

BOB™

BoB™ - 4 port wireless VoIP router



Table of Contents



Chapter 1 : Introduction	Pg. 01
Chapter 2 : Product Overview	Pg. 02
Chapter 3 : Knowing BoB™	Pg. 04
Chapter 4 : Connection & Configuration	Pg. 05
Chapter 5 : Advanced Setup	Pg. 07
Setup Wizard	Pg. 08
Menu Description	Pg. 10
System Time Setting	Pg. 11
Password Setting	Pg. 12
Remote Management	Pg. 12
DNS	Pg. 13
WAN	Pg. 13
ATM PVC	Pg. 14
ATM Interface	Pg. 15
Clone MAC Address	Pg. 16
LAN	Pg. 17
VLAN	Pg. 18
VLAN Access Control	Pg. 19
Channel and SSID	Pg. 20
Wireless Access Control	Pg. 21
Security	Pg. 22
WEP	Pg. 23
WPA/WPA2	Pg. 24
WDS	Pg. 25
NAT	Pg. 25
Address Mapping	Pg. 26
Port Forwarding	Pg. 27
Special Applications	Pg. 28
Route	Pg. 30
RIP Parameter	Pg. 31
Access Control	Pg. 34
MAC Filter	Pg. 36

Table of Contents



Schedule Rule	Pg. 38
Intrusion Detection	Pg. 39
DMZ	Pg. 40
SNMP	Pg. 41
Community	Pg. 41
Trap	Pg. 42
ADSL	Pg. 42
Status	Pg. 43
VoIP	Pg. 44
VoIP Advanced Setting	Pg. 46
Port Advanced Setting	Pg. 47
DECT Setting	Pg. 48
UPnP	Pg. 49
QoS	Pg. 50
Edit Traffic Class	Pg. 51
Traffic Statistics	Pg. 52
DDNS	Pg. 52
USB	Pg. 53
Configuration Tools	Pg. 55
Firmware Upgrade	Pg. 55
Diagnostic Utility	Pg. 56
Reset	Pg. 56
Status	Pg. 57
DHCP Client LOG	Pg. 58
Security Log	Pg. 58
Appendices	Pg. 59
A1 Troubleshooting	Pg. 61
A2 Troubleshooting	Pg. 62
B Cables	Pg. 63
C Specification	Pg. 64
Glossary-1	Pg. 65
Glossary-2	Pg. 66
Belkin International, Inc. Limited 2 Year Product Warranty	Pg. 67

Chapter I: Introduction

BoB™ 4 port integrated wireless router

Thank you for purchasing the BoB™ 4 port integrated wireless router (handset optional). Within minutes you will be able to connect to the internet and make Voice over Internet Protocol (VoIP) phone calls. The following is a list of features that make BoB™ an ideal solution for your home or small office and will contain important information on how to get what you want out of BoB™, so please read carefully before setting him up.



Chapter 2 : Product Overview

About BoB™ 4 port integrated wireless router

Product Overview

BoB™ - 4 port integrated wireless router, excluding BoB™ handset



Compatibility with both PC's and Mac® Computers

The router supports a variety of networking environments including Mac OS® 8.x, 9.x & v10.x, Linux®, Windows® 98SE, ME, NT, 2000, XP and Vista. You will 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 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 router indicate which functions are in operation. You'll know at-a-glance whether your router 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 router 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.

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 router 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 router 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.

USB/3g/Charge Ports

Your router is equipped with two USB ports, Storage/3g and Charge. The Storage/3g port currently supports FAT16/32 & NTFS USB Mass Storage Devices. With a mass storage device connected you can easily share your files to anyone on the network.

Future planned firmware upgrades will allow the router to support 3g USB wireless adapters as a backup if your ADSL connection is down. For more information on this feature and a list of support USB adapters, visit <http://www.belkin.com.au/support>

Chapter 2 : Product Overview

About BoB™ 4 port integrated wireless router

The 'Charge' port on your router is dedicated to charging USB powered devices, such as mobile phones, iPods, etc. The charge port will supply a maximum 5V 500mA. Connecting a USB device which requires more than 500mA may result in damage to your equipment.

QoS

QoS (Quality of Service) limits the traffic being sent from the router (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.

Virtual Server

If you have a fixed IP address, you can set the 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 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.

Support for VPN Pass-Through

If you connect to your office network from home using a VPN connection, your router will allow your VPN-equipped computer to pass through the router and to your office network. This router supports 1 VPN session at any one time

This router supports three of the most commonly used VPN protocols – PPTP, L2TP, and IPSec. The VPN protocols supported by the 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.

Wired & Wireless LAN

The 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. 802.11b, 802.11g & 802.11n wireless standards are supported.

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 on your network.

VLAN

VLAN (Virtual Local Area Network) adds the ability to manage multiple networks with the one router. The router is designed to be placed on a desktop. All of the cables exit from the rear of the router for better organisation and utility. The LED indicators are easily visible on the front of the router to provide you with information about network activity and status.

BoB™ Handset

The BoB™ handset is an optional device which slots into the front of the BoB™ router and allows you to make voice calls (including VoIP where available).

The BoB™ router can support up to 5 DECT-compatible handsets and the handset cradle also functions as a charger for the BoB™ handset when it is not in use.

Chapter 3 : Knowing BoB™

Knowing your BoB™ - 4 port integrated wireless router

Note

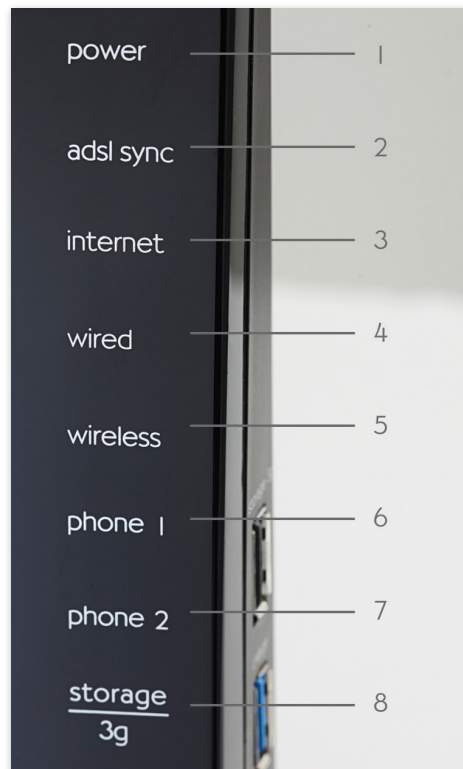
on Side Panel Ports:

The router has an aforementioned USB/3g port labelled '3g/storage' along with a USB charge port.

The charge port is able to charge devices which use a USB connection, such as iPods, etc.

LED indicators are easily visible on the front of the router to provide you with information about network activity and status. All cables and connections conveniently exit from the rear of the router.

Front Panel



1. Power LED

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

- **Off** - Router is off
- **Orange** - Router is booting
- **Blue** - Router is on and ready for use

2. ADSL SYNC LED

The ADSL LED will light up yellow indicating no ADSL sync. Once line sync is established the LED will light up blue.

- **Off** - No ADSL connection
- **Orange** - Negotiating connection/No ADSL sync
- **On** - ADSL link is up and connected

3. Internet LED

The Internet LED shows you when the router is connected to the Internet. If the LED is off or yellow the router is NOT connected to the Internet.

- **Off** - Not connected to Internet
- **Orange** - The router is not connected to the internet or a problem has been detected.
- **On** - Connected to internet

4. LAN Status LED

When a computer is properly connected to the LAN port on the rear of the router, the LED shown here 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** - Your computer is connected

5. Wireless Status LED

The Wireless status LED shows you when the router's wireless is enabled.

- **On** - Wireless enabled
- **Orange** - Solid, the router has detected a problem with a client connecting to the wireless
- **Off** - Wireless is disabled

6 & 7. Phone Status LED 1-2

The phone lights indicate whether VoIP account one or two has successfully registered on the network.

- **On** - VoIP registered successfully
- **Orange** - Solid, the router has detected a problem registering your VoIP account on the network
- **Off** - No VoIP activity

8. Storage/3g

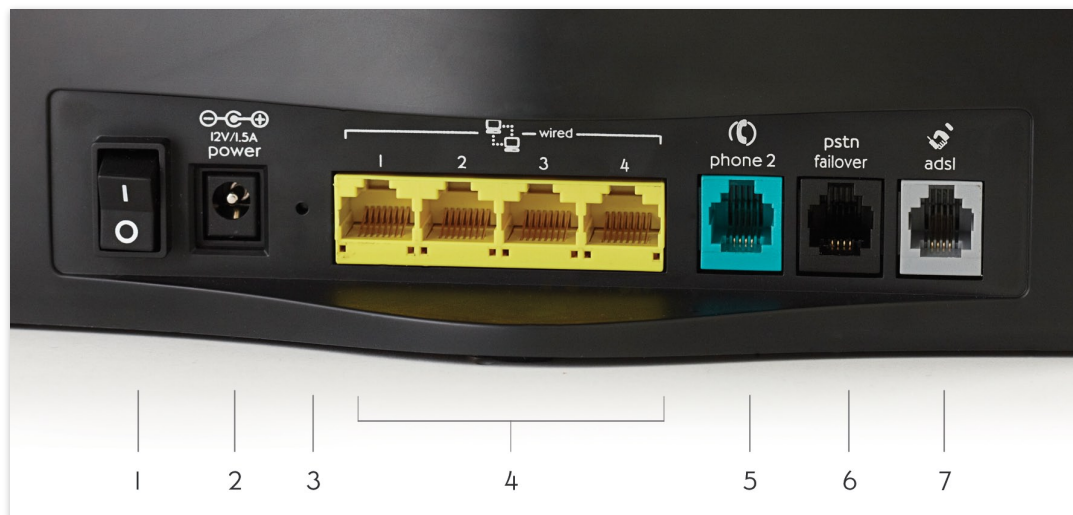
When a USB mass storage device is connected to this USB Port, this light will illuminate to inform you the attached storage device is ready for use. This USB port also accepts a 3g wireless modem service.

- **On** - Attached USB Mass Storage or 3g Device connected and ready for use
- **Off** - No attached USB Mass Storage or 3g Device

Chapter 4 : Connection & Configuration

Connect & Configure your BoB™

Back Panel



1. Power Switch

The power switch allows you to switch on or off the router. Once you have connected the power plug, flip the switch to ON (I) to power on the router.

2. Power Plug

Connect the included 12V 1.5A DC power supply to this inlet. Using the wrong type of power adapter may cause damage to your router.

3. Reset Button

- **Resetting the Router**
Push and hold the Reset button for one second then release it. When the power light becomes solid again the reset is complete.
- **Restoring the Factory Defaults**
Push and hold the Reset button for ten seconds then release it. When the power light becomes solid again the restore is complete.

4. LAN Ports

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

5. Phone Two Port

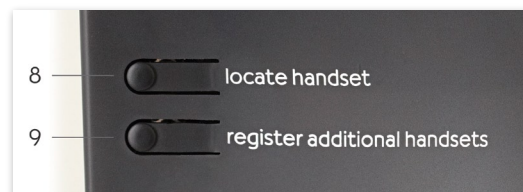
Phone Port connects to standard analogue telephone set or fax machine.

6. PSTN Failover Port

The Optional RJ11 port is for connection to your PSTN (Home Phone) line to provide Normal Phone call backup for when VoIP is unavailable or not required.

7. ADSL Line

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



8. Locate handset (if installed)

Press this button to signal the BoB™ handset to ring, allowing you to easily find its current location. Useful if you have lost the handset.

9. Register additional handsets

Allows you to register additional DECT compliant handsets to your router. A total of 5 DECT handsets can be registered to your router at any one time.

Chapter 4 : Connection & Configuration

Connect & Configure your BoB™

Notes:

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.

Step 1. Find a suitable location

Your BoB™ - 4 port integrated wireless 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 router away from any heating devices
- Do not place the 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 router.

Step 2. Connect the ADSL Line

Phone line configuration

Run a standard telephone cable from the wall jack providing ADSL service to the RJ-II ('ADSL') port on your router. When inserting an ADSL RJ-II 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).

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

Step 3. Attach to your network using Ethernet cabling

The LAN ports on the router auto-negotiate 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 router to an Ethernet adapter on your PC. Otherwise, cascade the LAN port on the router to an Ethernet hub or switch, and then 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 router. Instead, use only twisted-pair cables with RJ-45 connectors that conform to Australian standards.

Step 4. Connect the power adapter

Plug the power adapter into the power socket on the rear panel of the 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 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.

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

Step 1. How to log into the router

After you have configured TCP/IP on a client computer, use a web browser to configure the router. The 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 router and view statistics to monitor network.

To access the router's management interface, enter the IP address of the 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 section 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 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 ISP account user name and password

The 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 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 router please view the Advanced Setup table of contents in order to find the correct setup method.

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 times 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 an '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.'

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

Note:

VoIP port 1 is the BoB™ handset which slots into the front of the router or any DECT-compatible handsets you have registered to the router.

