iCoach

MOBILE INTERNET ROUTER

IC-RTR100-00
User Guide

For indoor and mobile vehicle use only.

Table of Contents

Chapter 1: Introduction.. 1

1.1 Overview 1

1.2 Top Panel 2

1.3 Rear Panel 2

1.4 Bottom Panel 3

1.5 System Requirements 3

1.6 Package Contents 3

Chapter 2: Quick Startup.. 4

2.1 Hardware Installation 4

2.2 Configuration 4

2.3 Connect/Disconnect USB Modem 6

Chapter 3: Hardware Installation 7

3.1 Step-by-step Guide.. 7

3.2 Connect/Disconnect USB Modem 7

3.3 Placement Options.. 8

3.3.1 Horizontal Placement..8

3.3.2 Wall-mounted (Stationary – Home/Office)..8

3.4 Establishing the Best Location.. 9

Chapter 4: Configuration..10

4.1 Accessing Web-based Utility 10

4.2 Basic 11

4.2.1 USB Modem..11

4.2.2 Wireless..12

4.2.3 LAN 15

4.2.4 DHCP 16

4.3 Advanced 18

4.3.1 Port Forwarding 18
4.3.2 Internet Access 20
4.3.3 Firewall 21
4.3.4 Wireless 23
4.3.5 Routing 24
4.3.6 MISC 25

4.4 Maintenance 26

4.4.1 Admin 26
4.4.2 Device Settings 27
4.4.3 Firmware 28
4.4.4 Time 28

4.5 Status 30

4.5.1 Device Info 30
4.5.2 Log 32
4.5.3 Statistics 33
4.5.4 Wireless 33

4.6 Help 33

Appendix A: Troubleshooting 34

Appendix B: Safety Information 38

Appendix C: Care and Maintenance 39

Appendix D: Technical Specifications 40

Appendix E: Manufacturer’s Limited Warranty 41

Appendix F: Regulatory Information 42

Appendix G: Contact Information 43

Glossary 44

Index 47

Chapter 1: Introduction

1.1 Overview

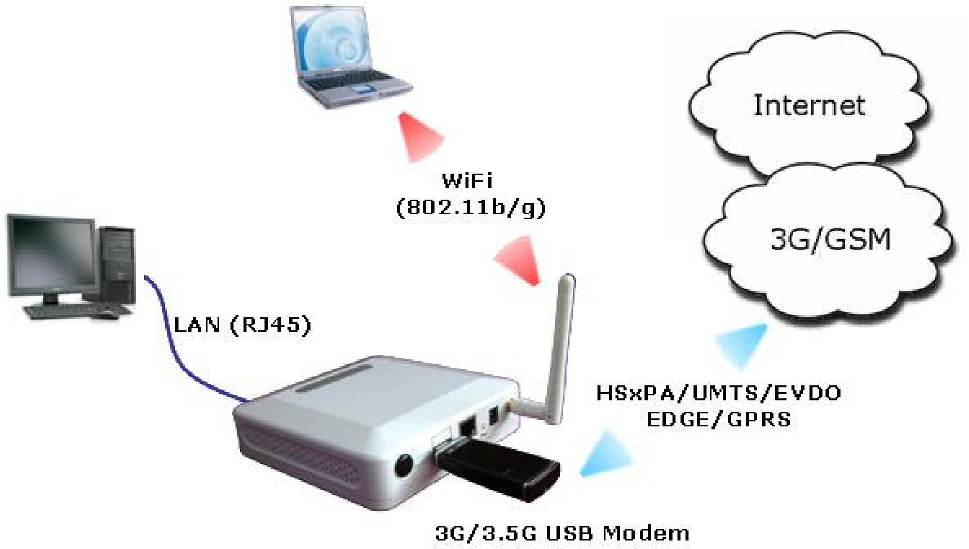
Thank you for purchasing the **iCoach IC-RTR100-00** Wireless Bridging Router. Your **iCoach IC-RTR100-00** router was either purchased as a component in the iCoach mobile kit or bought separately. The instructions in this manual apply to both the stand-alone or kit router.

With your iCoach router you can access the Internet through HSxPA, EDGE/GPRS, 1XRTT or CDMA services provided by your mobile network operator (the iCoach, or like, 3G/3.5G USB modem is required to connect to the mobile network. Your iCoach router allows you to seamlessly share the Internet access via wireless broadcast to multiple users in your vehicle or at home/office.

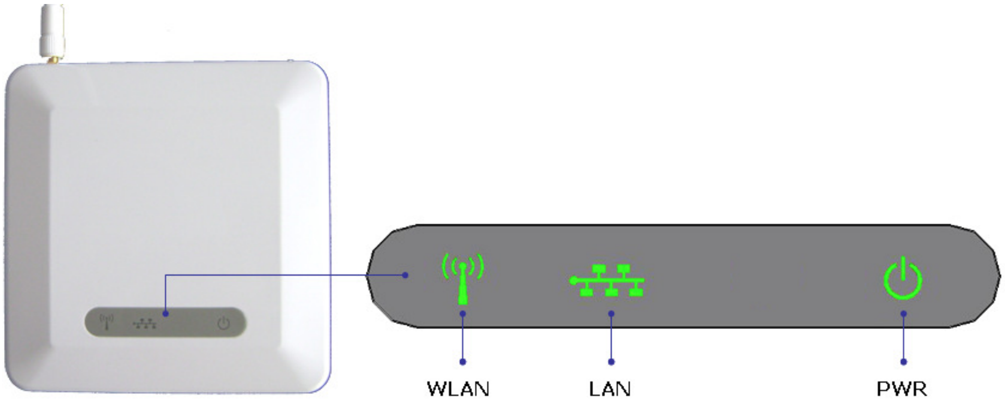
The **IC-RTR100-00** supports both 802.11g and 802.11b standards for wireless local area network (WLAN), enabling a transmission rate of up to 54Mbps (802.11g) or 11Mbps (802.11b).

With the **IC-RTR100-00**, your whole network is protected by a Stateful Packet Inspection (SPI) Firewall and the Network Address Translation (NAT) technology. At the same time, you can secure your wireless network by enabling authentication and data encryption using WEP 64/128-bit or WPA/WPA2 Personal protocols.

Welcome to the exciting world of Mobile Wireless Broadband!

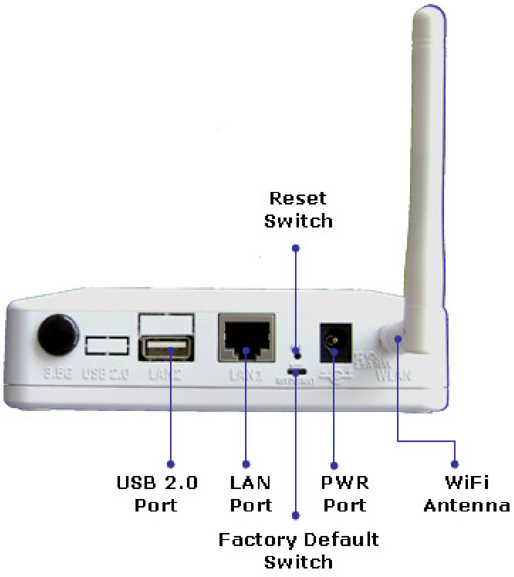


1.2 Top Panel

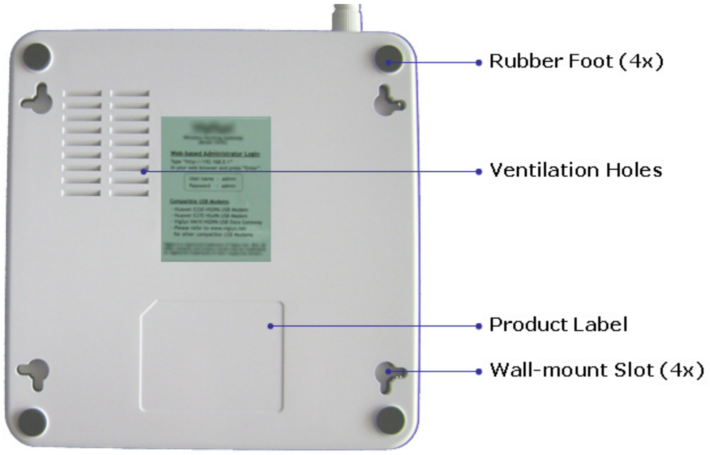


LED	Status	Description
PWR	Steadily On	The router is powered on.
LAN	Steadily On	LAN link ready.
	Blink at various rates	LAN activity - blink rate is proportional to transmission rate.
WLAN	Slow Blink	WiFi ready.
	Blink at various rates	WiFi network activity – blink rate is proportional to transmission rate.

1.3 Rear Panel



1.4 Bottom Panel



1.5 System Requirements

- Microsoft Windows Vista, XP, 2000, NT, Me, 98, 95, Mac OS, Netware, UNIX, Linux, and other operating systems supporting TCP/IP protocol.

- Microsoft Internet Explorer 5.0 or higher, Netscape 4.7 or higher, Firefox 1.0 or higher, and Safari.

- 3G/3.5G USB modem (Included in iCoach kit)

1.6 Package Contents

- **IC-RTR100-00** Wireless Bridging Router

- AC-DC Power Adapter (12V DC, 1.5A)

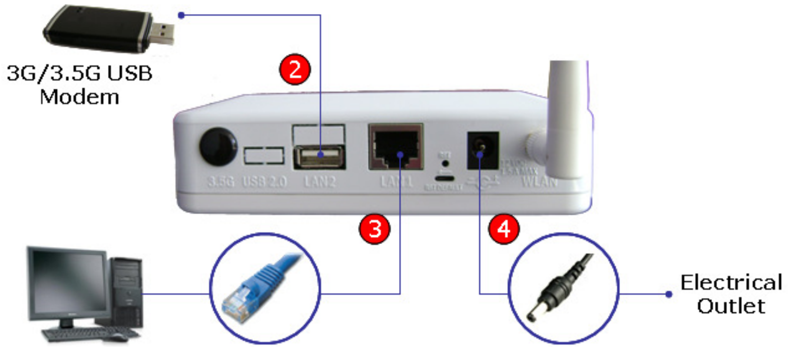
- RJ45 Ethernet Crossover Cable

- Quick Start Instructions

Chapter 2: Quick Startup

2.1 Hardware Installation

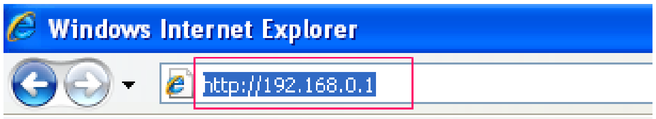
1. Power off the router.
2. Connect the 3G/3.5G USB modem to the router's USB 2.0 port located at the back.
3. Connect the RJ45 cable from the router's LAN port to your computer's network port.
4. Connect one end of the power adapter to the router's PWR port and the other end to the electrical wall outlet.



5. Power on the router.

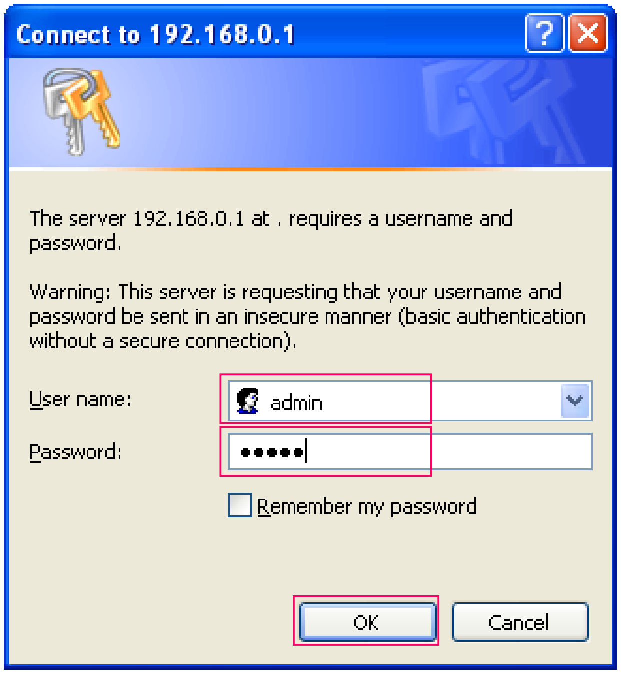
2.2 Configuration

1. To access the router's web-based utility, type "http://192.168.0.1" in your web browser and press "Enter".



http://192.168.0.1

2. When prompted to login, type “admin” in both the User name and Password fields, and then click on the “OK” button.



The server 192.168.0.1 at . requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

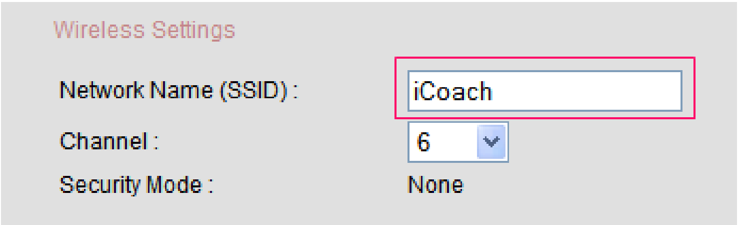
User name: admin

Password: •••••

□ Remember my password

3. To change the Network Name (SSID) for your wireless network, go to the **Basic > Wireless** page.

4. The default SSID is “iCoach”. You may want to change the SSID if:
   - You want to use your own preferred name.
   - Another wireless network operating in your area has already been using the default name.



Wireless Settings

Network Name (SSID) : iCoach

Channel : 6

Security Mode : None

5. We strongly recommend that you turn on the security for your wireless network. To do that, please refer to section **4.2.2.1 Wireless Settings** in this User Guide.

