BELKIN | ADSL2+ Modem

Broadband Voice Modem/Router

BELKIN

www.belkin.com/anz

User Manual

P75000au-A

Table of Contents

Introduction

Thank you for purchasing the Belkin ADSL 2+ Modem. In minutes you will be able to connect to the Internet and make Voice over Internet Phone calls. The following is a list of features that make your Modem an ideal solution for your home or small office and will contain important information on how to get what you want out of your VOIP Router so please read carefully before setting up your router.

Belkin Broadband Voice Modem/Router - 1 Port

Part # F1PI210ENau

Compatibility with both PC and Mac® Computers

The Modem supports a variety of networking environments including Mac OS® 8.x, 9.x & v10.x, AppleTalk®, Linux®, Windows® 98SE, ME, NT, 2000 and XP and others. You need an Internet browser and a network adapter that supports TCP/IP (the standard language of the Internet).

Internet Access

This device supports Internet access through an ADSL connection. Since many ADSL providers use PPPoE or PPPoA to establish communications with end users, the VoIP Router includes built-in clients for these protocols, eliminating the need to install these services on your computer.

Front-Panel LED Display

Light LED's on the front of the Modem indicate which functions are in operation. You'll know at-a-glance whether your Modem is connected to the Internet. This feature eliminates the need for advanced software and status-monitoring procedures.

Web-Based Advanced User Interface

You can set up the Modem advanced functions easily through your web browser, without having to install additional software onto the computer. There are no disks to install or keep track of and, best of all, you can make changes and perform setup functions from any computer on the network quickly and easily.

Built-in Dynamic Host Configuration Protocol (DHCP)

Built-In Dynamic Host Configuration Protocol (DHCP) on-board makes for the easiest possible connection of a network. The DHCP server will assign IP addresses to each computer automatically so there is no need for a complicated networking setup.

Product Overview

DMZ Host Support

DMZ Host Support allows a networked computer to be fully exposed to the Internet. This function is used when NAT and firewall security prevent an Internet application from functioning correctly.

NAT IP Address Sharing

Your Modem employs Network Address Translation (NAT) to share the single IP address assigned to you by your Internet Service Provider while saving the cost of adding additional IP addresses to your Internet service account.

SPI Firewall

Your Modem is equipped with a firewall that will protect your network from a wide array of common hacker attacks including:

IP Spoofing, Land Attack, Ping of Death (PoD), Denial of Service (DoS), IP with zero length, Smurf Attack, TCP Null Scan, SYN flood, UDP flooding, Tear Drop Attack, ICMP defect, RIP defect, and fragment flooding.

Universal Plug-and-Play (UPnP) Compatibility

UPnP (Universal Plug-and-Play) is a technology that offers seamless operation of voice messaging, video messaging, games, and other applications that are UPnP-compliant.

QoS

QoS (Quality of Service) limits the traffic being sent from the modem (upstream) when using VoIP at the same time. If QoS is disabled, the quality of the VoIP call can suffer due to excessive traffic from another source, such as a PC. When QoS is enabled, it limits the upstream traffic and sets it aside for VoIP, increasing the call quality.

Belkin Broadband Voice Modem/Router - 4 Port

Part # F1PI241ENau

Has all the features above but also has:

Virtual Server

If you have a fixed IP address, you can set the VoIP Router to act as a virtual host for network address translation. Remote users access various services at your site using a constant IP address. Then, depending on the requested service (or port number), the VoIP Router can route the request to the appropriate server (at another internal IP address). This secures your network from direct attack by hackers, and provides more flexible management by allowing you to change internal IP addresses without affecting outside access to your network.

Built in 4 Port Wired LAN compatibility

The VoIP Router provides access for up to 4 by 10/100 Mbps wired devices making it easy to create a network in small offices or homes.

Support for VPN Pass-Through

If you connect to your office network from home using a VPN connection, your Modem will allow your VPN-equipped computer to pass through the Modem and to your office network.

This VoIP Router supports three of the most commonly used VPN protocols – PPTP, L2TP, and IPSec. The VPN protocols supported by the VoIP Router are briefly described below.

- Point-to-Point Tunneling Protocol – Provides a secure tunnel for remote client access to a PPTP security gateway. PPTP includes provisions for call origination and flow control required by ISPs.
- L2TP merges the best features of PPTP and L2F – Like PPTP, L2TP requires that the ISP's routers support the protocol.
- IP Security – Provides IP network-layer encryption. IPSec can support large encryption networks (such as the Internet) by using digital certificates for device authentication.

VLAN

VLAN (Virtual Local Area Network) adds the ability to manage multiple networks with the one modem.

Belkin Broadband Voice Modem with Wireless Router - 4 port

Part # F1PI241EGau

Has all the features above but also has:

Wired & Wireless LAN

The VoIP Router provides access for up to 4 by 10/100 Mbps wired devices and up to an additional 32 wireless devices, making it easy to create a network in small offices or homes.

MAC Address Filtering

For added security, you can set up a list of MAC addresses (unique client identifiers) that are allowed access to your network. Every computer has its own MAC address. Simply enter these MAC addresses into a list using the web-based user interface and you can control access to your network.

WEP, WPA and WPA 2 Encryption protocols

The Router features WPA2, which is the second generation of the WPA-based 802.11i standard. It offers a higher level of wireless security by combining advanced network authentication and stronger Advanced Encryption Standard (AES) encryption methods. It also supports the legacy security standard called Wired Equivalent Privacy (WEP) in order to allow you to activate security with any legacy devices you may have in your network.

Voice over IP (VoIP)

An Introduction

Using Voice over IP (VoIP), instead of making calls over the regular telephone network, calls are made over computer (IP) networks, either through your Internet Service Provider's connection or through your local network. Calls made are generally cheaper than traditional calls.

The basic steps involved in VoIP include the conversion of an analog voice signal to digital, the encoding and then compression of the signal into Internet Protocol (IP) packets. The VoIP Router is equipped with a digital signal processor (DSP), which segments the voice signal into frames and stores them in voice packets. Using the industry standard codecs, G.711, G.723.3 and G.729, these packets are encoded. These IP packets are then transmitted in accordance with International Telecommunications Union specification SIP over the Internet to their destination where the process is reversed.

Advantages of Using VoIP

The main advantage of VoIP over the traditional Public Switched Telephone Network (PSTN) is the ability to make low-cost calls over the IP network. One of the greatest benefits is cheaper long distance calls.

Past Problems

Internet-based telephony has been around for years but, until now, has not reached the mainstream market.

Products with a true cost-saving advantage over standard telephones do not have comparable call quality. Users experience a prolonged delay making conversation difficult.

Call-completion rates are very low due to firewalls and the use of Network Address Translation (NAT), which renders over 50% of residential computers unable to communicate with traditional VoIP software.

The user interface is complicated, and requires substantial configuration and technical skills.

Recent Developments

Even as streaming audio and video over the Internet became common, VoIP quality was still sub-par. What, you may ask, is the reason for this? While it's relatively easy to convert a song or even a video into IP-based packets and have it arrive in decent shape, the Internet was not designed as a two-way street, i.e., to support two-way communications as in your typical conversation. Early VoIP calls were much like walkie-talkie speech, halting and unsynchronized. A common trick was to let the other speaker know you had finished talking by ending your statement with the word "Over." For example,

"How are you today? Over." "Not too good, I think I've the flu. Are you busy? Over."

This method was effective, but hardly conducive to a comfortable conversation! Therefore, substantial cost savings, although attractive, were not enough to make up for unacceptably poor call quality. Now, however, thanks to dedicated hardware processing and protocols like Session Initiation Protocol (SIP), VoIP can be as smooth as a session that uses the regular telephone network, greatly increasing its appeal.

Equally as important to VoIP's recent surge has been the widespread adoption of broadband in both homes and businesses, which delivers the bandwidth required to come close to PSTN quality.

Features and Benefits

NAT also enables multi-user Internet access via a single user account, and virtual server functionality (providing protected access to Internet services such as Web, FTP, email, and Telnet) VPN pass-through (IPSec-ESP Tunnel mode, L2TP, PPTP) User-definable application sensing tunnel supports applications requiring multiple connections easy setup through a web browser on any operating system that supports TCP/IP compatible with all popular Internet applications.

VoIP Features and Benefits

Full Session Initiation Protocol (SIP) support
Voice Activity Detection (VAD) conserves bandwidth
Quality of Service (QoS) provides superior voice quality

The Modem is designed to be placed on a desktop. All of the cables exit from the rear of the Modem for better organization and utility. The LED indicators are easily visible on the front of the Modem to provide you with information about network activity and status.

Front Panel

Broadband Voice Modem/Router - 1 Port Part # F1PI210ENau

Broadband Voice Modem/Router - 4 Port Part # F1PI241ENau

Broadband Voice Modem with Wireless Router - 4 port Part # F1PI241EGau

1. PSTN Failover Status LED

The PSTN Failover Status LED is designed to let you know when the system successfully detects that an additional back up phone line is installed and running correctly. This line is then used to route your phone calls in times when your ADSL service is incapable of making calls.

On - PSTN Line is in use
Off - PSTN Line not in use

2-3. Phone Status LED 1-2

Whenever you make a phone call on one of the handsets attached to the VoIP router the lights will inform you of the current status of that phone call.

On - VoIP activity, i.e. phone is in use
On - Flashing, incoming call, i.e. phone is ringing
Off - No VoIP activity

4. VOIP Status LED

When your ADSL connection is being used to make VoIP calls from one of the handsets connected this light will be on to assist you in knowing what kind of traffic your network working under.

On - VoIP activity
Off - No VoIP activity

5. LAN Status LED 1-4

When a computer is properly connected to the LAN port on the rear of the modem, the associated LED will light. A solid light means a computer or a network-enabled device is connected. When information is being sent over the port, the LED blinks rapidly.
Off - Your computer is not connected
On - Blinking connected and transmitting or receiving data
On - Your computer is connected

6. WLAN Status LED

The WLAN status LED shows you when a computer is connected wirelessly to the VOIP Router is connected. When the LED is OFF, the VOIP Router is NOT connected to any computer. When the LED is solid light, the VOIP Router is connected to a wireless computer. When the LED is blinking, the VOIP Router is negotiating with a wireless computer.

On - Wireless connection
On - Flashing, a wireless connection has been made and data is transmitting/receiving
Off - No wireless connection

7. ADSL ONLINE LED

The ADSL Online LED shows you when the Modem is connected to the Internet. When the LED is OFF, the Modem is NOT connected to the Internet. When the LED is solid light, the Modem is connected to the Internet. When the LED is blinking, the Modem is transmitting or receiving data from the Internet.

Off - Not connected to Internet
On - Blinking connected and transmitting or receiving data
On - Connected to Internet

8. **ADSL SYNC LED**
   The ADSL LED flashes light during negotiation with your ISP. It stays light when the Modem is connected properly to your ADSL service.

   Off - No ADSL connection
   On - Blinking negotiating connection/no ADSL Sync
   On - ADSL link is up and connected

9. **Power LED**
   When you apply power to the Modem or restart it, a short period of time elapses while the Modem boots up. When the Modem has completely booted up, the power LED becomes a SOLID light, indicating the Modem is ready for use.
   Off Modem is off
   On Modem is on

Back Panel

Broadband Voice Modem/Router - 1 Port Part # F1PI210ENau

Broadband Voice Modem/Router - 4 Port Part # F1PI241ENau

Broadband Voice Modem with Wireless Router - 4 port Part # F1PI241EGau

1. **ADSL Line**
   This port is for connection to your ADSL line. Connect your ADSL line to this port.

2. **LAN Ports**
   The Ethernet port is RJ45, 10/100 auto-negotiation. Connect your network-enabled computers or any networking devices to this port.

3. **Power Switch**
   Standard power switch used to turn the VOIP Router on and off.

4. **Power Plug**
   Connect the included 12V 1A DC power supply to this inlet. Using the wrong type of power adapter may cause damage to your Modem.

5. **Reset Button**
   The “Reset” button is used in rare cases when the Modem may function improperly. Resetting the Modem will restore the Modem’s normal operation while maintaining the programmed settings. You can also restore the factory default settings by using the Reset button. Use the restore option in instances where you may have forgotten your custom password.

   a. **Resetting the Modem**
      Push and hold the Reset button for one second then release it. When the PWR light becomes solid again the reset is complete.

   b. **Restoring the Factory Defaults**
      Push and hold the Reset button for twenty seconds then release it. When the PWR light becomes solid again the restore is complete.

6. **Phone Port**
   Phone Ports connect to standard analogue telephone set or fax machine.

7. **PSTN Failover Port**
   The Optional RJ-11 port is for connection to your PSTN (Home Phone) line to provide normal phone call backup for when VOIP is unavailable or not required.

Step 1. Find a suitable location

The VoIP Router can be positioned at any convenient location in your office or home where there is easy access to a phone jack and power point nearby. No special wiring or cooling requirements are needed and there is no necessity to keep the unit connected directly to a computer.

You should, however, comply with the following guidelines:

Keep the VoIP Router away from any heating devices.

Do not place the VoIP Router in a dusty or wet environment.

You should also remember to turn off the power, remove the power cord from the outlet, and keep your hands dry when you install the VoIP Router.

Step 2. Connect the ADSL Line

Phone line configuration

Run standard telephone cable from the wall jack providing ADSL service to the RJ-11 (“ADSL”) port on your VoIP Router. When inserting an ADSL RJ-11 plug, be sure the tab on the plug clicks into position to ensure that it is properly seated. If you are using a splitter less ADSL service, be sure you add low-pass filters between the ADSL wall jack and your telephones. (These filters pass voice signals through but filter data signals out.)

Note: If more than 4 connections of any kind (Ie faxes, phones, modems etc) are to be used you will need to get a central splitter installed.

Step 3. Attach to your network using Ethernet cabling

The LAN ports on the VoIP Router auto-negotiates the connection speed to 10 Mbps Ethernet or 100 Mbps Fast Ethernet, as well as the transmission mode to half duplex or full duplex.

Use twisted-pair cabling to connect any of the LAN ports on the VoIP Router to an Ethernet adapter on your PC. Otherwise, cascade the LAN port on the VoIP Router to an Ethernet hub or switch, and then

Connecting and Configuring your Router

connect your PC or other network equipment to the hub or switch. When inserting an RJ-45 connector, be sure the tab on the connector clicks into position to ensure that it is properly seated.

Warning: Do not plug a phone jack connector into an RJ-45 port. This may damage the VoIP Router. Instead, use only twisted-pair cables with RJ-45 connectors that conform to Australian standards.

Notes:

1. Use 100-ohm shielded or unshielded twisted-pair cable with RJ-45 connectors for all Ethernet ports. Use Category 3, 4, or 5 for connections that operate at 10 Mbps, and Category 5 for connections that operate at 100 Mbps.
2. Make sure each twisted-pair cable length does not exceed 100 meters (328 feet).

Step 4. Connect the power adapter

Plug the power adapter into the power socket on the side panel of the VoIP Router, and the other end into a power outlet.

Check the power indicator on the front panel is lit. If the power indicator is not lit, refer to “Troubleshooting”.

In case of a power failure, the VoIP Router will automatically restart and begin to operate once the power is restored.

At this time we have now completed connecting the router and may now move to the actual configuration of your connection.

* Time needed to obtain line sync will vary depending on various factors such as line noise and attempted sync speed.

Step 1. How to log into the Router

Using your web browser to configure the VoIP ADSL Wireless Router. The VoIP Router can be configured by any Java-supported browser such as Internet Explorer 5.0 or above. Using the web management interface, you may configure the VoIP Router and view statistics to monitor network activity.

To access the VoIP Router's management interface, enter the IP address of the VoIP Router in your web browser: **10.1.1.1**

Note: If you are unable to access this web page please look at the IP setup section of the Troubleshooting appendices at the back of this manual.

Type in "**admin**" as the password and click login. **Note:** Password is case sensitive.

ISP Settings

Please collect the following information from your ISP before setting up the VoIP Router:

ISP account user name and password
Protocol, encapsulation and VPI/VCI circuit numbers
DNS server address
IP address, subnet mask and default gateway (for fixed IP users only).

Step 2. Navigating the web browser interface

The VoIP Router's management interface consists of a Setup Wizard and an Advanced Setup section.

Setup Wizard: Use the Setup Wizard to quickly set up the VoIP Router.

Advanced Setup: Advanced Setup supports more advanced functions like hacker attack detection, IP and MAC address filtering, virtual server setup, virtual DMZ host, as well as other functions.

Note: If you would like to add any additional functions to your VoIP Router please view the Advanced Setup table of contents in order to find the correct setup method.