Step 3. Using Setup Wizard

This page allows you to quickly setup basic settings of the router 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:
Username:
Password:
[SAVE SETTINGS](#) [Refresh](#)

Line Status: Physical Up
Line Mode: G.992.5 (ADSL2+)
Connected/NO Connection: Connected
WAN IP: 203.59.255.162
[disconnect](#) [connect](#)

Wireless Parameter Setting:
Enable Wireless Radio:
Primary Wireless SSID:

VoIP Parameter Setting:
VoIP Account 1: [VoIP Registration: Up] [REGISTER](#) [UNREGISTER](#)
VoIP Phone Number:
VoIP Password:
VoIP Account 2: [VoIP Account: Unconfigured] [REGISTER](#) [UNREGISTER](#)
State:

[SAVE SETTINGS](#) [Refresh](#)

VOIP Parameter Setting

User Name: Enter your VoIP account user name for your ISP

Password: Enter your VoIP account password for your ISP

ADSL Parameter Setting

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

Password: Enter your internet account password for your ISP

Wireless Parameter Setting

Enable Wireless Radio: Enable or disable the routers wireless function.

Primary Wireless SSID: Change the routers primary SSID (wireless name).

VOIP Parameter Setting

Firstly you need to tick one of the VoIP account boxes. For instance if you wish to use VoIP port 2 on the back of the router then tick the box for VoIP account 2. 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 for 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.

Advanced Setup Method

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.

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

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 screenshot shows the iinet router's advanced setup interface. The top navigation bar includes 'ADVANCED SETUP', 'Home', and 'Logout'. A left sidebar lists menu items: SETUP WIZARD, SYSTEM, WAN, LAN, WIRELESS, NAT, ROUTE, FIREWALL, SNMP, ADSL, VoIP, UPnP, QoS, DDNS, USB, TOOLS, and STATUS. The main content area is titled 'Status' and contains the following information:

- Current Time:** 2009/6/25 - 9:57:47
- UPTIME:** 0:0:33:55
- INTERNET:** ADSL: CONNECTED, Mode: G.992.5 (ADSL2+), Download: 19560 Kbps, Upload: 1021 Kbps, WAN IP: 203.59.255.162, Subnet Mask: 255.255.255.255, Gateway: 203.59.14.16, Primary DNS: 203.0.178.191, Secondary DNS: 203.215.29.191
- GATEWAY:** IP Address: 10.1.1.1, Subnet Mask: 255.255.255.0, DHCP Server: Enabled, Firewall: Enabled, UPnP: Enabled, Wireless: Enabled
- WIRELESS:** Wireless: Enabled, Channel: 6, Wireless Devices: 0, Virtual AP1 SSID: WLAN, Wireless Security: Disabled, Virtual AP2 SSID: WLAN2, Security: Disabled
- INFORMATION:** Numbers of DHCP Clients: 1, Runtime Code Version: F1P1243EGau_v1.2.14.20, Boot Code Version: 1.0.37-102.9, ADSL Modem Code Version: A2pB0251L.d21k5, LAN MAC Address: 00:22:75:A7:68:CF, Wireless MAC Address: 00:22:75:A7:68:D0, WAN MAC Address: 00:22:75:A7:68:D1, Hardware Version: A610A354054R_R3, Serial Num: , Build Time: 2009.06.22-14:09:26

Below the Status page, there is a section for ATM PVCs. VC1 is active with the following settings:

VC1	
VPI/VCI	8/35
Encapsulation	LLC
Protocol	PPPoE
IP Address	203.59.255.162
Subnet Mask	255.255.255.255
Gateway	203.59.14.16
Primary DNS	203.0.178.191
Secondary DNS	203.215.29.191
<input type="button" value="Disconnect"/> <input type="button" value="Connect"/>	

VC2 is disabled.

The 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 44)

This section will explain the basics of turning on the Wireless Functions in your 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 44)

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 21)
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 22)
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 44)

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

Setting/Adjusting Quality of Service (Page 50)

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 27)

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.

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

Menu Description

System (Page 11)

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 13)

- 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 complete the Internet connection should it be required by your internet service provider in order to complete the Internet connection.

LAN (Page 17)

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.
- DHCP Server Control.
- VLAN Port routing.

The LAN Menu also has 2 sub-menus:

1. VLAN

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

2. 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 19)

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

1. 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 in case it is accidentally sharing the same channel as another wireless appliance in the area.

2. 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'.

3. 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.

4. 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 25)

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

Route (Page 30)

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

Firewall (Page 33)

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

SNMP (Page 41)

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

ADSL (Page 42)

Sets the ADSL operation type and shows the ADSL status.

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

VoIP (Page 44)

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

UPnP (Page 49)

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 50)

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 52)

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.

USB (Page 53)

You can plug-in your USB hard drive or memory stick and share these resources on your home network.

Tools (Page 55)

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 43)

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 Time Settings

Time Settings

Current Time: 2009/6/25 - 9:59:05

- **Set Time Zone:**

Use this setting to ensure the time-based client filtering feature and system log entries are based on the correct localised time.

(GMT+08:00) Perth

To enable daylight saving place a tick in the Enable Daylight Saving box, this will automatically adjust the reported time by one hour. When your region is not observing daylight saving take the tick out of the box for the correct time to be reported.

 Enable Daylight Savings
- **Configure Time Server (NTP):**

You can automatically maintain the system time on your ADSL router by synchronizing with a public time server over the Internet.

 Enable Automatic Time Server Maintenance

When you enable this option you will need to configure two different time servers, use the options below to set the primary and secondary NTP servers in your area:

Primary Server: time.nist.gov Manually Set NTP Server IP/DNS Name Here

Secondary Server: ntp1.tummy.com

Time Synchronization Interval: 1 (1-72 hours)

[HELP](#) | [SAVE SETTINGS](#) | [CANCEL](#)

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

Check 'Enable Automatic Time Server Maintenance' to automatically maintain the 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.

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

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').

Password Settings

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

iinet connect better
www.iinet.net.au
support - 132258
email support - support@iinet.net.au

ADVANCED SETUP [Home](#) [Logout](#)

SETUP WIZARD
SYSTEM
» Time Settings
» Password Settings
» Remote Management
» DNS
WAN
LAN
WIRELESS
NAT
ROUTE
FIREWALL
SNMP
ADSL
VoIP
UPnP
QoS
DDNS
USB
TOOLS
STATUS

Password Settings

Password:
You can change the password to restrict access to this modem. This is recommended if you intend to enable remote management. By default the modems password is *admin*.

Idle time out:
This is a determined time where by the modem will log the user out of this modems web configuration interface (you will still be connected to the internet and has no affect to your ability to browse the internet).

- Current Password :
- New Password :
- Re-Enter Password for Verification :
- Idle Time Out: Min (Idle Time =0 : NO Time Out)

[HELP](#) | [SAVE SETTINGS](#) | [CANCEL](#)

Passwords can contain from 3 to 12 alphanumeric characters which are case sensitive.

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 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.

iinet connect better
www.iinet.net.au
support - 132258
email support - support@iinet.net.au

ADVANCED SETUP [Home](#) [Logout](#)

SETUP WIZARD
SYSTEM
» Time Settings
» Password Settings
» Remote Management
» DNS
WAN
LAN
WIRELESS
NAT
ROUTE
FIREWALL
SNMP
ADSL
VoIP
UPnP
QoS
DDNS
USB
TOOLS
STATUS

Remote Management

To enable remote management tick the enable box and save changes. This will enable any computer on the internet to access your modem. If you only want a specific computer on the internet to access your modem then type in the wan ip address of that computer in the field marked 'Host Address'. If this is left as 0.0.0.0 then any computer can access your modem. It is strongly advised that you change the login password for your modem, as the default password for all modems is *admin*.

To remotely manage this device, the remote user should type into their browser.
http://<Device WAN IP address>: 8080.

Host Address:

Port for remotely manage this device:

Enabled:

[HELP](#) | [SAVE SETTINGS](#) | [CANCEL](#)

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

Note:

If you check 'Enabled' and specify an IP address of 0.0.0.0, any host can manage the 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

The screenshot shows the 'DNS' configuration page on the iinet router. The page includes a sidebar with navigation options: SETUP WIZARD, SYSTEM, Time Settings, Password Settings, Remote Management, DNS, WAN, LAN, WIRELESS, NAT, ROUTE, FIREWALL, SNMP, ADSL, VoIP, UPnP, QoS, DDNS, USB, TOOLS, and STATUS. The main content area is titled 'DNS' and contains the following text: 'Changes here are only necessary if advised by your internet service provider.' and 'A Domain Name Server (DNS) is an index of IP addresses and Web addresses. If you type a Web address into your browser, such as www.iinet.net.au/support, a DNS server will find that name in its index and find the matching IP address: xxx.xxx.xxx.xxx. Most ISPs provide a DNS server for speed and convenience. Since your Service Provider may connect to the Internet with dynamic IP settings, it is likely that the DNS server IP's are also provided dynamically. However, if there is a DNS server that you would rather use, you need to specify the IP address here.' There is a checkbox labeled 'Automatic from ISP' which is checked. Below this are two input fields: 'Domain Name Server (DNS) Address' and 'Secondary DNS Address (optional)'. At the bottom right, there are three buttons: 'HELP', 'SAVE SETTINGS', and 'CANCEL'.

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

The screenshot shows the 'WAN Settings' configuration page on the iinet router. The page includes a sidebar with navigation options: SETUP WIZARD, SYSTEM, WAN, ATM PVC, Clone MAC Address, LAN, WIRELESS, NAT, ROUTE, FIREWALL, SNMP, ADSL, VoIP, UPnP, QoS, DDNS, USB, TOOLS, and STATUS. The main content area is titled 'WAN Settings' and contains the following text: 'The router can be connected to your service provider in any of the following ways:' followed by two options: 'ATM PVC To configure ATM VC parameters' and 'Clone MAC To configure WAN Interface MAC Address'.

Specify the WAN connection parameters provided by your Internet Service Provider (ISP). The router can be connected to your ISP in one of the following ways:

- ATM PVC
- Clone MAC

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

ATM PVC

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

The screenshot shows the iinet router's web interface. The top navigation bar includes the iinet logo, contact information (www.iinet.net.au, support - 132258, email support - support@iinet.net.au), and links for ADVANCED SETUP, Home, and Logout. A left-hand menu lists various configuration options: SETUP WIZARD, SYSTEM, WAN, ATM PVC, Clone MAC Address, LAN, WIRELESS, NAT, ROUTE, FIREWALL, SNMP, ADSL, VoIP, UPnP, QoS, DDNS, USB, TOOLS, and STATUS. The main content area is titled 'ATM PVC' and contains a sub-header 'ADSL router uses ATM as its layer 2 protocol. ATM PVC is a virtual connection which acts as a WAN interface. The Gateway supports up to 8 ATM PVCs.' Below this is a table with four columns: Description, VPI/VCI, Encapsulation, and Protocol. The table lists eight Virtual Circuits (VC1 through VC8). VC1 is configured with VPI/VCI 8/35, LLC encapsulation, and PPPoE protocol. VCs 2 through 8 are shown with dashes in the VPI/VCI and Encapsulation columns, and dashes in the Protocol column. A 'HELP' link is located in the bottom right corner of the page.

Description	VPI/VCI	Encapsulation	Protocol
VC1	8/35	LLC	PPPoE
VC2	-/-	---	---
VC3	-/-	---	---
VC4	-/-	---	---
VC5	-/-	---	---
VC6	-/-	---	---
VC7	-/-	---	---
VC8	-/-	---	---

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.

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

ATM Interface

Clicking on the ATM VC brings up the following screen. The router uses ATM as its WAN interface. Protocols including I483 Routing, I483 Bridging, MAC Encapsulated Routing (MER), PPPoA and PPPoE with LLC-SNAP and VC-MUX encapsulations are supported for each ATM PVC.

The screenshot shows the 'ATM Interface' configuration page. The left-hand menu includes: SETUP WIZARD, SYSTEM, WAN, » ATM PVC, » Clone MAC Address, LAN, WIRELESS, NAT, ROUTE, FIREWALL, SNMP, ADSL, VoIP, UPnP, QoS, DDNS, USB, TOOLS, and STATUS. The main configuration area is titled 'ATM Interface' and is for the 'atm0' interface. The settings are as follows:

Protocol	PPPoE
VPI/VCI	8 / 35
Encapsulation	LLC
QoS Class	UBR
PCR/SCR/MBS	4000 / 3980 / 10
IP assigned by ISP	Yes
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Connect Type	Always Connected
Idle Time (Minute)	0
Username	iinetbob
Password
Confirm Password
MTU	1492
MRU	1492
Enable NAT	<input type="checkbox"/>

At the bottom of the form are links for HELP, SAVE SETTINGS, and CANCEL.

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 below for a description of the parameters.

Parameter Description

Protocol

- 1. Disable:** Disables the connection
- 2. I483 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
- 3. PPPoA:** Point-to-Point Protocol over ATM is a method of encapsulating data for transmission to a far point
- 4. I483 Routing:** I483 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 router at the head end)

5. PPPoE: Point-to-Point over Ethernet is a common connection method used for xDSL

6. MAC Encapsulated Routing: If your ADSL service is a Bridged mode service and you want to share the connection to multiple PCs, please select MAC Encapsulated Routing. MER is a protocol that allows you to 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.

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

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.

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.

