

# User's Manual

## Internet Broadband Router **XRT-401F**



## **Copyright**

Copyright (C) 2010 PLANET Technology Corp. All rights reserved.

The products and programs described in this User's Manual are licensed products of PLANET Technology. This User's Manual contains proprietary information protected by copyright, and this User's Manual and all accompanying hardware, software, and documentation are copyrighted. No part of this User's Manual may be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form by any means by electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, and without the prior express written permission of PLANET Technology.

## **Disclaimer**

PLANET Technology does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose PLANET has made every effort to ensure that this User's Manual is accurate; PLANET disclaims liability for any inaccuracies or omissions that may have occurred. Information in this User's Manual is subject to change without notice and does not represent a commitment on the part of PLANET. PLANET assumes no responsibility for any inaccuracies that may be contained in this User's Manual. PLANET makes no commitment to update or keep current the information in this User's Manual, and reserves the right to make improvements to this User's Manual and/or to the products described in this User's Manual, at any time without notice. If you find information in this manual that is incorrect, misleading, or incomplete, we would appreciate your comments and suggestions.

## **FCC Compliance Statement**

This equipment generates and uses radio frequency energy and if not installed and used properly, that is, in strict accordance with the instructions provided with the equipment, may cause interference to radio and TV communication. The equipment has been tested and found to comply with the limits for a Class A computing device in accordance with the specifications in Subpart B of Part 15 of FCC rules, which are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation. If you suspect this equipment is causing interference, turn your Ethernet Switch on and off while your radio or TV is showing interference, if the interference disappears when you turn your Ethernet Switch off and reappears when you turn it back on, there is interference being caused by the Ethernet Switch. You can try to correct the interference by one or more of the following measures:

1. Reorient the receiving radio or TV antenna where this may be done safely.
2. To the extent possible, relocate the radio, TV or other receiver away from the Switch.
3. Plug the Ethernet Switch into a different power outlet so that the Switch and the receiver are on different branch circuits.

If necessary, you should consult the place of purchase or an experienced radio/television technician for additional suggestions.

## **Energy Saving Note of the Device**

This power required device does not support Stand by mode operation.

For energy saving, please remove the DC-plug to disconnect the device from the power circuit.

Without remove the DC-plug, the device will still consuming power from the power circuit. In the view of Saving the Energy and reduce the unnecessary power consuming, it is strongly suggested to switch off or remove the DC-plug for the device if this device is not intended to be active.

## **CE mark Warning**

The is a class A device, In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

## **WEEE**

To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

## **Trademarks**

The PLANET logo is a trademark of PLANET Technology. This documentation may refer to numerous hardware and software products by their trade names. In most, if not all cases, these designations are claimed as trademarks or registered trademarks by their respective companies.

## **Revision**

User's Manual for PLANET Internet Broadband Router:

Model: XRT-401F

Rev: 1.1 (Aug. 2011)

Part No.: EM-XRT401Fv1 (2080-B40110-000)

## TABLE OF CONTENTS

Chapter 1 Introduction .....	6
1.1 Features.....	6
1.2 Minimum Requirements.....	7
1.3 Product Specification .....	8
1.4 Getting Started .....	10
Chapter 2 Quick Setup .....	17
2.1 Dynamic IP.....	19
2.2 Static IP .....	20
2.3 PPPoE .....	21
2.4 PPTP.....	22
2.5 L2TP .....	23
Chapter 3 Advance Features .....	25
3.1 Admin.....	26
3.1.1 Management.....	27
3.1.2 System Settings.....	28
3.1.3 Firmware Upgrade .....	29
3.1.4 Configuration and Tool .....	30
3.1.5 Log Setting.....	31
3.2 WAN .....	32
3.2.1 Dynamic IP .....	33
3.2.2 Static IP .....	35
3.2.3 PPPoE (PPP over Ethernet) .....	36
3.2.4 PPTP .....	38
3.2.5 L2TP.....	41
3.2.6 BigPond (Australia) .....	43
3.3 LAN .....	
3.3.1 LAN Settings .....	44
3.3.2 DHCP Client List .....	45
3.3.3 VLAN Settings.....	46
3.3.4 Broadcast Storm Control .....	48
3.3.5 IGMP .....	48
3.4 NAT .....	
3.4.1 Virtual Server .....	51
3.4.2 Port Triggering.....	52
3.4.3 Port Mapping.....	54
3.4.4 Passthrough.....	55
3.4.5 DMZ.....	56
3.5 Firewall .....	57
3.5.1 Firewall Options.....	58
3.5.2 Client Filtering .....	59
3.5.3 URL Filtering .....	60

3.5.4 MAC Filtering .....	61
3.6 Routing .....	62
3.6.1 Routing Table .....	62
3.6.2 Static Routing .....	63
3.6.3 Dynamic Routing .....	64
3.7 QoS	
3.7.1 IP based .....	65
3.7.2 Port based .....	66
3.7.3 DSCP .....	67
3.8 Other .....	69
3.8.1 UPnP .....	69
3.8.2 DDNS .....	71
3.9 Status .....	72
3.9.1 System Status .....	72
3.9.2 System Log .....	73
Appendix A .....	74
Appendix B .....	75
Glossary .....	1

# Chapter 1 Introduction

With the growth of the Internet activities, high-speed Internet access, on-line gaming and Triple-Play Internet application are often can be seen in our dailiy life. To respond this trends of Internet activities, the PLANET XRT-401F Broadband Router is an ideal solution to provide the high speed Internet access, easy-to-use, and worry-free for surfing on the internet.

With easy integration and full compatibility of existing network infrastructures, the PLANET XRT-401F comprises a 4-Port 10/100Mbps switch to allow the users quickly and easily transmitting the data through the single high-speed Internet connection.

The XRT-401F provides QoS and IGMP features to make the network services smooth. Traffic priority can be assigned by the router to guarantee some important and specific transmissions, especially for real-time streaming multimedia applications such as the on-line gaming, VoIP, and IPTV to keep the bandwidth usage smoothly.

Via the user-friendly management interface, users can setup and configure the router very easily, just follow the wizard to guide you the setup procedure step by step. Furthermore, the Router not only provides basic router functions such as DHCP server, Virtual Server, DMZ, and UPnP, but also provides full security functions including Firewall and NAT / NAPT (Network Address/Port Translation) features, to protect your network from internet intruders and attacks.

## 1.1 Features

### ■ Internet Access Features

- ◆ **Shared Internet Access:** All users on the LAN can access the Internet through the XRT-401F using only a single external IP Address. The local (invalid) IP Addresses are hidden from external sources. This process is called NAT (Network Address Translation).
- ◆ **Multiple WAN Connection:** On the Internet (WAN port) connection, the XRT-401F supports Dynamic IP Address (IP Address is allocated on connection), Fixed IP Address, PPPoE, PPTP and L2TP.
- ◆ **Bridge and Router Application:** The XRT-401F supports two application modes. Currently, it comes pre-configured with Router mode. Note that, Router mode and Bridge mode cannot be used simultaneously.

### ■ Advanced Internet Functions

- ◆ **Quick Setup:** Built-In configuration wizard helps users to complete network installation in a very short time via standard Internet browsers such as Microsoft Internet Explorer, Netscape Communicator...etc.
- ◆ **QoS:** Quality of service can classify the network packet based on the port base and DSCP; it can provide the best effect for real-time streaming multimedia applications such as the on-line gaming, VoIP, and IPTV.
- ◆ **Virtual Servers:** This feature allows Internet users to access Internet servers on your LAN. The required setup is quick and easy.

- ◆ **Universal Plug and Play (UPnP):** UPnP allows automatic discovery and configuration of the Broadband Router. UPnP is supported by Windows ME, XP, or later.
  - ◆ **User Friendly Interface:** The XRT-401F can be managed and controlled through Web UI.
  - ◆ **DMZ Support:** The XRT-401F can translate public IP addresses to private IP address to allow unlimited 2-Way communication with the servers or individual users on the Internet. It provides the most flexibility to run programs smoothly for programs that might be restricted in NAT environment.
  - ◆ **Client / URL / MAC Filtering:** The Filtering function can block the unallowable LAN users accessing to Internet. Or you can use the keyword based URL Filter to block access to undesirable Web sites by LAN users.
  - ◆ **RIP1/2 Routing:** It supports RIPv1/2 routing protocol for routing capability.
  - ◆ **VPN Pass through Support:** PCs with VPN (Virtual Private Networking) software are transparently supported - no configuration is required.
- **LAN Features**
- ◆ **4-Port Switch:** The XRT-401F incorporates a 4-port 10/100Base-TX switching hub, making it easy to create or extend your LAN.
  - ◆ **DHCP Server Support:** Dynamic Host Configuration Protocol provides a dynamic IP address to PCs and other devices upon request. The XRT-401F can act as a DHCP Server for devices on your local LAN.

## 1.2 Minimum Requirements

- One External xDSL (ADSL) or Cable modem with an Ethernet port (RJ-45)
- Network Interface Card (NIC) for each Personal Computer (PC)
- PCs with a Web-Browser (Internet Explorer 7.0 or higher, or Firefox 3.6 or higher)

## 1.3 Product Specification

### FUNCTIONAL SPECIFICATIONS

<b>Product</b>		Internet Broadband Router
<b>Model</b>		XRT-401F
<b>Hardware</b>		
<b>Standard</b>		IEEE 802.3, IEEE 802.3u 10/100Base-TX standard
<b>Ports</b>	<b>WAN</b>	1 x 10/100Base-TX, Auto-Negotiation, Auto MDI/MDI-X
	<b>LAN</b>	4 x 10/100Base-TX, Auto-Negotiation, Auto MDI/MDI-X
<b>LED Indicators</b>		PWR, WAN, LAN1-4
<b>Button</b>		1 x RESET button
<b>Software</b>		
<b>Protocol and Features</b>		Router and Bridge mode Static Routing and RIPv1/2 DMZ and Virtual Server QoS IGMP v1/v2 VLAN SNTP DHCP Server / Client UPnP and DDNS
<b>VPN</b>		IPSec / PPTP / L2TP VPN Pass-Through
<b>Security</b>		Built-in NAT Firewall Client / URL / MAC Filtering Password protection for system management
<b>Management</b>		Web-based configuration Quick Setup Wizard Local and Remote Log
<b>Environment Specification</b>		
<b>Dimension (W x D x H)</b>		176 x 104 x 29 mm
<b>Power</b>		12V DC, 0.5A
<b>Temperature / Humidity</b>		Operating: 0~50 degree C, 5%~ 90% (non-condensing), Storage: -10~70 degree C, 0~95% (non-condensing)

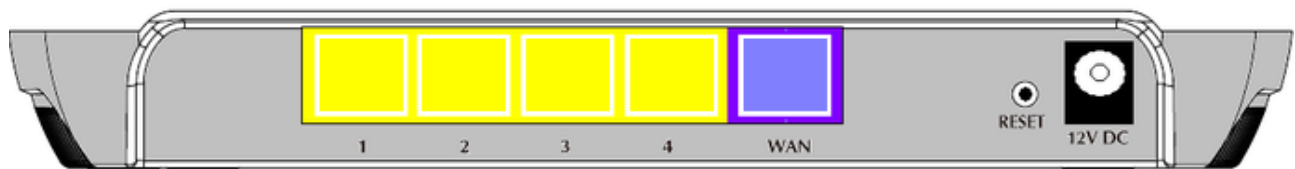


## Top Panel LED definition



LED		Description
PWR	ON	When the router is powered on, and in ready state.
	OFF	When the router is powered off.
WAN	Flashing	Data is being transmitted or received via the corresponding WAN port.
	ON	The port is up.
LAN1-4	Flashing	Data is being transmitted or received via the corresponding LAN port.
	ON	The port is up.

## Rear Panel Port and Button Definition

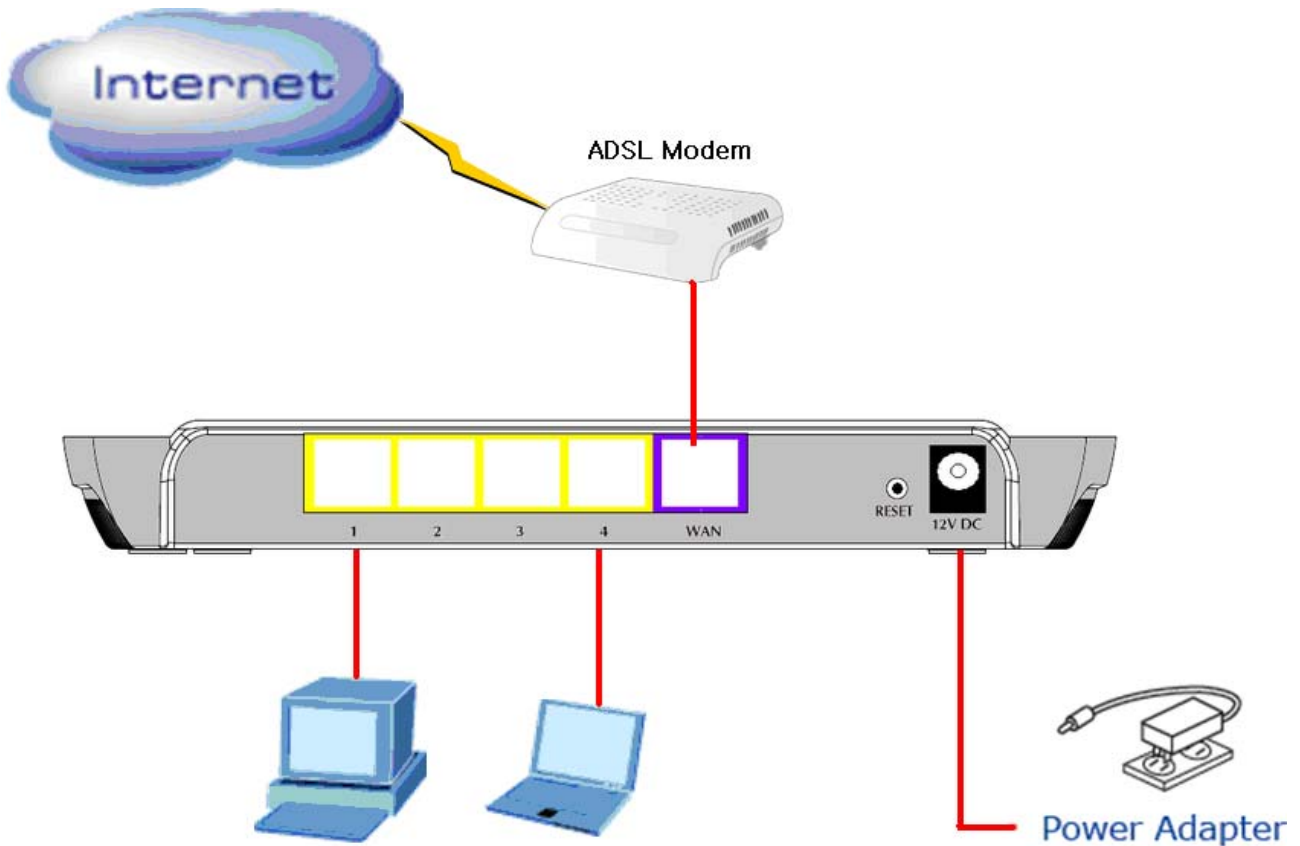


Port	Description
LAN (1-4)	Connect your LAN's PCs, printer servers, hubs and switches etc.
WAN	Connect your xDSL or Cable modem and is linked to the Internet.
RESET	One push and release, the Router will reboot At power on status, press more than 10 seconds and release for reset to factory default setting.
12V DC	DC Power in.

## 1.4 Getting Started

This is a step-by-step instruction on how to start using the router and get connected to the Internet.

1) Setup your network as shown in the setup diagram below.



2) Then, you need to setup your LAN PC clients so that it can obtain an IP address automatically. By default the XRT-401F's DHCP server is enabled so that you can obtain an IP address automatically.



### Note

Please make sure that the XRT-401F's DHCP server is the only DHCP server available on your LAN. If there is another DHCP on your network, then you'll need to switch one of the DHCP servers off.

