



# **Internet Broadband Router**

**XRT-401C**

**XRT-402C**

**XRT-204C**

**User's Manual**

# Copyright

Copyright (C) 2003 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.

# CE mark Warning

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

# 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-401C/XRT-402C/XRT-204C

Rev: 1.0 (Mar. 2003)

Part No. EM-XRTCV1

# Table of Contents

---

<b>CHAPTER 1 INTRODUCTION .....</b>	<b>1</b>
<b>XRT C series Features.....</b>	<b>1</b>
Internet Access Features.....	1
Advanced Internet Functions.....	1
LAN Features .....	2
Configuration & Management.....	2
Security Features .....	2
<b>Package Contents.....</b>	<b>3</b>
<b>Physical Details .....</b>	<b>4</b>
Front-mounted LEDs .....	4
Rear Panel.....	5
<b>CHAPTER 2 PREPARATIONS &amp; INSTALLATION .....</b>	<b>7</b>
<b>Requirements.....</b>	<b>7</b>
<b>Physical Installation .....</b>	<b>7</b>
<b>Preparations on your computer .....</b>	<b>9</b>
<b>Overview.....</b>	<b>9</b>
<b>Windows Clients .....</b>	<b>9</b>
TCP/IP Settings - Overview .....	9
Checking TCP/IP Settings - Windows 9x/ME: .....	10
Checking TCP/IP Settings - Windows NT4.0.....	12
Checking TCP/IP Settings - Windows 2000: .....	16
Checking TCP/IP Settings - Windows XP.....	18
Internet Access.....	20
<b>Macintosh Clients.....</b>	<b>21</b>
<b>Linux Clients .....</b>	<b>21</b>
<b>CHAPTER 3 MACHINE CONFIGURATIONS .....</b>	<b>22</b>
<b>Overview.....</b>	<b>22</b>
<b>Configuration Program .....</b>	<b>22</b>
Preparation .....	22
<b>Quick Setup Wizard.....</b>	<b>25</b>
Connection types supported in XRT C series.....	25
Main Screen .....	26
<b>Quick Setup Wizard Screen .....</b>	<b>27</b>
Time Zone .....	27
Broadband Type.....	28
<b>General Settings .....</b>	<b>32</b>
System Configuration .....	34
WAN Configuration.....	37
Extended WAN Configuration.....	39
LAN Configurations .....	44
<b>NAT Configurations.....</b>	<b>47</b>
Address Mapping.....	48
Virtual Server.....	49
Special Applications .....	51
<b>Firewall Configurations.....</b>	<b>53</b>
Access Control .....	54
URL Blocking.....	56
Schedule Rule .....	57
Intrusion Detection.....	58
DMZ Configurations.....	60
QoS Configurations (XRT-402C/XRT-204C).....	61

<b>CHAPTER 4 OPERATION AND STATUS .....</b>	<b>63</b>
<b>Operation.....</b>	<b>63</b>
<b>Status Screen.....</b>	<b>63</b>
Status and Information .....	64
Internet Connection .....	64
Device Status .....	66
Security Log.....	66
DHCP Client Log .....	67
<b>System Tools .....</b>	<b>68</b>
Configuration Tools .....	68
Firmware Upgrade.....	69
Reset .....	70
<b>APPENDIX A TROUBLESHOOTING .....</b>	<b>71</b>
<b>Overview.....</b>	<b>71</b>
<b>General Problems.....</b>	<b>71</b>
<b>Internet Access.....</b>	<b>71</b>
<b>Glossary .....</b>	<b>72</b>
<b>APPENDIX B SPECIFICATIONS.....</b>	<b>75</b>
<b>XRT C series Specifications .....</b>	<b>75</b>
<b>FCC Statement.....</b>	<b>75</b>
FCC Radiation Exposure Statement.....	76
<b>CE Marking Warning.....</b>	<b>76</b>

# Chapter 1

## Introduction



*This Chapter provides an overview of PLANET XRT C series features and capabilities.*

Congratulations on the purchase of your new XRT C series router. PLANET XRT C is a multi-function device providing the following services:

- **Multiple use of LAN to LAN/WAN accessing:** Supporting DHCP, and up to 253 dynamic users, the XRT-401C eliminates the need for a dedicated IP address scheme. LAN-to-LAN and LAN-to-WAN connectivity is now available to all enabled users. Meantime, WAN interfaces in XRT-402C (2 WAN) and XRT-204C (4 WAN) are suitable for SOHO networking Internet access.
- **Easy setup and network administration:** Via built-in configuration wizard and intuitive user interface, network administrator/IT personnel can complete Internet connection just in minutes! System administrators can logon machine locally from LAN or remotely check machine/network status and start administration or trouble-shooting from anywhere simply via Internet browsers.

### XRT C series Features

PLANET XRT C series incorporates many advanced features, carefully designed to provide sophisticated functions while being easy to use.

#### Internet Access Features

- **Shared Internet Access.** All users on LAN side can access the Internet through XRT-401C, using only a single external IP Address. XRT-402C/204C support dual/four WAN connections to ease the needs of heavy Internet access. All the local (invalid) IP Addresses are hidden from external sources. This process is called NAT (Network Address Translation).
- **DSL & Cable Modem Support.** Providing Internet access via single user account for everyone on your LAN. In the meantime, XRT-402C/204C are able to handle up to dual/four WAN connection (xDSL/Cable/fixed IP allocation) to provide more bandwidth choice to meet power users or enterprise network demands.
- **PPPoE, PPTP Support.** The Internet (WAN port) connection supports PPPoE (PPP over Ethernet), DHCP (Dynamic Host Configuration Protocol), PPTP (Peer-to-Peer Tunneling Protocol), and "Direct Connection" type services are supported as well.

#### Advanced Internet Functions

- **Virtual Server, multiple DMZ & Internet applications.** XRT C series supports Virtual server with port re-direction features to share local resources like Email, FTP or HTTP server to the Internet in a more convenient way. Multiple DMZ capability not only brings convenience to Internet applications demanding for bi-directional data transmission, also enable LAN side servers act as like an independent Internet node that communicate to the Internet in both direction. In the meantime, XRT supports various Internet applications, such as interactive Gaming, Telephony, and Conferencing applications; you may define customized application rules to meet various Internet applications. UPnP support in XRT-401C can bring users convenient management, and eliminate configuration time to

different application/software. (UPnP functionality requires Microsoft Windows ME/XP or later version)

- **Firewall, access control, and IDS mechanism.** XRT C series provides SPI firewall protection, Intrusion detection system to bring you peace of mind and prevent business or residential network from malicious attacking or hacking. The URL filtering, scheduled firewall and access control system in XRT C series also can give network administrators more privilege choices to apply to LAN users Internet access or prevent office workers improper Internet usages. Meantime, access control in XRT C series can be determined by application/service type, and make schedule to decide when and who should be limited Internet access on your network..
- **Multi-homing, Load balance, redundant link & QoS (XRT-402C and XRT-204C).** XRT-402C/XRT-204C equipped with dual/four WAN interfaces for different kinds of Internet access (xDSL/cable/fixed IP) satisfy high Internet bandwidth demands in enterprise environment. Network administrator may bind different kind of Internet access to respective WAN interfaces to enable load balance or redundant link (backup line) for optimization of network loading. Meantime, QoS support also can classify bandwidth usage to meet time-critical applications; administrators may define QoS rules by service type, source/destination IP, communication port numbers or MAC address to take full advantages of network bandwidth.
- **VPN Pass through Support.** PCs with VPN (Virtual Private Networking) software using PPTP, L2TP and IPSec are transparently supported - no configuration is required.

## LAN Features

- **DHCP Server Support.** Dynamic Host Configuration Protocol provides a dynamic IP address to PCs and other devices upon request. XRT C can act as a **DHCP Server** for devices on your local LAN.
- **Address Mapping.** When one or more IP address obtained from your ISP, XRT C allows one or more Public IP Address(es) to be mapped to a pool of local Private IP Address(es).

## Configuration & Management

- **Easy setup and network administration** Via built-in configuration wizard and intuitive user interface, network administrator/IT personnel can complete Internet connection just in minutes! System administrators can logon machine locally from LAN or remotely check machine/network status and start administration or trouble-shooting from anywhere simply via Internet browsers.
- **Remote Management.** XRT C can be managed from any PC on your LAN. And, if the Internet connection exists, it can also (optionally) be configured via the Internet.

## Security Features

- **Password - protected Configuration.** Optional password protection is provided to prevent unauthorized users from modifying the configuration data and settings.
- **NAT Protection.** An intrinsic side effect of NAT (Network Address Translation) technology is that by allowing all LAN users to share a single IP address, the location and even the existence of each PC is hidden. From the external viewpoint, there is no network, only a single device – your XRT C series router.
- **Stateful Inspection Firewall.** All incoming data packets are monitored and all incoming server requests are filtered, thus protecting your network from malicious attacks from external sources.

- ***Protection against DoS attacks.*** DoS (Denial of Service) attacks can flood your Internet connection with invalid packets and connection requests; using so much bandwidth and so many resources that Internet access becomes unavailable. PLANET XRT C series incorporates protection against DoS attacks to secure your network.
- ***Scheduled, and Rule-based Policy Firewall.*** To provide additional protection against malicious packets, you can define your own firewall rules. This can also be used to control the Internet services available to LAN users.

## Package Contents

The following items should be included:

- XRT C Broadband router Unit
- Power Adapter
- Quick Installation Guide
- CD-ROM containing the user's manual.

If any of the above items are damaged or missing, please contact our local dealer immediately.

# Physical Details

## Front-mounted LEDs

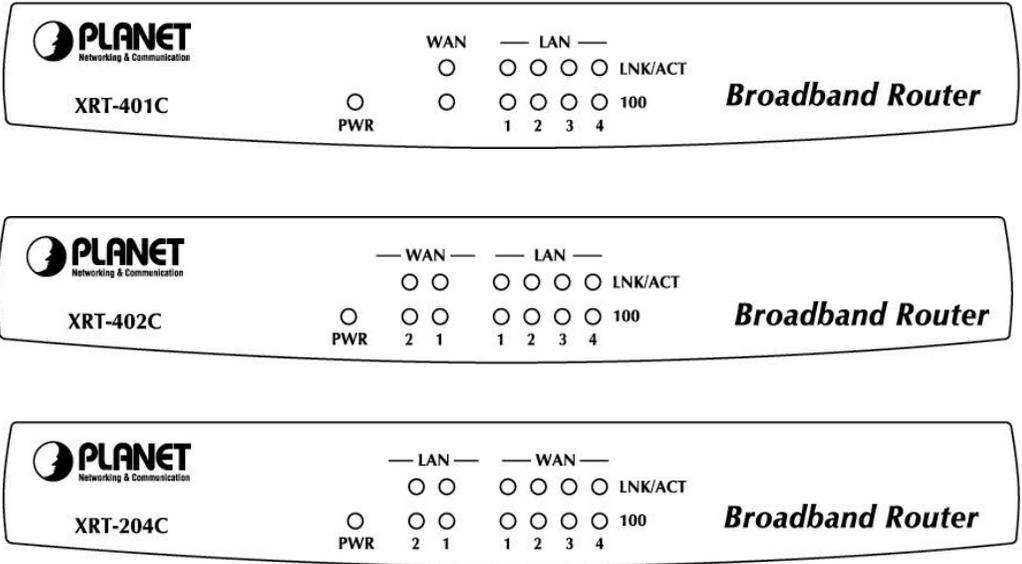
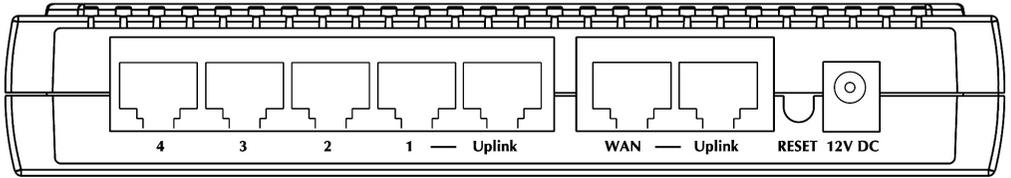


Figure: XRT C series Front Panel

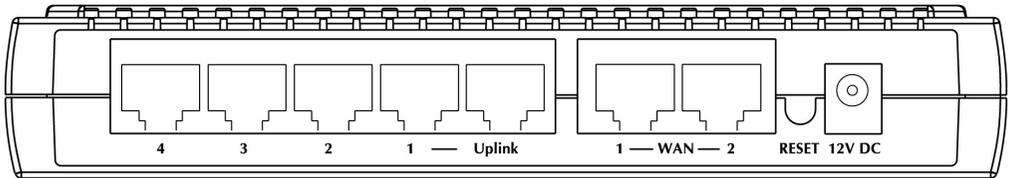
### LED definitions

<b>PWR</b>	<b>On</b> - Power on; <b>Off</b> - No power.
<b>LAN</b>	<p>For each port, there are 2 LEDs</p> <ul style="list-style-type: none"> <li>• <b>LNK/ACT</b> <ul style="list-style-type: none"> <li>• <b>On</b> - Corresponding LAN port is active.</li> <li>• <b>Off</b> - No active connection on the corresponding LAN port.</li> <li>• <b>Flashing</b> - Data is being transmitted or received via the corresponding LAN port.</li> </ul> </li> <li>• <b>100</b> <ul style="list-style-type: none"> <li>• <b>On</b> - Corresponding LAN port is using 100BaseT.</li> <li>• <b>Off</b> - Corresponding LAN port connection is using 10BaseT, or no active connection.</li> </ul> </li> </ul>
<b>WAN</b>	<ul style="list-style-type: none"> <li>• <b>LNK/ACT</b> <ul style="list-style-type: none"> <li>• <b>On</b> - Corresponding WAN port is active.</li> <li>• <b>Off</b> - No active connection on the corresponding WAN port.</li> <li>• <b>Flashing</b> - Data is being transmitted or received via the corresponding WAN port.</li> </ul> </li> <li>• <b>100</b> <ul style="list-style-type: none"> <li>• <b>On</b> - Corresponding WAN port is using 100BaseT.</li> <li>• <b>Off</b> - Corresponding WAN port connection is using 10BaseT, or no active connection.</li> </ul> </li> </ul>

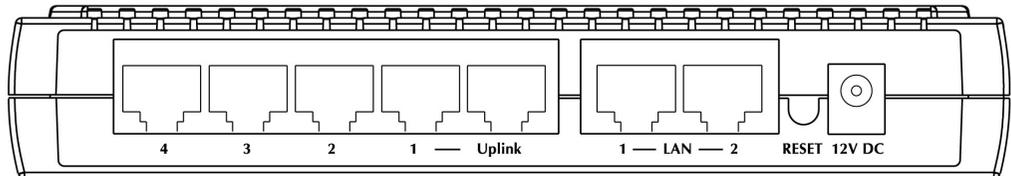
## Rear Panel



**XRT-401C rear panel**



**XRT-402C rear panel**



**XRT-204C rear panel**

### WAN port (10/100BaseT)

Connect the DSL or Cable Modem here. If your modem came with a cable, use the supplied cable. Otherwise, use a standard LAN cable.

#### ö Note

If the connection cannot be established (WAN LED is not on), please connect to the *Uplink* port instead, and check if the supplied cable is broken.

### 10/100BaseT LAN connections

Use standard LAN cables (RJ-45 connectors) to connect your PCs to these ports.

#### ö Note

If the connection cannot be established (LAN LED is not on), please connect to the *Uplink* port instead, and check if the supplied cable is broken.

**Reset Button**

This button has two (2) functions:

- **Reboot.** When pressed and released, the router will reboot (restart).
- **Clear All Data.** This button can also be used to clear ALL data and restore ALL settings to the factory default values.

**To Reboot machine without Clearing Existing Configurations:**

Press the reset button with a pencil tip (for less than 4 seconds), machine will re-boot itself, the existing configurations will be kept.

**To Clear All Data and restore the factory default values:**

- Press the reset button for longer than 4 seconds and the router will reset itself to the factory default settings (warning: your original configurations will be replaced with the factory default settings)

• **Note**

- 
1. These steps can restore machine factory default IP address: 192.168.0.1, without logon password while the password is forgotten.
- 

**Power port**

Connect the supplied power adapter here.

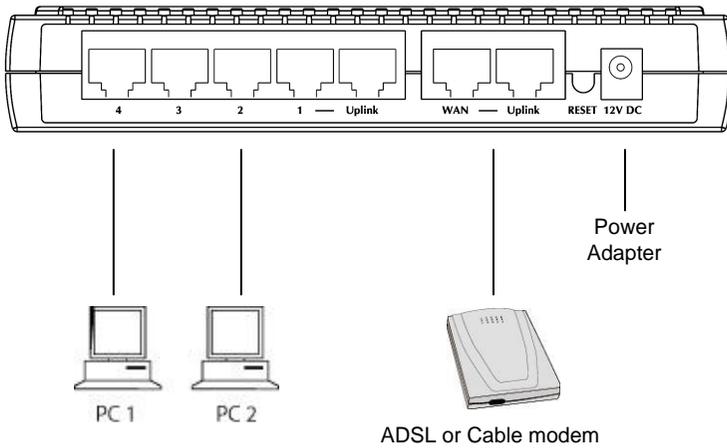
# Preparations & Installation

*This Chapter covers the physical installation of XRT C series.*

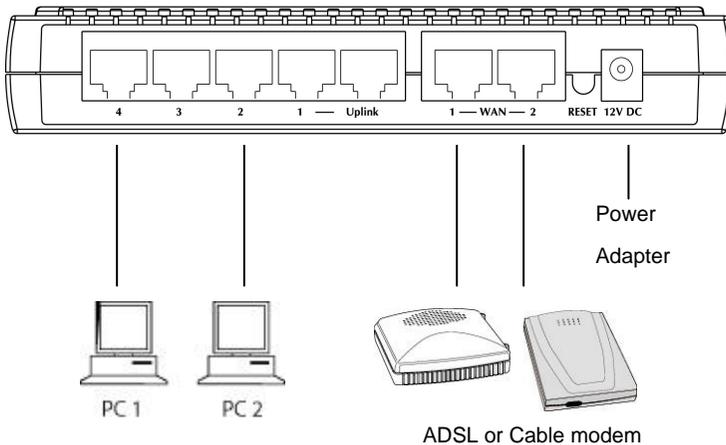
## Requirements

- Network cables. Use standard 10/100BaseT network (UTP) cables with RJ-45 connectors.
- TCP/IP protocol must be installed on all PCs.
- For Internet Access, an Internet Access account with an ISP, and either of a DSL or Cable modem (for WAN port usage).