Connecting and Configuring your Router

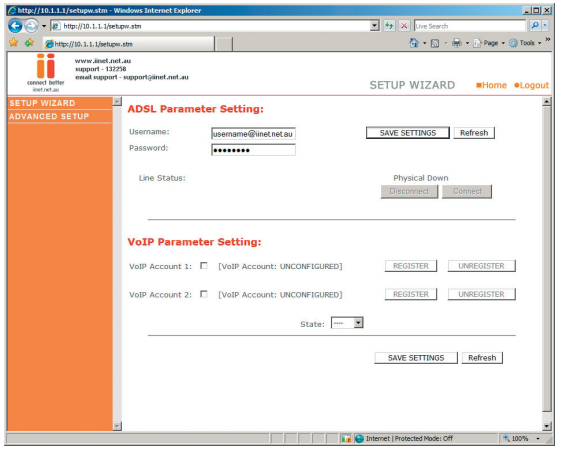
Making Configuration Changes

Configurable parameters have a dialog box or a drop-down list. Once a configuration change has been made on a page, most of the time you will need to click the "SAVE SETTINGS" or "NEXT" button at the bottom of the page to enable the new setting. Unless there is a "ADD" button for instance.

Note: To ensure proper screen refresh after a command entry, be sure that Internet Explorer 5.0 and above is configured as follows: Under the menu Tools/Internet Options/General/Temporary Internet Files/ Settings, the setting for "Check for newer versions of stored pages" should be "Every visit to the page."

Step 3. Using Setup Wizard

This page allows you to quickly setup basic settings of the modem to get you connected quickly. After making a change click on the save settings button on the screen to apply the changes.



ADSL Parameter Setting

User Name: Enter your internet account user name for you ISP.

Password: Enter your internet account password for you ISP.

ADSL Parameter Setting

Firstly you need to tick one of the VoIP account boxes. For instance if you wish to use VoIP port 1 on the back of the modem then tick the box for VoIP account 1. Then you must enter your VoIP account details and click on save settings.

Phone Number:
Enter your VoIP account phone number from your ISP.

Password:
Enter your VoIP account password from your ISP.

Register:
Click to register your VoIP account to be ready for use.

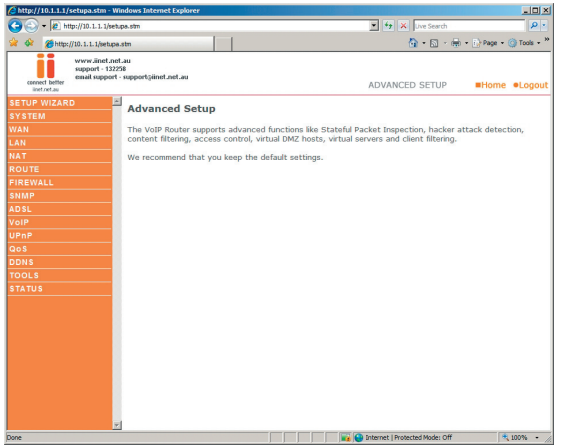
Unregister: Un-register your VoIP account, so that you can use it on another VoIP port or device.

Clicking the Home icon returns you to the home page. The Main Menu links are used to navigate to other menus that display configuration parameters and statistics.

Making configuration changes

Configurable parameters have a dialog box or a drop-down list. Once a configuration change has been made on a page, click the “SAVE SETTINGS” button at the bottom of the page to make the new settings active.

Note: To ensure proper screen refresh after a command entry, check that Internet Explorer 5.0 is configured as follows: Under the menu Tools/Internet Options/General/Temporary Internet Files/Settings, the setting for “Check for newer versions of stored pages” should be “Every visit to the page.”



The VoIP Router’s advanced management interface contains 15 main menu items as described in the following list.

Commonly requested features

Noted in this section is a quick reference guide to the most commonly requested advanced features and should save you the time of needing to read the entire section for the necessary features you are interested in.

Setting up wireless (Page 36)

This section will explain the basics of turning on the wireless functions in you Router, if you should require this service it is also suggested you look into the setting up wireless security area as well.

Setting up wireless security (Page 39)

This section describes the 2 forms of wireless security available and allows you to choose either or both types of security in order to protect your network from outside access.

Option 1: MAC address filtering (Page 38)

MAC address filtering uses a unique code that each computer has in order to create a list of computers that will be allowed onto your network.

Option 2: Wireless encryption (Page 40)

Wireless encryption uses a code much like a secret password in order to ensure only those computers which know the password are able to access your network.

Setting up VoIP (Page 66)

This section will guide you through the basics of setting up your VoIP service on your network.

Setting/adjusting quality of service (Page 75)

If you are having problems with the quality of your Voice service due to large amounts of network traffic you may adjust your Quality of Service in this section.

Port forwarding (Page 45)

Some programs will require you to direct certain port numbers to your computer in order to bypass the built in Firewall.

Should there be any further features within the product you would like to use please find a more extensive list on the next page.

Menu Description

System (Page 22)

Within the System menu you can:

- Set the local time and time zone as well as Time Sync Server
- Set the password for administrator access
- Enable remote management and set the IP address of a PC that will be allowed to access Router remotely
- The IP address of a Domain Name Server

WAN (Page 26)

- ATM PVC specifies the Internet connection setting for an ATM (Asynchronous Transfer Mode) Framework WAN, this service is used primarily in corporate environments and we would suggest contacting your corporate administrator in order to setup these features.
- MAC Address Cloning can also be performed in this section should it be required by your Internet service provider in order to complete the Internet connection.

LAN (Page 31)

The LAN menu itself has a number of special fields in which you can configure information about your Local Area Network like those functions noted below:

- LAN IP Address Settings
- Subnet Mask settings
- DCHP Server Control
- VLAN Port routing

The LAN Menu also has 2 sub-menus:

- **VLAN**

  This menu allows you to set the VLAN rules for the other ports and should only be accessed by experienced professionals.

- **DHCP Client Lists**

  This menu shows you a list of all computers currently connected to your network along with their host name and other details.

Wireless (Page 36)

The wireless menu allows you to turn on/off the wireless features on your router as well as having 4 sub-menus:

- **Channel & SSID**

  This area includes the most basic of router functions and allows you to give a unique name to your network as well as allowing you to change the channel your wireless is running on incase it is accidentally sharing the same channel as another wireless appliance in the area.

- **Access Control**

  Access Control or MAC address filtering as it is also known is an additional level of security which allows you to specify which computers are able to log into the network via their unique "MAC Address."

- **Security**

  The Security menu allows you access to the other form of Wireless Security known as Encryption. This works by using a numerical code as a key to your network.

- **WDS**

  WDS stands for Wireless Distribution System and is designed to allow you to add access points to your network. These work as a relay station to extend the range of your network.

NAT (Page 43)

- Shares a single ISP account with multiple users, sets up port forwarding.

Route (Page 48)

- Sets routing parameters and displays the current routing table. A route determines the way in which the data travels through the network.

Firewall (Page 52)

- Configures a variety of security and specialized functions including: Access Control, URL blocking, Internet access control scheduling, Intruder detection, and DMZ.

SNMP (Page 61)

- Community string and trap server setting. SNMP (Simple Network Management Protocol) is used by network administrators to manage attached network devices.

ADSL (Page 63)

- Sets the ADSL operation type and shows the ADSL status.

VoIP (Page 66)

- Configures VoIP settings for the VoIP Router, this section involves extensive and detailed settings. Please read the entire section carefully before attempting any changes.

UPnP (Page 75)

- Allows you to enable or disable the Universal Plug and Play function. UPnP is designed to allow users seamless Internet operation without the need to open any ports in the firewall.

QoS (Page 75)

- Allows you to optimize voice quality by prioritizing voice over data traffic. QoS (Quality of Service) can be set to prioritize traffic for many features such as VoIP, VPN, nominated IP Addresses and ports etc.

DDNS (Page 79)

- DDNS (Dynamic Domain Name Server) allows you to host services on the internet via a web address. For example it would allow you to host a web page or email server even with a dynamic WAN IP Address. In order to use this function you may need to purchase additional services like a Domain name from a service provider. This router supports DynDNS and TZO.

Tools (Page 80)

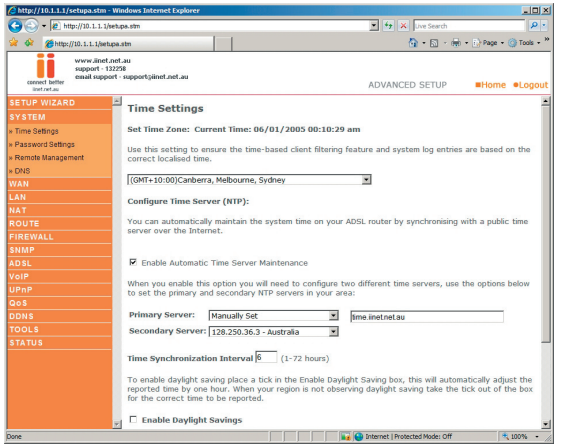
- Contains options to back up and restore the current configuration, restore all configuration settings to the factory defaults, update system firmware, or reset the system each under its own menu.

Status (Page 82)

- Provides WAN connection type and status, firmware and hardware version numbers, system IP settings, as well as DHCP, NAT, and firewall information.
- Displays the number of attached clients, the firmware versions, the physical MAC address for each media interface, and the hardware version and serial number.
- Shows the security and DHCP client log.

System Settings

Time Settings



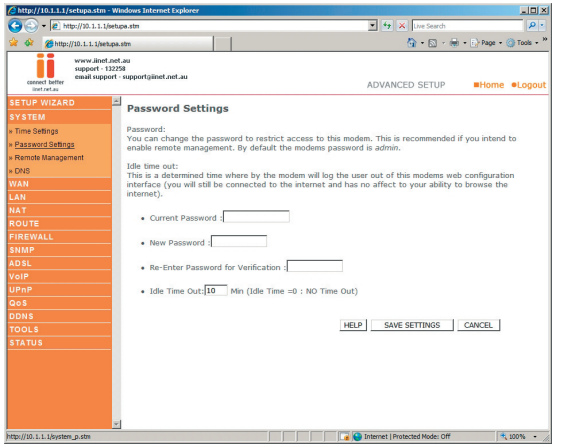
Set the time zone and time server for the VoIP Router. This information is used for log entries and client access control.

Check “Enable Automatic Time Server Maintenance” to automatically maintain the VoIP Router’s system time by synchronizing with a public time server over the Internet. Then configure two different time servers by selecting the options in the Primary Server and Secondary Server fields.

Advanced Setup Method

Password Settings

Use this page to restrict access based on a password. By default, the password is “admin”.



Passwords can contain from 3 to12 alphanumeric characters which are case sensitive.

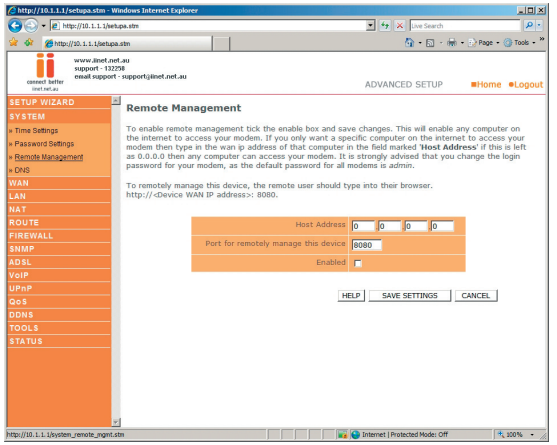
Note: If your password is lost, or you cannot gain access to the user interface, press the reset button (colored blue) on the rear panel (holding it down for at least 20 seconds) to restore the factory defaults. (By default the password is “admin”)

Enter a maximum Idle Time Out (in minutes) to define a maximum period of time an inactive login session will be maintained. If the connection is inactive for longer than the maximum idle time, it will be logged out, and you will have to login to the web management system again. (Default: 10 minutes)

Remote Management

By default, management access is only available to users on your local network. However, you can also manage the VoIP Router from outside your network via remote management by checking the Enabled check box. You can set a HOST ADDRESS, which will only

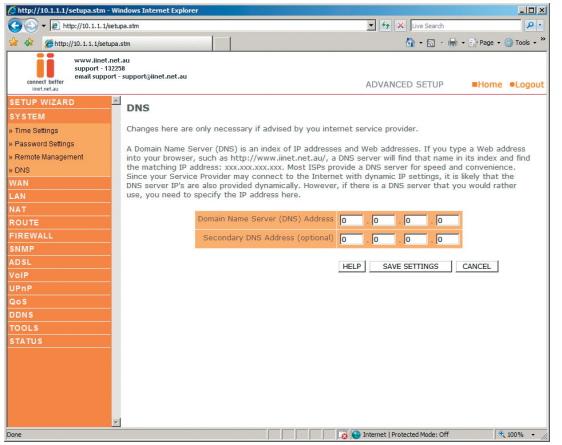
allow that computer to use remote management. The port field should be left as the default setting of 8080 unless you need to change it. After any changes are made you must click on “Save Settings” to apply them.



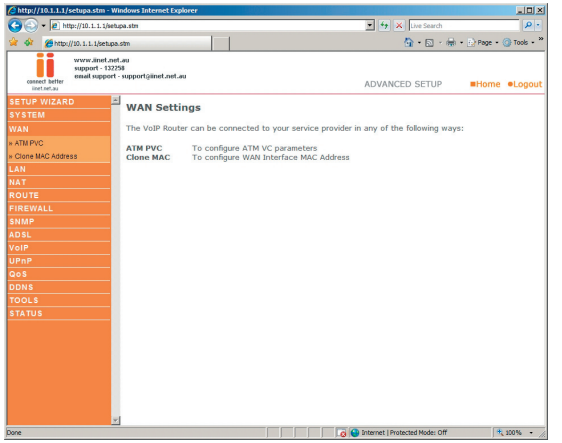
Note: If you check “Enabled” and specify an IP address of 0.0.0.0, any host can manage the VoIP Router.

For remote management via a WAN IP address you need to connect using port 8080. Simply enter WAN IP address followed by :8080 in the address field of your web browser, for example, http://212.120.68.20:8080. This applies unless you change the port setting, in which case you need to substitute the 8080 for whatever port you have assigned.

DNS



Domain Name Servers are used to map a domain name (e.g. www.somesite.com) to the equivalent numerical IP address (e.g. 64.147.25.20). Your ISP should provide the IP address of one or more Domain Name Servers. Enter those addresses on this page.



WAN

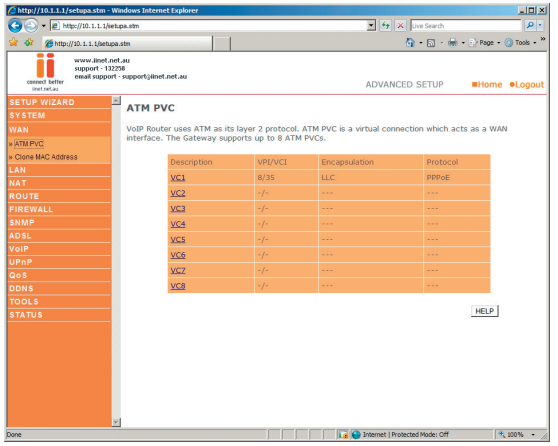
Specify the WAN connection parameters provided by your Internet Service Provider (ISP).

The VoIP Router can be connected to your ISP in one of the following ways:

- ATM PVC
- Clone MAC

ATM PVC

The VoIP Router uses ATM as its WAN interface. Click on each ATM VC for WAN configuration.



Parameter Description

Description:
Click on the VC to set the values for the connection.

VPI/VCI:
Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI).

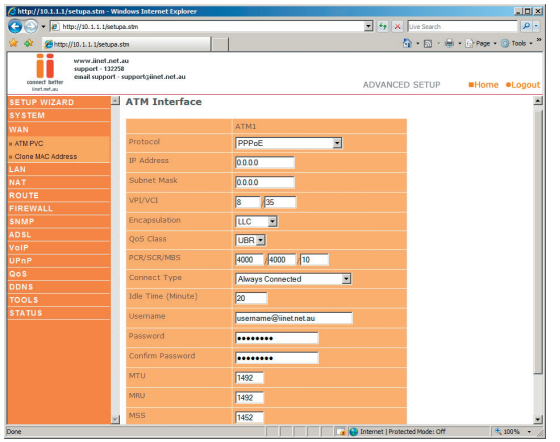
Encapsulation:
Specifies how to handle multiple protocols at the ATM transport layer.