6. If you make any changes that you want to save, please click on the “Submit” button to save the changes.

7. Reset the router by powering it off and then powering it on again.

8. Congratulations - you have successfully configured your router!

2.3 Connect/Disconnect USB Modem

1. It is safe to remove the USB modem from the router even when the power is present to the router.

2. After disconnecting the USB modem, you are recommended to wait for at least **5 seconds** before reconnecting it to the router.

Chapter 3: Hardware Installation

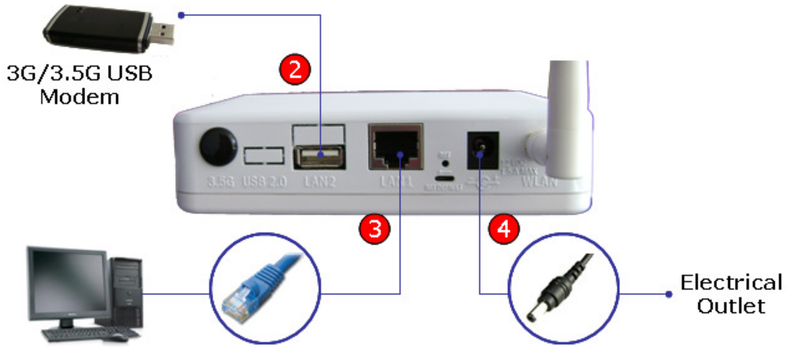
3.1 Step-by-step Guide

1. Power off the router.

2. Connect the 3G/3.5G USB modem to the router's USB 2.0 port located at the back.

3. Connect the RJ45 cable from the router's LAN port to your computer's network port.

4. Connect one end of the power adapter to the router's PWR port and the other end to the electrical wall outlet.



5. Power on the router.

3.2 Connect/Disconnect USB Modem

1. It is safe to remove the USB modem from the router even when the power is present to the router.

2. After disconnecting the USB modem, you are recommended to wait for at least **5 seconds** before reconnecting it to the router.

3.3 Placement Options

3.3.1 Horizontal Placement

Place the router horizontally on its surface, with the bottom panel facing down. It is recommended that the router is placed on top of any existing components in your RV / Vehicle. You can use the supplied industrial Velcro strips to secure the router on top of any equipment installed in your vehicle.

3.3.2 Wall-mounted (Stationary – Home/Office)

On the bottom panel of the router, there are 4 wall-mount slots.

- Choose screws of suitable size where the heads of the screws are small enough to enter easily into the centers of the slots, yet wide enough to fit firmly at the ends of the slots to secure the wall-mounted router.
- Determine where you want to place the router.
- Ensure that the router is properly aligned before marking the location to drill.
- Drill the holes at the marked locations.
- Secure a screw into each hole, leaving approximately 5mm of its head exposed.
- Place the router over the screws and insert the screws into the wall-mount slots.
- Slide the router down until the router sits securely on the screws.

3.4 Establishing the Best Location

Position the router:

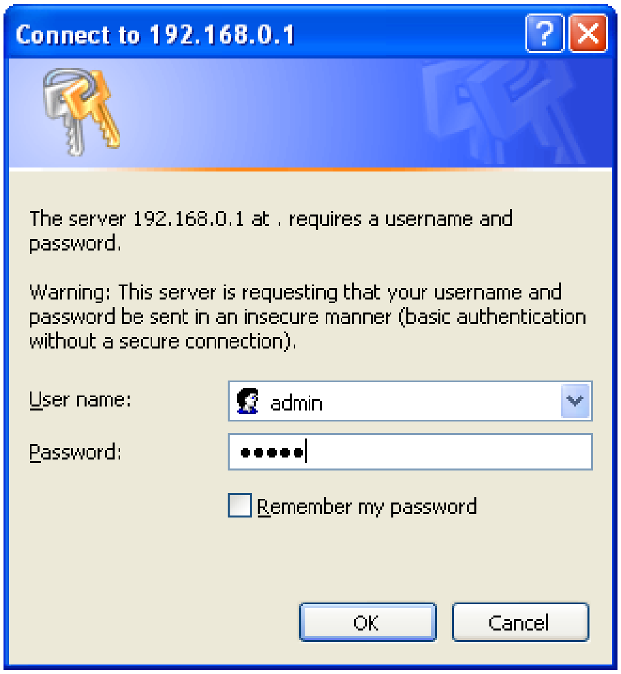
- In a central location, within reasonably close proximity to the network of computers utilizing the WLAN connection.
- Away from any physical barriers which may obstruct the radio signal, e.g. the furniture.
- Away from electrical devices that may cause interference, e.g. radios, transmitters, power cables, microwave ovens, 2.4GHz cordless phones, etc.
- On a high platform to optimize router’s performance vertically and horizontally.
- Out of direct sunlight and away from sources of heat.
- To allow for easy access to the LAN port on the rear panel, if required.
- Such that the LED’s on the top panel are clearly visible.

Chapter 4: Configuration

4.1 Accessing Web-based Utility

The web-based configuration pages can be accessed through a web browser:

- Connect an RJ45 cable from the router's LAN port to your computer's network port.
- Type "http://192.168.0.1" in your web browser and press "Enter".
- When prompted to login, type "admin" in both the User name and Password fields, and then click on the "OK" button.



Connect to 192.168.0.1

The server 192.168.0.1 at . requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

User name: admin

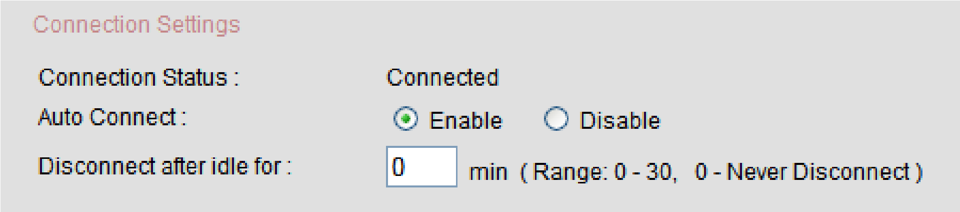
Password: •••••

□ Remember my password

4.2 Basic

4.2.1 USB Modem

4.2.1.1 Connection Settings



Connection Settings

Connection Status : Connected

Auto Connect : ● Enable ○ Disable

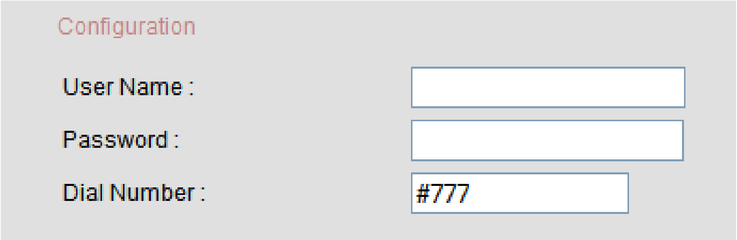
Disconnect after idle for : 0 min (Range: 0 - 30, 0 - Never Disconnect)

Connection Status: This indicates the status of the Internet connection (Connected/Disconnected).

Auto Connect: Select "Enable" if you want the router to automatically connect to the Internet when it is powered on.

Disconnect after idle for: The router will automatically disconnect from the Internet after being idle for this specified period of time. Enter "0" (zero) if you want the router to never disconnect.

4.2.1.2 Configuration



Configuration

User Name :

Password :

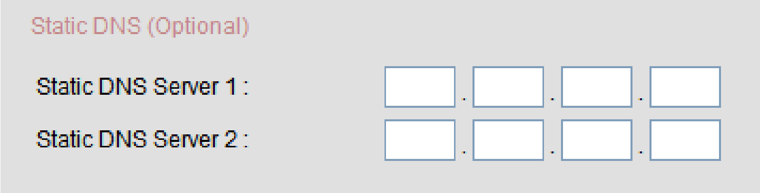
Dial Number : #777

User Name: Enter the user name as provided by your service provider.

Password: Enter the password as provided by your service provider.

Dial Number: The default setting is "#777". Do not alter unless specified by your service provider.

4.2.1.3 Static DNS



Static DNS (Optional)

Static DNS Server 1 : . . .

Static DNS Server 2 : . . .

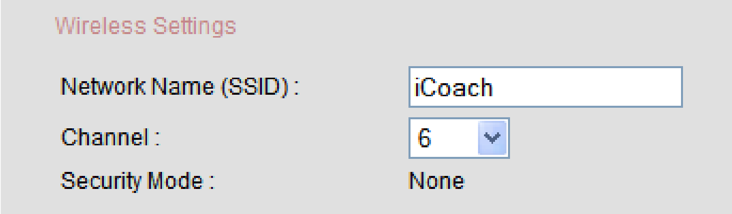
(**Note**: Leave the Static DNS Server settings empty unless specified by your service provider.)

Static DNS Server 1: Enter IP address of the first DNS server as provided by your service provider.

Static DNS Server 2: Enter IP address of the second DNS server as provided by your service provider.

4.2.2 Wireless

4.2.2.1 Wireless Settings



Wireless Settings

Network Name (SSID) : iCoach

Channel : 6

Security Mode : None

Network Name (SSID): This is the name that uniquely identifies your wireless network. The default SSID is “iCoach”. You may want to change the SSID if:

- You want to use your own preferred name.
- Another wireless network operating in your area has already been using the default name.

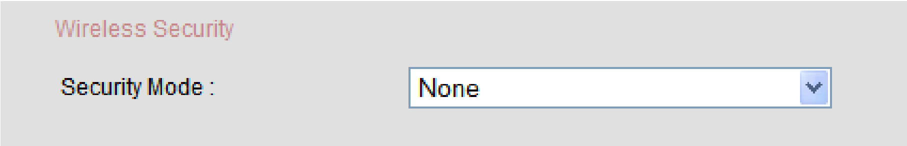
Channel: The default frequency channel is “6”. It is recommended that you keep this setting unless you experience interference with other wireless networks using the same frequency channel.

(**Note:** For best performance, use a channel that is at least 5 channels away from the other wireless networks, e.g. if other wireless networks are operating at channel 11, then set your router’s channel to channel 6 or below.)

Security Mode: Displays the current security mode of your wireless network. To configure the security settings of your wireless network, click on the "Configure Security" button.

4.2.2.2 Wireless Security

None

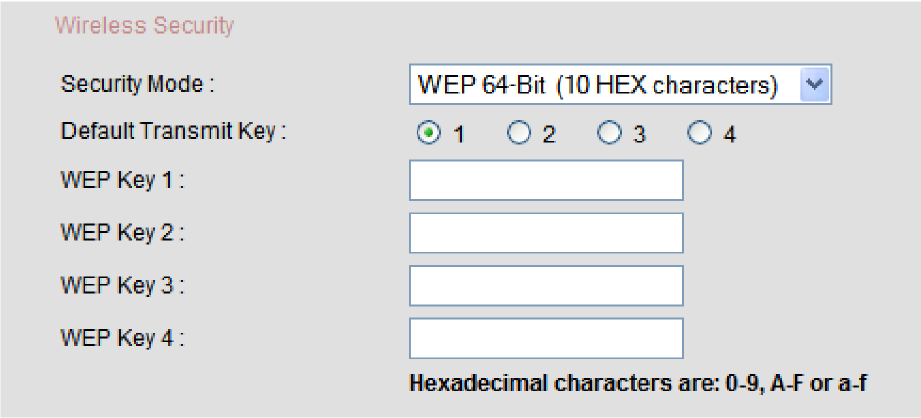


Wireless Security

Security Mode : None

No security is enabled for your wireless network. Not recommended!

WEP 64-Bit



Wireless Security

Security Mode : WEP 64-Bit (10 HEX characters)

Default Transmit Key : ● 1 ○ 2 ○ 3 ○ 4

WEP Key 1 :

WEP Key 2 :

WEP Key 3 :

WEP Key 4 :

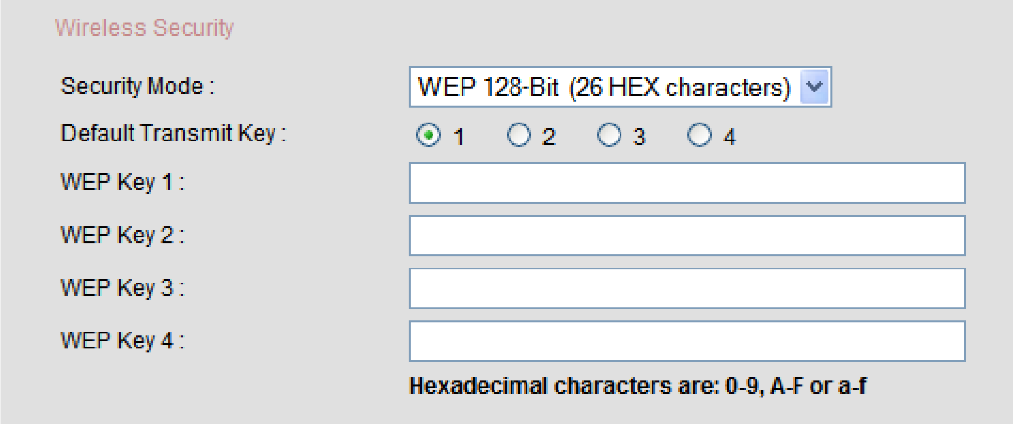
Hexadecimal characters are: 0-9, A-F or a-f

Default Transmit Key: Select the WEP key to use for authentication and data encryption.

WEP Key (1-4): WEP key is the security key used for authentication and data encryption. You can enter up to 4 WEP keys, and which key to use depends on the setting of “Default Transmit Key”. For WEP 64-Bit, the WEP key consists of 10 HEX characters.