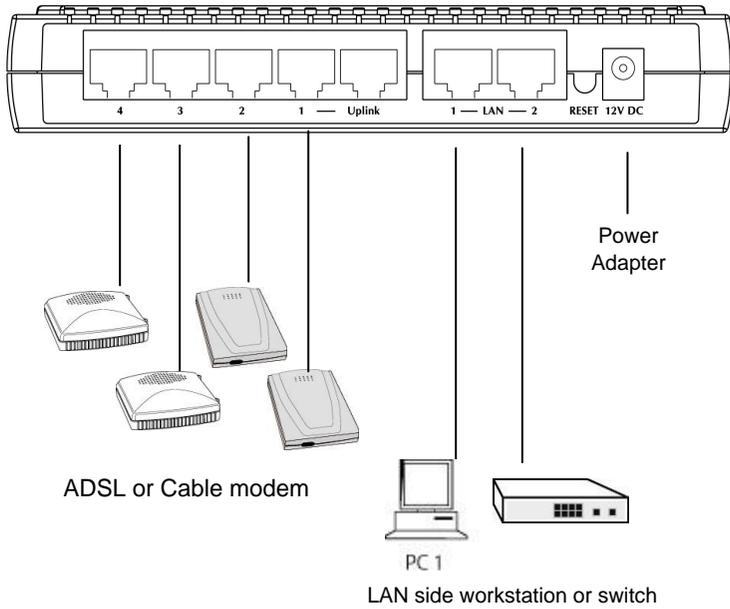
## Physical Installation



**Physical connection of XRT-401C**



**Physical connection of XRT-402C**



**Physical connection of XRT-204C**

### 1. Choose an Installation Site

Ensure your router and the Cable/DSL modem are powered OFF before commencing. Leave your Cable/DSL modem connected to its wall socket (phone line or cable input).

### 2. Connect LAN Cables

Use standard LAN cables to connect PCs to the switch ports on your Router.

### 3. Connect WAN Cable

Connect your Cable/DSL **Modem** to the **WAN** port on your Router. Use the cable supplied with your Cable/DSL modem. If no cable was supplied with your modem, use a standard network cable. Please make sure the connection is established (LED is on).

### 4. Power Up

Power on the Cable or DSL modem. Connect the supplied power adapter to router and power up. Use only the power adapter provided. Using a different one may cause hardware damage

### 5. Check the LEDs

- The *PWR* LED should be ON.
- For each LAN (PC) connection, the LAN *LNK/ACT* LED should be ON. (if your network is 100Mbps speed, the *100* LED will be on, too.)

The *WAN LNK/ACT* LED should be ON.

For more information, refer to Front-mounted LEDs in Chapter 1.

## Preparations on your computer

*This section details the PC Configuration required on the local ("Internal") LAN.*

### Overview

For each PC, the following may need to be configured:

- TCP/IP network settings
- Internet Access configuration

### Windows Clients

This section describes how to configure Windows clients for Internet access via XRT C series router.

The first step is to check the PC's TCP/IP settings.

PLANET XRT C series utilize the TCP/IP network protocol for all functions, so it is essential that the TCP/IP protocol is installed and configured on each PC.

### TCP/IP Settings - Overview

**If using machine default settings, and the default Windows TCP/IP settings, no changes need to be made.**

- By default, XRT will act as a DHCP Server, automatically providing a suitable IP Address (and related information) to each PC when the PC boots.
- For all non-Server versions of Windows, the default TCP/IP setting is to act as a DHCP client.

**If using a Fixed (specified) IP address, the following changes are required:**

- The *Gateway* must be set to the IP address of XRT.
- The *DNS* should be set to the address provided by your ISP.

## Checking TCP/IP Settings - Windows 9x/ME:

1. Select *Control Panel - Network*. You should see a screen like the following:

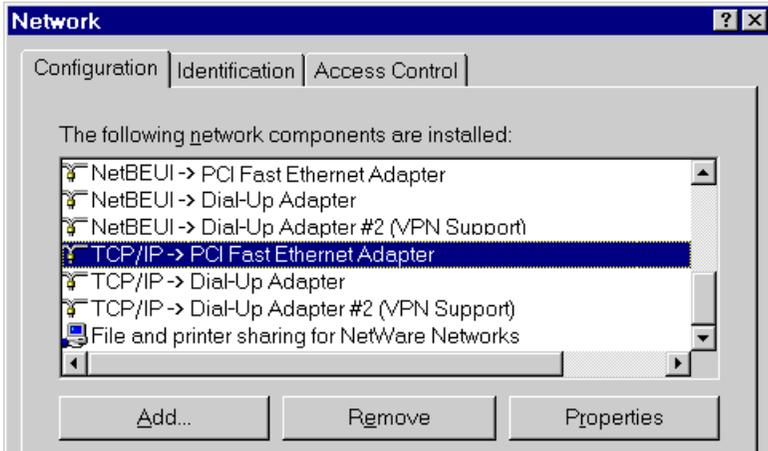


Figure: Network Configuration

2. Select the *TCP/IP* protocol for your network card.
3. Click on the *Properties* button. You should then see a screen like the following.

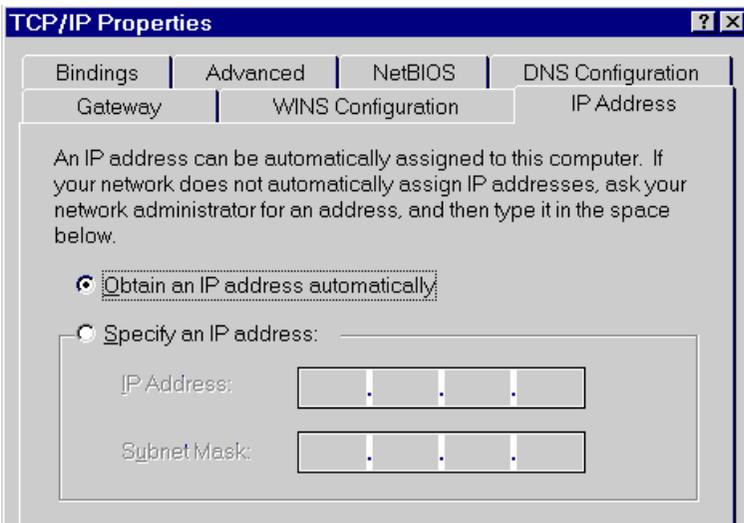


Figure: IP Address (Win 95)

Ensure your TCP/IP settings are correct, as follows:

### Using DHCP

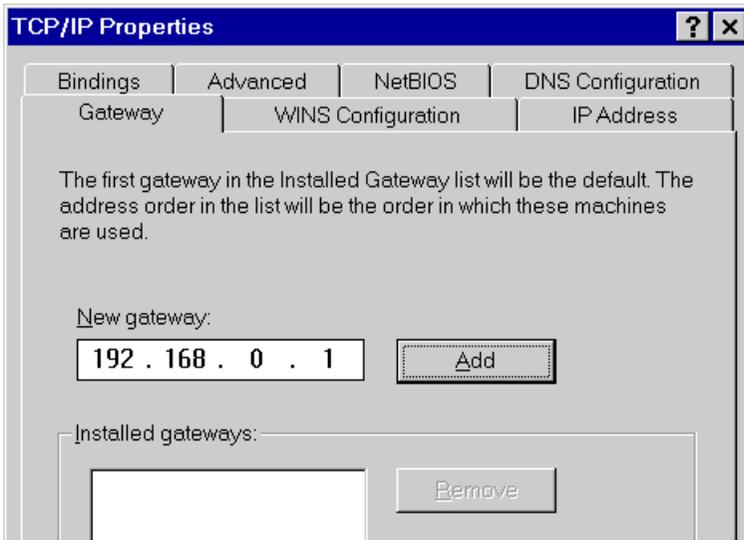
To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows setting. **Using this is recommended.** By default, XRT will act as a DHCP Server.

Restart your PC to ensure it obtains an IP Address from XRT.

### Using "Specify an IP Address"

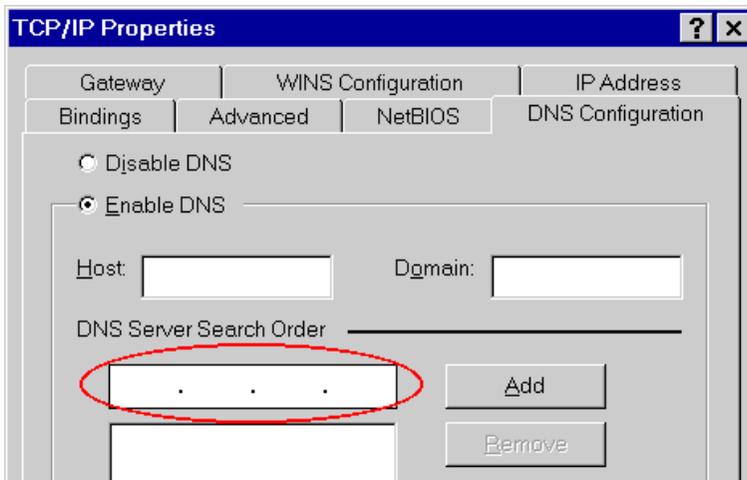
If your PC is already configured, check with your network administrator before making the following changes:

- On the *Gateway* tab, enter XRT's IP address in the *New Gateway* field and click *Add*, as shown below. Your LAN administrator can advise you of the IP Address they assigned to XRT.



**Figure: Gateway Tab (Win 95/98)**

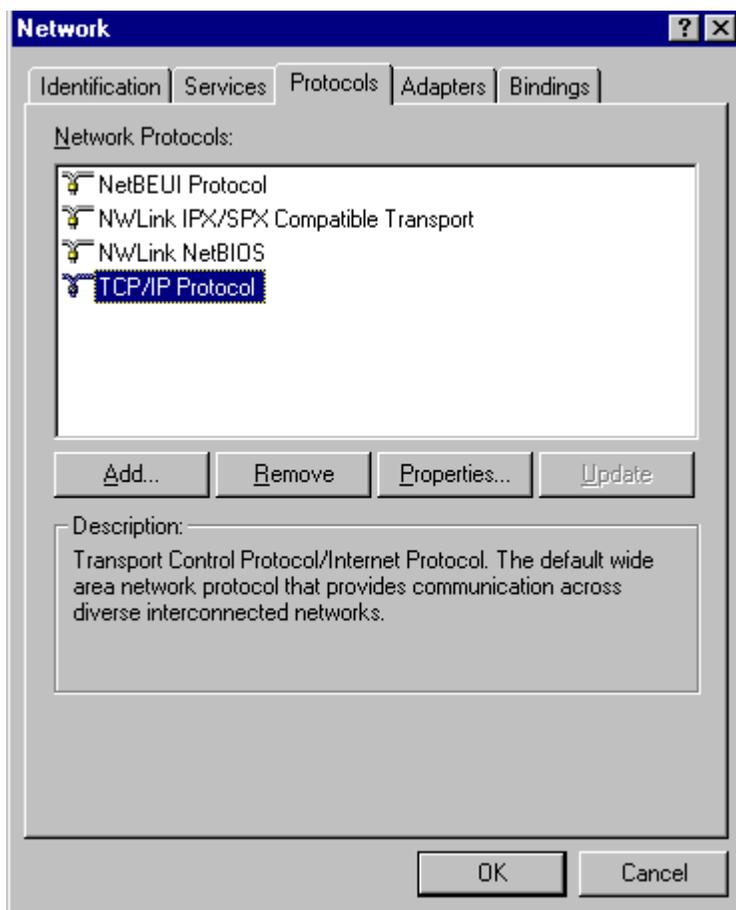
- On the *DNS Configuration* tab, ensure *Enable DNS* is selected. If the *DNS Server Search Order* list is empty, enter the DNS address provided by your ISP in the fields beside the *Add* button, then click *Add*.



**Figure: DNS Tab (Win 95/98)**

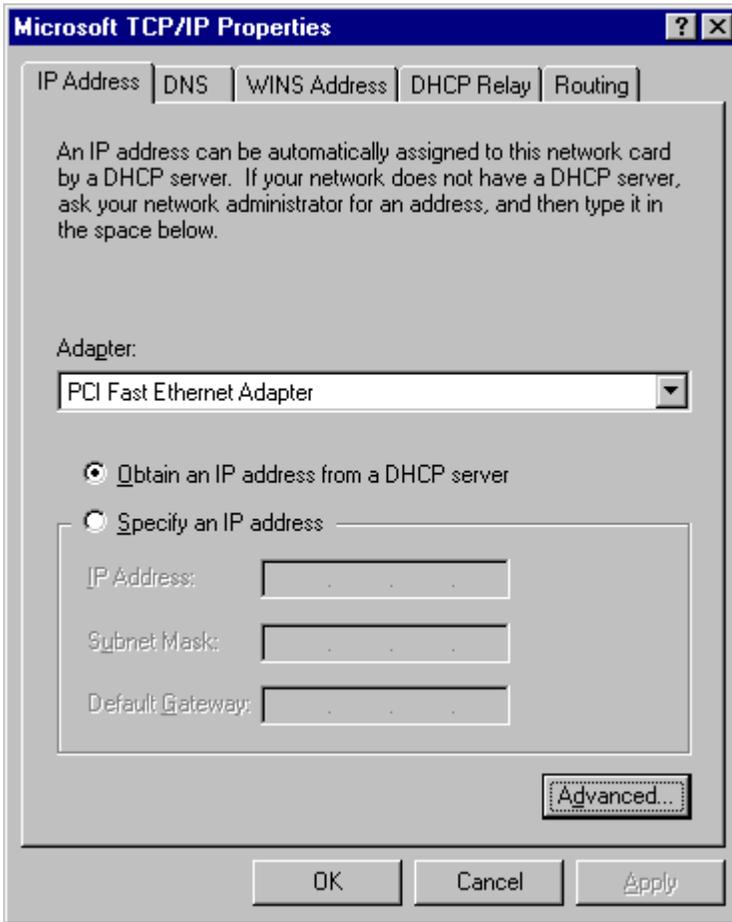
## Checking TCP/IP Settings - Windows NT4.0

1. Select *Control Panel - Network*, and, on the *Protocols* tab, select the TCP/IP protocol, as shown below.



**Figure: Windows NT4.0 - TCP/IP**

2. Click the *Properties* button to see a screen like the one below.



**Figure: Windows NT4.0 - IP Address**

3. Select the network card for your LAN.
4. Select the appropriate radio button - *Obtain an IP address from a DHCP Server* or *Specify an IP Address*, as explained below.

### Obtain an IP address from a DHCP Server

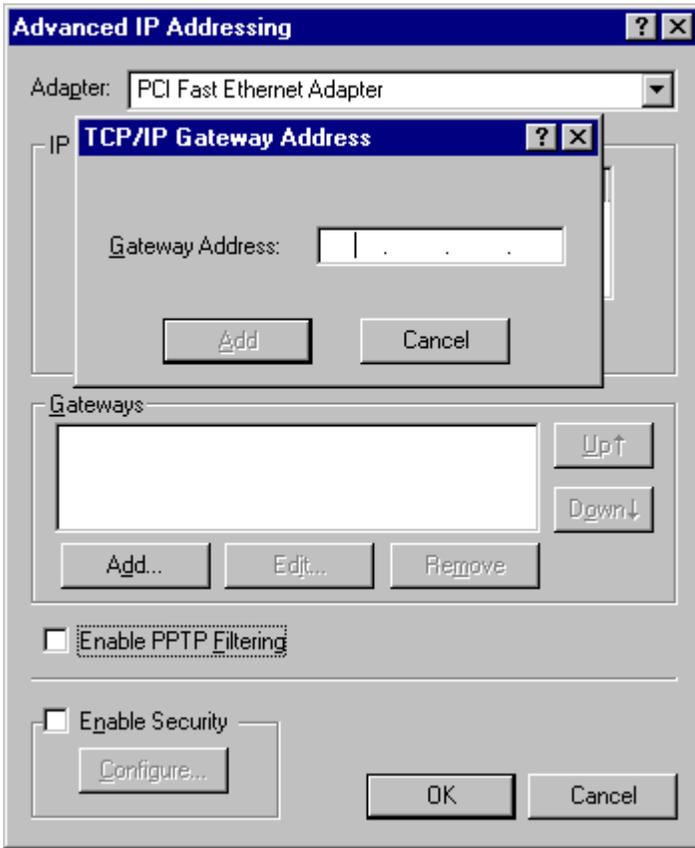
This is the default Windows setting. **Using this is recommended.** By default, XRT will act as a DHCP Server.

Restart your PC to ensure it obtains an IP Address from XRT.

