service provider when it is required. Default is disabled.

Obtain DNS: A Domain Name System (DNS) contains a mapping table for mapping between Domain Names and IP addresses. On the Internet, every host has a unique and user-friendly name (domain name) such as www.helloworld.com as well as an IP address. An IP address is a 32-bit number in the form of xxx.xxx.xxx.xxx, for example 10.0.0.2. You can think of an IP address as a telephone number for devices on the Internet, and the DNS will allow you to find the telephone number for any particular domain name. As an IP Address is hard to remember, the DNS converts the friendly name into its equivalent IP Address.

You can obtain a Domain Name System (DNS) IP address automatically if your ISP provides it when you logon. To use this automatically supplied DNS check the **Enable** box.

Primary DNS: Enter the primary DNS.

Secondary DNS: Enter the secondary DNS

PPPoA Connection

Configuration

WAN Connection

PPPoA Routed

Profile Port:

Protocol:

Description: VPI/VCI: / ATM Class:

Username: Password:

NAT: Enable IP (0.0.0.0: Auto): Auth. Protocol:

Connection: Idle Timeout: min(s) MTU:

RIP: RIP v1 RIP v2 RIP v2 Multicast TCP MSS Clamp: Enable

Obtain DNS: Automatic Primary: Secondary:

Edit	Name	Description	Creator	VPI	VCI	Delete
<input checked="" type="radio"/>	wanlink	PPPoE Routed with Multiple Session	WebAdmin	8	35	

Profile Port: Select the profile port ADSL.

Protocol: The ATM protocol will be used in the device.

Description: User-definable name for the connection.

VPI/VCI: Enter the information provided by your ISP.

ATM Class: The Quality of Service for ATM layer.

Username: Enter the username provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive). This will usually be in the format of “username@ispname” instead of simply “username”.

Password: Enter the password provided by your ISP. You can input up to **128** alphanumeric characters (case sensitive).

Billion 400G Router

Service Name: This item is for identification purposes. If it is required, your ISP will provide you the information. Maximum input is **15** alphanumeric characters.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

IP (0.0.0.0:Auto): Specify IP addresses that are allowed to logon and access the router's web server..

Note: IP 0.0.0.0 indicates all users who are connected to this router are allowed to logon to the device and modify data.

Auth. Protocol: Default is Chap (Auto). Your ISP will advise you whether to use Chap or Pap.

Connection:

Always on: If you want the router to establish a PPPoA session when starting up and to automatically re-establish the PPPoA session when disconnected by the ISP.

Connect on Demand: If you want to establish a PPPoA session only when there is a packet requesting access to the Internet (i.e. when a program on your computer attempts to access the Internet).

Idle Timeout: Auto-disconnect the broadband firewall gateway when there is no activity on the line for a predetermined period of time.

Detail: You can define destination port and packet type (TCP/UDP) information that will not result in the router checking the timer. It allows you to set which outgoing traffic will not trigger and reset the idle timer.

MTU: Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

RIP: RIP v1, RIP v2, and RIP v2 Multicast. Check to enable RIP function.

TCP MSS Clamp: This option helps to discover the optimal MTU size automatically. Default is enabled.

Obtain DNS: A Domain Name System (DNS) contains a mapping table for mapping between Domain Names and IP addresses. On the Internet, every host has a unique and user-friendly name (domain name) such as www.helloworld.com as well as an IP address. An IP address is a 32-bit number in the form of xxx.xxx.xxx.xxx, for example 10.0.0.2. You can think of an IP address as a telephone number for devices on the Internet, and the DNS will allow you to find the telephone number for any particular domain name. As an IP Address is hard to remember, the DNS converts the friendly name into its equivalent IP Address.

You can obtain a Domain Name System (DNS) IP address automatically if your ISP provides it when you logon. To use this automatically supplied DNS check the **Enable** box.

Primary DNS: Enter the primary DNS.

Secondary DNS: Enter the secondary DNS.

MPoA Connection

Configuration

WAN Connection

RFC 1483 Routed

Profile Port:

Protocol:

Description: VPI/VCI: / ATM Class:

NAT: Enable Encap. Method: MTU:

IP (0.0.0.0: Auto): Netmask: Gateway:

RIP: RIP v1 RIP v2 RIP v2 Multicast TCP MSS Clamp: Enable

MAC Spoofing: Enable : : : : :

Obtain DNS: Automatic Primary: Secondary:

Edit	Name	Description	Creator	VPI	VCI	Delete
<input type="checkbox"/>	wanlink	PPPoE Routed with Multiple Session	WebAdmin	8	35	<input type="checkbox"/>

Profile Port: Select the profile port ADSL.

Protocol: The ATM protocol will be used in the device.

Description: User-definable name for the connection.

VPI/VCI: Enter the information provided by your ISP.

ATM Class: The Quality of Service for ATM layer.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

Encap. mode: Select the encapsulation format, this is provided by your ISP.

MTU: Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

IP (0.0.0.0:Auto): Enter the WAN IP for the router. Leave this at 0.0.0.0 to obtain an IP address automatically from your ISP.

Netmask: The default is 255.255.255.0. This can be changed according to the settings assigned by you ISP.

Gateway: Enter the IP address of the default gateway (if specified).

RIP: RIP v1, RIP v2, and RIP v2 Multicast. Check to enable RIP function.

TCP MSS Clamp: This option helps to discover the optimal MTU size automatically. Default is enabled.

MAC Spoofing: This option is required by some service providers. You must fill in the MAC address that has been specified by the service provider when it is required. Default is disabled.

Obtain DNS: A Domain Name System (DNS) contains a mapping table for mapping between Domain Names and IP addresses. On the Internet, every host has a unique and user-friendly name (domain name) such as www.helloworld.com as well as an IP address. An IP address is a 32-bit number in the form of xxx.xxx.xxx.xxx, for example 10.0.0.2. You can think of an IP address as a telephone number for devices on the Internet, and the DNS will allow you to find the telephone number for any particular domain name. As an IP Address is hard to remember, the DNS converts the friendly name into its equivalent IP Address.

You can obtain a Domain Name System (DNS) IP address automatically if your ISP provides it when you logon. To use this automatically supplied DNS check the **Enable** box.

Primary DNS: Enter the primary DNS.

Secondary DNS: Enter the secondary DNS.

IPoA Routed Connection

Configuration

WAN Connection

IPoA Routed

Profile Port: ADSL

Protocol: IPoA (RFC1577, Classic IP and ARP over ATM)

Description: IPoA routed VPI/VCI: 8 / 35 ATM Class: UBR

NAT: Enable MTU: 1500

IP (0.0.0.0: Auto): 0.0.0.0 Netmask: 0.0.0.0 Gateway:

RIP: RIP v1 RIP v2 RIP v2 Multicast TCP MSS Clamp: Enable

Obtain DNS: Automatic Primary: Secondary:

Edit	Name	Description	Creator	VPI	VCI	Delete
<input checked="" type="radio"/>	wanlink	PPPoE Routed with Multiple Session	WebAdmin	8	35	

Profile Port: Select the profile port ADSL.

Protocol: The ATM protocol will be used in the device.

Description: User-definable name for the connection.

VPI/VCI: Enter the information provided by your ISP.

ATM Class: The Quality of Service for ATM layer.

NAT: The NAT (Network Address Translation) feature allows multiple users to access the Internet through a single IP account, sharing a single IP address. If users on your LAN have public IP addresses and can access the Internet directly, the NAT function can be disabled.

MTU: Maximum Transmission Unit. The size of the largest datagram (excluding media-specific headers) that IP will attempt to send through the interface.

IP (0.0.0.0:Auto): Enter the WAN IP for the router. Leave this at 0.0.0.0 to obtain an IP address automatically from your ISP.

Netmask: The default is 255.255.255.0. This can be changed according to the settings assigned by you ISP.

Gateway: Enter the IP address of the default gateway (if specified).

RIP: RIP v1, RIP v2, and RIP v2 Multicast. Check to enable RIP function.

TCP MSS Clamp: This option helps to discover the optimal MTU size automatically. Default is enabled.

Obtain DNS: A Domain Name System (DNS) contains a mapping table for mapping between Domain Names and IP addresses. On the Internet, every host has a unique and user-friendly name (domain name) such as www.helloworld.com as well as an IP address. An IP address is a 32-bit number in the form of xxx.xxx.xxx.xxx, for example 10.0.0.2. You can think of an IP address as a telephone number for devices on the Internet, and the DNS will allow you to find the telephone number for any particular domain name. As an IP Address is hard to remember, the DNS converts the friendly name into its equivalent IP Address.

You can obtain a Domain Name System (DNS) IP address automatically if your ISP provides it when you logon. To use this automatically supplied DNS check the **Enable** box.

Primary DNS: Enter the primary DNS.

Secondary DNS: Enter the secondary DNS.

Pure Bridge

Configuration

WAN Connection

RFC 1483 Bridged

Profile Port: ADSL

Protocol: Pure Bridge

Description: RFC 1483 bridged mod VPI/VCI: 8 / 35 ATM Class: UBR

Encap. Method: LLC Bridged Acceptable Frame Type: acceptall Filter Type: All

Obtain DNS: Automatic Primary: Secondary:

Apply

Edit	Name	Description	Creator	VPI	VCI	Delete
	wanlink	PPPoE Routed with Multiple Session	WebAdmin	8	35	

Profile Port: Select the profile port ADSL.

Protocol: The ATM protocol will be used in the device.

Description: User-definable name for the connection.

VPI/VCI: Enter the information provided by your ISP.

ATM Class: The Quality of Service for ATM layer.

Encap. mode: Select the encapsulation format, this is provided by your ISP.

Acceptable Frame Type: Specify which kind of traffic goes through this connection, all traffic or only VLAN tagged.

Filter Type: Specify the type of ethernet filtering performed by the named bridge interface.

All	Allows all types of ethernet packets through the port.
IP	Allows only IP/ARP types of ethernet packets through the port.
PPPoE	Allows only PPPoE types of ethernet packets through the port.

Obtain DNS: A Domain Name System (DNS) contains a mapping table for mapping between Domain Names and IP addresses. On the Internet, every host has a unique and user-friendly name (domain name) such as www.helloworld.com as well as an IP address. An IP address is a 32-bit number in the form of xxx.xxx.xxx.xxx, for example 10.0.0.2. You can think of an IP address as a telephone number for devices on the Internet, and the DNS will allow you to find the telephone number for any particular domain name. As an IP Address is hard to remember, the DNS converts the friendly name into its equivalent IP Address.

You can obtain a Domain Name System (DNS) IP address automatically if your ISP provides it when you logon. To use this automatically supplied DNS check the **Enable** box.

Primary DNS: Enter the primary DNS.

Secondary DNS: Enter the secondary DNS.

ADSL Mode



Configuration

ADSL Mode	
Parameters	
Connect Mode	All
Modulation	G.Dmt.BisPlusAuto
Profile Type	MAIN
Activate Line	true
Coding Gain	auto
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Connect Mode: This mode will automatically detect your ADSL line mode, ADSL2+, ADSL2, G.dmt, G.lite, T1.413, AnnexM2 or AnnexM2+. But in some areas, multimode cannot detect the ADSL line mode very well. If it is the case, please adjust the ADSL line code to G.dmt first. If it still fails, please check with your ISP for line connection information.

Modulation: It will automatically detect capability of your ADSL line mode. Please keep the factory settings unless ADSL is detected as the symptom of a synchronization problem.

Profile Type: The profile type should be left in the default settings unless the ADSL mode is determined as the symptom of low link rate or instability problems. If such a problem is encountered, the profile setting may need to be changed to conform to the different DSLAM in the area.


Activate Line: Select **false** and then select **true** to activate any new **Connect Mode** settings.

Coding Gain: This reduces the router's transmit power and will effect to router's downstream performance. General, the higher the gain, the higher the downstream rate, but sometimes a gain that is too high will cause an unstable ADSL connection. The configurable ADSL coding gain is from 0 dB to 7dB, or automatic.

System

Here are the items within the **System** section: [Time Zone](#), [Remote Access](#), [Firmware Upgrade](#), [Backup/Restore](#), [Restart](#) and [User Management](#).