(**Note**: HEX characters are from 0-9, A-F or a-f)

WEP 128-Bit



Wireless Security

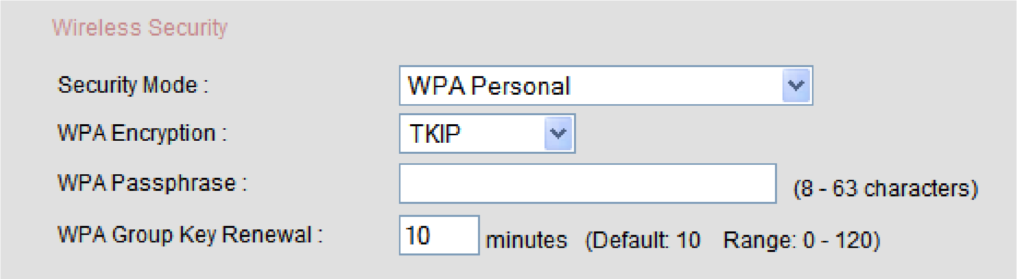
Security Mode :	WEP 128-Bit (26 HEX characters)
Default Transmit Key :	● 1 ○ 2 ○ 3 ○ 4
WEP Key 1 :	
WEP Key 2 :	
WEP Key 3 :	
WEP Key 4 :	
	Hexadecimal characters are: 0-9, A-F or a-f

Default Transmit Key: Select the WEP key to use for authentication and data encryption.

WEP Key (1-4): WEP key is the security key used for authentication and data encryption. You can enter up to 4 WEP keys, and which key to use depends on the setting of “Default Transmit Key”. For WEP 128-Bit, the WEP key consists of 26 HEX characters.

(**Note**: HEX characters are from 0-9, A-F or a-f)

WPA Personal



Wireless Security

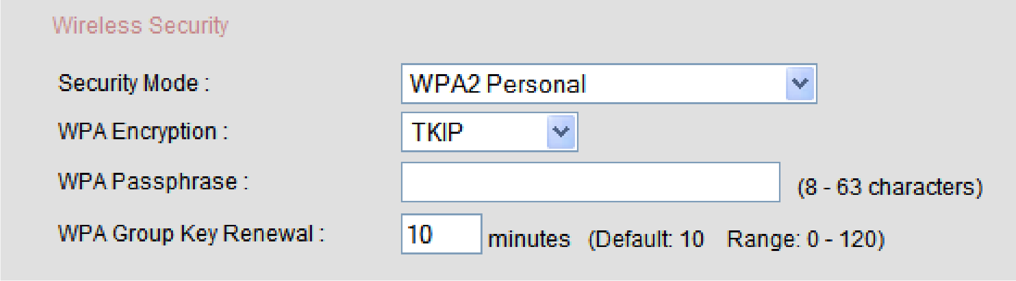
Security Mode :	WPA Personal
WPA Encryption :	TKIP
WPA Passphrase :	(8 - 63 characters)
WPA Group Key Renewal :	10 minutes (Default: 10 Range: 0 - 120)

WPA Encryption: Select the encryption algorithm used in authentication and data protection.

WPA Passphrase: Enter the pre-shared secret key which consists of 8 to 63 characters.

WPA Group Key Renewal: Group Key is used to encrypt/decrypt multicast and broadcast traffic. This setting specifies how frequent the Group Key will be updated between the router and its wireless clients.

WPA2 Personal



Wireless Security

Security Mode :	WPA2 Personal
WPA Encryption :	TKIP
WPA Passphrase :	(8 - 63 characters)
WPA Group Key Renewal :	10 minutes (Default: 10 Range: 0 - 120)

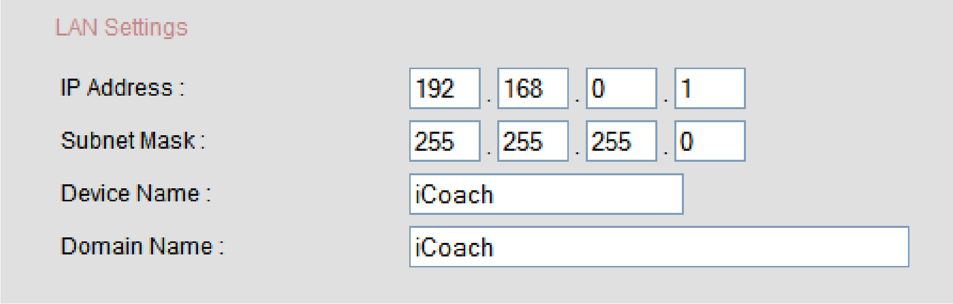
WPA Encryption: Select the encryption algorithm used in authentication and data protection.

WPA Passphrase: Enter the pre-shared secret key which consists of 8 to 63 characters.

WPA Group Key Renewal: Group Key is used to encrypt/decrypt multicast and broadcast traffic. This setting specifies how frequent the Group Key will be updated between the router and its wireless clients.

4.2.3 LAN

4.2.3.1 LAN Settings



LAN Settings

IP Address :	192 . 168 . 0 . 1
Subnet Mask :	255 . 255 . 255 . 0
Device Name :	iCoach
Domain Name :	iCoach

IP Address: The IP address assigned to the router as seen from your local network. The default setting is “192.168.0.1”. It is recommended that you keep this setting unless there is a clash of IP addresses on your network.

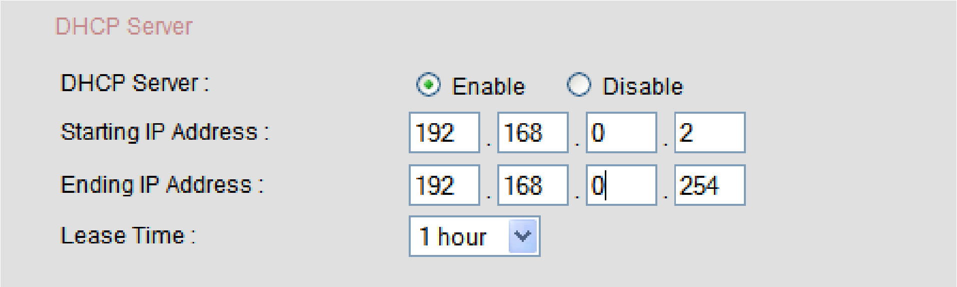
Subnet Mask: The default subnet mask is “255.255.255.0” and you shouldn’t need to change this.

Device Name: Please keep the default setting.

Domain Name: Please keep the default setting.

4.2.4 DHCP

4.2.4.1 DHCP Server



DHCP Server

DHCP Server : ● Enable ○ Disable

Starting IP Address : 192 . 168 . 0 . 2

Ending IP Address : 192 . 168 . 0 . 254

Lease Time : 1 hour

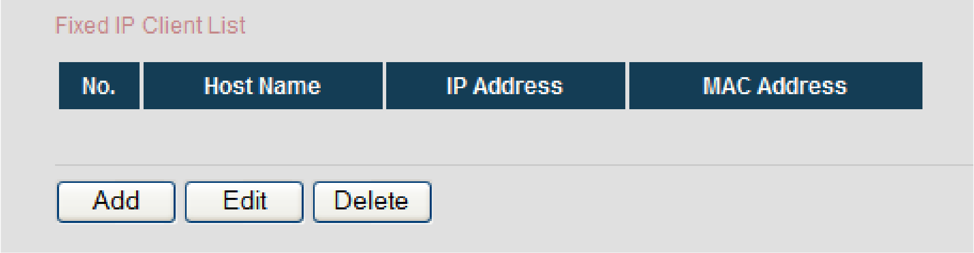
DHCP Server: Select “Enable” unless there is already a DHCP server running on your local network.

Starting IP Address: Enter the first IP address over the range of addresses from which the DHCP server starts issuing addresses. The default setting is “192.168.0.2”.

Ending IP Address: Enter the last IP address beyond the range of addresses where the DHCP server stops issuing addresses. The default setting is “192.168.0.254”.

Lease Time: After obtaining an IP address from the DHCP server, the client computer periodically renews the lease of the IP address with the DHCP server. This setting determines how frequent the renewal process is performed.

4.2.4.2 Fixed IP Client List



Fixed IP Client List

No.	Host Name	IP Address	MAC Address

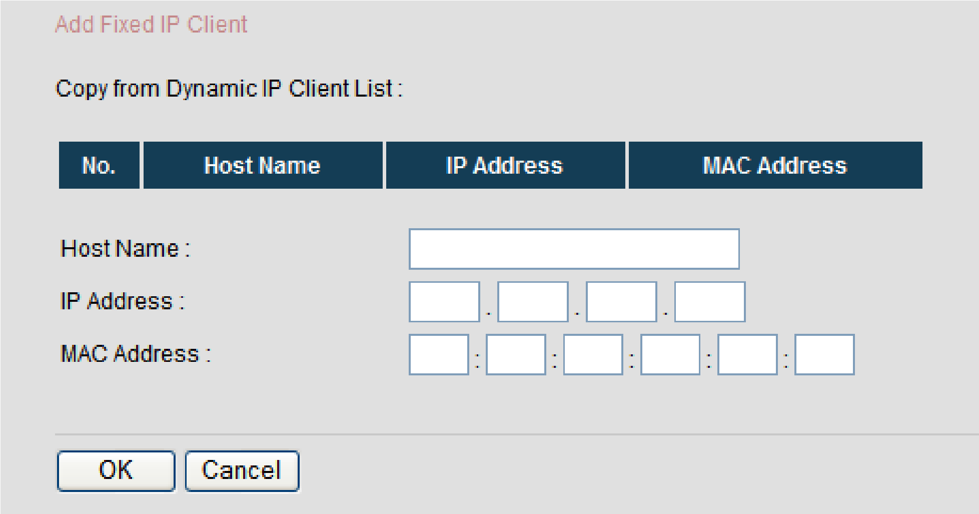
This list displays the host names, IP addresses and MAC addresses of the client computers whose IP addresses are fixed.

To add a client computer to the list, click on the “Add” button.

To edit an existing client, select the entry and click on the “Edit” button.

To delete a client from the list, select the client computer and click on the “Delete” button.

Add Fixed IP Client



Add Fixed IP Client

Copy from Dynamic IP Client List :

No.	Host Name	IP Address	MAC Address

Host Name :

IP Address : . . .

MAC Address : : : : : :

Host Name: Enter a name to identify the client computer.

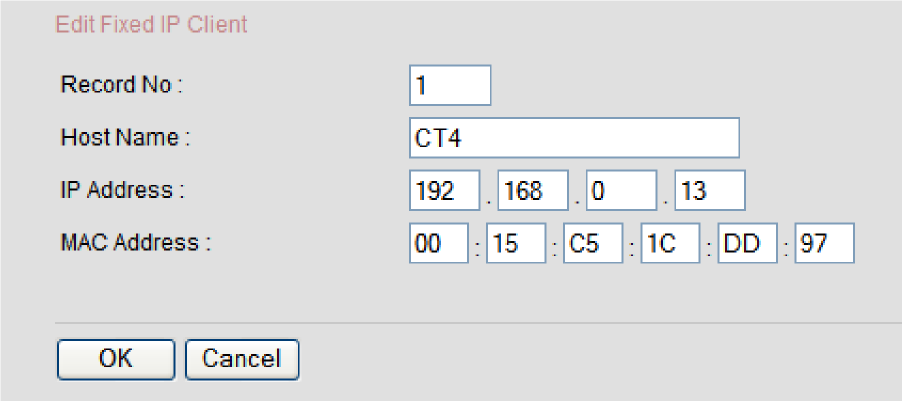
IP Address: Enter the IP address that you want to assign to this client computer. You can enter any IP address between the "Starting IP Address" and "Ending IP Address" that you set in the "DHCP Server" section, provided it has not already been assigned to an existing fixed IP client.

MAC Address: Enter the MAC address of the client computer.

You can also automatically fill these fields by selecting the client computer from the Dynamic IP Client List.

To save the changes, click on the "OK" button.

Edit Fixed IP Client



Edit Fixed IP Client

Record No : 1

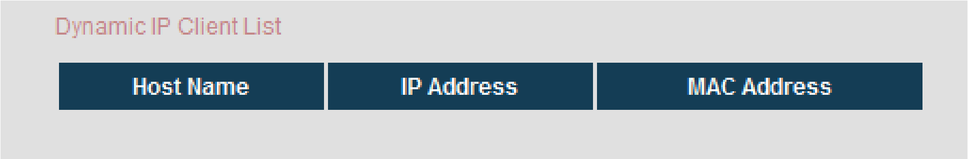
Host Name : CT4

IP Address : 192 . 168 . 0 . 13

MAC Address : 00 : 15 : C5 : 1C : DD : 97

Change the fields as required and click on the "OK" button to save the changes.

4.2.4.3 Dynamic IP Client List



Dynamic IP Client List

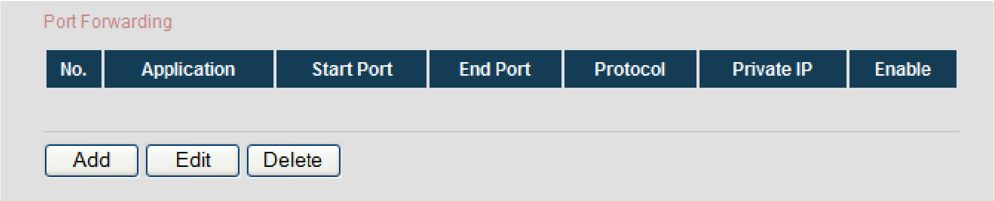
Host Name	IP Address	MAC Address

This list displays the host names, IP addresses and MAC addresses of the client computers which are currently connected to your network.

4.3 Advanced

4.3.1 Port Forwarding

4.3.1.1 Port Forwarding



Port Forwarding

No.	Application	Start Port	End Port	Protocol	Private IP	Enable

This list displays the port forwarding addresses and parameters.