The screenshot shows the iinet router's web interface. At the top left is the iinet logo with the tagline 'connect better' and contact information: www.iinet.net.au, support - 132298, and email support - support@iinet.net.au. On the top right, it says 'ADVANCED SETUP' with 'Home' and 'Logout' links. A vertical sidebar on the left contains a menu with items: SETUP WIZARD, SYSTEM, WAN, ATM PVC, Clone MAC Address (highlighted), LAN, WIRELESS, NAT, ROUTE, FIREWALL, SNMP, ADSL, VoIP, UPnP, QoS, DDNS, USB, TOOLS, and STATUS. The main content area is titled 'Clone MAC Address' and contains the following text: 'Some ISPs require you to register your MAC address with them. If you have done this, the MAC address of the Gateway must be changed to the MAC address that you supplied to your ISP.' Below this, it says 'WAN Interface MAC Address:' followed by three radio button options: 'Use the Gateway's default MAC address' (selected), 'Use this PC's MAC address:(00:00:00:00:00:00)', and 'Enter a new MAC address manually:([] : [] : [] : [] : [] : [])'. At the bottom right of the main area are links for 'HELP', 'SAVE SETTINGS', and 'CANCEL'.

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

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

LAN

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

The screenshot displays the 'LAN Settings' configuration page in the iinet BoB interface. The left sidebar contains a navigation menu with options like SETUP WIZARD, SYSTEM, WAN, LAN, VLAN, DHCP Client Lists, WIRELESS, NAT, ROUTE, FIREWALL, SNMP, ADSL, VoIP, UPnP, QoS, DDNS, USB, TOOLS, and STATUS. The main content area is titled 'LAN Settings' and includes a brief explanation of DHCP and VLAN Binding. Below this, there are four main configuration sections: 'LAN IP' with input fields for IP Address (10.1.1.1), IP Subnet Mask (255.255.255.0), Host Name, and a radio button for DHCP Server (Enabled); 'VLAN Binding' with dropdown menus for LAN1-4 and WLAN-1-2, all set to 'Default'; 'DHCP Server' with a text field for DHCP Option 60 Vendor ID and a dropdown for Lease Time (One Day); and 'IP Address Pool' with input fields for Address Pool Start IP (10.1.1.2), Address Pool End IP (10.1.1.254), and Domain Name (iinetBoB).

Parameter Description

LAN IP

IP Address: The IP address of the router

IP Subnet Mask: The subnet mask of the router

Host Name: If your ISP requires a hostname specified enter it here, otherwise leave blank

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'.

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 router in the client address pool (see 'TCP/IP Configuration'). If you attempt to include the 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

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

VLAN

VLAN

VLANs are organized and controlled by VLAN Profiles. Up to 4 VLAN profiles can be created. Once a VLAN profile is created, it is empty and user should add interfaces into the VLAN by changing the VLAN setting of that interface. Please note that only those interfaces of IEEE 802 bridging type (ex. LAN ports and 1483 Bridging PVCs) can be added to a VLAN.

- VLAN Table (up to 4 rules):

No.	VLAN	Grouped Interfaces	Configure
1	Default	WLAN1,WLAN2,LAN1,LAN2,LAN3,LAN4	Edit

Add VLAN

- VLAN Access Control:

VLAN	Default
Default	

HELP | SAVE SETTINGS | CANCEL

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

Enter parameters of the profile to define a VLAN.

Description	
IP Address	
Subnet Mask	255 255 255 0
IGMP Snooping	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

HELP | SAVE SETTINGS | CANCEL

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

Description: detailed 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 NAT 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 flow-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.

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

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 Clients 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.

No	IP Address	Host Name	MAC Address	Client Type	Fix	Configure
1	10.1.1.2		00-22-fc-5c-e8-08	Wireless	<input type="checkbox"/>	Release

Note: Only clients that have requested an IP address since the Router's last reboot and fixed associations are displayed in this list. Check *Fix* to fix an existing address, or click *New* to allocate an IP address to a MAC address. The maximum number of fixed associations is 10. The Client Type field of fixed association entry is displayed as *Wireless* if it is for a wireless client, otherwise, it might be a wired client or even not connected.

[New](#) [HELP](#) [Cancel](#) [Refresh](#)

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 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 router.

The router supports two wireless SSID's, to enable the second SSID place a tick in the 'Secondary Wireless Module' and click 'SAVE SETTINGS'.

Wireless Settings

This modem supports dual SSID (wireless signals), the primary and secondary SSID. If the 'enable or disable wireless function' is disabled then both SSIDs will cease to broadcast.

• Enable or disable Wireless function : Enable Disable

Enabled secondary Wireless SSID

[HELP](#) [SAVE SETTINGS](#) [CANCEL](#)

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

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 I, 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: I-13)

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 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.

The screenshot shows the 'Channel and SSID' configuration page in the iinet router's web interface. The page title is 'Channel and SSID' and it includes a sub-header: 'This page allows you to define SSID and Channel ID for wireless connection. In the wireless environment, the router can also act as an wireless access point. These parameters are used for the mobile stations to connect to this access point.' The configuration fields are as follows:

Primary	WLAN1	Hide: <input type="checkbox"/>
Secondary	WLAN2	Hide: <input type="checkbox"/>
Wireless Mode	802.11n only	
Channel	Auto	
Bandwidth	20MHz/40MHz	
Control SideBand	Upper	

At the bottom right, there are buttons for 'HELP', 'SAVE SETTINGS', and 'CANCEL'.

See the description of the parameters below.

Parameter Description

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

Show or hide the broadcasting of the SSID. Show SSID broadcasting on the wireless network for easy connection with client PCs

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

Wireless Mode: This device supports IIn, IIg and IIb wireless networks. Make your selection depending on the type of wireless network that you have. (Default: 802 IIn + 802 IIg + 802 IIb)

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 router and all of its wireless clients. (Default: 6)

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

Wireless 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 router.

Wireless Access Control

For a more secure Wireless network you can specify that only certain Wireless PCs can connect to the Access Point. Up to 32 MAC addresses can be added to the MAC Filtering Table. When enabled, all registered MAC addresses are controlled by the Access Rule.

- Enable MAC Filtering: Enable Disable
- Access Rule for registered MAC address: Allow Deny
- MAC Filtering Table (up to 32 stations):

ID	MAC Address
1	00 : 00 : 00 : 00 : 00 : 00
2	00 : 00 : 00 : 00 : 00 : 00
3	00 : 00 : 00 : 00 : 00 : 00
4	00 : 00 : 00 : 00 : 00 : 00
5	00 : 00 : 00 : 00 : 00 : 00
6	00 : 00 : 00 : 00 : 00 : 00
7	00 : 00 : 00 : 00 : 00 : 00
8	00 : 00 : 00 : 00 : 00 : 00
9	00 : 00 : 00 : 00 : 00 : 00
10	00 : 00 : 00 : 00 : 00 : 00
11	00 : 00 : 00 : 00 : 00 : 00
12	00 : 00 : 00 : 00 : 00 : 00
13	00 : 00 : 00 : 00 : 00 : 00
14	00 : 00 : 00 : 00 : 00 : 00
15	00 : 00 : 00 : 00 : 00 : 00
16	00 : 00 : 00 : 00 : 00 : 00
17	00 : 00 : 00 : 00 : 00 : 00

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).

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

Security

It is important to be aware of security issues, especially when using wireless. You can configure your security settings on this page. You can set security on one SSID or both, select the appropriate SSID from the 'Select Virtual AP' drop down box.

The screenshot shows the iinet router's web interface. The top left has the iinet logo and contact information. The top right shows 'ADVANCED SETUP', 'Home', and 'Logout'. A left-hand navigation menu lists various settings: SETUP WIZARD, SYSTEM, WAN, LAN, WIRELESS (selected), Channel and SSID, Access Control, Security, WDS, NAT, ROUTE, FIREWALL, SNMP, ADSL, VoIP, UPnP, QoS, DDNS, USB, TOOLS, and STATUS. The main 'Security' section contains the following text: 'The router can transmit your data securely over the wireless network. Matching security mechanisms must be setup on your router and wireless client devices. You can choose the allowed security mechanisms in this page and configure them in the sub-pages. WPA2 is the strongest encryption method and is recommended, in order to use WPA2 you will need to ensure all your wireless clients and Operating Systems are compatible with WPA2 protocol. Microsoft Windows users: For more information see knowledge base article 893357. Apple MAC OS users: For more information see knowledge base article 304821.' Below this text is a 'Select Virtual AP:' dropdown menu with 'WLAN' selected. Underneath is the 'Allowed Client Type:' section with radio buttons for 'WPA/WPA2', 'WPA2 Only', 'WPA Only', 'WEP', and 'Disabled' (which is selected). At the bottom right are buttons for 'HELP', 'SAVE SETTINGS', and 'CANCEL'.

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

For a more secure network, the 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. Some wireless cards may not support this, please check with the wireless card's manufacturer.

WPA2: Requires WPA2 enabled system and network card. Some wireless cards may not support this, please check with the wireless card's manufacturer.

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

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.

The screenshot shows the iinet router's web interface for the 'Security' section. The left sidebar contains a navigation menu with options like 'SETUP WIZARD', 'SYSTEM', 'WAN', 'LAN', 'WIRELESS', 'NAT', 'ROUTE', 'FIREWALL', 'SNMP', 'ADSL', 'VoIP', 'UPnP', 'QoS', 'DDNS', 'USB', 'TOOLS', and 'STATUS'. The main content area is titled 'Security' and includes a description of WEP, a 'Select Virtual AP' dropdown set to 'WLAN', and radio buttons for 'Allowed Client Type' (WPA/WPA2, WPA2 Only, WPA Only, WEP, Disabled). Below this are fields for 'WEP Mode' (64 bit, 128 bit), 'Key Entry Method' (HEX, ASCII), and 'Key Provisioning' (Static, Dynamic). There are four 'Key' input fields, each containing the value '1234567890123', and a 'Default Key ID' dropdown set to '1'. A 'Passphrase' checkbox is also present. At the bottom right, there are buttons for 'HELP', 'SAVE SETTINGS', and 'CANCEL'.

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.

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

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 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.

The screenshot shows the iinet router's Advanced Setup interface. The left sidebar contains a navigation menu with categories: SETUP WIZARD, SYSTEM, WAN, LAN, WIRELESS, NAT, ROUTE, FIREWALL, SNMP, ADSL, VoIP, UPnP, QoS, DDNS, USB, TOOLS, and STATUS. The 'WIRELESS' section is expanded to show 'Channel and SSID', 'Access Control', and 'Security'. The 'Security' page is titled 'Security' and contains the following information:

- Header: **Security**
- Text: "The router can transmit your data securely over the wireless network. Matching security mechanisms must be setup on your router and wireless client devices. You can choose the allowed security mechanisms in this page and configure them in the sub-pages."
- Text: "WPA2 is the strongest encryption method and is recommended, in order to use WPA2 you will need to ensure all your wireless clients and Operating Systems are compatible with WPA2 protocol. Microsoft Windows users: For more information see knowledge base article 893357. Apple MAC OS users: For more information see knowledge base article 304821."
- Form field: "Select Virtual AP: WLAN" (dropdown menu)
- Form field: "Allowed Client Type: WPA/WPA2 WPA2 Only WPA Only WEP Disabled"
- Form field: "Authentication: 802.1X Pre-shared Key"
- Form field: "Pre-shared key type: Passphrase (8~63 characters) Hex (64 digits)"
- Form field: "Pre-shared Key: [input field] [checkbox]"
- Buttons: [HELP](#), [SAVE SETTINGS](#), [CANCEL](#)

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: for an enterprise network with a RADIUS server installed.
- Pre-shared Key: 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.

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

WDS

Wireless Distribution System (WDS) provides a means to extend the range of a Wireless Local Area Network (WLAN). WDS allows an Access Point (AP) to establish a direct link to other APs and allows stations to roam freely within the area covered by the WDS.

The screenshot shows the iinet router's web interface for the WDS configuration. The page title is "WDS". The left sidebar contains a navigation menu with categories: SETUP WIZARD, SYSTEM, WAN, LAN, WIRELESS, NAT, ROUTE, FIREWALL, SNMP, ADSL, VoIP, UPnP, QoS, DDNS, USB, TOOLS, and STATUS. The "WIRELESS" category is expanded, showing sub-items: Channel and SSID, Access Control, Security, and WDS. The "WDS" sub-item is selected. The main content area includes the iinet logo and contact information (www.iinet.net.au, support - 132298, email support - support@iinet.net.au) in the top left, and "ADVANCED SETUP" with "Home" and "Logout" links in the top right. The main content area contains the following text: "The Wireless Distribution System (WDS) provides a means to extend the range of a Wireless Local Area Network (WLAN). WDS allows an Access Point (AP) to establish a direct link to other APs and to allows stations to roam freely within the area covered by the WDS." Below this text is a checkbox labeled "Enable WDS Function" which is currently unchecked. Underneath is a section titled "AP MAC Address Table (up to 4 APs):" followed by a table with two columns: "SSID" and "MAC Address". The table is currently empty. A "Rescan" button is located below the table. At the bottom right of the main content area are three buttons: "HELP", "SAVE SETTINGS", and "CANCEL".

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.