Time Zone

Configuration


Time Zone

Parameters

Time Zone	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Time Zone List	<input type="radio"/> By City <input checked="" type="radio"/> By Time Difference	
Local Time Zone (+-GMT Time)	<input type="text" value="(GMT+02:00) Middle European Summer [MEST"/>	
SNTP Server IP Address	1. <input type="text" value="igubu.saix.net"/>	2. <input type="text" value="sangoma.saix.net"/>
	3. <input type="text" value="induna.saix.net"/>	4. <input type="text" value="time-b.nist.gov"/>
	<input type="checkbox"/> Enabled	
	Resync Period <input type="text" value="1440"/> minutes	

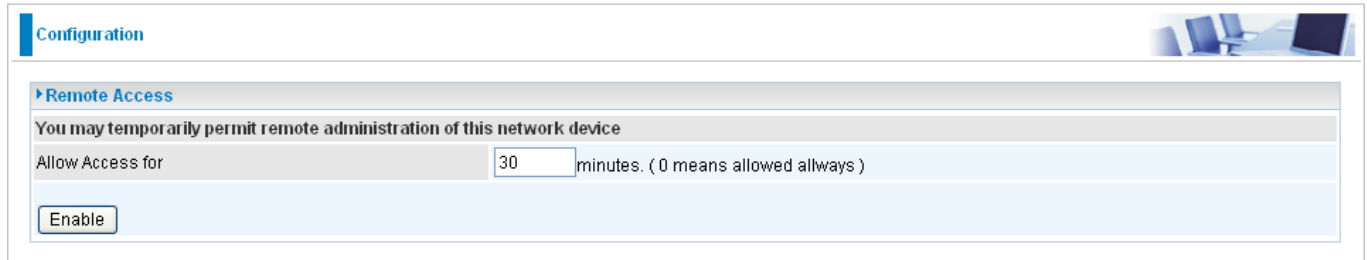


The router does not have a real time clock on board; instead, it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server outside your network. Choose your local time zone, click **Enable** and click the **Apply** button. After a successful connection to the Internet, the router will retrieve the correct local time from the SNTP server you have specified. If you prefer to specify an SNTP server other than those in the list, simply enter its IP address as shown above. Your ISP may provide an SNTP server for you to use.

Daylight Saving is also known as **Summer Time Period**. Many places in the world adapt it during summer time to move one hour of daylight from morning to the evening in local standard time. Check **Automatic** box to auto set your local time.

Resync Period (in minutes) is the periodic interval that the router will wait before it re-synchronizes the router's time with that of the specified SNTP server. In order to avoid unnecessarily increasing the load on your specified SNTP server you should keep the poll interval as high as possible – at the absolute minimum every few hours or even days.

Remote Access



Configuration

Remote Access

You may temporarily permit remote administration of this network device

Allow Access for minutes. (0 means allowed allways)

To temporarily permit remote administration of the router (i.e. from outside your LAN), select a time period the router will permit remote access for and click **Enable**. You may change other configuration options for the web administration interface using **Device Management** options in the **Advanced** section of the GUI.

If you wish to permanently enable remote access, choose a time period of 0 minute.

Firmware Upgrade



Configuration

Firmware Upgrade

You may upgrade the system software on your network device

New Firmware Image

Your router's "firmware" is the software that allows it to operate and provides all its functionality. Think of your router as a dedicated computer, and the firmware as the software it runs. Over time this software may be improved and revised, and your router allows you to upgrade the software it runs to take advantage of these changes.

Clicking on **Browse** will allow you to select the new firmware image file you have downloaded to your PC. Once the correct file is selected, click Upgrade to update the firmware in your router.



DO NOT power down the router or interrupt the firmware upgrading while it is still in process. Improper operation could damage the router.

Configuration

▶ Backup/Restore

Allows you to backup the configuration settings to your computer, or restore configuration from your computer.

Backup Configuration

Backup configuration to your computer.

Restore Configuration

Configuration File

"Restore" will overwrite the current configuration and restart the device. If you want to keep the current configuration, please use "Backup" first to save current configuration.

These functions allow you to save and backup your router's current settings to a file on your PC, or to restore a previously saved backup. This is useful if you wish to experiment with different settings, knowing that you have a backup handy in the case of any mistakes. It is advisable to backup your router's settings before making any significant changes to your router's configuration.

Press **Backup** to select where on your local PC to save the settings file. You may also change the name of the file when saving if you wish to keep multiple backups.

Press **Browse** to select a file from your PC to restore. You should only restore settings files that have been generated by the Backup function, and that were created when using the **current version** of the router's firmware. **Settings files saved to your PC should not be manually edited in any way.**

After selecting the settings file you wish to use, pressing **Restore** will load those settings into the router.

Restart Router

Click **Restart** with option **Current Settings** to reboot your router (and restore your last saved configuration).

If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select **Factory Default Settings** to reset to factory default settings.

You may also reset your router to factory settings by holding the small RESET pinhole button on the back of your router in for 6 – 8 seconds whilst the router is turned on, and then power cycling your router.

User Management

Valid	User	Comment	Password	Confirm Password
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Add Edit / Delete

Edit	Valid	User	Comment	Delete
<input type="radio"/>	true	admin	Default admin user	

In order to prevent unauthorized access to your router’s configuration interface, it requires all users to login with a password. You can set up multiple user accounts, each with their own password.

You are able to **Edit** existing users and **Add** new users who are able to access the device’s configuration interface. Once you have clicked on **Edit**, you are shown the following options:

Valid	User	Comment	Password	Confirm Password
<input checked="" type="checkbox"/>	admin	Default admin user	•••••	•••••

Add Edit / Delete

Edit	Valid	User	Comment	Delete
<input checked="" type="radio"/>	true	admin	Default admin user	

You can change the user’s **password**, whether their account is active and **valid**, as well as add a comment to each user account. Click Edit/Delete button to save your revise. You cannot delete the default admin account; if you do you will be logged out. However, you can delete any other created accounts by clicking **Delete** when editing the user. You are strongly advised to change the password on the default “**admin**” account when you receive your router, and any time you reset your configuration to Factory Defaults.

Configuration

User Management

Current Defined Users

Valid	User	Comment	Password	Confirm Password
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="button" value="Add"/> <input type="button" value="Edit / Delete"/>				
Edit	Valid	User	Comment	Delete
<input type="radio"/>	true	admin	Default admin user	

To create a new user account, first check the Valid box and then enter in the relevant details for User, Comment, Password and Confirm Password. Click the **Add** button to add the new user account.

Configuration

User Management

Current Defined Users

Valid	User	Comment	Password	Confirm Password
<input checked="" type="checkbox"/>	<input type="text" value="Test"/>	<input type="text" value="Test"/>	<input type="text" value="....."/>	<input type="text" value="....."/>
<input type="button" value="Add"/> <input type="button" value="Edit / Delete"/>				
Edit	Valid	User	Comment	Delete
<input type="radio"/>	true	admin	Default admin user	

Configuration

User Management

Current Defined Users

Valid	User	Comment	Password	Confirm Password
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="button" value="Add"/> <input type="button" value="Edit / Delete"/>				
Edit	Valid	User	Comment	Delete
<input type="radio"/>	true	admin	Default admin user	
<input type="radio"/>	true	Test	Test	<input type="radio"/>

To delete the user account, select the Delete option and then click the **Edit/Delete** button.

Configuration

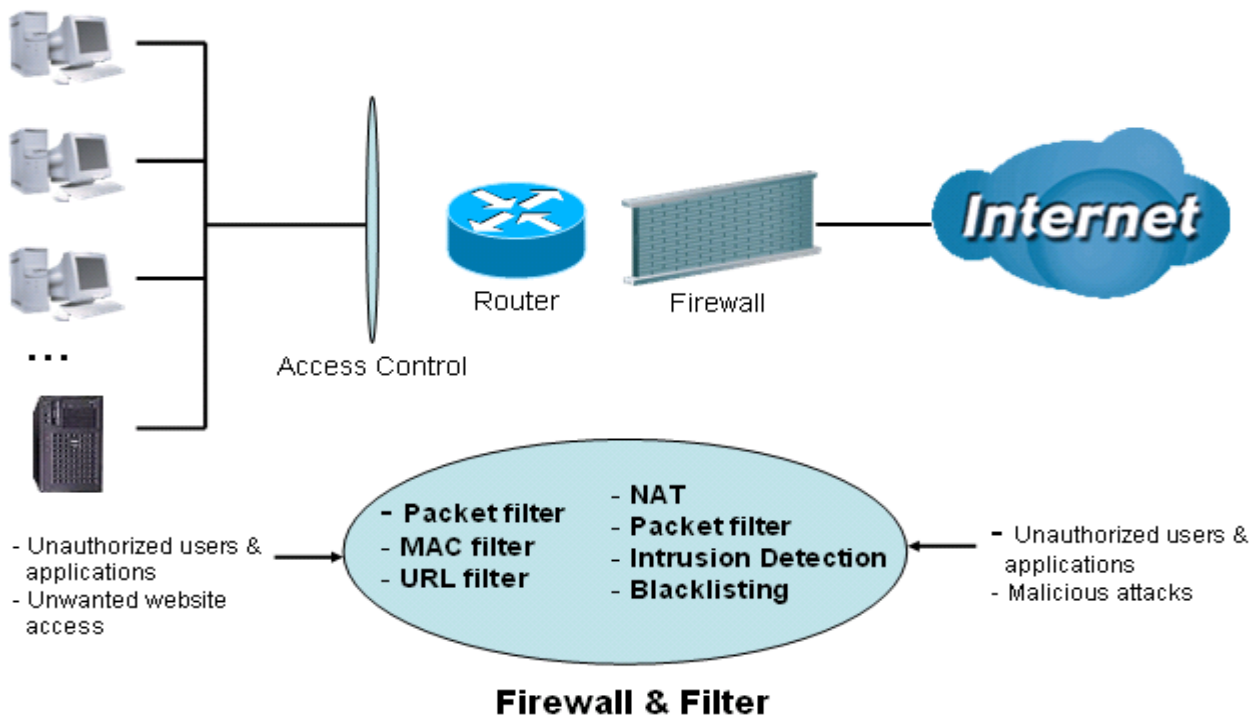
User Management

Current Defined Users

Valid	User	Comment	Password	Confirm Password
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="button" value="Add"/> <input type="button" value="Edit / Delete"/>				
Edit	Valid	User	Comment	Delete
<input type="radio"/>	true	admin	Default admin user	
<input type="radio"/>	true	Test	Test	<input checked="" type="radio"/>

Firewall and Access Control

Your router includes a full SPI (Stateful Packet Inspection) firewall for controlling Internet access from your LAN, as well as helping to prevent attacks from hackers. Besides, when using NAT, the router acts as a “natural” Internet firewall, as all PCs on your LAN will use private IP addresses that cannot be directly accessed from the Internet.



Firewall: Prevents access from outside your network. The router provides three levels of security support:

NAT natural firewall: This masks LAN users' IP addresses which is invisible to outside users on the Internet, making it much more difficult for a hacker to target a machine on your network. This natural firewall is on when NAT function is enabled.

NOTE:

When using Virtual Servers your PCs will be exposed to the degree specified in your Virtual Server settings provided the ports specified are opened in your firewall packet filter settings.

Firewall Security and Policy (General Settings): Inbound direction of Packet Filter rules to prevent unauthorized computers or applications accessing your local network from the Internet.

Intrusion Detection: Enable Intrusion Detection to detect, prevent and log malicious attacks.

Access Control: Prevents access from PCs on your local network:

Firewall Security and Policy (General Settings): Outbound direction of Packet Filter rules to prevent unauthorized computers or applications accessing the Internet.

URL Filter: To block PCs on your local network from unwanted websites.

Here are the items within the **Firewall** section: [General Settings](#), [Packet Filter](#), [Intrusion Detection](#), [URL Filter](#), [IM/P2P Blocking](#) and [Firewall Log](#).

General Settings

You can choose not to enable the Firewall and still have access to URL Filter and IM/P2P Blocking, or you can enable the Firewall using preset filter rules and modify the port filter rules as required. The Packet Filter is used to filter packets based-on Applications (Port) or IP addresses.


There are four options when you enable the Firewall, they are:

- ⊙ **All blocked/User-defined:** no pre-defined port or address filter rules by default, meaning that all inbound (Internet to LAN) and outbound (LAN to Internet) packets will be blocked. Users have to add their own filter rules for further access to the Internet.
- ⊙ **High/Medium/Low security level:** the predefined port filter rules for High, Medium and Low security are displayed in Port Filters of Packet Filter.

Select either **High, Medium** or **Low security level** to enable the Firewall. The only difference between these three security levels is the preset port filter rules in the Packet Filter. Firewall functionality is the same for all levels; it is only the list of preset port filters that changes between each setting. For more detailed on level of preset port filter information, refer to **Table 1: Predefined Port Filter**.

If you choose of the preset security levels and add custom filters, this level of filter rules will be saved even and do not need to re-configure the rules again if you disable or switch to other firewall level.

