

# P-660RU-Tx

ADSL2+ Ethernet/USB Router

## User's Guide



### Default Login Details

|            |                    |
|------------|--------------------|
| IP Address | http://192.168.1.1 |
| User Name  | admin              |
| Password   | 1234               |

Firmware Version 1.0  
Edition 1, 01/2010

[www.zyxel.com](http://www.zyxel.com)

# ZyXEL



# About This User's Guide

## Intended Audience

This manual is intended for people who want to configure the P-660RU-Tx using the web configurator.

## Tips for Reading User's Guides On-Screen

When reading a ZyXEL User's Guide On-Screen, keep the following in mind:

- If you don't already have the latest version of Adobe Reader, you can download it from <http://www.adobe.com>.
- Use the PDF's bookmarks to quickly navigate to the areas that interest you. Adobe Reader's bookmarks pane opens by default in all ZyXEL User's Guide PDFs.
- If you know the page number or know vaguely which page-range you want to view, you can enter a number in the toolbar in Reader, then press [ENTER] to jump directly to that page.
- Type [CTRL]+[F] to open the Adobe Reader search utility and enter a word or phrase. This can help you quickly pinpoint the information you require. You can also enter text directly into the toolbar in Reader.
- To quickly move around within a page, press the [SPACE] bar. This turns your cursor into a "hand" with which you can grab the page and move it around freely on your screen.
- Embedded hyperlinks are actually cross-references to related text. Click them to jump to the corresponding section of the User's Guide PDF.

## Related Documentation

- Quick Start Guide

The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up your network and configuring for Internet access.

- Web Configurator Online Help

The embedded Web Help contains descriptions of individual screens and supplementary information.

- Support Disc

Refer to the included CD for support documents.

## Documentation Feedback

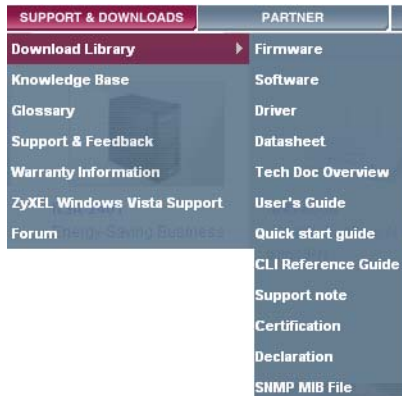
Send your comments, questions or suggestions to: [techwriters@zyxel.com.tw](mailto:techwriters@zyxel.com.tw)

Thank you!

The Technical Writing Team, ZyXEL Communications Corp.,  
6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 30099, Taiwan.

## Need More Help?

More help is available at [www.zyxel.com](http://www.zyxel.com).



- **Download Library**  
Search for the latest product updates and documentation from this link. Read the Tech Doc Overview to find out how to efficiently use the User Guide, Quick Start Guide and Command Line Interface Reference Guide in order to better understand how to use your product.
- **Knowledge Base**  
If you have a specific question about your product, the answer may be here. This is a collection of answers to previously asked questions about ZyXEL products.
- **Forum**  
This contains discussions on ZyXEL products. Learn from others who use ZyXEL products and share your experiences as well.

## Customer Support

Should problems arise that cannot be solved by the methods listed above, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device.

See [http://www.zyxel.com/web/contact\\_us.php](http://www.zyxel.com/web/contact_us.php) for contact information. Please have the following information ready when you contact an office.

- Product model and serial number.
- Warranty Information.
- Date that you received your device.

- Brief description of the problem and the steps you took to solve it.

### **Disclaimer**

Graphics in this book may differ slightly from the product due to differences in operating systems, operating system versions, or if you installed updated firmware/software for your device. Every effort has been made to ensure that the information in this manual is accurate.

# Document Conventions

## Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

**Warnings tell you about things that could harm you or your device.**




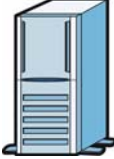
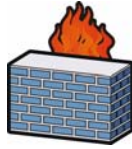



Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

## Syntax Conventions

- The P-660RU-Tx may be referred to as the "device", the "system" or the "product" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

## Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The P-660RU-Tx icon is not an exact representation of your device.

|   |   |  |
|---|---|--|
| P-660RU-Tx<br> | Computer<br> | Notebook computer<br> |
| Server<br>     | Firewall<br> | Telephone<br>          |
| Router<br>    | Switch<br>  |  |

# Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.