- **VC-MUX:** Point-to-Point Protocol over ATM Virtual Circuit Multiplexer (null encapsulation) allows only one protocol running per virtual circuit with less overhead.
- **LLC:** Point-to-Point Protocol over ATM Logical Link Control (LLC) allows multiple protocols running over one virtual circuit (using slightly more overhead).

Protocol:
Protocol used for the connection.

ATM Interface

Clicking on the ATM VC brings up the following screen. The VoIP Router uses ATM as its WAN interface. Protocols including 1483 Routing, 1483 Bridging, MAC Encapsulated Routing (MER), PPPoA and PPPoE with LLC-SNAP and VC-MUX encapsulations are supported for each ATM PVC.



When you have finished entering your connection parameters, click “SAVE SETTINGS”. You can verify that you have established an ADSL connection by clicking Status at the bottom of the left-hand menu.

See the table below for a description of the parameters.

Parameter Description

Protocol

- **Disable:** Disables the connection.
- **1483 Bridging:** Bridging is a standardized layer 2 technology. It is typically used in corporate networks to extend the physical reach of a single LAN segment and increase the number of stations on a LAN without compromising performance. Bridged data is encapsulated using the RFC1483 protocol to enable data transport. Please note that setting the router to bridged mode disables all advanced features such as VoIP, Firewall, and QoS etc.
- **PPPoA:** Point-to-Point Protocol over ATM is a method of encapsulating data for transmission to a far point.
- **1483 Routing:** 1483 Routing allows a simple, low-cost connection to the Internet via a standard Ethernet port. The router looks up the network address for each packet seen on the LAN port. If the address is listed in the routing table as local, it is filtered. If the address is listed under the ADSL port, it is forwarded. Or if the address is not found, then it is automatically forwarded to the default router (i.e. the VoIP Router at the head end).
- **PPPoE:** Point-to-Point over Ethernet is a common connection method used for xDSL.
- **MAC Encapsulated Routing:** If your ADSL service is a Bridged mode service and you want to share the connection to multiple PC's, please select MAC Encapsulated Routing. MER is a protocol that allows you do IP routing with NAT enabled.

VPI/VCI

Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI). Data flows are broken up into fixed length cells, each of which contains a Virtual Path Identifier (VPI) that identifies the path between two nodes, and a Virtual Circuit Identifier (VCI) that identifies the data channel within that virtual path. Each virtual circuit maintains a constant flow of cells between the two end points. When there is no data to transmit, empty cells are sent. When data needs to be transmitted, it is immediately inserted into the cell flows.

Advanced Setup Method

Parameter Description

Encapsulation

Shows the packet encapsulation type.

Packet encapsulation specifies how to handle multiple protocols at the ATM transport layer.

- VC-MUX: Point-to-Point Protocol over ATM Virtual Circuit Multiplexer (null encapsulation) allows only one protocol running per virtual circuit with less overhead.
- LLC: Point-to-Point Protocol over ATM Logical Link Control allows multiple protocols running over one virtual circuit (using slightly more overhead).

QoS Class

ATM QoS classes including CBR, UBR and VBR.

PCR/SCR/MBS

QoS Parameters - PCR (Peak Cell Rate), SCR (Sustainable Cell Rate) and MBS (Maximum Burst Size) are configurable.

IP Address: If your IP address is assigned by the ISP each time you connect, leave this field all zeros. Otherwise, enter your ISP supplied static IP address here.

Subnet Mask: If your subnet mask is assigned by the ISP each time you connect, leave this field all zeros. Otherwise, enter your subnet mask here.

Connect Type

Sets connection mode to always connected, automatic or manual connection.

Idle Time: Enter the maximum idle time for the Internet connection. (in minutes) After this time has been exceeded the connection will be terminated.

Username: Enter user name

Password: Enter password

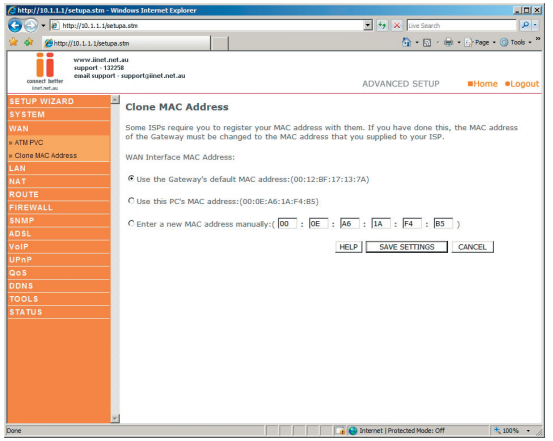
Confirm Password: Confirm password

MTU

Leave the Maximum Transmission Unit (MTU) at the default value (1500) unless you have a particular reason to change it.

Clone MAC Address

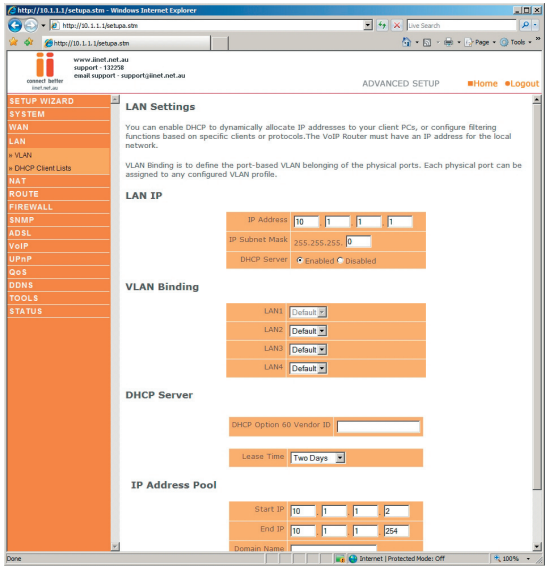
Clicking on the Clone MAC Address brings up the following screen.



Some ISPs may require that you register your MAC address with them. If this is the case, the MAC address of the VoIP Router must be changed manually to the MAC address that you have registered with your ISP.

LAN

Use the LAN menu to configure the LAN IP address and to enable the DHCP server for dynamic client address allocation.



Parameter Description

LAN IP

IP Address:
The IP address of the VoIP Router.

IP Subnet Mask:
The subnet mask of the VoIP Router.

DHCP Server:
To dynamically assign an IP address to client PCs, enable the DHCP (Dynamic Host Configuration Protocol) Server.

VLAN Binding

In this section you can assign VLAN's that you have created in the VLAN page to certain ports such as LAN port 1, 2, 3 or 4 and the

WLAN connection. For instance if you have created a VLAN Binding called “Test”, and you want anything connected to the wireless to be on that VLAN, then you would change the WLAN setting on this page from “Default” to the one you created called “Test”.

Parameter Description

DHCP SERVER

DHCP Option 60 Vendor ID:
If you wish you can specify the Name of your DHCP Server (Optional)

Lease Time:
Specify the length of time that the DHCP will assign an IP address to a computer for.

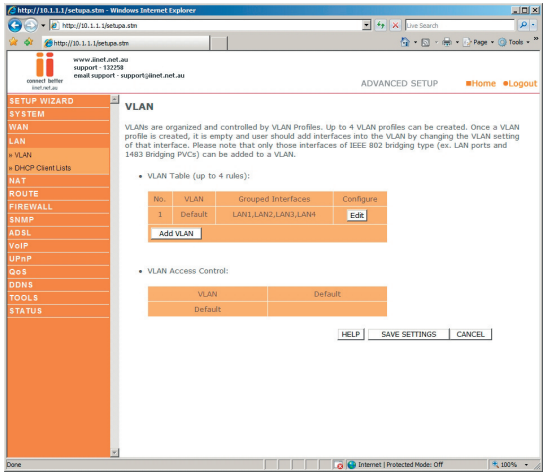
IP Address Pool

Start IP:
Specify the start IP address of the DHCP pool. Do not include the gateway address of the VoIP Router in the client address pool. (See “TCP/IP Configuration”). If you attempt to include the VoIP Router gateway address (10.1.1.1 by default) in the DHCP pool, an error dialog box will appear. If you change the pool range, make sure the first three octets match the gateway’s IP address, i.e. 10.1.1.xxx.

End IP:
Specify the end IP address of the DHCP pool.

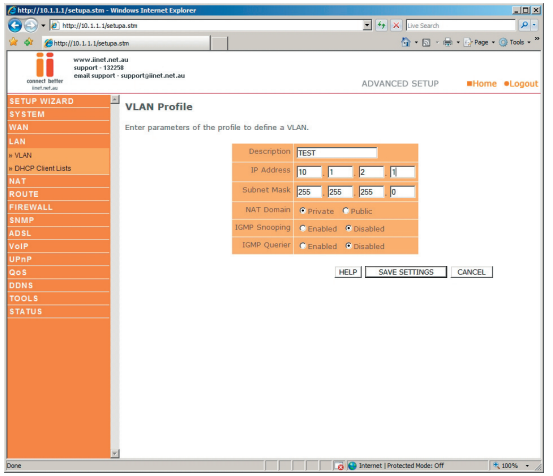
Domain Name:
If your network uses a domain name, enter it here. Otherwise, leave this field blank.

VLAN



VLAN Table:
In this table you can click on the ADD VLAN button to add a VLAN binding or click on EDIT to edit an existing binding, or click on DELETE to remove a Binding.

VLAN Profile:
This screen will appear if you click on “ADD VLAN” or “EDIT” from the VLAN page.



Description:
Detail description of the VLAN.

IP Address:
IP address of the VLAN virtual interface on the gateway.

Subnet Mask:
Subnet mask of the VLAN virtual interface.

NAT Domain:
NAT addressing domain to define the NAPT operation of the VLAN virtual interface. Public means that this VLAN will be visible to the Internet. Private means NAT is enabled to protect the subnet from visibility to the Internet.

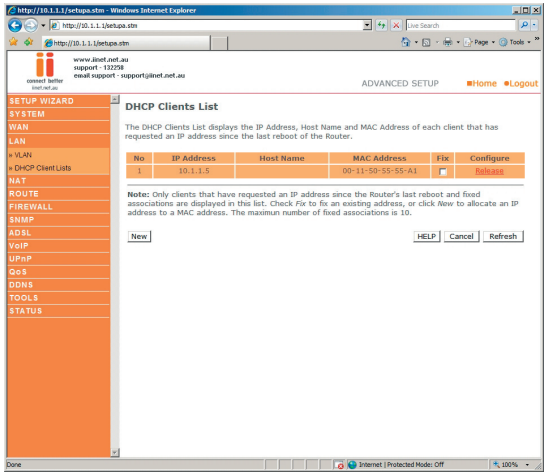
IGMP Snooping:
Enable/disable the feature to block unnecessary IP multicast traffic flooding among VLAN ports without the specific multicast membership. This feature is working based on snooping IGMP Join/Leave messages among the VLAN ports to update the bridging forwarding database. IGMP Snooping is extremely useful in saving bandwidth of low-speed interfaces (ex. WLAN) to improve the network utilization.

IGMP Querier:
Enable/disable IGMP querying to the VLAN virtual interface. The option is to control whether to behave as an IGMP querier on the VLAN bridging network. If IGMP Querier option is disabled, the router will act as an IP multicast compliant host and send IGMP reports for its own joined IP multicast groups. No IGMP query messages will be sent to the specific VLAN.

VLAN Access Control:

In this table you can enable or disable the communication between the VLAN bindings by ticking (enable) or un-ticking (disable) the corresponding name in the table.

DHCP Client List



The DHCP Clients List displays the IP Address, Host Name and MAC Address of each client that has requested an IP address since the last reboot of the Router. Check the FIX box to have the IP address and the MAC address linked so that the IP address will always be assigned as it is on this screen.

Wireless

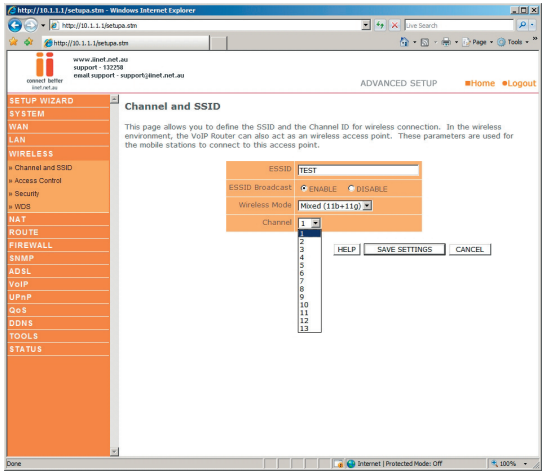
The VoIP Router also operates as a wireless access point, allowing wireless computers to communicate with each other. To configure this function, you need to enable the wireless function, and you may also setup the security options if needed.

Wireless Settings

Check Enable or Disable and click “SAVE SETTINGS”. This will turn the wireless function on or off and enable or disable wireless clients to connect to the modem.

Channel and SSID

These settings should be left as default unless you have a reason to change them. You can change the Service Set ID (SSID) and a common radio channel to be used by the VoIP Router and all of its wireless clients. Be sure you configure all of its clients to the same values. The SSID is case-sensitive and can consist of up to 32 alphanumeric characters. Functioning as an access point, the Gateway can be configured for roaming clients by setting the SSID and wireless channel.



See the description of the parameters below.

Parameter Description

SSID: Service Set ID. The SSID must be the same on the VoIP Router and all of its wireless clients. The SSID is the name of your wireless.

Note: The SSID is **case sensitive** and can consist of up to 32 alphanumeric characters. (Default: WLAN)

SSID Broadcast: Enable or disable the broadcasting of the SSID. Enable SSID broadcasting on the wireless network for easy connection with client PCs. (Default: Enable)

Wireless Mode: This device supports both 11g and 11b wireless networks. Make your selection depending on the type of wireless network that you have. (Default: Mixed mode 11b+11g)

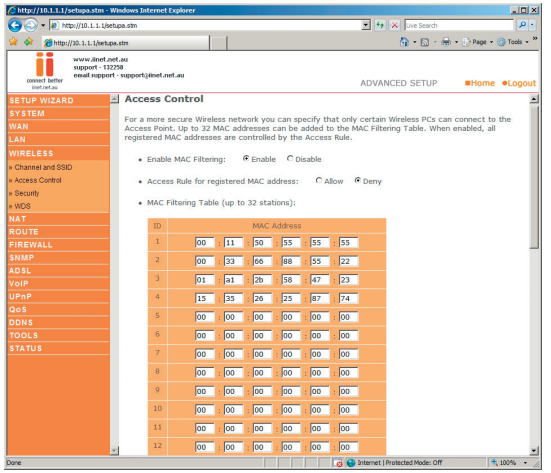
Channel: The radio channel used by the wireless router and its clients to communicate with each other. This channel must be the same on the VoIP Router and all of its wireless clients. (Default: 6)

Note: If you experience poor performance, you may be encountering interference from another wireless device. Try changing the channel, as this may eliminate interference and increase performance.

Channels 1, 6, and 11, as the three non-overlapping channels in the 2.4GHz range, are preferred. The available channel settings are limited by local regulations. (Default Range: 1-13)

Access Control

Using the Access Control functionality, you can specify which PCs can wirelessly connect to the access point. Each PC has a unique identifier known as a Medium Access Control (MAC) address. With MAC filtering enabled, only the computers whose MAC address you have listed in the filtering table may connect to the VoIP Router.



See the description of the Access Control features below.

Parameter Description

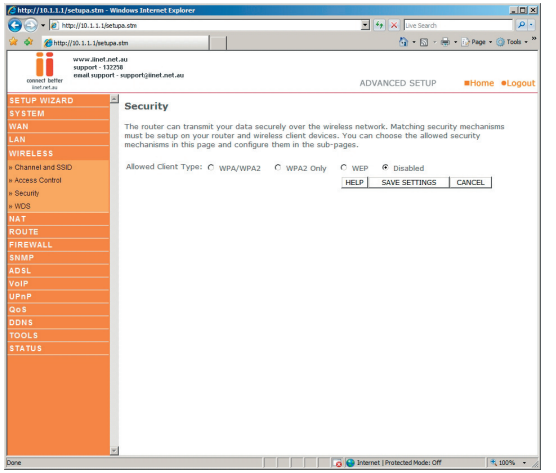
Enable MAC Filtering: Enable or disable the MAC filtering function.

Access Rule for registered MAC address: When MAC filtering is enabled, all registered MAC addresses are controlled by this Access Rule.

MAC Filtering Table: Enter the MAC addresses of the network card you wish to allow or deny connection. (Up to 32 stations)

Security

It is important to be aware of security issues, especially when using wireless. You can configure your security settings on this page. Do not change settings if are not sure what they are for, default settings are normally fine.