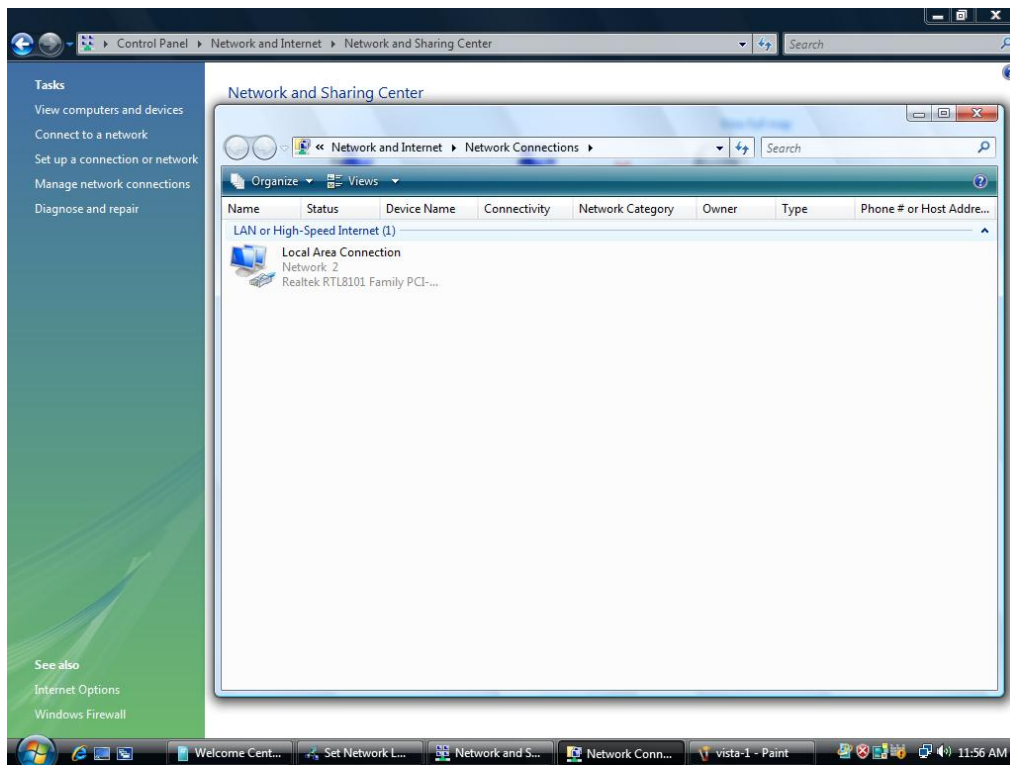
### Step1 → Configure your PC to obtain an IP address automatically

This section will show you how to configure your PC's so that it can obtain an IP address automatically for either Windows 98/Me, 2000 or later operating systems. For other operating systems (Macintosh, Sun, etc.), please follow the manufacturer's instructions.

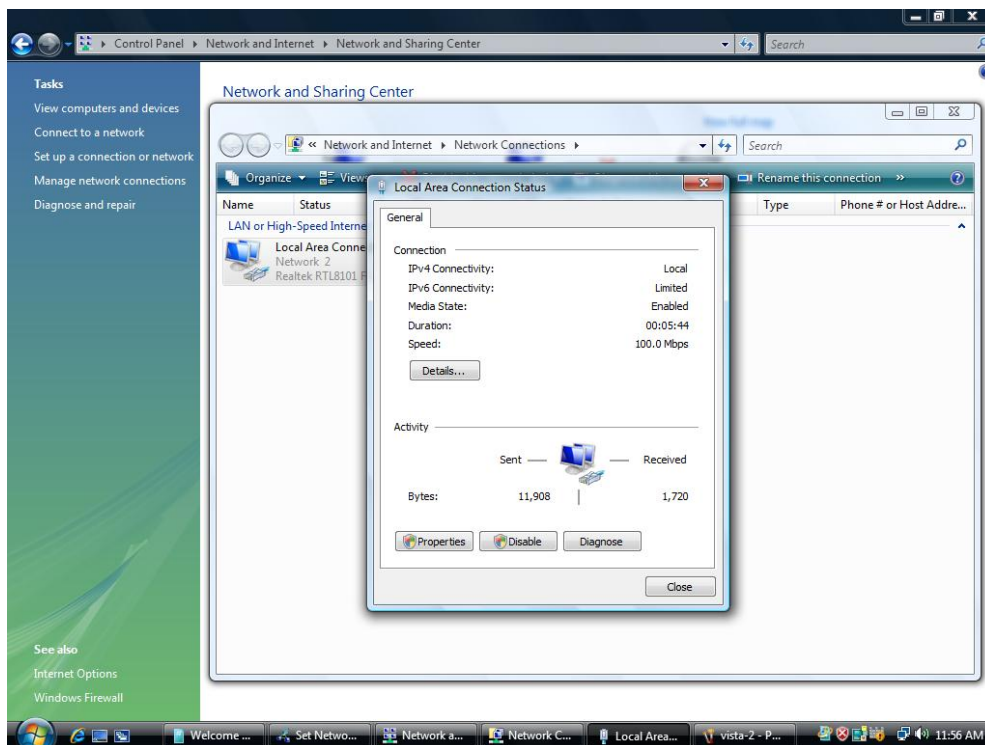
The following is a step-by-step illustration on how to configure your PC to obtain an IP address automatically for **a) Windows Vista, b) Windows XP, c) Windows 2000**

## a) Configuring PC in Windows Vista

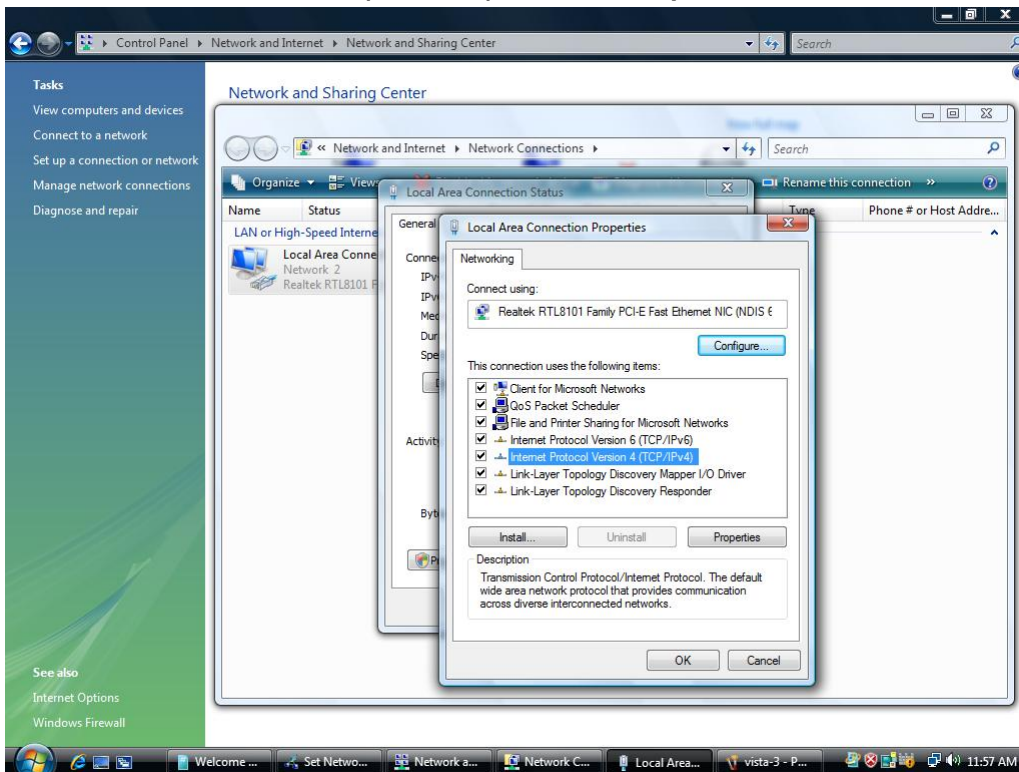
1. Go to **Start / Control Panel / Network and Internet / Network and Sharing Center**. Double-click on **Network Connections**.
2. Double-click **Local Area Connection**.



3. In the **Local Area Connection Status** window, click **Properties**.

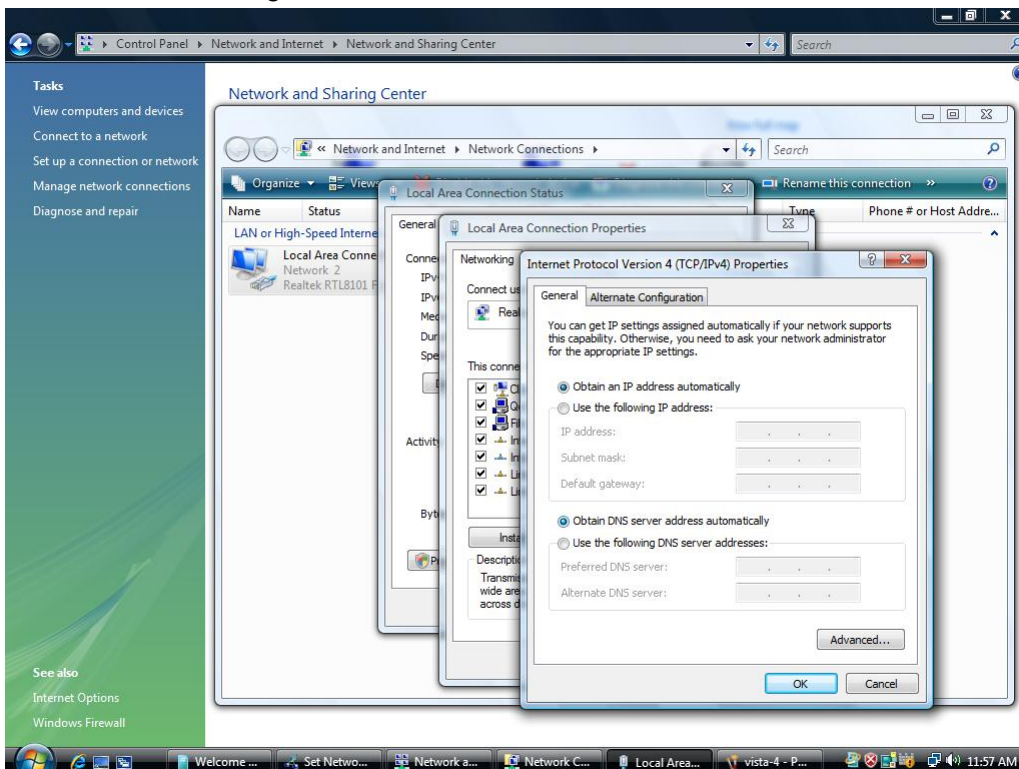


4. Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.



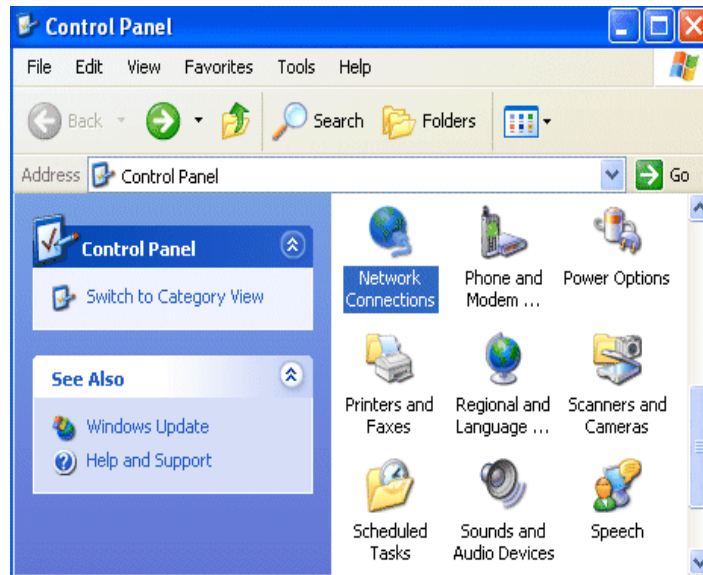
5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.

6. Click **OK** to finish the configuration.

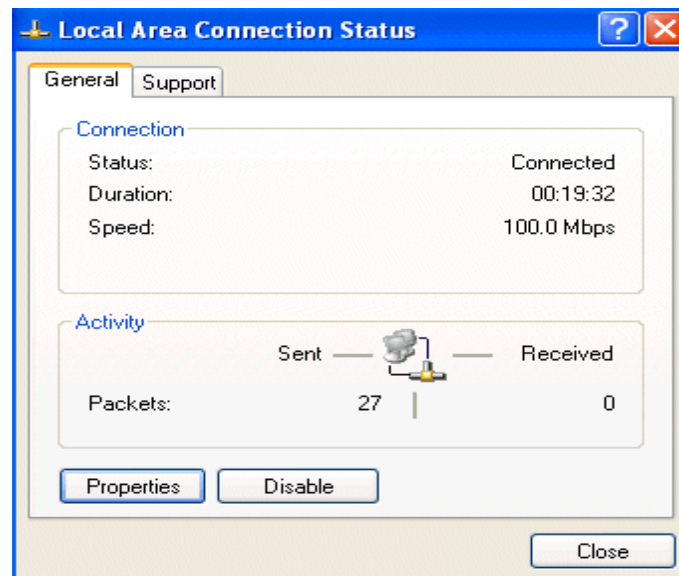


## b) Configuring PC in Windows XP

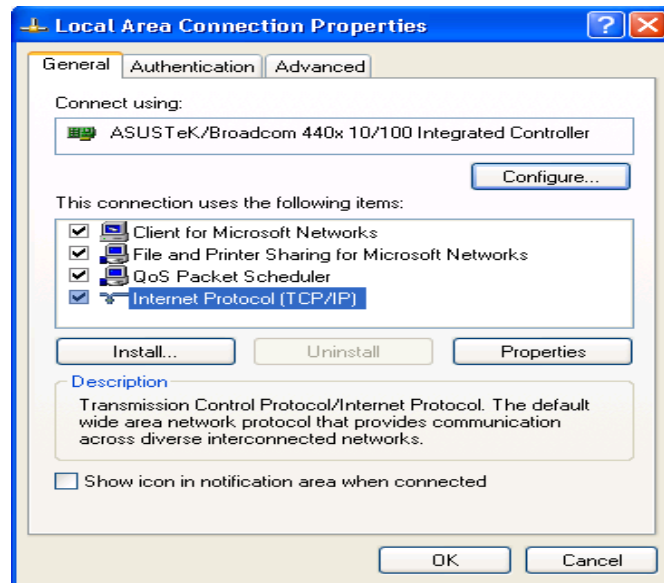
1. Go to **Start / Control Panel (in Classic View)**. In the Control Panel, double-click on **Network Connections**
2. Double-click **Local Area Connection**.