The “**Block WAN Request**” is a stand-alone function and not related to whether security is enabled or disabled. Mostly this is used to preventing a hacker on the WAN from using any scan tools.

Configuration


▶ General Settings

Firewall Security

Security	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Policy	<input type="radio"/> All blocked/User-defined <input type="radio"/> High security level <input checked="" type="radio"/> Medium security level <input type="radio"/> Low security level

(⚠ If some applications cannot work after enabling Firewall, please check the Packet Filter especially Port Filter rules. For example, adding (TCP:443,outbound allowed) will let HTTPS data go through Firewall.)

Block WAN Request	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
-------------------	---


(⚠ Enable for preventing any ping test from Internet, such as hacker attack.)

NOTE:


Attempting to perform this action remotely may result in blocking of all access to configuration and management of the device from the Internet. Use this with caution when connecting over the WAN

Packet Filter

This function is only available when the Firewall is enabled and one of these four security levels is chosen (All blocked, High, Medium and Low). The preset port filter rules in the Packet Filter must be modified according to the level of Firewall, which is selected. See **Table1: Predefined Port Filter** for more detailed information.

Configuration 

▼ Packet Filter

Parameters

Rule Name Helper << --Select-- ▼

Time Schedule Always On ▼

Source IP Address(es) Netmask

Destination IP Address(es) Netmask

Type TCP ▼ Protocol Number

Source Port -

Destination Port -

Inbound Allow ▼

Outbound Allow ▼

Edit	Rule Name	Time Schedule	Source IP / Netmask	Protocol	Source port(s)	Inbound		Delete
			Destination IP / Netmask		Destination port(s)	Block	Outbound	
<input type="radio"/>	mei_http	Always On	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	Block	Allow	<input type="radio"/>
			0.0.0.0 / 0.0.0.0		80 ~ 80	Allow		
<input type="radio"/>	mei_dns	Always On	0.0.0.0 / 0.0.0.0	UDP	0 ~ 65535	Block	Allow	<input type="radio"/>
			0.0.0.0 / 0.0.0.0		53 ~ 53	Allow		

Example: Predefined Port Filters Rules

The predefined port filter rules for High, Medium and Low security levels are listed. See Table 1.

Note: Firewall – For Blocked/User-defined, you must define and create the port filter rules yourself. No predefined rules are configured for these modes.

Table 1: Predefined Port Filter

Application	Protocol	Port Number		Firewall - Low		Firewall - Medium		Firewall – High	
		Start	End	Inbound	Outbound	Inbound	Outbound	Inbound	Outbound
HTTP(80)	TCP(6)	80	80	NO	YES	NO	YES	NO	YES
DNS (53)	UDP(17)	53	53	NO	YES	NO	YES	NO	YES
DNS (53)	TCP(6)	53	53	NO	YES	NO	YES	NO	YES
FTP(21)	TCP(6)	21	21	NO	YES	NO	YES	NO	NO
Telnet(23)	TCP(6)	23	23	NO	YES	NO	YES	NO	NO
SMTP(25)	TCP(6)	25	25	NO	YES	NO	YES	NO	YES
POP3(110)	TCP(6)	110	110	NO	YES	NO	YES	NO	YES
NEWS(NNTP) (Network News Transfer Protocol)	TCP(6)	119	119	NO	YES	NO	YES	NO	NO
RealAudio/ RealVideo (7070)	UDP(17)	7070	7070	YES	YES	YES	YES	NO	NO
PING	ICMP(1)	N/A	N/A	NO	YES	NO	YES	NO	YES
H.323(1720)	TCP(6)	1720	1720	YES	YES	NO	YES	NO	NO
T.120(1503)	TCP(6)	1503	1503	YES	YES	NO	YES	NO	NO
SSH(22)	TCP(6)	22	22	NO	YES	NO	YES	NO	NO
NTP /SNTP	UDP(17)	123	123	NO	YES	NO	YES	NO	YES
HTTP/HTTP Proxy (8080)	TCP(6)	8080	8080	NO	YES	NO	NO	NO	NO
HTTPS(443)	TCP(6)	443	443	NO	YES	NO	YES	N/A	N/A
ICQ (5190)	TCP(6)	5190	5190	YES	YES	N/A	N/A	N/A	N/A

Billion 400G Router

MSN (1863)	TCP(6)	1863	1863	YES	YES	N/A	N/A	N/A	N/A
MSN (7001)	UDP(17)	7001	7001	YES	YES	N/A	N/A	N/A	N/A
MSN VEDIO (9000)	TCP(6)	9000	9000	NO	YES	N/A	N/A	N/A	N/A

Inbound: Internet to LAN ; **Outbound:** LAN to Internet.
YES: Allowed ; **NO:** Blocked ; **N/A:** Not Applicable

Packet Filter – Add TCP/UDP Filter

Configuration

Packet Filter

Parameters

Rule Name Helper	<input type="text"/>	<<	--Select--	>>	
Time Schedule	Always On v				
Source IP Address(es)	<input type="text" value="0.0.0.0"/>	Netmask	<input type="text" value="0.0.0.0"/>		
Destination IP Address(es)	<input type="text" value="0.0.0.0"/>	Netmask	<input type="text" value="0.0.0.0"/>		
Type	TCP/UDP v		Protocol Number	<input type="text"/>	
Source Port	0 - 65535				
Destination Port	0 - 65535				
Inbound	Allow v				
Outbound	Allow v				

Rule Name: Users-define description to identify this entry or click **“Select” drop-down menu** to select existing predefined rules. The maximum name length is 32 characters.

Time Schedule: It is self-defined time period. You may specify a time schedule for your prioritization policy. For setup and detail, refer to **Time Schedule** section

Source IP Address(es) / Destination IP Address(es): This is the Address-Filter used to allow or block traffic to/from particular IP address(es). Selecting the **Subnet Mask** of the IP address range you wish to allow/block the traffic to or from; set IP address and Subnet Mask to **0.0.0.0** to inactive the Address-Filter rule.

Tip: To block access, to/from a single IP address, enter that IP address as the **Host IP Address** and use a **Host Subnet Mask** of “255.255.255.255”.

Source Port: This Port or Port Range defines the port allowed to be used by the Remote/WAN to connect to the application. Default is set from range **0 ~ 65535**. It is recommended that this option only be configured by advanced users.

Destination Port: This is the Port or Port Ranges that define the application.

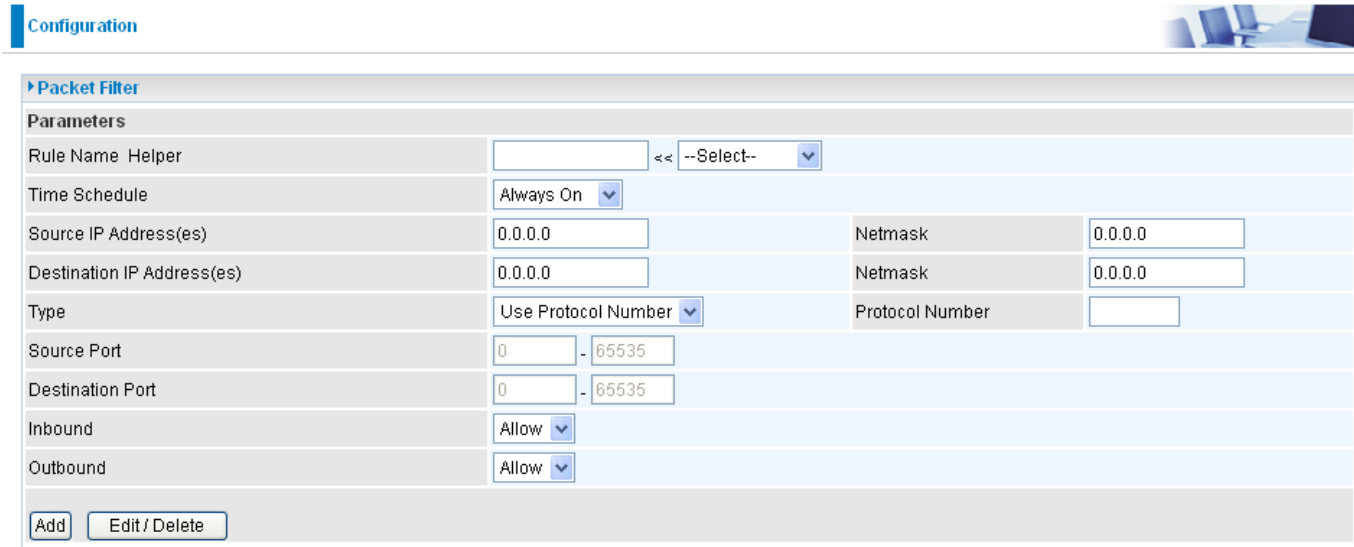
Type: It is the packet protocol type used by the application, select **TCP**, **UDP** or both **TCP/UDP**. **Protocol Number:** Insert the port number.

Inbound / Outbound: Select **Allow** or **Block** the access to the Internet (**“Outbound”**) or from the Internet (**“Inbound”**).

Click **Add** button to apply your changes.

Packet Filter – Add Raw IP Filter

Go to “Type” drop-down menu, select “Use Protocol Number”.



Configuration

Packet Filter

Parameters

Rule Name	Helper	<<	--Select--	▼
Time Schedule	Always On ▼			
Source IP Address(es)	0.0.0.0	Netmask	0.0.0.0	
Destination IP Address(es)	0.0.0.0	Netmask	0.0.0.0	
Type	Use Protocol Number ▼	Protocol Number		
Source Port	0	-	65535	
Destination Port	0	-	65535	
Inbound	Allow ▼			
Outbound	Allow ▼			

Rule Name Helper: Specifies a user-defined description identifying this entry or click the drop-down menu to select existing predefined rules.

Time Schedule: This is the user-defined time period applicable to the rule. You may specify a time schedule for your prioritization policy. For setup and detail, refer to **Time Schedule** section.

Protocol Number: Insert the port number, i.e. GRE 47.

Inbound / Outbound: Select **Allow** or **Block** the access to the Internet (“**Outbound**”) or from the Internet (“**Inbound**”).

Click **Add** button to apply your changes.

Example: Configuring your firewall to allow a publicly accessible web server on your LAN

The predefined port filter rule for HTTP (TCP port 80) is the same no matter whether the firewall is set to a high, medium or low security level. To setup a web server located on the local network when the firewall is enabled, you have to configure the Port Filters setting for HTTP.

As you can see from the diagram below, when the firewall is enabled with one of the three presets (Low/Medium/High), inbound HTTP access is not allowed which means remote access through HTTP to your router is not allowed.

Note: Inbound indicates accessing from Internet to LAN and Outbound is from LAN to the Internet.

Packet Filter

Parameters

Rule Name Helper << --Select--

Time Schedule Always On

Source IP Address(es) 0.0.0.0 Netmask 0.0.0.0

Destination IP Address(es) 0.0.0.0 Netmask 0.0.0.0

Type TCP Protocol Number

Source Port 0 - 65535

Destination Port 0 - 65535

Inbound Allow

Outbound Allow

Add Edit / Delete

Edit	Rule Name	Time Schedule	Source IP / Netmask	Protocol	Source port(s)	Inbound	
			Destination IP / Netmask		Destination port(s)	Outbound	
<input type="radio"/>	mei_http	Always On	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	Block	<input type="radio"/>
			0.0.0.0 / 0.0.0.0		80 ~ 80	Allow	<input type="radio"/>
<input type="radio"/>	mei_dns	Always On	0.0.0.0 / 0.0.0.0	UDP	0 ~ 65535	Block	<input type="radio"/>
			0.0.0.0 / 0.0.0.0		53 ~ 53	Allow	<input type="radio"/>
<input type="radio"/>	mei_tdns	Always On	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	Block	<input type="radio"/>
			0.0.0.0 / 0.0.0.0		53 ~ 53	Allow	<input type="radio"/>
<input type="radio"/>	mei_ftp	Always On	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	Block	<input type="radio"/>
			0.0.0.0 / 0.0.0.0		21 ~ 21	Allow	<input type="radio"/>

Configuring Packet Filter:

1. Click **Packet Filters**. You will then be presented with the predefined port filter rules screen (in this case for the low security level), shown below:

Note: You may click Edit the predefined rule instead of Delete it. This is an example to show to how you add a filter on your own.

Configuration

Packet Filter

Parameters

Rule Name Helper << --Select--

Time Schedule Always On

Source IP Address(es) Netmask

Destination IP Address(es) Netmask

Type

- TCP
- UDP
- TCP/UDP
- Use Protocol Number

Source Port

Destination Port

Inbound Allow

Outbound Allow

2. Choose the radio button for the existing HTTP rule that you wish to delete. Click **Edit/Delete** button to delete this existing HTTP rule.