# Contents Overview

|   |           |
|---|-----------|
| <b>User's Guide .....</b>               | <b>23</b> |
| Introducing the P-660RU-Tx .....        | 25        |
| Introducing the Web Configurator .....  | 37        |
| <b>Status .....</b>                     | <b>41</b> |
| Device Information .....                | 43        |
| System Logs .....                       | 47        |
| Traffic Statistics .....                | 49        |
| Quick Start Wizard .....                | 51        |
| Internet Setup .....                    | 59        |
| LAN Setup .....                         | 75        |
| Static Route .....                      | 85        |
| Network Address Translation (NAT) ..... | 89        |
| Quality of Service (QoS) .....          | 101       |
| ADSL .....                              | 109       |
| Firewall .....                          | 111       |
| Access Control .....                    | 115       |
| Filters .....                           | 119       |
| SNMP .....                              | 125       |
| Universal Plug-and-Play (UPnP) .....    | 127       |
| Dynamic DNS Setup .....                 | 141       |
| CWMP .....                              | 143       |
| Administrator Settings .....            | 147       |
| Time Zone .....                         | 149       |
| Firmware .....                          | 151       |
| System Restart .....                    | 159       |
| Diagnostic .....                        | 161       |
| Troubleshooting .....                   | 163       |
| Product Specifications .....            | 169       |



# Table of Contents

|   |           |
|---|-----------|
| <b>About This User's Guide .....</b>              | <b>3</b>  |
| <b>Document Conventions.....</b>                  | <b>6</b>  |
| <b>Safety Warnings.....</b>                       | <b>8</b>  |
| <b>Contents Overview .....</b>                    | <b>9</b>  |
| <b>Table of Contents.....</b>                     | <b>11</b> |
| <b>List of Figures .....</b>                      | <b>17</b> |
| <b>List of Tables.....</b>                        | <b>21</b> |
| <br>  |           |
| <b>Part I: User's Guide.....</b>                  | <b>23</b> |
| <br>  |           |
| <b>Chapter 1</b>                                  |           |
| <b>Introducing the P-660RU-Tx.....</b>            | <b>25</b> |
| 1.1 Overview .....                                | 25        |
| 1.2 Ways to Manage the P-660RU-Tx .....           | 25        |
| 1.3 Good Habits for Managing the P-660RU-Tx ..... | 26        |
| 1.4 Applications for the P-660RU-Tx .....         | 26        |
| 1.4.1 Internet Access .....                       | 27        |
| 1.5 LEDs (Lights) .....                           | 28        |
| 1.6 The RESET Button .....                        | 29        |
| 1.6.1 Using the Reset Button .....                | 29        |
| 1.7 USB Port .....                                | 29        |
| 1.7.1 Installing the USB Driver in Windows .....  | 30        |
| 1.7.2 Verifying Your USB Installation .....       | 34        |
| <br>  |           |
| <b>Chapter 2</b>                                  |           |
| <b>Introducing the Web Configurator .....</b>     | <b>37</b> |
| 2.1 Overview .....                                | 37        |
| 2.1.1 Accessing the Web Configurator .....        | 37        |
| 2.2 Web Configurator Main Screen .....            | 38        |
| 2.2.1 Navigation Panel .....                      | 39        |
| 2.2.2 Main Window .....                           | 40        |

|  |           |
|--|-----------|
| <b>Part II: Status .....</b>                                 | <b>41</b> |
| <b>Chapter 3</b>   |           |
| <b>Device Information.....</b>                               | <b>43</b> |
| 3.1 Overview .....   | 43        |
| 3.2 The Device Info Screen .....                             | 43        |
| <b>Chapter 4</b>   |           |
| <b>System Logs.....</b>                                      | <b>47</b> |
| 4.1 Overview .....   | 47        |
| 4.2 The System Log Screen .....                              | 47        |
| <b>Chapter 5</b>   |           |
| <b>Traffic Statistics .....</b>                              | <b>49</b> |
| 5.1 Overview .....   | 49        |
| 5.2 The Statistics Screen .....                              | 49        |
| <b>Chapter 6</b>   |           |
| <b>Quick Start Wizard .....</b>                              | <b>51</b> |
| 6.1 Overview .....   | 51        |
| 6.2 Quick Start Wizard .....                                 | 51        |
| <b>Chapter 7</b>   |           |
| <b>Internet Setup.....</b>                                   | <b>59</b> |
| 7.1 Overview .....   | 59        |
| 7.1.1 What You Can Do in the Internet Screens .....          | 59        |
| 7.1.2 What You Need to Know About ADSL Internet Access ..... | 59        |
| 7.1.3 Before You Begin .....                                 | 61        |
| 7.2 The Internet Screen .....                                | 62        |
| 7.2.1 Dynamic IP Address .....                               | 63        |
| 7.2.2 Static IP Address .....                                | 65        |
| 7.2.3 PPPoA/PPPoE .....                                      | 67        |
| 7.2.4 Bridge Mode .....                                      | 69        |
| 7.2.5 The PVCs Summary Screen .....                          | 70        |
| 7.3 WAN Technical Reference .....                            | 70        |
| 7.3.1 Encapsulation .....                                    | 70        |
| 7.3.2 Multiplexing .....                                     | 71        |
| 7.3.3 VPI and VCI .....                                      | 72        |
| 7.3.4 IP Address Assignment .....                            | 72        |
| 7.3.5 Always-On Connection (PPP) .....                       | 72        |
| 7.3.6 ATM QoS .....  | 73        |
| 7.3.7 ATM Traffic Classes .....                              | 74        |