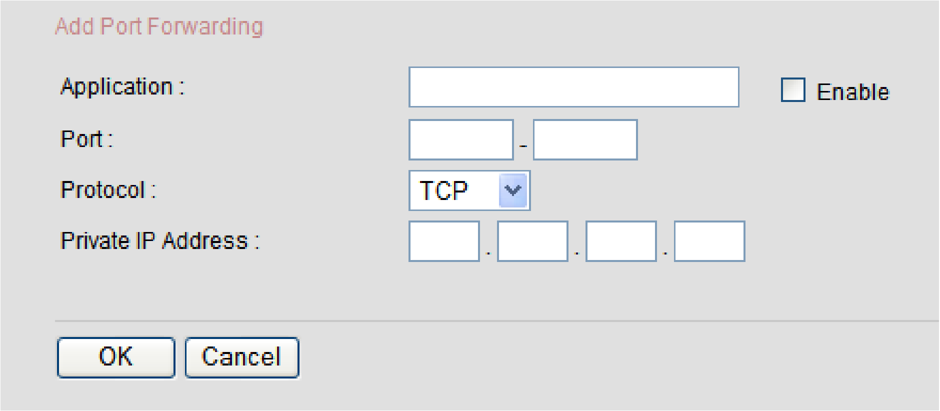
To enable/disable an entry, check/uncheck the “Enable” checkbox of that address.

To add an address to the list, click on the “Add” button.

To edit an existing entry, select the entry and click on the “Edit” button.

To delete an entry from the list, select the entry and click on the “Delete” button.

Add Port Forwarding



Protocol : TCP

Application: Enter a name in this field to identify this port forwarding record. A maximum of 25 characters can be entered.

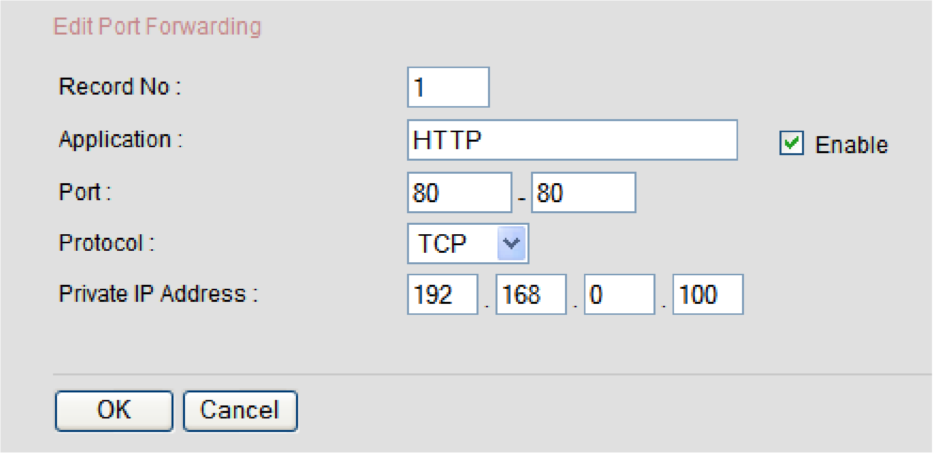
Enable: To enable this port forwarding record, check the “Enable” checkbox.

Port: Enter the port range to forward. The left field is the Start Port while the right field is the End Port. If you want to forward only a single port, enter the same port number in both the Start Port and End Port fields, or enter the port number in the Start Port field and leave the End Port field empty.

Protocol: Select the protocol for this port forwarding changes. The options are “TCP”, “UDP” or “BOTH”.

Private IP Address: Enter the IP address of the computer on your local network to which the ports will be forwarded. To save the entry, click on the “OK” button.

Edit Port Forwarding



Record No : 1

Application : HTTP ☑ Enable

Port : 80 - 80

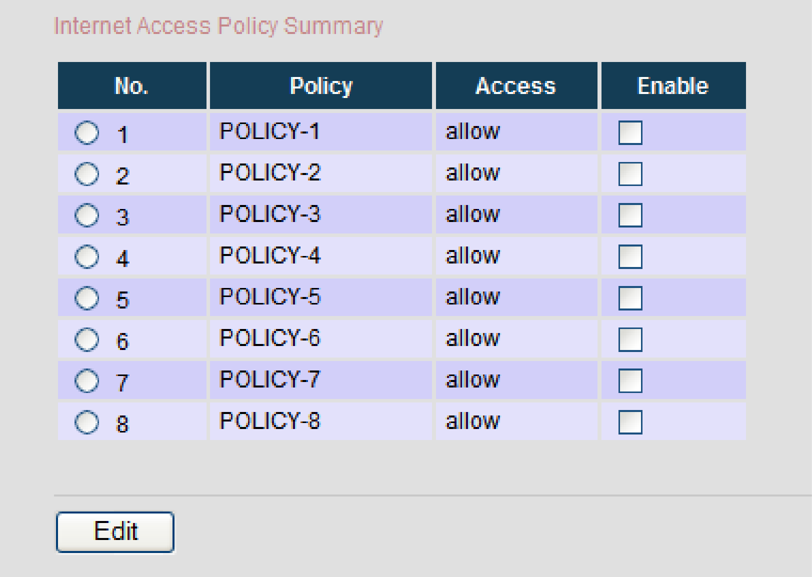
Protocol : TCP

Private IP Address : 192 . 168 . 0 . 100

Change the fields as required and click on the “OK” button to save the changes.

4.3.2 Internet Access

4.3.2.1 Internet Access Policy Summary



Internet Access Policy Summary

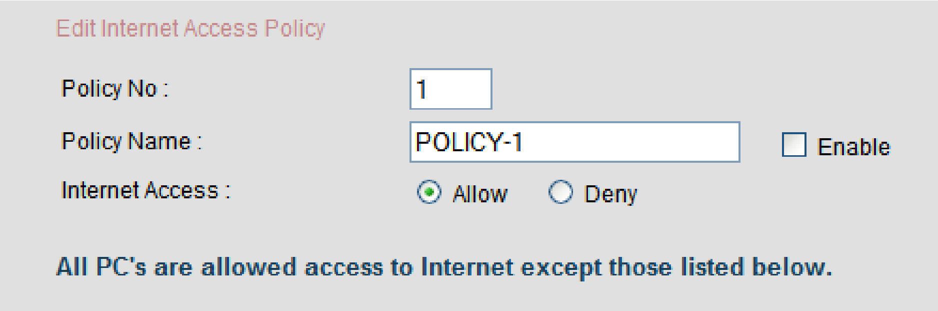
No.	Policy	Access	Enable
○ 1	POLICY-1	allow	□
○ 2	POLICY-2	allow	□
○ 3	POLICY-3	allow	□
○ 4	POLICY-4	allow	□
○ 5	POLICY-5	allow	□
○ 6	POLICY-6	allow	□
○ 7	POLICY-7	allow	□
○ 8	POLICY-8	allow	□

This list displays the summary of Internet access policies. There are a total of eight policies and only one policy can be enabled at a time.

To enable/disable a policy, check/uncheck the “Enable” checkbox of that policy.

To edit a policy, select the policy and click on the “Edit” button.

Edit Internet Access Policy



Edit Internet Access Policy

Policy No :	1	
Policy Name :	POLICY-1	□ Enable
Internet Access :	● Allow ○ Deny	

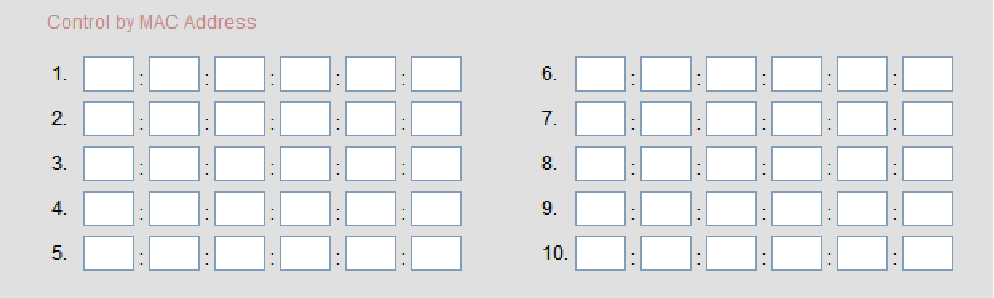
All PC's are allowed access to Internet except those listed below.

Policy Name: Enter a name in this field to identify the policy. A maximum of 25 characters can be entered.

Enable: To enable this policy, check the “Enable” checkbox.

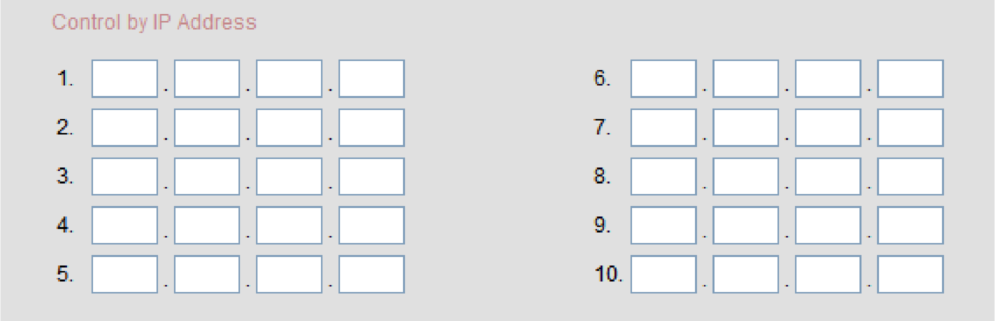
Internet Access: Select “Allow” if you want all computers on your network to have Internet access except those listed in the “Control by MAC Address” and “Control by IP Address” sections. Select “Deny” if you do not want any computers on your network to have Internet access except those listed in the “Control by MAC Address” and “Control by IP Address” sections.

Control by MAC Address



Specify the computers that you want to allow/deny Internet access by entering their MAC addresses.

Control by IP Address

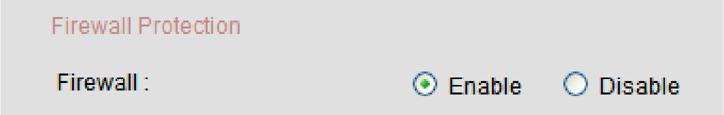


Specify the computers that you want to allow/deny Internet access by entering their IP addresses.

When you are done editing the policy, click on the “OK” button to save the changes.

4.3.3 Firewall

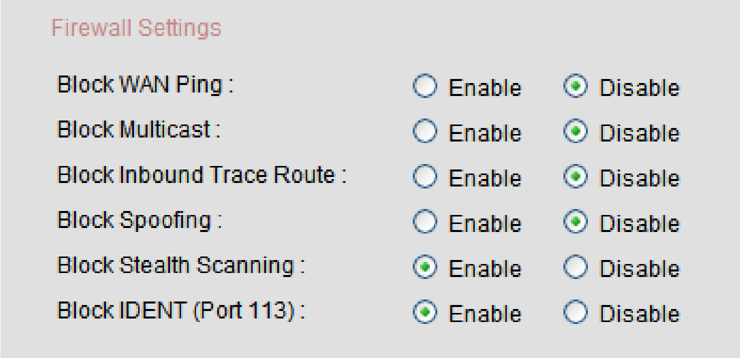
4.3.3.1 Firewall Protection



Firewall : ● Enable ○ Disable

Firewall: Select “Enable” to turn on the SPI firewall. Select “Disable” to turn off the firewall.

4.3.3.2 Firewall Settings



Firewall Settings

Block WAN Ping :	○ Enable	● Disable
Block Multicast :	○ Enable	● Disable
Block Inbound Trace Route :	○ Enable	● Disable
Block Spoofing :	○ Enable	● Disable
Block Stealth Scanning :	● Enable	○ Disable
Block IDENT (Port 113) :	● Enable	○ Disable

Block WAN Ping: Select “Enable” if you do not want the router to respond to ping requests from the Internet.

Block Multicast: Select “Enable” if you want to prevent multicast packets from being forwarded to your local network.

Block Inbound Trace Route: Traceroute has been frequently used by attackers to map out one’s local network architecture. Select “Enable” to prevent the potential attackers from acquiring this sensitive information.

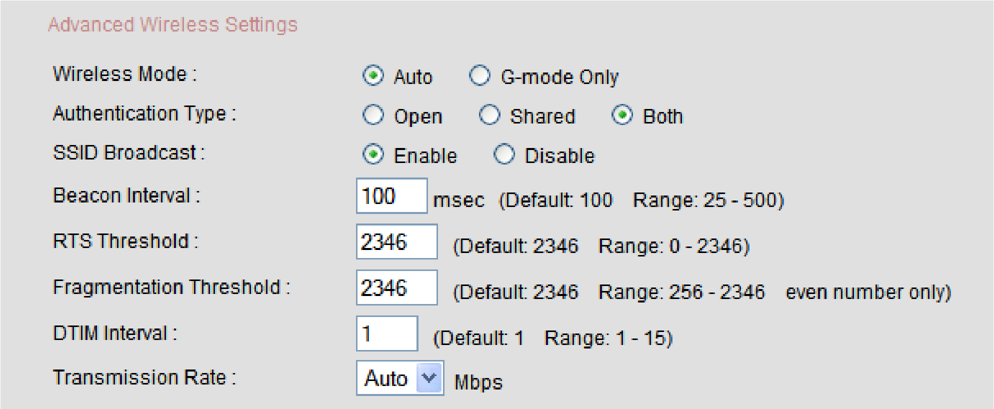
Block Spoofing: Select “Enable” to filter packets received from the Internet that pretend to originate from the local network.

Block Stealth Scanning: Stealth scanning is a technique used by attackers to discover open ports on a network device, searching for vulnerabilities that can be exploited to compromise the network. Select “Enable” to protect your router from stealth scanning.

Block IDENT (Port 113): Select “Enable” to prevent port 113 from being scanned by other Internet users.