If you are transmitting sensitive data across radio channels, you should enable wireless security.

For a more secure network, the VoIP Router can implement one or a combination of the following security mechanisms:

- Disabled
- WEP Only
- WPA and/or WPA2
- WPA and 802.1x *

* Using 802.1x security requires support to do so from your OS or other third party radius server software, and is not recommended unless you are familiar with setting up such systems.

Security client support implementation considerations

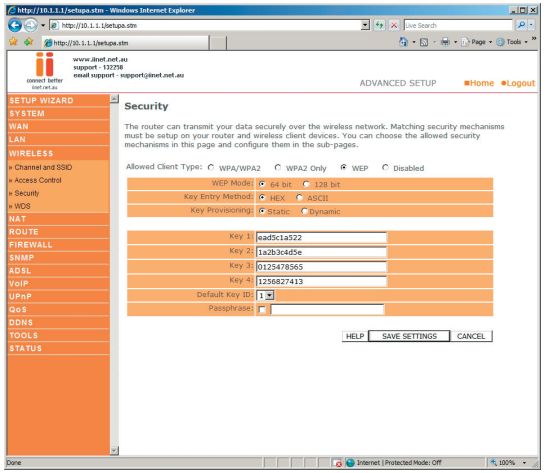
WEP: Built-in support on all 802.11b and 802.11g devices

WPA: Requires WPA enabled system and network card driver (New security which might not be supported by most wireless network cards)

WPA2: Requires WPA2 enabled system and network card driver (New security which might not be supported by most wireless network cards)

WEP

Wired Equivalent Privacy (WEP) encryption requires you to use the same set of encryption/decryption keys for the router and all of your wireless clients.



See the description of the Security features below.

Parameter Description

WEP Mode: You can choose 64-bit or 128-bit encryption. (Default: 64Bit)

Key Entry Method: You can choose HEX or ASCII (Default/ Recommended: HEX)

Key Provisioning: Select static key or dynamic key. (Default/ Recommended: Static)

Static WEP Key: You may manually enter the keys or automatically generate

Settings: Encryption keys. To manually configure the keys, enter 10 digits for each 64-bit key, or enter 26 digits for the single 128-bit key. (A hexadecimal digit is a number or letter in the range 0-9 or A-F.)

Default Key ID: Select the default key. (Default/Recommended: 1)

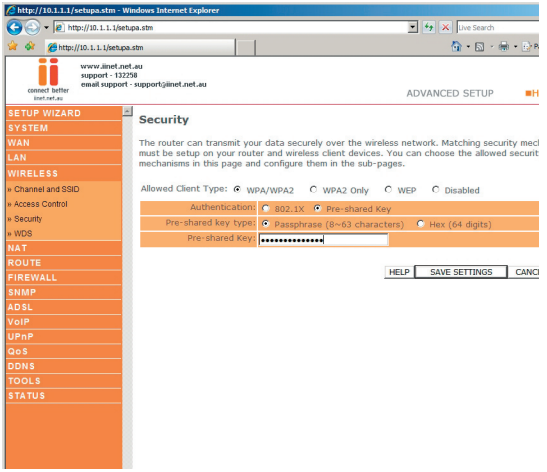
Passphrase: For automatic key generation, check the Passphrase box, enter a Passphrase and click “SAVE SETTINGS”. When you return to this screen the Passphrase will be gone and the single 128Bit or the 4 64Bit keys will be generated.

Key 1-4: If you do not choose to use the Passphrase for automatic key generation, you must manually enter four keys. For 64-bit encryption, enter exactly 10 hex digits. For 128-bit encryption, enter exactly 26 hex digits. (A hex digit is a number or letter in the range 0-9 or A-F.)

Click “SAVE SETTINGS” to apply your settings.

WPA / WPA2

Wi-Fi Protected Access (WPA) combines Temporal Key Integrity Protocol (TKIP) and 802.1x mechanisms. It provides dynamic key encryption and 802.1x authentication service. With TKIP, WPA uses 48-bit initialization vectors, calculates an 8-byte message integrity code, and generates an encryption key periodically. For authentication, it allows you to use 802.1x authentication for an environment with a RADIUS server installed on your network. Selecting the Pre-shared Key enables WPA to use the pre-shared key in a SOHO network.



See the description of the WPA settings below.

Field Default Parameter Description

Cipher suite TKIP One of the security mechanisms used by WPA for frame body and CRC frame encryption.

Authentication:

- 802.1x: It is for an enterprise network with a RADIUS server installed.
- Pre-shared Key: It is for a SOHO network without any authentication server installed.

Pre-shared key type:

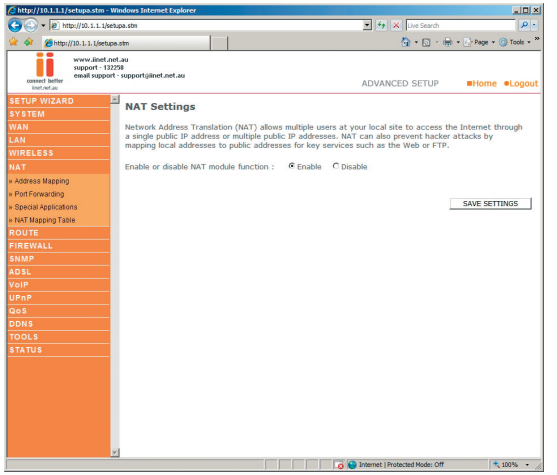
- **Passphrase:** Input 8~63 characters.
- **Hex:** Input 64 hexadecimal digits. (A hexadecimal digit is a number or letter in the range 0-9 or A-F.)

Pre-shared Key: Specify in Passphrase style or in 64-Hex characters.

Group Key Re-Keying: The period of renewing broadcast/multicast keys.

NAT

From this section you can configure the Virtual Server, and Special Application features that provide control over the TCP/ UDP port openings in the router's firewall. This section can be used to support several Internet based applications such as web, email, FTP, and Telnet.

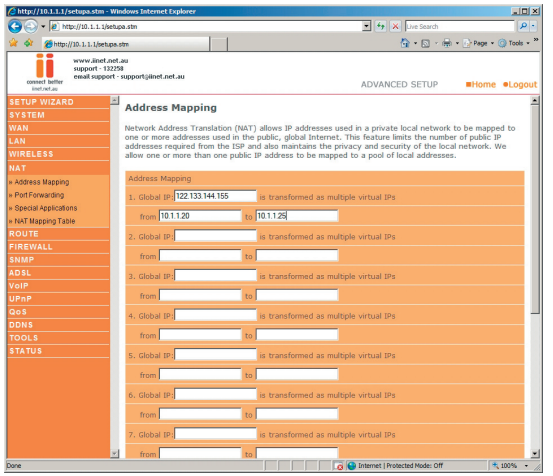


NAT Settings

NAT allows one or more public IP addresses to be shared by multiple internal users. Enter the Public IP address you wish to share into the Global IP field. Enter a range of internal IPs that will share the global IP.

Enable or disable NAT module function: Enable or disable the function and then click "SAVE SETTINGS" to apply the change.

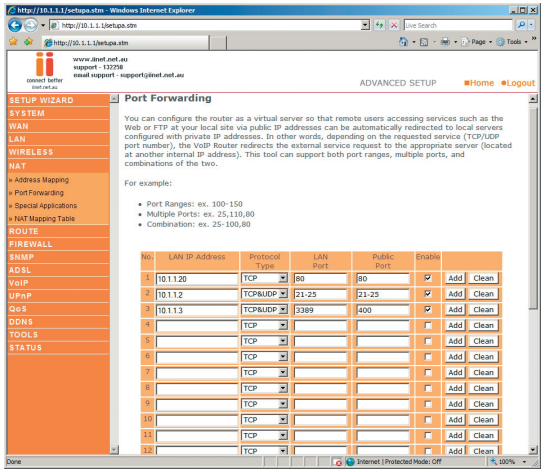
Address Mapping



Use Address Mapping to allow a limited number of public IP addresses to be translated into multiple private IP addresses for use on the internal LAN network. This also hides the internal network for increased privacy and security.

Advanced Setup Method

Port Forwarding



Using this feature, you can put PCs with public IPs and PCs with private IPs in the same LAN area.

If you configure the Port Forwarding settings, remote users accessing services such as web or FTP at your local site via public IP addresses can be automatically redirected to local servers configured with private IP addresses. In other words, depending on the requested service (TCP/UDP port number), the VoIP Router redirects the external service request to the appropriate server (located at another internal IP address).

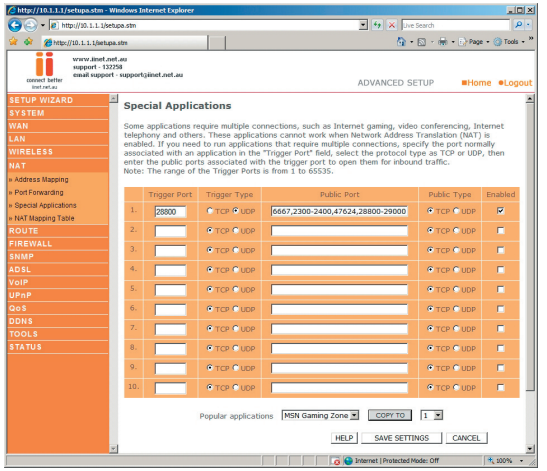
For example, if you set Type/Public Port to TCP/80 (HTTP or web) and the LAN IP Address/LAN Port to 10.1.1.2/80, then all HTTP requests from outside users will be transferred to 10.1.1.2 on port 80. Therefore, by just entering the IP address provided by the ISP, Internet users can access the service they need at the local address to which you redirect them.

The more common TCP service ports include:

HTTP: 80, FTP: 21, Telnet: 23, and POP3: 110.

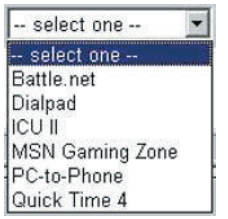
Special Applications

Some applications, such as Internet gaming, video conferencing, Internet telephony and others, require multiple connections. These applications cannot work with Network Address Translation (NAT) enabled. If you need to run applications that require multiple connections, use the following screen to specify the additional public ports to be opened for each application.



Specify the public port number normally associated with an application in the Trigger Port field. Set the protocol type to TCP or UDP, and then enter the ports that the application requires. The ports may be in the format 7, 11, 57, or in a range, e.g., 72-96, or a combination of both, e.g. 7, 11, 57, 72-96.

Popular applications requiring multiple ports are listed in the Popular Applications field. From the drop-down list, choose the application and then choose a row number to copy this data into.



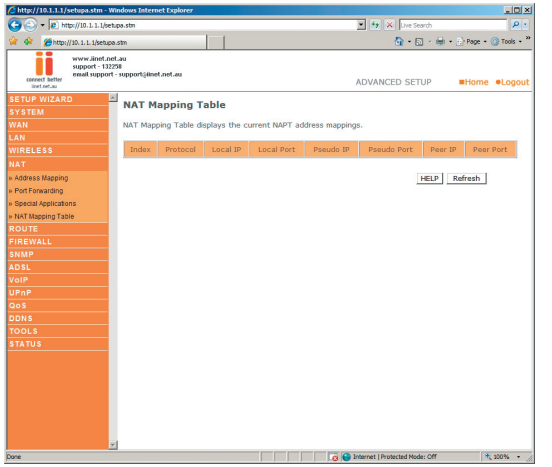
Note: Choosing a row that already contains data will overwrite the current settings.

Example:

ID	Trigger	Trigger Port	Public Type	Public Port	Comment Type
1	6112	UDP	6112	UDP	Battle.net
2	28800	TCP	2300-2400	TCP	MSN Game Zone

For a full list of ports and the services that run on them, see www.iana.org/assignments/port-numbers.

NAT Mapping Table



NAT Mapping Table displays the current NAPT address mappings. The NAT address mappings are listed 20 lines per page, click the control buttons to move forwards and backwards. As the NAT mapping is dynamic, a Refresh button is provided to refresh the NAT Mapping Table with the most up-to-date values.

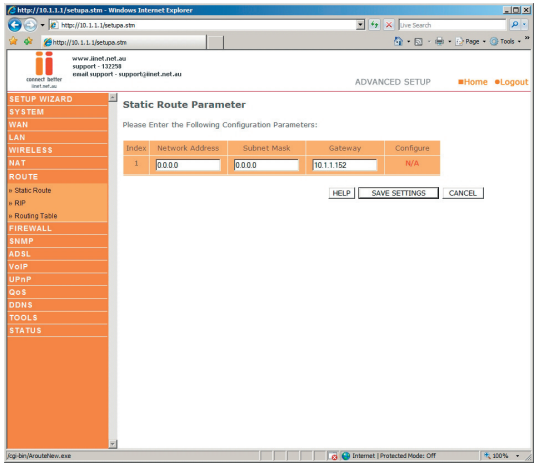
The content of the NAT Mapping Table is described as follows:

- Protocol - protocol of the flow.
- Local IP - local (LAN) host's IP address for the flow.
- Local Port - local (LAN) host's port number for the flow.
- Pseudo IP - translated IP address for the flow.
- Pseudo Port - translated port number for the flow.
- Peer IP - remote (WAN) host's IP address for the flow.
- Peer Port - remote (WAN) host's port number for the flow.

Route

These pages define routing related parameters, including static routes and Routing Information Protocol (RIP) parameters.

Static Route Parameters



Parameter Description

Index: Displays the number of the route.

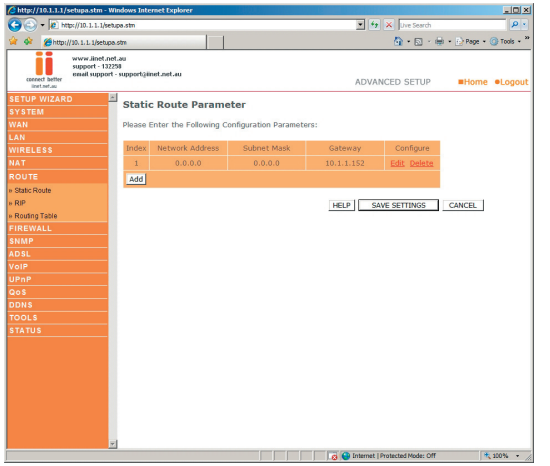
Network Address: Displays the IP address of the remote computer for which to set a static route.

Subnet Mask: Displays the subnet mask of the remote network for which to set a static route.

Gateway: Displays the WAN IP address of the gateway to the remote network.

Configure: Allows you to modify or delete configuration settings.

Click Add or Edit to display the following page and add a new static route to the list.



Parameter Description

Index: Displays the number of the route.

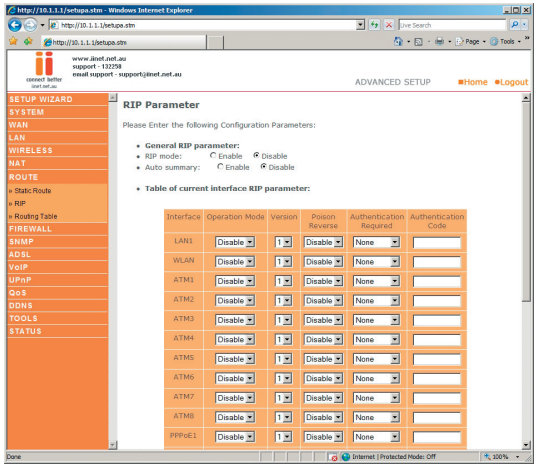
Network Address: Enter the IP address of the remote computer for which to set a static route.

Subnet Mask: Enter the subnet mask of the remote network for which to set a static route.

Gateway: Enter the WAN IP address of the gateway to the remote network.

RIP Parameter

The device supports RIP v1 and v2 to dynamically exchange routing information with adjacent routers.



Parameter Description

General RIP Parameters

RIP mode: Globally enables or disables RIP.

Auto summary: If Auto summary is disabled, then RIP packets will include sub-network information from all sub-net works connected to the ADSL Router. If enabled, this sub-network information will be summarized to one piece of information covering all sub-networks.

Table of current Interface RIP parameter:

Interface: The WAN interface to be configured.

Operation Mode:

Disable: RIP disabled on this interface.

Enable: RIP enabled on this interface.

Silent: Listens for route broadcasts and updates its route table. It does not participate in sending route broadcasts.

Version: Sets the RIP version to use on this interface.

Poison Reverse: A method for preventing loops that would cause endless retransmission of data traffic.

Authentication Required: None, No authentication.