### Specify an IP Address

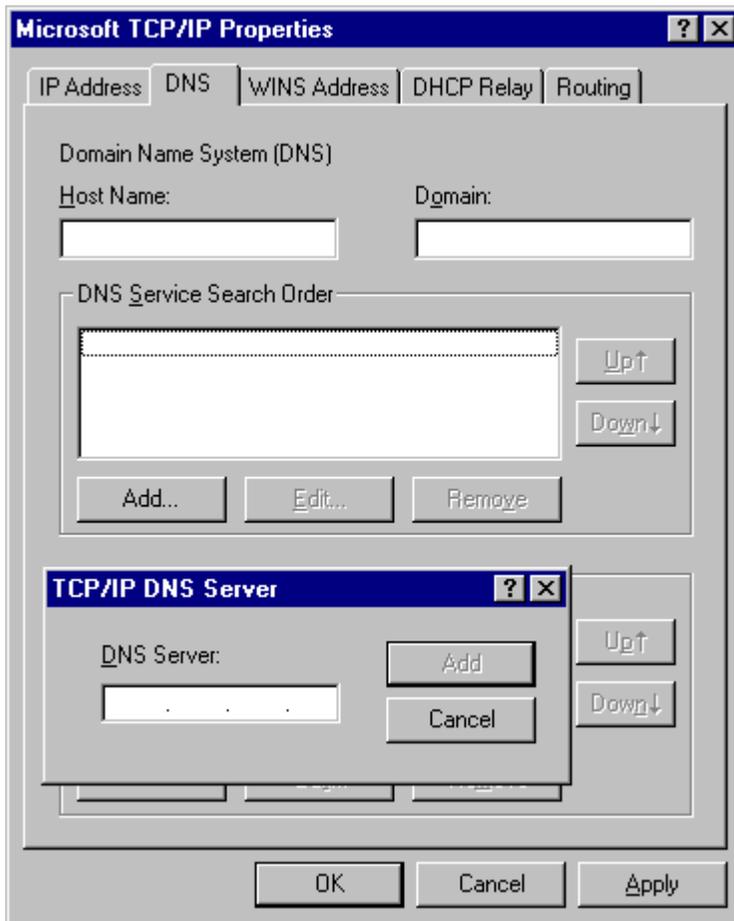
If your PC is already configured, check with your network administrator before making the following changes.

1. The *Default Gateway* must be set to the IP address of XRT. To set this:
  - Click the *Advanced* button on the screen above.
  - On the following screen, click the *Add* button in the *Gateways* panel, and enter XRT's IP address, as shown in below.
  - If necessary, use the *Up* button to make XRT the first entry in the *Gateways* list.



**Figure - Windows NT4.0 - Add Gateway**

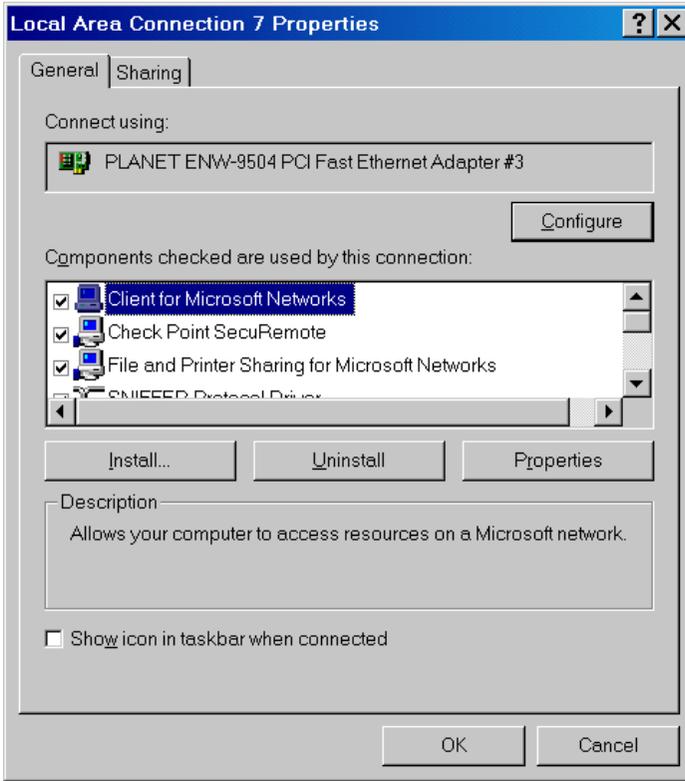
2. The DNS should be set to the address provided by your ISP, as follows:
  - Click the DNS tab.
  - On the DNS screen, shown below, click the *Add* button (under *DNS Service Search Order*), and enter the DNS provided by your ISP.



**Figure: Windows NT4.0 - DNS**

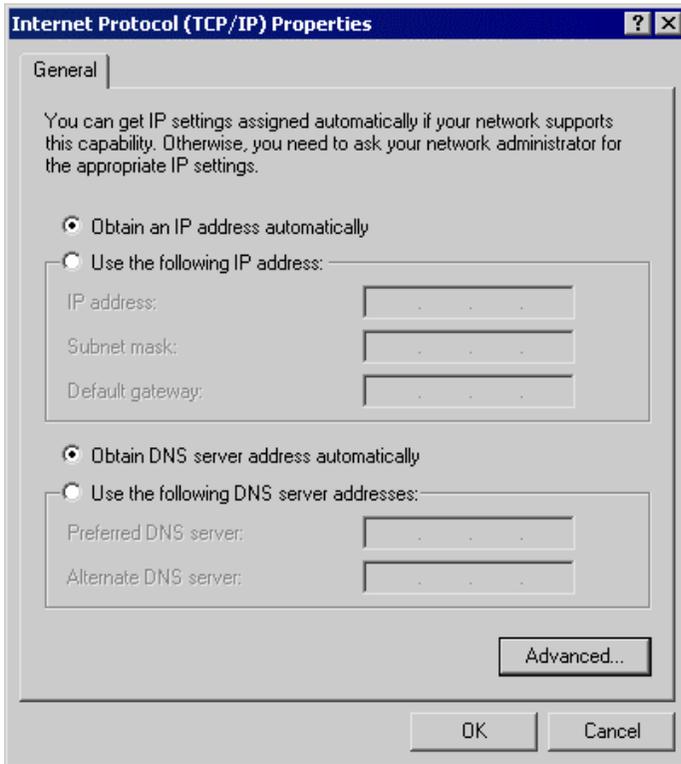
## Checking TCP/IP Settings - Windows 2000:

1. Select *Control Panel - Network and Dial-up Connection*.
2. Right - click the *Local Area Connection* icon and select *Properties*. You should see a screen like the following:



**Figure: Network Configuration (Win 2000)**

3. Select the *TCP/IP* protocol for your network card.
4. Click on the *Properties* button. You should then see a screen like the following.



**Figure: TCP/IP Properties (Win 2000)**

5. Ensure your TCP/IP settings are correct, as described below.

### Using DHCP

To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows setting. **Using this is recommended.** By default, XRT will act as a DHCP Server.

Restart your PC to ensure it obtains an IP Address from XRT.

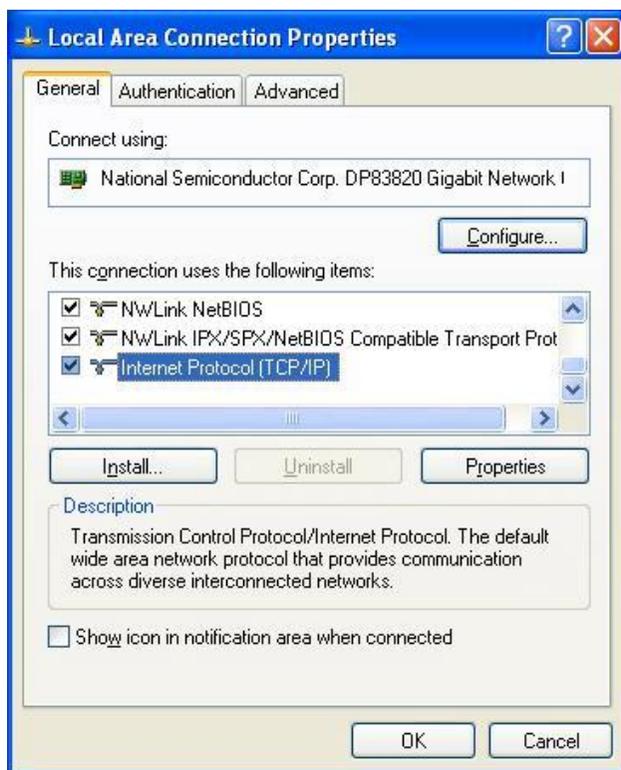
### Using a fixed IP Address ("Use the following IP Address")

If your PC is already configured, check with your network administrator before making the following changes.

- Enter XRT's IP address in the *Default gateway* field and click *OK*. (Your LAN administrator can advise you of the IP Address they assigned to XRT.)
- If the *DNS Server* fields are empty, select *Use the following DNS server addresses*, and enter the DNS address or addresses provided by your ISP, then click *OK*.

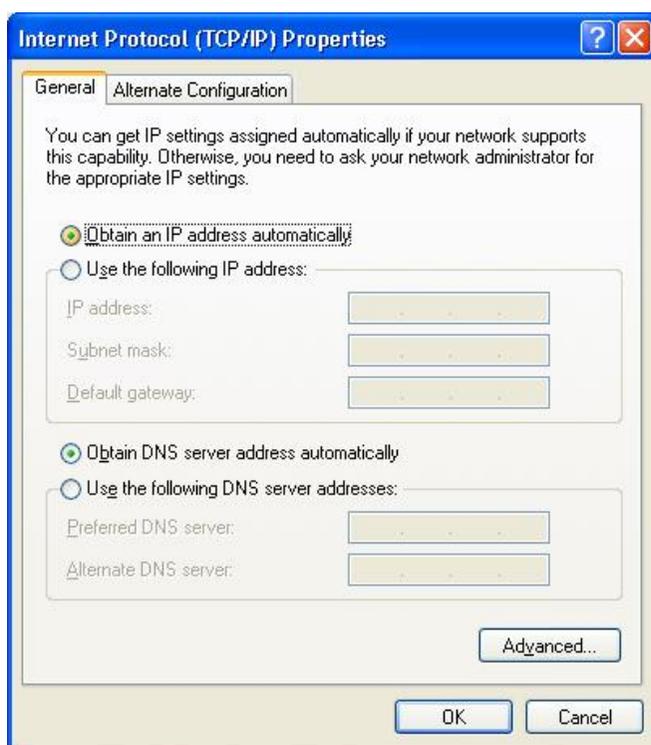
## Checking TCP/IP Settings - Windows XP

1. Select *Control Panel - Network Connection*.
2. Right click the *Local Area Connection* and choose *Properties*. You should see a screen like the following:



**Figure: Network Configuration (Windows XP)**

3. Select the *TCP/IP* protocol for your network card.
4. Click on the *Properties* button. You should then see a screen like the following.



**Figure: TCP/IP Properties (Windows XP)**

5. Ensure your TCP/IP settings are correct.

### Using DHCP

To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows setting. **Using this is recommended.** By default, XRT will act as a DHCP Server.

Restart your PC to ensure it obtains an IP Address from XRT.

### Using a fixed IP Address ("Use the following IP Address")

If your PC is already configured, check with your network administrator before making the following changes.

- In the *Default gateway* field, enter XRT's IP address and click *OK*. Your LAN administrator can advise you of the IP Address they assigned to XRT.
- If the *DNS Server* fields are empty, select *Use the following DNS server addresses*, and enter the DNS address or addresses provided by your ISP, then click *OK*.

## Internet Access

To configure your PCs to use XRT for Internet access:

- Ensure that the DSL modem, Cable modem, or other permanent connection is functional.
- Use the following procedure to configure your Browser to access the Internet via the LAN, rather than by a Dial-up connection.

### For Windows 9x/ME/2000

1. Select *Start Menu - Settings - Control Panel - Internet Options*.
2. Select the *Connection* tab, and click the *Setup* button.
3. Select "I want to set up my Internet connection manually, or I want to connect through a local area network (LAN)" and click *Next*.
4. Select "I connect through a local area network (LAN)" and click *Next*.
5. Ensure all of the boxes on the following Local area network Internet Configuration screen are **unchecked**.
6. Check the "No" option when prompted "Do you want to set up an Internet mail account now?"
7. Click *Finish* to close the Internet Connection Wizard.  
Setup is now completed.

### For Windows XP

1. Select *Start Menu - Control Panel - Network and Internet Connections*.
2. Select *Set up or change your Internet Connection*.
3. Select the *Connection* tab, and click the *Setup* button.
4. Cancel the pop-up "Location Information" screen.
5. Click *Next* on the "New Connection Wizard" screen.
6. Select "Connect to the Internet" and click *Next*.
7. Select "Set up my connection manually" and click *Next*.
8. Check "Connect using a broadband connection that is always on" and click *Next*.
9. Click *Finish* to close the New Connection Wizard.  
Setup is now completed.

### Accessing AOL

To access AOL (America On Line) through XRT, the *AOL for Windows* software must be configured to use TCP/IP network access, rather than a dial-up connection. The configuration process is as follows:

- Start the *AOL for Windows* communication software. Ensure that it is Version 2.5, 3.0 or later. This procedure will not work with earlier versions.
- Click the *Setup* button.
- Select *Create Location*, and change the location name from "New Locality" to "XRT".
- Click *Edit Location*. Select *TCP/IP* for the *Network* field. (Leave the *Phone Number* blank.)
- Click *Save*, then *OK*.  
Configuration is now complete.
- Before clicking "Sign On", always ensure that you are using the "XRT" location.

## Macintosh Clients

From your Macintosh, you can access the Internet via XRT. The procedure is as follows.

1. Open the TCP/IP Control Panel.
2. Select *Ethernet* from the *Connect via* pop-up menu.
3. Select *Using DHCP Server* from the *Configure* pop-up menu. The DHCP Client ID field can be left blank.
4. Close the TCP/IP panel, saving your settings.

-----  
 If using manually assigned IP addresses  
 instead of DHCP, the required changes are:

• **Note**

- Set the Router Address field to XRT's IP Address.
  - Ensure your DNS settings are correct.
- 

## Linux Clients

To access the Internet via XRT, it is only necessary to set XRT as the "Gateway".

**Ensure you are logged in as "root" before attempting any changes.**

### Fixed IP Address

By default, most Unix installations use a fixed IP Address. If you wish to continue using a fixed IP Address, make the following changes to your configuration.

- Set your "Default Gateway" to the IP Address of XRT.
- Ensure your DNS (Name server) settings are correct.

### To act as a DHCP Client (recommended)

The procedure below may vary according to your version of Linux and X -windows shell.

1. Start your X Windows client.
2. Select *Control Panel - Network*
3. Select the "Interface" entry for your Network card. Normally, this will be called "eth0".
4. Click the *Edit* button, set the "protocol" to "DHCP", and save this data.
5. To apply your changes
  - Use the "Deactivate" and "Activate" buttons, if available.
  - OR, restart your system.

## Chapter 3

# Machine Configurations

# 3

*This Chapter provides Setup details of XRT.*

## Overview

This chapter describes the setup procedure for:

- Internet Access
- LAN configuration

PCs on your local LAN may also require configuration. For details, see

Other configuration may also be required, depending on which features and functions of XRT you wish to use. Use the table below to locate detailed instructions for the required functions.

To Do this:	Refer to:
Configure PCs on your LAN.	Chapter 2: Preparations & Installation
Check machine operation and Status.	Chapter 4: Operation and Status
Use any of the following Internet features: <ul style="list-style-type: none"><li>• Special Applications, DMZ</li><li>• Dynamic DNS</li><li>• Virtual Servers</li></ul>	Chapter 3: Machine Configurations

### Note

Where use of a certain feature requires that PCs or other LAN devices be configured, this is also explained in the relevant chapter.

## Configuration Program

PLANET XRT C series routers integrate an HTTP server. This enables you to connect to it, and start configuration via standard Web Browser. Your Browser must have JavaScript support. The web UI in XRT has been tested on the following browsers:

- Netscape V4.08 or later
- Internet Explorer V4 or later

## Preparation

Before attempting to configure your router, please ensure that:

- Your PC can establish a physical connection to the Broadband Router. The PC and the Broadband Router must be directly connected (using the switch ports on the router) or on the same LAN segment.
- Your router must be installed and powered ON.

- If your router's default IP Address (192.168.0.1) is already used by another device, the other device must be turned OFF until router is allocated a new IP Address during configuration.

### Using UPnP (XRT-401C)

If your Windows system supports UPnP, after proper UPnP service configuration. When you connect your computer with XRT-401C, an icon for XRT-401C will appear in the system tray, notifying you that a new network device has been found, and offering configurations in *My Network Places* to the newly-discovered device.

- Unless you intend to change the IP Address of XRT-401C, you can accept the desktop shortcut.
- Whether you accept the desktop shortcut or not, you can always find UPnP devices in *My Network Places* (previously called *Network Neighborhood*).
- Double - click the icon for XRT-401C to start the configuration. Refer to the following section for details of the initial Internet connection configuration process.

### Using your Web Browser

To establish a connection from your PC to XRT:

1. After installing XRT in your LAN, start your PC. If your PC is already running, restart it.
2. Start your WEB browser.
3. In the *Address* box, enter "HTTP://" and the IP Address of XRT, as in this example, which uses XRT's default IP Address:

[HTTP://192.168.0.1](http://192.168.0.1)

#### If you can't connect

If your router does not respond, check the following:

- XRT is properly installed, LAN connection is OK, and it is powered ON. You can test the connection by using the "Ping" command:
  - Open the MS-DOS window or command prompt window.
  - Enter the command:  

```
ping 192.168.0.1
```

If no response is received, either the connection is not working, or your PC's IP address is not compatible with XRT's IP Address. (See next item.)
- If your PC is using a fixed IP Address, its IP Address must be within the range 192.168.0.2 to 192.168.0.254 to be compatible with XRT-401C's default IP Address of 192.168.0.1. Also, the *Network Mask* must be set to 255.255.255.0. See *Chapter 4 - PC Configuration* for details on checking your PC's TCP/IP settings.
- Ensure that your PC and XRT are on the same network segment. (If you don't have a router, this must be the case.)

4. You will be prompted for a username and password, as shown below.



**Figure: Password Dialog**

- Please leave the Password blank (without password).

You may change the logon password in the *General Setting* , using the *Password Settings* screen. (Passwords can contain 0 to 12 alphanumeric characters, and are case sensitive.)