Configuration

Packet Filter

Parameters

Rule Name Helper << --Select--

Time Schedule Always On

Source IP Address(es) Netmask

Destination IP Address(es) Netmask

Type TCP Protocol Number

Source Port -

Destination Port -

Inbound Block

Outbound Allow

Edit	Rule Name	Time Schedule	Source IP / Netmask Destination IP / Netmask	Protocol	Source port(s) Destination port(s)	Inbound Outbound	Delete
<input checked="" type="radio"/>	lei_http	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535 80 ~ 80	Block Allow	<input type="radio"/>
<input type="radio"/>	lei_dns	Always On	0.0.0.0 / 0.0.0.0 0.0.0.0 / 0.0.0.0	UDP	0 ~ 65535 53 ~ 53	Block Allow	<input type="radio"/>

3. Input the Rule Name, Time Schedule, Source/Destination IP, Type, Source/Destination Port, Inbound and Outbound.

Example:

Application: *Cindy_HTTP*
 Time Schedule: *Always On*
 Source / Destination IP Address(es): *0.0.0.0 (Allow all addresses)*
 Type: *TCP (Please refer to Table1: Predefined Port Filter)*
 Source Port: *0-65535 (I allow all ports to connect with the application)*
 Redirect Port: *80-80 (This is Port defined for HTTP)*
 Inbound / Outbound: *Allow*

The screenshot shows the 'Configuration' page of the router. Under the 'Packet Filter' section, a rule named 'Cindy_HTTP' is configured. The parameters are as follows:

Rule Name	Helper	Cindy_HTTP	<<	--Select--
Time Schedule		Always On		
Source IP Address(es)		0.0.0.0	Netmask	0.0.0.0
Destination IP Address(es)		0.0.0.0	Netmask	0.0.0.0
Type		TCP	Protocol Number	
Source Port		0 - 65535		
Destination Port		80 - 80		
Inbound		Allow		
Outbound		Allow		

Below the configuration form are buttons for 'Add' and 'Edit / Delete'. At the bottom, a table lists the configured rules:

Edit	Rule Name	Time Schedule	Source IP / Netmask	Destination IP / Netmask	Protocol	Source port(s)	Destination port(s)	Inbound	Outbound
	Cindy_HTTP	Always On	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	80 ~ 80	Allow	Allow

4. The new port filter rule for HTTP is shown below:

<input type="radio"/>	Cindy_HTTP	Always On	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	80 ~ 80	Allow	Allow	<input type="radio"/>
-----------------------	------------	-----------	-------------------	-------------------	-----	-----------	---------	-------	-------	-----------------------

5. Configure your Virtual Server (“port forwarding”) settings so that incoming HTTP requests on port 80 will be forwarded to the PC running your web server:

Note: For how to configure the HTTP in Virtual Server, go to Add Virtual Server in Virtual Server section for more details.



Configuration

Port Forwarding

Add Virtual Server in " IP interface

Virtual Server Entry

Application	Helper ▶	<input type="text"/>	<<	--Select--	▼
Protocol		tcp	▼	Time Schedule	Always On
External Port		from	<input type="text" value="0"/>	to	<input type="text" value="0"/>
Internal IP Address	Candidates ▶	<input type="text"/>			
Redirect Port		from	<input type="text" value="0"/>	to	<input type="text" value="0"/>

Apply Edit / Delete Return ▶

Edit	Application	Time Schedule	Protocol	External Port	Redirect Port	IP Address	Interface	Delete
<input type="radio"/>	HTTP_Server	Always On	tcp	80 - 80	80 - 80	192.168.1.101	ipwan	<input type="radio"/>

Intrusion Detection



Configuration

Intrusion Detection

Parameters

Intrusion Detection	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Victim Protection Block Duration	<input type="text" value="600"/> seconds
Scan Attack Block Duration	<input type="text" value="86400"/> seconds
DOS Attack Block Duration	<input type="text" value="1800"/> seconds
Maximum TCP Open Handshaking Count	<input type="text" value="100"/> per second
Maximum Ping Count	<input type="text" value="15"/> per second
Maximum ICMP Count	<input type="text" value="100"/> per second

Apply

Clear Blacklist

The router's *Intrusion Detection System* (IDS) is used to detect hacker attacks and intrusion attempts from the Internet. If the IDS function of the firewall is enabled, inbound packets are filtered and blocked depending on whether they are detected as possible hacker attacks, intrusion attempts or other connections that the router determines to be suspicious.

Blacklist: If the router detects a possible attack, the source IP or destination IP address will be added to the Blacklist. Any further attempts using this IP address will be blocked for the time period specified as the **Block Duration**. The default setting for this function is false (disabled). Some attack types are denied immediately without using the Blacklist function, such as *Land attack* and *Echo/CharGen scan*.

Intrusion Detection: If enabled, IDS will block Smurf attack attempts. Default is false.

Block Duration:

⊙ **Victim Protection Block Duration:** This is the duration for blocking *Smurf* attacks. Default value is 600 seconds.

⊙ **Scan Attack Block Duration:** This is the duration for blocking hosts that attempt a possible Scan attack. Scan attack types include *X'mas scan*, *IMAP SYN/FIN scan* and similar attempts. Default value is 86400 seconds.

⊙ **DoS Attack Block Duration:** This is the duration for blocking hosts that attempt a possible Denial of Service (DoS) attack. Possible DoS attacks this attempts to block include *Ascend Kill* and *WinNuke*. Default value is 1800 seconds.

Billion 400G Router

Max TCP Open Handshaking Count: This is a threshold value to decide whether a *SYN Flood* attempt is occurring or not. Default value is 100 TCP SYN per seconds.

Max PING Count: This is a threshold value to decide whether an *ICMP Echo Storm* is occurring or not. Default value is 15 ICMP Echo Requests (PING) per second.

Max ICMP Count: This is a threshold to decide whether an *ICMP flood* is occurring or not. Default value is 100 ICMP packets per seconds except ICMP Echo Requests (PING).

For *SYN Flood*, *ICMP Echo Storm* and *ICMP flood*, IDS will just warn the user in the Event Log. It cannot protect against such attacks.

Table 2: Hacker attack types recognized by the IDS

Intrusion Name	Detect Parameter	Blacklist	Type of Block Duration	Drop Packet	Show Log
Ascend Kill	Ascend Kill data	Src IP	DoS	Yes	Yes
WinNuke	TCP Port 135, 137~139, Flag: URG	Src IP	DoS	Yes	Yes
Smurf	ICMP type 8 Des IP is broadcast	Dst IP	Victim Protection	Yes	Yes
Land attack	SrcIP = DstIP			Yes	Yes
Echo/CharGen Scan	UDP Echo Port and CharGen Port			Yes	Yes
Echo Scan	UDP Dst Port = Echo(7)	Src IP	Scan	Yes	Yes
CharGen Scan	UDP Dst Port = CharGen(19)	Src IP	Scan	Yes	Yes
X'mas Tree Scan	TCP Flag: X'mas	Src IP	Scan	Yes	Yes
IMAP SYN/FIN Scan	TCP Flag: SYN/FIN DstPort: IMAP(143) SrcPort: 0 or 65535	Src IP	Scan	Yes	Yes
SYN/FIN/RST/ACK Scan	TCP, No Existing session And Scan Hosts more than five.	Src IP	Scan	Yes	Yes
Net Bus Scan	TCP No Existing session DstPort = Net Bus 12345,12346, 3456	SrcIP	Scan	Yes	Yes
Back Orifice Scan	UDP, DstPort = Orifice Port (31337)	SrcIP	Scan	Yes	Yes
SYN Flood	Max TCP Open Handshaking Count (Default 100 c/sec)				Yes
ICMP Flood	Max ICMP Count (Default 100 c/sec)				Yes
ICMP Echo	Max PING Count (Default 15 c/sec)				Yes

Src IP: Source IP**Src Port:** Source Port**Dst Port:** Destination Port**Dst IP:** Destination IP

URL Filter

URL (Uniform Resource Locator – e.g. an address in the form of <http://www.abcde.com> or <http://www.example.com>) filter rules allow you to prevent users on your network from accessing particular websites by their URL. There are no pre-defined URL filter rules; you can add filter rules to meet your requirements.



Configuration

URL Filter	
Configuration	
URL Filtering	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Block Mode	Always On ▾
Keywords Filtering	<input type="checkbox"/> Enable Details ▸
Domains Filtering	<input type="checkbox"/> Enable Details ▸ <input type="checkbox"/> Disable all WEB traffic except for Trusted Domains
Restrict URL Features	<input type="checkbox"/> Block Java Applet <input type="checkbox"/> Block surfing by IP address
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> Exception List	

Enable/Disable: To enable or disable URL Filter feature.

Block Mode: A list of the modes that you can choose to check the URL filter rules. The default is set to **Always On**.

- Ⓒ **Disabled:** No action will be performed by the Block Mode.
- Ⓒ **Always On:** Action is enabled. URL filter rules will be monitoring and checking at all hours of the day.
- Ⓒ **TimeSlot1 ~ TimeSlot16:** These are user-defined time periods. You may specify the time period during which the URL filter rules apply, i.e. during working hours. For setup and details, refer to **Time Schedule** section.

Keywords Filtering: Allows blocking by specific keywords within a particular URL rather than having to specify a complete URL (e.g. to block any image called “advertisement.gif”). When enabled, your specified keywords list will be checked to see if any keywords are present in URLs accessed to determine if the connection attempt should be blocked. Please note that the URL filter blocks web browser (HTTP) connection attempts using port 80 only.

For example, if the URL is <http://www.abc.com/abcde.html>, it will be dropped as the keyword “abcde” occurs in the URL.



Configuration

Keywords Filtering	
Create	
Keyword	<input type="text"/>
<input type="button" value="Apply"/>	
Block WEB URLs which contain these keywords	
Name	Keyword
Return ▸	

Domains Filtering: This function checks the whole URL not the IP address, in URLs accessed against your list of domains to block or allow. If it is matched, the URL request will be sent (Trusted) or dropped (Forbidden). For this function to be activated, both check-boxes must be checked. Here is the checking procedure:

1. The router checks the domain in the URL to determine if it is in the trusted list. If it is, then the connection attempt is sent to correct the remote web server.

Billion 400G Router

2. If not, the router checks if the domain is listed in the forbidden list. If it is, then the connection attempt will be dropped.
3. If the packet does not match either of the above two items, it is sent to the remote web server.
4. Please be note that the completed URL, “www” + domain name shall be specified. For example to block traffic to www.google.com.au, enter “www.google” or “www.google.com”

In the example below, the URL request for www.abc.com will be sent to the remote web server because it is listed in the trusted list, whilst the URL request for www.google or www.google.com will be dropped, because www.google is in the forbidden list.

Configuration

Domains Filtering

Domain Name

Domain Name

Type

Trusted Domain

Name	Domain	
item0	www.abc	Delete ▶

Forbidden Domain

Name	Domain	
item1	www.google	Delete ▶

[Return ▶](#)

Example: Andy wishes to disable all WEB traffic except for ones listed in the trusted domain, which would prevent Bobby from accessing other web sites. Andy selects both check boxes in **Domain Filtering** and thinks that this will stop Bobby. But Bobby knows this function, **Domain Filtering**, ONLY disables all WEB traffic except for **Trusted Domain**, BUT not connections using **IP addresses**. In this situation, the **Block surfing by IP address** function can be handy and helpful to Andy. Now, Andy can prevent Bobby from accessing sites, both by IP and by domain name.

Restrict URL Features: This function enhances the restriction to your URL rules.

- ⊙ **Block Java Applet:** This function can block Web content that includes a Java Applet. This is to prevent someone who wants to damage your system via standard HTTP protocol.
- ⊙ **Block surfing by IP address:** This prevents someone who uses the IP address as URL from skipping the Domains Filtering function. This is only Activate if Domain Filtering is enabled.

IM / P2P Blocking

IM, short for Instant Messaging, is required to use client program software that allows users to communicate, exchanging text message, with other IM users, in real time, over the Internet. A P2P application, known as Peer-to-Peer, is a group of computer users who share files to specific groups of people across the Internet. Both Instant Messaging and Peer-to-Peer applications make communication faster and easier, but your network can become increasingly insecure at the same time. This router's IM and P2P blocking system helps users to restrict LAN computers from access to the commonly used IM, Yahoo and MSN, and P2P, BitTorrent and eDonkey, applications over the Internet.