The screenshot shows the iinet router's web interface for the NAT Settings configuration. The page title is "NAT Settings". The left sidebar contains a navigation menu with categories: SETUP WIZARD, SYSTEM, WAN, LAN, WIRELESS, NAT, ROUTE, FIREWALL, SNMP, ADSL, VoIP, UPnP, QoS, DDNS, USB, TOOLS, and STATUS. The "NAT" category is expanded, showing sub-items: Address Mapping, Port Forwarding, Special Applications, and NAT Mapping Table. The "NAT" sub-item is selected. The main content area includes the iinet logo and contact information (www.iinet.net.au, support - 132298, email support - support@iinet.net.au) in the top left, and "ADVANCED SETUP" with "Home" and "Logout" links in the top right. The main content area contains the following text: "Network Address Translation (NAT) allows multiple users at your local site to access the Internet through a single public IP address or multiple public IP addresses. NAT can also prevent hacker attacks by mapping local addresses to public addresses for key services such as the Web or FTP." Below this text is a section titled "Enable or disable NAT module function :" followed by two radio buttons: "Enable" (which is selected) and "Disable". At the bottom right of the main content area is a button labeled "SAVE SETTINGS".

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.

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

Address Mapping

The screenshot displays the iinet BoB™ Advanced Setup Method web interface. The page title is "Address Mapping". On the left is a navigation menu with categories: SETUP WIZARD, SYSTEM, WAN, LAN, WIRELESS, NAT (expanded to show Address Mapping, Port Forwarding, and NAT Mapping Table), ROUTE, FIREWALL, SNMP, ADSL, VoIP, UPnP, QoS, DDNS, USB, TOOLS, and STATUS. The main content area includes the iinet logo and contact information (www.iinet.net.au, support - 132258, email support - support@iinet.net.au) and navigation links (ADVANCED SETUP, Home, Logout). Below the title is a descriptive paragraph: "Network Address Translation (NAT) allows IP addresses used in a private local network to be mapped to one or more addresses used in the public, global Internet. This feature limits the number of public IP addresses required from the ISP and also maintains the privacy and security of the local network. We allow one or more than one public IP address to be mapped to a pool of local addresses." The main configuration area is titled "Address Mapping" and contains 10 rows, each representing a mapping rule. Each row has a "Global IP" field with four input boxes (all set to 0), a description "is transformed as multiple virtual IPs", and a "from" field with four input boxes (all set to 0) and a "to" field with four input boxes (all set to 0).

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.

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

Port Forwarding

Port Forwarding

You can configure the router as a virtual server so that remote users accessing services such as the 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 router redirects the external service request to the appropriate server (located at another internal IP address). This tool can support both port ranges and single port.

Add [Application]
Clear entry [1]
Wan Interface [pppoe_atm0/ppp0]

Enable	Description	Wan Interface	Inbound port	Type	Private IP address	Private port
<input type="checkbox"/>		pppoe_atm0/ppp0		TCP	10.1.1.	
<input type="checkbox"/>		pppoe_atm0/ppp0		TCP	10.1.1.	
<input type="checkbox"/>		pppoe_atm0/ppp0		TCP	10.1.1.	
<input type="checkbox"/>		pppoe_atm0/ppp0		TCP	10.1.1.	
<input type="checkbox"/>		pppoe_atm0/ppp0		TCP	10.1.1.	
<input type="checkbox"/>		pppoe_atm0/ppp0		TCP	10.1.1.	
<input type="checkbox"/>		pppoe_atm0/ppp0		TCP	10.1.1.	
<input type="checkbox"/>		pppoe_atm0/ppp0		TCP	10.1.1.	
<input type="checkbox"/>		pppoe_atm0/ppp0		TCP	10.1.1.	
<input type="checkbox"/>		pppoe_atm0/ppp0		TCP	10.1.1.	
<input type="checkbox"/>		pppoe_atm0/ppp0		TCP	10.1.1.	
<input type="checkbox"/>		pppoe_atm0/ppp0		TCP	10.1.1.	
<input type="checkbox"/>		pppoe_atm0/ppp0		TCP	10.1.1.	
<input type="checkbox"/>		pppoe_atm0/ppp0		TCP	10.1.1.	
<input type="checkbox"/>		pppoe_atm0/ppp0		TCP	10.1.1.	
<input type="checkbox"/>		pppoe_atm0/ppp0		TCP	10.1.1.	
<input type="checkbox"/>		pppoe_atm0/ppp0		TCP	10.1.1.	
<input type="checkbox"/>		pppoe_atm0/ppp0		TCP	10.1.1.	
<input type="checkbox"/>		pppoe_atm0/ppp0		TCP	10.1.1.	
<input type="checkbox"/>		pppoe_atm0/ppp0		TCP	10.1.1.	
<input type="checkbox"/>		pppoe_atm0/ppp0		TCP	10.1.1.	

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 router redirects the external service request to the appropriate server (located at another internal IP address).

There is a list of commonly used applications and their associated port(s), to add an application to the Port Forwarding list simply select the desired application and click 'Add'.

The more common TCP service ports include: HTTP: 80, FTP: 21, Telnet: 23, and POP3: 110.

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.

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

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.

Special Applications

Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications cannot work when Network Address Translation (NAT) is enabled. If you need to run applications that require multiple connections, specify the port normally associated with an application in the "Trigger Port" field, select the protocol type as TCP or UDP, then enter the public ports associated with the trigger port to open them for inbound traffic.

Note: The range of the Trigger Ports is from 1 to 65535.

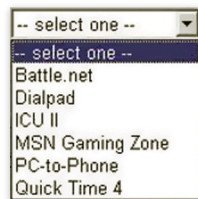
	Trigger Port	Trigger Type	Public Port	Public Type	Wan Interface	Enabled
1.	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	pppoe_atm0/ppp0	<input type="checkbox"/>
2.	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	pppoe_atm0/ppp0	<input type="checkbox"/>
3.	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	pppoe_atm0/ppp0	<input type="checkbox"/>
4.	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	pppoe_atm0/ppp0	<input type="checkbox"/>
5.	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	pppoe_atm0/ppp0	<input type="checkbox"/>
6.	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	pppoe_atm0/ppp0	<input type="checkbox"/>
7.	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	pppoe_atm0/ppp0	<input type="checkbox"/>
8.	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	pppoe_atm0/ppp0	<input type="checkbox"/>
9.	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	pppoe_atm0/ppp0	<input type="checkbox"/>
10.	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	pppoe_atm0/ppp0	<input type="checkbox"/>

Popular applications:

[HELP](#) [SAVE SETTINGS](#) [CANCEL](#)

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

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

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

NAT Mapping Table

iinet connect better
www.iinet.net.au
support - 132258
email support - support@iinet.net.au

ADVANCED SETUP [Home](#) [Logout](#)

NAT Mapping Table

NAT Mapping Table displays the current NAPT address mappings.

Index	Protocol	Source IP	Source Port	Pseudo IP	Pseudo Port	Destination IP	Destination Port
1	TCP	10.1.1.11	3230	203.59.255.162	3230	65.55.202.157	443
2	OTHER	203.13.74.144	22748	203.59.255.162	22748	203.59.255.162	80
3	OTHER	203.13.74.144	22835	203.59.255.162	22835	203.59.255.162	80
4	OTHER	203.13.74.144	23809	203.59.255.162	23809	203.59.255.162	80
5	OTHER	203.13.74.144	22785	203.59.255.162	22785	203.59.255.162	80
6	OTHER	203.13.74.144	23013	203.59.255.162	23013	203.59.255.162	80
7	OTHER	203.13.74.144	22848	203.59.255.162	22848	203.59.255.162	80
8	OTHER	203.13.74.144	22753	203.59.255.162	22753	203.59.255.162	80
9	OTHER	10.1.1.11	3320	203.59.255.162	3320	65.55.202.157	443
10	OTHER	203.59.255.162	53	203.59.255.162	53	203.0.178.191	53
11	OTHER	203.13.74.144	23119	203.59.255.162	23119	203.59.255.162	80
12	OTHER	203.13.74.144	23217	203.59.255.162	23217	203.59.255.162	80
13	OTHER	203.13.74.144	23517	203.59.255.162	23517	203.59.255.162	80
14	OTHER	203.13.74.144	23512	203.59.255.162	23512	203.59.255.162	80
15	OTHER	203.13.74.144	23015	203.59.255.162	23015	203.59.255.162	80
16	OTHER	203.13.74.144	23069	203.59.255.162	23069	203.59.255.162	80
17	OTHER	203.13.74.144	23096	203.59.255.162	23096	203.59.255.162	80
18	OTHER	203.13.74.144	23032	203.59.255.162	23032	203.59.255.162	80
19	OTHER	10.1.1.11	3235	203.59.255.162	3235	65.55.202.157	443
20	OTHER	203.13.74.144	23511	203.59.255.162	23511	203.59.255.162	80

Page: 1/2

[|<<](#) [>](#) [>>|](#) [Refresh](#) [HELP](#)

NAT Mapping Table displays the current NAPT address mappings 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

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

Route

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

Static Route Parameters

www.iinet.net.au
support - 132258
email support - support@iinet.net.au

ADVANCED SETUP Home Logout

Static Route Parameter

Please Enter the Following Configuration Parameters:

Index	Network Address	Subnet Mask	Gateway	Configure
1				N/A

HELP | SAVE SETTINGS | CANCEL

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.

www.iinet.net.au
support - 132258
email support - support@iinet.net.au

ADVANCED SETUP Home Logout

Static Route Parameter

Please Enter the Following Configuration Parameters:

Index	Network Address	Subnet Mask	Gateway	Configure
1				N/A

No Valid Static Route Entry !!!

Add

HELP | SAVE SETTINGS | CANCEL

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.

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

RIP Parameter

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

The screenshot shows the iinet BoB™ Advanced Setup Method interface. The left sidebar contains a navigation menu with options: SETUP WIZARD, SYSTEM, WAN, LAN, WIRELESS, NAT, ROUTE, Static Route, RIP, Routing Table, FIREWALL, SNMP, ADSL, VoIP, UPnP, QoS, DDNS, USB, TOOLS, and STATUS. The main content area is titled "RIP Parameter" and includes the following text: "The device supports Routing Information Protocol (RIP) v1 and v2 to dynamically exchange routing information with adjacent routers. Please Enter the following Configuration Parameters:"

General RIP parameter:

- RIP mode: Enable Disable
- Auto summary: Enable Disable

Table of current interface RIP parameter:

Interface	Operation Mode	Version	Poison Reverse	Authentication Required	Authentication Code
LAN1	Silent	2	Enable	None	*****

At the bottom right of the configuration area, there are buttons for HELP, SAVE SETTINGS, and CANCEL.

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-bit message 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.

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

Routing Table

The screenshot shows the iinet BoB™ Advanced Setup Method interface. The left sidebar contains a navigation menu with the following items: SETUP WIZARD, SYSTEM, WAN, LAN, WIRELESS, NAT, ROUTE, Static Route, RIP, Routing Table, FIREWALL, SNMP, ADSL, VoIP, UPnP, QoS, DDNS, USB, TOOLS, and STATUS. The main content area is titled "Routing Table" and includes the following information:

www.iinet.net.au
support - 132256
email support - support@iinet.net.au

ADVANCED SETUP [Home](#) [Logout](#)

Routing Table

• List Routing Table:

Flags	Network Address	Netmask	Gateway	Interface	Metric
UH	203.59.14.16	255.255.255.255	0.0.0.0	ppp0	0
U	10.1.1.0	255.255.255.0	0.0.0.0	br0	0
U	0.0.0.0	0.0.0.0	0.0.0.0	ppp0	0

Flags: U - up, I - reject, G - gateway, H - host, R - reinstate
D - dynamic (redirect), M - modified (redirect).

[HELP](#)

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 I to the metric value indicated in the update and enters the network in the routing table.

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

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.

Security Settings (Firewall)

The screenshot displays the 'Security Settings (Firewall)' configuration page. On the left is a vertical sidebar menu with orange buttons for various settings: SETUP WIZARD, SYSTEM, WAN, LAN, WIRELESS, NAT, ROUTE, FIREWALL, Access Control, MAC Filter, URL Blocking, Schedule Rule, Intrusion Detection, DMZ, SNMP, ADSL, VoIP, UPnP, QoS, DDNS, USB, TOOLS, and STATUS. The main content area has a header with the iinet logo and contact information (www.iinet.net.au, support - 132258, email support - support@iinet.net.au) and navigation links for ADVANCED SETUP, Home, and Logout. The title 'Security Settings (Firewall)' is centered. Below the title is a descriptive paragraph: 'The Device provides extensive firewall protection by restricting connection parameters to limit the risk of hacker attack, and defending against a wide array of common attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server as a demilitarized zone (DMZ)'. Below this is a radio button group for 'Enable or disable firewall' with 'Enable' selected. A 'Firewall Level' dropdown menu is set to 'High Level'. A 'SAVE SETTINGS' button is located at the bottom right of the main content area.

The 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.

You can select a pre-defined firewall level from the drop down list. Available options are High, Medium, Low Level & User Defined. Select User Defined to manually adjust the firewall settings.