|   |            |
|---|------------|
| <b>Chapter 8</b>  |            |
| <b>LAN Setup</b> .....  | <b>75</b>  |
| 8.1 Overview .....  | 75         |
| 8.1.1 What You Can Do in the LAN Screens .....                    | 75         |
| 8.1.2 What You Need To Know About LAN .....                       | 75         |
| 8.2 The LAN Screen .....  | 77         |
| 8.2.1 The DHCP IP Pool Summary Screen .....                       | 79         |
| 8.3 LAN Technical Reference .....                                 | 79         |
| 8.3.1 LANs, WANs and the ZyXEL Device .....                       | 80         |
| 8.3.2 DHCP Setup .....  | 80         |
| 8.3.3 DNS Server Addresses .....                                  | 80         |
| 8.3.4 LAN TCP/IP .....  | 81         |
| 8.3.5 RIP Setup .....   | 82         |
| 8.3.6 Multicast .....   | 83         |
| <b>Chapter 9</b>  |            |
| <b>Static Route</b> .....   | <b>85</b>  |
| 9.1 Overview .....  | 85         |
| 9.1.1 What You Can Do in the Static Route Screens .....           | 85         |
| 9.2 The Routing Table List Screen .....                           | 86         |
| 9.2.1 The Static Route Screen .....                               | 87         |
| <b>Chapter 10</b>   |            |
| <b>Network Address Translation (NAT)</b> .....                    | <b>89</b>  |
| 10.1 Overview .....   | 89         |
| 10.1.1 What You Can Do in the NAT Screens .....                   | 89         |
| 10.1.2 What You Need To Know About NAT .....                      | 89         |
| 10.2 The NAT Screen .....   | 91         |
| 10.3 The DMZ Screen .....   | 91         |
| 10.4 The Virtual Server Screen .....                              | 92         |
| 10.4.1 Configuring Servers Behind Port Forwarding (Example) ..... | 93         |
| 10.4.2 Configuring the Virtual Server Screen .....                | 94         |
| 10.5 The IP Address Mapping Screen .....                          | 95         |
| 10.6 NAT Technical Reference .....                                | 97         |
| 10.6.1 NAT Definitions .....                                      | 98         |
| 10.6.2 What NAT Does .....  | 98         |
| 10.6.3 How NAT Works .....  | 99         |
| <b>Chapter 11</b>   |            |
| <b>Quality of Service (QoS)</b> .....                             | <b>101</b> |
| 11.1 Overview .....   | 101        |
| 11.1.1 What You Can Do in the QoS Screens .....                   | 102        |
| 11.1.2 What You Need To Know About QoS .....                      | 102        |

|  |            |
|--|------------|
| 11.2 The QoS Screen .....                                | 103        |
| 11.2.1 The QoS Settings Summary Screen .....             | 105        |
| 11.3 QoS Technical Reference .....                       | 106        |
| 11.3.1 IEEE 802.1p .....                                 | 106        |
| 11.3.2 IP Precedence .....                               | 107        |
| 11.3.3 Automatic Priority Queue Assignment .....         | 107        |
| <b>Chapter 12</b>  |            |
| <b>ADSL .....</b>  | <b>109</b> |
| 12.1 Overview .....                                      | 109        |
| 12.2 The ADSL Screen .....                               | 109        |
| <b>Chapter 13</b>  |            |
| <b>Firewall.....</b>                                     | <b>111</b> |
| 13.1 Overview .....                                      | 111        |
| 13.1.1 What You Can Do in the Firewall Screens .....     | 111        |
| 13.1.2 What You Need to Know About Firewall .....        | 111        |
| 13.2 The Firewall Screen .....                           | 112        |
| <b>Chapter 14</b>  |            |
| <b>Access Control.....</b>                               | <b>115</b> |
| 14.1 Access Control Overview .....                       | 115        |
| 14.1.1 The Access Control Setup Screen .....             | 115        |
| 14.1.2 Access Control Interfaces .....                   | 115        |
| 14.1.3 System Timeout .....                              | 116        |
| 14.1.4 Configuring the Access Control Setup Screen ..... | 116        |
| <b>Chapter 15</b>  |            |
| <b>Filters .....</b>                                     | <b>119</b> |
| 15.1 Overview .....                                      | 119        |
| 15.1.1 What You Can Do in the Filter Screens .....       | 119        |
| 15.1.2 What You Need to Know About Filtering .....       | 119        |
| 15.2 The IP/MAC Filter Screen .....                      | 120        |
| 15.3 The Application Filter Screen .....                 | 122        |
| 15.4 The URL Filter Screen .....                         | 123        |
| <b>Chapter 16</b>  |            |
| <b>SNMP.....</b>   | <b>125</b> |
| 16.1 Overview .....                                      | 125        |
| 16.1.1 Supported MIBs .....                              | 126        |
| 16.2 The SNMP Screen .....                               | 126        |
| <b>Chapter 17</b>  |            |
| <b>Universal Plug-and-Play (UPnP).....</b>               | <b>127</b> |