The screenshot shows the 'IM/P2P Blocking' configuration page. It has a 'Configuration' section with the following settings:

Setting	Value
Instant Message Blocking	Disabled
Yahoo Messenger	<input type="checkbox"/> Block
MSN Messenger	<input type="checkbox"/> Block
Peer to Peer Blocking	Disabled
BitTorrent (BitTorrent, BitComet)	<input type="checkbox"/> Block
eDonkey (eDonkey, eMule)	<input type="checkbox"/> Block

Buttons: Apply, Cancel

Instant Message Blocking: The default is set to **Disabled**.

- ⊙ **Disabled:** The Instant Messaging blocking function is not activated. No blocking will be performed.
- ⊙ **Always On:** The Instant Messaging blocking function is activated. Blocking is enabled.
- ⊙ **TimeSlot1 ~ TimeSlot16:** These are user-defined time periods. You may specify the time period during which the URL filter rules apply, i.e. during working hours. For setup and details, refer to **Time Schedule** section.

Yahoo/MSN Messenger: Select this box to block either Yahoo and/or MSN Messenger. Be sure that you have enabled the *Instant Message Blocking* first.

Peer to Peer Blocking: The default is set to **Disabled**.

- ⊙ **Disabled:** The Instant Messaging blocking function is not active. No connections will be blocked
- ⊙ **Always On:** The Instant Messaging blocking function is activated. Blocking is enabled.
- ⊙ **TimeSlot1 ~ TimeSlot16:** These are user-defined time periods. You may specify the time period during which the URL filter rules apply, i.e. during working hours. For setup and details, refer to **Time Schedule** section.

BitTorrent / eDonkey: Select this box to block either Bit Torrent and/or eDonkey. To be sure you have first enabled the *Peer to Peer Blocking* function.

Firewall Log

Configuration

Firewall Log

Event will be shown in the Status - Event Log

Filtering Log	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Intrusion Log	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
URL Blocking Log	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Apply

Firewall Log display log information of any unexpected action with your firewall settings.

Check the **Enable** box to activate the logs.

Log information can be seen in the **Status – Event Log** after enabling.

QoS - Quality of Service

The QoS function helps you to control your network traffic for each LAN (Ethernet and/or Wireless) application that accesses the WAN (Internet). It allows you to control the quality and speed of throughput for each application, when the system is running with a fully loaded upstream channel.

Here are the items within the **QoS** section: **Prioritization** and **Outbound / Inbound IP Throttling** (bandwidth management).

Prioritization

There are three priority settings to be provided in the Router:

- High**
- Normal** (The default is normal priority for all of traffic without setting)
- Low**

And the balances of utilization for each priority are High (60%), Normal (30%) and Low (10%).

To delete the application, you can choose the Delete option and then click Edit/Delete.

Configuration

Prioritization

Configuration (from LAN to WAN packet)

Name	<input type="text"/>	Time Schedule	Always On <input type="button" value="v"/>
Priority	High <input type="button" value="v"/>	Protocol	any <input type="button" value="v"/>
Source IP Address Range	<input type="text"/> ~ <input type="text"/>	Source Port	<input type="text"/> ~ <input type="text"/>
Destination IP Address Range	<input type="text"/> ~ <input type="text"/>	Destination Port	<input type="text"/> ~ <input type="text"/>
DSCP Marking	Disabled <input type="button" value="v"/>		

Add

Edit	Name	Time Schedule	Protocol	Priority	DSCP Marking	Delete
------	------	---------------	----------	----------	--------------	--------

Name: A user-defined description identifying this new policy/application.

Time Schedule: The details of when this rule of your prioritization policy is active.

Priority: The priority given to each policy/application. The default setting is High; you may adjust this setting to fit your requirements.

Protocol: The name of supported protocol.

Source IP Address Range: The source IP address or range of packets to be monitored.

Source Port: The source port of packets to be monitored.

Destination IP address Range: The destination IP address or range of packets to be monitored.

Destination Port: The destination port of packets to be monitored.

DSCP Marking: Differentiated Services Code Point (DSCP), it is the first 6 bits in the ToS byte. DSCP Marking allows users to assign specific application traffic to be executed in priority by the backbone routers, based on the DSCP value. See Table 4. The DSCP Mapping Table:

Note: To be sure all the routers on the backbones network have the capability of executing and checking DSCP so as to provide a QoS network.

Table 4: DSCP Mapping Table

DSCP Mapping Table	
(Wireless) ADSL Router	Standard DSCP
Disabled	None
Best Effort	Best Effort (000000)
Premium	Express Forwarding (101110)
Gold service (L)	Class 1, Gold (001010)
Gold service (M)	Class 1, Silver (001100)
Gold service (H)	Class 1, Bronze (001110)
Silver service (L)	Class 2, Gold (010010)
Silver service (M)	Class 2, Silver (010100)
Silver service (H)	Class 2, Bronze (010110)
Bronze service (L)	Class 3, Gold (011010)
Bronze service (M)	Class 3, Silver (011100)
Bronze service (H)	Class 3, Bronze (011110)

Outbound IP Throttling (LAN to WAN)

IP Throttling allows you to limit the speed of IP traffic. The value entered will limit the speed of the specified application to the specified value (Set in multiples of 32kbps.)

Configuration

Outbound IP Throttling

Configuration (from LAN to WAN packet)

Name	<input type="text"/>	Time Schedule	Always On <input type="button" value="v"/>
Protocol	any <input type="button" value="v"/>	Rate Limit	1 <input type="text"/> *32 (kbps)
Source IP Address Range	0.0.0.0 <input type="text"/> ~ 0.0.0.0 <input type="text"/>	Source port(s)	0 <input type="text"/> ~ 0 <input type="text"/>
Destination IP Address Range	0.0.0.0 <input type="text"/> ~ 0.0.0.0 <input type="text"/>	Destination port(s)	0 <input type="text"/> ~ 0 <input type="text"/>

Edit	Application	Time Schedule	Protocol	Rate Limit	Delete
------	-------------	---------------	----------	------------	--------

Name: A user-define description to identify this new policy/name.

Time Schedule: The details of when this rule of your prioritization policy is active. Refer to **Time Schedule** for more information.

Protocol: The name of supported protocol.

Rate Limit: Used to limit the speed of outbound traffic (Set in multiples of 32kbps.)

Source IP Address Range: The source IP address or range of packets to be monitored.

Source Port(s): The source port of packets to be monitored.

Destination IP Address Range: The destination IP address or range of packets to be monitored.

Destination Port(s): The destination port of packets to be monitored.

Inbound IP Throttling (WAN to LAN)

IP Throttling allows you to limit the speed of IP traffic. The value entered will limit the speed of the specified application to the specified value (Set in multiples of 32kbps.)

Configuration

Inbound IP Throttling

Configuration (from WAN to LAN packet)

Name	<input type="text"/>	Time Schedule	Always On ▼
Protocol	any ▼	Rate Limit	1 *32 (kbps)
Source IP Address Range	0.0.0.0 ~ 0.0.0.0	Source port(s)	0 ~ 0
Destination IP Address Range	0.0.0.0 ~ 0.0.0.0	Destination port(s)	0 ~ 0

Apply
Edit / Delete

Edit	Application	Time Schedule	Protocol	Rate Limit	Delete
✖					✖

Name: a user-define description to identify this new policy/application.

Time Schedule: The details of when this rule of your prioritization policy is active. Refer to **Time Schedule** for more information.

Protocol: The name of supported protocol.

Rate Limit: Used to limit the speed of inbound traffic (Set in multiples of 32kbps.)

Source IP Address Range: The source IP address or range of packets to be monitored.

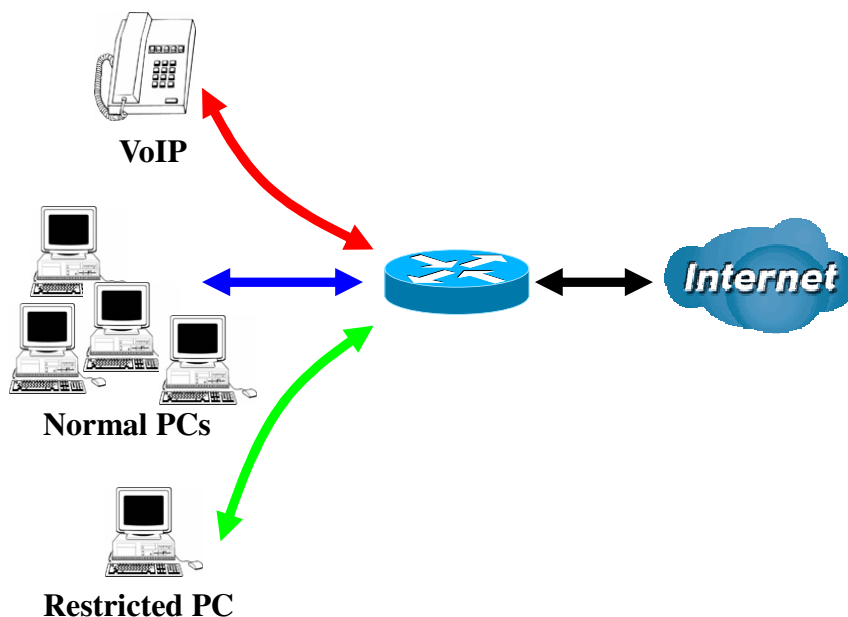
Source Port(s): The source port of packets to be monitored.

Destination IP Address Range: The destination IP address or range of packets to be monitored.

Destination Port(s): The destination port of packets to be monitored.

Example: QoS for your Network

Connection Diagram



Information and Settings

Upstream: 928 kbps
Downstream: 8 Mbps

VoIP User : 10.0.0.1
Normal Users : 10.0.0.10~10.0.0.13
Restricted User : 10.0.0.100

Configuration

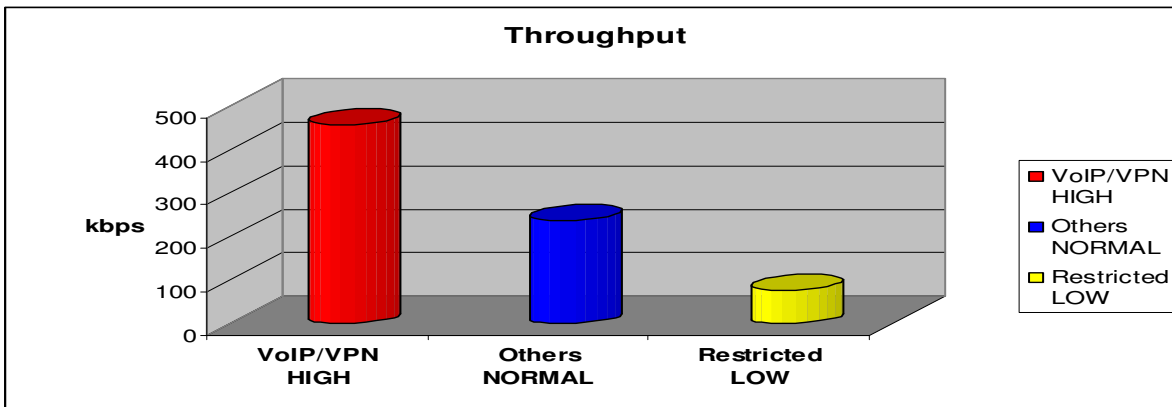
▼ Prioritization

Configuration (from LAN to WAN packet)

Name	<input type="text"/>	Time Schedule	Always On <input type="button" value="v"/>
Priority	High <input type="button" value="v"/>	Protocol	any <input type="button" value="v"/>
Source IP Address Range	0.0.0.0 ~ 0.0.0.0	Source Port	0 ~ 0
Destination IP Address Range	0.0.0.0 ~ 0.0.0.0	Destination Port	0 ~ 0
DSCP Marking	Disabled <input type="button" value="v"/>		

Edit	Name	Time Schedule	Protocol	Priority	DSCP Marking	Delete
<input type="radio"/>	PPTP	Always On	GRE	High	Gold service (L)	<input type="radio"/>
<input type="radio"/>	VoIP	Always On	Any	High	Gold service (L)	<input type="radio"/>
<input type="radio"/>	Restricted	TimeSlot1	Any	High	Gold service (L)	<input type="radio"/>

Billion 400G Router



Mission-critical application

Often, a VPN connection is a mission-critical application for exchanging data between Head and Branch offices.

Configuration

▼ Prioritization

Configuration (from LAN to WAN packet)

Name	PPTP	Time Schedule	Always On
Priority	High	Protocol	gre
Source IP Address Range	0.0.0.0 ~ 0.0.0.0	Source Port	0 ~ 0
Destination IP Address Range	0.0.0.0 ~ 0.0.0.0	Destination Port	0 ~ 0
DSCP Marking	Gold service (L)		

Edit	Name	Time Schedule	Protocol	Priority	DSCP Marking	Delete
<input checked="" type="radio"/>	PPTP	Always On	GRE	High	Gold service (L)	<input type="radio"/>

This mission-critical application must be connected smoothly, without any dropping. To ensure this, you should set the priority to the high level to preventing any other applications from saturating the bandwidth.