4.3.4 Wireless

4.3.4.1 Advanced Wireless Settings



Advanced Wireless Settings

Wireless Mode :	● Auto ○ G-mode Only
Authentication Type :	○ Open ○ Shared ● Both
SSID Broadcast :	● Enable ○ Disable
Beacon Interval :	100 msec (Default: 100 Range: 25 - 500)
RTS Threshold :	2346 (Default: 2346 Range: 0 - 2346)
Fragmentation Threshold :	2346 (Default: 2346 Range: 256 - 2346 even number only)
DTIM Interval :	1 (Default: 1 Range: 1 - 15)
Transmission Rate :	Auto Mbps

Wireless Mode: Select "G-mode Only" if all your wireless clients are 802.11g devices. Select "Auto" if you have both 802.11b and 802.11g wireless clients on your network.

Authentication Type: Select "Open" to allow wireless clients to connect to your access point without authentication. Select "Shared" to implement WEP key authentication before a wireless client can attach to your access point. Select "Both" to support both authentication types.

SSID Broadcast: Select "Enable" to allow wireless devices to detect your access point. Select "Disable" to prevent wireless devices from detecting your access point, which helps to secure your wireless network from probable hackers or unauthorized users.

Beacon Interval: The interval between transmissions of beacon frames which are used by the access point to announce its presence. The default value is 100 milliseconds.

RTS Threshold: RTS (Request To Send) Threshold sets the size of the data packet that will trigger the RTS/CTS mechanism on your access point. The default value is 2346.

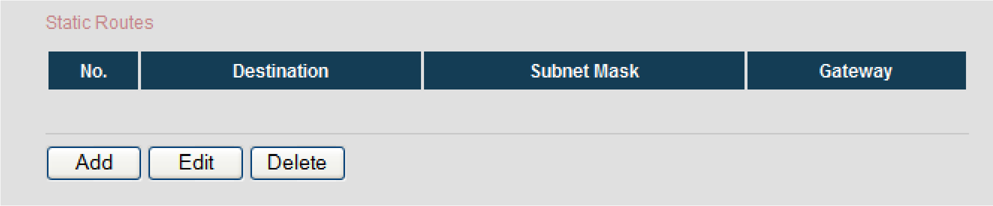
Fragmentation Threshold: Fragmentation Threshold sets the maximum size of a data packet. Data packets exceeding this size will be fragmented into smaller packets before transmission. The default value is 2346.

DTIM Interval: DTIM (Delivery Time Indication Message) Interval specifies the number of beacon frames that must be transmitted before the access point sends the buffered multicast frames. The default value is 1.

Transmission Rate: Typical transmission rates are 11Mbps for 802.11b and 54Mbps for 802.11g. From the dropdown box, select “Auto” to allow the router to use the fastest available data rate, select “11” to allow only 11Mbps data rate, or select “54” to allow only 54Mbps data rate.

4.3.5 Routing

4.3.5.1 Static Routes



Static Routes

No.	Destination	Subnet Mask	Gateway

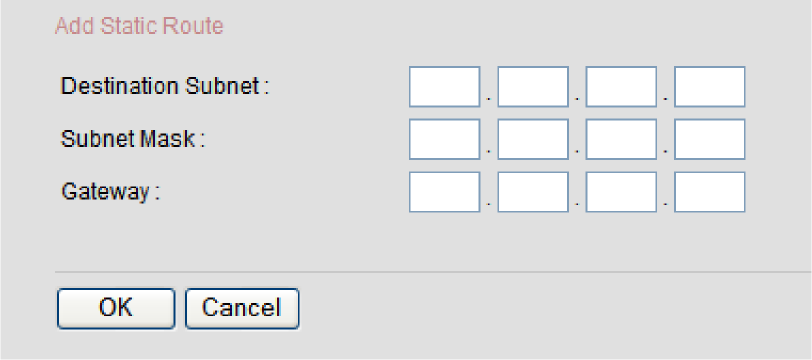
This list displays the static route entries.

To add an entry to the list, click on the “Add” button.

To edit an existing entry, select the record and click on the “Edit” button.

To delete an entry from the list, select the record and click on the “Delete” button.

Add Static Route

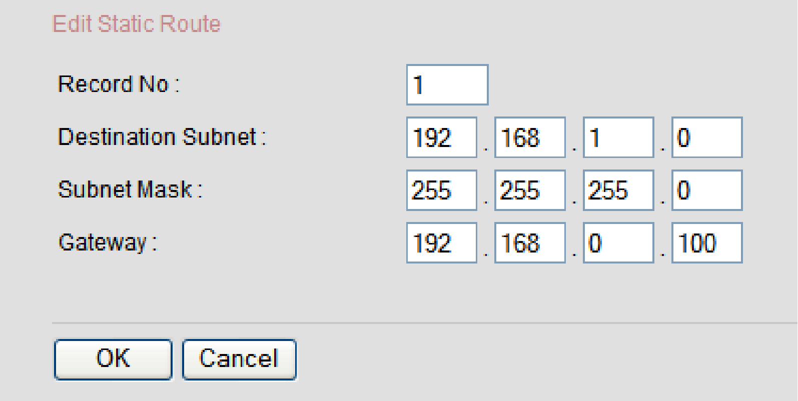


Destination Subnet: Enter the IP address of the remote network or host for which you want to assign the static route.

Subnet Mask: Enter the subnet mask of the remote network for which you want to assign the static route. To route to a single host, enter the subnet mask as “255.255.255.255”.

Gateway: Enter the IP address of the gateway or routing device to which the data packets destined for the specified remote network or host will be forwarded. Click on the “OK” button to save the changes.

Edit Static Route


Edit Static Route

Record No : 1

Destination Subnet : 192 . 168 . 1 . 0

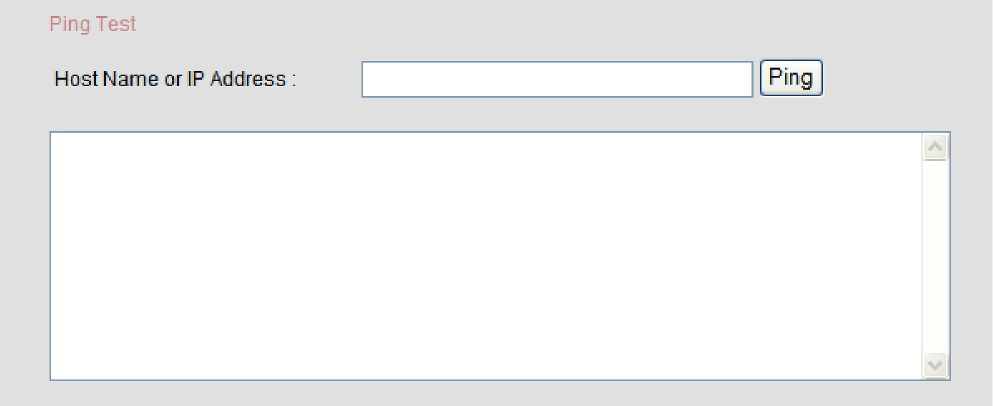
Subnet Mask : 255 . 255 . 255 . 0

Gateway : 192 . 168 . 0 . 100

Change the fields as required and click on the “OK” button to save the changes.

4.3.6 MISC

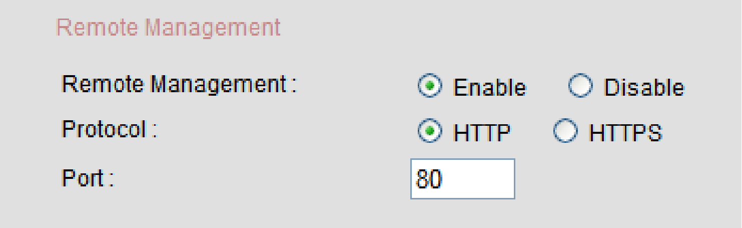
4.3.6.1 Ping Test


Ping Test

Host Name or IP Address :

Host Name or IP Address: Enter the host name or IP address of the host that you want to ping and click on the “Ping” button. The ping result will be displayed in the text box below it.

4.3.6.2 Remote Management


Remote Management

Remote Management : ● Enable ○ Disable

Protocol : ● HTTP ○ HTTPS

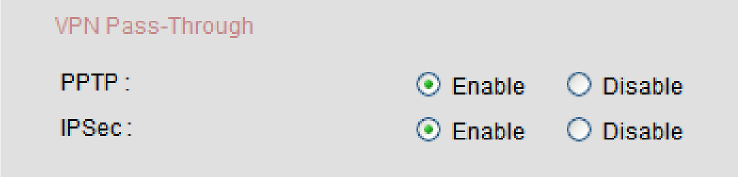
Port : 80

Remote Management: Select “Enable” if you want the web-based utility of the router to be accessible from the Internet. Select “Disable” if you want the web-based utility to be accessible only from your local network.

Protocol: Select the protocol to use when accessing the web-based utility from the Internet. You can select either HTTP or HTTPS. HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) is similar to HTTP but provides a secure connection by encrypting the transmitted data.

Port: Enter the port number to use when accessing the web-based utility from the Internet.

4.3.6.3 VPN Pass-Through



VPN Pass-Through

PPTP : ● Enable ○ Disable

IPSec : ● Enable ○ Disable

PPTP: Select “Enable” to allow PPTP packets to pass through the router.

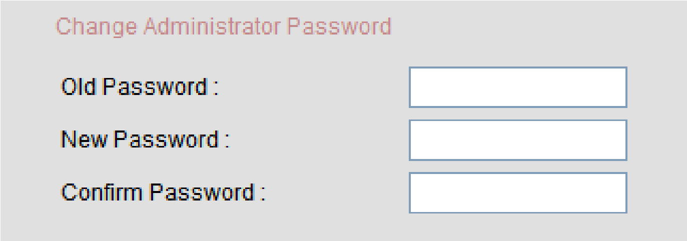
IPSec: Select “Enable” to allow IPSec packets to pass through the router.

(**Note:** PPTP and IPSec are the most common protocols used for implementing virtual private network (VPN).)

4.4 Maintenance

4.4.1 Admin

4.4.1.1 Change Administrator Password



Change Administrator Password

Old Password :

New Password :

Confirm Password :

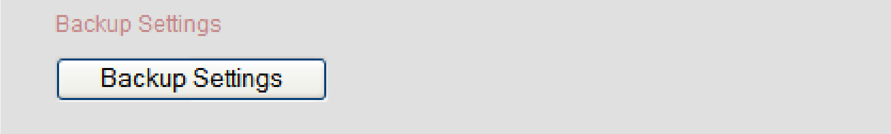
Old Password: Enter the old password or default password if you have not changed the password before.

New Password: Enter the new password that you would like to set for the router.

Confirm Password: Re-enter the new password.

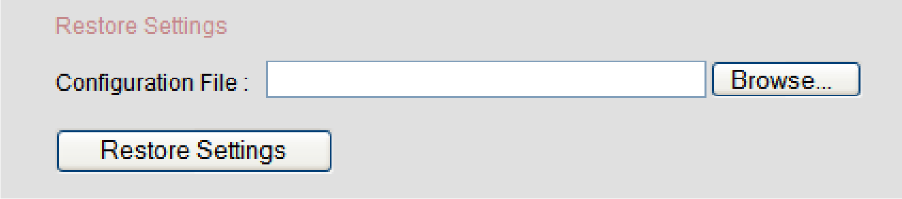
4.4.2 Device Settings

4.4.2.1 Backup Settings



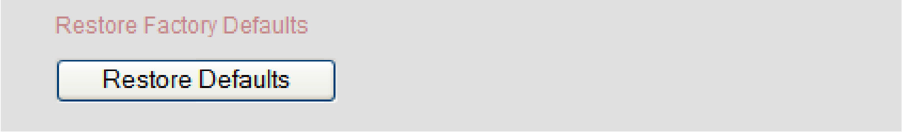
Click on the “Backup Settings” button to save the router’s configuration settings to the local hard drive of your computer.

4.4.2.2 Restore Settings



Configuration File: To restore the router’s configuration settings from the configuration file saved in your local hard drive, click on the “Browse” button to locate the file, and then click on the “Restore Settings” button.

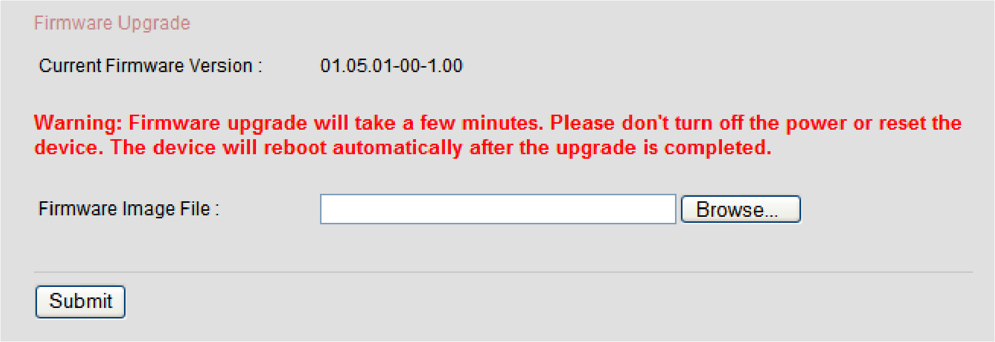
4.4.2.3 Restore Factory Defaults



To delete the router’s current configuration settings and restore to factory defaults, click on the “Restore Defaults” button.

4.4.3 Firmware

4.4.3.1 Firmware Upgrade



Firmware Upgrade

Current Firmware Version : 01.05.01-00-1.00

Warning: Firmware upgrade will take a few minutes. Please don't turn off the power or reset the device. The device will reboot automatically after the upgrade is completed.