## Quick Setup Wizard

The first time you connect to XRT, click on the Quick Setup Wizard link to start machine configuration. Please:

1. Ensure the Cable/DSL modem is connected and powered ON. Meanwhile, you need the data provided by your ISP.
2. Start the Wizard, follow the screen text and step through it until finished.

### Connection types supported in XRT C series

Type	Details	ISP Data required
Cable Modem	<p>A connection through a cable modem requires minimal configuration. When you set up an account with your Cable provider, the Cable provider and your Broadband router will automatically establish a connection, so you probably do not need to enter anything more.</p> <p>Note for @Home type service user: The IP Address is allocated automatically, but a "Host Name" and "Domain Name" are allocated to you. Sometimes, the ISP will record the MAC (Hardware) address of your PC.</p>	<p>None.</p> <p>Host Name and Domain Name; sometimes the MAC (hardware) address is required to establish the Internet access.</p>
Fixed-IP xDSL	<p>Some xDSL Internet Service Providers may assign a Fixed IP Address for your Broadband router. If you have been provided with this information, choose this option and enter the assigned IP Address, Subnet Mask, Gateway IP Address and DNS IP Address for your Broadband router.</p>	<p>IP address, Subnet Mask, Gateway, and DNS related TCP/IP parameters</p>
PPPoE xDSL	<p>If you connect to the Internet using an xDSL Modem and your ISP has provided you Username/Password and a Service Name, then your ISP uses PPPoE to establish a connection. You must choose this option and enter the required information.</p>	<p>User name and password. (service name is optional, depends on ISP demands.)</p>
PPTP xDSL	<p>If you connect to the Internet using an xDSL Modem and your ISP has provided you with a Password, Local IP Address, Remote IP Address and a Connection ID, then your ISP uses PPTP to establish a connection. You must choose this option and enter the required information.</p>	<p>User name and password.</p> <p>IP Address allocated to you, if Static (Fixed). PPTP Server IP Address.</p>

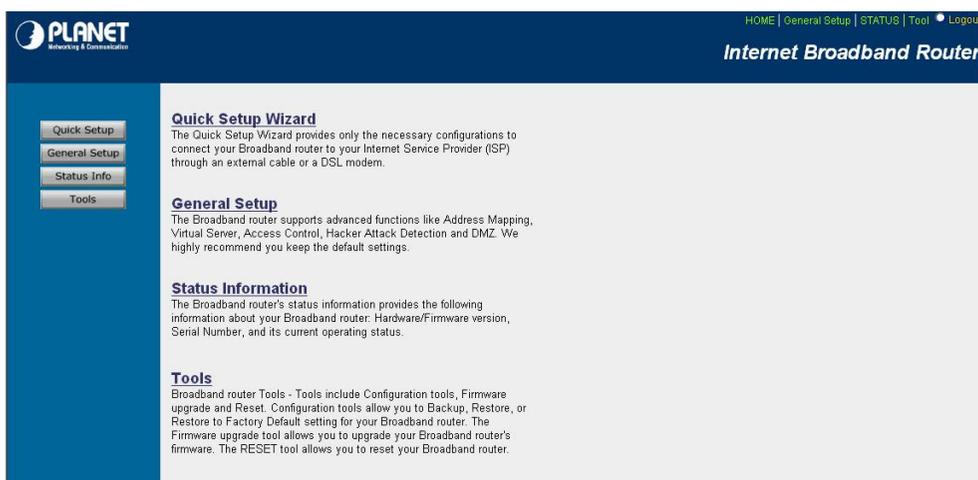
If the connection test fails:

- Please determine proper connection type for your Internet access, and inserting all necessary parameters obtained from your service provider, on the final screen of the Wizard, click **OK** button to finish the Internet access configuration. At this moment, your router will try to use the data provided to establish the Internet connection.
- If the connection fails, please verify if all the parameters are correct, and the physical connections between your computer and the Cable/DSL modem.

If your ISP has recorded your MAC (hardware) address, please go back to Wizard and select Clone MAC Address on the **Cable modem** menu. Change the MAC address to match the value expected by your ISP.

## Main Screen

After logging in XRT, you will see the *Home* screen. When you connect in future, you will see this screen when you connect. An example screen is shown below.



**Figure: Home Screen**

## Navigation & Data Input

- Use the menu bar on the left of the Home screen, and the "Back" button on your Browser, for navigation.
- Changing to another screen without clicking "Save" does NOT save any changes you may have made. You must "Save" before changing screens or your modifications will be ignored.

### Hint

On each configuration page, clicking the



button will display help for that screen. From help screen, you can access the list of all help files (help index).

## Quick Setup Wizard Screen

Click on the Quick Setup Wizard in the HOME page can lead you to establish your Internet connection in the very short time. Related example screens can be shown below:

### Time Zone

The Time Zone allows XRT to allocate its time on the settings configured here, it will affect log display functions such as Security Log and Firewall settings.

Figure: Time Zone Screen

### Parameter Description

<b>Set Time Zone</b>	Select the time zone of the country you are currently in. XRT will set its time based on your selection.
<b>Enable Daylight Saving</b>	The router can also take Daylight savings into account. If you wish to use this function, you must check/tick the enable box to enable your daylight saving configuration (below).
<b>Start Daylight Saving Time</b>	Select the period in which you wish to start daylight Savings Time.
<b>End Daylight Savings Time</b>	Select the period in which you wish to end daylight Savings Time.

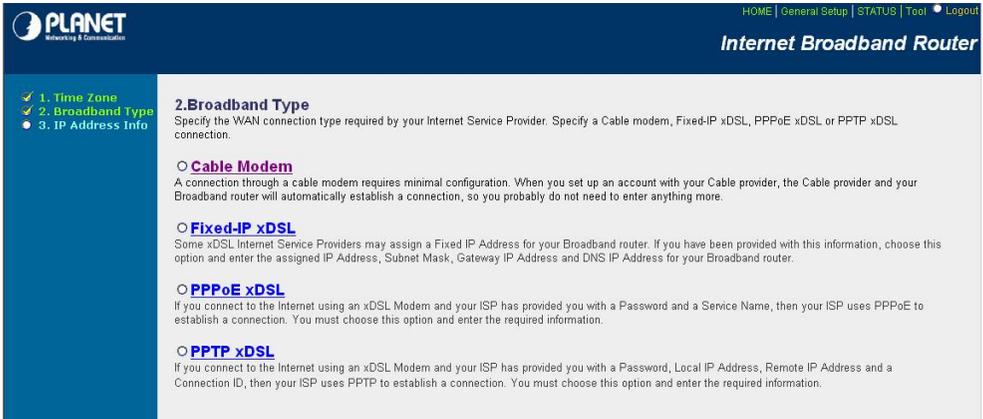
Please click **NEXT** button to proceed to the next page (step 2) **Broadband Type**.

## Broadband Type

In this section you have to select proper types of connections that will be applied on your XRT for Internet access.

### Hint

If you're not sure what kind of connection you have, and different ISP's may require different methods of connecting to the Internet, please contact your ISP for detail and proper information.



The screenshot shows the configuration interface for a Planet Internet Broadband Router. The page title is "Internet Broadband Router". The navigation menu includes "HOME", "General Setup", "STATUS", "Tool", and "Logout". On the left, a sidebar shows a progress indicator with three steps: "1. Time Zone" (checked), "2. Broadband Type" (checked), and "3. IP Address Info" (selected). The main content area is titled "2. Broadband Type" and contains the following text: "Specify the WAN connection type required by your Internet Service Provider. Specify a Cable modem, Fixed-IP xDSL, PPPoE xDSL or PPTP xDSL connection." Below this, there are four radio button options:
 

- Cable Modem**: A connection through a cable modem requires minimal configuration. When you set up an account with your Cable provider, the Cable provider and your Broadband router will automatically establish a connection, so you probably do not need to enter anything more.
- Fixed-IP xDSL**: Some xDSL Internet Service Providers may assign a Fixed IP Address for your Broadband router. If you have been provided with this information, choose this option and enter the assigned IP Address, Subnet Mask, Gateway IP Address and DNS IP Address for your Broadband router.
- PPPoE xDSL**: If you connect to the Internet using an xDSL Modem and your ISP has provided you with a Password and a Service Name, then your ISP uses PPPoE to establish a connection. You must choose this option and enter the required information.
- PPTP xDSL**: If you connect to the Internet using an xDSL Modem and your ISP has provided you with a Password, Local IP Address, Remote IP Address and a Connection ID, then your ISP uses PPTP to establish a connection. You must choose this option and enter the required information.

## Parameter Description

### Cable Modem

A connection through a cable modem requires minimal configuration. When you set up an account with your Cable service provider, the Cable provider and your router will automatically establish a connection, so you probably do not need to enter anything more.

### Fixed-IP xDSL

Some xDSL Internet Service Providers may assign a Fixed IP Address for your Broadband router. If you have been provided with this information, choose this option and enter the assigned IP Address, Subnet Mask, Gateway IP Address and DNS IP Address for your Broadband router.

### PPPoE

If you connect to the Internet using an xDSL Modem and your ISP has provided you with a Password and a Service Name, then your ISP uses PPPoE to establish a connection. Please choose this option and enter the required information.

### PPTP

If you connect to the Internet using an xDSL Modem and your ISP has provided you with a Password, Local IP Address, Remote IP Address and a Connection ID, then your ISP uses PPTP to establish a connection. Please choose this option and enter the required information.

Please choose the proper WAN connection type and then proceed to relevant sub-section in following pages.

## Cable Modem

Choose Cable Modem if your ISP will automatically give you an IP address. Some ISP's may also require that you fill in additional information such as Host Name and MAC address to establish Internet connection.

### Note

Please do not modify the MAC address field unless there is demand from your ISP for Internet access, and prevent network conflict.

## Parameter Description

<b>Host Name</b>	If your ISP requires a Host Name, type in the host name provided by your ISP, otherwise leave it blank if your ISP does not require a Host Name.
<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 <b>Clone MAC Address</b> button to work). If necessary, you can use the Release and Renew buttons to release and renew the WAN IP address.

Click <OK> to finish the **Cable modem** configuration. Now, you have completed the configuration for the Cable Modem connection. You can start Internet access now, if you'd like to use the advance features in XRT, please refer to the related chapters in this manual.

### Note

In most circumstances, machine will work well without inputting Host Name and MAC address field in **Cable Modem** settings, please skip this section if your ISP does not require these settings for Internet access.

## Fixed-IP xDSL

Select Fixed-IP xDSL if your ISP has given you a specific IP address for Internet access. Your ISP should provide all the information required in this section.

- ✓ 1. Time Zone
- ✓ 2. Broadband Type
- ✓ 3. IP Address Info

### 3.IP Address Info ?

**Fixed-IP xDSL**

IP	0	0	0	0
Gateway IP	0	0	0	0
DNS	0	0	0	0
Subnet Mask	0	0	0	0

Enter the IP Address, Subnet Mask, Gateway IP Address and DNS IP Address provided to you by your ISP in the appropriate fields.

## Parameter Description

<b>IP</b>	IP address assigned by your ISP
<b>Gateway</b>	Gateway IP address assigned by your ISP
<b>DNS</b>	DNS server IP address
<b>Subnet Mask</b>	Subnet Mask information provided by your ISP

Click **<OK>** to finish the *Fixed-IP DSL* configuration. Now, you have completed the configuration for the Internet connection and you can start Internet access now. If you'd like to use the advance features in XRT, please refer to the related chapters in this manual.

## 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.

- ✓ 1. Time Zone
- ✓ 2. Broadband Type
- ✓ 3. IP Address Info

### 3.IP Address Info ?

**PPPoE**

**Use PPPoE Authentication**

User Name :

Password :

Please retype your password :

Service Name :

MTU :  (144) <= MTU Value <= 1492

Maximum Idle Time :

Auto-reconnect

Enter the User Name and Password required by your ISP in the appropriate fields. If your ISP has provided you with a "Service Name" enter it in the Service Name field, otherwise, leave it blank.

## Parameter Description

<b>Username</b>	Enter the User Name provided by your ISP for the PPPoE connection
<b>Password</b>	Enter the User Name provided by Enter the Password provided by your ISP for the PPPoE connection.
<b>Please re-type your password</b>	Confirm the password you've inserted
<b>Service Name</b>	This field is optional. If your ISP demands for this parameter, enter the Service name here; otherwise leave it blank.
<b>MTU</b>	This field is optional. You can specify the maximum size of your transmission packet to the Internet. Leave it as it is if you to not wish to set a maximum packet size.
<b>Maximum idle time</b>	You can specify an idle time (minutes) for the WAN port. This means if no packets have been sent (no one using the Internet) during this specified period, XRT will automatically disconnect the connection with your ISP.
<b>Auto-reconnect</b>	If you check the Auto-reconnect function, then when the WAN connection is disconnected, XRT will automatically re-connect when there is a request from LAN side to access the Internet.

### Hint

.....  
 If the Max. idle time is set to **zero**, that means there is no time out, e.g. no time restriction (always On) on the Internet connection.  
 .....

Click <OK> to finish the **PPPoE** configuration. Now, you have completed the configuration for the Internet connection. You can start Internet access now, if you'd like to use the advance features in XRT, please refer to the related chapters in this manual.

## 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.

- 1. Time Zone
- 2. Broadband Type
- 3. IP Address Info

### 3.IP Address Info

#### PPTP

IP Address :	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
Subnet Mask :	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
Default Gateway :	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
User ID:	<input type="text"/>
Password:	<input type="text"/>
PPTP Gateway:	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
Idle Time Out:	<input type="text" value="10"/> (min)

## Parameter Description

<b>IP address</b>	IP address given by your ISP to establish the PPTP connection.
<b>Subnet Mask</b>	Enter the Subnet Mask information provided by your ISP.
<b>Gateway</b>	Enter the IP address of the ISP PPTP Gateway.
<b>User ID</b>	Enter the User Name provided by your ISP for the PPTP connection. Sometimes is called Connection ID.
<b>Password</b>	Enter the Password provided by your ISP for the PPTP connection.
<b>PPTP Gateway</b>	If your LAN has a PPTP gateway, then enter that PPTP gateway IP address here. If you do not have a PPTP gateway then enter the ISP's Gateway IP address above.
<b>Idle Time Out</b>	You can specify an idle time (minutes) for the WAN port. This means if no packets have been sent (no one using the Internet) during this specified period, XRT will automatically disconnect the connection with your ISP.

### Hint

-----  
 If the idle time out is set to **zero**, that means there is no time out, e.g. no time restriction (always On) on the Internet connection.  
 -----

Click <OK> to finish the **PPTP** configuration. Now, you have completed the configuration for the Internet connection. You can start Internet access now, if you'd like to use the advance features in XRT, please refer to the related chapters in this manual.

## General Settings

Once you click on the **General Setup** button at XRT's Home Page, you should see the screen below.



**General Setup**

The Broadband router supports advanced functions like Address Mapping, Virtual Server, Access Control, Hacker Attack Detection and DMZ.

We highly recommend you keep the default settings.

If you have already complete Internet access configuration via the **Quick Setup Wizard**, it is NOT needed to configure the same parameters in the **General Setup** screen for you to start using the Internet, except that you have multiple WAN lines and you may configure the WAN connections respectively in the General setting menu.

The **General Setup** menu contains advanced features that allow you to configure XRT to meet your network applications or environment needs such as: Multi-homing, Address Mapping, Virtual Server, Access Control, Intrusion Detection, Special Applications, DMZ and other functions.

Below is the description of the advanced functions available in PLANET XRT C series broadband router.

## Sub-menu Description

---

<b>System</b>	This section allows you to setup XRT's system Time Zone, Password and Remote Management related parameters.
<b>WAN</b>	WAN section allows you to select the connection method in order to establish connections with your ISPs (same as the Quick Setup Wizard section)
<b>NAT</b>	You may configure the Address Mapping, Virtual Server and Special Applications functions in this section. This allows you to specify what user/packet can pass your XRT.
<b>Firewall</b>	Firewall section allows you to configure Access Control, Intrusion Detection and DMZ related functionalities.
<b>DDNS</b>	DDNS section allows you to configure Dynamic DNS related parameters to bring convenience while other Internet users sharing your LAN resources.
<b>PPTP Gateway</b>	If your LAN has a PPTP gateway, then enter that PPTP gateway IP address here. If you do not have a PPTP gateway then enter the ISP's Gateway IP address above.
<b>UPnP (XRT-401C)</b>	UPnP section allows you to turn on/off UPnP function.
<b>QoS (XRT-402C/204C)</b>	QoS section allows you to configure QoS bandwidth control to prioritize the bandwidth for your network.

---

### Note

1. Multiple WAN connections only supported in XRT-402C and XRT-204C.
2. UPnP support only available in XRT-401C.
3. QoS function only supported in XRT-402C and XRT-204C.

Please choose the desired item and start configuration to make XRT optimized to your network applications or environment.

## System Configuration

In this section, you may specify the time zone, XRT system password and assign the remote management user for your broadband router.



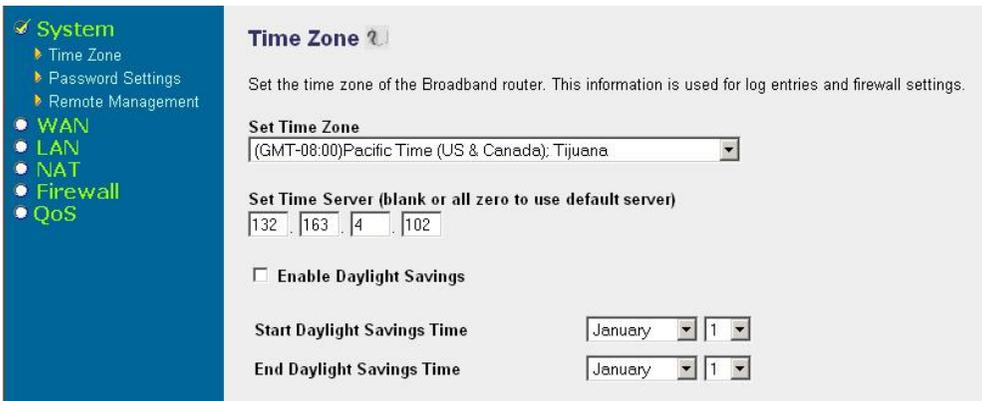
### Sub-menu Description

- Time Zone** Select the time zone of the country you are currently in. XRT will set its time based on your selection.
- Password setting** Allows you to setup the password for logon XRT’s web-based configuration.
- Remote Management** You may specify a Host IP address that can perform remote management functions toward your XRT.