Voice application

Voice applications are latency-sensitive. Most VoIP devices use the SIP protocol, which automatically assigns a port number. This means that it is better to use a fixed IP address to catch VoIP packets and route them as high priority traffic.

Configuration

▼ Prioritization

Configuration (from LAN to WAN packet)

Name	VoIP	Time Schedule	Always On
Priority	High	Protocol	any
Source IP Address Range	10.0.0.123 ~ 10.0.0.123	Source Port	0 ~ 0
Destination IP Address Range	0.0.0.0 ~ 0.0.0.0	Destination Port	0 ~ 0
DSCP Marking	Gold service (L)		

Edit	Name	Time Schedule	Protocol	Priority	DSCP Marking	Delete
<input type="radio"/>	PPTP	Always On	GRE	High	Gold service (L)	<input type="radio"/>
<input checked="" type="radio"/>	VoIP	Always On	Any	High	Gold service (L)	<input type="radio"/>

The settings shown above will help to improve the quality of your VoIP service when the link is fully loaded.

Restricted Application

Some users will setup a FTP server for downloading of their files by means of FTP.

Configuration

▼ Prioritization

Configuration (from LAN to WAN packet)

Name	Restricted	Time Schedule	TimeSlot1
Priority	High	Protocol	any
Source IP Address Range	10.0.0.111 ~ 10.0.0.111	Source Port	0 ~ 0
Destination IP Address Range	0.0.0.0 ~ 0.0.0.0	Destination Port	0 ~ 0
DSCP Marking	Gold service (L)		

Edit	Name	Time Schedule	Protocol	Priority	DSCP Marking	Delete
<input type="radio"/>	PPTP	Always On	GRE	High	Gold service (L)	<input type="radio"/>
<input type="radio"/>	VoIP	Always On	Any	High	Gold service (L)	<input type="radio"/>
<input checked="" type="radio"/>	Restricted	TimeSlot5	Any	High	Gold service (L)	<input type="radio"/>

The above settings will help to limit utilization of upstream bandwidth by the FTP connections. A time schedule can be implemented to limit file downloads to non-busy times.

Advanced setting by using IP throttling

With IP throttling you can specify more detail for allocating bandwidth; even the applications are located in the same level.

- Upstream: 928kbps (29*32kbps)
- Mission-critical Application: 192kbps (6*32kbps)
- Voice Application: 128kbps (4*32kbps)
- Restricted Application: 160kbps (5*32kbps)
- Other Applications: 448kbps (14*32kbps)

$6+4+14+5=29, 29*32\text{kbps}=928\text{kbps}$

Configuration

▼ Outbound IP Throttling

Configuration (from LAN to WAN packet)

Name		Time Schedule	Always On
Protocol	any	Rate Limit	1 *32 (kbps)
Source IP Address Range	0.0.0.0 ~ 0.0.0.0	Source port(s)	0 ~ 0
Destination IP Address Range	0.0.0.0 ~ 0.0.0.0	Destination port(s)	0 ~ 0

Edit	Name	Time Schedule	Protocol	Rate Limit	Delete
<input type="radio"/>	PPTP	Always On	GRE	6	<input type="radio"/>
<input type="radio"/>	VoIP	Always On	Any	4	<input type="radio"/>
<input type="radio"/>	Restricted	TimeSlot1	Any	5	<input type="radio"/>
<input type="radio"/>	Others	TimeSlot1	Any	14	<input type="radio"/>

Billion 400G Router

Sometime your customers or friends may upload their files to your FTP server and that will saturate your downstream bandwidth. The settings below will help you to limit bandwidth for such an application that needs restriction.

Configuration

Outbound IP Throttling

Configuration (from LAN to WAN packet)

Name	<input type="text" value="Restricted"/>	Time Schedule	<input type="text" value="TimeSlot1"/>
Protocol	<input type="text" value="any"/>	Rate Limit	<input type="text" value="64"/> *32 (kbps)
Source IP Address Range	<input type="text" value="0.0.0.0"/> ~ <input type="text" value="0.0.0.0"/>	Source port(s)	<input type="text" value="0"/> ~ <input type="text" value="0"/>
Destination IP Address Range	<input type="text" value="10.0.0.111"/> ~ <input type="text" value="10.0.0.111"/>	Destination port(s)	<input type="text" value="0"/> ~ <input type="text" value="0"/>

Edit	Name	Time Schedule	Protocol	Rate Limit	Delete
<input type="button" value="⊕"/>	Restricted	TimeSlot1	Any	64	<input type="button" value="⊖"/>

Virtual Server (known as Port Forwarding)

In TCP/IP and UDP networks, a port is a 16-bit number used to identify which application program incoming connections should be delivered to. Some ports have numbers that are pre-assigned to them by the IANA (the Internet Assigned Numbers Authority), and these are referred to as “well-known ports”. Servers follow the well-known port assignments so clients can locate them.

If you wish to run a server, or any application (e.g. Peer-to-peer/P2P software such as instant messaging applications and P2P file-sharing applications) on your network that can be accessed from the WAN (i.e. from machines on the Internet that are outside your local network, and you are using NAT (Network Address Translation), then you will need to configure your router to forward these incoming connection attempts using specific ports to the computer on your network that is running the application/server. You will also need to use port forwarding if you want to host an online game server.

The reason for this is that when using NAT, your publicly accessible IP address will be used by and point to your router, which then needs to deliver all traffic to the private IP addresses used by your PCs. Please see the **WAN** configuration section of this manual for more information on NAT.

The device can be configured as a virtual server so that remote users accessing services such as Web or FTP services on the routers public (WAN) IP address can be automatically redirected to local servers on the LAN network. Depending on the requested service (TCP/UDP port number), the router redirects the external service request to the appropriate server within the LAN network

Configuration

Port Forwarding

Add Virtual Server in 'ipwan' IP interface

Virtual Server Entry


Application	<input type="text" value=""/>	<<	<input type="text" value="--Select--"/>	>>	
Protocol	<input type="text" value="tcp"/>		Time Schedule	<input type="text" value="Always On"/>	
External Port	from <input type="text" value="0"/> to <input type="text" value="0"/>		Redirect Port	from <input type="text" value="0"/> to <input type="text" value="0"/>	
Internal IP Address	<input type="text" value=""/>	<<	<input type="text" value="--Select--"/>	>>	

Edit	Application	Time Schedule	Protocol	External Port	Redirect Port	IP Address	Interface	Delete

Add Virtual Server

Because NAT can act as a “natural” Internet firewall, your router protects your network from being accessed by outside users when NAT is enabled – all incoming connection attempts will point to your router unless you specifically created Virtual Server entries to forward those ports to a computer on your network.

When your router needs to allow outside users to access internal servers, e.g. a web server, FTP server, Email server or game server, the router can act as a “virtual server”. You can set up a local server with a specific port number for the service to use e.g. web/HTTP (port 80), FTP (port 21), Telnet (port 23), SMTP (port 25), or POP3 (port 110). When an incoming access request for a specified port is received by the router, it will be forwarded to the corresponding internal server.

Configuration 

▼ Port Forwarding

Add Virtual Server in 'ipwan' IP interface

Virtual Server Entry

Application	<input type="text"/>	<< --Select--	▼
Protocol	tcp	▼	Time Schedule
External Port	from <input type="text" value="0"/> to <input type="text" value="0"/>	Redirect Port	from <input type="text" value="0"/> to <input type="text" value="0"/>
Internal IP Address	<input type="text"/>	<< --Select--	▼

Add Edit / Delete

Edit	Application	Time Schedule	Protocol	External Port	Redirect Port	IP Address	Interface	Delete
------	-------------	---------------	----------	---------------	---------------	------------	-----------	--------

Application: A user-defined description used to identify this entry. You can click drop-down menu to select existing predefined rules.

: 20 predefined rules are available. Application, Protocol and External/Redirect Ports will be filled after the selection has been made.

Protocol: This is the protocol supported by the virtual server. In addition to specifying the port number to be used, you will also need to specify the protocol used. The protocol used is determined by the particular application. Most applications will use TCP or UDP.

Time Schedule: The user-defined time period to enable your virtual server. You may specify a time schedule or Always on for the use of this Virtual Server Entry. For setup and detail, refer to the **Time Schedule** section.

External Port: The Port number on the Remote/WAN side used when accessing the virtual server.

Redirect Port: The Port number used by the Local server in the LAN network.

Internal IP Address: The private IP in the LAN network, which will be providing the virtual server application.

List all existing computers currently connected to the network. You may assign a computer with an IP address or a MAC address from this list.

Example:

If you would like to remotely access your routers' Web/HTTP interface all the time, you would need to enable port number 80 (Web/HTTP) and map it to the Router's LAN IP Address. All incoming HTTP requests on the WAN network will then be forwarded to the router's IP address of 10.0.0.2. Since port number 80 is already a predefined rule, click **Helper** in the **Application** section. A predefined rules window will pop and you can select **HTTP_Server**.

Application: *HTTP_Server*
 Time Schedule: *Always On*
 Protocol: *tcp*
 External Port: *80-80*
 Redirect Port: *80-80*
 IP Address: *10.0.0.2*

Configuration

▼ **Port Forwarding**

Add Virtual Server in 'ipwan' IP interface

Virtual Server Entry

Application: HTTP_Server << --Select-- ▼

Protocol: tcp ▼ Time Schedule: Always On ▼

External Port: from 80 to 80 Redirect Port: from 80 to 80

Internal IP Address: 10.0.0.100 << --Select-- ▼

Edit	Application	Time Schedule	Protocol	External Port	Redirect Port	IP Address	Interface	Delete
	HTTP_Server	Always On	tcp	80 - 80	80 - 80	10.0.0.100	ipwan	

Add: Click it to apply your settings.

Edit/Delete: Click it to edit or delete this virtual server application.



Using port forwarding has security implications, since outside users will be able to connect to Computers on your network. For this reason you are advised to add specific Virtual Server entries only for the ports that your application actually requires, instead of using the DMZ function. Using the DMZ function will result in all connection attempts from the WAN network having access to the public IP specified in the DMZ config section.



Attention

If you have disabled the NAT option in the WAN-ISP section, the Virtual Server function will not work.

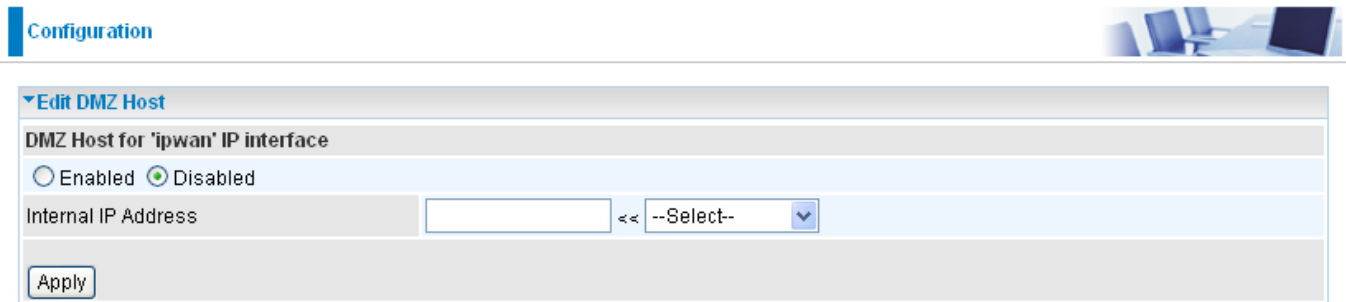
If the DHCP server option is enabled, you have to be very careful when assigning the IP addresses of virtual servers so that you avoid conflicting IP addresses. The easiest method of configuring Virtual Servers is to manually assign static IP address to each virtual server Computer, with an address that does not fall into the range of IP addresses that are to be issued by the DHCP server. These manually configured IP addresses **MUST** still be in the same subnet as the router.

Edit DMZ Host

A DMZ Host is a computer on the LAN that is completely exposed to the Internet. When you have configured a particular internal IP address as the DMZ Host, all incoming packets will be checked by the routers firewall and NAT algorithms, and if the packet does not use a port number that has been assigned by any Virtual Server entry, it will be passed to the DMZ host.

Caution: This local computer, which is exposed to the Internet, may face a variety of security risks. You should make quite sure that it is adequately protected.

Go to **Configuration** → **Virtual Server** → **Edit DMZ Host**



Enabled: This option disables the DMZ function.