Firmware Image File :

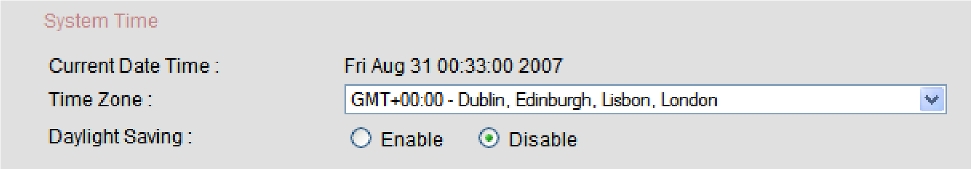
Current Firmware Version: The router's existing firmware version.

Firmware Image File: Click on the "Browse" button to locate the firmware image file that you have downloaded from the iCoach website at www.icoach.net/support. After that, click on the "Submit" button to upgrade the firmware.

(**Warning:** Firmware upgrade will take a few minutes. Please don't turn off the power or reset the router.)

4.4.4 Time

4.4.4.1 System Time



System Time

Current Date Time : Fri Aug 31 00:33:00 2007

Time Zone : GMT+00:00 - Dublin, Edinburgh, Lisbon, London

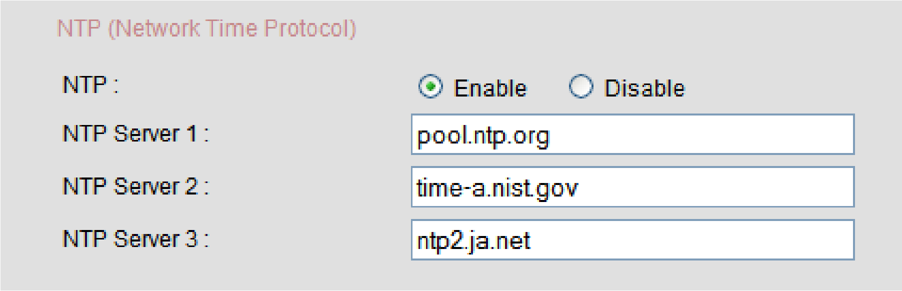
Daylight Saving : ○ Enable ● Disable

Current Date Time: Displays the current date and time of the router.

Time Zone: From the dropdown box, select the time zone of your geographical location.

Daylight Saving: For countries practicing daylight saving, select "Enable" during the daylight saving period and select "Disable" when the daylight saving period has ended.

4.4.4.2 NTP (Network Time Protocol)



NTP (Network Time Protocol)

NTP : ● Enable ○ Disable

NTP Server 1 : pool.ntp.org

NTP Server 2 : time-a.nist.gov

NTP Server 3 : ntp2.ja.net

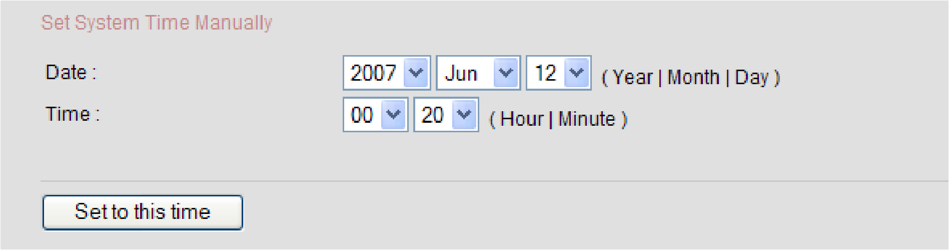
NTP: Select “Enable” if you want the router’s clock time to be synchronized with an NTP server.

NTP Server 1: Enter the host name or IP address of your preferred NTP server.

NTP Server 2: Enter the host name or IP address of a second NTP server. If NTP Server 1 is unavailable, the router’s clock time will be synchronized with this server.

NTP Server 3: Enter the host name or IP address of a third NTP server. If NTP Servers 1 and 2 are unavailable, the router’s clock time will be synchronized with this server.

4.4.4.3 Set System Time Manually



Set System Time Manually

Date : 2007 Jun 12 (Year | Month | Day)

Time : 00 20 (Hour | Minute)

Date: From the dropdown boxes, select the current date.

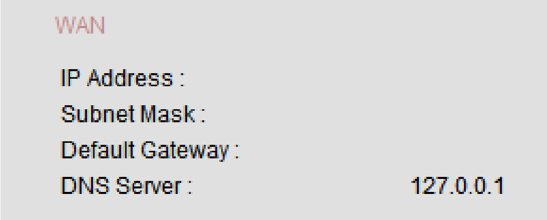
Time: From the dropdown boxes, select the current time.

Click on the “Set to this time” button to set the router’s date and time manually.

4.5 Status

4.5.1 Device Info

4.5.1.1 WAN



WAN

IP Address :	
Subnet Mask :	
Default Gateway :	
DNS Server :	127.0.0.1

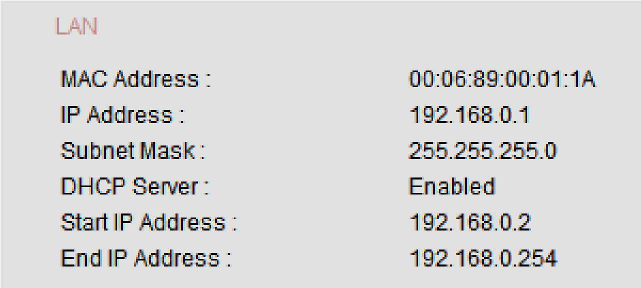
IP Address: Displays the IP address of the router’s WAN interface.

Subnet Mask: Displays the subnet mask of the router’s WAN interface.

Default Gateway: Displays the default gateway of the router’s WAN interface.

DNS Server: Displays the DNS servers used by the router.

4.5.1.2 LAN



LAN

MAC Address :	00:06:89:00:01:1A
IP Address :	192.168.0.1
Subnet Mask :	255.255.255.0
DHCP Server :	Enabled
Start IP Address :	192.168.0.2
End IP Address :	192.168.0.254

MAC Address: Displays the MAC address of the router’s LAN interface.

IP Address: Displays the IP address of the router’s LAN interface.

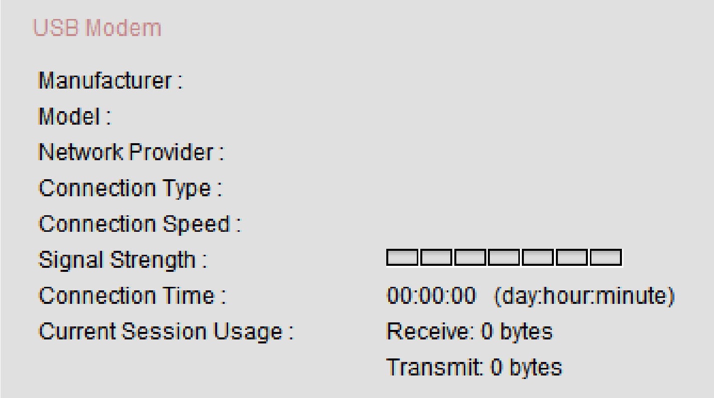
Subnet Mask: Displays the subnet mask of the router’s LAN interface.

DHCP Server: Displays the status of the DHCP server (Enabled/Disabled).

Start IP Address: The first IP address in the DHCP server’s address pool.

End IP Address: The last IP address in the DHCP server’s address pool.

4.5.1.3 USB Modem



USB Modem

Manufacturer :	
Model :	
Network Provider :	
Connection Type :	
Connection Speed :	
Signal Strength :	□□□□□□□
Connection Time :	00:00:00 (day:hour:minute)
Current Session Usage :	Receive: 0 bytes Transmit: 0 bytes

Manufacturer: Displays the manufacturer of the 3G/3.5G USB modem connected to the router.

Model: Displays the model of the 3G/3.5G USB modem connected to the router.

Network Provider: Displays the name of the mobile network operator.

Connection Type: Displays the type of connection to the mobile network. It could be GPRS, EDGE, EVDO, UMTS or HSxPA.

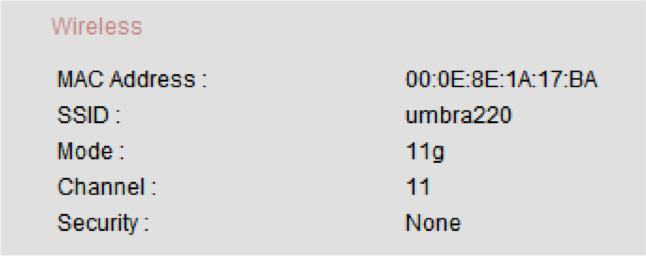
Connection Speed: Displays the highest possible speed of connection to the mobile network. The actual connection speed will vary depending on the service provider.

Signal Strength: Illustrates the strength of the radio signal received from the mobile network.

Connection Time: Displays how long the router has been connected to the mobile network.

Current Session Usage: Displays the number of bytes received and transmitted throughout the duration of the connection.

4.5.1.4 Wireless



Wireless

MAC Address :	00:0E:8E:1A:17:BA
SSID :	umbra220
Mode :	11g
Channel :	11
Security :	None

MAC Address: Displays the MAC address of the router’s WiFi interface.

SSID: Displays the SSID broadcast by the router's WiFi interface.

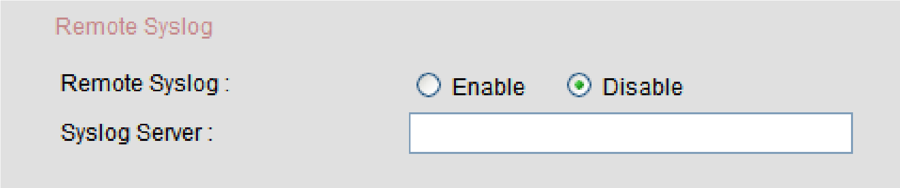
Mode: Displays the current WiFi connection mode.

Channel: Displays the operating frequency channel of the router's WiFi interface.

Security: Displays the security mode enabled on the router's WiFi interface.

4.5.2 Log

4.5.2.1 Remote Syslog



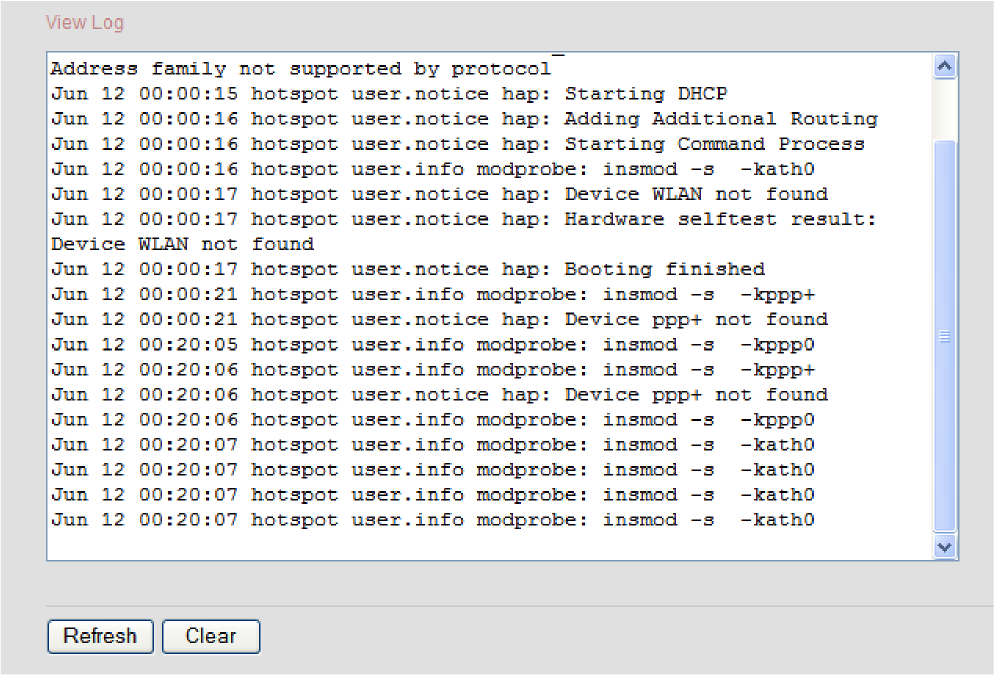
Remote Syslog : ○ Enable ● Disable

Syslog Server :

Remote Syslog: Select "Enable" if you want to log the system activities of the router locally and to a remote Syslog server. Select "Disable" if you only want to log the system activities locally.

Syslog Server: Enter the host name or IP address of the Syslog server if you have selected "Enable" for Remote Syslog.