After selecting one of the system settings, please refer to following relevant sub-section for proper configurations.

### Time Zone

The Time Zone allows XRT to allocate its time on the settings configured here, it will affect log display functions such as Security Log and Firewall settings.



## Parameter Description

---

<b>Set Time Zone</b>	Select the time zone of the country you are currently in. XRT will set its time based on your selection.
<b>Enable Daylight Saving</b>	The router can also take Daylight savings into account.
<b>Start Daylight Saving Time</b>	If you wish to use this function, you must check/tick the enable box to enable your daylight saving configuration (below).
<b>End Daylight Savings Time</b>	Select the period in which you wish to start daylight Savings Time.
<b>End Daylight Savings Time</b>	Select the period in which you wish to end daylight Savings Time.

---

Click **Apply** button to save the configurations. You may now continue other configurations or start using your router.

## Password setting

You can change the logon password of your XRT's web-based management. By default, there is no password. So please assign a password to the Administrator as soon as possible, and store it in a safe place.

**System**

- Time Zone
- Password Settings
- Remote Management
- WAN
- LAN
- NAT
- Firewall
- QoS

### Password Settings ?

You can change the password required to log into the broadband router's system web-based management. By default, there is no password. So please assign a password to the Administrator as soon as possible, and store it in a safe place. Passwords can contain 0 to 12 alphanumeric characters, and are case sensitive.

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

**Apply** **Cancel**

### Note

The admin password for XRT web UI can contain 0 to 12 alphanumeric characters, and are case sensitive.

Note: By default there is NO password.

---

## Parameter Description

<b>Current Password</b>	Enter your current password for the remote management administrator to login to your router.
<b>New Password</b>	Assign the new logon password for your router.
<b>Re-Enter Password for Verification</b>	Re-type the password to confirm the new logon password for your router.

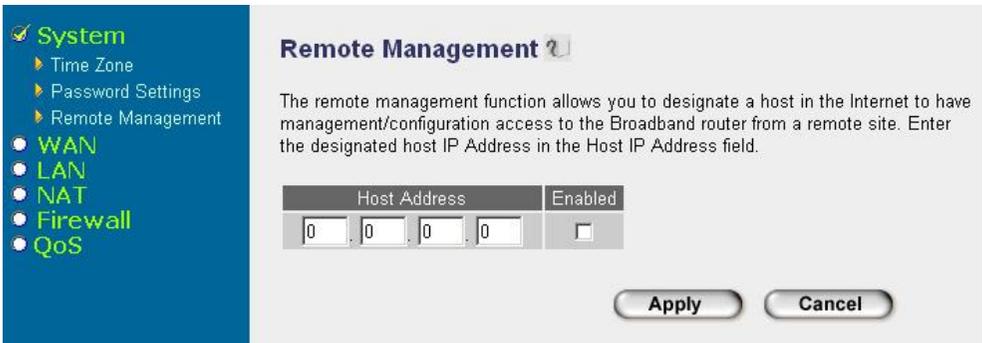
### Note

If the admin password is forgotten, you'll have to reset the router to factory default (No password) with the reset button.

Click **Apply** button to save the configurations. You may now continue other configurations or start using your router.

## Remote Management

The remote management function allows you to specify a host on the Internet to have the remote management privilege on your XRT. Please enter the designated host IP Address in the Host IP Address field.



## Parameter Description

<b>Host Address</b>	This is the IP address of the host in the Internet that will have management/configuration privilege to XRT from a remote site. This means if you are at home and your home IP address has been designated the Remote Management host IP address for this router (located in your company office), then you are able to configure this router from your home.
---------------------	---

### Hint

If the Host Address is left 0.0.0.0 this means anyone can access your XRT's web UI from a remote location.

## Note

When you want to access the web-based management from a remote site, you must enter the router's WAN IP address (e.g. 10.0.0.1) in your web-browser followed by port number 8080, e.g. 10.0.0.1:8080. You'll also need to know the password in order to access XRT's web-based management.

Click **Apply** button to save the configurations. You may now continue other configurations or start using your router.

## WAN Configuration

You may modify the WAN Settings in **WAN** menu if you have already configured the **Quick Setup Wizard** section and you would like to change your Internet connection type.

Or you have XRT-402C/204C, this **WAN** Settings menu also allows you to specify the type of each WAN port connection you want to establish with your ISP. The WAN settings offer the following selections for router's WAN connection, Dynamic IP, PPPoE, PPTP, Static IP Address. You have to select desired WAN port first and please start configuration one at a time.

### XRT-401C WAN Configuration

**System**

**WAN**

- ▶ Dynamic IP
- ▶ PPPoE
- ▶ PPTP
- ▶ Static IP
- ▶ Bridge
- ▶ DNS
- ▶ DDNS

**LAN**

**NAT**

**Firewall**

### WAN Settings

PLANET XRT-401C can be connected to your Service Provider through the following methods:

- Dynamic IP** Obtains an IP Address automatically from your Service Provider.
- PPPoE** PPP over Ethernet is a common connection method used in xDSL connections.
- PPTP** Point-to-Point Protocol is a common connection method used in xDSL connections.
- Static IP Address** Uses a Static IP Address. Your Service Provider gives a Static IP Address to access Internet services.
- Bridge** Bridge packets to LAN.

[More Configuration](#)

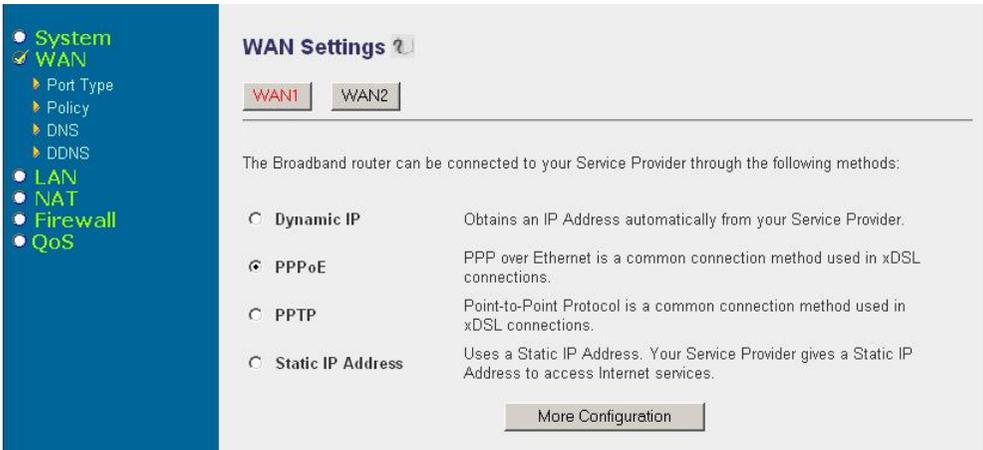
XRT-401C WAN configuration page

## Sub-menu Description

<b>Dynamic IP address</b>	The IP address is dynamically assigned by your ISP.
<b>PPPoE</b>	Broadband connection on your side is a PPPoE connection.
<b>PPTP</b>	Your ISP uses a Point-to-Point Tunneling Protocol (PPTP) connection for Internet access service.
<b>Static IP address</b>	Your ISP has provided fixed IP for Internet access.
<b>Bridge</b>	If this option is enabled on XRT-401C, it can be used as a bridge between LANs.
<b>DNS</b>	You can specify a DNS server you'd like to use.
<b>DDNS</b>	DDNS allows you to map the dynamic IP address to a static domain name. It is required to obtain an account, password and DDNS domain name from the DDNS service providers. DDNS service support in XRT C series are DynDNS and TZO.

Once you have made a selection, click **More Configuration** at the bottom of the screen and refer relevant sub-sections for further configurations.

## XRT-402C/XRT-204C WAN Configuration



XRT-402C WAN configuration page

**System**

- WAN
  - Port Type
  - Policy
  - DNS
  - DDNS
- LAN
- NAT
- Firewall
- QoS

## WAN Settings

WAN1 WAN2 WAN3 WAN4

The Broadband router can be connected to your Service Provider through the following methods:

- Dynamic IP** Obtains an IP Address automatically from your Service Provider.
- PPPoE** PPP over Ethernet is a common connection method used in xDSL connections.
- PPTP** Point-to-Point Protocol is a common connection method used in xDSL connections.
- Static IP Address** Uses a Static IP Address. Your Service Provider gives a Static IP Address to access Internet services.

[More Configuration](#)

### XRT-204C WAN configuration page

## Parameter Description

<b>Port Type</b>	WAN port connection type enabled on your router.
<b>Policy</b>	Specify the interactions between WAN connection interfaces.
<b>DNS</b>	You can specify a DNS server you'd like to use.
<b>DDNS</b>	DDNS allows you to map the dynamic IP address to a static domain name. It is required to obtain an account, password and DDNS domain name from the DDNS service providers. DDNS service support in XRT C series are DynDNS and TZO.

Once you have made a selection, click **More Configuration** at the bottom of the screen and refer relevant sub-sections for further configurations.

## Extended WAN Configuration

### Port Type settings (XRT-402C/XRT-204C)

#### Dynamic IP configuration

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 Host Name, Domain Name and MAC address (Please refer to "**Cable Modem**" section for more detail information.)

#### PPPoE (PPP over Ethernet) configuration

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. (Please refer to "**PPPoE**" section for more detail information.)

## PPTP (Point-to-Point Tunneling Protocol) configuration

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. (Please refer to “**PPTP**” section for more detail information.)

## Static IP Address configuration

Select Static IP address if your ISP has given you a specific IP address for you to use. Your ISP should provide all the information required in this section. (Please refer to “**Fixed IP**” section for more detail information)

## WAN Policy Configuration (XRT-402C/XRT-204C)

When multiple WAN connections are connected with XRT-402C/XRT-204C, you may configure WAN policy for multi-homing feature in XRT-402C/XRT-204C. Each WAN policy can be configured separately. When all WAN interfaces are set as “**Enable (Activated on start)**”, XRT will balance the load between all active WAN connections according to the Send/Receive rate of the WAN ports. You can setup an IP for the router to detect if the WAN line is connected. If the router fails to ping the IP, it would recognize the WAN line as not connected, and will stop directing the Internet traffic to this WAN port. The LAN-to-WAN traffic will be redirected to the other active WAN port. The Intranet users will not become aware of this change and keep surfing the Internet smoothly. You also can setup a WAN port as a backup WAN port. Backup WAN port would not be activated when your router start up. When the other active WAN port fails to connect to the Internet, the backup WAN port will be activated and take over all the traffic.

- System
- **WAN**
- ▶ Port Type
- ▶ Policy
- ▶ DNS
- ▶ DDNS
- LAN
- NAT
- Firewall
- QoS

### WAN Policy ?

You can set the policy of using WAN ports in this page. Traffic load is shared among all active ports automatically. Backup ports are inactive usually and will be activated round-robinly when all other WAN ports fail to take over the works.

**WAN1**

<b>Speed</b>	Send: <input type="text" value="10000"/> Kbps	Receive: <input type="text" value="10000"/> Kbps
<b>Connectivity check</b>	<input type="radio"/> Ping Default Gateway <input checked="" type="radio"/> Ping the IP <input type="text" value="168"/> <input type="text" value="95"/> <input type="text" value="192"/> <input type="text" value="1"/>	
<b>Operation</b>	<input checked="" type="radio"/> Enable (Activated on start) <input type="radio"/> Backup (Activated only when all other ports fail) <input type="radio"/> Disable	

**WAN2**

<b>Speed</b>	Send: <input type="text" value="10000"/> Kbps	Receive: <input type="text" value="10000"/> Kbps
<b>Connectivity check</b>	<input checked="" type="radio"/> Ping Default Gateway <input type="radio"/> Ping the IP <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>	
<b>Operation</b>	<input type="radio"/> Enable (Activated on start) <input type="radio"/> Backup (Activated only when all other ports fail) <input type="radio"/> Disable	

## Parameter Description

<b>Speed</b>	The send/upstream and receive/downstream speed of the WAN interface.
<b>Connectivity check</b>	You can key in an IP address in this field. XRT will ping that IP to verify if the WAN connection is established. You also can select “Ping Default Gateway”, and XRT will check if the WAN line is OK by ping the default gateway of the WAN interface.
<b>Operation</b>	If you select “ <i>Enable</i> ”, the WAN port will be activated when the system boot up. If you select “ <i>Backup</i> ”, the WAN port is disabled on start up. But when all other enabled WAN ports fail, the backup WAN port will be activated and take over all the traffic.

Click **Apply** button to save the configurations. You may now continue other configurations or start using your router.

## DNS configuration

**System**

- WAN
  - Port Type
  - Policy
  - DNS
  - DDNS
- LAN
- NAT
- Firewall
- QoS

### 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.broadbandrouter.com](http://www.broadbandrouter.com), a DNS server will find that name in its index and find the matching IP address. Most ISPs provide a DNS server for speed and convenience. Since your Service Provider may connect you to the Internet through dynamic IP settings, it is likely that the DNS server IP Address is also provided dynamically. However, if there is a DNS server that you would rather use, you need to specify the IP Address of that DNS server. The primary DNS will be used for domain name access first, in case the primary DNS access failures, the secondary DNS will be used.

Has your Internet service provider given you a DNS address?

Domain Name Server (DNS) Address : 0 0 0 0

Secondary DNS Address (optional) : 0 0 0 0

Apply Cancel

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.planet.com.tw](http://www.planet.com.tw), 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.

- System
- ✓ WAN
  - ▶ Port Type
  - ▶ Policy
  - ▶ DNS
  - ▶ DDNS
- LAN
- NAT
- Firewall
- QoS

### 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.broadbandrouter.com, a DNS server will find that name in its index and find the matching IP address. Most ISPs provide a DNS server for speed and convenience. Since your Service Provider may connect you to the Internet through dynamic IP settings, it is likely that the DNS server IP Address is also provided dynamically. However, if there is a DNS server that you would rather use, you need to specify the IP Address of that DNS server. The primary DNS will be used for domain name access first, in case the primary DNS access failures, the secondary DNS will be used.

Has your Internet service provider given you a DNS address?

Domain Name Server (DNS) Address :

Secondary DNS Address (optional) :

## Parameter Description

**Domain Name Server (DNS) Server** This is the ISP’s DNS server IP address that they gave you; or you can specify your own preferred DNS server IP address

**Secondary DNS Address (optional)** This is optional. You can enter another DNS server’s IP address as a backup. The secondary DNS will be used should the above DNS fail.

Click **Apply** button to save the configurations. You may now continue other configurations or start using your router.

## Bridge configuration (XRT-401C)

The bridge mode in XRT-401C enables your machine to work as multi-port bridge and allows you to assign an IP address for management purposes. When the bridge mode is selected, XRT-401C in effect becomes a switch, transferring packets from the WAN port to the LAN port and vice versa without any NAT involvement. In bridge mode, the original WAN MAC is ignored, and the original LAN MAC address will be used as the MAC address. These values will be restored when you set the device to operating modes other than the bridge mode.

- System
- ✓ WAN
  - ▶ Dynamic IP
  - ▶ PPPoE
  - ▶ PPTP
  - ▶ Static IP
  - ▶ Bridge
  - ▶ DNS
  - ▶ DDNS
- LAN
- NAT
- Firewall

### Bridge Mode ?

Enter the assigned IP Address, Subnet Mask for the Bridge Mode management.

Has your network administrator given you an IP Address for this device?

IP address :

Subnet Mask : 255. 255. 255. 0

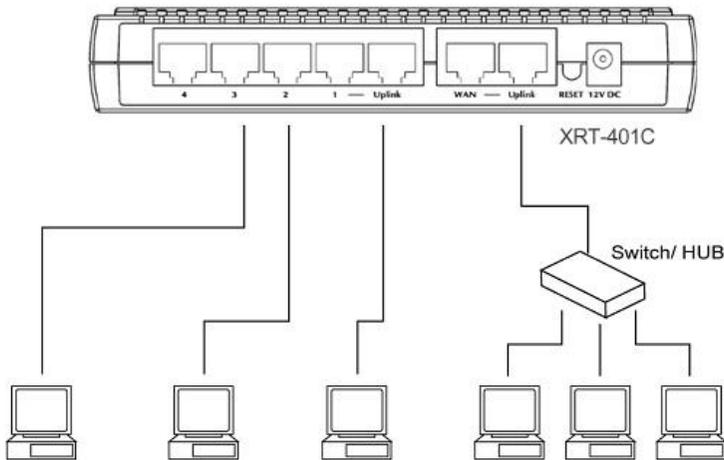
## Parameter Description

**IP address** Enter an IP Address for the Bridge Mode. This IP address allows you to access the web-based management when you decide to switch back to the router mode.

**Subnet Mask** The Subnet Mask for the Bridge Mode management

Click **Apply** button to save the configurations. You may now continue other configurations or start using your router.

The diagram below demonstrates how the Bridge mode can be used in XRT-401C. Your XRT-401C basically turns into a switch allowing you to connect LAN clients to your Local Area Network.



## DDNS Configuration

DDNS service allows you to map the dynamic IP address to a static domain name, which brings convenience to webmasters or network administrators sharing the LAN side resource toward Internet users. To activate the DDNS service in PLANET XRT C series, it is required to obtain an account, password and DDNS domain name from the DDNS service providers. Current DDNS service support in XRT C series are DynDNS and TZO.