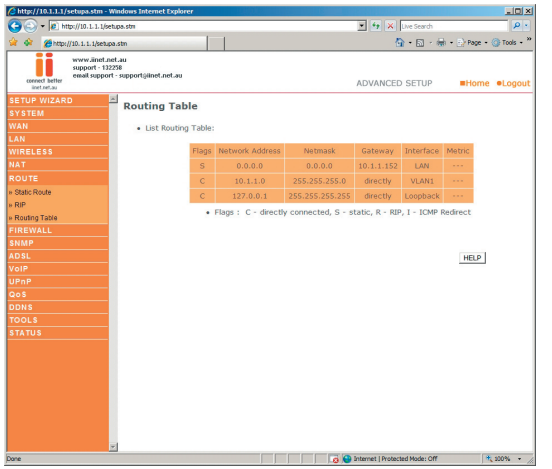
Password: A password authentication key is included in the packet. If this does not match what is expected, the packet will be discarded. This method provides very little security as it is possible to learn the authentication key by watching RIP packets.

MD5: An algorithm that is used to verify data integrity through the creation of a 128-bitmessage digest from data input (which may be a message of any length) that is claimed to be as unique to that specific data as a fingerprint is to a specific individual.

Authentication Code: Password or MD5 Authentication key.

RIP sends routing-update messages at regular intervals and when the network topology changes. When a router receives a routing update that includes changes to an entry, it updates its routing table to reflect the new route. RIP routers maintain only the best route to a destination. After updating its routing table, the router immediately begins transmitting routing updates to inform other network routers of the change.

Routing Table



Parameter Description

Flags: Indicates the route status:

C = Direct connection on the same subnet.
S = Static route.
R = RIP (Routing Information Protocol) assigned route.
I = ICMP (Internet Control Message Protocol) Redirect route.

Network Address: Destination IP address.

Netmask: The subnetwork associated with the destination.

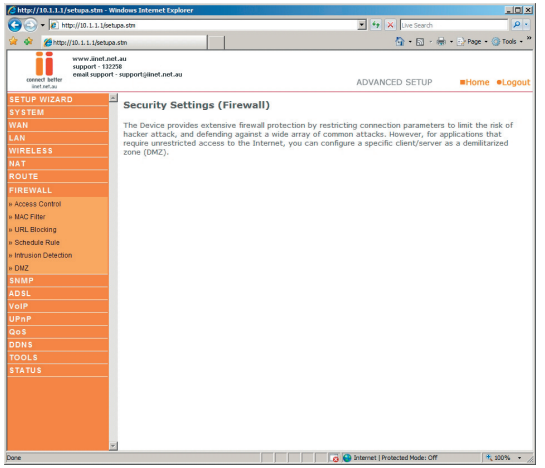
This is a template that identifies the address bits in the destination address used for routing to specific subnets. Each bit that corresponds to a "1" is part of the subnet mask number; each bit that corresponds to "0" is part of the host number.

Gateway: The IP address of the router at the next hop to which frames are forwarded.

Interface: The local interface through which the next hop of this route is reached.

Metric: When a router receives a routing update that contains a new or changed destination network entry, the router adds 1 to the metric value indicated in the update and enters the network in the routing table.

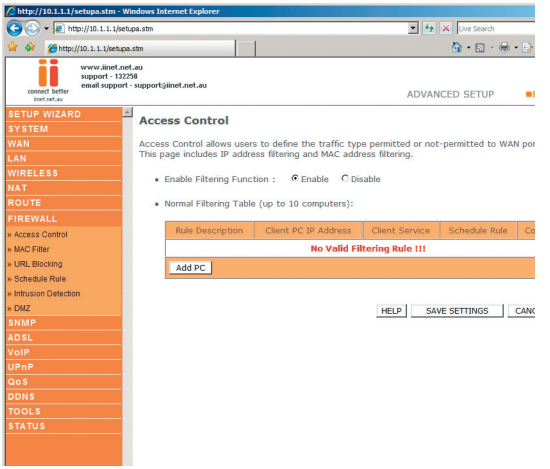
Firewall



The VoIP Router's firewall enables access control of client PCs, blocks common hacker attacks, including IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan, and TCP SYN flooding. The firewall does not significantly affect system performance and we advise leaving it enabled to protect your network.

Note: After you check the radio button in the "Enable or disable Firewall features" field, you must click the "SAVE SETTINGS" button to display the list of firewall features.

Access Control



Access Control allows users to define the outgoing traffic permitted or not-permitted through the WAN interface. In the example above, all incoming and outgoing emails are blocked. The default is to permit all outgoing traffic. (See the following page for details.)

The VoIP Router can also limit the access of hosts within the local area network (LAN). The MAC Filtering Table allows the VoIP Router to enter up to 32 MAC addresses that are not allowed access to the WAN port.

The following items are displayed on the Access Control screen:

Parameter Description

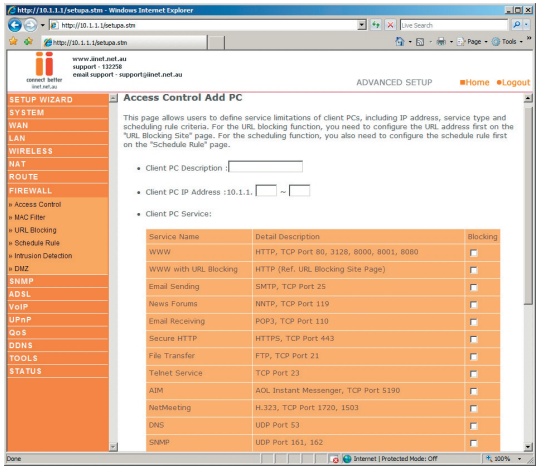
Enable Filtering: Enables or disables the filtering function.

Normal Filtering Table: Displays the IP address (or an IP address range) filtering table.

Click Add PC on the Access Control screen to view the following page.

Access Control Add PC

The settings in the screen shot below will block all email sending and receiving.

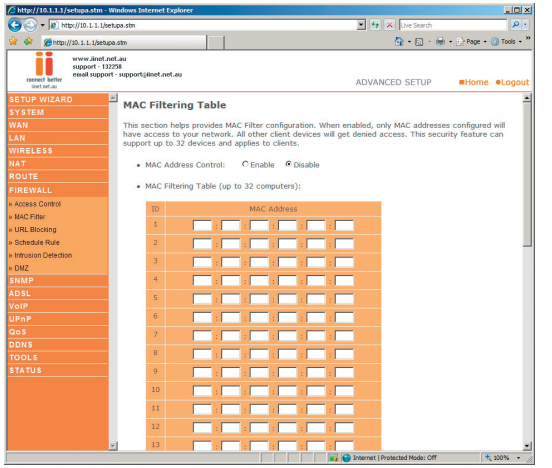


Define the appropriate settings for client PC services (as shown above). Click “OK” to save your settings. The added PC will now appear in the Access Control page.

MAC Filter

Use this page to block access to your network using MAC addresses.

Advanced Setup Method



The VoIP Router can also limit the access of hosts within the local area network (LAN). The MAC Filtering Table allows the VoIP Router to enter up to 32 MAC addresses that are allowed access to the WAN port. All other devices will be denied access.

URL Blocking

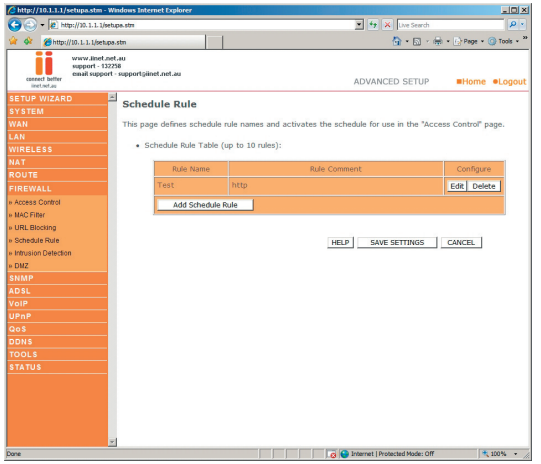
To configure the URL Blocking feature, use the table below to specify the web sites (www.somesite.com) and/or keywords you want to filter on your network.

To complete this configuration, you will need to create or modify an access rule in “Access Control”. To modify an existing rule, click the Edit option next to the rule you want to modify. To create a new rule, click on the Add PC option.

From the Access Control Page, Add PC section, check the option for “WWW with URL Blocking” in the Client PC Service table to filter out the web sites and keywords selected below, on a specific PC.

The VoIP Router allows the user to block access to web sites from a particular PC by entering either a full URL address or just a keyword. This feature can be used to protect children from accessing violent or pornographic web sites.

Schedule Rule



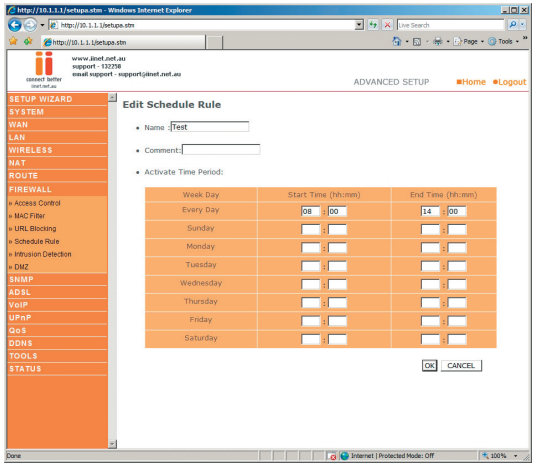
You may filter Internet access for local clients based on rules.

Each access control rule may be activated at a scheduled time. Define the schedule on the Schedule Rule page, and apply the rule on the Access Control page.

Click Add Schedule Rule to add a new rule and bring up the following page.

Edit Schedule Rule

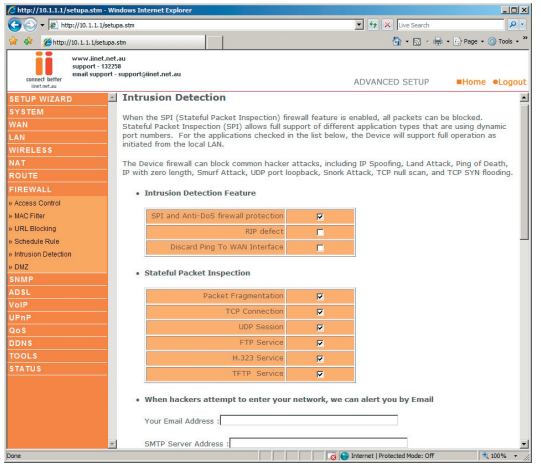
You can create and edit schedule rules on this page.



Define the appropriate settings for a schedule rule (as shown on the above screen).

Intrusion Detection

The VoIP Router's firewall inspects packets at the application layer, maintains TCP and UDP session information including timeouts and number of active sessions, and provides the ability to detect and prevent certain types of network attacks such as Denial-of-Service (DoS) attacks.



Network attacks that deny access to a network device are called DoS attacks. DoS attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources.

The VoIP Router protects against DoS attacks including: Ping of Death (Ping flood) attack, SYN flood attack, IP fragment attack (Teardrop Attack), Brute-force attack, Land Attack, IP Spoofing attack, IP with zero length, TCP null scan (Port Scan Attack), UDP port loopback, Snork Attack.

Note: The firewall does not significantly affect system performance, so we advise enabling the prevention features to protect your network.

Parameter Description

Enable SPI and Anti-DoS firewall protection:

The Intrusion Detection feature of the VoIP Router limits the access of incoming traffic at the WAN port. When the Stateful Packet Inspection (SPI) feature is turned on, all incoming packets are blocked except those types marked with a check in the Stateful Packet Inspection section at the top of the screen.

Stateful Packet Inspection:

This option allows you to select different application types that are using dynamic port numbers. If you wish to use Stateful Packet Inspection (SPI) for blocking packets, click on the Yes radio button in the “Enable SPI and Anti-DoS firewall protection” field and then check the inspection type that you need, such as Packet Fragmentation, TCP Connection, UDP Session, FTP Service, H.323 Service, and TFTP Service.

It is called a “stateful” packet inspection because it examines the contents of the packet to determine the state of the communication; i.e. it ensures that the stated destination computer has previously requested the current communication. This is a way of ensuring that all communications are initiated by the recipient computer and are taking place only with sources that are known and trusted from previous interactions. In addition to being more rigorous in their inspection of packets, stateful inspection firewalls also close off ports until a connection to the specific port is requested.

When particular types of traffic are checked, only the particular type of traffic initiated from the internal LAN will be allowed. For example, if the user only checks FTP Service in the Stateful Packet Inspection section, all incoming traffic will be blocked except for FTP connections initiated from the local LAN.

DoS Detect Criteria

Total incomplete TCP/UDP sessions HIGH:
Defines the rate of new un-established sessions that will cause the software to start deleting half-open sessions.

Total incomplete TCP/UDP sessions LOW:
Defines the rate of new un-established sessions that will cause the software to stop deleting half-open sessions.

Incomplete TCP/UDP sessions (per min.) HIGH:
Maximum number of allowed incomplete TCP/UDP sessions per minute.

Incomplete TCP/UDP sessions (per min.) LOW:
Minimum number of allowed incomplete TCP/UDP sessions per minute.

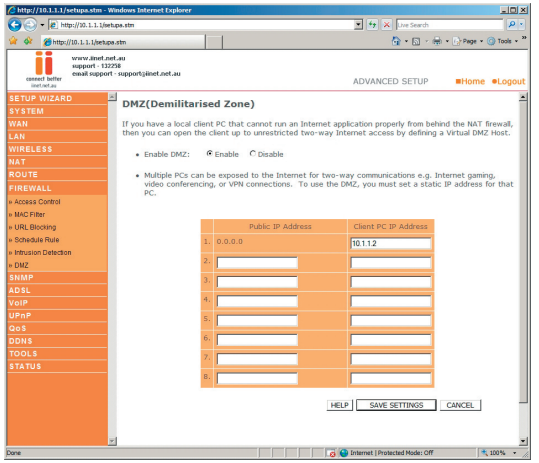
Maximum incomplete TCP/UDP sessions number from same host:
Maximum half-open fragmentation packet number from same host

Incomplete TCP/UDP sessions detect sensitive time period:
Length of time before an incomplete TCP/UDP session is detected as incomplete.

Maximum half-open fragmentation packet number from same host:
Maximum number of incomplete TCP/UDP sessions from the same host.

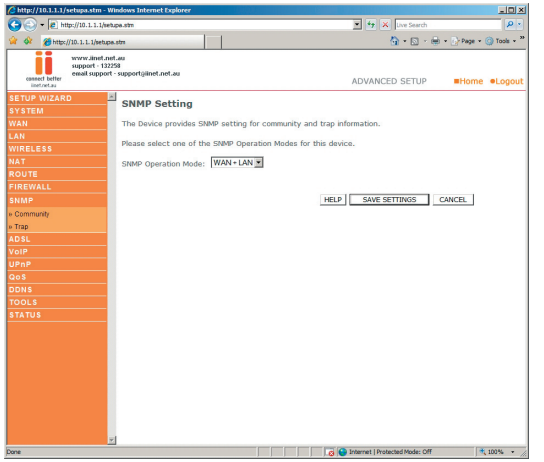
Half-open fragmentation detect sensitive time period:
Length of time before a half-open fragmentation session is detected as half-open.

DMZ



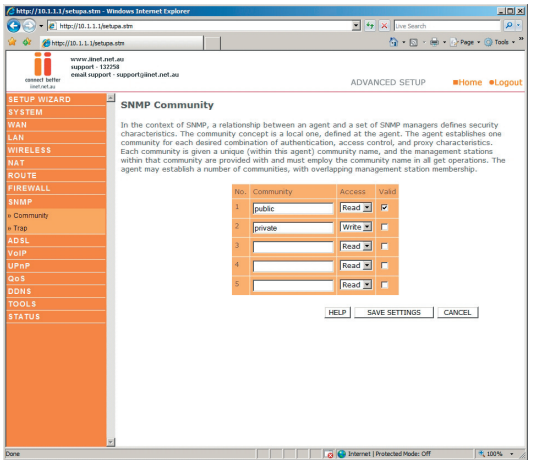
If you have a client PC that cannot run an Internet application properly from behind the firewall, you can open the client up to unrestricted two-way Internet access. Enter the IP address of a DMZ (Demilitarized Zone) host on this screen. Adding a client to the DMZ may expose your local network to a variety of security risks, so only use this option as a last resort.

SNMP



On this page you can enable the SNMP (Simple Network Management Protocol) functions for LAN, WAN or both LAN and WAN. By default it is set to disabled.