3. In the **Local Area Connection Status** window, click **Properties**.

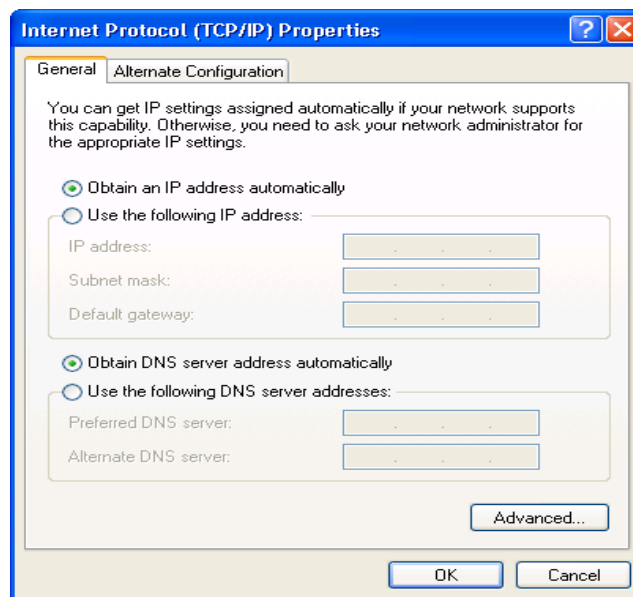


4. Select **Internet Protocol (TCP/IP)** and click **Properties**.



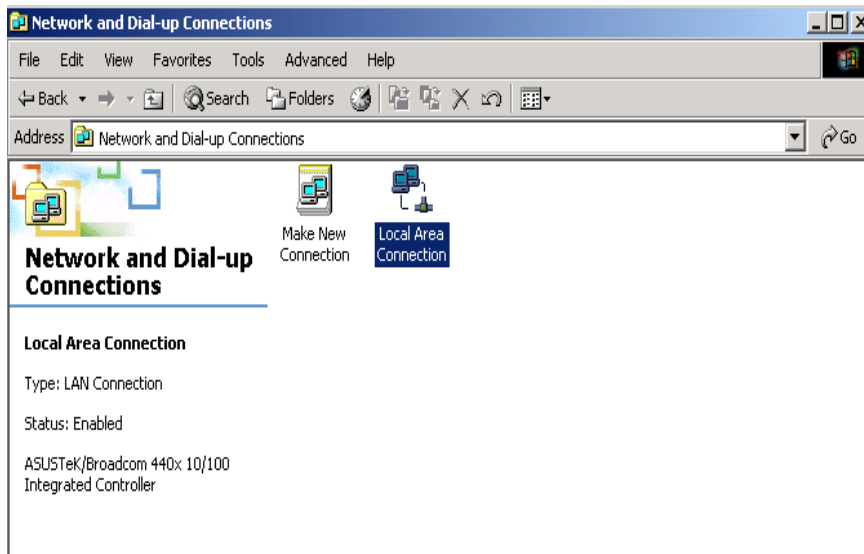
5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.

6. Click **OK** to finish the configuration.

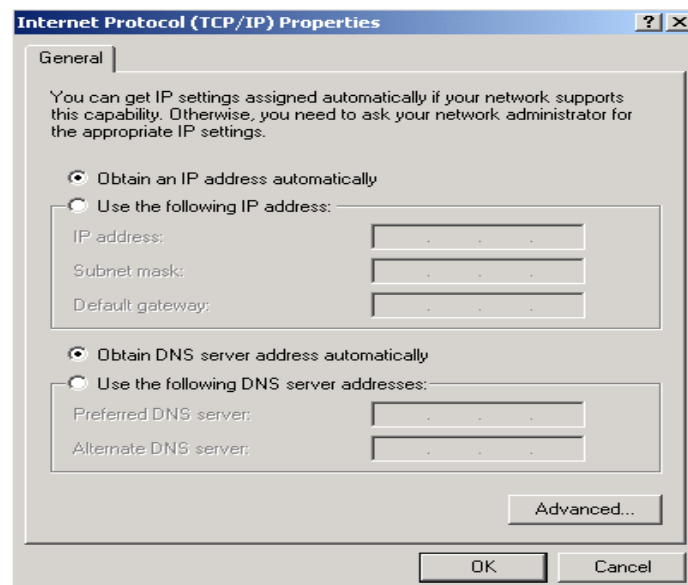


## c) Configuring PC in Windows 2000

1. Go to **Start / Settings / Control Panel**. In the Control Panel, double-click on **Network and Dial-up Connections**.
2. Double-click **Local Area Connection**.



3. In the **Local Area Connection Status** window click **Properties**.
4. Select **Internet Protocol (TCP/IP)** and click **Properties**.
5. Select the **Obtain an IP address automatically** and the **Obtain DNS server address automatically** radio buttons.
6. Click **OK** to finish the configuration.





## Step2→ Configuring with Web Browser

Once your PC has obtained an IP address from your router, enter the default IP address “**http: //192.168.0.1**” (XRT-401F’s LAN IP address) into your PC’s web browser and press <enter>



Save this address in your Favorites for future reference.



At the User name prompt, type “**admin**”.

And the Password prompt, type “**admin**”. You can change these later if you wish.

Click “**OK**”.




## Chapter 2 Quick Setup

The Wizard section is designed to get you using XRT-401F as quick as possible. In the Wizard, you are required to fill in only the information necessary to access the Internet. Once you click on the **Wizard** in the web page, you should see the screen below.

### Step 1) Host Settings

The Host Settings allows your router to set up Host name and Domain name, it also can set up its Time Zone and Daylight Saving Time, these will affect functions such as Log entries and Firewall settings.


Parameter	Description
<b>Host Name</b>	This is optional. You can specify a Host name for XRT401F.
<b>Time Zone</b>	Select the time zone of the country where you currently are. The router will set its time based on your selection.
<b>Daylight Savings</b>	The XRT-401F can also take Daylight savings into account. If you wish to use this function, you must select the enable box to enable your daylight saving configuration.
<b>Function Mode</b>	By default, XRT-401F is set as Router mode. If set to Bridge mode will turn the Router into 5-port Ethernet Switch where WAN port comes to Port # 5.

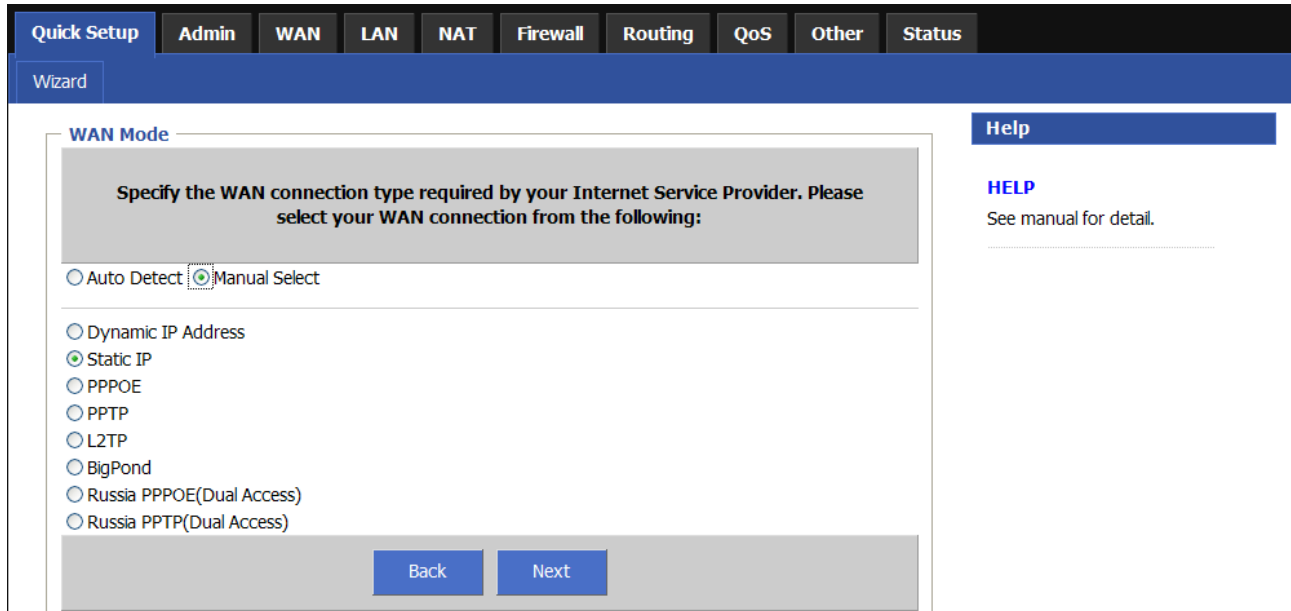
 <b>Note</b>	In this setup wizard, we set it as Router mode
--	--

Click on **NEXT** to proceed to the next page (step 2) WAN Settings.

## Step 2) WAN Settings

In this section you have to select one of these types of connections that you will be using to connect your XRT-401F's WAN port to your ISP (see screen below).

 <b>Note</b>	<p>Different ISP's require different methods of connecting to the Internet, please check with your ISP as to the type of connection it requires.</p>
--	--




Parameter	Description
<b>Dynamic IP</b>	Your ISP will automatically give you an IP address.
<b>Static IP</b>	Your ISP has given you an IP address already
<b>PPPoE</b>	Your ISP requires you to use a Point-to-Point Protocol over Ethernet (PPPoE) connection.
<b>PPTP</b>	Your ISP requires you to use a Point-to-Point Tunneling Protocol (PPTP) connection.
<b>L2TP</b>	Layer 2 Tunneling Protocol is a common connection method used in xDSL connections.
<b>Dual Acces</b>	This mode only active for Russia ISP that support dual layer Access to the Internet.

Click on one of the WAN types and then proceed to the manual's relevant sub-section (**2.1, 2.2, 2.3, 2.4 or 2.5**). Click on **Back** to return to the previous screen.

## 2.1 Dynamic IP

Choose Dynamic IP if your ISP will automatically give you an IP address. Some ISP's may also require that you fill in additional information such as MAC address (see screen below).

 <b>Note</b>	The MAC address section is <i>optional</i> and you can skip this section if your ISP does not require these settings for you to connect to the Internet.
--	--

Parameter	Description
<b>MAC Cloning</b>	If you want to clone your PC's MAC address to XRT-401F, you must enable it first.
<b>MAC Address</b>	Your ISP may require a particular MAC address in order for you to connect to the Internet. This MAC address is the PC's MAC address that your ISP had originally connected your Internet connection to. Type in this MAC address in this section or use the <b>Clone MAC Address</b> button to replace the WAN MAC address with the MAC address of that PC (you have to be using that PC for the Clone MAC Address button to work).

## 2.2 Static IP

Select Static IP if your ISP has given you a specific IP address to use. Your ISP should provide all the information required in this section.

The screenshot shows a configuration wizard for WAN Static IP. At the top, there is a navigation bar with tabs for 'Quick Setup', 'Admin', 'WAN', 'LAN', 'NAT', 'Firewall', 'Routing', 'QoS', 'Other', and 'Status'. Below this is a 'Wizard' section. The main configuration area is titled 'WAN Static IP' and contains three input fields: 'IP Address' with the value '61.62.27.185', 'Subnet Mask' with '255.255.255.0', and 'Gateway IP' with '61.62.27.254'. At the bottom of this area are 'Back' and 'Next' buttons. To the right, there is a 'Help' section with a 'HELP' link and the text 'See manual for detail.'.

Parameter	Description
<b>IP address assigned by your ISP</b>	This is the IP address that your ISP has given you.
<b>Subnet Mask</b>	Enter the Subnet Mask provided by your ISP. (e.g. 255.255.255.0)
<b>ISP Gateway Address</b>	This is the ISP's IP address gateway.

## 2.3 PPPoE

Select PPPoE if your ISP requires the PPPoE protocol to connect you to the Internet. Your ISP should provide all the information required in this section.

The screenshot shows the 'PPPOE Mode' configuration page. At the top, there are navigation tabs: Quick Setup, Admin, WAN, LAN, NAT, Firewall, Routing, QoS, Other, and Status. Below these is a 'Wizard' section. The main content area is titled 'PPPOE Mode' and contains the following fields:

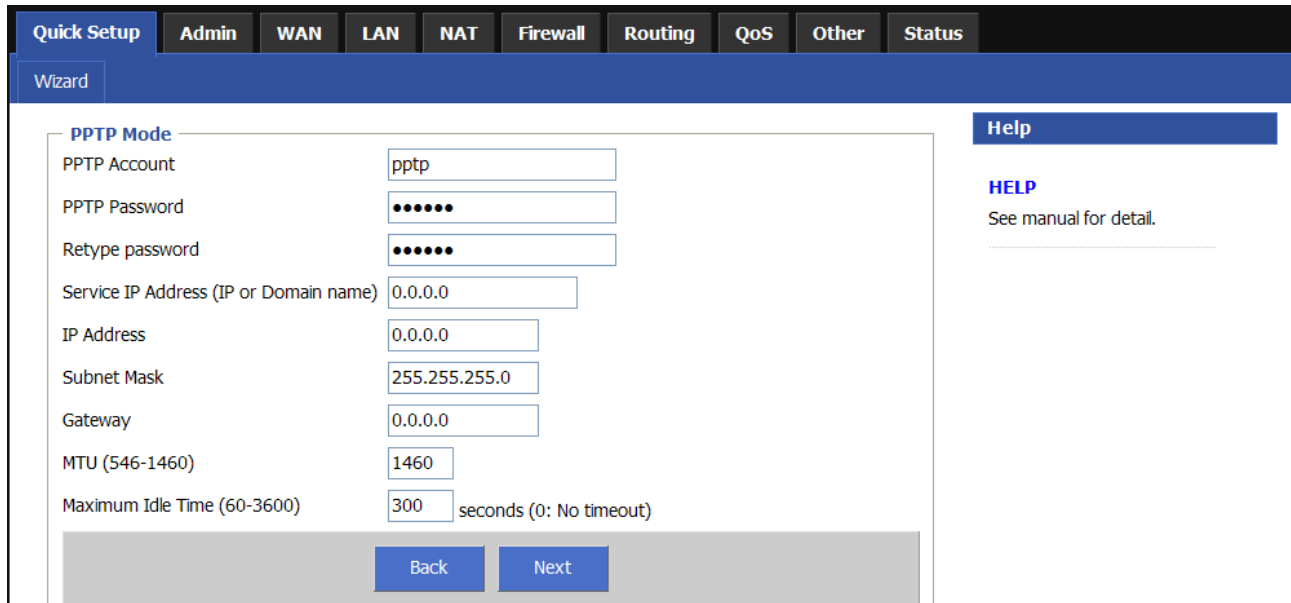
- User Name:
- Password:
- Retype password:
- Service Name:
- MTU (546-1492):
- Maximum Idle Time (60-3600):  seconds (0: No timeout)

At the bottom of the form are two buttons: 'Back' and 'Next'. To the right of the form is a 'Help' section with a 'HELP' link and the text 'See manual for detail.'

Parameter	Description
<b>User Name</b>	Enter the User Name provided by your ISP for the PPPoE connection.
<b>Password</b>	Enter the Password provided by your ISP for the PPPoE connection.
<b>Retype Password</b>	Re-enter the Password for confirmation.
<b>Service Name</b>	This is optional. Enter the Service name should your ISP requires it, otherwise leave it blank.
<b>MTU</b>	This is optional. You can specify the maximum size of your transmission packet to the Internet. Leave it as it is if you do not wish to set a maximum packet size. (The default settings is 1492)
<b>Maximum Idle Time</b>	You can specify an idle time threshold (seconds) for the WAN port. This means if no packets have been sent (no one using the Internet) during this specified period, the router will automatically disconnect the connection with your ISP. (The default settings is 300 seconds)

## 2.4 PPTP

Select PPTP if your ISP requires the PPTP protocol to connect you to the Internet. Your ISP should provide all the information required in this section.



The screenshot shows the 'PPTP Mode' configuration page. It includes the following fields and values:

- PPTP Account: pptp
- PPTP Password: [masked]
- Retype password: [masked]
- Service IP Address (IP or Domain name): 0.0.0.0
- IP Address: 0.0.0.0
- Subnet Mask: 255.255.255.0
- Gateway: 0.0.0.0
- MTU (546-1460): 1460
- Maximum Idle Time (60-3600): 300 seconds (0: No timeout)

Navigation buttons: Back, Next. Help text: See manual for detail.

Parameter	Description
<b>PPTP Account</b>	Enter the PPTP Account provided by your ISP for the PPTP connection.
<b>PPTP Password</b>	Enter the Password provided by your ISP for the PPTP connection.
<b>Retype Password</b>	Re-enter the Password for confirmation.
<b>Service IP Address</b>	Specify PPTP Server IP address that you want to connect to.
<b>My IP Address</b>	This is the IP address that your ISP has given you to establish a PPTP connection.
<b>My Subnet Mask</b>	Enter the Subnet Mask provided by your ISP. (e.g. 255.255.255.0)
<b>Gateway Address</b>	This is the ISP's IP address gateway.
<b>MTU</b>	This is optional. You can specify the maximum size of your transmission packet to the Internet. Leave it as it is if you do not wish to set a maximum packet size. (The default setting is 1460)
<b>Maximum Idle Time</b>	You can specify an idle time threshold (seconds) for the WAN port. This means if no packets have been sent (no one using the Internet) during this specified period, the router will automatically disconnect the connection with your ISP. (The default settings is 300 seconds)

## 2.5 L2TP

Select L2TP if your ISP requires the L2TP protocol to connect you to the Internet. Your ISP should provide all the information required in this section.