- System
- ✓ WAN
  - ▶ Port Type
  - ▶ Policy
  - ▶ DNS
  - ▶ DDNS
- LAN
- NAT
- Firewall
- QoS

### DDNS ?

DDNS allows users 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. Our products have DDNS support for [www.dyndns.org](http://www.dyndns.org) and [www.tzo.com](http://www.tzo.com) now

Dynamic DNS	<input type="radio"/> ENABLE <input checked="" type="radio"/> DISABLE
Provider	<input type="text" value="DynDNS.org"/>
Domain Name	<input type="text"/>
Account / E-mail	<input type="text"/>
Password / Key	<input type="text"/>

## Parameter Description

<b>Enable/Disable</b>	Enable or disable DDNS service in XRT.
<b>Provider</b>	DDNS service provider selection, currently supported: Dyn dns.org, and TZO.com.
<b>Domain name</b>	The DDNS domain name applied from the DDNS service provider.
<b>Account/E-mail</b>	The account that DDNS service provider assigned.
<b>Password/Key</b>	Password or key for updating your DDNS domain name.

Click **Apply** button to save the configurations. You may now continue other configurations or start using your router.

## LAN Configurations

LAN configuration menu in XRT allows you to specify the IP address for your router’s LAN ports for your LAN segment. In the meantime, XRT C series is able to act as DHCP server for DHCP clients in your LAN.

**LAN Settings**

You can enable the Broadband router's DHCP server to dynamically allocate IP Addresses to your LAN client PCs. The broadband router must have an IP Address for the Local Area Network.

**LAN IP**

IP address: 192 168 0 1

IP Subnet Mask: 255.255.255.0

DHCP Server:  Enabled  Disabled

Lease Time: One Week

**IP Address Pool**

Start IP: 192 168 0 100

End IP: 192 168 0 199

Domain Name: \_\_\_\_\_

Apply Cancel

## Parameter Description

---

**LAN IP**

**LAN IP address** XRT's LAN port IP address (Your LAN clients default gateway IP address) **Default LAN IP of XRT: 192.168.0.1**

**IP Subnet Mask** Subnet Mask value for your LAN segment.

**DHCP Server** 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 configure LAN client's IP addresses; make sure the LAN Client is in the same subnet as your router if you want XRT to be your LAN client's default gateway.

**Default DHCP server operation in XRT is turned on.**

**Lease Time** You can specify the time period that the DHCP lends an IP address to your LAN clients in the *Lease Time* field. DHCP server in XRT will issue different IP address for LAN side clients while the DHCP leased time reached.

**IP Address Pool** You can assign an IP address range for DHCP server in XRT to issue IP addresses to for LAN side clients.

**Domain Name** A domain name can be specified in this field for your LAN.

---

Click **Apply** button to save the configurations. You may now continue other configurations or start using your router.

---

**Hint**

You must NOT have two (2) or more DHCP Servers on the same LAN segment. (If your LAN does not have other Routers, this means there must only be one (1) DHCP Server on your LAN.)

---

**Note**

You still can assign Fixed IP Addresses to some devices while using DHCP, however, please provide Fixed IP Addresses **NOT** within the range used by XRT's DHCP Server.

---

**UPnP Configuration (XRT-401C)**

UPnP support in RT-401C can let your UPnP service ready workstation, for example Windows ME, XP or later, easily find your router without rebooting your computers. More than these, UPnP function also can let UPnP enabled applications that using special protocols pass through your XRT-401C smoothly.

**System**

**WAN**

**LAN**

Interface

UPnP

**NAT**

**Firewall**

## UPnP ?

UPnP is more than just a simple extension of the Plug and Play peripheral model. It is designed to support zero-configuration, "invisible" networking, and automatic discovery for a breadth of device categories from a wide range of vendors.

With UPnP, a device can dynamically join a network, obtain an IP address, convey its capabilities, and learn about the presence and capabilities of other devices-all automatically, truly enabling zero configuration networks. Devices can subsequently communicate with each other directly, thereby further enabling peer to peer networking.

UPnP Feature :  ENABLE  DISABLE

Apply Cancel

## Parameter Description

### Enable/Disable

Enable or disable UPnP service in XRT

After enabling the UPnP feature in XRT-401C, all client systems that support UPnP, like Windows XP, can discover this router automatically and access the Internet through XRT without configuration. The NAT Traversal function provided by UPnP can let applications that support UPnP smoothly connect to Internet sites without any incompatibility via the assistance of NAT port translation.

**Default value: UPnP service is enabled.**

Click **Apply** button to save the configurations. You may now continue other configurations or start using your router.

## NAT Configurations

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 Internet applications or sharing your LAN resources such as H.323 VoIP service, web hosting and FTP service.

<ul style="list-style-type: none"> <li>● System</li> <li>● WAN</li> <li>● LAN</li> <li>● <b>NAT</b> <ul style="list-style-type: none"> <li>▶ Address Mapping</li> <li>▶ Virtual Server</li> <li>▶ Special Applications</li> </ul> </li> <li>● Firewall</li> </ul>	<h3>NAT Settings</h3> <p>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 the Web or FTP.</p>
---	--

### Sub-menu Description

<b>Address Mapping</b>	XRT allows one or more Public IP Address(es) to be mapped to a pool of local Private IP Address(es). This feature is particular useful when you have multiple public IP addresses and you'd like to divide local users into different groups.
<b>Virtual Server</b>	Virtual server feature is mostly utilized for sharing your LAN resources toward Internet users. You may assign different LAN side services (e.g. email, FTP, Web etc.) sharing with WAN users. In the meantime, Virtual Server feature in XRT 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 to prevent port conflict while the same service is provided from LAN side.
<b>Special Applications</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.

Please click on one of *NAT* features and refer to following sections for further information.

## Address Mapping

Network Address Translation (NAT) allows IP addresses used in a Local Area Network (LAN) to be mapped to one or more Public IP Addresses used in the public, global Internet. NAT feature eliminates the number of Public IP addresses required from the ISP and also maintains the privacy and security of the Local Area Network. PLANET XRT C series router allows one or more Public IP Address(es) to be mapped to a pool of local Private IP Address(es).

### Address Mapping

Network Address Translation (NAT) allows IP addresses used in a private Local Area Network (LAN) to access the public, global Internet through several WAN ports. This feature limits the number of Public IP addresses required from the ISP and also maintains the privacy and security of the Local Area Network. The Broadband router allows one or more Public IP Address(es) to be mapped to a pool of local Private IP Address(es).

Virtual IPs	WAN 1	WAN 2
1. From 192.168.0. <input type="text" value="0"/> to 192.168.0. <input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>
2. From 192.168.0. <input type="text" value="0"/> to 192.168.0. <input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>
3. From 192.168.0. <input type="text" value="0"/> to 192.168.0. <input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>
4. From 192.168.0. <input type="text" value="0"/> to 192.168.0. <input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>
5. From 192.168.0. <input type="text" value="0"/> to 192.168.0. <input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>
6. From 192.168.0. <input type="text" value="0"/> to 192.168.0. <input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>
7. From 192.168.0. <input type="text" value="0"/> to 192.168.0. <input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>
8. From 192.168.0. <input type="text" value="0"/> to 192.168.0. <input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>
9. From 192.168.0. <input type="text" value="0"/> to 192.168.0. <input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>
10. From 192.168.0. <input type="text" value="0"/> to 192.168.0. <input type="text" value="0"/>	<input type="checkbox"/>	<input type="checkbox"/>

### Parameter Description

#### WAN ports

You may assign WAN ports that each virtual IP range can use to access the Internet. The Public/legal IP addresses of WAN ports that exist in the Internet that will be transformed to one or more private/Virtual IP address (LAN PC clients) e.g. 192.168.0.x. This means that the private IP address(es) selected will use the public IP addresses of designated WAN ports when accessing the Internet

#### Note

You need to give your LAN PC clients a fixed/static IP address for Address Mapping to work properly.

## Virtual Server

- System
- WAN
- LAN
- **NAT**
  - ▶ Address Mapping
  - ▶ Virtual Server
  - ▶ Special Applications
- Firewall
- QoS

### Virtual Server ?

You can configure the Broadband router as a Virtual Server so that remote users accessing services such as the Web or FTP at your local site via Public IP Addresses can be automatically redirected to local servers configured with Private IP Addresses. In other words, depending on the requested service (TCP/UDP) port number, the Broadband router redirects the external service request to the appropriate internal server (located at one of your LAN's Private IP Address).

	Private IP	Private Port	Type	WAN Port	Public Port
1.	192.168.0. <input style="width: 40px;" type="text"/>	<input style="width: 40px;" type="text"/>	TCP / UDP	WAN1	<input style="width: 40px;" type="text"/>
2.	192.168.0. <input style="width: 40px;" type="text"/>	<input style="width: 40px;" type="text"/>	TCP / UDP	WAN1	<input style="width: 40px;" type="text"/>
3.	192.168.0. <input style="width: 40px;" type="text"/>	<input style="width: 40px;" type="text"/>	TCP / UDP	WAN1	<input style="width: 40px;" type="text"/>
4.	192.168.0. <input style="width: 40px;" type="text"/>	<input style="width: 40px;" type="text"/>	TCP / UDP	WAN1	<input style="width: 40px;" type="text"/>
5.	192.168.0. <input style="width: 40px;" type="text"/>	<input style="width: 40px;" type="text"/>	TCP / UDP	WAN1	<input style="width: 40px;" type="text"/>
6.	192.168.0. <input style="width: 40px;" type="text"/>	<input style="width: 40px;" type="text"/>	TCP / UDP	WAN1	<input style="width: 40px;" type="text"/>
7.	192.168.0. <input style="width: 40px;" type="text"/>	<input style="width: 40px;" type="text"/>	TCP / UDP	WAN1	<input style="width: 40px;" type="text"/>

### Parameter Description

<b>Private IP</b>	Please fill the IP address of LAN side server, which shares its resources with Internet users in this field.
<b>Private Port</b>	Service port number of configured on the LAN side server.
<b>Type</b>	Choose the proper port number protocol type (TCP or UDP) for the application on LAN side. If you are unsure, you may leave it to the default TCP protocol.
<b>WAN Port</b>	Select through which WAN port Internet users will access to. The server's mapped public IP would be the public IP of the selected WAN port. ( <b>Note: this item only valid in XRT-402C/204C</b> )
<b>Public Port</b>	Enter the service (service/Internet application) port number from the Internet that will be re-directed to the Private IP address host in your LAN

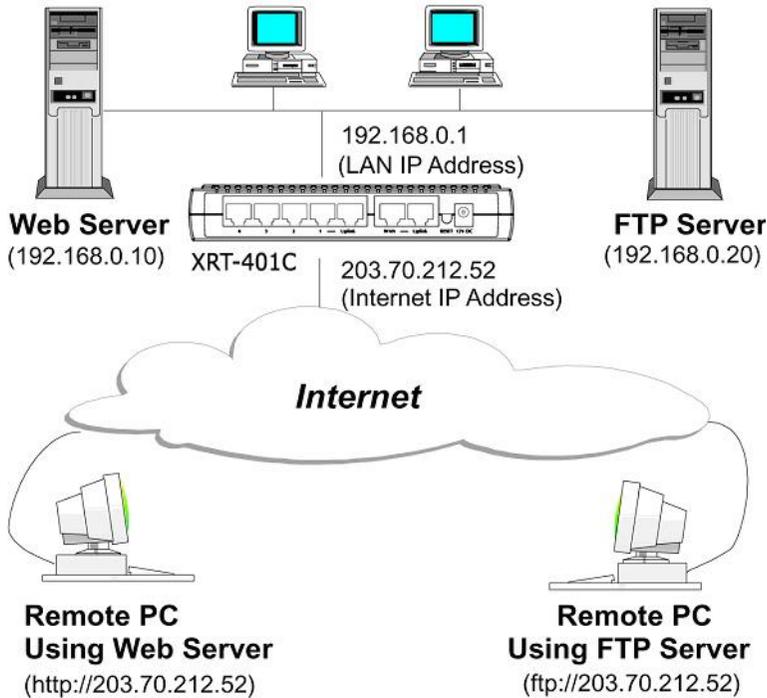
#### Note

You need to give your LAN PC clients a fixed/static IP address for Virtual Server to work properly.

Click **Apply** button to save the configurations. You may now continue other configurations or start using your router.

## Virtual server configuration sample

The diagram below demonstrates usage of Virtual Server function in XRT. Use the Virtual Server when you want the web server located in your private LAN to be accessible to Internet users. The configuration below means that any request coming from the Internet to access your web server will be translated to your LAN's web server (192.168.0.2).



### Note

For the virtual server to work properly Internet/remote users must know your domain name or the public IP address allocated on your machine. (In general cases, you will need to have a public IP address for hosting your website, however, you may enable the DDNS service in XRT to bring convenience to those who wish to build up their own website in dynamic IP address environment.)

## Special Applications

In the Special Applications page, you may configure XRT to support multiple connections to meet the applications on your side.

Some applications demand for multiple communication ports, such as Internet games, video conferencing, and Internet telephony service, these applications cannot work well when Network Address Translation (NAT) service is enabled. To eliminate the inconvenience, you may specify the port normally associated with an application in the "*Trigger Port*" field and choose proper protocol type: TCP or UDP, then enter the public ports associated with the trigger port to open them for inbound traffic in Special Applications menu.

- System
- WAN
- LAN
- ✓ NAT
  - ▶ Address Mapping
  - ▶ Virtual Server
  - ▶ Special Applications
- Firewall

### Special Applications ?

Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications cannot work when Network Address Translation (NAT) is enabled. If you need to run applications that require multiple connections, -specify the port normally associated with an application in the "Trigger Port" field, select the protocol type as TCP or UDP, then enter the public ports associated with the trigger port to open them for inbound traffic. Note: The range of the Trigger Port is 0 to 65535.

	Trigger Port	Trigger Type	Public Port	Public Type	Enabled
1.	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
2.	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
3.	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
4.	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>
5.	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input type="radio"/> TCP <input type="radio"/> UDP	<input type="checkbox"/>

### Parameter Description

<b>Trigger Port</b>	The out going (Outbound) port number for this particular application
<b>Trigger Type</b>	Choose the protocol type of the outbound traffic.
<b>Public Port</b>	Enter the incoming (Inbound) port or port range for the LAN side application (for example, 1000-3000, 30011)
<b>Public Type</b>	Choose the protocol type of the inbound traffic.
<b>Enabled</b>	It is required to check the Enabled box to enable the specified special application configuration
<b>Popular applications</b>	There are pre-defined popular applications lists in machine. To apply the settings, please choose an application from the list, and select a location (1-10) in the <i>Copy to</i> selection box and then click the button to add the application parameter in Special Applications menu.

**Note**

- W** The allowed Trigger Port is from 0 to 65535
  - W** When assigning individual port numbers, symbol comma "," can be used to separate the numbers (for example, 47624, 5190, 6541 etc.).
  - W** When inserting a port range, please use a "dash" to separate the two port number range (e.g. 30000-30100)
  - W** Only single LAN side client can use a particular special application at a time
- 

Click **Apply** button to save the configurations. You may now continue other configurations or start using your router.

**Special Application Configuration sample**

Supposing you'd like to access MSN game zone, and Battle Net for Internet gaming. These applications demand for multiple connections to establish the communications. To achieve this, please logon XRT, and 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 in Special Applications menu.

**Parameters Example:**

<b>ID</b>	<b>Trigger Port</b>	<b>Trigger Type</b>	<b>Public Port</b>	<b>Public Type</b>	<b>Comment</b>
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 XRT will allow incoming packets for ports 2300-2400 and 47624 to be directed to that user.

**Note**

Only single LAN side client can use a special application at a time

---

## Firewall Configurations

PLANET XRT C series provides extensive, scheduled, SPI based firewall protection by restricting connection parameters, thus limiting the risk of hacker attack, and defending against a wide array of common Internet attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server as a Demilitarized Zone (DMZ).

- System
- WAN
- LAN
- NAT
- **Firewall**
  - ▶ Access Control
  - ▶ URL Blocking
  - ▶ Schedule Rule
  - ▶ Intrusion Detection
  - ▶ DMZ
- QoS

### Security Settings (Firewall)

The Broadband router provides extensive firewall protection by restricting connection parameters, thus limiting the risk of hacker attack, and defending against a wide array of common attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server as a Demilitarized Zone (DMZ).

Enable or disable Firewall module function :  Enable  Disable

### Sub-menu Description

<b>Access Control</b>	Access Control allows you to have privileges to determine which LAN side computer/user can or cannot have Internet access or certain Internet applications. You can also control which computer, what services and the time period in which allowed to grant access to these services can be controlled as well.
<b>URL Blocking</b>	URL Blocking allows you to restrict particular websites which can not be accessed by LAN users.
<b>Schedule Rule</b>	You may define name of scheduled firewall or access control rule and activates the schedule to be used in the "Access Control" page.
<b>Intrusion Detection</b>	When the SPI (Stateful Packet Inspection) firewall feature is enabled, traffic pass through XRT will be examined, and abnormal packets will be discarded. Firewall in XRT supports full operation as initiated from the local LAN.
<b>DMZ</b>	If you have a local client PC that cannot run an Internet application properly in the NAT environment, then you may enable DMZ to the client to have unrestricted two-way Internet access. In XRT C series, multiple PCs can be exposed to the Internet for two-way communications e.g. Internet gaming, video conferencing, or VPN connections. To enable DMZ feature, one or more public IP address(es) is required.
<b>QoS (XRT0-402C/204C)</b>	XRT-402C/XRT-204C provides the QoS functionality through which packets can be classified and prioritized. Up to 16 rules can be defined to classify the time-critical traffic for LAN side applications

## Access Control

Access Control in XRT allows you to restrict users from accessing certain Internet applications/services from your LAN. You can apply privilege to LAN side computers based on service type and also make schedule to start the access control of access to these services.

**Access Control**

Access Control allows users to define the traffic type permitted or not permitted in your LAN. You can control which PC client uses what services and also the time period in which they can have access to these services.