---

|  |            |
|--|------------|
| 17.1 Overview .....                                    | 127        |
| 17.1.1 What You Can Do in the UPnP Screen .....        | 127        |
| 17.1.2 What You Need to Know About UPnP .....          | 127        |
| 17.2 The UPnP Screen .....                             | 128        |
| 17.3 Installing UPnP in Windows Example .....          | 130        |
| 17.4 Using UPnP in Windows XP Example .....            | 133        |
| <b>Chapter 18</b>                                      |            |
| <b>Dynamic DNS Setup .....</b>                         | <b>141</b> |
| 18.1 Overview .....                                    | 141        |
| 18.1.1 What You Can Do in the DDNS Screen .....        | 141        |
| 18.1.2 What You Need To Know About DDNS .....          | 141        |
| 18.2 The Dynamic DNS Screen .....                      | 142        |
| <b>Chapter 19</b>                                      |            |
| <b>CWMP .....</b>                                      | <b>143</b> |
| 19.1 Overview .....                                    | 143        |
| 19.2 The CWMP Setup Screen .....                       | 144        |
| <b>Chapter 20</b>                                      |            |
| <b>Administrator Settings .....</b>                    | <b>147</b> |
| 20.1 Overview .....                                    | 147        |
| 20.2 The Administrator Screen .....                    | 147        |
| <b>Chapter 21</b>                                      |            |
| <b>Time Zone .....</b>                                 | <b>149</b> |
| 21.1 Overview .....                                    | 149        |
| 21.2 The Time Zone Screen .....                        | 149        |
| <b>Chapter 22</b>                                      |            |
| <b>Firmware .....</b>                                  | <b>151</b> |
| 22.1 Overview .....                                    | 151        |
| 22.1.1 What You Need To Know About Firmware .....      | 151        |
| 22.1.2 Before You Begin .....                          | 152        |
| 22.1.3 Firmware and Configuration Files Examples ..... | 153        |
| 22.2 The Firmware Screen .....                         | 157        |
| <b>Chapter 23</b>                                      |            |
| <b>System Restart .....</b>                            | <b>159</b> |
| 23.1 Overview .....                                    | 159        |
| 23.2 The System Restart Screen .....                   | 159        |
| <b>Chapter 24</b>                                      |            |
| <b>Diagnostic .....</b>                                | <b>161</b> |

|   |            |
|---|------------|
| 24.1 Overview .....   | 161        |
| 24.2 The Diagnostic Screen .....                                  | 161        |
| <b>Chapter 25</b>   |            |
| <b>Troubleshooting.....</b>                                       | <b>163</b> |
| 25.1 Power, Hardware Connections, and LEDs .....                  | 163        |
| 25.2 P-660RU-Tx Access and Login .....                            | 164        |
| 25.3 Internet Access .....  | 166        |
| <b>Chapter 26</b>   |            |
| <b>Product Specifications.....</b>                                | <b>169</b> |
| 26.1 Hardware Specifications .....                                | 169        |
| 26.2 Firmware Specifications .....                                | 169        |
| 26.3 Power Adaptor Specifications .....                           | 173        |
| Appendix A Setting up Your Computer's IP Address.....             | 175        |
| Appendix B Pop-up Windows, JavaScripts and Java Permissions ..... | 199        |
| Appendix C IP Addresses and Subnetting .....                      | 209        |
| Appendix D Services .....   | 219        |
| Appendix E Legal Information .....                                | 223        |
| Appendix F Customer Support.....                                  | 225        |
| <b>Index.....</b>   | <b>233</b> |