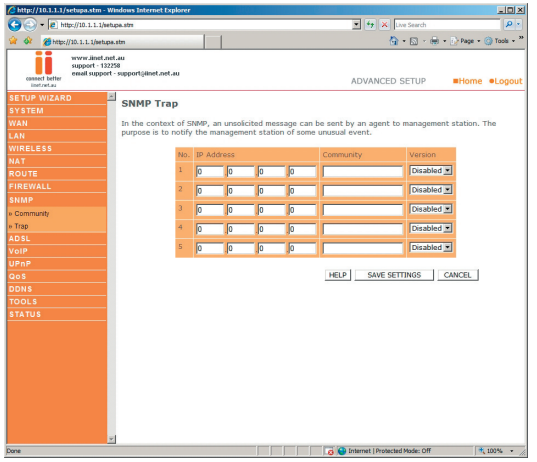
Community



Use the SNMP configuration screen to display and modify parameters for the Simple Network Management Protocol (SNMP). A computer attached to the network, called a Network Management Station (NMS), can be used to access this information. Access rights to the agent are controlled by community strings. To communicate with the VoIP Router, the NMS must first submit a valid community string for authentication.

Parameter	Description
Community	A community name authorized for management access.
Access	Management access is restricted to Read or Write.
Valid	Enables or disables the entry.
	Note: Up to 5 community names may be entered.

Trap



Parameter Description

IP Address: Traps are sent to this address when errors or specific events occur on the network.

Community: A community string (password) specified for trap management. Enter a word, something other than public or private,

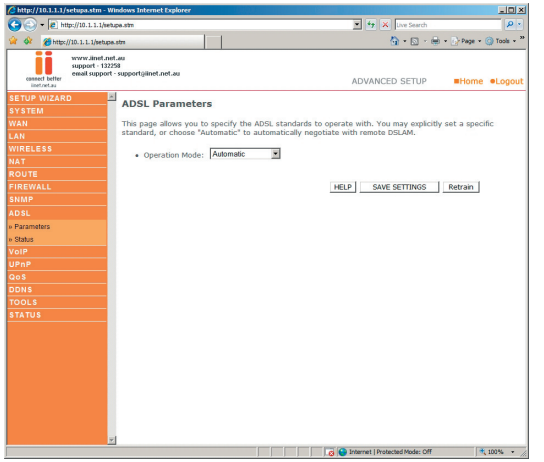
to prevent unauthorized individuals from reading information on your system.

Version: Sets the trap status to disabled, or enabled with V1 or V2c.

The v2c protocol was proposed in late 1995 and includes enhancements to v1 that are universally accepted. These include a get-bulk command to reduce network management traffic when retrieving a sequence of MIB variables, and a more elaborate set of error codes for improved reporting to a Network Management Station.

ADSL

ADSL Parameters



We recommend leaving the Operation Mode at the default Automatic setting unless having line sync issues, to automatically negotiate with remote DSLAM.

Parameter Description

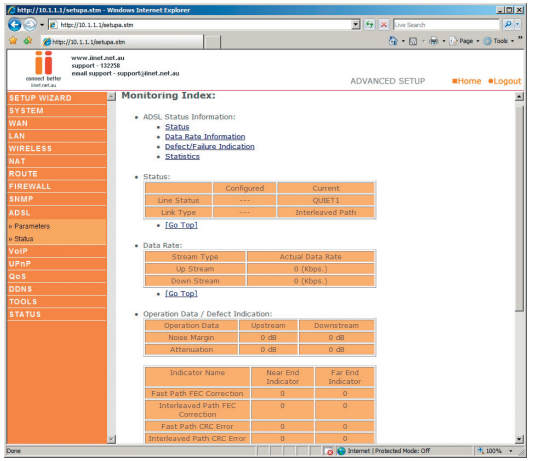
Operation Mode

- Automatic
- T1.413 Issue 2
- G.992.1 (G.DMT)

- G.922.2 (G.Lite)
- G.922.3 (ADSL2)
- G.922.5 (ADSL2+)

Status

The Status page displays ADSL status information.



Parameter Description

Status

Line Status: Shows the current status of the ADSL line.

Data Rate

Upstream: Actual and maximum upstream data rate.

Downstream: Actual and maximum downstream data rate.

Operation Data/Defect Indication:

Noise Margin Upstream: Minimum noise margin upstream.

Downstream: Minimum noise margin downstream.

Output Power: Maximum fluctuation in the output power.

Attenuation Upstream: Maximum reduction in the strength of the upstream signal.

Attenuation Downstream: Maximum reduction in the strength of the downstream signal.

There are two latency paths that may be used: fast and Correction interleaved. For either path a forward error correction (FEC) scheme is employed to ensure higher data integrity. For maximum noise immunity, an interleaver may be used to supplement FEC. Interleaved Path An interleaver is basically a buffer used to introduce a delay, FEC Correction allowing for additional error correction techniques to handle noise. Interleaving slows the data flow and may not be optimal for real-time signals such as video transmission.

Fast Path CRC indicates the number of Fast Path Cyclic Redundancy Check Error errors. Interleaved Path indicates the number of Interleaved Path Cyclic Redundancy Error Check errors.

Loss of Signal Momentary signal discontinuities. Defect Loss of Frame Failures due to loss of frames.

Loss of Power Defect: Failures due to loss of power.

Fast Path HEC Error: Fast Path Header Error Concealment errors.

Interleaved Path HEC Error: Interleaved Path Header Error Concealment errors.

Statistics: (Superframes represent the highest level of data presentation. Each superframe contains regular ADSL frames, one of which is used to provide superframe synchronization, identifying the start of a superframe. Some of the remaining frames are also used for special functions.)

Received Cells: Number of interleaved superframes received Interleaved

Transmitted Cells: Number of interleaved super frames transmitted. Superframes Interleaved

Received Number of fast super frames received.
Superframes Fast

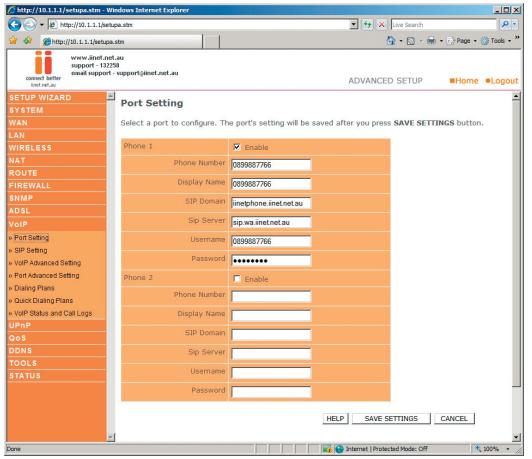
Transmitted Number of fast super frames transmitted.
Superframes Fast

VoIP

Note: It is advised to leave all default settings unless instructed otherwise.

Port Setting

Configure the port settings on this page, and click “SAVE SETTINGS” to save the parameters. VoIP providers operate SIP proxies that allow you to register your VoIP Router on their system so that your can call friends, family and business associates. Your Belkin/iiNet modem comes pre-configured for the iiNet VoIP service. iiNet and Belkin will only provide support for use with the iiNet VoIP service.



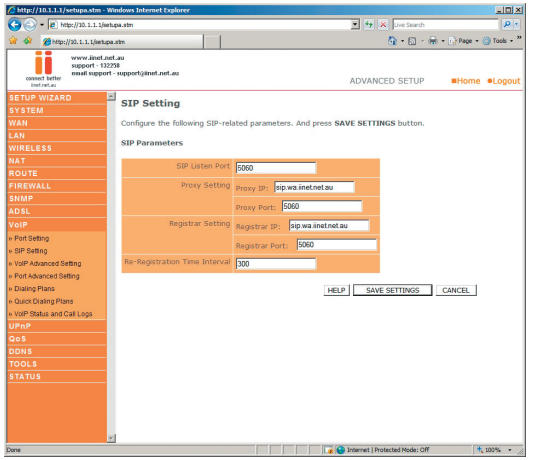
See the table below for a description of the parameters.

Parameter Description

Phone 1/2 Enable: Enable/disable phone 1 and/or 2.
Phone Number: Your phone number.
Display Name: Your name, often the same as your phone number.
SIP Domain: (From your VoIP provider.)
Sip Server: (From your VoIP provider.)
Username: (From your VoIP provider.)
Password: (From your VoIP provider.)

SIP Setting

Configure your SIP parameters on this page, and click “SAVE SETTINGS” to apply them.



SIP, the Session Initiation Protocol, is a signaling protocol for Internet conferencing, telephony, presence, events notification and instant messaging. The call waiting feature allows the user to take an incoming call, even though the user is already on the phone. The user upon hearing the new call can put the original caller on hold and speak to the new caller. When the user hasn’t finished talking to the new caller, he can resume his conversation with the original caller. According to the SIP RFC, a proxy server is “An intermediary entity that acts as both a server and a client for the purpose of making requests on behalf of other clients. A proxy server primarily plays the role of routing, which means its job is to ensure that request is sent to another entity ‘closer’ to the targeted user”.
The proxy server therefore, is an intermediate device that receives SIP requests from a client and then forwards the requests on the client’s behalf. Proxy servers receive SIP messages and forward them to the next SIP server in the network. A series of proxy and redirect servers receive requests from a client and decide where to send these requests. Proxy servers can provide functions such as authentication, authorization, network access control, routing, reliable request retransmission, and security.

From the SIP RFC, “A registrar is a server that accepts REGISTER requests and places the information it receives in those requests into the location service for the domain it handles.”

See the table below for a description of the parameters.

Parameter Description

SIP Listen Port: It is strongly recommended that you to leave the SIP port unchanged (Default: 5060).

Proxy Setting set the proxy settings.

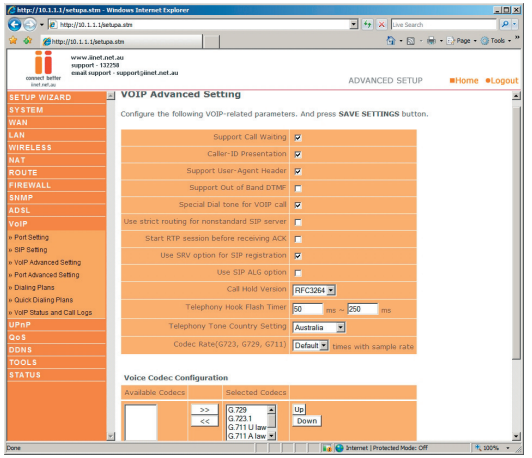
- Proxy IP: IP address of your proxy server. (From your VoIP provider.)
- Proxy Port: Port number of the proxy server. (From your VoIP provider.)

Registrar Setting set the registrar settings.

- Registrar IP: IP address of SIP registrar.
- Registrar Port: Port number of SIP registrar.

VoIP Advanced Setting

Configure the VoIP advanced settings on this page, and click “SAVE SETTINGS”.



SIP is a peer-to-peer protocol. The peers in a session are called User Agents (UAs). A user agent can function in one of the following roles:

1. User agent client (UAC) - A client application that initiates the SIP request.
2. User agent server (UAS) - A server application that contacts the user when a SIP request is received and that returns a response on behalf of the user.

Typically, a SIP end point is capable of functioning as both a UAC and a UAS, but functions only as one or the other per transaction.

Phone standards vary internationally and from provider to provider, so it is important that the VoIP router is configured correctly for your provider.

Codecs are used to convert an analog voice signal to digitally encoded version. Codecs vary in the sound quality, the bandwidth required, the computational requirements, etc. You can specify which audio coding process you would like to use. There are four voice codecs supported by the VoIP router, you may try different settings to determine the best audio quality you obtain from the combination of your network connection and your used audio device (head set or hand set). The default codec sequence is listed below. You can use the Up and Down buttons to change priority.

1. G.729
2. G.723.1
3. G.711 U law
4. G.711 A law

See the below for a description of the parameters.

Parameter Description

Support Call Waiting: Enables or disables support for call waiting. (Default: Disabled)

Support User-Agent Header: Enables or disables user-agent header support. Enabling this feature includes user agent information in the packet, e.g., the caller’s ID may be displayed. (Default: Disabled)

Telephony Hook Flash Timer: The hook flash timer is the length of time before the hook flash indicates a time-out (or call disconnect).

(Default: 50 ~ 250 milliseconds.)

Telephony Tone Country Setting: Select the country.

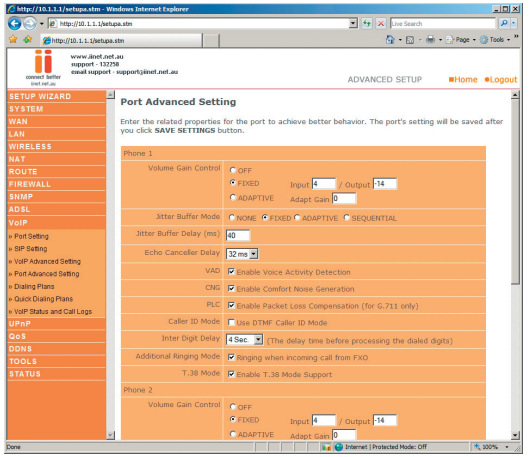
Voice Codec Configuration: Set the voice codecs.

Available Codecs: List of available codecs.

Selected Codecs: List of selected codecs, move the preferred codec to the top of the list with up and down buttons to the right. The codec at the top of the list will be used when it can.

Port Advanced Setting

Configure advanced VoIP settings on this page then click “SAVE SETTINGS”.



Volume Gain Control

Use this option to adjust the volume of calls made through VoIP:

OFF – Standard volume level 0dB.
FIXED – Set the volume to amplify or attenuate at a fixed dB.
ADAPTIVE – The volume will automatically amplify or attenuate according to the current call.

Advanced Setup Method

Jitter Buffer Mode

Jitter Buffer helps eliminate jitter caused by transmission delays on a VoIP call. As the jitter buffer receives the voice packets it adds a small amount of delay to the packets so it appears they were all received without delays.

NONE – Jitter Buffer is disabled
FIXED – Jitter Buffer Mode is fixed
ADAPTIVE – Jitter Buffer Mode will automatically adapt to the current call.
SEQUENTIAL – Jitter Buffer Mode set to Sequential

Jitter Buffer Delay

Specifies the delay in milliseconds for the Jitter Buffer. Default/ recommended is 40ms.

Echo Canceller Delay

Echo cancellation is the process in removing echo from voice communication over the VoIP. It improves the quality of the call and conserves bandwidth.

Default/recommended setting = 32 milliseconds

VAD

Voice Activation Detection. VAD is designed to conserve bandwidth by halting transmission of voice packets until it has detected a noise either by voice or outside noise. The downside to this is it may miss some packets due to a slight delay in the transmission of packets. Disable this if you are experiencing issues with phone system menus, Faxing over IP etc.

Default/recommended = Enabled

CNG

Comfort Noise Generation. As VoIP is digital, there is no background interference like there is on the standard analogue PSTN (Public Switched Telephone Network). This option will generate slight noises in the background to make the digital call sound more like an

analogue call. Disable this if you are experiencing issues with phone system menus, Faxing over IP etc.

Default/recommended = Enabled

PLC

Packet Loss Compensation. PLC is used only when utilising the G.711 codec, the algorithm is designed to compensate for loss packets. Re-transmitting the lost packets is obviously not a viable option with a digital VoIP telephone call.

Default/recommended = Enabled

Caller ID Mode

Use DTMF Caller ID Mode. Enabling this option enables the Dual Tone, Multi-Frequency (touch tone) mode for Caller ID.

Default/recommended = Disabled

Inter Digit Delay

This is the delay time before processing the dialled digits. This will delay the VoIP unit dial the telephone number after the digits have been entered.

Default/recommended = 4 Seconds

Additional Ringing Mode

Enabling this option will force the VoIP telephone to ring when an incoming call is made through via the PSTN number. You will need to have a filtered telephone cable connected to the PSTN Failover.

Default/recommended = Enabled

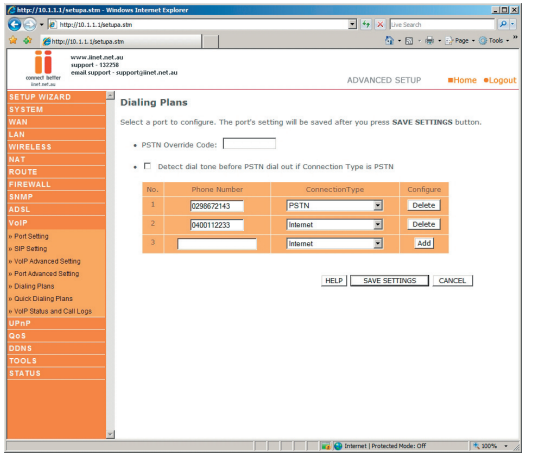
T.38 Mode

T.38 is the standard for sending faxes over IP networks. Enable this option for Faxing over IP.