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

Access Control

iinet connect better
www.iinet.net.au
support - 132258
email support - support@iinet.net.au

ADVANCED SETUP [Home](#) [Logout](#)

Access Control

Access Control allows users to define the traffic type permitted or not-permitted to WAN port service. To add a rule, click **Add PC** then select the type of traffic you want to block. To block specific times, you will need to create a rule first by selecting **Schedule Rule** from the menu on the left.

- Enable Filtering Function : Enable Disable
- Normal Filtering Table (up to 10 computers):

Rule Description	Client PC IP Address	Client Service	Schedule Rule	Configure
No Valid Filtering Rule !!!				
Add PC				

[HELP](#) | [SAVE SETTINGS](#) | [CANCEL](#)

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 router can also limit the access of hosts within the local area network (LAN). The MAC Filtering Table allows the 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.

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.

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

Access Control Add PC

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

Access Control Add PC

This page allows users to define service limitations of client PCs, including IP address, service type and scheduling rule criteria. For the URL blocking function, you need to configure the URL address first on the [URL Blocking](#) page. For the scheduling function, you also need to configure the schedule rule first on the [Schedule Rule](#) page.

- Client PC Description :
- Client PC IP Address : .undefined.undefined. ~
- Client PC Service:

Service Name	Detail Description	Blocking
WWW	HTTP, TCP Port 80, 3128, 8000, 8001, 8080	<input type="checkbox"/>
WWW with URL Blocking	HTTP (Ref. URL Blocking Site Page)	<input type="checkbox"/>
E-mail Sending	SMTP, TCP Port 25	<input checked="" type="checkbox"/>
News Forums	NNTP, TCP Port 119	<input type="checkbox"/>
E-mail Receiving	POP3, TCP Port 110	<input checked="" type="checkbox"/>
Secure HTTP	HTTPS, TCP Port 443	<input type="checkbox"/>
File Transfer	FTP, TCP Port 21	<input type="checkbox"/>
Telnet Service	TCP Port 23	<input type="checkbox"/>
AIM	AOL Instant Messenger, TCP Port 5190	<input type="checkbox"/>
NetMeeting	H.323, TCP Port 1720, 1503	<input type="checkbox"/>
DNS	UDP Port 53	<input type="checkbox"/>
SNMP	UDP Port 161, 162	<input type="checkbox"/>
VPN-PPTP	TCP Port 1723	<input type="checkbox"/>
VPN-L2TP	UDP Port 1701	<input type="checkbox"/>
TCP	All TCP Port	<input type="checkbox"/>
UDP	All UDP Port	<input type="checkbox"/>

User Define Service: Protocol: TCP UDP
Port Range: ~ , ~ , ~

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.

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

MAC Filter

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

MAC Filtering Table

This section helps provide MAC Filter configuration. When enabled, only MAC addresses configured will have access to your network. All other client devices will get denied access. This security feature can support up to 32 devices and applies to clients.

- MAC Address Control: Enable Disable
- MAC Filtering Table (up to 32 computers):

ID	MAC Address
1	..:..:..:..:..:..
2	..:..:..:..:..:..
3	..:~:~:~:~:~:~
4	..:..:..:..:..:..
5	..:..:..:..:..:..
6	..:..:..:..:..:..
7	..:..:..:..:..:..
8	..:..:..:..:..:..
9	..:..:..:..:..:..
10	..:..:..:..:..:..
11	..:..:..:..:..:..
12	..:..:..:..:..:..
13	..:..:..:..:..:..
14	..:..:..:..:..:..
15	..:..:..:..:..:..
16	..:..:..:..:..:..
17	..:..:..:..:..:..
18	..:..:..:..:..:..
19	..:..:..:..:..:..

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

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

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.

URL Blocking
Disallowed Web Sites and Keywords.

You can block access to certain Web sites from a particular PC by entering either a full URL address or just a keyword of the Web site.

To specify the particular PC, go back to the "Access Control" page and check the box for "Http with URL Blocking" in the "Normal Filtering Table".

Rule Number	URL / Keyword	Rule Number	URL / Keyword
Site 1		Site 16	
Site 2		Site 17	
Site 3		Site 18	
Site 4		Site 19	
Site 5		Site 20	
Site 6		Site 21	
Site 7		Site 22	
Site 8		Site 23	
Site 9		Site 24	
Site 10		Site 25	
Site 11		Site 26	
Site 12		Site 27	
Site 13		Site 28	
Site 14		Site 29	
Site 15		Site 30	

[Clear All](#)

[HELP](#) | [SAVE SETTINGS](#) | [CANCEL](#)

The 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.

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

Schedule Rule

inet www.inet.net.au
support - 132258
email support - support@inet.net.au

ADVANCED SETUP Home Logout

Schedule Rule

This page defines schedule rule names and activates the schedule for use in the [Access Control](#) page. To create a new schedule, click **Add Schedule Rule**.

- Schedule Rule Table (Up to 10 rules):

Rule Name	Rule Comment	Configure
No Valid Schedule Rule !!!		
Add Schedule Rule		

[HELP](#) | [SAVE SETTINGS](#) | [CANCEL](#)

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.

inet www.inet.net.au
support - 132258
email support - support@inet.net.au

ADVANCED SETUP Home Logout

Add Schedule Rule

Please specify a name for this rule and add the times you wish the [Access Control](#) rules to run. Add times are to be added in 24 hour time(00:00-23:59).

- Name :
- Comment :
- Activate Time Period:

Week Day	Start Time (hh:mm)	End Time (hh:mm)
Every Day	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Sunday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Monday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Tuesday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Wednesday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Thursday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Friday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>
Saturday	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>

[SAVE SETTINGS](#) | [Cancel](#)

Define the appropriate settings for a schedule rule (as shown on the above screen). The rule in the screen shot above prohibits emailing after 3.00pm to 11.00pm. Upon completion, click 'OK' to save your schedule rules.

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

Intrusion Detection

The 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.

Intrusion Detection

When the SPI (Stateful Packet Inspection) firewall feature is enabled, all packets can be blocked. Stateful Packet Inspection (SPI) allows full support of different application types that are using dynamic port numbers. For the applications checked in the list below, the Device will support full operation as initiated from the local LAN.

The Device firewall can block common hacker attacks, including IP Spoofing, TCP SYN flood attack, FIN/URG/PSH attack, Ping attack, Xmas Tree attack, TCP reset attack, Null scanning attack, Ping of Death attack, SYN/RST SYN/FIN attack.

- Intrusion Detection Feature**

SPI and Anti-DoS firewall protection	<input checked="" type="checkbox"/>
RIP defect	<input checked="" type="checkbox"/>
Discard Ping To WAN Interface	<input type="checkbox"/>

- Stateful Packet Inspection**

TCP Connection	<input checked="" type="checkbox"/>
UDP Session	<input checked="" type="checkbox"/>
FTP Service	<input checked="" type="checkbox"/>
H.323 Service	<input checked="" type="checkbox"/>
TFTP Service	<input checked="" type="checkbox"/>

- DoS Detect Criteria:**

TCP SYN flood attack	<input checked="" type="checkbox"/>
FIN/URG/PSH attack	<input checked="" type="checkbox"/>
Ping attack	<input checked="" type="checkbox"/>
Xmas Tree attack	<input checked="" type="checkbox"/>
TCP reset attack	<input checked="" type="checkbox"/>
Null scanning attack	<input checked="" type="checkbox"/>
Ping of Death attack	<input checked="" type="checkbox"/>
SYN/RST SYN/FIN attack	<input checked="" type="checkbox"/>
IP Spoofing attack	<input checked="" type="checkbox"/>

• When hackers attempt to enter your network, we can alert you by e-mail

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 it.

The 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.

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 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, 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; 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.

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

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.

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: 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

DMZ (Demilitarized Zone)

If you have a local client PC that cannot run an Internet application properly from behind the NAT firewall, then you can open the client up to unrestricted two-way Internet access by defining a Virtual DMZ Host.

- Enable DMZ: Enable Disable
- Multiple PCs can be exposed to the Internet for two-way communications e.g. Internet gaming, video conferencing, or VPN connections. To use the DMZ, you must set a static IP address for that PC.

	Public IP Address	Client PC IP Address
1.	203.59.255.162	10.1.1.0
2.	0 . 0 . 0 . 0	10.1.1.0
3.	0 . 0 . 0 . 0	10.1.1.0
4.	0 . 0 . 0 . 0	10.1.1.0
5.	0 . 0 . 0 . 0	10.1.1.0
6.	0 . 0 . 0 . 0	10.1.1.0
7.	0 . 0 . 0 . 0	10.1.1.0
8.	0 . 0 . 0 . 0	10.1.1.0

[HELP](#) | [SAVE SETTINGS](#) | [CANCEL](#)

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.

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

SNMP

www.iinet.net.au
support - 132258
email support - support@iinet.net.au

ADVANCED SETUP Home Logout

SETUP WIZARD
SYSTEM
WAN
LAN
WIRELESS
NAT
ROUTE
FIREWALL
SNMP
» Community
» Trap
ADSL
VoIP
UPnP
QoS
DDNS
USB
TOOLS
STATUS

SNMP Setting

The Device provides SNMP setting for community and trap information.

Please select one of the SNMP Operation Modes for this device.

SNMP Operation Mode:

SAVE SETTINGS

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

www.iinet.net.au
support - 132258
email support - support@iinet.net.au

ADVANCED SETUP Home Logout

SETUP WIZARD
SYSTEM
WAN
LAN
WIRELESS
NAT
ROUTE
FIREWALL
SNMP
» Community
» Trap
ADSL
VoIP
UPnP
QoS
DDNS
USB
TOOLS
STATUS

SNMP Community

In the context of SNMP, a relationship between an agent and a set of SNMP managers defines security characteristics. The community concept is a local one, defined at the agent. The agent establishes one community for each desired combination of authentication, access control, and proxy characteristics. Each community is given a unique (within this agent) community name, and the management stations within that community are provided with and must employ the community name in all get operations. The agent may establish a number of communities, with overlapping management station membership.

No.	Community	Access	Valid
1	public	Read	<input checked="" type="checkbox"/>
2	private	Write	<input type="checkbox"/>
3		Read	<input type="checkbox"/>
4		Read	<input type="checkbox"/>
5		Read	<input type="checkbox"/>

HELP | SAVE SETTINGS | CANCEL

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 router, the NMS must first submit a valid community string for authentication.

Parameter	Description
Community	A Community name authorised 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

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

Trap

No.	IP Address	Community	Version
1	0 . 0 . 0 . 0		Disabled
2	0 . 0 . 0 . 0		Disabled
3	0 . 0 . 0 . 0		Disabled
4	0 . 0 . 0 . 0		Disabled
5	0 . 0 . 0 . 0		Disabled

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

• Operation Mode:
ADSL-Standard:

We recommend leaving the Operation Mode at the default Automatic setting unless you are 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+)
- G.922.5 (ADSL2+M)

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

Status

The Status page displays ADSL status information

Monitoring Index:

- ADSL Status Information:
 - Status
 - Data Rate Information
 - Defect/Failure Indication
 - Statistics
- Status:

	Configured	Current
--	------------	---------
- Line Status:

	Automatic	Up
--	-----------	----
- Link Type:

	Automatic	Automatic
--	-----------	-----------
- Data Rate:

	Upstream	Downstream
Actual Data Rate	1021 (Kbps.)	19550 (Kbps.)
- Operation Data / Defect Indication:

	Upstream	Downstream
Noise Margin	12 dB	7 dB
Attenuation	14 dB	25 dB
- Indicator Name:

	Near End Indicator	Far End Indicator
CRC Error	0	0
HEC Error	0	0
- Statistics:

	Transmitted Cells	Received Cells
Cell Counter	275186	272213

Parameter Description

Status

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

Data Rate:

Downstream: Actual and maximum downstream data rate.

Upstream: Actual and maximum upstream 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

Fast Path FEC: 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 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 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 superframes transmitted Superframes Interleaved.

Received Number of fast super frames received.

Superframes Fast

Transmitted Number of fast super frames transmitted.

Superframes Fast

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

VoIP

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 router on their system so that you can call friends, family and business associates. Your BoB™ - 4 port integrated wireless router comes pre-configured for the iiNet VoIP service. iiNet and Belkin will only provide support for use with the iiNet VoIP service.

www.iinet.net.au
support - 132258
email support - support@iinet.net.au

ADVANCED SETUP [Home](#) [Logout](#)

Port Setting
Select a port to configure. The port's setting will be saved after you press **SAVE SETTINGS** button.

Phone 1	<input checked="" type="checkbox"/> Enable
Phone Number	<input type="text"/>
Display Name	<input type="text"/>
SIP Domain	<input type="text"/>
SIP Server	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>

Phone 2	<input checked="" type="checkbox"/> Enable
Phone Number	<input type="text"/>
Display Name	<input type="text"/>
SIP Domain	<input type="text"/>
SIP Server	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>

[HELP](#) | [SAVE SETTINGS](#) | [CANCEL](#)

See 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).

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

SIP Setting

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

SIP Parameters	
SIP Listen Port	5060
Proxy Setting	Proxy IP: inetphone.iinet.net.au
	Proxy Port: 5060
Registrar Setting	Registrar IP: inetphone.iinet.net.au
	Registrar Port: 5060
Re-Registration Time Interval	1800

SIP, the Session Initiation Protocol, is a signalling 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 has 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 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.