# List of Figures

|  |    |
|--|----|
| Figure 1 P-660RU-Tx's Router Features .....                  | 27 |
| Figure 2 LEDs on the Top of the Device .....                 | 28 |
| Figure 3 Login Screen .....                                  | 38 |
| Figure 4 Main Screen .....                                   | 38 |
| Figure 5 Status > Device Information .....                   | 43 |
| Figure 6 Status > System Log .....                           | 47 |
| Figure 7 Status > Statistics (Ethernet) .....                | 49 |
| Figure 8 Status > Statistics (ADSL) .....                    | 50 |
| Figure 9 Access Quick Start Wizard .....                     | 51 |
| Figure 10 Run Wizard .....                                   | 52 |
| Figure 11 Wizard Summary .....                               | 52 |
| Figure 12 Password .....                                     | 52 |
| Figure 13 Time Zone .....                                    | 53 |
| Figure 14 ISP Connection Type .....                          | 53 |
| Figure 15 ISP Connection: Dynamic IP .....                   | 53 |
| Figure 16 ISP Connection: Static IP Address .....            | 54 |
| Figure 17 ISP Connection: PPPoE/PPPoA .....                  | 55 |
| Figure 18 ISP Connection: Bridge Mode .....                  | 56 |
| Figure 19 Complete Quick Start .....                         | 57 |
| Figure 20 LAN and WAN .....                                  | 59 |
| Figure 21 Interface Setup > Internet .....                   | 62 |
| Figure 22 Interface Setup > Internet (Dynamic IP) .....      | 63 |
| Figure 23 Interface Setup > Internet (Static IP) .....       | 65 |
| Figure 24 Interface Setup > Internet (PPPoA/PPPoE) .....     | 67 |
| Figure 25 Interface Setup > Internet (Bridge) .....          | 69 |
| Figure 26 Interface Setup > PVCs Summary .....               | 70 |
| Figure 27 Example of ATM OoS .....                           | 73 |
| Figure 28 Interface Setup > LAN .....                        | 77 |
| Figure 29 Interface Setup > LAN > DHCP IP Pool Summary ..... | 79 |
| Figure 30 LAN and WAN IP Addresses .....                     | 80 |
| Figure 31 Example of Static Routing Topology .....           | 85 |
| Figure 32 Advanced Setup > Routing Table List .....          | 86 |
| Figure 33 Advanced > Routing > Static Route .....            | 87 |
| Figure 34 Advanced Setup > NAT .....                         | 91 |
| Figure 35 Advanced Setup > NAT > DMZ .....                   | 92 |
| Figure 36 Multiple Servers Behind NAT Example .....          | 93 |
| Figure 37 Advanced Setup > NAT > Virtual Server .....        | 94 |
| Figure 38 Advanced Setup > NAT > IP Address Mapping .....    | 96 |

|   |     |
|---|-----|
| Figure 39 How NAT Works .....   | 99  |
| Figure 40 QoS Example .....   | 102 |
| Figure 41 Advanced Setup > QoS .....  | 103 |
| Figure 42 Advanced Setup > QoS > QoS Settings Summary .....                   | 105 |
| Figure 43 Advanced Setup > ADSL .....   | 109 |
| Figure 44 Advanced Setup > Firewall .....                                     | 112 |
| Figure 45 Access Control .....  | 115 |
| Figure 46 Access Management > ACL .....                                       | 116 |
| Figure 47 Access Management > Filter (IP/MAC) .....                           | 120 |
| Figure 48 Access Management > Filter (Application) .....                      | 122 |
| Figure 49 Access Management > Filter (URL) .....                              | 123 |
| Figure 50 SNMP Management Model .....   | 125 |
| Figure 51 Access Management > SNMP .....                                      | 126 |
| Figure 52 Access Management > UPnP .....                                      | 128 |
| Figure 53 Add/Remove Programs: Windows Setup: Communication .....             | 130 |
| Figure 54 Add/Remove Programs: Windows Setup: Communication: Components ..... | 131 |
| Figure 55 Network Connections .....   | 131 |
| Figure 56 Windows Optional Networking Components Wizard .....                 | 132 |
| Figure 57 Networking Services .....   | 133 |
| Figure 58 Network Connections .....   | 134 |
| Figure 59 Internet Connection Properties .....                                | 135 |
| Figure 60 Internet Connection Properties: Advanced Settings .....             | 136 |
| Figure 61 Internet Connection Properties: Advanced Settings: Add .....        | 136 |
| Figure 62 System Tray Icon .....  | 137 |
| Figure 63 Internet Connection Status .....                                    | 137 |
| Figure 64 Network Connections .....   | 138 |
| Figure 65 Network Connections: My Network Places .....                        | 139 |
| Figure 66 Network Connections: My Network Places: Properties: Example .....   | 139 |
| Figure 67 Access Management > DDNS .....                                      | 142 |
| Figure 68 LAN and WAN .....   | 143 |
| Figure 69 Access Management > CWMP .....                                      | 144 |
| Figure 70 Maintenance > Administration .....                                  | 147 |
| Figure 71 Maintenance > Time Zone .....                                       | 149 |
| Figure 72 Restore Using FTP Session Example .....                             | 153 |
| Figure 73 FTP Session Example of Firmware File Upload .....                   | 154 |
| Figure 74 FTP Session Example .....   | 156 |
| Figure 75 Maintenance > Firmware .....  | 157 |
| Figure 76 Maintenance > System Restart .....                                  | 159 |
| Figure 77 Maintenance > Diagnostic .....                                      | 161 |
| Figure 78 WIndows 95/98/Me: Network: Configuration .....                      | 176 |
| Figure 79 Windows 95/98/Me: TCP/IP Properties: IP Address .....               | 177 |
| Figure 80 Windows 95/98/Me: TCP/IP Properties: DNS Configuration .....        | 178 |
| Figure 81 Windows XP: Start Menu .....  | 179 |