The screenshot shows the 'L2TP Mode' configuration page. The interface includes a top navigation bar with tabs for 'Quick Setup', 'Admin', 'WAN', 'LAN', 'NAT', 'Firewall', 'Routing', 'QoS', 'Other', and 'Status'. Below this is a 'Wizard' section. The main configuration area contains the following fields:

- L2TP Account:** Input field containing 'l2tp'.
- L2TP Password:** Password input field with masked characters.
- Retype password:** Password input field with masked characters.
- Service IP Address (IP or Domain name):** Input field containing '0.0.0.0'.
- IP Address:** Input field containing '0.0.0.0'.
- Subnet Mask:** Input field containing '255.255.255.0'.
- Gateway:** Input field containing '0.0.0.0'.
- MTU (546-1460):** Input field containing '1460'.
- Maximum Idle Time (60-3600):** Input field containing '300' with the text 'seconds (0: No timeout)'.

At the bottom of the configuration area are 'Back' and 'Next' buttons. On the right side, there is a 'Help' section with a 'HELP' link and the text 'See manual for detail.'.

Parameter	Description
<b>L2TP Account</b>	Enter the L2TP Account provided by your ISP for the PPTP connection.
<b>L2TP Password</b>	Enter the Password provided by your ISP for the L2TP connection.
<b>Retype Password</b>	Re-enter the Password for confirmation.
<b>Service IP Address</b>	Specify L2TP Server IP address that you want to connect to.
<b>My IP Address</b>	This is the IP address that your ISP has given you to establish a L2TP connection.
<b>My Subnet Mask</b>	Enter the Subnet Mask provided by your ISP. (e.g. 255.255.255.0)
<b>Gateway Address</b>	This is the ISP's IP address gateway.
<b>MTU</b>	This is optional. You can specify the maximum size of your transmission packet to the Internet. Leave it as it is if you do not wish to set a maximum packet size. (Default setting is 1460)
<b>Maximum Idle Time</b>	You can specify an idle time threshold (seconds) for the WAN port. This means if no packets have been sent (no one using the Internet) during this specified period, the router will automatically disconnect the connection with your ISP. (The default settings is 300 seconds)

### Step 3) DNS

A Domain Name System (DNS) server is like an index of IP addresses and Web addresses. If you type a Web address into your browser, such as [www.router.com](http://www.router.com), a DNS server will find that name in its index and the matching IP address. Most ISPs provide a DNS server for speed and convenience. If your Service Provider connects you to the Internet with dynamic IP settings, it is likely that the DNS server IP address is provided automatically. However, if there is a DNS server that you would rather use, you need to specify the IP address of that DNS server here.

Parameter	Description
<b>Static DNS Server</b>	Select "Enabled" to allow configuring DNS manually.
<b>Primary DNS Address</b>	This is the ISP's DNS server IP address that they gave you; or you can specify your own preferred DNS server IP address
<b>Secondary DNS Address</b>	This is optional. You can enter another DNS server's IP address as a backup. The secondary DNS will be used if the above DNS fail.

Click on <**Finish**> when you have finished the configuration above.

**Now!** You have completed the connection configuration. You can start using the router now.



## Chapter 3 Advance Features

If you have already configured the Wizard, you do NOT need to configure anything for you to start using the Internet.

Advance features that allow you to configure the router to meet your network's needs such as: Firewall setup, Port Mapping, DMZ, Virtual Servers, QoS, and VLAN option.

Below is a general description of what advance functions are available for this broadband router.

<b>Parameter</b>	<b>Description</b>
<b>3.1 Admin</b>	This section allows you to set XRT-401F's system settings, password and Remote Management Administrator, it also allows you to check system status and log, and provide you the configuration tools.
<b>3.2 WAN</b>	This section allows you to select the connection method in order to establish a connection with your ISP (same as the Wizard section)
<b>3.3 LAN</b>	You can specify the LAN segment's IP address, subnet Mask, enable/disable DHCP and select an IP range for your LAN, you also can check DHCP client list in here.
<b>3.4 NAT</b>	You can configure the Virtual Server, Special Applications, Port Mapping, ALG and DMZ functions in this section. This allows you to specify what user/packet can pass your router's NAT.
<b>3.5 Firewall</b>	The Firewall section allows you to configure Firewall, Client Filtering, URL Filtering and MAC Control.
<b>3.6 Routing</b>	You can configure Static Routing in this section, and check the concurrent Routing Table.
<b>3.7 QoS</b>	You can assign the bandwidth for specific LAN / WAN port. Each LAN Port will follow the bandwidth you assigned.
<b>3.8 Other</b>	You can configure UPnP and DDNS service in this section.
<b>3.9 Status</b>	You can check system information in here, including system status and concurrent hardware information.

Select one of the above advance features selections and proceed to the manual's relevant subsection.

## 3.1 Admin

This section allows you to set XRT-401F's system settings, password and Remote Management Administrator, it also allows you to check system status and log, and provide you the configuration tools.

Parameter	Description
<b>3.1.1 System Status</b>	You can check system information in here, including system status and concurrent hardware information.
<b>3.1.2 System Settings</b>	This section Includes Host Name, Domain Name, Time Zone, Daylight Saving and NAT enable/disable.
<b>3.1.3 Administrator Settings</b>	Allows you to set user name, password and the idle time out, you can specify a Host IP address that can perform remote management functions.
<b>3.1.4 Firmware Upgrade</b>	This section allows you to upgrade the router's firmware and display the concurrent firmware version.
<b>3.1.5 Configuration Tools</b>	This section allows you to backup or restore the router's configuration. It also allows you to restart router or reset it to factory default setting.
<b>3.1.6 System Log</b>	This section shows the current system and security log of XRT-401F, you also can specify a syslog server to save the log remotely.

### 3.1.1 Management

The Management Settings function allows you to design user name, password and the idle time, it also can allow you to configure Remote Management function.

Parameter	Description
<b>Password Settings</b>	
<b>User Name</b>	To specify a login name, the default is admin.
<b>Current assword</b>	Enter the current password for verification. Max. length is 12 characters.
<b>New Password</b>	Type a new password in order to access the web-based management website.
<b>Re-type Password</b>	Re-type the password for confirmation.
<b>Remote Management</b>	
<b>Enable</b>	To enable Remote Management function.
<b>IP Address</b>	This is the IP address of the host in the Internet that will have management / configuration access to XRT-401F from a remote site. If the IP Address is <b>0.0.0.0</b> , this means anyone can access the router's web console from a remote location
<b>Port</b>	The port number of remote management web interface. For example, port 8080 means, from the Internet, you are required to use the URL: <u>http://XRT401's WAN IP:8080/</u> to have the access / remote mangement to this Router.

### 3.1.2 System Settings

The system screen allows you to specify a time zone, Host Name, Function mode, and enable or disable NAT function of XRT-401F.

The screenshot shows the 'System Settings' page for the XRT-401F. The 'Time' section includes an optional NTP Server field, a Time Zone dropdown menu set to '(GMT+08:00) Hong Kong, Perth, Singapore, Taipei', and a Daylight Saving checkbox that is currently unchecked. The 'Name' section has a Host Name field containing 'XRT-401F'. The 'Operating Mode' section has a NAPT checkbox that is checked and labeled 'Enabled'. The 'Function Mode' section has a dropdown menu set to 'Router'. A 'Help' sidebar on the right provides instructions for the Time Zone selection. At the bottom of the page are 'OK' and 'Cancel' buttons.

Parameter	Description
Host Name	Optional. You can specify a Host name for XRT-401F.
Set Time Zone	Select the time zone of the country where you are currently are. The router will set its time based on your selection.
Daylight Saving	The XRT-401F can also take Daylight savings into account. If you wish to use this function, you must select the enable box to enable your daylight saving configuration.
Host Name	Optional. You can specify a Host name for XRT-401F.
NAPT	Select to enable or disable NAT / NAPT function.
Function Mode	The XRT-401F supports two mode for your application, select the Router mode to act as a Router / Gateway which provides the firewall function to protect your private network. To select the Bridge mode, the XRT-401F will act as a pure 5-Port Ethernet Switch. The default mode is Router.

### 3.1.3 Firmware Upgrade

This page allows you to upgrade the router's firmware.

**Firmware Upgrade**

Current Firmware Version: 1.0  
 Firmware Date: #71 Fri Feb 12 09:52:39 2010

Enter the path and name of the upgrade file then click the OK button below.

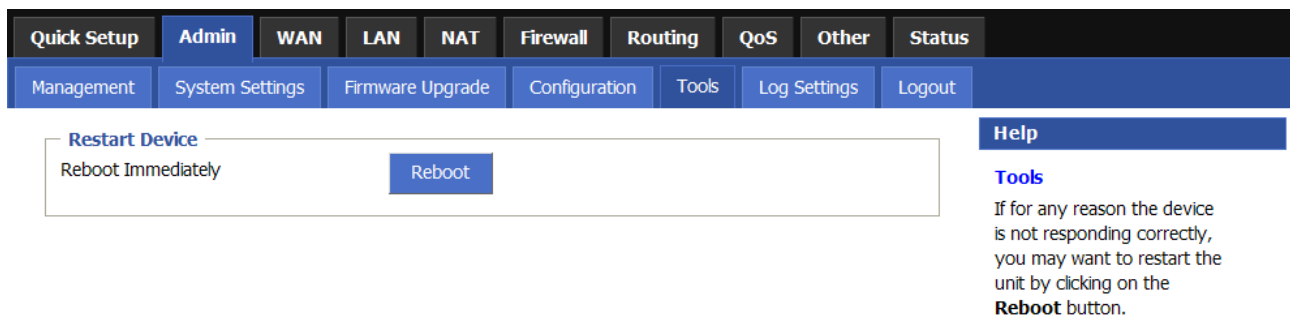
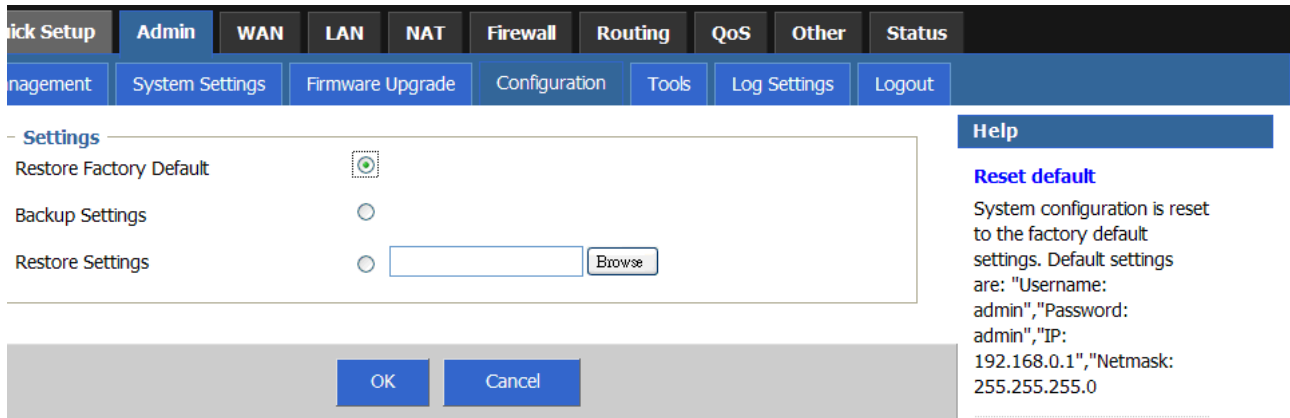
**Help**

**Firmware Upgrade**  
 You can upgrade the firmware of the device using this tool. Make sure that the firmware you want to use is saved on the local hard drive of the computer. Click on Browse to search the local hard drive for the firmware to be used for the update.

Parameter	Description
Firmware Upgrade	This tool allows you to upgrade XRT-401F's system firmware. To upgrade the firmware of your Broadband router, you need to download the firmware file to your local hard disk, and enter that file name and path in the appropriate field on this page. You can also use the <b>Browse</b> button to find the firmware file on your PC.

### 3.1.4 Configuration and Tool

The Configuration Tools screen allows you to save (**Backup**) the router's current configuration setting. Saving the configuration settings provides an added protection and convenience, if the problems occur with the router and you have to reset to factory default. When you save the configuration setting (**Backup**) you can re-load the saved configuration into the router through the **Restore** selection. If extreme problems occur, you can use the **Restore to Factory Defaults** selection, this will set all configurations to its original default settings (e.g. when you first purchased the router). You also can **Restart** the router's system if any problems exist.



Parameter	Description
<b>Restore Factory Default</b>	If extreme problems occur, you can use the <b>Restore Factory Default</b> selection, this will set all configurations to its original default settings (e.g. when you first purchased the Router).
<b>Backup Settings</b>	<b>Backup</b> the configuration settings provide an added protection and convenience, if the problems occur with the router and you have to reset to factory default.
<b>Restore Settings</b>	When you save the configuration setting (Backup) you can reload the saved configuration into the router through the <b>Restore Settings</b> selection.
<b>Reboot</b>	In the event that the system stops responding correctly or in some way stops functioning, you can perform a reset. <b>Your settings will not be changed.</b>

### 3.1.5 Log Setting

The Logs record various types of activity on XRT-401F. This data is useful for troubleshooting, but enabling all logs will generate a large amount of data and adversely affect performance. Since only a limited amount of log data can be stored in XRT-401F, log data can also be e-mailed to your PC or sent to a Syslog Server.

Parameter	Description
<b>Remote Log</b>	Select <Enabled> to allow saving the log to Syslog Server.
<b>Log Server</b>	Enter the IP address of your Syslog Server.
<b>Email Log</b>	Select <Enabled> to allow mailing the log to specific user. By default, it is Disabled.
<b>Send Email to</b>	Enter the mail address that your want to mail log to.
<b>SMTP Server</b>	Enter the address or IP address of the SMTP (Simple Mail Transport Protocol) Server you use for outgoing E-mail.

## 3.2 WAN

Use the WAN Settings screen if you have already configured the Wizard section and you would like to change your Internet connection type. The WAN Settings screen allows you to specify the type of WAN port connect you want to establish with your ISP. The WAN settings offer the following selections for the router's WAN port, **Dynamic IP**, **Static IP Address**, **PPPoE**, **PPTP**, and **L2TP**.

The screenshot shows the WAN Mode configuration page. The 'WAN Connection Mode' section lists several options:

- Dynamic IP Address: Obtain an IP address automatically from your service provider.
- Static IP: Use a static IP address. Your service provider gives a static IP address to access Internet services.
- PPPOE: PPP over Ethernet is a common connection method used for xDSL.
- PPTP: PPP Tunneling Protocol can support multi-protocol Virtual Private Networks (VPN).
- L2TP: Layer 2 Tunneling Protocol can support multi-protocol Virtual Private Networks (VPN).
- BigPond: Australia ISP service.
- Russia PPPOE(Dual Access): Russia PPP over Ethernet(Dual Access) is a common connection method used for xDSL.
- Russia PPTP(Dual Access): Russia PPP Tunneling Protocol(Dual Access) can support multi-protocol Virtual Private Networks (VPN).

The 'Help' sidebar on the right contains the following information:

- Static IP Mode**: The router's IP Address and Subnet Mask as seen by external users on the Internet (including your ISP). If your Internet connection requires a static IP address, then your ISP will provide you with a Static IP Address and Subnet Mask.
- Default Gateway**: Your ISP will provide you with the Gateway IP Address.
- MTU (Maximum Transmission Unit)**: Configure the largest packet...

Parameter	Description
<b>3.2.1 Dynamic IP</b>	Your ISP will automatically give you an IP address
<b>3.2.2 Static IP</b>	Your ISP has given you an IP address already
<b>3.2.3 PPPoE</b>	Your ISP requires PPPoE connection
<b>3.2.4 PPTP</b>	Your ISP requires you to use a Point-to-Point Tunneling Protocol (PPTP) connection.
<b>3.2.5 L2TP</b>	Your ISP requires L2TP connection.



### 3.2.1 Dynamic IP

Choose the Dynamic IP selection if your ISP will automatically give you an IP address. Some ISP's may also require that you fill in additional information such as MAC address (see chapter 2 "Dynamic IP" for more detail).