Disabled: This option enables the DMZ function and is the default setting.

Internal IP Address: When the DMZ function is enabled, supply the static IP address of the DMZ Host. Be aware that this IP will be exposed to the WAN/Internet.

List all Computers currently connected to the network. You may assign a Computer using its IP address and/or its MAC address from this list. Select the **Apply** button to apply your changes.

Edit One-to-One NAT (Network Address Translation)

One-to-One NAT maps a specific private/local (LAN) IP address to a particular global/public (WAN) IP address. If you have multiple public/WAN IP addresses provided by your ISP, you will be able to use the One-to-One NAT function to utilize these IP addresses.

Go to **Configuration**→**Virtual Server**→**Edit One-to-one NAT**

NAT Type: Select the desired NAT type. By default, the One-to-One NAT function is disabled.

Global IP Address:

- Subnet:** The subnet of the public/WAN IP addresses given by your ISP. If your ISP has provided this information, you may insert it here. Otherwise, use the IP Range method to define your addresses.
- IP Range:** The IP address range of your public/WAN IP addresses. For example, IP: 10.0.0.5, end IP: 10.0.0.14

Select the **Apply** button to apply your changes.

Check **One-to-one NAT Table** to create a new One-to-One NAT rule:

Application: Users-defined description to identify this entry or click drop-down menu to select existing predefined rules.

: 20 predefined rules are available. Application, Protocol and External/Redirect Ports will be filled after the selection.

Protocol: This is the protocol to be supported by the virtual server. In addition to specifying the port number to be used, you will also need to specify the protocol used. The protocol used is determined by the particular application. Most applications will use TCP or UDP.

Time Schedule: The user-defined time period during which your virtual server is enabled. You may specify a time schedule or you can select **Always on** for this Virtual Server Entry. For setup and details, refer to the **Time Schedule** section.

Global IP: Define a public/ WAN IP address for this Application to use.

Billion 400G Router

External Port: The Port number on the Remote/WAN side that is used when accessing the virtual server.

Redirect Port: The Port number that the Local server on the LAN network will be listening on.

Internal IP Address: The private IP, on the LAN network, of the virtual server application.

Lists all the existing computer connections on the network. You may assign a Computer by IP address or MAC address from this list.

Select the **Add** button to apply your changes.

Example: List of some well-known and registered port numbers.

The Internet Assigned Numbers Authority (IANA) is the central coordinator for the assignment of unique parameter values for Internet protocols. Port numbers range from 0 to 65535, but only ports numbers 0 to 1023 are reserved for privileged services and are designated as “well-known ports” (Please refer to Table 5). Registered ports are numbered from 1024 through 49151. The remaining ports, referred to as dynamic or private ports, are numbered from 49152 through 65535.

For further information, please see IANA’s website at: <http://www.iana.org/assignments/port-numbers>

Table 5: Well-known and registered Ports

Port Number	Protocol	Description
20	TCP	FTP Data
21	TCP	FTP Control
22	TCP & UDP	SSH Remote Login Protocol
23	TCP	Telnet
25	TCP	SMTP (Simple Mail Transfer Protocol)
53	TCP & UDP	DNS (Domain Name Server)
69	UDP	TFTP (Trivial File Transfer Protocol)
80	TCP	World Wide Web HTTP
110	TCP	POP3 (Post Office Protocol Version 3)
119	TCP	NEWS (Network News Transfer Protocol)
123	UDP	NTP (Network Time Protocol) / SNTP (Simple Network Time Protocol)
161	TCP	SNMP
443	TCP & UDP	HTTPS
1503	TCP	T.120
1720	TCP	H.323
4000	TCP	ICQ
7070	UDP	RealAudio

Time Schedule

The Time Schedule function supports up to 16 time slots, helping you to manage your Internet connection. In each time profile, you may schedule specific day(s) i.e. Monday through Sunday to restrict or allowing the usage of the Internet by users or applications.

This Time Schedule correlates closely to real time. Since router does not have a real time clock on board; it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server from the Internet. Refer to **Time Zone** for details. Your router time should correspond with your local time. If the time settings on you router are not set correctly, the Time Schedule will not function properly.

Configuration

Time Schedule

Name:

Day: Sun. Mon. Tue Wed Thu Fri. Sat.

Start Time: 08 : 00

End Time: 18 : 00

[Edit / Delete](#)

Time Slot						
Edit;	ID	Name	Day in a week	Start Time	End Time	Delete
<input type="radio"/>	1	TimeSlot1	sMTWTFs	08 : 00	18 : 00	<input type="radio"/>
<input type="radio"/>	2	TimeSlot2	sMTWTFs	08 : 00	18 : 00	<input type="radio"/>
<input type="radio"/>	3	TimeSlot3	sMTWTFs	08 : 00	18 : 00	<input type="radio"/>
<input type="radio"/>	4	TimeSlot4	sMTWTFs	08 : 00	18 : 00	<input type="radio"/>
<input type="radio"/>	5	TimeSlot5	sMTWTFs	08 : 00	18 : 00	<input type="radio"/>
<input type="radio"/>	6	TimeSlot6	sMTWTFs	08 : 00	18 : 00	<input type="radio"/>
<input type="radio"/>	7	TimeSlot7	sMTWTFs	08 : 00	18 : 00	<input type="radio"/>
<input type="radio"/>	8	TimeSlot8	sMTWTFs	08 : 00	18 : 00	<input type="radio"/>
<input type="radio"/>	9	TimeSlot9	sMTWTFs	08 : 00	18 : 00	<input type="radio"/>
<input type="radio"/>	10	TimeSlot10	sMTWTFs	08 : 00	18 : 00	<input type="radio"/>
<input type="radio"/>	11	TimeSlot11	sMTWTFs	08 : 00	18 : 00	<input type="radio"/>
<input type="radio"/>	12	TimeSlot12	sMTWTFs	08 : 00	18 : 00	<input type="radio"/>
<input type="radio"/>	13	TimeSlot13	sMTWTFs	08 : 00	18 : 00	<input type="radio"/>
<input type="radio"/>	14	TimeSlot14	sMTWTFs	08 : 00	18 : 00	<input type="radio"/>
<input type="radio"/>	15	TimeSlot15	sMTWTFs	08 : 00	18 : 00	<input type="radio"/>
<input type="radio"/>	16	TimeSlot16	sMTWTFs	08 : 00	18 : 00	<input type="radio"/>

Configuration of Time Schedule

Edit a Time Slot

1. Choose any Time Slot (ID 1 to ID 16) to edit, click **Edit** radio button.

Configuration

Time Schedule

Name: TimeSlot1

Day: Sun. Mon. Tue Wed Thu Fri. Sat.

Start Time: 08 : 00

End Time: 18 : 00

Time Slot						
Edit:	ID	Name	Day in a week	Start Time	End Time	Delete
<input checked="" type="radio"/>	1	TimeSlot1	sMTWTFs	08 : 00	18 : 00	<input type="radio"/>
<input type="radio"/>	2	TimeSlot2	sMTWTFs	08 : 00	18 : 00	<input type="radio"/>
<input type="radio"/>	3	TimeSlot3	sMTWTFs	08 : 00	18 : 00	<input type="radio"/>

Note: The days that you have selected will show as capital letters. Lower case letters show the day(s) that are not selected, and no rule will apply on these days.

2. The setting of this Time Slot will be shown in detail.

Configuration

Time Schedule

Name: TimeSlot1

Day: Sun. Mon. Tue Wed Thu Fri. Sat.

Start Time: 08 : 00

End Time: 18 : 00

Time Slot						
Edit:	ID	Name	Day in a week	Start Time	End Time	Delete
<input checked="" type="radio"/>	1	TimeSlot1	sMTWTFs	08 : 00	18 : 00	<input type="radio"/>
<input type="radio"/>	2	TimeSlot2	sMTWTFs	08 : 00	18 : 00	<input type="radio"/>
<input type="radio"/>	3	TimeSlot3	sMTWTFs	08 : 00	18 : 00	<input type="radio"/>

ID: This is the index of the time slot.

Name: A user-defined description identifying this time slot.

Day: The default setting is for Monday till Friday to be enabled. You should modify this according to your requirements.

Start Time: The default is set at 8:00 AM. You may specify any required start time for your schedule.

End Time: The default is set at 18:00 (6:00PM). You may specify any required end time for your schedule.

Select the Edit radio button and click the **Edit/Delete** button to apply your changes.

Delete a Time Slot

Select the Delete radio button, and click the **Edit/Delete** button to delete the existing Time profile, i.e. Erase the selected Days and return to the default settings of Start Time / End Time.

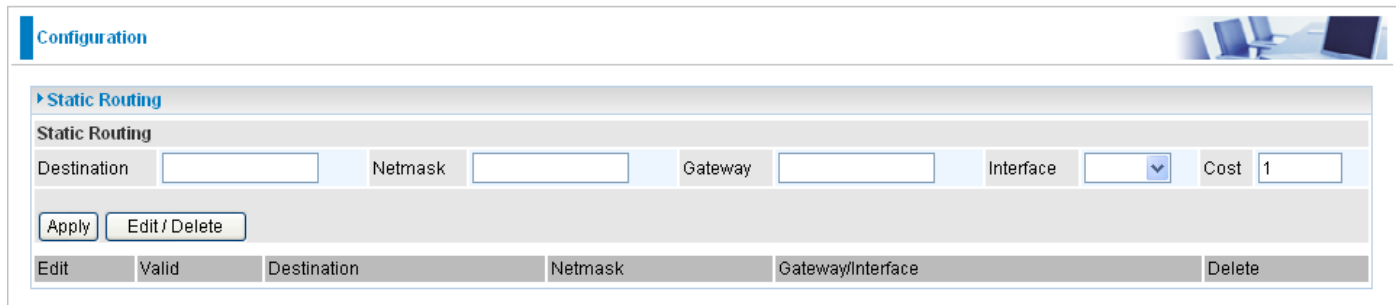
Advanced

Configuration options within the **Advanced** section are for users who wish to take advantage of the more advanced features of the router. Users who do not understand the features should not attempt to reconfigure their router, unless advised to do so by support staff.

Here are the items within the **Advanced** section: [Static Route](#), [Dynamic DNS](#), [Check Email](#), [Device Management](#), [IGMP](#) and [VLAN Bridge](#).

Static Route

Go to Configuration/Advanced/Static Route.



The screenshot shows the 'Configuration' page with a sub-section for 'Static Routing'. The 'Static Routing' section contains a form with the following fields: 'Destination', 'Netmask', 'Gateway', 'Interface' (a dropdown menu), and 'Cost' (set to 1). Below the form are 'Apply' and 'Edit / Delete' buttons. At the bottom, there is a table with columns: 'Edit', 'Valid', 'Destination', 'Netmask', 'Gateway/Interface', and 'Delete'.

Destination: This is the destination subnet IP address.

Netmask: Subnet mask of the destination IP addresses given above.

Gateway: This is the gateway IP address to which packets sent to the network defined above are to be forwarded.

Interface: Select the interface through which packets are to be forwarded.

Cost: This is the same meaning as Hop. This should usually be left at 1 unless you know the actual path length.

Dynamic DNS

The Dynamic DNS function allows you to alias a dynamic IP address to a static hostname, allowing users whose ISP does not assign them a static IP address to use a domain name. This is especially useful for hosting servers via your ADSL connection, so that anyone wishing to connect to you may use your domain name, rather than having to use your dynamic IP address, which changes from time to time. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your ISP.

Configuration

Dynamic DNS

Parameters

Dynamic DNS	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Dynamic DNS Server	<input type="text" value="www.dyndns.org (dynamic)"/>
Wildcard	<input type="checkbox"/> Enable
Domain Name	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>
Period	<input type="text" value="25"/> <input type="text" value="Day(s)"/>

You will first need to register and establish an account with the Dynamic DNS provider using their website, for example <http://www.dyndns.org/>

There are more than 5 DDNS services supported.

Dynamic DNS:

- Disable:** Select this option to disable the Dynamic DNS function.
- Enable:** Select this option to enable the Dynamic DNS function. The following fields will be activated and must be filled in:

Dynamic DNS Server: Select the DDNS service you have established an account with.

Domain Name, Username and Password: Enter your registered domain name and your username and password provided by your DDNS service.

Period: Set the time period between updates. This is the interval after which your router will exchange information with the DDNS server. In addition to updating periodically as per your settings, the router will perform an update when your dynamic IP address changes.

Check Email

This function allows you to have the router check your POP3 mailbox for new Email messages. You may view the status of this function using the Status – Email Checking section of the web interface, which also provides details on the number of new messages waiting. See the Status section of this manual for more information.