|  |     |
|--|-----|
| Figure 82 Windows XP: Control Panel .....  | 179 |
| Figure 83 Windows XP: Control Panel: Network Connections: Properties .....       | 180 |
| Figure 84 Windows XP: Local Area Connection Properties .....                     | 180 |
| Figure 85 Windows XP: Internet Protocol (TCP/IP) Properties .....                | 181 |
| Figure 86 Windows XP: Advanced TCP/IP Properties .....                           | 182 |
| Figure 87 Windows XP: Internet Protocol (TCP/IP) Properties .....                | 183 |
| Figure 88 Windows Vista: Start Menu .....  | 184 |
| Figure 89 Windows Vista: Control Panel .....                                     | 184 |
| Figure 90 Windows Vista: Network And Internet .....                              | 184 |
| Figure 91 Windows Vista: Network and Sharing Center .....                        | 185 |
| Figure 92 Windows Vista: Network and Sharing Center .....                        | 185 |
| Figure 93 Windows Vista: Local Area Connection Properties .....                  | 186 |
| Figure 94 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties ..... | 187 |
| Figure 95 Windows Vista: Advanced TCP/IP Properties .....                        | 188 |
| Figure 96 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties ..... | 189 |
| Figure 97 Macintosh OS 8/9: Apple Menu .....                                     | 190 |
| Figure 98 Macintosh OS 8/9: TCP/IP .....   | 191 |
| Figure 99 Macintosh OS X: Apple Menu .....                                       | 192 |
| Figure 100 Macintosh OS X: Network .....   | 192 |
| Figure 101 Red Hat 9.0: KDE: Network Configuration: Devices .....                | 193 |
| Figure 102 Red Hat 9.0: KDE: Ethernet Device: General .....                      | 194 |
| Figure 103 Red Hat 9.0: KDE: Network Configuration: DNS .....                    | 194 |
| Figure 104 Red Hat 9.0: KDE: Network Configuration: Activate .....               | 195 |
| Figure 105 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0 .....        | 195 |
| Figure 106 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0 .....         | 196 |
| Figure 107 Red Hat 9.0: DNS Settings in resolv.conf .....                        | 196 |
| Figure 108 Red Hat 9.0: Restart Ethernet Card .....                              | 196 |
| Figure 109 Red Hat 9.0: Checking TCP/IP Properties .....                         | 197 |
| Figure 110 Pop-up Blocker .....  | 199 |
| Figure 111 Internet Options: Privacy .....                                       | 200 |
| Figure 112 Internet Options: Privacy .....                                       | 201 |
| Figure 113 Pop-up Blocker Settings .....   | 202 |
| Figure 114 Internet Options: Security .....                                      | 203 |
| Figure 115 Security Settings - Java Scripting .....                              | 204 |
| Figure 116 Security Settings - Java .....  | 205 |
| Figure 117 Java (Sun) .....  | 206 |
| Figure 118 Mozilla Firefox: Tools > Options .....                                | 206 |
| Figure 119 Mozilla Firefox Content Security .....                                | 207 |
| Figure 120 Network Number and Host ID .....                                      | 210 |
| Figure 121 Subnetting Example: Before Subnetting .....                           | 213 |
| Figure 122 Subnetting Example: After Subnetting .....                            | 213 |



# List of Tables

|   |     |
|---|-----|
| Table 1 LED Descriptions .....                              | 28  |
| Table 2 Navigation Panel Summary .....                      | 39  |
| Table 3 Status > Device Information .....                   | 44  |
| Table 4 Status > System Log .....                           | 48  |
| Table 5 Status > Statistics (Ethernet) .....                | 49  |
| Table 6 Status > Statistics (ADSL) .....                    | 50  |
| Table 7 ISP Connection: Dynamic IP .....                    | 54  |
| Table 8 ISP Connection: Static IP Address .....             | 55  |
| Table 9 ISP Connection: PPPoE/PPPoA .....                   | 56  |
| Table 10 ISP Connection: Bridge Mode .....                  | 56  |
| Table 11 Interface Setup > Internet .....                   | 62  |
| Table 12 Interface Setup > Internet (Dynamic IP) .....      | 64  |
| Table 13 Interface Setup > Internet (Static IP) .....       | 65  |
| Table 14 Interface Setup > Internet (PPPoA/PPPoE) .....     | 67  |
| Table 15 Interface Setup > Internet (Bridge) .....          | 69  |
| Table 16 Interface Setup > PVCs Summary .....               | 70  |
| Table 17 Interface Setup > LAN .....                        | 77  |
| Table 18 Interface Setup > LAN > DHCP IP Pool Summary ..... | 79  |
| Table 19 Advanced Setup > Routing Table List .....          | 86  |
| Table 20 Advanced > Static Route: Edit .....                | 87  |
| Table 21 Network > NAT > General .....                      | 91  |
| Table 22 Advanced Setup > NAT > DMZ .....                   | 92  |
| Table 23 Multiple Servers Behind NAT Example .....          | 93  |
| Table 24 Advanced Setup > NAT > Virtual Server .....        | 94  |
| Table 25 Network > NAT > Address Mapping .....              | 96  |
| Table 26 NAT Definitions .....                              | 98  |
| Table 27 Advanced Setup > QoS .....                         | 104 |
| Table 28 Advanced Setup > QoS > QoS Settings Summary .....  | 106 |
| Table 29 IEEE 802.1p Priority Level and Traffic Type .....  | 106 |
| Table 30 Internal Layer2 and Layer3 QoS Mapping .....       | 107 |
| Table 31 Advanced Setup > ADSL .....                        | 109 |
| Table 32 Advanced > Firewall .....                          | 113 |
| Table 33 Access Management > ACL .....                      | 116 |
| Table 34 Access Management > Filter (IP/MAC) .....          | 120 |
| Table 35 Access Management > Filter (Application) .....     | 122 |
| Table 36 Access Management > Filter (URL) .....             | 123 |
| Table 37 Access Management > SNMP .....                     | 126 |
| Table 38 Access Management > UPnP .....                     | 129 |