**Dynamic IP Address**

Request IP address

MTU(576-1500)

Static DNS Server

Primary DNS

Secondary DNS  (Optional)

MAC Cloning  Enabled

MAC Address (XX:XX:XX:XX:XX:XX)

Parameter	Description
<b>MTU</b>	This is optional. You can specify the maximum size of your transmission packet to the Internet. Leave it as it is if you do not wish to set a maximum packet size. (The default settings is 1500)
<b>Static DNS Server</b>	Select "Enabled" to allow configuring DNS manually.
<b>Primary DNS Address</b>	This is the ISP's DNS server IP address that they gave you; or you can specify your own preferred DNS server IP address
<b>Secondary DNS Address</b>	This is optional. You can enter another DNS server's IP address as a backup. The secondary DNS will be used if the above DNS fail.
<b>MAC Cloning</b>	If you want to clone your PC's MAC address to XRT-401F, you must enable it first.
<b>MAC Address</b>	Your ISP may require a particular MAC address in order for you to connect to the Internet. This MAC address is the PC's MAC

address that your ISP had originally connected your Internet connection to. Type in this MAC address in this section or use the **Clone MAC Address** button to replace the WAN MAC address with the MAC address of that PC (you have to be using that PC for the Clone MAC Address button to work).

### 3.2.2 Static IP

Select Static IP address if your ISP has given you one or more IP address for you to use. Your ISP should provide all the information required in this section. (See chapter 2 “**Static IP**” for more detail)

**WAN Static IP**

**Static IP Address**

IP Address

Subnet Mask

Gateway IP

MTU (576-1500)

Static DNS Server

Primary DNS

Secondary DNS  (Optional)

MAC Cloning  Enabled

MAC Address (XX:XX:XX:XX:XX:XX)

**More IP addresses**

Does ISP provide more IP addresses?

Parameters	Description
<b>Static IP</b>	Your ISP has given you an IP address already, and you must type in the related IP address such as <b>IP Address</b> , <b>Subnet Mask</b> and <b>Gateway</b> .
<b>Does ISP provide more IP addresses?</b>	Select <Yes> if your ISP provide more than one IP address.
<b>More IP address</b>	Type the other IP address that ISP provide to you, This IP address will be useful in DMZ function. Max IP address allowed is 6 separated IP address.

### 3.2.3 PPPoE (PPP over Ethernet)

Select PPPoE if your ISP requires the PPPoE protocol to connect you to the Internet. Your ISP should provide all the information required in this section. (See chapter 2 “PPPoE” for more detail)

**PPPOE**

Address Mode  Dynamic PPPoE  Static PPPoE

IP Address

PPPOE Account

PPPOE Password

Please retype your password

Service Name

MTU (546-1492)

Maximum Idle Time (60-3600)  seconds (0: No timeout)

Connection Mode  ▼

Primary DNS

Secondary DNS  (Optional)

MAC Cloning  Enabled

MAC Address (XX:XX:XX:XX:XX:XX)

Parameter	Description
<b>PPPoE</b>	Your ISP requires PPPoE connection, and you must type in the User Name, Password that your ISP provide.
<b>MTU</b>	This is optional. You can specify the maximum size of your transmission packet to the Internet. Leave it as it is if you do not wish to set a maximum packet size. (The default settings is 1492)
<b>Connection Mode</b>	Select the desired option: <b>Keep-alive (maintain connection)</b> The connection will never be disconnected by this device. If disconnected by your ISP, the connection will be re-established immediately. (However, this does not ensure that your Internet IP address will remain unchanged.) <b>Auto-Connect</b> An Internet connection is automatically made when required,

	<p>and disconnected when idle for the time period specified by the "Maximum Idle Time (60~3600)".</p> <p><b>Manual-on</b> You must manually establish and terminate the connection.</p>
<b>Static DNS Server</b>	Select "Enabled" to allow configuring DNS manually.
<b>Primary DNS Address</b>	This is the ISP's DNS server IP address that they gave you; or you can specify your own preferred DNS server IP address
<b>Secondary DNS Address</b>	This is optional. You can enter another DNS server's IP address as a backup. The secondary DNS will be used if the above DNS fail.
<b>MAC Cloning</b>	If you want to clone your PC's MAC address to XRT-401F, you must enable it first.
<b>MAC Address</b>	Your ISP may require a particular MAC address in order for you to connect to the Internet. This MAC address is the PC's MAC address that your ISP had originally connected your Internet connection to. Type in this MAC address in this section or use the <b>Clone MAC Address</b> button to replace the WAN MAC address with the MAC address of that PC (you have to be using that PC for the Clone MAC Address button to work).

### 3.2.4 PPTP

Select PPTP if your ISP requires the PPTP protocol to connect you to the Internet. Your ISP should provide all the information required in this section.

**WAN PPTP**

**WAN Interface Settings**

WAN Interface IP	Static IP	▼
IP Address	<input type="text" value="0.0.0.0"/>	
Subnet Mask	<input type="text" value="255.255.255.0"/>	
Gateway	<input type="text" value="0.0.0.0"/>	
Primary DNS	<input type="text" value="61.64.127.1"/>	
Secondary DNS	<input type="text" value="61.64.127.2"/>	(Optional)
MAC Cloning	<input type="checkbox"/> Enabled	
MAC Address (XX:XX:XX:XX:XX:XX)	<input type="text" value="00:00:00:00:00:00"/>	<input type="button" value="Clone MAC"/>

**PPTP Settings**

PPTP Account	<input type="text" value="pptp"/>	
PPTP Password	<input type="password" value="••••••"/>	
Please retype your password	<input type="password" value="••••••"/>	
PPTP Server (IP or Domain name)	<input type="text" value="0.0.0.0"/>	
Connection ID	<input type="text"/>	(Optional)
MTU (546-1460)	<input type="text" value="1460"/>	
Maximum Idle Time (60-3600)	<input type="text" value="300"/>	seconds (0: No timeout)
Connection Mode	keep-alive ▼	
MPPE	<input type="checkbox"/>	

Parameter	Description
<b>WAN Interface Settings</b>	To configure WAN Interface IP
<b>Dynamic IP</b>	<p>The ISP requires you to obtain an IP address by DHCP before connecting to the PPTP server.</p> <p><b>Clone MAC Address</b> Select &lt;Enabled&gt; to allow replacing the WAN MAC address with a specific MAC address.</p> <p><b>MAC Address</b> Your ISP may require a particular MAC address in order for you to connect to the Internet. This MAC address is the PC's MAC address that your ISP had originally connected your Internet connection to. Type in this MAC address in this section or use the "<b>Clone MAC Address</b>" button to replace the WAN MAC address with the MAC address of that PC.</p>
<b>Static IP</b>	The ISP gives you a static IP to be used to connect to the PPTP server. You must type in the related IP address such as <b>IP Address, Subnet Mask</b> and <b>Gateway</b> .
<b>PPTP Settings</b>	
<b>PPTP Account</b>	Enter the PPTP Account provided by your ISP for the PPTP connection.
<b>PPTP Password</b>	Enter the Password provided by your ISP for the PPTP connection.
<b>Retype Password</b>	Re-enter the Password for confirmation.
<b>PPTP Server</b>	If your LAN has a PPTP gateway, then enter that PPTP gateway IP address or domain name here. If you do not have a PPTP gateway then enter the ISP's Gateway IP address above or domain name.
<b>Connection ID</b>	This is the ID given by ISP. This is optional.
<b>MTU</b>	This is optional. You can specify the maximum size of your transmission packet to the Internet. Leave it as it is if you do not wish to set a maximum packet size. (The default settings is 1460)
<b>Maximum Idle Time</b>	You can specify an idle time threshold (seconds) for the WAN port. This means if no packets have been sent (no one using the Internet) during this specified period, the router will automatically disconnect the connection with your ISP.
<b>Connection Mode</b>	Select the desired option: <b>Keep-alive (maintain connection)</b>

	<p>The connection will never be disconnected by this device. If disconnected by your ISP, the connection will be reestablished immediately. (However, this does not ensure that your Internet IP address will remain unchanged.)</p> <p><b>Auto-Connect</b> An Internet connection is automatically made when required, and disconnected when idle for the time period specified by the "Maximum Idle Time (60~3600)".</p> <p><b>Manual-on</b> You must manually establish and terminate the connection.</p>
<b>MPPE</b>	<p>Select &lt;Enabled&gt; to enable "Microsoft Point to Point Encryption" ability.</p>



### 3.2.5 L2TP

Select L2TP if your ISP requires the L2TP protocol to connect you to the Internet. Your ISP should provide all the information required in this section.

**WAN L2TP**

**WAN Interface Settings**

WAN Interface IP Static IP

IP Address

Subnet Mask

Gateway

Static DNS Server

Primary DNS

Secondary DNS  (Optional)

MAC Cloning  Enabled

MAC Address (XX:XX:XX:XX:XX:XX)

**L2TP Settings**

L2TP Account

L2TP Password

Please retype your password

L2TP Server (IP or Domain name)

MTU (546-1460)

Maximum Idle Time (60-3600)  seconds (0: No timeout)

Connection Mode keep-alive

Parameter	Description
<b>WAN Interface Settings</b>	To configure WAN Interface IP
<b>Dynamic IP</b>	The ISP requires you to obtain an IP address by DHCP before connecting to the L2TP server.
	<b>MAC Cloning</b> Select <Enabled> to allow replacing the WAN MAC address with

	<p>a specific MAC address.</p> <p><b>MAC Address</b></p> <p>Your ISP may require a particular MAC address in order for you to connect to the Internet. This MAC address is the PC's MAC address that your ISP had originally connected your Internet connection to. Type in this MAC address in this section or use the "<b>Clone MAC Address</b>" button to replace the WAN MAC address with the MAC address of that PC.</p>
<b>Static IP</b>	<p>The ISP gives you a static IP to be used to connect to the PPTP server. You must type in the related IP address such as <b>IP Address, Subnet Mask</b> and <b>Gateway</b>.</p>
<b>L2TP Settings</b>	
<b>L2TP Account</b>	<p>Enter the L2TP Account provided by your ISP for the L2TP connection.</p>
<b>L2TP Password</b>	<p>Enter the Password provided by your ISP for the L2TP connection.</p>
<b>Retype Password</b>	<p>Re-enter the Password for confirmation.</p>
<b>L2TP Server</b>	<p>gateway IP address or domain name here. If you do not have a L2TP gateway then enter the ISP's Gateway IP address above or domain name.</p>
<b>MTU</b>	<p>This is optional. You can specify the maximum size of your transmission packet to the Internet. Leave it as it is if you do not wish to set a maximum packet size. (The default settings is 1460)</p>
<b>Maximum Idle Time</b>	<p>You can specify an idle time threshold (seconds) for the WAN port. This means if no packets have been sent (no one using the Internet) during this specified period, the router will automatically disconnect the connection with your ISP.</p>
<b>Connection Mode</b>	<p>Select the desired option:</p> <p><b>Keep-alive (maintain connection)</b></p> <p>The connection will never be disconnected by this device. If disconnected by your ISP, the connection will be reestablished immediately. (However, this does not ensure that your Internet IP address will remain unchanged.)</p> <p><b>Auto-Connect</b></p> <p>An Internet connection is automatically made when required, and disconnected when idle for the time period specified by the "Maximum Idle Time (60~3600)".</p> <p><b>Manual-on</b></p> <p>You must manually establish and terminate the connection.</p>

### 3.2.6 BigPond (Australia)

Select BigPond if your ISP requires the BigPond protocol to connect you to the Internet. Your ISP should provide all the information required in this section.

**BigPond**

BigPond Account

BigPond Password

Please retype your password

BigPond Server (IP or Domain name)

Request IP address

MTU (576-1500)

Static DNS Server

Primary DNS

Secondary DNS  (Optional)

MAC Cloning  Enabled

MAC Address (XX:XX:XX:XX:XX:XX)

Parameter	Description
<b>BigPond Account</b>	Enter the L2TP Account provided by your ISP for the BigPond connection.
<b>BigPond Password</b>	Enter the Password provided by your ISP for the BigPond connection.
<b>Retype Password</b>	Re-enter the Password for confirmation.
<b>BigPond Server</b>	gateway IP address or domain name here. If you do not have a BigPond gateway then enter the ISP's Gateway IP address above or domain name.
<b>MTU</b>	This is optional. You can specify the maximum size of your transmission packet to the Internet. Leave it as it is if you do not wish to set a maximum packet size. (The default settings is 1500)

## 3.3 LAN

The LAN Port screen below allows you to specify a private IP address for your router's LAN ports as well as a subnet mask for your LAN segment.

### 3.3.1 LAN Settings

The screenshot shows the LAN Settings configuration page. The navigation tabs at the top include Quick Setup, Admin, WAN, LAN (selected), NAT, Firewall, Routing, QoS, Other, and Status. The sub-tabs are LAN Settings, DHCP Client List, and VLAN Port Settings. The main settings area includes:

- IP Address:** 192.168.0.1
- Subnet Mask:** 255.255.255.0
- The Gateway acts as DHCP Server:**  Enabled
- IP Pool Starting Address:** 192.168.0.
- IP Pool Ending Address:** 192.168.0.
- Lease Time:**  (dropdown menu)
- DNS Proxy:**  Enabled

At the bottom, there are OK and Cancel buttons. On the right, a Help section titled "LAN Setting" explains that the router IP Address and Subnet Mask are used for the internal LAN, with default values of 192.168.1.1 for IP Address and 255.255.255.0 for Subnet Mask. Below that, a section titled "DHCP (Dynamic Host Configuration Protocol)" explains that DHCP is used to obtain information for network operation, reducing system administration workload.

Parameter	Default	Description
<b>IP address</b>	192.168.0.1	This is the router's LAN port IP address (Your LAN clients default gateway IP address)
<b>IP Subnet Mask</b>	255.255.255.0	Specify a Subnet Mask for your LAN segment
<b>DHCP Server</b>	Enabled	You can enable or disable the DHCP server. By enabling the DHCP server the router will automatically give your LAN clients an IP address. If the DHCP is not enabled then you'll have to manually set your LAN client's IP addresses; make sure the LAN Client is in the same subnet as this broadband router if you want the router to be your LAN client's default gateway.
<b>IP Pool Starting/Ending Address</b>	The IP range is from <b>192.168.0.2</b> to <b>192.168.0.100</b> .	You can select a particular IP address range for your DHCP server to issue IP addresses to your LAN Clients.
<b>Lease Time</b>	Eight Hours	The DHCP when enabled will temporarily give your LAN clients an IP address. In the Lease Time setting you can specify the time period that the DHCP lends an IP address to your LAN

		clients. The DHCP will change your LAN client's IP address when this time threshold period is reached
<b>DNS Proxy</b>	<b>Enable</b>	Select <Enabled> that all DNS requests to a specific Domain Name will be routed to the XRT-401F's IP address. If you want to use the DNS Proxy function of the device, the end user's main DNS server IP address should be the same IP Address as the device.

### 3.3.2 DHCP Client List

You can check your current status of the DHCP client here, it also allow you to add the client IP address with specific MAC address manually.

Parameter	Description
<b>DHCP Client List</b>	
<b>Host Name</b>	The DHCP client list allows you to see which clients are connected to the Router via IP address, host name, remaining time and MAC address. You can select static to fix it.
<b>IP Address</b>	
<b>MAC Address</b>	
<b>Remaining Time</b>	
<b>Static</b>	You can specify the current client to be a static client.
<b>Static Client</b>	
<b>Host Name</b>	This is optional, you can specify a host name for your static client.
<b>IP Address</b>	Fill in the IP address which you wish to be a static client.
<b>MAC Address</b>	Fill in the MAC address which you wish to be a static client.

### 3.3.3 VLAN Settings

By default, the VLAN setting is disabled, however, you can turn it on for purpose, or setup the port based priority base on the VLN setting here.

The default setting is that, All the ports, say port 1 to port 4 is bound to WAN interface.

And WAN interface is bound to port 5 of the Router (where now, it is physically with printing **WAN**)

So, all the network traffic that is going to Internet, all with going out through the WAN port. Unless VLAN is enabled yet the port's VLAN is being disabled.