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

VoIP Advanced Setting

Configure the VoIP advanced settings on this page, and click 'OK.'

The screenshot shows the 'VoIP Advanced Setting' page in the iinet web interface. The page is titled 'VoIP Advanced Setting' and includes a navigation menu on the left. The main content area is titled 'VoIP Advanced Setting' and contains several sections:

- Support Call Waiting:**
- Caller-ID Presentation:**
- Support User-Agent Header:**
- Support Out of Band DTMF:**
- Use SRV option for SIP registration:**
- Use SIP ALG option:**
- Call Hold Version:** RFC3264
- Telephony Hook Flash Timer:** 50 ms ~ 250 ms
- Telephony Tone Country Setting:** Australia

Below this is the 'Advanced Call Feature' section:

- Do Not Disturb Enable:**
- Call forwarding number:** [input field]
- Forward unconditionally:**
- Forward on "busy":**
- Forward on "no answer":**

The 'Voice Codec Configuration' section shows a table with 'Available Codecs' and 'Selected Codecs' (G.711 U law, G.711 A law) and 'Up'/'Down' buttons.

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, an 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 router is configured correctly for your provider.

Codec are used to convert an analogue voice signal to digitally encoded version. Codec 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 codec supported by the 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.711 A law
2. G.711 U 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.

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

Port Advanced Setting

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

The screenshot shows the 'Port Advanced Setting' page in the iinet web interface. The left sidebar contains a navigation menu with categories like SETUP WIZARD, SYSTEM, WAN, LAN, WIRELESS, NAT, ROUTE, FIREWALL, SNMP, ADSL, and VoIP. The VoIP section is expanded, showing options for Port Setting, SIP Setting, VoIP Advanced Setting, Port Advanced Setting, Dialing Plans, Quick Dialing Plans, DECT Setting, and VoIP Status and Call Logs. The main content area is titled 'Port Advanced Setting' and includes instructions: 'Enter the related properties for the port to achieve better behavior. The port's setting will be saved after you click SAVE SETTINGS button.' The settings are organized into sections: 'Phone FXS' and 'Phone DECT', each with 'Volume Gain Control' (Input 0 / Output 0), 'VAD' (checked), and 'Inter Digit Delay' (4 Sec). A 'Common Setting(s)' section includes 'T.38 Mode' (checked), 'Caller ID Mode' (unchecked), 'Dial Tone Frequency(Hz)' (425), and 'Australian Dial Tone' (checked). At the bottom right, there are buttons for 'HELP', 'SAVE SETTINGS', and 'CANCEL'.

Volume Gain Control

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

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.

Caller ID Mode

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

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.

T.38 Mode

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

Dial Tone(Hz)

Adjust the pitch of the VoIP dial tone. Dialling Plans Configure the VoIP dialling plans on this page, and click 'SAVE SETTINGS'.

The screenshot shows the 'Dialing Plans' page in the iinet web interface. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Dialing Plans' and includes instructions: 'Select a port to configure. The port's setting will be saved after you press SAVE SETTINGS button.' There is a 'PSTN Override Code' field. Below it is a table with columns 'No.', 'Phone Number', 'ConnectionType', and 'Configure'. The table has one row with '1' in the 'No.' column, an empty 'Phone Number' field, 'Internet' in the 'ConnectionType' dropdown, and an 'Add' button in the 'Configure' column. At the bottom right, there are buttons for 'HELP', 'SAVE SETTINGS', and 'CANCEL'.

Set the Phone Number and Connection Type on this page.

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

DECT Setting

View and configure advanced DECT handset settings such as DECT PIN, register, unregister and page your DECT handset (s).

DECT Setting

The table below describes the Dect settings.

DECT Handset

Register DECT Handset	<input type="button" value="Register"/>
Unregister DECT Handset	<input type="button" value="Unregister"/>
Page DECT Handset	<input type="button" value="Page"/>

DECT PIN CODE

Old Pin Code	<input type="text"/>
New Pin Code	<input type="text"/>
Repeat New Pin Code	<input type="text"/>
Save New Pin Code	<input type="button" value="Apply"/>

Handset Registration State

Handset	Registration Status
Handset 1	registered
Handset 2	not registered
Handset 3	not registered
Handset 4	not registered

Register DECT Handset

To register an existing DECT handset, click the 'register additional handsets' button once, then follow the settings in your Handset User Manual. For BoB Handset users, refer to the Handset Quick Installation Guide

Unregister DECT Handset

Pressing the Unregister button once will unregister all DECT handsets

Page DECT Handset

If you have misplaced your handset, pressing the Page button will ring all DECT handsets.

DECT PIN Code

The default PIN Code is '0000' however you can change this PIN by typing in the old PIN, then typing in the new PIN into the 'New Pin Code' field and confirm in the 'Repeat New Pin Code' field. Press 'Apply' to apply these changes.

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 router.

See the table below for a description of the parameters.

Parameter	Description
Port Type	Displays the port type
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.
Received Call	Number of received calls
Dialled Call	Number of calls made
Rejected Call	Number of rejected calls
Forwarded Call	Number of forwarded calls

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

UPnP

The screenshot shows the iinet BoB™ Advanced Setup Method interface for the UPnP (Universal Plug and Play) settings page. The page has a header with the iinet logo and contact information (www.iinet.net.au, support - 132258, email support - support@iinet.net.au) on the left, and 'ADVANCED SETUP' with 'Home' and 'Logout' links on the right. A left-hand navigation menu lists various setup categories: SETUP WIZARD, SYSTEM, WAN, LAN, WIRELESS, NAT, ROUTE, FIREWALL, SNMP, ADSL, VoIP, UPnP (highlighted), QoS, DDNS, USB, TOOLS, and STATUS. The main content area is titled 'UPnP(Universal Plug and Play) Setting' and contains the following text: '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.' Below this text, there is a control for 'Enable or disable UPnP features' with two radio buttons: 'Enable' (which is selected) and 'Disable'. At the bottom right of the main content area, there are three buttons: 'HELP', 'SAVE SETTINGS', and 'CANCEL'.

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.

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

QoS

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

QoS Settings

To ensure optimum voice quality, your router should prioritize voice over data packages. Therefore, we recommend enabling the QoS feature.

Name	Description	Priority	Bandwidth Allocation	
			Minimum	Allow More
BE	Best Effort forwarding	Lowest	0 %	<input checked="" type="checkbox"/>
AF1x	Assured Forwarding, provides delivery of packets in four independently forwarded AF classes. Within each AF class, an IP packet can be assigned one of three different levels of drop precedence.	Low	0 %	<input checked="" type="checkbox"/>
AF2x		↓	0 %	<input checked="" type="checkbox"/>
AF3x		↓	0 %	<input checked="" type="checkbox"/>
AF4x		High	0 %	<input checked="" type="checkbox"/>
EF	Expedited Forwarding, is intended to provide low delay, low jitter and low loss delivery of packets.	Highest	0 %	<input checked="" type="checkbox"/>

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.

Rule Name	Traffic Description	Map to Diffserv	Outgoing VC	Configure
VoIP	VOIP	EF		Edit Del

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.

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

Edit Traffic Class

www.iinet.net.au
support - 132258
email support - support@iinet.net.au

ADVANCED SETUP [Home](#) [Logout](#)

Edit Traffic Class

This page is for user to specify a classify rule. First, define the class by the traffic type and the local and remote addresses. Then set the Diffserv forwarding group this class is mapped to. Finally, select the outgoing VC that traffic of this class would be routed to.

Rule Name	<input type="text"/>
Traffic Type	Any <input type="button" value="ADVANCED CONFIG"/>
Map to Forwarding Group	BE <input type="button" value="Remark DSCP as No Remark"/>
Direct to VC	By Routing <input type="button" value=""/>

[HELP](#) [Apply](#) [CANCEL](#)

This page is for user to specify a classify rule.

Rule Name: Assign a Name to the rule.

Traffic Type: Choose a Traffic type for the rule, or click on 'Advanced Config' for more advance 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.

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

Traffic Statistics

Traffic Statistics

This page shows the Internet VC outbound traffic statistics of all the Diffserv forwarding groups(automatically updated every 5 mins).

Forwarding Behavior	Sent data			Dropped data
	send(bytes)	send packet	rate (bps)	dropped(bytes)
BE				
AF1x				
AF2x				
AF3x				
AF4x				
EF				

[HELP](#) | [Refresh](#)

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

DDNS (Dynamic DNS) Settings

Dynamic DNS provides users on the Internet a method to tie their domain name(s) to computers or servers. DDNS allows your domain name to follow your IP address automatically by having your DNS records changed when your IP address changes.

With a DDNS 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.

Dynamic DNS	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Provider	TZO.com
Domain Name	
Account / E-mail	
Password / Key	
Status	Success

[HELP](#) | [SAVE SETTINGS](#) | [CANCEL](#)

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.

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

USB

You can plug-in your USB hard-drive or memory stick and share these resources on your home network. Once you have plugged in the USB device you can see the device information in the following 'Status'.

IMPORTANT: The router's USB port does not support a USB Hub, only directly connected USB Mass Storage Devices are supported. File system supporting list: FAT12, FAT16, FAT32 and NTFS. Linux ext2 and new WinXP FAT64 are not supported by this router.

The screenshot shows the 'USB' configuration page in the iinet router's web interface. The left sidebar contains a navigation menu with options like SETUP WIZARD, SYSTEM, WAN, LAN, WIRELESS, NAT, ROUTE, FIREWALL, SNMP, ADSL, VoIP, UPnP, QoS, DDNS, USB, File Server, FTP Server, Web Server, TOOLS, and STATUS. The main content area is titled 'USB' and includes the following information:

- Header: **USB**
- Description: This iinet IAD supports the USB Host controller function. You can enable this function and plug-in your USB device to share it with other people over your LAN network. The supported USB devices include:
 - USB mass storage: hard disk, flash disk or single slot card reader, up to 1 device.
 - USB-Hub: up to 1 device.
- Instructions: After you plug-in the USB device into this iinet IAD. You may click "Update Status" to see the device information in the "Current USB Device Status" table. Three different file system formats are supported: FAT12, FAT16 and FAT32, and up to 4 partitions could be activated at the same time. For your convenience, the iinet IAD will activate the first 4 partitions automatically when you plug-in an USB storage device. If you have more than 4 partitions in your storage device, you could "Deactivate" some unused partitions and "Activate" other partitions that you would like to use. Please activate the partitions before you configure the "File Server", "FTP Server" and "Web FTP Server".
- Configuration: Enable USB function
- Status: Current USB Device Status:
 - Mass storage Disconnected [Update Status]
- Buttons: [HELP](#) | [SAVE SETTINGS](#) | [CANCEL](#)

Advanced Setup | USB | File Server

This page allows you to enable or disable the File Server features. NetBIOS/SMB share protocol can be used in Windows® 95, 98, NT 4.0, 2000, XP or other Operating Systems supporting the NetBIOS/SMB protocol. You need to select which partition (maximum 4 partitions) and folder you want to share. You could specify username, password and security level for each share resource.

If you see some partitions can not be selected in the partition list table, check the FTP Server partition share status to make sure you did not share more than 4 disk partitions at the same time.

The screenshot shows the 'File Server' configuration page in the iinet router's web interface. The left sidebar is identical to the previous screenshot. The main content area is titled 'File Server' and includes the following information:

- Header: **File Server**
- Description: This page allows for configuration of the File Server features so as to share files with desktops/laptops using Windows? 95, 98, NT 4.0, 2000, XP or other OS supporting NetBIOS/SMB protocol. If you have a hard drive or flash disk connected to the modem's USB port, you may create a sharing folder by specifying which device and directory(path) you would like to share. Then set some other parameters: username, password and security level for each shared resource. After you've configured the folders and enabled the File Server function, you could access the folders by typing the following URL in the IE browser or Windows Explorer:
 - \\(IP-Adresse). Ex.: \\10.1.1.1
 - \\(Server Name). Ex.: \\IINET
 - \\(IP-Adresse)\(Folder name). Ex.: \\10.1.1.1\partition1
 - \\(Server Name)\(Folder name). Ex.: \\IINET\partition1
- Instructions: If you would like to access the USB storage from the WAN side, you need to enable the "Remote Access" parameter and can only use the WAN IP address to access the modems file server.
- Configuration: Enable File Server function
- Form fields:
 - Server Name:
 - Server Description:
 - Group Name:
 - Remote Access:
- Status: Sharing Folder List (up to 16 folders):
 - No any USB mass storage connected !
- Buttons: [HELP](#) | [SAVE SETTINGS](#) | [CANCEL](#)

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

Advanced Setup | USB | FTP Server

FTP service is a very common network protocol that enables you to share your files to a local or public network. By using this feature you can share any files/folders on your USB hard drive or memory stick. You need to specify which partition (maximum 4 partitions) and folders you want to share. You can specify different passwords and security levels for different users.

FTP Server and File Server share the same partition share limitation. If you see the error message 'Partition share number exceed' when you select some partitions, check the File Server partition share status.