4.5.2.2 View Log



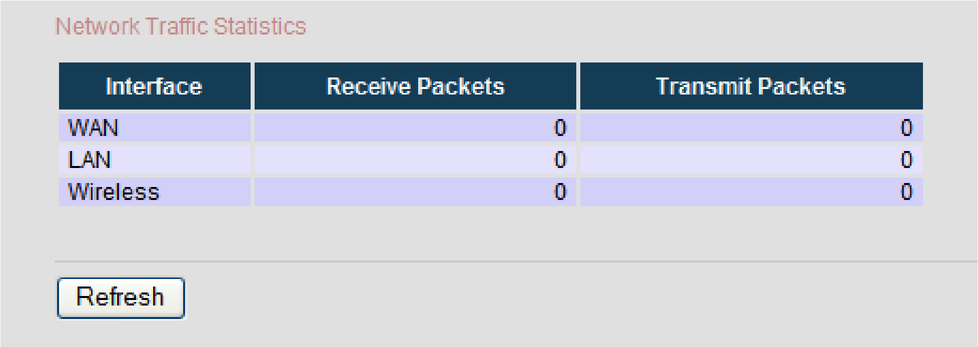
```
Address family not supported by protocol
Jun 12 00:00:15 hotspot user.notice hap: Starting DHCP
Jun 12 00:00:16 hotspot user.notice hap: Adding Additional Routing
Jun 12 00:00:16 hotspot user.notice hap: Starting Command Process
Jun 12 00:00:16 hotspot user.info modprobe: insmod -s  -kath0
Jun 12 00:00:17 hotspot user.notice hap: Device WLAN not found
Jun 12 00:00:17 hotspot user.notice hap: Hardware selftest result:
Device WLAN not found
Jun 12 00:00:17 hotspot user.notice hap: Booting finished
Jun 12 00:00:21 hotspot user.info modprobe: insmod -s  -kppp+
Jun 12 00:00:21 hotspot user.notice hap: Device ppp+ not found
Jun 12 00:20:05 hotspot user.info modprobe: insmod -s  -kppp0
Jun 12 00:20:06 hotspot user.info modprobe: insmod -s  -kppp+
Jun 12 00:20:06 hotspot user.notice hap: Device ppp+ not found
Jun 12 00:20:06 hotspot user.info modprobe: insmod -s  -kppp0
Jun 12 00:20:07 hotspot user.info modprobe: insmod -s  -kath0
Jun 12 00:20:07 hotspot user.info modprobe: insmod -s  -kath0
Jun 12 00:20:07 hotspot user.info modprobe: insmod -s  -kath0
Jun 12 00:20:07 hotspot user.info modprobe: insmod -s  -kath0
```

Click on the "Refresh" button to update the display of the system log.

Click on the "Clear" button to delete the system log.

4.5.3 Statistics

4.5.3.1 Network Traffic Statistics



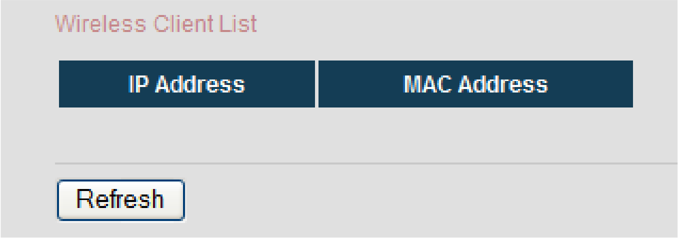
Network Traffic Statistics

Interface	Receive Packets	Transmit Packets
WAN	0	0
LAN	0	0
Wireless	0	0

This list shows the numbers of data packets received and transmitted through each of the router's interfaces up to the time when this web page was displayed. Click on the "Refresh" button to update the figures.

4.5.4 Wireless

4.5.4.1 Wireless Client List



Wireless Client List

IP Address	MAC Address

This list displays the IP addresses and MAC addresses of the wireless clients currently connected to your router. Click on the "Refresh" button to update the list.

4.6 Help

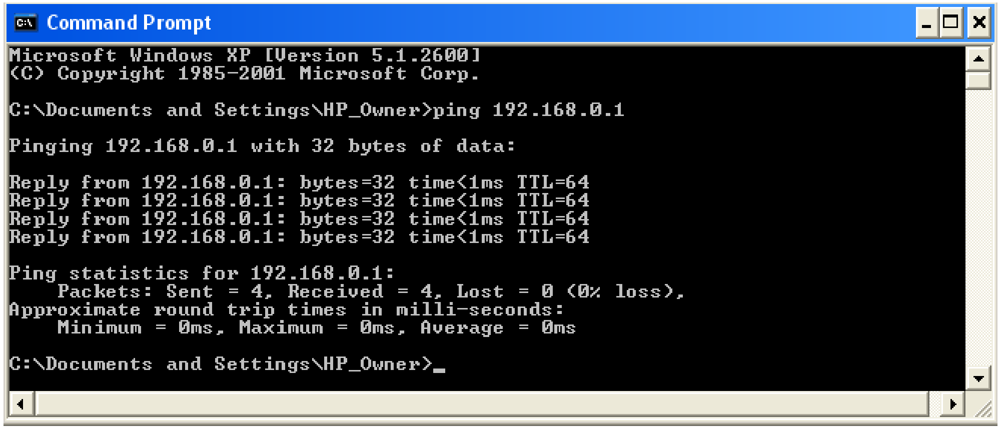
Please refer to this web page if you need help when configuring the router.

Appendix A: Troubleshooting

1. How do I test my Internet connection?

i. Go to Start > Run, type “cmd” and press “Enter”. A command prompt window will appear. In the command prompt window, type “ping” and the IP address of the router, i.e. “ping 192.168.0.1” and press “Enter”. If the router is connected, ping replies from the router will be observed as shown below. If there is no reply (Request timed out), try the ping command again using a different computer to verify that your computer is not the cause of the problem.

(**Note**: If you changed the IP address of the router, enter the new IP address of the router instead of “192.168.0.1”)



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\HP_Owner>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\HP_Owner>_
```

ii. In the command prompt window, type “ping www.google.com” and press “Enter”. If your computer is connected to the Internet, ping replies from the web server will be observed. If there is no reply (Request timed out), try the ping command again using a different computer to verify that your computer is not the cause of the problem.

2. How do I restore default/factory configuration?

There are two ways to restore default/factory configuration:

(**Warning**: All the user configuration settings will be deleted.)

i. Soft reset – Resetting the router to its factory configuration using the web-based utility:

- Type “http://192.168.0.1” in your web browser and press “Enter”.
- Go to Maintenance > Device Settings.
- In the “Restore Factory Defaults” section, click on the “Restore Defaults” button.

    - Reboot the router.

ii. Hard reset – Resetting the router to its factory configuration without knowing the administrator password or entering the web-based utility:

    - Turn off the router.
    - Set the Factory Default Switch to the ON position on the rear panel of the router.
    - Turn on the router and the factory default settings will be restored.
    - Remember to set the Factory Default Switch back to the OFF position; otherwise the router will restore to factory default settings on each power cycle.

(**Note**: The default username is “admin”, password is “admin”, and the router IP address is “192.168.0.1”.)

3. How do I reset the administrator password?

To reset the administrator password, perform a hard reset on the router as below:

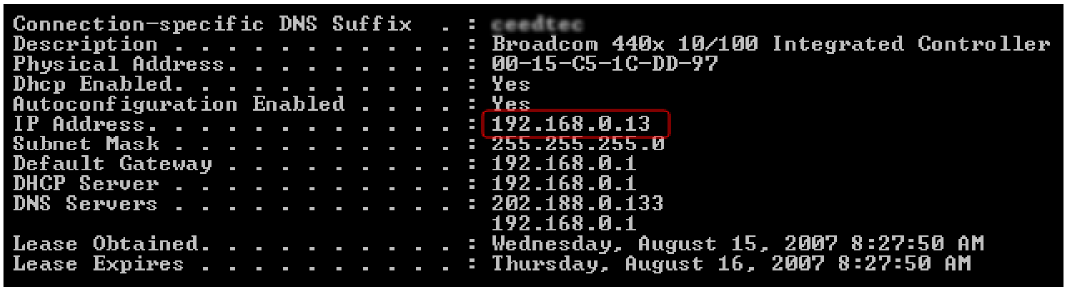
(**Warning**: All the user configuration settings will be deleted.)

- Turn off the router.
- Set the Factory Default Switch to the ON position on the rear panel of the router.
- Turn on the router and the factory default settings will be restored.
- Remember to set the Factory Default Switch back to the OFF position; otherwise the router will restore to factory default settings on each power cycle.

(**Note**: The default username is “admin”, password is “admin”, and the router IP address is “192.168.0.1”.)

4. How do I retrieve my computer’s IP address?

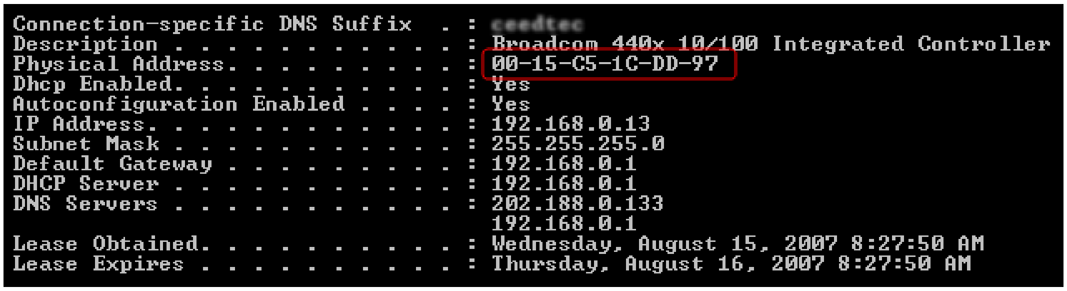
Go to Start > Run, type “cmd” and press “Enter”. A command prompt window will appear. In the command prompt window, type “ipconfig /all” and press “Enter”.



```
Connection-specific DNS Suffix  . : [redacted]
Description . . . . . . . . . . . : Broadcom 440x 10/100 Integrated Controller
Physical Address. . . . . . . . . : 00-15-C5-1C-DD-97
Dhcp Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . . . . . . . . : 192.168.0.13
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 192.168.0.1
DHCP Server . . . . . . . . . . . : 192.168.0.1
DNS Servers . . . . . . . . . . . : 202.188.0.133
                                    192.168.0.1
Lease Obtained. . . . . . . . . . : Wednesday, August 15, 2007 8:27:50 AM
Lease Expires . . . . . . . . . . : Thursday, August 16, 2007 8:27:50 AM
```

5. How do I retrieve my computer’s MAC address?

Go to Start > Run, type “cmd” and press “Enter”. A command prompt window will appear. In the command prompt window, type “ipconfig /all” and press “Enter”.