And once turn it on, you can base on PVID to separate the LAN. For example as the figure below, port 1 is connected with IP Phone, port 2 is connected with Video device, and port 3, port 4 is normal data ports. You can just change the PVID of port #1 to 4, port #2 to 5. Then, port #1, #2, are being separated from port 3 and port 4.


At the same time, you can also set the priority for port #1 to **7**, port #2 to **4**, and then for port #3, port #4 to **0**, then, the Router will schedule the network packets base on the priority for packet out from that dedicated LAN port.

The screenshot shows the router's configuration interface with the following elements:

- Navigation Tabs:** Quick Setup, Admin, WAN, LAN (selected), NAT, Firewall, Routing, QoS, Other, Status.
- Sub-Tabs:** LAN Settings, DHCP Client List, VLAN Port Settings (selected).
- Settings Panel:**
  - VLAN Control:** Enabled VLAN function (dropdown menu).
  - Enabled:**
  - Port-:** 1 (dropdown menu)
  - PVID:** 4 (input field)
  - 802.1p Priority:** 7 (dropdown menu)
  - Wan:**
  - Modify:** Button
- Table:**

	Port-	PVID	802.1p Priority	Wan	Action
<input checked="" type="checkbox"/>	1	4	7	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	2	5	4	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	3	1	0	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	4	1	0	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	5	2	7	<input checked="" type="checkbox"/>	
- Footer:** OK, Cancel buttons.

Parameter	Default	Description
<b>VLAN Enable</b>	Disable	Enable will turn on the port based VLAN. [After enabled, the options will show up.]
<b>Port VLAN Enable</b>	Enabled	The port join to the WAN VLAN group. To disable will make the port isolated from the WAN.
<b>PVID</b>	1	The VLAN ID of the selected port. 1 for LAN 1 -4 2 for WAN at port 5
<b>Priority</b>	4	The priority of the selected port.
<b>WAN</b>	Disabled	By default, the check box only enabled for port #5.

 <b>Note</b>	<ol style="list-style-type: none"> <li>1. Different VLAN will have different PVID. Those ports with the same PVID will still see each other.</li> <li>2. WAN should use different VID to LAN VID.</li> <li>3. Due to the Router is a single port WAN Router, <b>ONLY ONE</b> WAN check box is allowed. By default, it is set on port 5.</li> <li>4. This Router support port based VLAN at Router mode, yet at <b>Bridge mode</b> there are two different VLAN types, port based and 802.1q tagged VLAN for choice</li> </ol>
--	---

### 3.3.4 Broadcast Storm Control

A broadcast storm means that the network is overwhelmed with constant broadcast or multicast traffic. Broadcast storms can eventually lead to a complete loss of network connectivity as the packets proliferate. This page can set the broadcast and the multicast storm control parameter, you can limit the broadcast and multicast per second through this port, the default value is 255. Tick the **Enabled** blank to adjust those parameter.

The screenshot shows a web interface for configuring Broadcast Storm Control. The top navigation bar includes tabs for Quick Setup, Admin, WAN, LAN (selected), NAT, Firewall, Routing, QoS, Other, and Status. Below this, there are sub-tabs for LAN Settings, DHCP Client List, VLAN Port Settings, Broadcast Storm Control (selected), and IGMP Snooping. The main content area is titled 'Settings' and contains the following configuration options:

Interface	Broadcast Storm Control	Multicast Storm Control	Rate
Broadcast Storm Control Function	<input checked="" type="checkbox"/> Enabled		
LAN-1	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	Rate <input type="text" value="255"/> Packets/10ms
LAN-2	<input type="checkbox"/> Enabled		
LAN-3	<input type="checkbox"/> Enabled		
LAN-4	<input type="checkbox"/> Enabled		
WAN	<input type="checkbox"/> Enabled		

At the bottom of the page, there are two buttons: 'OK' and 'Cancel'.

### 3.3.5 IGMP

The Internet Group Management Protocol (IGMP) is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships.

IGMP Snooping is the process of listening to IGMP traffic, its feature that allows the switch to "listen in" on the IGMP conversation between hosts and routers by processing the layer 3 packets IGMP packets sent in a multicast network.

When IGMP snooping is enabled in a switch it analyses all the IGMP packets between hosts connected to the switch and multicast routers in the network. When a switch hears an IGMP report from a host for a given multicast group, the switch adds the host's port number to the multicast table list for that group. And, when the switch hears an IGMP leave, it removes the host's port from the multicast table list.

IGMP snooping can very effectively reduce multicast traffic from streaming and other bandwidth intensive IP applications. While a switch that does not understand multicast will



broadcast the multicast traffic to all the ports in a collision domain (a LAN), a switch using IGMP snooping will only forward multicast traffic to the hosts interested in that traffic. This reduction of multicast traffic reduces the packet processing at the switch (at the cost of needing additional memory to handle the multicast tables) and also reduces the workload at the end hosts since their network cards (or operating system) will not have to receive and filter all the multicast traffic generated in the network.

<b>Quick Setup</b>	<b>Admin</b>	<b>WAN</b>	<b>LAN</b>	<b>NAT</b>	<b>Firewall</b>	<b>Routing</b>	<b>QoS</b>	<b>Other</b>	<b>Status</b>
LAN Settings	DHCP Client List	VLAN Port Settings	Broadcast Storm Control	IGMP Snooping					

**Settings**

IGMP Snooping  Enabled

## 3.4 NAT

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 provides Firewall protection from hacker attacks and has the flexibility to allow you to map Private IP Addresses to Public IP Addresses for key services such as Websites and FTP. To meet various field applications, XRT-401F NAT function can be disabled to as a regular router. If NAT is disabled, all LAN side workstations must have valid IP addresses for Internet access. If the router is used for routing application, not for Internet access, then the NAT function can be disabled.

Parameter	Description
<b>3.4.1 Virtual Server</b>	You can have different services (e.g. email, FTP, Web etc.) going to different service servers/clients in your LAN. The Virtual Server allows you to re-direct a particular service port number (from the Internet/WAN Port) to a particular LAN IP address and its service port number.
<b>3.4.2 Port Triggering</b>	Some applications require multiple connections, such as Internet games, video conferencing, Internet telephony and others. In this section you can configure the router to support these types of applications.
<b>3.4.3 Port Mpping</b>	You can have different services (e.g. email, FTP, Web etc.) going to different service servers/clients in your LAN. The Port Forwarding allows you to re-direct a particular range of service port numbers (from the Internet/WAN Ports) to a particular LAN IP address.
<b>3.4.4 Passthrough</b>	You can select special applications that need "Passthrough" to support here.
<b>3.4.5 DMZ</b>	The DMZ function allows you to re-direct all packets going to your WAN port IP address to a particular IP address in your LAN.

### 3.4.1 Virtual Server

Use the Virtual Server function when you want different servers/clients in your LAN to handle different service/Internet application type (e.g. Email, FTP, Web server etc.) from the Internet. Computers use numbers called port numbers to recognize a particular service/Internet application type. The Virtual Server allows you to re-direct a particular service port number (from the Internet/WAN Port) to a particular LAN private IP address and its service port number.

The screenshot shows the 'Virtual Server' configuration page. The 'Settings' section includes:

- Enabled:**
- Private IP:** 192.168.0.2
- Private Port:** [Empty field]
- Public Port:** [Empty field]
- Type:** TCP
- Comment:** [Empty field]

Buttons for 'Add' and 'Modify' are present. Below is a 'Rules Listing' table:

Comment	Private IP	Private Port	Public Port	Action
HTTP	192.168.0.2	80	tcp	80

The 'Help' section on the right states: 'Virtual Server Allow you to set up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications. Specialized Internet applications are any applications that use Internet access to perform functions such as videoconferencing or online gaming. When users send this type of request to your network via the Internet, the router will forward those requests to the appropriate PC.'

Parameter	Description
<b>Enable</b>	To enable the rule of Virtual Server.
<b>Private IP</b>	This is the LAN client/host IP address that the Public Port number packet will be sent to. <b>Note:</b> You need to give your LAN PC clients a fixed/static IP address for Virtual Server to work properly.
<b>Private Port</b>	This is the port number (of the above Private IP host) that the below Public Port number will be changed to when the packet enters your LAN (to the LAN Server/Client IP)
<b>Type</b>	Select the port number protocol type (TCP, UDP or both). If you are unsure, then leave it to the default both protocols.
<b>Public Port</b>	Enter the service (service/Internet application) port number from the Internet that will be re-directed to the above Private IP address host in your LAN
<b>Comment</b>	The description of this setting.

### 3.4.2 Port Triggering

Some applications require multiple connections, such as Internet games, video conferencing, Internet telephony and others. In this section you can configure the router to support multiple connections for these types of applications.

Parameter	Description
<b>Enable</b>	To enable the rule of Port Triggering.
<b>Trigger Port</b>	This is the out going (Outbound) range of port numbers for this particular application
<b>Trigger Type</b>	Select whether the outbound port protocol is "TCP", "UDP" or both.
<b>Public Port</b>	Enter the In-coming (Inbound) port or port range for this type of application (e.g. 2300-2400, 47624) <b>Note:</b> Individual port numbers are separated by a comma (e.g. 47624, 5775, 6541 etc.). To input a port range use a "dash" to separate the two port number range (e.g. 2300-2400)
<b>Public Type</b>	Select the Inbound port protocol type: "TCP", "UDP" or both
<b>Comment</b>	The description of this setting.


#### Example: Special Applications

If you need to run applications that require multiple connections, then specify the port (outbound) normally associated with that application in the "Trigger Port" field. Then select the protocol type (TCP or UDP) and enter the public ports associated with the trigger port to open them up for inbound traffic.

**Example:**

ID	Trigger Port	Trigger Type	Public Port	Public Type	Comment
1	28800	UDP	2300-2400,47624	TCP	MSN Game Zone
2	6112	UDP	6112	UDP	Battle.net

In the example above, when a user trigger's port 28800 (outbound) for MSN Game Zone then the router will allow incoming packets for ports 2300-2400 and 47624 to be directed to that user.

 <b>Note</b>	Only one LAN client can use a particular special application at a time.
--	---

### 3.4.3 Port Mapping

The Port Mapping allows you to re-direct a particular range of service port numbers (from the Internet/WAN Ports) to a particular LAN IP address. It helps you to host some servers behind the router NAT firewall.

The screenshot shows the 'Port Mapping' configuration page. At the top, there are navigation tabs: Quick Setup, Admin, WAN, LAN, NAT (selected), Firewall, Routing, QoS, Other, and Status. Below these are sub-tabs: Virtual Server, Port Triggering, Port Mapping (selected), Passthrough, and DMZ. The main content area is divided into 'Settings' and 'Rules Listing'.

**Settings:**

- Enabled:
- Comment:
- Server IP: 192.168.0.
- Mapping Ports (port1, port2, port3-port4...):
- Type: TCP (dropdown menu)

Buttons: Add, Modify

**Rules Listing:** 0/10(using/max)

Comment	Server IP	Mapping Ports	Action

Buttons: OK, Cancel

**Help:**

**Port Mapping**  
Allow you to set up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications. Specialized Internet applications are any applications that use Internet access to perform functions such as videoconferencing or online gaming. When users send this type of request to your network via the Internet, the router will forward those requests to the appropriate PC.

Parameter	Description
<b>Enable</b>	To enable the rule of Port Mapping
<b>Comment</b>	The description of this setting.
<b>Server IP</b>	This is the private IP of the server behind the NAT firewall. <b>Note:</b> You need to give your LAN PC clients a fixed/static IP address for Port Forwarding to work properly.
<b>Type</b>	This is the protocol type to be forwarded. You can choose to forward "TCP" or "UDP" packets only or select "both" to forward both "TCP" and "UDP" packets.
<b>Mapping Ports</b>	The range of ports to be forward to the private IP.

### 3.4.4 Passthrough

You can select applications such as PPTP/IPSec/L2TP VPN, FTP and H323 Netmeeting that need “Passthrough” to support. It can let these applications correctly pass through the NAT Router.

Parameter	Description
Enable	You can select to enable “Passthrough” of an application and then the router will let that application correctly pass through the NAT gateway.

### 3.4.5 DMZ

If you have a local client PC that cannot run an Internet application (e.g. Games) properly from behind the NAT firewall, then you can open the client up to unrestricted two-way Internet access by defining a DMZ Host. The DMZ function allows you to re-direct all packets going to your WAN port IP address to a particular IP address in your LAN. The difference between the virtual server and the DMZ function is that the virtual server re-directs a particular service/Internet application (e.g. FTP, websites) to a particular LAN client/server, whereas DMZ re-directs all packets (regardless of services) going to your WAN IP address to a particular LAN client/server.

The screenshot shows the DMZ configuration page. The 'Settings' section includes:

- Enabled:**
- Public IP Address:** 61.62.27.185
- IP Address of Virtual DMZ Host:** 192.168.0.2
- Get current LAN IP automatically
- Buttons:** Add, Modify
- Rules Listing:** 0/6(using/max)

The 'Help' section on the right contains the following text:

**DMZ (DeMilitarized Zone)**  
 Allow one local user to be exposed to the Internet for use of a special-purpose service such as Internet gaming or videoconferencing. It forwards all the ports at the same time to one PC. The Port Forwarding feature is more secure because it only opens the ports you want to have opened, while DMZ hosting opens all the ports of one computer, exposing the computer so the Internet can see it.

**SDMZ (Super DMZ)**

Parameter	Description
<b>Enable</b>	Enable/disable DMZ
<b>Public IP Address</b>	The IP address of the WAN port or any other Public IP addresses given to you by your ISP
<b>IP Address of Virtual DMZ</b>	Input the IP address of a particular host in your LAN that will receive all the packets originally going to the WAN port/Public IP address above.
<b>Action</b>	Press <Add> to add DMZ rule.



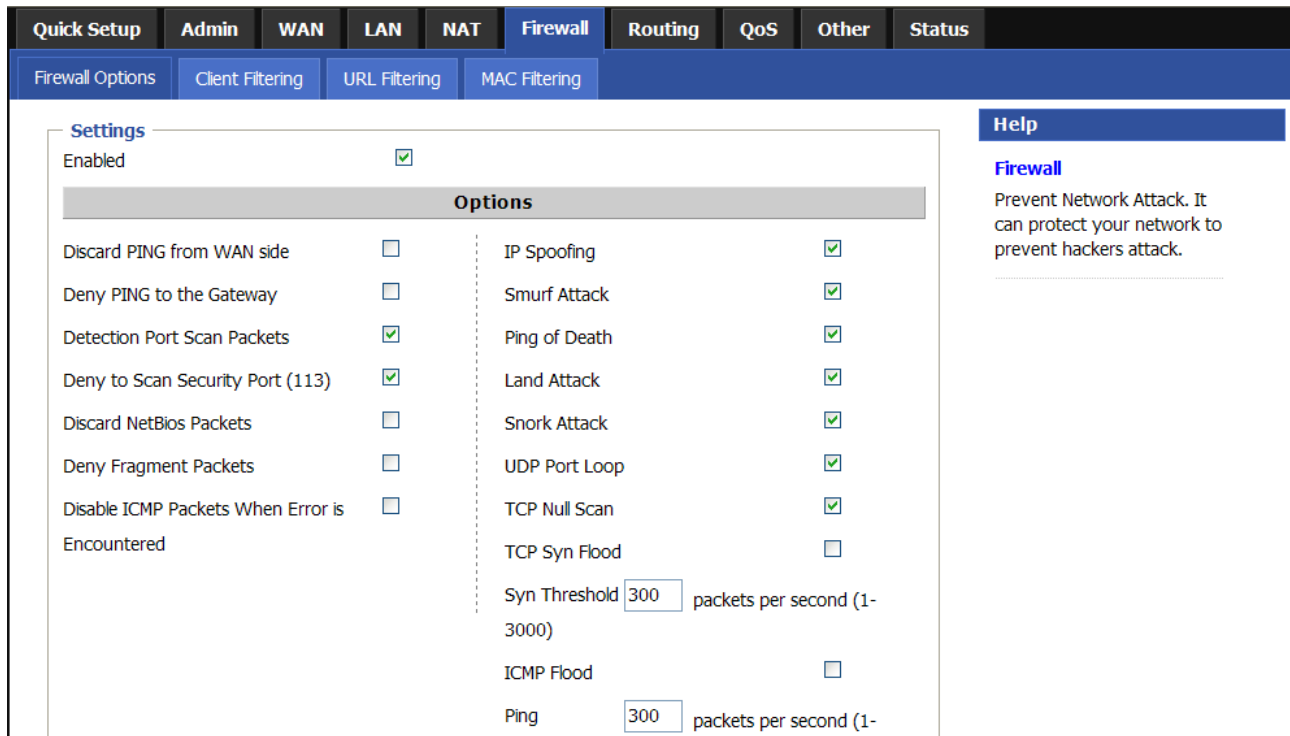
## 3.5 Firewall

XRT-401F provides extensive firewall protection by restricting connection parameters, thus limiting the risk of hacker attack, and defending against a wide array of common Internet attacks.