- **Enable Filtering Function :**  Yes  No
- **Normal Filtering Table (up to 10 computers)**

Client PC Description	Client PC IP Address	Client Service	Schedule Rule	Configure
<b>No Valid Filtering Rule !!!</b>				

[Add PC](#)

- **MAC Filtering Table (up to 32 computers)**

Rule Number	Client PC MAC Address										
1	<input type="text"/>	:	<input type="text"/>	:	<input type="text"/>	:	<input type="text"/>	:	<input type="text"/>	:	<input type="text"/>
2	<input type="text"/>	:	<input type="text"/>	:	<input type="text"/>	:	<input type="text"/>	:	<input type="text"/>	:	<input type="text"/>

### Parameter Description

**Enable Filtering** Enable (Yes) or disable (No) Access control mechanism in XRT.

**Add PC** You can click *Add PC* link to apply an access control rule to users by IP addresses.

**MAC Filtering Table** Enter the MAC addresses of client PCs that you'd like to restrict Internet access.

Click *Apply* button to save the configurations. You may now continue other configurations or start using your router.

## Access Control extension page – Add PC

**Access Control Add PC**

This page allows users to define service limitation of client PC, including IP address, service type and scheduling rule criteria. For URL blocking function, you need config URL address first in "URL Blocking Site" page. For scheduling function, you also need config schedule rule first in "Schedule Rule" page.

- Client PC Description:
- Client PC IP Address: 192.168.0.  ~
- Client PC Service:
 

Service Name	Detail Description	Blocking
WWW	HTTP, TCP Port 80, 3128, 8000, 8001, 8080	<input type="checkbox"/>
WWW with URL Blocking	HTTP (Ref. URL Blocking Site Page)	<input type="checkbox"/>
E-mail Sending	SMTP, TCP Port 25	<input type="checkbox"/>
News Forums	NNTP, TCP Port 119	<input type="checkbox"/>
E-mail Receiving	POP3, TCP Port 110	<input type="checkbox"/>
Secure HTTP	HTTPS, TCP Port 443	<input type="checkbox"/>
File Transfer	FTP, TCP Port 21	<input type="checkbox"/>
MSN Messenger	TCP Port 1863	<input type="checkbox"/>
Telnet Service	TCP Port 23	<input type="checkbox"/>
AIM	AOL Instant Messenger, TCP Port 5190	<input type="checkbox"/>
NetMeeting	H.323, TCP Port 1720, 1503	<input type="checkbox"/>
DNS	UDP Port 53	<input type="checkbox"/>
SNMP	UDP Port 161, 162	<input type="checkbox"/>
VPN-PPTP	TCP Port 1723	<input type="checkbox"/>
VPN-L2TP	UDP Port 1701	<input type="checkbox"/>
TCP	All TCP Port	<input type="checkbox"/>
UDP	All UDP Port	<input type="checkbox"/>

Protocol:  TCP  UDP

Port Range: - - - - -

Scheduling Rule (Ref. Schedule Rule Page):

## Parameter Description

<b>Client PC Description</b>	Description for access control rule on client PC.
<b>Client PC IP Addresses</b>	Enter the IP address range that you wish to apply the Access Control rule. This is the user's IP address(es) that you wish to setup an Access Control rule. You can select a range of users simply by inputting the starting users' last digit (octet) IP address and the last user's last octet IP address in the appropriate boxes. If you want to select only one user then input the user's last digit IP address in both boxes.
<b>Client PC Service</b>	You can apply limitation on the clients from accessing some Internet services by checking the services you want to block.
<b>Protocol</b>	Select UDP or TCP traffic you'd like to block.
<b>Port Range</b>	You may configure up to five port ranges in Access control. XRT will block clients from accessing Internet services that utilizes these ports for communications.
<b>Scheduling Rule</b>	You may select one of the existing Scheduling Rule and XRT will block Internet access on the clients during schedule.

Click **Apply** button to save the configurations. You may now continue other configurations or start using your router.

## URL Blocking

Disallowed Web Sites and Keywords.

You can block access to certain Web sites from a particular PC by entering either a full URL address or just a keyword of the Web site. To enable URL blocking on a particular PC, please go back to the "**Access Control**" page and check the box of "**Http with URL Blocking**" to the specific computer in the "Normal Filtering Table".

**URL Blocking** ?

**Disallowed Web Sites and Keywords.**

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

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

Rule Number	URL / Keyword	Rule Number	URL / Keyword
Site 1	<input type="text"/>	Site 16	<input type="text"/>
Site 2	<input type="text"/>	Site 17	<input type="text"/>
Site 3	<input type="text"/>	Site 18	<input type="text"/>
Site 4	<input type="text"/>	Site 19	<input type="text"/>
Site 5	<input type="text"/>	Site 20	<input type="text"/>

### Parameter Description

**URL/Keyword**

Enter the keyword or full domain name of the website you'd like to block..

Click **Apply** button to save the configurations. You may now continue other configurations or start using your router.

**i** Hint

If you'd like to like to restrict users to access the website **www.mysite.com**, you should enter either **www.mysite.com** or **mysite** (as a keyword in the URL). If you enter **my** or **site** in the field, all access to websites containing **my** or **site** in their URL names will be blocked.

## Schedule Rule

You may define schedule rule names and activates the schedule for use in the "Access Control" page.

- System
- WAN
- LAN
- NAT
- ✓ Firewall
  - ▶ Access Control
  - ▶ URL Blocking
  - ▶ Schedule Rule
  - ▶ Intrusion Detection
  - ▶ DMZ

### Schedule Rule ?

This page defines schedule rule names and activates the schedule for use in the "Access Control" page.

- **Schedule Rule Table (up to 10 rules)**

Rule Name	Rule Comment	Configure
test	test	<a href="#">Edit</a> <a href="#">Delete</a>

[Add Schedule Rule](#)

## Parameter Description

### Edit

Click *Edit* to modify the time range of the rule schedule.

### Delete

Click *Delete* to delete the schedule rule.

### Add Schedule Rule

Click *Add Schedule Rule* to add a new schedule rule and enter the detail edit page to edit the time range of the schedule rule.

Click *Apply* button to save the configurations. You may now continue other configurations or start using your router.

## Schedule Rule extension – Add/Edit Schedule Rule page

- System
- WAN
- LAN
- NAT
- ✓ Firewall
  - ▶ Access Control
  - ▶ URL Blocking
  - ▶ Schedule Rule
  - ▶ Intrusion Detection
  - ▶ DMZ

### Edit Schedule Rule

Name:

Comment:

Activate Time Period:

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

## Parameter Description

<b>Name</b>	Name of the schedule rule.
<b>Comment</b>	You can enter comment for the schedule rule.
<b>Activate Time Period</b>	You may specify the start time and end time of each day in a week for the schedule rule.

Click **OK** button to save the configurations. You may now continue other configurations or start using your router.

## Intrusion Detection

Firewall mechanism in XRT C series is able to detect malicious attacks from external sources.

You may specify related parameters to prevent hacker attacks, such as, IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan, and TCP SYN flooding.

**Intrusion Detection** ?

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

The firewall can block common hacker attacks, including IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan, and TCP SYN flooding.

- Intrusion Detection Feature**

SPI and Anti-DoS firewall protection	<input checked="" type="checkbox"/>
RIP detect	<input checked="" type="checkbox"/>
Discard Ping to WAN Port	<input type="checkbox"/>
- Stateful Packet Inspection**

Packet Fragmentation	<input checked="" type="checkbox"/>
TCP Connection	<input checked="" type="checkbox"/>
UDP Session	<input checked="" type="checkbox"/>
FTP Service	<input checked="" type="checkbox"/>
H.323 Service	<input checked="" type="checkbox"/>
TFTP Service	<input checked="" type="checkbox"/>
- When hackers attempt to enter your network, we can alert you by e-mail**

E-mail Address	<input type="text"/>
SMTP Server Address	<input type="text"/>
POP3 Server Address	<input type="text"/>
User name	<input type="text"/>
Password	<input type="password"/>
- Connection Policy**

Fragmentation half-open wait:	10	secs
TCP SYN wait:	30	sec.
TCP FIN wait:	5	sec.
TCP connection idle timeout:	3600	sec.
UDP session idle timeout:	30	sec.
H.323 data channel idle timeout:	180	sec.
- DoS Detect Criteria**

Total incomplete TCP/UDP sessions HIGH	300	session
Total incomplete TCP/UDP sessions LOW	250	session
Incomplete TCP/UDP sessions (per min) HIGH	250	session
Incomplete TCP/UDP sessions (per min) LOW	200	session
Maximum incomplete TCP/UDP sessions number to same host	10	session
Incomplete TCP/UDP sessions detect sensitive time period	300	msec.
Maximum half-open fragmentation packet number to same host	30	
Half-open fragmentation detect sensitive time period	10000	msec.
Flooding cracker block time	300	sec.

## Sub-Menu and Parameter Description

---

### **Intrusion Detection Feature**

<b>DoS Protection</b>	Enter the keyword or full domain name of the website
<b>Discard Ping From WAN</b>	Protections from any Denial of Service Attacks
<b>RIP defect</b>	Disable ping response toward WAN interface
	RIP defect attack prevention

### **Stateful Packet Inspection**

If SPI feature is enabled, all incoming packets will be examined to prevent malicious attacks from external sources.

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

<b>Email Address</b>	Email address that you would like the alert warning to be sent to while attacks occurred.
<b>SMTP Server Address</b>	IP address of the SMTP server
<b>POP3 Server Address</b>	IP address of the POP3 server
<b>Username</b>	User Name of the POP3 server
<b>Password</b>	Password of the POP3 server

### **Connection Policy**

Configure waiting and idle timeout of session states. All timeout sessions will be removed to prevent from DoS attacks.

### **DoS Detect Criteria**

The criteria of each kind of abnormal events. Any abnormal event that happens more often than the allowed criteria will be treated as DoS attack and XRT will record this event in the security log and alert you via e-mail.

---

Click ***Apply*** button to save the configurations. You may now continue other configurations or start using your router.

## DMZ Configurations

DMZ (DeMilitarized Zone) feature will allow un-restricted bi-directional traffic passed through XRT, this will bring great convenience while configuring Internet applications that have difficulties running behind firewall or NAT environment. Difference between 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 service types) from the WAN IP to a specific LAN side client/server.

- System
- WAN
- LAN
- NAT
- **Firewall**
  - ▶ Access Control
  - ▶ URL Blocking
  - ▶ Schedule Rule
  - ▶ Intrusion Detection
  - ▶ DMZ
- QoS

### DMZ(Demilitarized Zone) ?

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

**Enable DMZ:**  Yes  No

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

Public IP Address	Client PC IP Address
1. DNS-Looked-up WAN (0.0.0.0)	192.168.0. <input style="width: 30px;" type="text"/>
2. <input style="width: 30px;" type="text"/> . <input style="width: 30px;" type="text"/> . <input style="width: 30px;" type="text"/> . <input style="width: 30px;" type="text"/>	192.168.0. <input style="width: 30px;" type="text"/>
3. <input style="width: 30px;" type="text"/> . <input style="width: 30px;" type="text"/> . <input style="width: 30px;" type="text"/> . <input style="width: 30px;" type="text"/>	192.168.0. <input style="width: 30px;" type="text"/>
4. <input style="width: 30px;" type="text"/> . <input style="width: 30px;" type="text"/> . <input style="width: 30px;" type="text"/> . <input style="width: 30px;" type="text"/>	192.168.0. <input style="width: 30px;" type="text"/>
5. <input style="width: 30px;" type="text"/> . <input style="width: 30px;" type="text"/> . <input style="width: 30px;" type="text"/> . <input style="width: 30px;" type="text"/>	192.168.0. <input style="width: 30px;" type="text"/>
6. <input style="width: 30px;" type="text"/> . <input style="width: 30px;" type="text"/> . <input style="width: 30px;" type="text"/> . <input style="width: 30px;" type="text"/>	192.168.0. <input style="width: 30px;" type="text"/>
7. <input style="width: 30px;" type="text"/> . <input style="width: 30px;" type="text"/> . <input style="width: 30px;" type="text"/> . <input style="width: 30px;" type="text"/>	192.168.0. <input style="width: 30px;" type="text"/>
8. <input style="width: 30px;" type="text"/> . <input style="width: 30px;" type="text"/> . <input style="width: 30px;" type="text"/> . <input style="width: 30px;" type="text"/>	192.168.0. <input style="width: 30px;" type="text"/>

### Parameter Description

<b>Enable DMZ</b>	Enable or Disable DMZ feature in XRT.
<b>Public IP Address</b>	IP address of the WAN interface or other Public IP addresses given by your ISP
<b>Client PC IP Address</b>	Insert the IP address of the specific LAN side computer that will be associated with the DMZ feature.

Click **Apply** button to save the configurations. You may now continue other configurations or start using your router.

---

**Note** If there is a port conflict between the Virtual Server and the DMZ configurations, Virtual Server function will have higher priority than the DMZ function.

---



---

**Hint** It is required to assign LAN side computer(s) to have a fixed/static IP address while enabling DMZ feature.

---

## QoS Configurations (XRT-402C/XRT-204C)

QoS feature in XRT-402C/204C can let you classify packets by source/destination IP, MAC address, port number and type of service. Network traffic that matches with the QoS rules can have higher priority than other packets to be passed through while the WAN connection is loaded. QoS feature can bring you better experiences of using real time services like Internet telephony service, video conference ...etc.

**QoS**

The bandwidth gap between LAN and the outbound access link can significantly degrade performance of critical network applications especially when the access link is congested. This router provides the QoS facility through which packets can be classified, rate-shaped, and prioritized. Up to 16 rules can be defined to classify user's critical applications.

Enable QoS Function :  Yes  No

Rule Name	Local Addr	Remote Addr	Traffic Type	Configure
H323_VoIP	WILDCARD	WILDCARD	H.323 VoIP	<a href="#">Edit</a> <a href="#">Delete</a>

[Add critical class](#)

**Apply** **Cancel**

### Sub-Menu and Parameter Description

<b>Enable QoS Function</b>	Enable or Disable QoS feature in XRT.
<b>Edit</b>	Click Edit to modify the QoS rule.
<b>Delete</b>	Click Delete to delete the QoS rule
<b>Add critical class</b>	Click “Add critical class” to add a new QoS rule.

Click **Apply** button to save the configurations. You may now continue the extended QoS configurations or start using your router.

### Extended QoS configurations - QoS Edit Rule

The QoS Edit Rule page is for user to specify QoS rules to classify network packets. Rules can be defined by the combination of MAC address, IP addresses, service types, and port numbers.

- System
- WAN
- LAN
- NAT
- Firewall
- ✓ QoS

### QoS Edit Rule

This page is for user to specify rules to classify packets. Rules can be defined by the combination of MAC address, IP addresses, service types, and port numbers.

- Rule Name:
- Local Address : MAC addr ▾  
 :  :  :  :  :  or  
 :  :  :  :
- Remote Address : IP range ▾  
 .  .  .  ~
- Traffic Type : CUSTOMIZED SERVICE ▾
- Protocol : TCP ▾  
 Local Port :  ~  ,  ~  ,  ~  ,  ~  ,  ~   
 Remote Port :  ~  ,  ~  ,  ~  ,  ~  ,  ~
- DiffServ Type : Best Effort ▾

## Parameter Description

<b>Rule Name</b>	Name of the QoS rule
<b>Source Address</b>	You may define the source address of packet here. If “ <i>MAC address</i> ” is selected, you may define up to five source MAC addresses in this rule. If “ <i>IP range</i> ” is selected, you may define source IP address range. You also can select “ <i>WILDCARD</i> ” to let any source address matches this part of the QoS rule.
<b>Destination Address</b>	You may define the destination address of packet here. If “ <i>MAC address</i> ” is selected, you can define up to five destination MAC addresses. If “ <i>IP range</i> ” is selected, you can define one destination IP address range. You also can select “ <i>WILDCARD</i> ” to let any destination address matches this part of the rule.
<b>Traffic Type</b>	You may specify the traffic types such as, FTP, SMTP ...etc. Meanwhile, you can select “ <i>CUSTOMIZED SERVICE</i> ” to define your own service type by protocol, source port and destination port as well.
<b>Protocol</b>	If you select “ <i>IP</i> ” protocol in this field, XRT will check the packets by IP information, like source address, destination address ...etc. If “ <i>TCP</i> ” or “ <i>UDP</i> ” is selected, the QoS rule will not only apply to network packets by IP information, but also session layer information, like source port and destination port. You may enter several ranges for source and destination port for XRT to check with.
<b>DiffServ Type</b>	You can select one of the DiffServ type to match or select “ <i>WILDCARD</i> ” to match all DiffServ types.

Click **Apply** button to add the QoS rules into machine. You may now continue other configurations or start using your router.

*This Chapter details the operation of XRT and the status screens.*

## Operation

**Once both XRT and the PCs are configured, operation is automatic.**

However, there are some situations where additional Internet configuration may be required:

- If using Internet-based *Communication Applications*, it may be necessary to specify which PC receives an incoming connection. Please refer to *Virtual server*, *Special Application*, and *DMZ* related sections for further details.
- Applications that use non-standard connections or port numbers may be blocked by XRT's built-in firewall. You can define such applications as *Special Applications* to allow them to function normally. You may refer to *Special Application* section for further details.
- Some non-standard applications may require use of the *DMZ* feature. You may refer to *DMZ* section for further details.

## Status Screen

The Status section allows you to monitor the machine status of your XRT. You can use the Status page to monitor: WAN/LAN interfaces connection status, current firmware and hardware version information, system operation logs, illegal activities toward your network, and information on DHCP clients connected to your XRT.