|   |     |
|---|-----|
| Table 39 Advanced > Dynamic DNS .....                         | 142 |
| Table 40 Access Management > CWMP .....                       | 144 |
| Table 41 Maintenance > Administration .....                   | 147 |
| Table 42 Maintenance > Time Zone .....                        | 149 |
| Table 43 Filename Conventions .....                           | 152 |
| Table 44 General Commands for GUI-based FTP Clients .....     | 156 |
| Table 45 Maintenance > Firmware .....                         | 157 |
| Table 46 Maintenance > System Restart .....                   | 159 |
| Table 47 Hardware Specifications .....                        | 169 |
| Table 48 Firmware Specifications .....                        | 169 |
| Table 49 Standards Supported .....                            | 172 |
| Table 50 P-660RU-Tx Series Power Adaptor Specifications ..... | 173 |
| Table 51 Subnet Masks .....                                   | 210 |
| Table 52 Subnet Masks .....                                   | 211 |
| Table 53 Maximum Host Numbers .....                           | 211 |
| Table 54 Alternative Subnet Mask Notation .....               | 212 |
| Table 55 Subnet 1 .....                                       | 214 |
| Table 56 Subnet 2 .....                                       | 214 |
| Table 57 Subnet 3 .....                                       | 215 |
| Table 58 Subnet 4 .....                                       | 215 |
| Table 59 Eight Subnets .....                                  | 215 |
| Table 60 24-bit Network Number Subnet Planning .....          | 216 |
| Table 61 16-bit Network Number Subnet Planning .....          | 216 |
| Table 62 Examples of Services .....                           | 219 |

---

# **PART I**

## **User's Guide**

---





# Introducing the P-660RU-Tx

This chapter introduces the main applications and features of the P-660RU-Tx. It also introduces the ways you can manage the P-660RU-Tx.

## 1.1 Overview

The P-660RU-Tx is an ADSL2+ router. By integrating DSL and NAT, you are provided with ease of installation and high-speed, shared Internet access. Provided with both USB and Ethernet ports, computers can share local resources (such as printers and files) and access to the Internet - simultaneously.

Models ending in "1", for example P-660RU-T1, denote a device that works over the analog telephone system, POTS (Plain Old Telephone Service). Models ending in "3" denote a device that works over ISDN (Integrated Services Digital Network) or T-ISDN (UR-2).

**Only use firmware for your P-660RU-Tx' specific model. Refer to the label on the bottom of your P-660RU-Tx.**

Note: All screens displayed in this user's guide are from the P-660RU-T1 v3 model.

See the product specifications for a full list of features.

## 1.2 Ways to Manage the P-660RU-Tx

Use any of the following methods to manage the P-660RU-Tx.

- Web Configurator. This is recommended for everyday management of the P-660RU-Tx using a (supported) web browser.
- Command Line Interface. Line commands are mostly used for troubleshooting by service engineers.
- FTP for firmware upgrades and configuration backup/restore.

- SNMP. The device can be monitored by an SNMP manager. See the SNMP chapter in this User's Guide.
- TR-069. This is an auto-configuration server used to remotely configure your device.

## 1.3 Good Habits for Managing the P-660RU-Tx

Do the following things regularly to make the P-660RU-Tx more secure and to manage the P-660RU-Tx more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the P-660RU-Tx to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the P-660RU-Tx. You could simply restore your last configuration.

## 1.4 Applications for the P-660RU-Tx

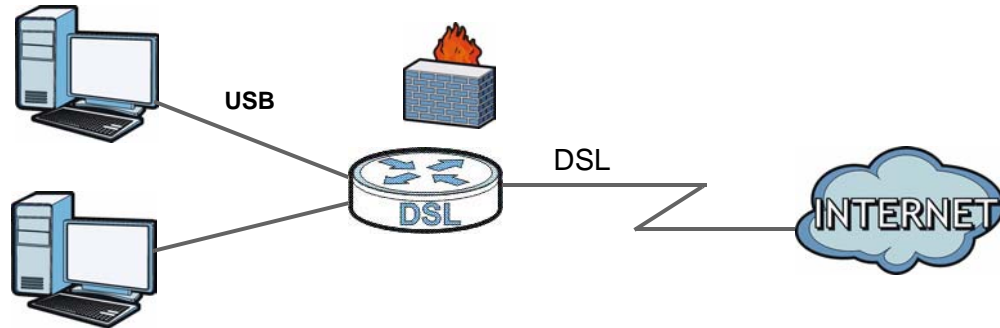
Here are some example uses for which the P-660RU-Tx is well suited.