The screenshot shows the 'FTP Server' configuration page in the iinet BoB™ Advanced Setup interface. The page includes a navigation menu on the left with categories like SETUP WIZARD, SYSTEM, WAN, LAN, WIRELESS, NAT, ROUTE, FIREWALL, SNMP, ADSL, VoIP, UPnP, QoS, DDNS, USB, and STATUS. The main content area is titled 'FTP Server' and contains the following information:

- Introduction:** FTP service is a very common network protocol to let you share your files to the local or public network. By using these feature, you could share any files/folders in your USB hard drive or memory stick. You need to specify user profile and which partition/directory you would like to share. You could specify different passwords and security levels for different user profiles. After you've configured the profiles and enable the FTP Server function, you could use following URL to access the shared files/folders: ftp://(IP address) ex. ftp://10.1.1.1
- Remote Access:** If you would like to access the shared resource from the WAN side, you need to enable the "Remote Access" parameter and use WAN IP to access it.
- Enable FTP Server function:** A checkbox that is currently unchecked.
- Configuration Fields:**
 - Port Number: 21
 - Maximum connections: 10
 - Idle timeout: 10 min. (0 for no timeout)
 - Remote Access: Unchecked checkbox
- Login user profile (up to 5 profiles):** A table with columns for User ID, Path, and Configure. Below the table, it states 'No any USB mass storage connected !'.
- Buttons:** HELP, SAVE SETTINGS, CANCEL

Advanced Setup | USB | Web Server

This function allows you to share your mass storage through HTTP protocol. After you enable this function and specified parameters, you can access via a web browser.

The screenshot shows the 'Web Server' configuration page in the iinet BoB™ Advanced Setup interface. The page includes a navigation menu on the left with categories like SETUP WIZARD, SYSTEM, WAN, LAN, WIRELESS, NAT, ROUTE, FIREWALL, SNMP, ADSL, VoIP, UPnP, QoS, DDNS, USB, and STATUS. The main content area is titled 'Web Server' and contains the following information:

- Introduction:** You could share your USB mass storage via HTTP protocol. After you enable this function and configure all the necessary parameters, you could access your USB storage from the LAN side by typing the following URL into your web browser:
- URL Examples:**
 - http://(IP address):(port number) ex: http://10.1.1.1:8000
 - http://(host name):(port number) ex: http://inet.iad:8000
 - http://(IP address) ex: http://10.1.1.1/inet_usb
 - http://(host name) ex: http://inet.iad/inet_usb
- Enable Web Server function:** A checkbox that is currently unchecked.
- Configuration Fields:**
 - Volume: No any USB mass storage connected !
 - Path: / Browse
 - Port Number: 8000
 - Remote Access: Unchecked checkbox
- Buttons:** HELP, SAVE SETTINGS, CANCEL

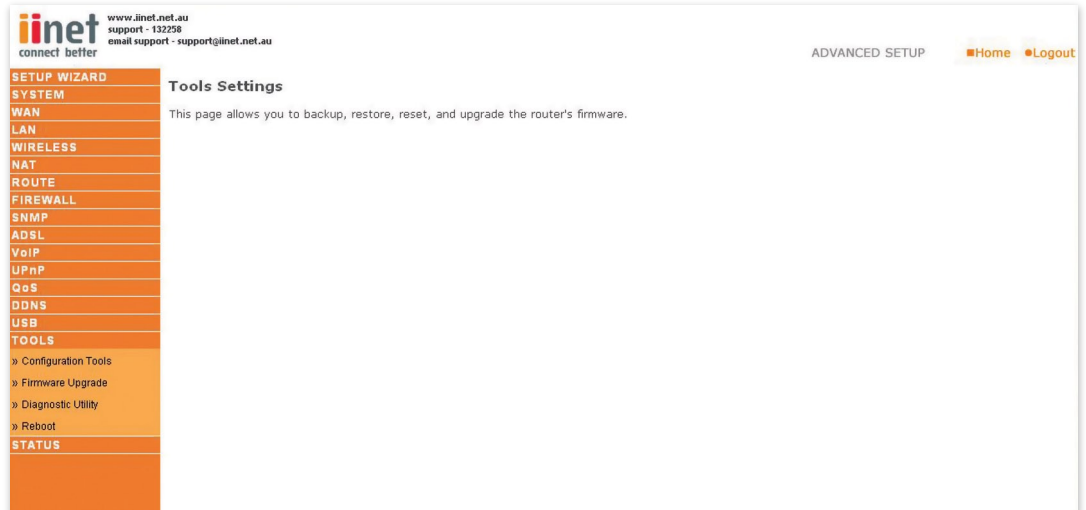
Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

Configuration Tools

Tools

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



The screenshot shows the iinet router configuration interface. The top left features the iinet logo and contact information: www.iinet.net.au, support - 132258, and email support - support@iinet.net.au. The top right shows 'ADVANCED SETUP' with 'Home' and 'Logout' links. A left-hand navigation menu lists various settings categories: SETUP WIZARD, SYSTEM, WAN, LAN, WIRELESS, NAT, ROUTE, FIREWALL, SNMP, ADSL, VoIP, UPnP, QoS, DDNS, USB, TOOLS, and STATUS. The 'TOOLS' category is expanded, showing sub-options: Configuration Tools, Firmware Upgrade, Diagnostic Utility, and Reboot. The main content area is titled 'Tools Settings' and contains the text: 'This page allows you to backup, restore, reset, and upgrade the router's firmware.'

Check Backup Router Configuration and click 'NEXT' to save your router's configuration to a file named 'backup.cfg' on your PC.

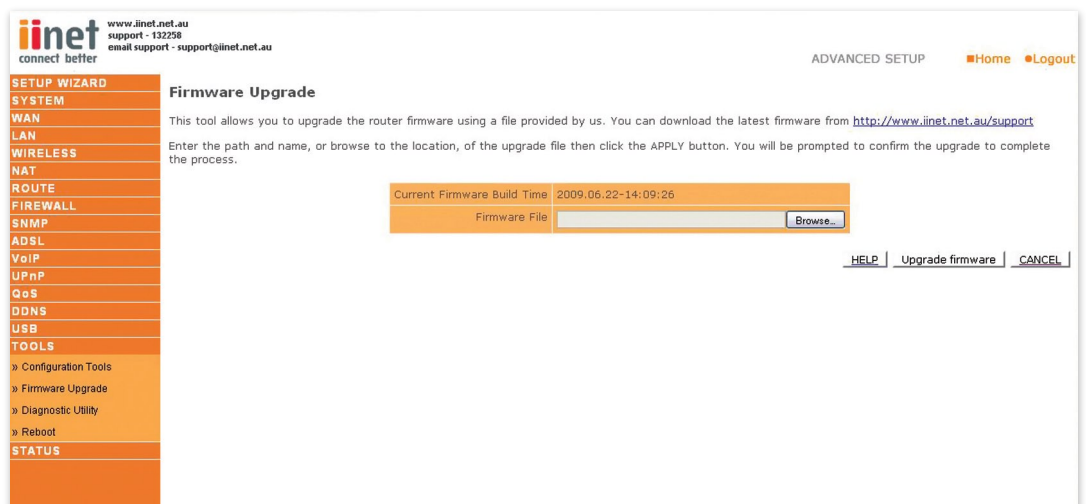
You can then check Restore from saved Configuration file (backup.cfg) to restore the saved backup configuration file.

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.



The screenshot shows the iinet router configuration interface for the Firmware Upgrade screen. The top left features the iinet logo and contact information: www.iinet.net.au, support - 132258, and email support - support@iinet.net.au. The top right shows 'ADVANCED SETUP' with 'Home' and 'Logout' links. A left-hand navigation menu lists various settings categories: SETUP WIZARD, SYSTEM, WAN, LAN, WIRELESS, NAT, ROUTE, FIREWALL, SNMP, ADSL, VoIP, UPnP, QoS, DDNS, USB, TOOLS, and STATUS. The 'TOOLS' category is expanded, showing sub-options: Configuration Tools, Firmware Upgrade, Diagnostic Utility, and Reboot. The main content area is titled 'Firmware Upgrade' and contains the text: 'This tool allows you to upgrade the router firmware using a file provided by us. You can download the latest firmware from <http://www.iinet.net.au/support>. Enter the path and name, or browse to the location, of the upgrade file then click the APPLY button. You will be prompted to confirm the upgrade to complete the process.' Below this text, there is a form with two fields: 'Current Firmware Build Time' with the value '2009.06.22-14:09:26' and 'Firmware File' with a 'Browse...' button. At the bottom right, there are links for 'HELP', 'Upgrade firmware', and 'CANCEL'.

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

Diagnostic Utility

This page allows user use the ping function by entering the destination address and pressing the EXECUTE button. Ping results will then show on the screen.

The screenshot shows the iinet web interface for the Diagnostic Utility. The top navigation bar includes the iinet logo, contact information (www.iinet.net.au, support - 132258, email support - support@iinet.net.au), and links for ADVANCED SETUP, Home, and Logout. A left-hand menu lists various configuration options: SETUP WIZARD, SYSTEM, WAN, LAN, WIRELESS, NAT, ROUTE, FIREWALL, SNMP, ADSL, VoIP, UPnP, QoS, DDNS, USB, TOOLS, Configuration Tools, Firmware Upgrade, Diagnostic Utility, Reboot, and STATUS. The main content area is titled "Diagnostic Utility" and contains the following text: "This tool allows you to test network connection status. You can specify a domain name or a valid IP address of the remote host for ping test." Below this is a "Ping Test" section with a form containing a "Destination Address" input field and an "Execute" button. The "Execution Result" table shows: "Destination IP Address is empty" and "Test Result Stopped". A "HELP" link is located at the bottom right of the main content area.

Reset

Perform a reset from this page.

The screenshot shows the iinet web interface for the Reboot function. The top navigation bar is identical to the Diagnostic Utility page. The left-hand menu is also identical. The main content area is titled "Reboot" and contains the following text: "In the event that the system stops responding correctly or in some way stops functioning, you can perform a reset. Your settings will not be changed. To perform the reset, click on the 'REBOOT ROUTER' button below. You will be asked to confirm your decision. The reset will be complete when the power light stops blinking." A "REBOOT ROUTER" button is located at the bottom right of the main content area, along with a "HELP" link.

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.

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

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.

iinet connect better
www.iinet.net.au
support - 132258
email support - support@iinet.net.au

ADVANCED SETUP Home Logout

STATUS

You can use the Status screen to see the connection status for the router's WAN/LAN interfaces, firmware and hardware version numbers, any illegal attempts to access your network, as well as information on all DHCP client PCs currently connected to your network.

- Current Time: 2009/6/25 - 11:10:58
- UPTIME: 0:1:47:06

INTERNET	GATEWAY	WIRELESS	INFORMATION
ADSL: CONNECTED	IP Address: 10.1.1.1	Wireless: Enabled	Numbers of DHCP Clients: 2
Mode: G.992.5 (ADSL2+)	Subnet Mask: 255.255.255.0	Channel: 6	Runtime Code Version: F1P243EGAU_v1.2.14.20
Download: 19560 Kbps	DHCP Server: Enabled	Wireless Devices: 0	Boot Code Version: 1.0.37-102.9
Upload: 1021 Kbps	Firewall: Enabled	Virtual AP1 SSID: WLAN	ADSL Modem Code Version: A2p802511.d21k5
WAN IP: 203.59.255.162	UPnP: Enabled	Wireless Security: Disabled	LAN MAC Address: 00:22:75:A7:68:CF
Subnet Mask: 255.255.255.255	Wireless: Enabled	Virtual AP2 SSID: WLAN2	Wireless MAC Address: 00:22:75:A7:68:D0
Gateway: 203.59.14.16		Security: Disabled	WAN MAC Address: 00:22:75:A7:68:D1
Primary DNS: 203.0.178.191			Hardware Version: A610A354054R_R3
Secondary DNS: 203.215.29.191			Serial Num:
			Build Time: 2009.06.22-14:09:26

Reconnect

ATM PVC

VC1	VC2
VPI/VC1: 8/35	Disabled
Encapsulation: LLC	
Protocol: PPPoE	
IP Address: 203.59.255.162	
Subnet Mask: 255.255.255.255	
Gateway: 203.59.14.16	
Primary DNS: 203.0.178.191	
Secondary DNS: 203.215.29.191	
Disconnect Connect	

VC3	VC4

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 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.

Chapter 5 : Advanced Setup

BoB™ Advanced Setup Method

DHCP Client Log

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

The screenshot shows the DHCP Client Log page. The left sidebar contains a navigation menu with options: SETUP WIZARD, SYSTEM, WAN, LAN, WIRELESS, NAT, ROUTE, FIREWALL, SNMP, ADSL, VoIP, UPnP, QoS, DDNS, USB, TOOLS, STATUS, » DHCP Client Log (selected), and » Security Log. The main content area displays the DHCP Client Log for the current time (2009/6/25 - 11:11:27). It shows information on LAN DHCP clients currently linked to the VoIP Router, including IP addresses and MAC addresses. For example, one client has IP=10.1.1.2 and mac=00:22:fc:5c:e8:08. Another client has IP=10.1.1.4 and mac=00:24:36:70:f5:f1, named 'Deans-iPhone'. The page also includes a 'HELP' link in the bottom right corner.

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, etc.