Parameter	Description
<b>3.5.1 Firewall Options</b>	XRT-401F's firewall can block common hacker attacks and can log the attack activities.
<b>3.5.2 Client Filtering</b>	Client Filtering allows you to specify which hosts users can or cannot access to certain Internet applications by IP address.
<b>3.5.3 URL Filtering</b>	URL Filtering allow you to specify which URLs can not be accessed by users.
<b>3.5.4 MAC Filtering</b>	MAC Filtering allows you to specify which hosts users can or cannot access to Internet by MAC address.

### 3.5.1 Firewall Options

XRT-401F's firewall can block common hacker attacks, including Denial of Service, Ping of Death, Port Scan and Sync Flood. If Internet attacks occur the router can log the events.



Firewall Options	
Parameter	Description
<b>Enable</b>	Select it to enable Firewall Options function.
<b>Discard Ping From WAN</b>	The router's WAN port will not respond to any Ping requests
<b>Deny to Ping the Gateway</b>	The router's LAN port will not respond to any Ping requests
<b>Drop Port Scan Packets</b>	Protection the router from Port Scan.
<b>Allow to Scan Security Port (113)</b>	Select to allow Identification Protocol (Port 113) to be scanned.
<b>Discard NetBIOS Packets</b>	Select to not allow NetBIOS protocol to pass through router
<b>Deny Fragment Packets</b>	Select to deny Fragment Packets passing through.
<b>Send ICMP packets when error</b>	Select to allow sending ICMP error packets to the node who send out the wrong packets..
<b>IP Spoofing</b>	Protection the router from IP Spoofing attack.
<b>Smurf Attack</b>	Protection the router from Smurf Attack attack.
<b>Ping of Death</b>	Protection the router from Ping of Death attack.
<b>Land Attack</b>	Protection the router from Land Attack attack.
<b>Snork Attack</b>	Protection the router from Snork Attack attack.
<b>UDP Port Loop</b>	Protection the router from UDP Port Loop attack.

<b>TCP Sync Flood</b>	Protection the router from Sync Flood attack.
<b>ICMP Flood</b>	Protection the router from ICMP Flood Packet attack.

### 3.5.2 Client Filtering

You can filter Internet access for local clients based on IP addresses, application types, (i.e.,HTTP port), and time of day.

The screenshot shows the 'Client Filtering' configuration page. The 'Settings' section includes:
 

- Enable Client Filter:** Checked.
- Enable:** Unchecked.
- IP Address:** 192.168.0. [ ] ~ [ ]
- Port:** [ ] ~ [ ]
- Type:** TCP
- Block Time:** Radio buttons for 'Always' and 'Block'.
- Day:** Checkboxes for SUN, MON, TUE, WED, THU, FRI, SAT.
- Time:** Dropdowns for 'Always' ~ 'Always'.
- Comment:** Text input field.
- Buttons:** 'Add' and 'Modify'.

 The 'Rules Listing' table at the bottom has columns for IP Address, PortType, Block Time, Comment, and Action. A 'Help' sidebar on the right states: 'Client Filter: Allow you to block Internet access for local clients based on IP addresses, application types, (i.e., HTTP port), and time of day.'

Parameter	Description
<b>Enable Client Filter</b>	Select to enable "Client Filtering" function.
<b>IP</b>	Enter the IP address range that you wish to apply this rule.
<b>Port</b>	You can assign the specific port ranges. The router will block clients from accessing Internet services that use these ports.
<b>Type</b>	This allows you to select UDP, TCP or both protocols that you want to block.
<b>Block Time</b>	Select <Always> router will block the access forever. Select <Block> router will block the access according to the time schedule.
<b>Day</b>	Select a certain days in the week to block the access.
<b>Time</b>	Select a certain time in a day that you want to block.
<b>Comment</b>	The description of this setting.
<b>Enable</b>	To enable the rule of Client Filtering

### 3.5.3 URL Filtering

You can deny or allow the access for some Web sites from particular PCs by entering a full URL address or just keyword of the Web site.

The screenshot shows the 'URL Filtering' configuration page. At the top, there are navigation tabs: Quick Setup, Admin, WAN, LAN, NAT, Firewall (selected), Routing, QoS, Other, and Status. Below these are sub-tabs: Firewall Options, Client Filtering, URL Filtering (selected), and MAC Filtering. The main content area is titled 'Settings' and includes the following fields:

- URL Filter Control:** A dropdown menu set to 'Allow Internet access for the following URL addresses'.
- IP Address:** A field containing '192.168.0.' followed by a small input box and a tilde '~' symbol, and another small input box.
- URL filter string:** An empty text input field.
- Enable:** An unchecked checkbox.

Below the settings are two buttons: 'Add' and 'Modify'. Underneath is a 'Rules Listing' section showing '0/20(using/max)' rules. A table header is visible with columns: IP Address, URL filter string, and Action. At the bottom of the page are 'OK' and 'Cancel' buttons. On the right side, there is a 'Help' section titled 'URL Filter' with the text: 'Url Filtering allowing you to prevent users from accessing specified websites on the basis of some policy.'

Parameter	Description
<b>URL Filter Control</b>	<b>Enable/disable</b> URL Blocking <b>Deny</b> Internet access for the following URL address <b>Allow</b> Internet access for the following URL address
<b>IP</b>	Enter the IP address range that you wish to apply this rule.
<b>URL filter string</b>	You can enter the full URL address or the keyword of the web site you want to block.
<b>Enable</b>	To enable the rule of URL Filtering.

### 3.5.4 MAC Filtering

You can filter Internet access for local clients based on MAC Address. The MAC address filter enables you to allow or restrict specified nodes from communicating with other nodes.

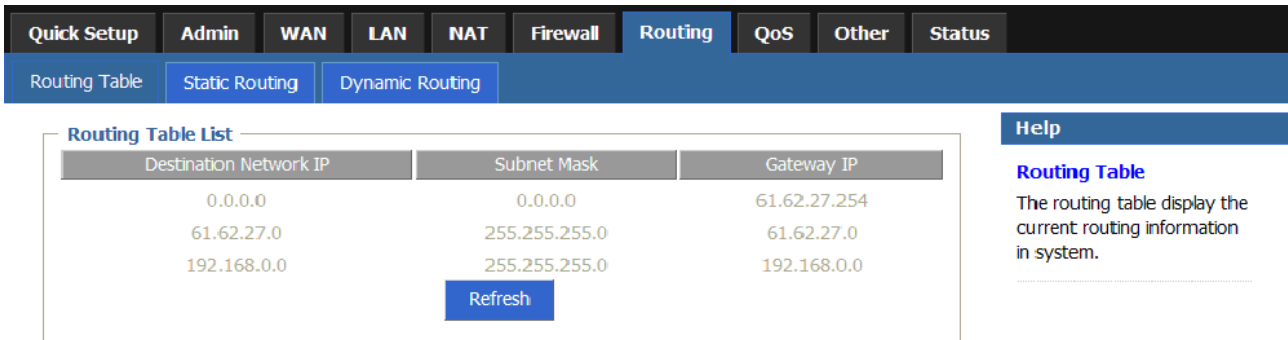
Parameters	Description
<b>MAC Address Control</b>	Check <b>“Enabled”</b> to enable MAC Filtering. Select <b>Deny</b> or <b>Allow</b> the Internet access for the following MAC address connects to Internet.
<b>Configure MAC Address</b>	Fill in or “MAC Address” and “Comment” of the PC, or select the MAC Address from “Action”, and then click “Add”.

## 3.6 Routing

This section allows you to configure XRT-401F's static route and check the current routing table. The routing is only for internal routing using, so you do not need to disable NAT function, and there are two ways to manage the device's routing information, it includes **RIP** and **Static**.

### 3.6.1 Routing Table

The routing table display the current routing information in system.



Destination Network IP	Subnet Mask	Gateway IP
0.0.0.0	0.0.0.0	61.62.27.254
61.62.27.0	255.255.255.0	61.62.27.0
192.168.0.0	255.255.255.0	192.168.0.0

[Refresh](#)

**Help**

**Routing Table**

The routing table display the current routing information in system.

Parameter	Description
<b>Destination LAN IP</b>	The IP address where packets will go to.
<b>Subnet Mask</b>	The subnet mask of the destination IP address.
<b>Gateway</b>	The gateway that the packets will pass by during transmission.

### 3.6.2 Static Routing

This page is used to configure the routing information. Here you can add / delete IP routes.

A static route is a pre-determined pathway that network information must travel to reach a specific host or network. (For example: Destination Network IP: 192.168.100.1, Subnet Mask: 255.255.255.0, Gateway IP: 192.168.0.2)

Parameter	Description
<b>Destination LAN IP, Subnet Mask</b>	Specify the destination LAN IP where the packets will be routing to packets will be routing to.
<b>Gateway</b>	Specify the other gateway IP that will route the packets to the destination.
<b>Add</b>	Click <b>“Add”</b> to add this routing information.

### 3.6.3 Dynamic Routing

Dynamic Routing can be used to cache routes learned by routing protocols, thus allowing the automation of static routing maintenance. The router, using the RIP (Routing Information Protocol) protocol, determines the network packet's route based on the fewest number of hops between the source and the destination. In this case, you could automatically adjust to physical changes in the network layout.

**Dynamic Routing**

Enable Dynamic Routing

Working Mode Router

Listen Mode Both(RIP1+RIP2)

Supply Mode RIP2 (Broadcast)

OK Cancel

**Help**

**RIP**

Dynamic Routing can be used to cache routes learned by routing protocols, thus allowing the automation of static routing maintenance. The router, using the RIP (Routing Information Protocol) protocol, determines the network packet's route based on the fewest number of hops between the source and the destination. In the

Parameter	Description
<b>Working Mome</b>	Specify your XRT-401F work as Router or Gateway.
<b>Listen Mode</b>	Select the <b>RIP version</b> , and to start or stop RIP based on the Global RIP mode selected.
<b>Supply Mode</b>	This parameter determines if the XRT-401F includes the router to this remote node in its RIP broadcasts or RIP Multicast. Select the Mode you want to use.



## 3.7 QoS

By configuring the QoS, you can assign the bandwidth for specific LAN / WAN port. Each LAN Port will follow the bandwidth you assigned. The QoS can smooth your network usage for Triple-Play applications such as the VoIP, IPTV and Internet.

### 3.7.1 IP based

When select this mode,it means the QoS rule by IP,you can set the total bandwidth or specified the bandwidth with the IP range or single IP address.Tick the **Enable Rate Control** and set those parameter.

**Quick Setup** **Admin** **WAN** **LAN** **NAT** **Firewall** **Routing** **QoS** **Other** **Status**

Qos Mode

---

**Qos Mode**

IP Base Rate control by IP

Port Base Rate control by Physical port

DSCP Base Rate control by DSCP value

---

**Settings**

Enable Rate Control

Total upload bandwidth  kbps

Total download bandwidth  kbps

---

Enable Rule

IP Address 192.168.0.  ~

Mode  ▾

Upload  kbps

Download  kbps

Rules Listing 0/10(using/max)

IP Range	Mode	upload (max)	download (max)	Action
----------	------	--------------	----------------	--------

---

Parameter	Description
<b>Total upload bandwidth</b>	Specify the total upload bandwidth.
<b>Total download bandwidth</b>	Specify the total download bandwidth.
<b>IP Address</b>	You can set the IP range or the single IP address.
<b>Mode</b>	Select the <b>Independent</b> or the <b>Share</b> mode. <b>Independent mode:</b> Means the above IP address have the independent bandwidth with the below rule. <b>Share mode:</b> Means the above IP address share the bandwidth with the below rule.
<b>Upload</b>	Set the upload bandwidth.
<b>Download</b>	Set the download bandwidth.
<b>Rules Listing</b>	You can check the rule status you just set on this item


### 3.7.2 Port based

When enabled, you can key in the max / gurantee transmit bandwidth in Kbps, for example, if the WAN **upload** bandwidth is 2Mbps, then, key in 2048, and if the LAN 1 is a PC that want to limit the **PC receiving rate** below 1Mbps, then, key in 1024. That is, key in a number that nuber will be the maximum bandwidth that the Router will give to the connected devices. And keep it in 0 for un-limits at the transmit rate.

**Settings**

Enable Port rate Control

LAN-1	<input type="text" value="0"/>	kbps
LAN-2	<input type="text" value="0"/>	kbps
LAN-3	<input type="text" value="0"/>	kbps
LAN-4	<input type="text" value="0"/>	kbps
WAN	<input type="text" value="0"/>	kbps

 <b>Note</b>	This option can cowork with VLAN priority (refer to section 3.3.3) options to have a optimal network packet transmission.
--	---

### 3.7.3 DSCP

The XRT-401F also support DSCP (Differentiated Services Code Point) that can help to recognize and provide the QoS features to the network packets.

When turned on, the Router will look up the DS (Differentiated Services) field for packet priority.

It will help to forward the packets that contain the priority information accordingly. The DSCP value can be from 0 (lowest priority) to 63 (highest priority). The Router can base on the priority to put the packets into three Weighted Queue, where each queue can have its buffer level from 1 to 15.

<b>Quick Setup</b>	<b>Admin</b>	<b>WAN</b>	<b>LAN</b>	<b>NAT</b>	<b>Firewall</b>	<b>Routing</b>	<b>QoS</b>	<b>Other</b>	<b>Status</b>
--------------------	--------------	------------	------------	------------	-----------------	----------------	------------	--------------	---------------

Qos Mode

**Qos Mode**

IP Base Rate control by IP

Port Base Rate control by Physical port

DSCP Base Rate control by DSCP value

**Settings**

Enable DSCP

High queue weight  (1-15)

Medium queue weight  (1-15)

Low queue weight  (1-15)

---

Enable Rule

DSCP value  (0-63)

Queue map  ▼

Description

Rules Listing 0/10(using/max)

DSCP value	Queue map	Description	Action
------------	-----------	-------------	--------

Below is a reference table for the values. And also the reference about IP precedence level

DSCP Name	DS Field Value		IP Precedence
	Binary	Decimal	
CS0	000 000	0	0
CS1	001 000	8	1
AF11	001 010	10	1
AF12	001 100	12	1
AF13	001 110	14	1
CS2	010 000	16	2
AF21	010 010	18	2
AF22	010 100	20	2
AF23	010 110	22	2
CS3	011 000	24	3
AF31	011 010	26	3
AF32	011 100	28	3
AF33	011 110	30	3
CS4	100 000	32	4
AF41	100 010	34	4
AF42	100 100	36	4
AF43	100 110	38	4
CS5	101 000	40	5
EF	101 110	46	5
CS6	110 000	48	6
CS7	111 000	56	7

IP Precedence Level:

Priority Level	Traffic Type
0 (lowest)	Best Effort
1	Background
2	Standard (Spare)
3	Excellent Load (Business Critical)
4	Controlled Load (Streaming Multimedia)
5	Voice and Video (Interactive Media and Voice)
6	Layer 3 Network Control Reserved Traffic
7 (highest)	Layer 2 Network Control Reserved Traffic

## 3.8 Other

### 3.8.1 UPnP

With **UPnP (Universal Plug and Play)**, all PCs in your Intranet will discover this router automatically. So you do not have to do any configuration for your PC and can access the Internet through this router easily.

UPnP allows automatic discovery and configuration of equipment attached to your LAN. UPnP is supported by Windows ME, XP, or later. It provides compatibility with networking equipment, software and peripherals of the over 400 vendors that cooperate in the Universal Plug and Play forum.