Configuration

Check Email

Parameters

Check Email	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Account Name	<input type="text"/>
Password	<input type="text"/>
POP3 Mail Server	<input type="text"/>
Period	<input type="text" value="60"/> minutes
Dial-out for Checking Emails	<input type="checkbox"/> Automatic

Check Email:

- Disable:** Select this option to disable the router's Email checking function.
- Enable:** Select this option to enable the router's Email checking function. The following fields will be activated and must be filled in:

Account Name: Enter the name (login) of the POP3 account you wish to check. Normally, it is the text in your email address before the "@" symbol. If you have trouble with it, please contact your ISP.

Password: Enter the account's password.

POP3 Mail Server: Enter your (POP) mail server name. Your Internet Service Provider (ISP) or network administrator will be able to supply you with this.

Period: Enter the value in minutes between periodic mail checks.

Dial-out for checking emails: When this function is enabled and your Internet connection is dropped, your ADSL router will automatically connect to your ISP to check for emails. Please be careful when using this feature if your ADSL service is charged by time spent online.

Device Management

The **Device Management** configuration settings allow you to control your router's security options and device monitoring features.

Configuration

Device Management

Device Host Name			
Host Name	<input type="text" value="Billion.400G"/>		
Embedded Web Server			
* HTTP Port	<input type="text" value="80"/>	(80 is default HTTP port)	
Management IP Address	<input type="text" value="0.0.0.0"/>	('0.0.0.0' means Any)	
Management IP Netmask	<input type="text" value="255.255.255.255"/>		
Management IP Address(2)	<input type="text" value="0.0.0.0"/>		
Management IP Netmask(2)	<input type="text" value="255.255.255.255"/>		
Expire to auto-logout	<input type="text" value="180"/>	seconds	
Universal Plug and Play (UPnP)			
UPnP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
* UPnP Port	<input type="text" value="2800"/>		
SNMP Access Control			
SNMP V1 and V2			
Read Community	<input type="text" value="public"/>	IP Address	<input type="text" value="0.0.0.0"/>
Write Community	<input type="text" value="password"/>	IP Address	<input type="text" value="0.0.0.0"/>
Trap Community	<input type="text"/>	IP Address	<input type="text"/>
SNMP V3			
Username	<input type="text"/>	Password	<input type="text"/>
Access Right	<input checked="" type="radio"/> Read <input type="radio"/> ReadWrite		IP Address
		<input type="text"/>	
* : This setting will become effective after you save to flash and restart the router. * : When you enable remote access, please disable/enable the remote access to update the HTTP port.			
<input type="button" value="Apply"/>			

Device Host Name

Host Name: This is the name given to your router; this should be in the form of name.name

Example:

Host Name: homegateway ==> Incorrect

Host Name: home.gateway or my.home.gateway ==> Correct

Embedded Web Server (2 Management IP Accounts)

HTTP Port: This is the port number of the router's embedded web server (for web-based configuration.) The default value is the standard HTTP port, 80. Users may specify an alternative if, for example, they are running a web server on a PC within their LAN.

Management IP Address: You may specify the IP addresses allowed to logon and access the router's web server. Setting the IP address to 0.0.0.0 will disable IP address restrictions, allowing users to login from any IP address.

Expire to auto-logout: Specify a time frame for the system to auto-logout the user's configuration session.

For Example: User A changes the routers HTTP port number to **100**, specifies their own IP address of **10.0.0.55**, and sets the logout time to be **100** seconds. The router will only allow User A access from the IP address **10.0.0.55** to logon to the Web GUI by typing: <http://10.0.0.2:100> in their web browser. After 100 seconds, the device will automatically logout User A.

Universal Plug and Play (UPnP)

UPnP offers peer-to-peer network connectivity for PCs and other network devices, along with control and data transfer between devices. UPnP offers many advantages for users running NAT routers through UPnP NAT Traversal. On supported systems, it makes tasks such as port forwarding much easier by letting the application control the required settings, thus removing the need for the user to control the advanced configuration of their router.

Both the user's Operating System and the relevant application must support UPnP in addition to the router. Windows XP and Windows ME natively support UPnP (when the component is installed), and Windows 98 users may install the Internet Connection Sharing client from Windows XP in order to support UPnP. Windows 2000 does not support UPnP.

Disable: Select this option to disable the router's UPnP functionality.

Enable: Select this option to enable the router's UPnP functionality.

UPnP Port: The default port setting is 2800. It is highly recommended that users use this port value. If this value conflicts with other ports that are already being used, you may wish to change it.

SNMP Access Control (Software on a PC within the LAN is required in order to utilize this function) – Simple Network Management Protocol.

SNMP V1 and V2:

Read Community: Specify a name to be identified as the Read Community, and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, the user on this IP address will be able to view the data.

Write Community: Specify a name to be identified as the Write Community, and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, users on this IP address will be able to view and modify the data.

Trap Community: Specify a name to be identified as the Trap Community, and an IP address. This community string will be checked against the string entered in the configuration file. Once the string name is matched, users on this IP address will be sent SNMP Traps.

SNMP V3:

Specify a name and password for authentication. And define the access rights from identified IP address. Once the authentication has succeeded, users from this IP address will be able to view and modify the data.

SNMP Version: SNMPv2c and SNMPv3

SNMPv2c is a combination of the enhanced protocol features of SNMPv2 without the SNMPv2 security. The "c" comes from the fact that SNMPv2c uses the SNMPv1 community string paradigm for "security", but is widely accepted as the SNMPv2 standard.

SNMPv3 is a strong authentication mechanism, authorization with fine granularity for remote monitoring.

Traps supported: Cold Start, Authentication Failure.

The following MIBs are supported:

From RFC 1213 (MIB-II):

- System group
- Interfaces group
- Address Translation group
- IP group
- ICMP group
- TCP group
- UDP group
- EGP (not applicable)
- Transmission
- SNMP group

From RFC1650 (EtherLike-MIB):

- dot3Stats

From RFC 1493 (Bridge MIB):

- dot1dBase group
- dot1dTp group
- dot1dStp group (if configured as spanning tree)

From RFC 1471 (PPP/LCP MIB):

- pppLink group
- pppLqr group (not applicable)

From RFC 1472 (PPP/Security MIB):

- PPP Security Group)

From RFC 1473 (PPP/IP MIB):

- PPP IP Group

From RFC 1474 (PPP/Bridge MIB):

- PPP Bridge Group

From RFC1573 (IfMIB):

- ifMIBObjects Group

From RFC1695 (atmMIB):

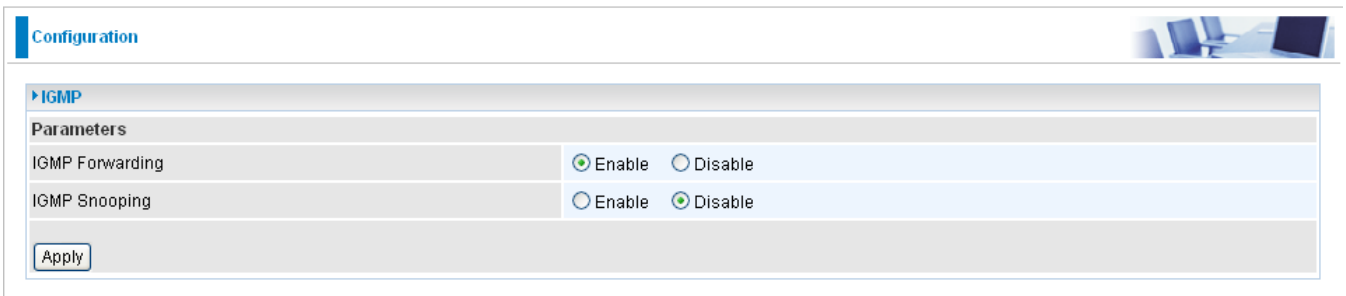
- atmMIBObjects

From RFC 1907 (SNMPv2):

- only snmpSetSerialNo OID

IGMP

IGMP, known as *Internet Group Management Protocol*, is used to management hosts from multicast group.



Configuration

IGMP

Parameters

IGMP Forwarding Enable Disable

IGMP Snooping Enable Disable

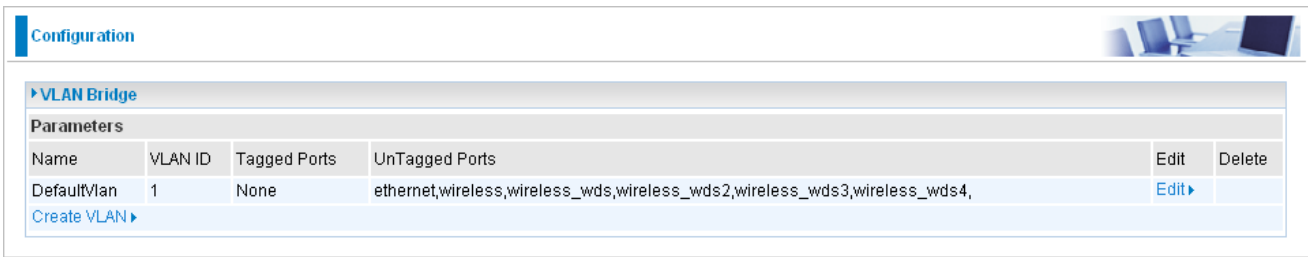
Apply

IGMP Forwarding: Accepting multicast packet. Default is set to **Enable**.

IGMP Snooping: Allowing switched Ethernet to check and make correct forwarding decisions. Default is set to **Disable**.

VLAN Bridge

This section allows you to create VLAN groups and specify the members.



Configuration

VLAN Bridge

Parameters

Name	VLAN ID	Tagged Ports	UnTagged Ports	Edit	Delete
DefaultVlan	1	None	ethernet,wireless,wireless_wds,wireless_wds2,wireless_wds3,wireless_wds4,	Edit	Delete

Create VLAN ▶

Edit: Edit your member ports in selected VLAN group.

Create VLAN: To create another VLAN group.

Logout

To exit the router's web interface, choose **Logout**. Please ensure that you have saved the configuration settings before you logout.

Be aware that the router is restricted to only one PC accessing the configuration web pages at a time. Once a PC has logged into the web interface, other PCs cannot get access until the current PC has logged out of the web interface. If the previous PC forgets to logout, the second PC can access the page after a user-defined period, by default 3 minutes. You can modify this value using the **Advanced – Device Management** section of the web interface. Please see the **Advanced** section of this manual for more information.

Chapter 5: Troubleshooting

If the router is not functioning properly, first check this chapter for simple troubleshooting before contacting the Help desk.

Problems starting up the router

<i>Problem</i>	<i>Corrective Action</i>
None of the LEDs are on when you turn on the router.	Check the connection between the adapter and the router. If the error persists, you may have a hardware problem. In this case you should contact technical support.
You have forgotten your router login and/or password.	Try the default login and password, refer to Chapter 3. If this fails, you can restore your router to its factory settings by holding the Reset button on the back of your router for 6 – 8 seconds.

Problems with the WAN Interface

<i>Problem</i>	<i>Corrective Action</i>
Initialization of the PVC connection (“linesync”) failed.	Ensure that the telephone cable is connected properly from the ADSL port to the wall jack. The ADSL LED on the front panel of the router should be on. Check that your VPI, VCI, encapsulation type and type of multiplexing settings are the same as those provided by your ISP. Reboot the router. If you still have problems, you may need to verify these settings with your ISP.
Frequent loss of ADSL linesync (disconnections).	Ensure that all other devices connected to the same telephone line as your router (e.g. telephones, fax machines, analogue modems) have a line filter connected between them and the wall socket, and ensure that all line filters are correctly installed and the right way around. Missing line filters or line filters installed the wrong way around can cause problems with your ADSL connection, including causing frequent disconnections.

Problems with the LAN Interface

<i>Problem</i>	<i>Corrective Action</i>
Can't ping any PCs on the LAN.	Check the Ethernet LEDs on the front panel. The LED should be on for a port that has a PC connected. If it is off, check the cables between your router and the PC. Make sure you have uninstalled any software firewall for troubleshooting.
	Verify that the IP address and the subnet mask are consistent between the router and the workstations.

Most problems can be solved by referring to the **Troubleshooting** section in the User's Manual. If you cannot resolve the problem with the **Troubleshooting** chapter, please contact the dealer where you purchased this product.

Contact Telkom ADSL support

Telephone: 0800 375 375
Operating hours: 24hrs – 7 days a week

Contact SizweBroadband for Router Support

Telephone: 0860 110 041
Website: www.sizwebroadband.co.za
Operating hours: 8:00am to 17:00pm (work days only)