Default/recommended = Enabled

Dialing Plans

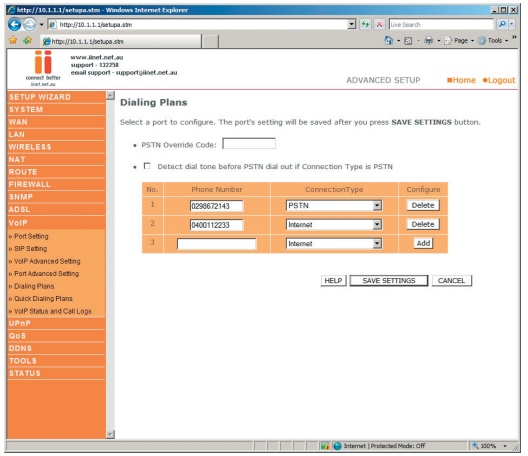
Configure the VoIP dialing plans on this page, and click “SAVE SETTINGS”.



Set the Phone Number and Connection Type on this page.

VoIP Status and Call Logs

View the VoIP status for both FXS ports on this page. Click “Refresh” to update this page.



This page displays the Port Type, SIP URL and Registration status of the VoIP router.

See the table below for a description of the parameters.

Parameter	Description
Port Type	Displays the port type, i.e., FXS.
SIP URL	Shows the SIP URL.
Registration	Indicates whether the user has successfully registered or not.

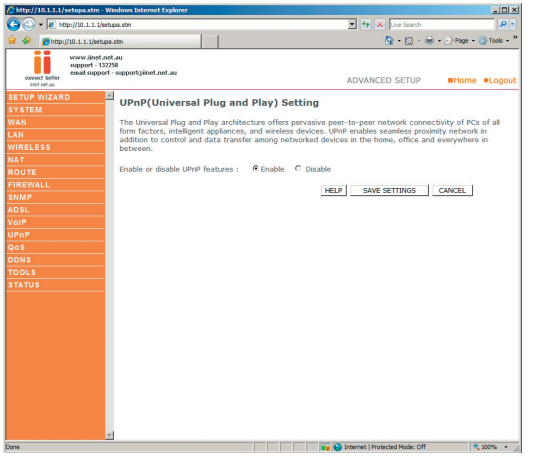
VoIP Call Logs

View the call log for both FXS ports on this page. Click “Refresh” to update the page.

See the table below for a description of the parameters.

Parameter	Description
Port Type	Displays the port type, i.e. FXS.
Received Call	Number of received calls.
Dialed Call	Number of calls made.
Rejected Call	Number of rejected calls.
Forwarded Call	Number of forwarded calls.

UPnP



The Universal Plug and Play architecture offers pervasive peer-to-peer network connectivity of PCs of all form factors, intelligent appliances, and wireless devices. UPnP enables seamless proximity network in addition to control and data transfer among networked devices in the home, office and everywhere in between.

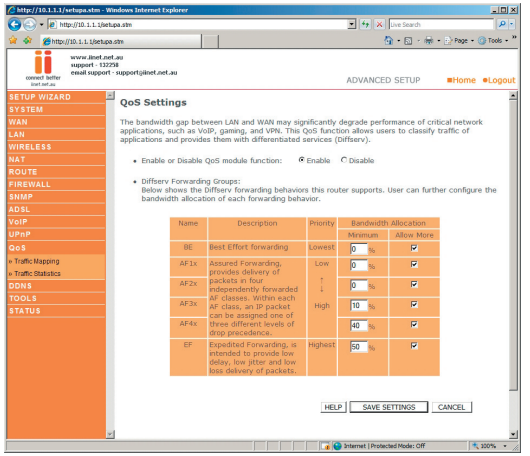
Enable or disable UPnP features: Enable or disable the UPnP function.

QoS

With converging voice and data, it is imperative to establish Quality of Service (QoS) parameters to appropriately allocate bandwidth. QoS will only monitor and limit upstream traffic.

QoS Settings

To ensure optimum voice quality, your VoIP Router should prioritize voice over data packets. Therefore, we recommend enabling the QoS feature.

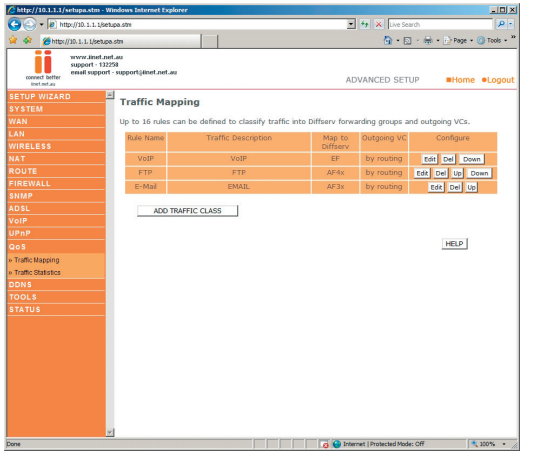


Parameter Description

Enable or disable. QoS module function: Enables or disables QoS

Diffserv Forwarding Groups: You can set the minimum amount of bandwidth you want allocated for certain QOS groups in a Percentage. The different groups allow you to manage your different types of connections more efficiently.

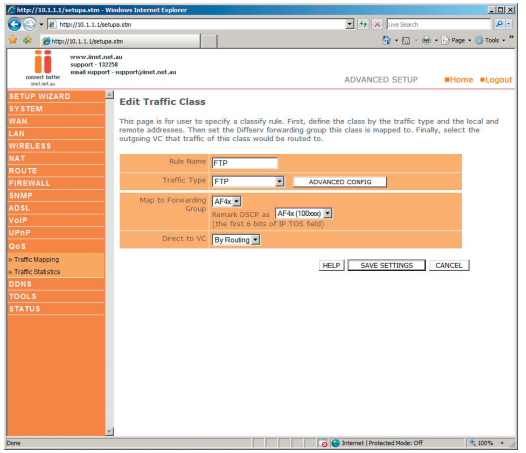
Traffic Mapping



Up to 16 rules can be defined to classify traffic into Diffserv forwarding groups and outgoing VCs.

Click on “Add Traffic Class” or click on “Edit” and a mapping already in the list to bring up the following screen and enter a setting which is to be mapped to a QOS group.

Edit Traffic Class



This page is for user to specify a classify rule.

Rule Name: Assign a Name to the rule.

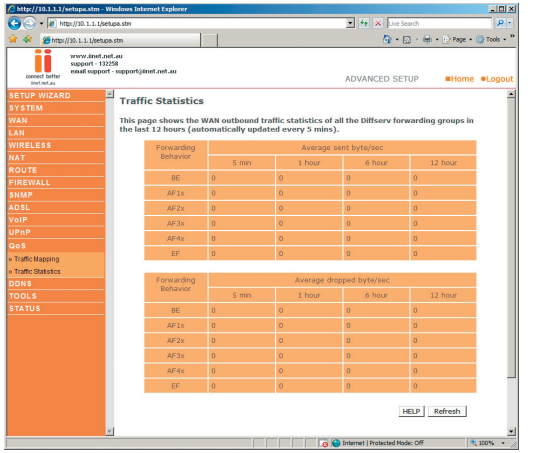
Traffic Type: Choose a Traffic type foe the rule, or click on “Advanced Config” for more advanced options.

Map to Forwarding

Group: Choose which QOS group you wish to have the rule mapped to, which determines how much bandwidth is to be allocated with this rule.

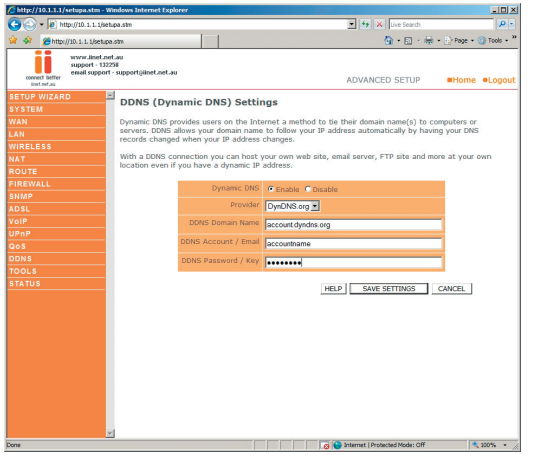
Direct to VC: Choose which ATM connection you wish to have the rule mapped to. The default setting of “By Routing” should be used.

Traffic Statistics



This page shows the WAN outbound traffic statistics of all the Diffserv forwarding groups in the last 12 hours (automatically updated every 5 mins).

DDNS



With a DDNS (Dynamic DNS) connection you can host your own web site, email server, FTP site and more at your own location even if you have a dynamic IP address.

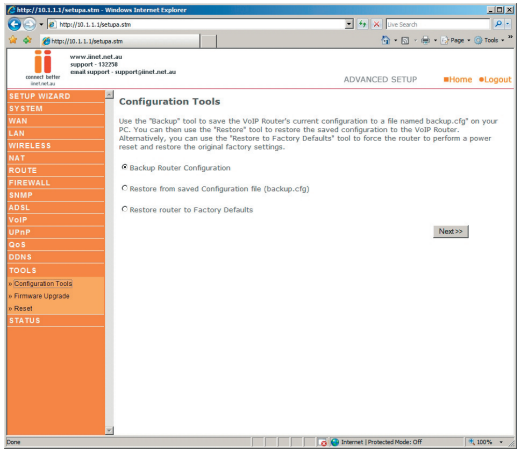
Parameter Description

Dynamic DNS: Enable or disable the DDNS function.
Provider: Select which provider you wish to use for your DDNS service, either DynDNS or TZO.

Tools

Use the Tools menu to back up the current settings, to restore previously saved settings, or to restore the factory default settings.

Configuration Tools



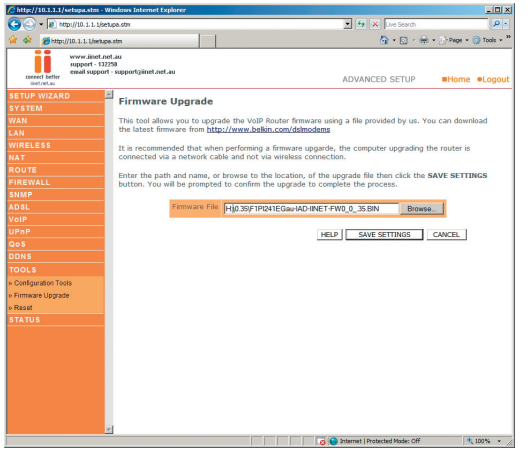
Check Backup Router Configuration and click “NEXT” to save your VoIP Router’s configuration to a file named “backup.cfg” on your PC.

You can then check Restore from saved configuration file (backup.cfg) to restore the saved backup configuration file.

To restore the factory settings, check Restore router to Factory Defaults and click “NEXT.” You will be asked to confirm your decision. Click “APPLY” to proceed, or “CANCEL” to go back.

Firmware Upgrade

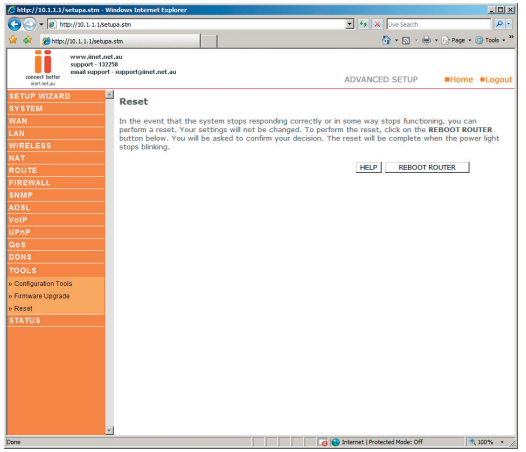
Use this screen to update the firmware or user interface to the latest versions.



Download the file to your hard drive from the Belkin web site or from another source. Then click Browse... to find the file on your computer. Select the firmware file and click “Open”. Click “Save Settings” to start the upgrade process.

Reset

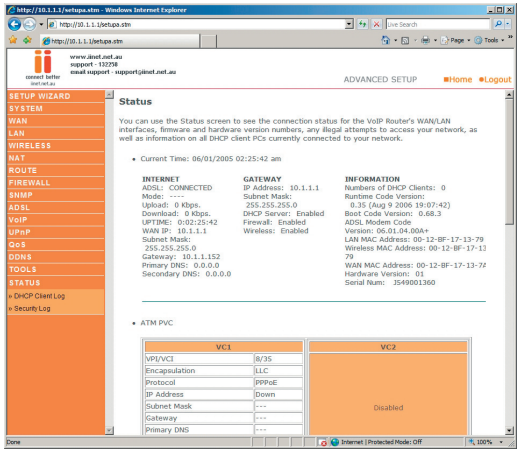
Perform a reset from this page.



Should your unit become unresponsive for any reason, you can simply perform a reset from this page. Performing a reset will reboot the device. Your configuration settings will remain the same.

Status

The Status screen displays WAN/LAN connection status, firmware and hardware version numbers, as well as information on DHCP clients connected to your network.



The security log may be saved to a file by clicking “Save” and choosing a location.

The following items are included on the Status screen:

Parameter Description

Internet: Displays WAN connection type and status. Release Click on this button to disconnect from the WAN. Renew Click on this button to establish a connection to the WAN.

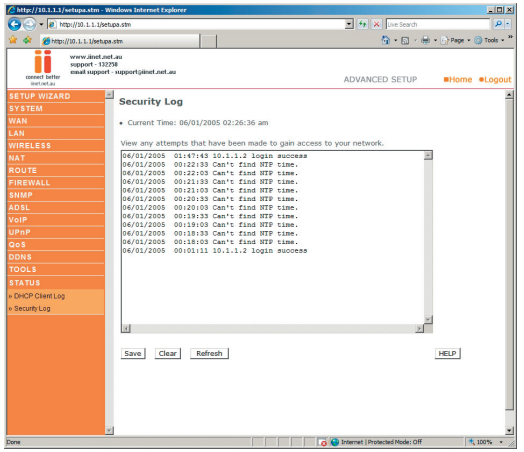
Gateway: Displays system IP settings, as well as DHCP Server and Firewall status.

Information: Displays the number of attached clients, the firmware versions, the physical MAC address for each media interface and for the VoIP Router, as well as the hardware version and serial number.

ATM PVC: Displays ATM connection type and status.
Save: Click on this button to save the security log file.
Clear: Click on this button to delete the access log.
Refresh: Click on this button to refresh the screen.

DHCP Client LOG

DHCP Client Log: Displays information on DHCP clients on your network.



Security LOG

Security Log: Displays information about attempts to access ports and addresses. Also displays information about your ADSL connection such as Login failures, disconnections and etc.

Appendix A1 Troubleshooting

After completing hardware setup by connecting all your network devices, you should automatically be able to connect to the VoIP ADSL Wireless Router by entering 10.1.1.1 into your Internet browsers address bar.

Should this not work please first determine how your ISP issues your IP address. Many ISPs issue these numbers automatically using Dynamic Host Configuration Protocol (DHCP). Other ISPs provide a static IP address and associated numbers, which you must enter manually. How your ISP assigns your IP address determines how you may need to change the configuration of your computer as per the steps below.

TCP/IP Configuration

To access the Internet through the VoIP Router, you must configure the network settings of the computers on your LAN to use the same IP subnet as the VoIP Router. The default network settings for the ADSL Router are:

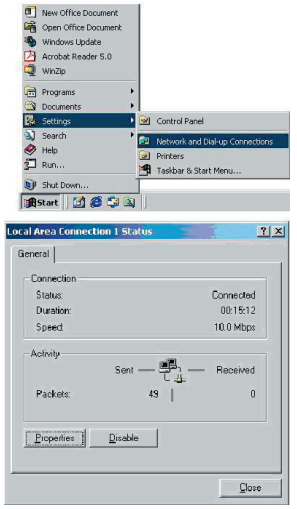
IP Address: 10.1.1.1 Subnet Mask: 255.255.255.0

Note: These settings can be changed to fit your network requirements, but you must first configure at least one computer to access the VoIP Router's web configuration interface in order to make the required changes.