```
Connection-specific DNS Suffix  . : [redacted]
Description . . . . . . . . . . . : Broadcom 440x 10/100 Integrated Controller
Physical Address. . . . . . . . . : 00-15-C5-1C-DD-97
Dhcp Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . . . . . . . . : 192.168.0.13
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 192.168.0.1
DHCP Server . . . . . . . . . . . : 192.168.0.1
DNS Servers . . . . . . . . . . . : 202.188.0.133
                                    192.168.0.1
Lease Obtained. . . . . . . . . . : Wednesday, August 15, 2007 8:27:50 AM
Lease Expires . . . . . . . . . . : Thursday, August 16, 2007 8:27:50 AM
```

6. **How do I upgrade the router's firmware?**

- Download the latest firmware for your router from the iCoach website at www.icoach.net /support
- Access the router's web-based utility by typing "http://192.168.0.1" in the web browser and press "Enter".
- Go to Maintenance > Firmware.
- Click the "Browse" button to locate the downloaded firmware image file.
- Click the "Submit" button to upgrade the firmware.

(**Warning**: Firmware upgrade will take a few minutes. Don't turn off the power or reset the router during the firmware upgrade.)

7. **Why does my WiFi connection keep on disconnecting, show low signal strength, or suffer from slow data transfer rate?**

- WiFi connections use radio-based technology. Thus, the signal strength (and data transfer rate) decreases when the distance between your wireless device and the router increases. Hence, try to move your wireless devices as near as possible to the router. (The indoor operating range is up to 100m, varies depending on the surrounding environment.)

- The use of 2.4 GHz cordless phones, transmitters, or other wireless connections operating at the same frequency might affect the router's signal strength. Changing the frequency channel of the router might help to improve your network's signal strength, performance and reliability. Please refer to section "4.2.2.1 Wireless Settings" on how to change the frequency channel.

- Place the router at least 5-10 inches from the wall or any other objects.

- Avoid electromagnetic interference by placing the router at least 5 feet from electrical devices generating RF noise, such as television, microwave oven, etc.

8. **Why am I unable to connect to the wireless LAN?**

Check the LED's on the top panel of the router. The "PWR" LED should be on.

If the “PWR” LED is off, check the power connector and make sure the router is powered on properly.

If the “PWR” LED is on, then open the wireless utility software which is located in the system tray at the bottom right of your computer screen. Look out for the list of “Available Networks”.

If your network name is listed in the “Available Networks”, click on your network name to connect to it. You will need to enter the WEP key if WEP encryption is enabled in the router; or WPA passphrase if WPA/WPA2 is enabled in the router. The WEP key or WPA passphrase can be found in the router’s web page Basic > Wireless.

If your network name is not in the list, try to move your device (notebook) as near as five to ten feet to the router. If your network name does appear in the list this time, it means you have a signal interference problem. Please refer to section “3.3 Establishing the Best Location” for more information.

If your network name still does not appear in the list even after you have moved your device nearer, make a wired (LAN) connection between your computer and the router. Type “http://192.168.0.1” in your web browser and press “Enter”. Go to Advanced > Wireless and make sure the “SSID Broadcast” is enabled.

9. **I have my computer connected to the router using Ethernet cable. The LAN LED of the router is on, and the LAN port light is flashing, however, I cannot access to the router. When I look at the connection properties, it says "Invalid IP Address". I've clicked on the "Repair" button a few times but it either says cannot repair or changes to "Automatic Private Address" but still no connectivity.**

   After connecting a network cable between your computer and the router’s LAN port, if your computer fails to access the network including the web-based utility from the router, then the network port of your computer may not support Auto MDI/MDIX. Replace the network cable with a crossover network cable (included with the router).

   If you require further technical assistance with your iCoach router please email customercare@icoach.net, visit www.icoach.net/support or call 1-866-418-1803.

Appendix B: Safety Information

- Follow any special regulations in force in any areas and always turn off the device when its use is prohibited or when it may cause interference or danger.

- When on board an aircraft, turn off the device when instructed to do so. Wireless devices can cause interference in the aircraft.

- Do not use the device in areas with potentially explosive atmospheres. These areas include fuelling areas such as below decks on boats, fuel or chemical transfer or storage facilities, areas where the air contains chemicals or particles such as grain, dust or metal powders.

- Do not use the device in blasting areas to avoid possible interference with the blasting operations.

- In hospitals or other health care facilities, turn off the device when instructed to do so. Some medical equipment may be sensitive to external RF energy.

- Do not hold the antenna when the device is in use. Holding the antenna may affect signal quality, causing the device to operate at a higher power level than necessary.

Appendix C: Care and Maintenance

- Do not use and store the device in areas with high temperature or high humidity.
- Keep the device dry - the device is not water-resistant.
- Avoid using the device or its accessories outdoors.
- Do not share the power source for this device with other equipments.
- If the device becomes too hot, turn off the power immediately and have it checked by an authorized service personnel.
- Only install the device in the positions described by this User Guide or the Mobile Installation instructions.
- Only use the power adapter comes with the package. Using power adapter with a different rating may damage the device.
- Do not open and repair the device yourself. If you suspect the device is not functioning properly, take it to the authorized service centre for service.
- Do not shake, knock, or drop the device.
- Do not use cleaning solvents, or strong detergents to clean the device.

Appendix D: Technical Specifications

- **Data and Routing Protocols:**
  TCP/IP, NAT, DHCP Server, NTP

- **Wireless Security:**
  WEP 64-bit/128-bit, WPA/WPA2 Personal

- **LAN Security:**
  NAT, Firewall with SPI Mode, VPN Pass-through, IP Filtering, MAC Filtering

- **Protected Configuration for Web-based Utility:**
  Password Protection, Remote Access via HTTPS

- **Power Adapter Input:**
  100-240V AC, 50/60Hz, 0.35A

- **Power Adapter Output:**
  12V DC, 1.0A - 1.5A

- **Dimensions (W x H x D):**
  132mm x 36.5mm x 134mm (5.20” x 1.44” x 5.28”)

- **Weight:**
  277.6g

- **Operating Temperature:**
  0˚C to 40˚C (32˚F to 104˚F)

- **Storage Temperature:**
  -20°C to 70°C (-4°F to 158°F)

- **Operating Humidity:**
  20% to 80% Non-condensing

- **Storage Humidity:**
  10% to 90% Non-condensing

Appendix E: Manufacturer’s Limited Warranty

Tech Electronic Services warrants its product to be substantially free from defects in materials and workmanship under normal use for a period of twelve (12) months from the date of purchase.

During the warranty period, Tech Electronic Services will, at its option, either repair the defective product, or replace it with a similar product.

To exercise this warranty contact Tech Electronic Services at www.icoach.net/support, email: customercare@icoach.net or call 1-866-418-1803.

If you are requested to return the product, send the product, transportation prepaid, to the indicated service facility. You must include a copy of your original proof of purchase. Repairs will be made and the product will be returned, transportation prepaid. Repaired or replaced products are warranted for the remainder of the original warranty period or for sixty (60) days from the date of repair, whichever is longer.

This limited warranty extends only to the original purchaser, and is valid only in the country of purchase.

This warranty does not cover normal wear and tear, and is invalidated if the product (a) has been modified without Tech Electronic Services’ express written consent, (b) has not been installed, operated, or maintained in accordance to the instructions and guidelines supplied by Tech Electronic Services, or (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident.

Tech Electronic Services provides no warranty or support for any third-party software or accessories included or bundled with the product or installed by the customer.

This warranty is in lieu of all other warranties, expressed or implied, including any implied warranty of merchantability or fitness for a particular use. The remedies provided herein are buyer’s sole and exclusive remedies.

Neither Tech Electronic Services nor any of its employees shall be liable for any lost data, revenue or profit, or for any direct, indirect, special, incidental or consequential damages arising out of the use of its products even if have been advised in advance of the possibility of such damages. In no event will Tech Electronic Services’ liability exceed the amount paid by you for the product.

All warranty information, product features and specifications are subject to change without notice.

Appendix F: Regulatory Information

Federal Communication Commission (FCC) Interference Statement

FCC Part 15: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

MODIFICATION: Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the device.

This product contain FCC ID: W63-RWW023

WARNING: To satisfy FCC RF exposure requirements for mobile transmitting devices, a separation distance of 20cm or more should be maintained between the antenna of this device and persons during device operation. To ensure compliance, operations at closer than this distance is not recommended. The antenna used for this transmitter must not be co-located in conjunction with any other antenna or transmitter.

Appendix G: Contact Information

For technical support or questions regarding your iCoach router please contact us via:

Email: customercare@icoach.net

Web: www.icoach.net/support

Phone: 1-866-418-1803

Mail:

Tech Electronic Services - iCoach
76 St David Street
Lindsay, ON
Canada
K9V 1N7

Glossary

3G: 3G is third-generation technology for mobile phone system which enables wide-area wireless voice telephony and broadband wireless data.

APN: *Access Point Name.* An APN represents a point of connection of GPRS/3G network to other external network, e.g. the Internet.

Class A Network: In a Class A network, the first 8 binary digits of the IP address indicate the network address while the rest 24 binary digits indicate the host address. A Class A network is able to support up to 16,777,214 (2^{24} – 2) host IP addresses.

Class B Network: In a Class B network, the first 16 binary digits of the IP address indicate the network address while the rest 16 binary digits indicate the host address. A Class B network is able to support up to 65,534 (2^{16} – 2) host IP addresses.

Class C Network: In a Class C network, the first 24 binary digits of the IP address indicate the network address while the rest 8 binary digits indicate the host address. A Class C network is able to support up to 254 (2^{8} – 2) host IP addresses.

DHCP Server: *Dynamic Host Configuration Protocol Server*. A DHCP server assigns unique IP addresses to clients (computers, routers or network adapters) attached to an IP network.

DNS Server: *Domain Name System Server*. A DNS server translates human-language URLs and email addresses into machine-language IP addresses. An IP address is made up of 32 bits which is normally expressed in 8-bit decimal numbers of the format xxx.xxx.xxx.xxx.

EVDO: *Evolution Data Optimized*. EVDO is one of two major 3G standards for high speed wireless broadband. The other competing standard is known as WCDMA.

Firewall: A firewall filters through all inbound data packets from the Internet to ensure that they are safe before forwarding the data packets through. Any data packets that do not fulfill the security criteria will be blocked from entering the network.

GPRS: *General Packet Radio Service*. GPRS is a technology that uses the existing GSM network to transmit and receive IP packets to and from GPRS mobile devices.

GSM: *Global Systems for Mobile Communications*. GSM is a 2G mobile phone system. It is the most popular standard for mobile phones used world-wide.

HSDPA: *High-Speed Downlink Packet Access*. HSDPA is a 3.5G wireless technology which provides download speeds on wireless devices equivalent to wired ADSL connections. HSDPA improves on WCDMA by using different techniques for modulation and coding.

.

IEEE 802.11b: A set of standards developed for wireless LAN which allows wireless devices from different manufacturers to communicate with each other. The IEEE 802.11b standard operates at a maximum data transfer rate of 11 Mbps at frequency 2.4GHz.

IEEE 802.11g: A set of standards developed for wireless LAN which allows wireless devices from different manufacturers to communicate with each other. The IEEE 802.11g standard operates at a maximum data transfer rate of 54 Mbps at frequency 2.4GHz.

IP: *Internet Protocol.* IP is the network protocol used for delivering data across the Internet.

IP Address: *Internet Protocol Address.* An IP address is a unique address used to identify individual computer connected to an IP network, e.g. the Internet. An IP address is made up of 32 bits which is normally expressed in 8-bit decimal numbers of the format xxx.xxx.xxx.xxx.

IPSec: *Internet Protocol Security.* IPSec is a suite of protocols that provides traffic encryption, integrity validation, peer authentication and anti-replay. IPSec is widely used to implement virtual private network (VPN).

LAN: *Local Area Network*. A LAN is a network formed by a group of computers connected to each other via cabled or wireless connections. A computer connected to the LAN is able to access other computers on the network, allowing a convenient way of sharing resources over the established links.

MAC Address: *Media Access Control Address*. A MAC address is a unique identifier attached to each network card which can be used to identify individual computer on a network. It is made up of 12 hexadecimal digits of the format xx-xx-xx-xx-xx-xx.

NTP Server: *Network Time Protocol Server*. An NTP server updates the clock times of computers connected to the network via Network Time Protocol (NTP). This ensures accurate synchronization of computer clock times of all computers on the network.

PDP: *Packet Data Protocol*. PDP is a network protocol used for exchanging data between a packet switching network and a GPRS/3G network.

PPP: *Point-to-Point Protocol*. PPP is a standard protocol used for dial-up modem connections to the Internet. PPP provides a link from your computer to a server where your data packets will be forwarded to the Internet and vice versa.

PPTP: *Point-to-Point Tunneling Protocol*. PPTP is a protocol used for implementing virtual private network (VPN). It enables the secure transfer of data between two VPN end points.

SPI Mode: *Stateful Packet Inspection Mode*. A firewall typically behaves as a filter between one network to another. A firewall with SPI mode examines the contents of the data packets instead of just filtering them. All incoming data packets are analyzed to confirm that they are legitimate replies to outgoing requests made from client computers within the network.

.

Subnet Mask: A subnet mask determines which portion of an IP address belongs to the network and which portion belongs to the client computer.

TCP: *Transmission Control Protocol.* TCP is a communication protocol used by the Internet. TCP breaks up the data packets at the sending end and reassembles them at the receiving end. Received packets are checked and acknowledged, while lost or corrupted packets are resent.

UDP: *User Datagram Protocol.* UDP is a communication protocol used by the Internet. UDP is more efficient than TCP but it is less reliable. Unlike TCP, UDP does not break up and reassemble packets, nor does it check or acknowledge received packets.

VPN: Virtual Private Network. VPN is a technology that enables a private or secure network connection to be established within an open public network, such as the Internet.

VPN Pass-through: A VPN pass-through device allows data traffic from the two VPN end points to pass through, but itself is not a VPN end point.

WAN: *Wide Area Network.* A WAN spans a large geographical area, connecting two or more local area networks (LANs). The Internet is an example of a public WAN.

WAN Ping: WAN ping is the action of pinging a WAN IP address to verify the IP address's validity. The "ping" command sends packets to the target host and waits for its replies to verify the existence of the target host.

WCDMA: *Wideband Code Division Multiple Access.* WCDMA is a 3G wireless technology with higher wireless data speed. WCDMA transmits over a pair of 5 MHz wide radio channels.

WEP: *Wired Equivalent Privacy.* WEP was designed to give wireless networks the equivalent data protection as wired networks. There are two levels of WEP encryption available: 64-bit and 128-bit.

WLAN: *Wireless Local Area Network.* WLAN (or more commonly known as WiFi) enables local area network (LAN) to be deployed without cabling. WLAN transmits and receives data via radio signals.

Index

2

2G, 44

3

3.5G, 44
3G, 3, 44, 45, 46

A

Access Point Name, 44
APN, 11, 44

B

beacon interval, 23

D

daylight saving, 28
DHCP, 16, 17, 30, 40, 44
DNS, 12, 30, 44
Domain Name System, 44
DTIM interval, 23
Dynamic Host Configuration Protocol, 44

E

EDGE, 1, 31
EVDO, 31, 44

F

firewall, 1, 21, 22, 40, 44, 45
  settings, 22
firmware
  upgrade, 28, 36
  version, 28
fragmentation threshold, 23

G

General Packet Radio Service, 44
Global Systems for Mobile Communications, 44
GPRS, 1, 31, 44, 45
GSM, 44

H

High-Speed Downlink Packet Access, 44
HSDPA, 44
HSxPA, 1, 31

I

IEEE 802.11b, 45
IEEE 802.11g, 45
Internet access policy, 20
Internet Protocol, 45
Internet Protocol Security, 45
IP, 44, 45
  dynamic client, 17, 18
  fixed client, 13, 14, 15, 16, 17
IP address, 12, 15, 16, 17, 18, 19, 21, 24, 25, 29, 30, 32, 33, 34, 35, 44, 45, 46
IP filtering, 40
IPSec, 26, 45

L

LAN, 2, 4, 7, 9, 10, 15, 16, 30, 36, 37, 40, 45, 46
Local Area Network, 45

M

MAC address, 16, 17, 18, 21, 30, 31, 33, 35, 45
MAC filtering, 40
Media Access Control, 45

N

NAT, 1, 40
network
  Class A, 44
  Class B, 44
  Class C, 15, 44
Network Address Translation, 1
Network Time Protocol, 29, 45
NTP, 29, 40, 45

P

Packet Data Protocol, 45
PDP, 45
ping, 22, 25, 34, 46
Point-to-Point Protocol, 45
Point-to-Point Tunneling Protocol, 45
port forwarding, 18, 19
PPP, 45
PPTP, 26, 45

R

remote management, 25, 26
RTS threshold, 23

S

settings
- backup to file, 27
- restore factory defaults, 27, 34
- restore from file, 27

SIM card, 1, 3, 4
SPI, 1, 22, 40, 45
SSID, 5, 12, 23, 32, 37, 42
Stateful Packet Inspection, 1, 45
static route, 24, 25
subnet mask, 15, 24, 30, 46
syslog, 32
system time, 28, 29

T

TCP, 19, 46
TCP/IP, 40
time zone, 28
Transmission Control Protocol, 46

U

UDP, 19, 46
UMTS, 1, 31
User Datagram Protocol, 46

V

Virtual Private Network, 46
VPN, 26, 45, 46
VPN end point, 45, 46
VPN pass-through, 26, 40, 46

W

WAN, 22, 30, 46
WCDMA, 44, 46
WEP, 1, 13, 14, 23, 37, 40, 46
Wide Area Network, 46
Wideband Code Division Multiple Access, 46
WiFi, 2, 31, 32, 36, 46
Wired Equivalent Privacy, 46
Wireless Local Area Network, 46
WLAN, 1, 2, 9, 46