The screenshot shows the 'Other' configuration page for UPnP. The 'Settings' section has 'Enable UPnP' checked, 'Advertise Time' set to 1800, and a 'Refresh' button. The 'Port Mapping' table is as follows:

Remote Host	External Port	Internal Client	Internal Port	Protocol	Description
0.0.0.0	36877	192.168.0.2	36877	tcp	uTorrent (TCP)
0.0.0.0	36877	192.168.0.2	36877	udp	uTorrent (UDP)

The 'Help' section states: UPnP allows automatic discovery and configuration of equipment attached to your LAN. UPnP is supported by Windows ME, XP, or later. It provides compatibility with networking equipment, software and peripherals of the over 400 vendors that cooperate in the Universal Plug and Play forum.

Parameter	Description
<b>Enable UPnP</b>	After you enable the UPnP feature, all client systems that support UPnP, like Windows XP can discover this router automatically and access the Internet through this router without any configuration.
<b>Advertise Time (60 ~ 1800)</b>	When UPnP service is working, router will broadcast a message to LAN that the specific port number has been used in a period of time. The maximum timing is up to <b>1800</b> seconds.

#### UPnP Table

The table display the current UPnP Port Mapping information in system.

Parameter	Description
<b>Remote Host</b>	It shows the IP address of the remote Host.
<b>External Port</b>	It shows the external port number

<b>Internal Port, Internal Client</b>	It shows the internal port number and client.
<b>Protocol</b>	It shows the protocol.
<b>Description</b>	It describes this setting.

### 3.8.2 DDNS

**DDNS (Dynamic DNS)** allows you to map the static domain name to a dynamic IP address. You must get an account, password and your static domain name from the DDNS service providers. DDNS provides you on the Internet with a method to tie their domain name to a computer or server. DDNS allows your domain name to follow your IP address automatically by having your DNS records changed when your IP address changes.

Parameters	Description
<b>Enable / Disable</b>	Enable/Disable the DDNS function of this router
<b>Host Name</b>	Your static domain name that use DDNS.
<b>DDNS Server</b>	Select a DDNS service provider.
<b>User Name</b>	The account that your DDNS service provider assigned to you.
<b>Password</b>	The password you set for the DDNS service account above.
<b>DDNS Retry Time</b>	To set up the time schedule to refresh DDNS setting.

## 3.9 Status

### 3.9.1 System Status

The section allows you to check XRT-401F system status and concurrent hardware information.

Quick Setup	Admin	WAN	LAN	NAT	Firewall	Routing	QoS	Other	Status
<div style="display: flex; justify-content: space-between;"> <span>Status</span> <span>Log</span> </div>									
<b>Gateway</b> IP Address: 192.168.0.1 Subnet Mask: 255.255.255.0 DHCP Server: Enabled NAT: Enabled Firewall: Enabled			<b>Internet</b> Cable/DSL: Connected IP Address: 61.62.27.185 Subnet Mask: 255.255.255.0 Gateway: 61.62.27.254 DNS: 61.64.127.1 Secondary DNS: 61.64.127.2 Domain Name: Connection Type: Static IP Connection Time: 00:07:31				<b>Help</b> <b>Status</b> This status page displays the router's current status and configuration. All information is read-only. <hr/> <b>Firmware Version</b> The version number of the firmware currently installed is displayed here. Visit the web site to find out if there is updated firmware. <hr/> <b>Current Time</b> The current date and time are displayed. <hr/> <b>MAC Address</b>		
<b>Information</b> System Up Time: 00:32:46 System Date: Sat Feb 13 09:22:59 2010 Connected Clients: 1 Firmware Version: 1.0 LAN MAC Address: 00:30:4F:00:AD:01 WAN MAC Address: 00:30:4F:00:AD:02									

Parameter	Description
<b>INTERNET</b>	This item shows XRT-401F's current device settings, including the current <b>WAN IP Address, Subnet Mask, Gateway, DNS and Connection Type</b> .
<b>GATEWAY</b>	This item displays XRT-401F's current device settings, including <b>IP Address, Subnet Mask, DHCP Server, NAT and Firewall Status</b> .
<b>INFORMATION</b>	This item displays XRT-401F hardware device Settings, including <b>Connected Clients, Runtime Code Version and MAC Address</b> .



## 3.9.2 System Log

The Logs record various types of activity on XRT-401F. This data is useful for troubleshooting, but enabling all logs will generate a large amount of data and adversely affect performance. Since only a limited amount of log data can be stored in XRT-401F, log data can also be e-mailed to your PC or sent to a Syslog Server.

The Log displays events occurring within the router by time and date, and also view the description of the event. The user can use the **First Page**, **Prev Page**, **Next Page** and **Last Page** buttons to change the log page listed in the window. The user can click **Setting** to configure your log settings, click **Clear** to clear the log events and click **download** to download the log file on your local PC.

**System Log**

First Page Prev Page Next Page Last Page

No.	Time	Record
1	Sat Feb 13 09:17:19 2010	[FW]Detected Port Scan from 219.85.203.110, drop it
2	Sat Feb 13 09:17:19 2010	[FW]Detected Port Scan from 203.73.91.114, drop it
3	Sat Feb 13 09:17:19 2010	[FW]Detected Port Scan from 125.232.130.11, drop it
4	Sat Feb 13 09:17:24 2010	[FW]Message repeat 1 times
5	Sat Feb 13 09:17:24 2010	[FW]Detected Port Scan from 61.227.195.133, drop it
6	Sat Feb 13 09:17:25 2010	[FW]Detected Port Scan from 122.142.207.92, drop it
7	Sat Feb 13 09:17:28 2010	[FW]Detected Port Scan from 124.11.212.244, drop it
8	Sat Feb 13 09:17:28 2010	[FW]Detected Port Scan from 221.138.1.248, drop it
9	Sat Feb 13	[FW]Detected Port Scan from 125.232.130.11. drop it

**Help**

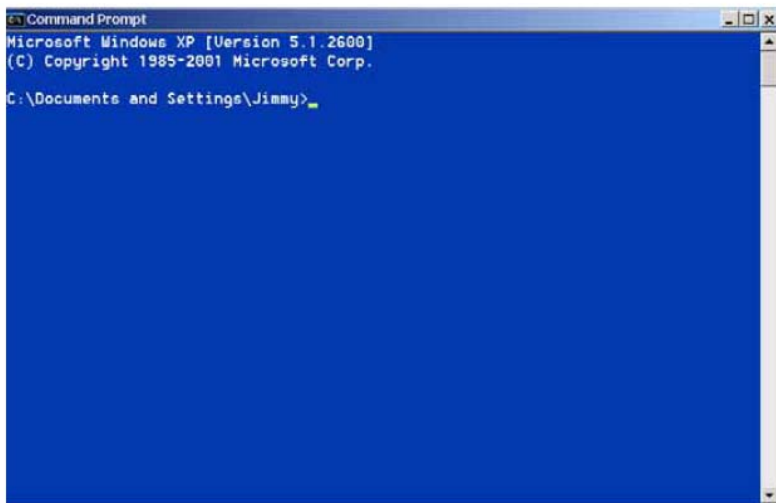
**Log**

The log file keeps a running log of events and activities occurring on the device. You may want to save the log files by clicking on Log Setting. When the device is rebooted, the logs are automatically cleared.

# Appendix A

## How to Manually find your PC's IP and MAC address

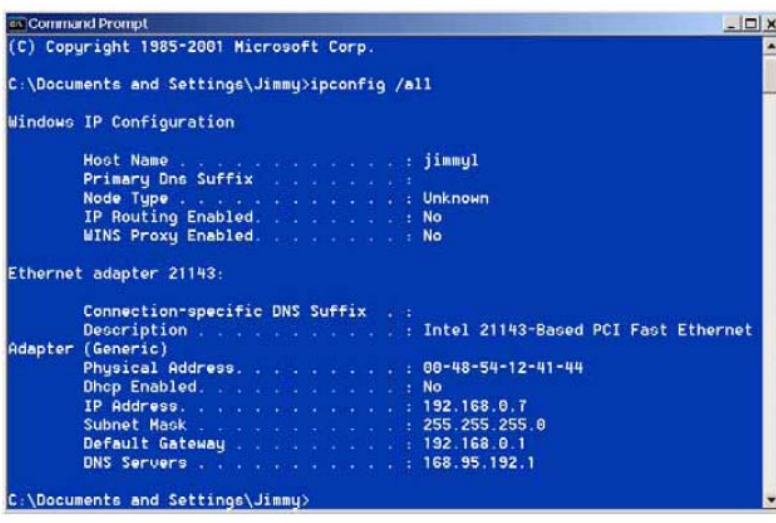
1) In Window's open the Command Prompt program



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

C:\Documents and Settings\Jimmy>
```

2) Type **ipconfig /all** and <enter>



```
Command Prompt
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Jimmy>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : jimmy1
    Primary Dns Suffix . . . . . :
    Node Type . . . . . : Unknown
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

Ethernet adapter 21143:

    Connection-specific DNS Suffix  . :
    Description . . . . . : Intel 21143-Based PCI Fast Ethernet
    Adapter (Generic)
    Physical Address. . . . . : 00-48-54-12-41-44
    Dhcp Enabled. . . . . : No
    IP Address. . . . . : 192.168.0.7
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1
    DNS Servers . . . . . : 168.95.192.1

C:\Documents and Settings\Jimmy>
```

- Your PC's IP address is the one entitled **IP address** (192.168.0.7)
- The router's IP address is the one entitled **Default Gateway** (192.168.0.1)
- Your PC's MAC Address is the one entitled **Physical Address** (00-48-54-12-41-44)

# Appendix B

## About Bridge Mode

This Router supports Bridge mode and the difference between **Bridge mode** and **Router mode** is as following table.

Features \ Mode	Bridge	Router	Remark
<b>Physical Ports</b>	WAN port comes to port 5 of the Router	WAN port	
<b>IP Subnet Operating</b>	<b>One IP Subnet</b> The Router won't route any more	<b>Two IP Subnets</b> The Router route toward the two IP Subnets	
<b>Router Features</b>	<b>Not support</b>	<b>WAN</b> <b>NAT</b> <b>Firewall</b> <b>Routing</b>	
<b>LAN Features</b>	Port Based VLAN 802.1q-based VLAN	DHCP Serve Port Based VLAN	
<b>Management Feature</b>	Only LAN local management	LAN local management WAN remote mangemetn	

# Glossary

**Default Gateway (Router):** Every non-router IP device needs to configure a default gateway's IP address. When the device sends out an IP packet, if the destination is not on the same network, the device has to send the packet to its default gateway, which will then send it out towards the destination.

**DHCP:** Dynamic Host Configuration Protocol. This protocol automatically gives every computer on your home network an IP address.

**DNS Server IP Address:** DNS stands for Domain Name System, which allows Internet servers to have a domain name (such as [www.Broadbandrouter.com](http://www.Broadbandrouter.com)) and one or more IP addresses (such as 192.34.45.8). A DNS server keeps a database of Internet servers and their respective domain names and IP addresses, so that when a domain name is requested (as in typing "[www.planet.com.tw](http://www.planet.com.tw)" into your Internet browser), the user is sent to the proper IP address. The DNS server IP address used by the computers on your home network is the location of the DNS server your ISP has assigned to you.

**DSL Modem:** DSL stands for Digital Subscriber Line. A DSL modem uses your existing phone lines to transmit data at high speeds.

**Ethernet:** A standard for computer networks. Ethernet networks are connected by special cables and hubs, and move data around at up to 10/100 million bits per second (Mbps).

**Idle Timeout:** Idle Timeout is designed so that after there is no traffic to the Internet for a preconfigured amount of time, the connection will automatically be disconnected.

**IP Address and Network (Subnet) Mask:** IP stands for Internet Protocol. An IP address consists of a series of four numbers separated by periods, that identifies a single, unique Internet computer host in an IP network. Example: 192.168.0.1. It consists of 2 portions: the IP network address, and the host identifier.

The IP address is a 32-bit binary pattern, which can be represented as four cascaded decimal numbers separated by "aaa.aaa.aaa.aaa", where each "aaa" can be anything from 000 to 255, or as four cascaded binary numbers separated by "bbbbbbbb.bbbbbbbb.bbbbbbbb.bbbbbbbb", where each "b" can either be 0 or 1.

A network mask is also a 32-bit binary pattern, and consists of consecutive leading 1's followed by consecutive trailing 0's, such as 11111111.11111111.11111111.00000000.

Therefore sometimes a network mask can also be described simply as "x" number of leading 1's. When both are represented side by side in their binary forms, all bits in the IP address that correspond to 1's in the network mask become part of the IP network address, and the remaining bits correspond to the host ID.

For example, if the IP address for a device is, in its binary form, 11011001.10110000.10010000.00000111, and if its network mask is, 11111111.11111111.11110000.00000000 It means the device's network address is 11011001.10110000.10010000.00000000, and its host ID is, 00000000.00000000.00000000.00000111. This is a convenient and efficient method for routers to route IP packets to their destination.

**ISP Gateway Address:** (see ISP for definition). The ISP Gateway Address is an IP address for the Internet router located at the ISP's office.

**ISP:** Internet Service Provider. An ISP is a business that provides connectivity to the Internet for individuals and other businesses or organizations.

**LAN:** Local Area Network. A LAN is a group of computers and devices connected together in a relatively small area (such as a house or an office). Your home network is considered a LAN.

**MAC Address:** MAC stands for Media Access Control. A MAC address is the hardware address of a device connected to a network. The MAC address is a unique identifier for a device with an Ethernet interface. It is comprised of two parts: 3 bytes of data that corresponds to the Manufacturer ID (unique for each manufacturer), plus 3 bytes that are often used as the product's serial number.

**NAT:** Network Address Translation. This process allows all of the computers on your home network to use one IP address. Using XRT-401F's NAT capability, you can access the Internet from any computer on your home network without having to purchase more IP addresses from your ISP.

**Port:** Network Clients (LAN PC) uses port numbers to distinguish one network application/protocol over another. Below is a list of common applications and protocol/port numbers:

Application	Protocol	Port Number
Telnet	TCP	23
FTP	TCP	21
SMTP	TCP	25
POP3	TCP	110
H.323	TCP	1720
SNMP	UCP	161
SNMP Trap	UDP	162
HTTP	TCP	80
PPTP	TCP	1723
PC Anywhere	TCP	5631
PC Anywhere	UDP	5632

**PPPoE:** Point-to-Point Protocol over Ethernet. Point-to-Point Protocol is a secure data transmission method originally created for dial-up connections; PPPoE is for Ethernet connections. PPPoE relies on two widely accepted standards, Ethernet and the Point-to-Point Protocol. It is a communications protocol for transmitting information over Ethernet between different manufacturers

**Protocol:** A protocol is a set of rules for interaction agreed upon between multiple parties so that when they interface with each other based on such a protocol, the interpretation of their behavior is well defined and can be made objectively, without confusion or misunderstanding.

**Router:** A router is an intelligent network device that forwards packets between different networks based on network layer address information such as IP addresses.

**Subnet Mask:** A subnet mask, which may be a part of the TCP/IP information provided by your ISP, is a set of four numbers (e.g. 255.255.255.0) configured like an IP address. It is used to create IP address numbers used only within a particular network (as opposed to valid IP address numbers recognized by the Internet, which must be assigned by InterNIC).

**TCP/IP, UDP:** Transmission Control Protocol/Internet Protocol (TCP/IP) and Unreliable Datagram Protocol (UDP). TCP/IP is the standard protocol for data transmission over the Internet. Both TCP and UDP are transport layer protocol. TCP performs proper error detection and error recovery, and thus is reliable. UDP on the other hand is not reliable. They both run on top of the IP (Internet Protocol), a network layer protocol.

**WAN:** Wide Area Network. A network that connects computers located in geographically separate areas (e.g. different buildings, cities, countries). The Internet is a wide area network.

**Web-based management Graphical User Interface (GUI):** Many devices support a graphical user interface that is based on the web browser. This means the user can use the familiar Netscape or Microsoft Internet Explorer to Control/configure or monitor the device being managed.