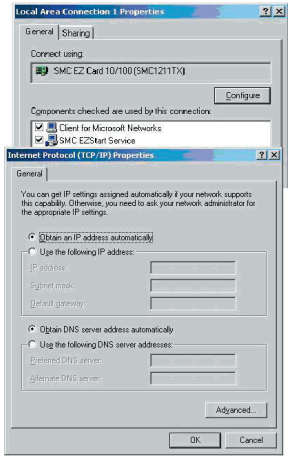
Configuring Your Computer in Windows 2000

DHCP IP Configuration

1. On the Windows desktop, click Start/Settings/Network and Dial-Up Connections.
2. Click the icon that corresponds to the connection to your VoIP Router.
3. The connection status screen will open. Click Properties.



1. Double-click Internet Protocol (TCP/IP).
2. If “Obtain an IP address automatically” and “Obtain DNS server address automatically” are already selected, your computer is already configured for DHCP. If not, select these options and then click ok and then ok again, or click Cancel to close each window.



Manual IP Configuration

1. Follow steps 1-4 in “DHCP IP Configuration” on the previous page.
2. Select “Use the following IP address.” Enter an IP address based on the default network

   10.1.1.x (where x is between 2 and 254), use

   255.255.255.0 for the subnet mask and the IP address of the VoIP Router 10.1.1.1 for the Default gateway field.
3. Select “Use the following DNS server addresses.”
4. Enter the IP address for the VoIP Router in the Preferred DNS server field. This automatically relays DNS requests to the DNS server(s) provided by your ISP. also, add a specific DNS server of your ISP into the Alternate DNS Server field and click OK to close the dialog boxes.
5. Record the configured information in the following table.

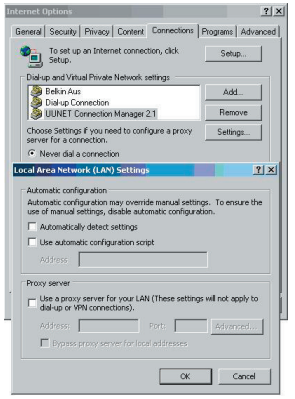
TCP/IP Configuration Setting

IP Address	____.____.____.____
Subnet Mask	____.____.____.____
Default Gateway	____.____.____.____
Preferred DNS Server	____.____.____.____
Alternate DNS Server	____.____.____.____

Disable HTTP Proxy

You need to verify that the “HTTP Proxy” feature of your web browser is disabled. This is so that your browser can view the VoIP Router’s HTML configuration pages.

1. Open control panel.
2. Open internet options
3. Go to the connections tab and click on the LAN settings button.
4. Ensure that NOTHING is ticked on this screen and click ok.
5. On the connections tab, make sure that there are no dial up connections, select the “Never dial a connection” radio button.

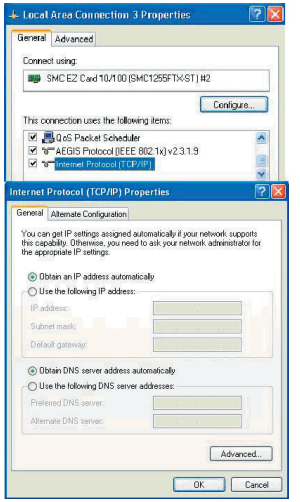


Your computer is now configured to connect to the VoIP Router.

Configuring Your Computer in Windows XP

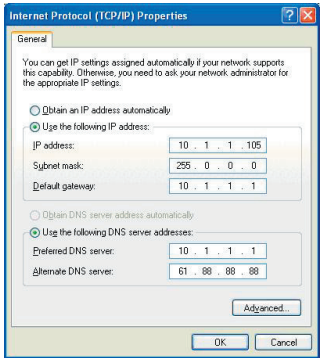
DHCP IP Configuration

1. On the Windows desktop, click Start/Control Panel.
2. In the Control Panel window, click Network Connections or click Network and Internet Connections and then Network Connections.
3. The Network Connections window will open. Locate and double-click the Local Area Connection icon for the Ethernet or Wireless adapter that is connected to the VoIP Router.
4. In the connection status screen, click Properties.
5. Double-click Internet Protocol (TCP/IP).
6. If “Obtain an IP address automatically” and “Obtain DNS server address automatically” are already selected, your computer is already configured for DHCP. Click Cancel to close each window.



Manual IP Configuration

1. Follow steps 1-5 in “DHCP IP Configuration” on the previous page.
2. Select “Use the following IP address.” Enter an IP address based on the default network which is 10.1.1.x (where x is between 2 and 254), use 255.255.255.0 for the subnet mask and the IP address of the VoIP Router 10.1.1.1 for the Default gateway field.



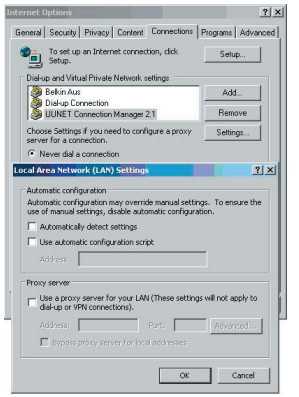
3. Select “Use the following DNS server addresses.”
4. Enter the IP address for the VoIP Router in the Preferred DNS server field. This automatically relays DNS requests to the DNS server(s) provided by your ISP. also, add a specific DNS server of your ISP into the Alternate DNS Server field and click OK to close the dialog boxes.
5. For future reference you may record the configured information in the following table.

TCP/IP Configuration Setting	
IP Address	____.____.____.____
Subnet Mask	____.____.____.____
Default Gateway	____.____.____.____
Preferred DNS Server	____.____.____.____
Alternate DNS Server	____.____.____.____

Disable HTTP Proxy

You need to verify that the “HTTP Proxy” feature of your web browser is disabled. This is so that your browser can view the VoIP Router’s HTML configuration pages.

6. Open control panel.
7. Open internet options
8. Go to the connections tab and click on the LAN settings button.
9. Ensure that NOTHING is ticked on this screen and click ok.
10. On the connections tab, make sure that there are no dial up connections, select the “Never dial a connection” radio button.



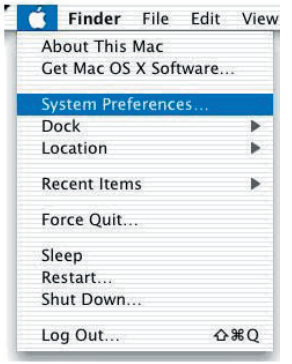
Your computer is now configured to connect to the VoIP Router.

Configuring Your Macintosh Computer

You may find that the instructions here do not exactly match your operating system. This is because these steps and screen shots were created using Mac OS 10.2. Mac OS 7.x and above are similar, but may not be identical to the Mac OS you are using.

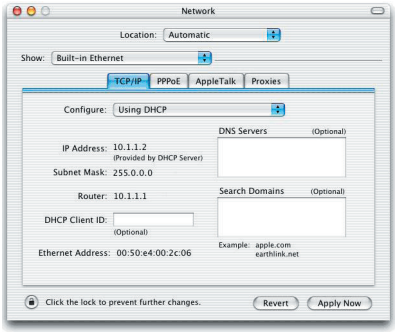
Follow these instructions:

1. Open the Systems Preferences window.



2. Double Click “Network”

3. If “Using DHCP Server” is already selected in the configure field, your computer is already configured for DHCP. If not, select this option.
4. Your new settings are shown in the TCP/IP tab. Verify that your IP Address is now 10.1.1.xxx, your Subnet Mask is 255.0.0.0 or 255.255.255.0 and your Default Gateway is 10.1.1.1. These values confirm that your VoIP Router is functioning.
5. Close the Network window.



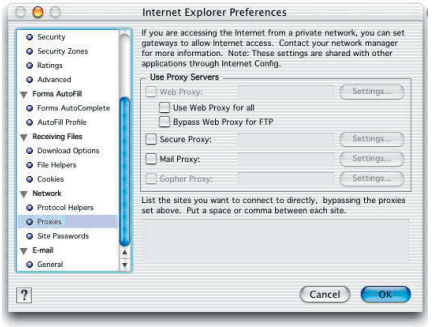
Now your computer is configured to connect to the VoIP Router.

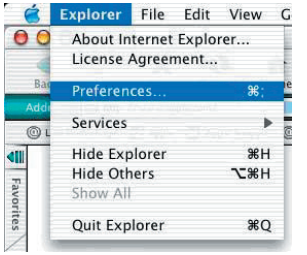
Disable HTTP Proxy

You need to verify that the “HTTP Proxy” feature of your web browser is disabled. This is so that your browser can view the VoIP Router’s HTML configuration pages. The following steps are for Internet Explorer.

Internet Explorer

1. Open Internet Explorer and click the Stop button. Click Explorer/Preferences.
2. In the Internet Explorer Preferences window, under Network, select Proxies.
3. Uncheck all check boxes and click OK.





Appendix A2 Troubleshooting

This section describes common problems you may encounter and possible solutions to them. The VoIP Router can be easily monitored through panel indicators to identify problems.

Troubleshooting

Symptom	Action
LED Indicators	
POWER LED is Off	• Check connections between the VoIP Router, the external power supply, and the wall outlet. • If the power indicator does not turn on when the power cord is plugged in, you may have a problem with the power outlet, power cord, or external power supply. However, if the unit powers off after running for a while, check for loose power connections, power losses, or surges at the power outlet. If you still cannot isolate the problem, then the external power supply may be defective. In this case, contact Technical Support for assistance.

Troubleshooting

Symptom	Action
LED Indicators	
LAN LED is Off	• Verify that the VoIP Router and attached device are powered on. • Be sure the cable is plugged into both the VoIP Router and the corresponding device. • Verify that the proper cable type is used and that its length does not exceed the specified limits. • Be sure that the network interface on the attached device is configured for the proper communication speed and duplex mode. • Check the adapter on the attached device and cable connections for possible defects. Replace any defective adapter or cable if necessary.

Network Connection Problems	
Cannot ping the VoIP Router from the attached LAN, or the VoIP Router cannot ping any device on the attached LAN	• Verify that the IP addresses are properly configured. For most applications, you should use the VoIP Router's DHCP function to dynamically assign IP addresses to hosts on the attached LAN. However, if you manually configure IP addresses on the LAN, verify that the same network address (network component of the IP address) and subnet mask are used for both the VoIP Router and any attached LAN devices. • Be sure the device you want to ping (or from which you are pinging) has been configured for TCP/IP. • Disable any installed Firewalls

Troubleshooting

Symptom	Action
Management Problems	
Cannot connect using the Web browser	• Be sure to have configured the VoIP Router with a valid IP address, subnet mask, and default gateway. • Check that you have a valid network connection to the VoIP Router and that the port you are using has not been disabled. • Check the network cabling between the management station and the VoIP Router. • Disable any installed Firewalls. • Disable any proxies
Forgot or lost the password	• Press the Reset button on the rear panel (holding it down for at least 20 seconds) to restore the factory defaults. Note: All settings will need to be re-entered – this option wipes all settings and restore the unit back to the factory defaults.

Appendix B Cables

Ethernet Cable

Caution: Do not plug a phone jack connector into an RJ-45 port. For Ethernet connections, use only twisted-pair cables with RJ-45 connectors that conform to FCC standards.

Specifications

Cable Types and Specifications

Cable	Type	Max. Length	Connector
10BASE-T	Cat. 3, 4, 5 100-ohm UTP	100 m (328 ft)	RJ-45
100BASE-TX	Cat. 5 100-ohm UTP	100 m (328 ft)	RJ-45

Appendix C Specifications

Standards Compliance

CE Mark

Emissions

FCC Class B, VCCI Class B
Industry Canada Class B
EN55022 (CISPR 22) Class B
C-Tick - AS/NZS 3548 (1995) Class B

Immunity

EN 61000-3-2/3
EN 61000-4-2/3/4/5/6/8/11

Safety

UL 1950
EN60950 (TÜV)
CSA 22.2 No. 950

IEEE 802.3 10 BASE-T Ethernet
IEEE 802.3u 100 BASE-TX Fast Ethernet

Modem Standards

ITU G.992.1 (G.dmt)
ITU G.992.2 (G.lite)
ITU G.994.1 (G.handshake)
ITU T.413 issue 2 - ADSL full rate

LAN Interface

RJ-45 10 BASE-T/100 BASE-TX ports
Auto-negotiates the connection speed to 10 Mbps Ethernet or 100 Mbps
Fast Ethernet, and the transmission mode to half-duplex or full-duplex

USB Interface

1 USB port (F1PI210ENau only)

WAN Interface

1 ADSL RJ-11 port

FXO Interface

1 FXO port

FXS Interface

2 FXS ports

Indicator Panel

Line, Phone 1-2, VoIP, USB (F1PI210ENau only), LAN 1-4 (4 port F1PI241ENau & F1PI241ENau only), WLAN (F1PI241EGau only), Online, ADSL, PWR (power)

Dimensions

16 x 120 x 190 mm (0.63 x 4.72 x 7.48 in.)

Weight

610 g (1.63 lbs)

Input Power

12 V 1.25 A

Power Consumption

2.52 Watts maximum

Management

Web management

Advanced Features

VoIP-QoS, VAD, call waiting, call forwarding, caller ID, jitter buffer.
Codecs supported - G.711 U/A law, G.729, G.723.1
Dynamic IP Address Configuration – DHCP, DNS, DDNS
Firewall – Client privileges, hacker prevention and logging, Stateful Packet Inspection
Virtual Private Network – PPTP, IPSec pass-through, VPN pass-through

Internet Standards

RFC 826 ARP, RFC 791 IP, RFC 792 ICMP, RFC 768 UDP, RFC 793 TCP, RFC 783 TFTP, RFC 1483 AAL5 Encapsulation, RFC 1661 PPP, RFC 1866 HTML, RFC 2068 HTTP, RFC 2364 PPP over ATM

Temperature

Operating 0 to 40 °C (32 to 104 °F)
Storage -40 to 70 °C (-40 to 158 °F)

Humidity

5% to 95% (non-condensing)

Glossary-1

10BASE-T

IEEE 802.3 specification for 10 Mbps Ethernet over two pairs of Category 3, 4, or 5 UTP cable.

100BASE-TX

IEEE 802.3u specification for 100 Mbps Fast Ethernet over two pairs of Category 5 UTP cable.

Auto-Negotiation

Signaling method allowing each node to select its optimum operational mode (e.g., 10 Mbps or 100 Mbps and half or full duplex) based on the capabilities of the node to which it is connected.

Bandwidth

The difference between the highest and lowest frequencies available for network signals. Also synonymous with wire speed, the actual speed of the data transmission along the cable.

Collision

A condition in which packets transmitted over the cable interfere with each other. Their interference makes both signals unintelligible.

Collision Domain

Single CSMA/CD LAN segment.

CSMA/CD

CSMA/CD (Carrier Sense Multiple Access/Collision Detect) is the communication method employed by Ethernet, Fast Ethernet, or Gigabit Ethernet.

End Station

A workstation, server, or other device that does not forward traffic.

Ethernet

A network communication system developed and standardized by DEC, Intel, and Xerox, using baseband transmission, CSMA/ CD access, logical bus topology, and coaxial cable. The successor IEEE 802.3 standard provides for integration into the OSI model and extends the physical layer and media with

repeaters and implementations that operate on fiber, thin coax and twisted-pair cable.

Fast Ethernet

A 100 Mbps network communication system based on Ethernet and the CSMA/CD access method.

Full Duplex

Transmission method that allows two network devices to transmit and receive concurrently, effectively doubling the bandwidth of that link.

IEEE

Institute of Electrical and Electronic Engineers.

IEEE 802.3

Defines carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications.

IEEE 802.3ab

Defines CSMA/CD access method and physical layer specifications for 1000BASE-T Fast Ethernet.

IEEE 802.3u

Defines CSMA/CD access method and physical layer specifications for 100BASE-TX Fast Ethernet.

Glossary-2

IEEE 802.3x

Defines Ethernet frame start/stop requests and timers used for flow control on full-duplex links.

Local Area Network

(LAN) A group of interconnected computer and support devices.

LAN Segment

Separate LAN or collision domain.

LED

Light emitting diode used or monitoring a device or network condition.

Local Area Network

A group of interconnected computers and support devices. Media Access Control (MAC) A portion of the networking protocol that governs access to the transmission medium, facilitating the exchange of data between network nodes.

MIB

An acronym for Management Information Base. It is a set of database objects that contains information about the device.

RJ-45 Connector

A connector for twisted-pair wiring.

Straight-through Port

An RJ-45 port which does not cross the receive and transmit signals internally (MDI) so it can be connected with straight-through twisted-pair cable to any device having a crossover port (MDI-X). Also referred to as a “Daisy-Chain” port. The RJ-45, 10/100 Mbps port supports Auto MDI/ MDI-X.

Switched Ports

Ports that are on separate collision domains or LAN segments.

UTP

Unshielded twisted-pair cable.