### Sub-Menu and Parameter Description

---

<b>Status and Information</b>	Displays XRT's system information (MAC address, Firmware version, etc.)
<b>Internet Connection</b>	Display your XRT current Internet connection status and other related information.
<b>Device Status</b>	Displays XRT's current IP address, DHCP, Firewall setting status
<b>Security Log</b>	Displays machine system wide information, and illegal attempts or hack activities toward your network.
<b>DHCP PC Client Log</b>	Displays XRT DHCP client's information

---

Please select one of the *Status* selections and proceed to relevant sub-section for further information.

## Status and Information

You may check machine status in the status and information menu.

The screenshot shows the 'Status and Information' page. On the left is a blue sidebar with a 'Status' menu containing: Internet Connection, Device Status, Security Log, and DHCP Client Log. The main content area is titled 'Status and Information' and includes a help icon. Below the title is a paragraph explaining that the page monitors connection status, WAN/LAN interfaces, firmware/hardware versions, and DHCP client information. Under the heading 'INFORMATION', the following details are listed:

- LAN MAC Address: 00-30-4F-25-A5-50
- WAN MAC Address: 00-30-4F-25-A5-51
- Hardware Model: XRT-402C
- Hardware Version: 002
- Boot Code Version: V1.05
- Runtime Code Version: 0.96M2WD (Feb 21 2003 10:05:05)

## Parameter Description

### Information

XRT's system information such as: LAN/WAN MAC Address, Hardware version, firmware version information will be displayed here.

Please select other selections in *Status* menu and proceed to relevant sub-section for further information.

## Internet Connection

In the Internet connection menu, you may check XRT current Internet connection information.

The screenshot shows the 'Internet Connection' page. The left sidebar has the 'Status' menu with 'Internet Connection' selected. The main content area is titled 'Internet Connection' and includes a help icon. Below the title is the instruction: 'View the current internet connection status and related information'. A table displays the connection status:

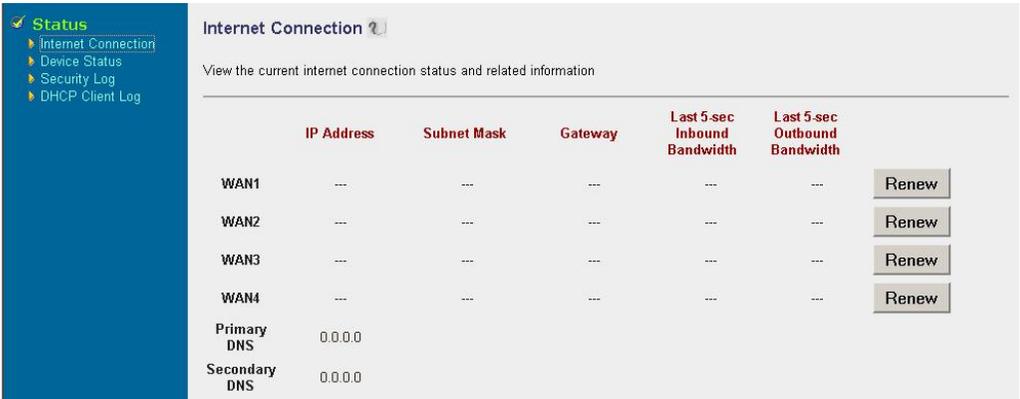
Cable/DSL:	DISCONNECTED
WAN IP:	N.A.
Subnet Mask:	N.A.
Gateway:	N.A.
Primary DNS:	N.A.
Secondary DNS:	N.A.

To the right of the table are two buttons: 'Release' and 'Renew'.

XRT-401C Internet connection screen



XRT-402C Internet connection screen



XRT-204C Internet connection screen

## Parameter Description

**Internet Connection** This page displays connection status of XRT’s WAN interface: WAN IP address, Subnet Mask, and ISP Gateway as well as the Primary DNS and Secondary DNS being used.

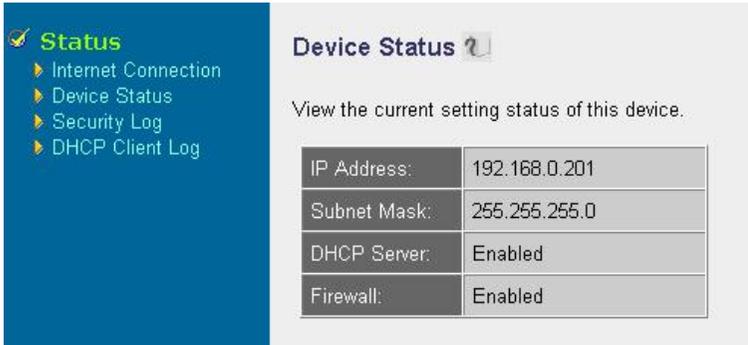
### Note

When the WAN connection is a Dynamic IP connection, the **Release** and **Renew** button can be used to release machine’s WAN IP address and renew to obtain IP address from the DHCP server. If the WAN port uses PPPoE, **Disconnect** button will tear down current PPP session, and **Connect** button will re-initialize a PPP session.

Please select other selections in **Status** menu and proceed to relevant sub-section for further information.

## Device Status

Device status menu displays machine configuration settings you've done in the *Quick Setup Wizard/General Setup* sections.



## Parameter Description

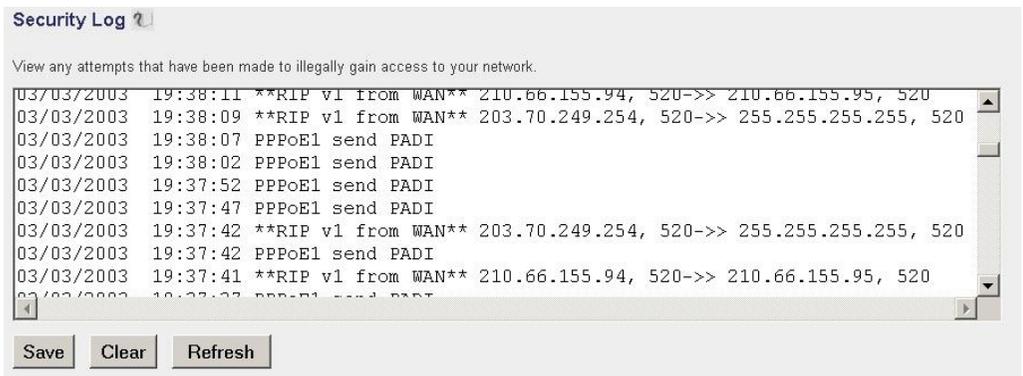
**Device Status** This page displays running configurations in XRT. LAN port **IP Address** and **Subnet Mask**, **DHCP Server** and **Firewall** functions enabled/disabled information will be displayed.

**Note** The firewall status is shown enabled if the firewall is enabled (regardless of whether you've configured any of the firewall features)

Please select other selections in *Status* menu and proceed to relevant sub-section for further information.

## Security Log

Security log displays machine system wide information, and illegal attempts or hack activities toward your network.



## Parameter Description

### Device Status

The security log page displays current security log of XRT. It records the system wide activities, and illegal attempts to access your network.

At the bottom of the page, there are three function buttons: Click **Save** button to save the logged messages a local file for further processing. Click **Clear** button to clear the logged messages, and click on the **Refresh** button to get the most updated log information.

### Note

When your turn off XRT, the security log will disappear if not saved to a local file.

Please select other selections in **Status** menu and proceed to relevant sub-section for further information.

## DHCP Client Log

Displays XRT DHCP client's information

DHCP Client Log View your LAN client's information that are currently linked to the XRT-401C's DHCP server.

Numbers of DHCP Clients: 0

Refresh

## Parameter Description

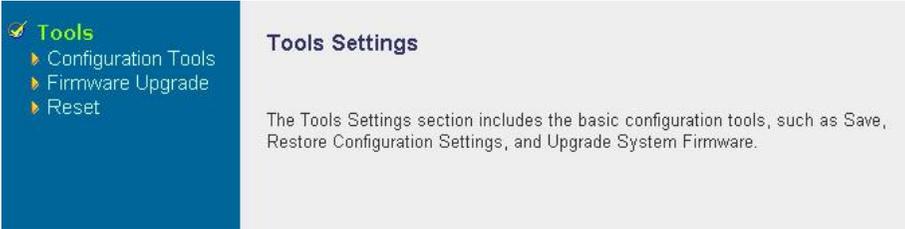
### DHCP Client Log

This page displays DHCP clients (LAN PCs) currently connected to your XRT. Number of DHCP Clients displays the number of LAN clients that are currently linked to XRT's DHCP server. The DHCP Client Log displays the IP address and the MAC address of each LAN Client. You may use the **Refresh** button to get the most updated information.

Please select other selections in **Status** menu and proceed to relevant sub-section for further information.

## System Tools

The **Tools** page contains several convenient utilities for you to save or restore configuration settings (**Configuration Tools**), to upgrade machine firmware (**Firmware Upgrade**) and to reboot machine (**Reset**).



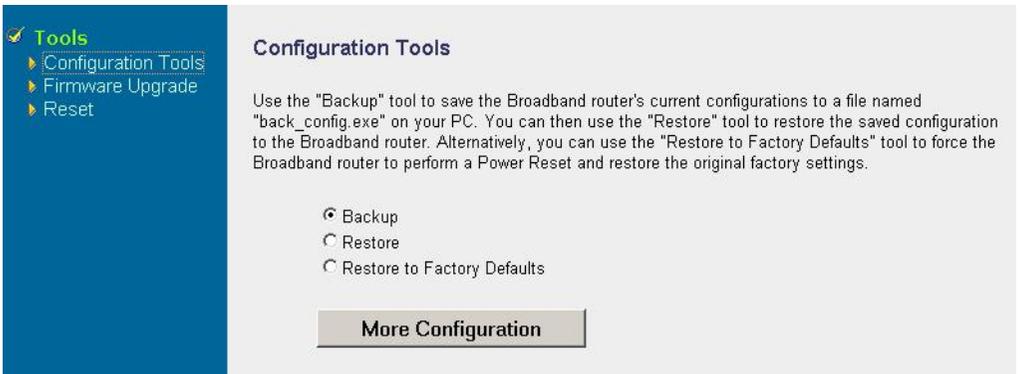
### Sub-Menu and Parameter Description

<b>Configuration Tools</b>	You may backup the machine running configuration, restore configuration files or restore machine factory default settings in this menu.
<b>Firmware Upgrade</b>	Firmware upgrade page will allow you to upgrade machine's firmware
<b>Reset</b>	You may reboot machine in the reset page.

Please select one of the **Tools** selections and proceed to relevant sub-section for further information.

## Configuration Tools

The Configuration Tools screen allows you to save (**Backup**) the machine running configurations to bring you protection and convenience while improper configurations occur, you might need to reset machine to factory default as well. When saving the configuration setting (**Backup**), you may re-load the configuration through the **Restore** selection at a latter time. If extreme problems occurred in machine, you can use the **Restore to Factory Defaults** function to erase all existing configurations and restore the original default settings into machine.



### Parameter Description

**Configuration Tools**

Use the "**Backup**" tool to save current configuration to a file. You can then use the "**Restore**" tool to restore saved configuration into machine. Alternatively, you can use the "**Restore to Factory Defaults**" tool to erase all existing configurations and restore the original default settings into machine.

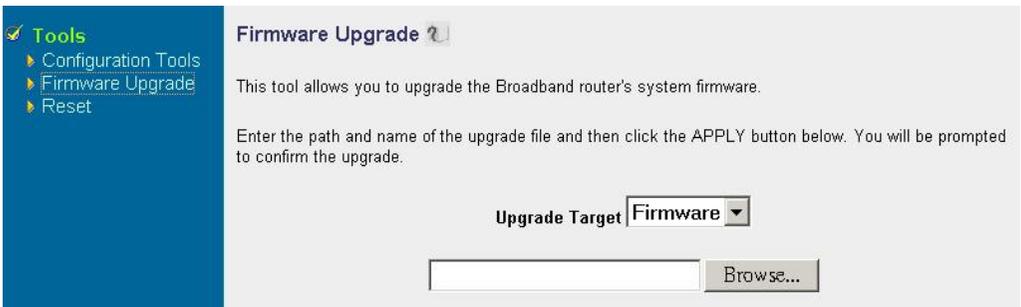
**Note**

Click **More Configuration** button, after making a selection and follow the screen text to complete the configurations.

Please select one of the selections and proceed to relevant sub-section for further information.

**Firmware Upgrade**

While download or receiving maintenance firmware from local distributor or from our server, you may proceed firmware upgrade in this page.



**Parameter Description**

**Firmware Upgrade**

This tool page allows you to upgrade XRT’s firmware. To upgrade the firmware of your router, you need to download the firmware file to your local hard disk, and enter proper file name and path in the appropriate field on this page. You can also use the **Browse** button to allocate the firmware file on your PC.

Once the new firmware file is selected, click **Apply** at the bottom of the screen to start the upgrade process. (You may have to wait a few minutes for the upgrade to complete). Once the upgrade is complete you can start using your router.

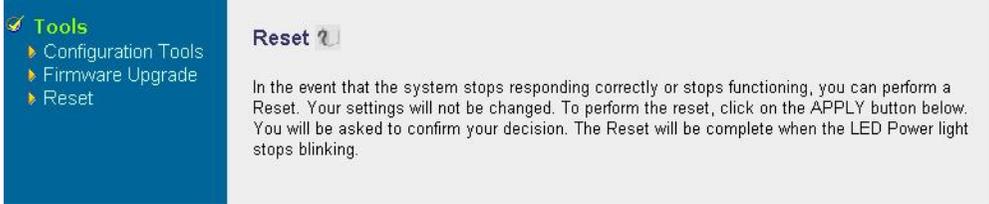
**Note**

1. It is suggested to read the firmware release note to determine if the firmware is suitable for your machine, and in most cases, there is no need to perform firmware upgrade if machine operates smoothly.
2. Be sure to keep the power supply stable before starting firmware upgrade. If there is a power interruption during firmware upgrade, there could be unrecoverable

Please follow the screen text to complete firmware upgrade.

## Reset

In the event that the system stops responding correctly or stops functioning, you can perform a Reset. You may restart your machine in this **Reset** tool page. The reset function is essentially rebooting your router.



**Tools**

- ▶ Configuration Tools
- ▶ Firmware Upgrade
- ▶ Reset

### Reset ?

In the event that the system stops responding correctly or stops functioning, you can perform a Reset. Your settings will not be changed. To perform the reset, click on the **APPLY** button below. You will be asked to confirm your decision. The Reset will be complete when the LED Power light stops blinking.

## Parameter Description

### Reset

---

In the event that the system stops responding correctly or in some way stops functioning, you can perform a reset to reboot machine, and settings on machine will not be changed. To perform the reset, click on the **APPLY** button. You will be asked to confirm your decision. Reboot process will be complete when the machine power light stops blinking. Once the reset process is done, you may start using your router again.

---

### Note

---

During machine reboot, all Internet connections will be torn down, please double confirm the reset to prevent accidentally disconnect an important session.

---

# Appendix A

## Troubleshooting



*This Appendix covers the most likely problems and their solutions.*

### Overview

This chapter covers some common problems that may be encountered while using XRT-401C and some possible solutions to them. If you follow the suggested steps and XRT-401C still does not function properly, contact your dealer for further advice.

### General Problems

**Problem 1:** Can't connect to XRT to configure it.

**Solution 1:** Check the following:

- XRT is properly installed, LAN connections are OK, and it is powered ON.
- Ensure that your PC and XRT are on the same network segment. (If you don't have a router, this must be the case.)
- If your PC is set to "Obtain an IP Address automatically" (DHCP client), restart it.
- If your PC uses a Fixed (Static) IP address, ensure that it is using an IP Address within the range 192.168.0.2 to 192.168.0.254 and thus compatible with XRT's default IP Address of 192.168.0.1. Also, the Network Mask should be set to 255.255.255.0 to match XRT. In Windows, you can check these settings by using *Control Panel-Network* to check the *Properties* for the TCP/IP protocol.

### Internet Access

**Problem 1:** When I enter a URL or IP address I get a time out error.

**Solution 1:** A number of things could be causing this. Try the following troubleshooting steps.

- Check if other PCs work. If they do, ensure that your PCs IP settings are correct. If using a Fixed (Static) IP Address, check the Network Mask, Default gateway and DNS as well as the IP Address.
- If the PCs are configured correctly, but still not working, check XRT. Ensure that it is connected and ON. Connect to it and check its settings. (If you can't connect to it, check the LAN and power connections.)
- If XRT is configured correctly, check your Internet connection (DSL/Cable modem etc) to see that it is working correctly.

**Problem 2:** Some applications do not run properly when using XRT-401C.

**Solution 2:** XRT-401C processes the data passing through it, so it is not transparent.

Use the *Special Applications* feature to allow the use of Internet applications, which do not function correctly.

If this does solve the problem you can use the *DMZ* function. This should work with almost every application, but:

- It is a security risk, since the firewall is disabled.

## Glossary

**Bridge:** A bridge is an intelligent, internetworking device that forwards or filters packets between different networks based on data link layer (MAC) address information.

**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).

**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 “.”: bbbbbb.bbbbbb.bbbbbb.bbbbbb, 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 the broadband router'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:

<b>Application</b>	<b>Protocol</b>	<b>Port Number</b>
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.

# Appendix B

## Specifications



### XRT C series Specifications

Model	XRT-401C	XRT-402C	XRT-204C
Dimensions (mm)	167 (W) x 80 (D) x 25 (H)		
Operating Temperature	0° C to 50° C		
Storage Temperature	-10° C to 70° C		
Network Protocol:	TCP/IP, NAT, DHCP, HTTP, DNS, PAP, CHAP, TFTP		
Network Interface: LAN	4 * RJ-45	4 * RJ-45	2 * RJ-45
Network Interface: WAN	1 * RJ-45	2 * RJ-45	4 * RJ-45
LEDs	10	12	
Power Adapter	12 V DC External		

### FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

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

To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. (Example - use only shielded interface cables when connecting to computer or peripheral devices).

## **FCC Radiation Exposure Statement**

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

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

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

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

## **CE Marking Warning**

This is a Class B product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.