The screenshot shows the Security Log page. The left sidebar is identical to the DHCP Client Log page. The main content area displays the Security Log for the current time (2009/6/25 - 11:11:55). It shows any attempts that have been made to gain access to your network. The log entries include: Jun 25 11:10:02 sending ACK to 10.1.1.4, Jun 25 11:10:02 received REQUEST, Jun 25 11:10:01 sending OFFER of 10.1.1.4, Jun 25 11:10:01 received DISCOVER, Jun 25 11:10:01 sending OFFER of 10.1.1.4, Jun 25 11:09:59 received DISCOVER, Jun 25 11:09:58 sending NAK, Jun 25 11:09:58 received REQUEST, Jun 25 11:09:57 sending NAK, Jun 25 11:09:57 received REQUEST, Jun 25 10:54:26 203.13.74.144 login success., Jun 25 10:51:41 203.13.74.144 logout success., Jun 25 10:50:16 sending OFFER of 10.1.1.3, Jun 25 10:50:16 received DISCOVER, Jun 25 10:50:16 sending OFFER of 10.1.1.3, Jun 25 10:50:16 received DISCOVER, Jun 25 10:50:16 received RELEASE, Jun 25 10:50:11 sending OFFER of 10.1.1.3, Jun 25 10:50:11 received DISCOVER, Jun 25 10:48:13 sending ACK to 10.1.1.3. The page also includes a 'HELP' link in the bottom right corner and a 'Save | Clear | Refresh' button at the bottom.

After completing hardware setup by connecting all your network devices, you should automatically be able to connect to the BoB™ - 4 port integrated 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.

Appendices

Appendix A1 - Troubleshooting

TCP/IP Configuration

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

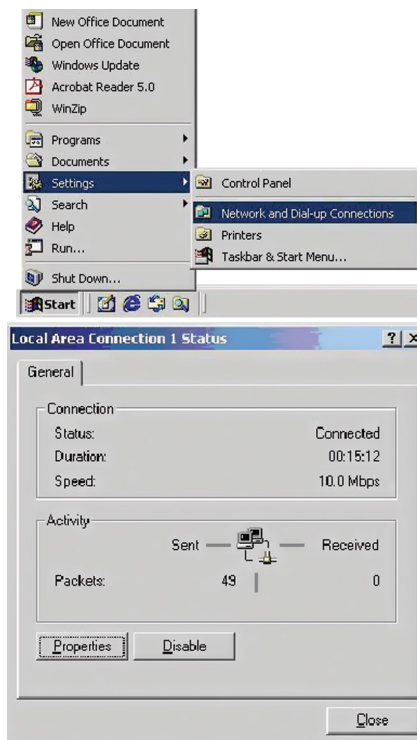
IP Address: 10.1.1.1 **Subnet Mask:** 255.255.255.0

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

Configuring Your Computer in Windows 2000

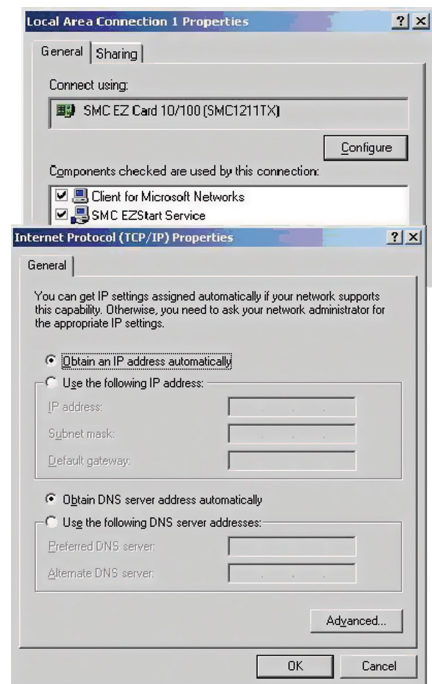
DHCP IP Configuration

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



4. Double-click Internet Protocol (TCP/IP).

5. 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.

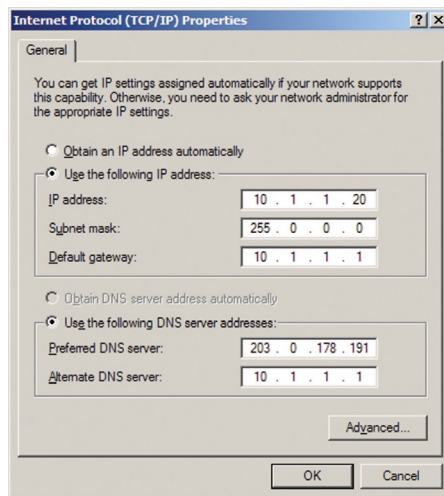


Appendices

Appendix AI - Troubleshooting

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 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 touter 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 close the dialog boxes 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 _____

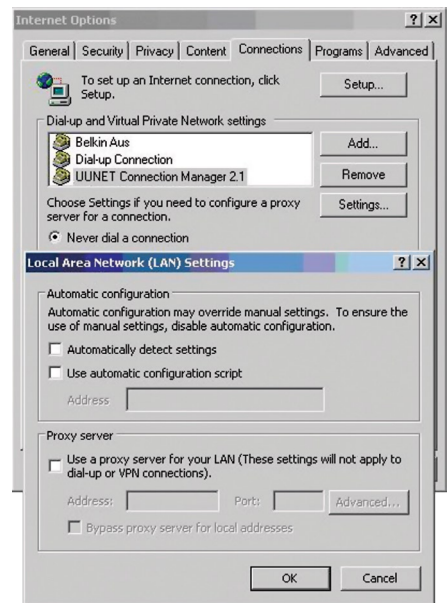
Preferred DNS Server _____

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 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 router.

Appendices

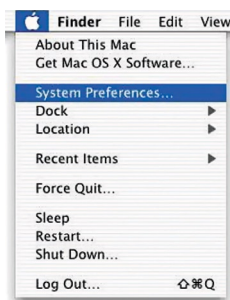
Appendix AI - Troubleshooting

Configuring Your Macintosh Computer

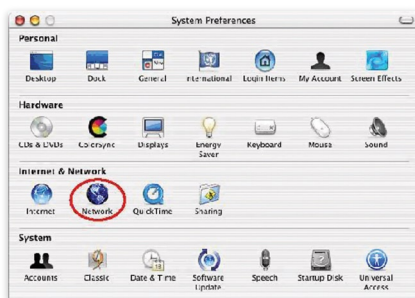
You may find that the instructions here do not exactly match your operating system. This is because these steps and screen shots were created using Mac OS 10.2..Mac OS 7.x and above are similar, but may not be identical to the Mac OS you are using.

Follow these instructions:

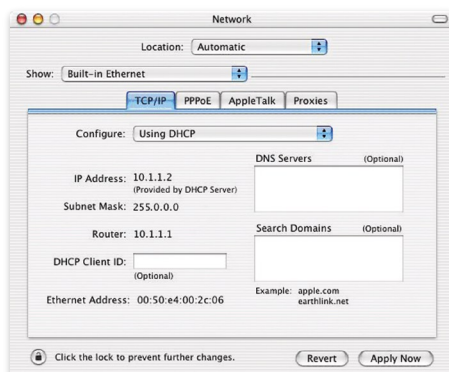
1. Open the 'Systems Preferences' window.



1. Double Click 'Network'.



2. If 'Using DHCP Server' is already selected in the configure field, your computer is already configured for DHCP. If not, select this option.
1. 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 router is functioning.
2. Close the 'Network' window.



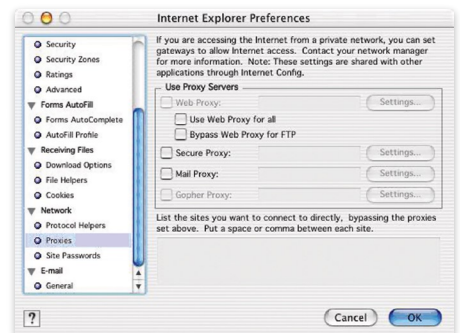
Now your computer is configured to connect to the router.

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 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.



Appendices

Appendix A2 - Troubleshooting

This section describes common problems you may encounter and possible solutions to them. The BoB™ - 4 port integrated wireless router can be easily monitored through panel indicators to identify problems.

Troubleshooting

Symptom

Action

LED Indicators

Power LED is Off

- Check connections between the 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.

LAN LED is Off

- Verify that the router and attached device are powered on.
- Be sure the cable is plugged into both the LAN port on the 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 router from the attached LAN, or the router cannot ping any device on the attached LAN

- Verify that the IP addresses are properly configured. For most applications, you should use the 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 addresses (network component of the IP address) and subnet mask are used for both the 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, refer to your Firewall User Manual for instructions.

Management Problems

Cannot connect using the Web Browser

- Be sure to have configured the router with a valid IP address, subnet mask, and default gateway.
- Check that you have a valid network connection to the router and the port you are using has not been disabled.
- Check the network cabling between the management station and the 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.

Appendices

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.

Specification

Cable Types and Specification

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

Appendices

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
G.992.3 (ADSL2)
G 992.5 (ADSL2+)
G 992.5M (ADSL2+M)

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

2 USB Ports, charging plus 3G/storage

WAN Interface

1 ADSL RJ-11 port

FXO Interface

1 FXO port

FXS Interface

2 FXS lines

Indicator Panel

Line, Phone 1-2, VoIP, USB, LAN 1-4, Wireless, Internet, power

Dimensions

67.5 x 214 x 177.5 mm (L x W x H)

Input Power

12V 1.5A

Management

Web management

Advanced Features

VoIP-QoS, VAD, call waiting, call forwarding, caller ID, jitter buffer. Codec supported - G.711 U/A Law

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

Glossary- I

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 (eg., 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 8023 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

IEEE 802.3x

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

Glossary

Glossary-2

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

Belkin International, Inc.

Limited Two Year Product Warranty

What this warranty covers.

Belkin International, Inc. ('Belkin') warrants to the original purchaser of this Belkin product that the product shall be free of defects in design, assembly, material, or workmanship.

What the period of coverage is.

Belkin warrants the Belkin product for two years.

What will we do to correct problems?

Product Warranty. Belkin will repair or replace, at its option, any defective product free of charge (except for shipping charges for the product). Belkin reserves the right to discontinue any of its products without notice, and disclaims any limited warranty to repair or replace any such discontinued products. In the event that Belkin is unable to repair or replace the product (for example, because it has been discontinued), Belkin will offer a refund in an amount equal to the purchase price of the product as evidenced on the original purchase receipt as discounted by its natural use.

What is not covered by this warranty?

All above warranties are null and void if the Belkin product is not provided to Belkin for inspection upon Belkin's request at the sole expense of the purchaser, or if Belkin determines that the Belkin product has been improperly installed, altered in any way, or tampered with. The Belkin Product Warranty does not protect against acts of God such as flood, earthquake, lightning, war, vandalism, theft, normal-use wear and tear, erosion, depletion, obsolescence, abuse, damage due to low voltage disturbances (i.e. brownouts or sags), non-authorized program, or system equipment modification or alteration.

How to get service.

To get service for your Belkin product you must take the following steps:

1. Contact Belkin Tech Support within 15 days of the Occurrence. Be prepared
 - The part number of the Belkin product.
 - Where you purchased the product.
 - When you purchased the product.
 - Copy of original receipt.
2. Your Belkin Customer Service Representative will then instruct you on how to forward your receipt and Belkin product and how to proceed with your claim.

Belkin reserves the right to review the damaged Belkin product. All costs of shipping the Belkin product to Belkin for inspection shall be borne solely by the purchaser. If Belkin determines, in its sole discretion, that it is impractical to ship the damaged equipment to Belkin, Belkin may designate, in its sole discretion, an equipment repair facility to inspect and estimate the cost to repair such equipment. The cost, if any, of shipping the equipment to and from such repair facility and of such estimate shall be borne solely by the purchaser. Damaged equipment must remain available for inspection until the claim is finalized. Whenever claims are settled, Belkin reserves the right to be subrogated under any existing insurance policies the purchaser may have.

How state law relates to the warranty.

THIS WARRANTY CONTAINS THE SOLE WARRANTY OF BELKIN. THERE ARE NO OTHER WARRANTIES, EXPRESSED OR, EXCEPT AS REQUIRED BY LAW, IMPLIED, INCLUDING THE IMPLIED WARRANTY OR CONDITION OF QUALITY, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, AND SUCH IMPLIED WARRANTIES, IF ANY, ARE LIMITED IN DURATION TO THE TERM OF THIS WARRANTY.

Some states do not allow limitations on how long an implied warranty lasts, so the above limitations may not apply to you.

IN NO EVENT SHALL BELKIN BE LIABLE FOR INCIDENTAL, SPECIAL, DIRECT, INDIRECT, CONSEQUENTIAL OR MULTIPLE DAMAGES SUCH AS, BUT NOT LIMITED TO, LOST BUSINESS OR PROFITS ARISING OUT OF THE SALE OR USE OF ANY BELKIN PRODUCT, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

This warranty gives you specific legal rights, and you may also have other rights, which may vary from state to state. Some states do not allow the exclusion or limitation of incidental, consequential, or other damages, so the above limitations may not apply to you.



iinet

iinet Support

13 22 58

support@iinet.net.au

iinet Business Support

13 24 49

bizsupport@iinet.net.au

Belkin

1800 235 546

Open 24 hours a day,
7 days a week

iinet
connect better