## 1.4.1 Internet Access

Your P-660RU-Tx provides shared Internet access by connecting the DSL port to the **DSL** or **MODEM** jack on a splitter or your telephone jack. Computers can connect to the P-660RU-Tx's LAN ports.

**Figure 1** P-660RU-Tx's Router Features

### LAN



You can also configure firewall and content filtering on the P-660RU-Tx for secure Internet access. By default, the P-660RU-Tx prevents DDOS, LAND and Ping of Death attacks whether the firewall is enabled or disabled. You can further block SYN Flood and Port Scanner attacks by turning on the firewall.

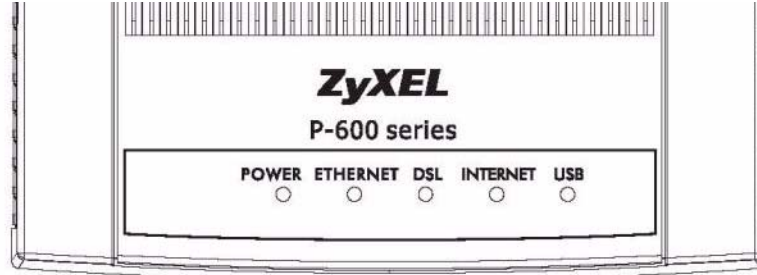
Use content filtering to block access to specific web sites, with URL's containing keywords that you specify. For example, you could block access to certain web sites for the kids.

Use QoS to efficiently manage traffic on your network by giving priority to certain types of traffic and/or to particular computers. For example, you could make sure that the P-660RU-Tx gives voice over Internet calls high priority, and/or limit bandwidth devoted to the boss's excessive file downloading.

## 1.5 LEDs (Lights)

The following graphic displays the labels of the LEDs.

**Figure 2** LEDs on the Top of the Device



None of the LEDs are on if the P-660RU-Tx is not receiving power.

**Table 1** LED Descriptions

| LED      | COLOR | STATUS   | DESCRIPTION  |
|----------|-------|----------|--|
| POWER    | Green | On       | The P-660RU-Tx is receiving power and ready for use.   |
|          |       | Blinking | The P-660RU-Tx is self-testing.  |
|          |       | Off      | The P-660RU-Tx is not receiving power.   |
| ETHERNET | Green | On       | The P-660RU-Tx has an Ethernet connection with a device on the Local Area Network (LAN).   |
|          |       | Blinking | The P-660RU-Tx is sending/receiving data to /from the LAN.   |
|          |       | Off      | The P-660RU-Tx does not have an Ethernet connection with the LAN.  |
| DSL      | Green | On       | The DSL line is up.  |
|          |       | Blinking | The P-660RU-Tx is initializing the DSL line.   |
|          |       | Off      | The DSL line is down.  |
| INTERNET | Green | On       | The P-660RU-Tx has an IP connection but no traffic.<br><br>Your device has a WAN IP address (either static or assigned by a DHCP server), PPP negotiation was successfully completed (if used) and the DSL connection is up. |
|          |       | Blinking | The P-660RU-Tx is sending or receiving IP traffic.   |
|          | Red   | On       | The P-660RU-Tx attempted to make an IP connection but failed. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed.  |
|          |       | Off      | The P-660RU-Tx does not have an IP connection.   |

**Table 1** LED Descriptions

| LED | COLOR | STATUS   | DESCRIPTION   |
|-----|-------|----------|---|
| USB | Green | On       | There is a USB connection.                                    |
|     |       | Blinking | The P-660RU-Tx is sending or receiving data via the USB port. |
|     |       | Off      | There is no USB connection.                                   |

Refer to the Quick Start Guide for information on hardware connections.

## 1.6 The RESET Button

If you forget your password or cannot access the web configurator, you will need to use the **RESET** button at the back of the device to reload the factory-default configuration file. This means that you will lose all configurations that you had previously and the password will be reset to "1234".

### 1.6.1 Using the Reset Button

- 1 Make sure the **POWER** LED is on (not blinking).
- 2 To set the device back to the factory default settings, press the **RESET** button for ten seconds or until the **POWER** LED begins to blink and then release it. When the **POWER** LED begins to blink, the defaults have been restored and the device restarts.

## 1.7 USB Port

The USB port is useful if you have an USB-enabled computer that does not have a network interface card for attaching to your Ethernet network. See the following sections for USB driver installation procedures in your operating system.

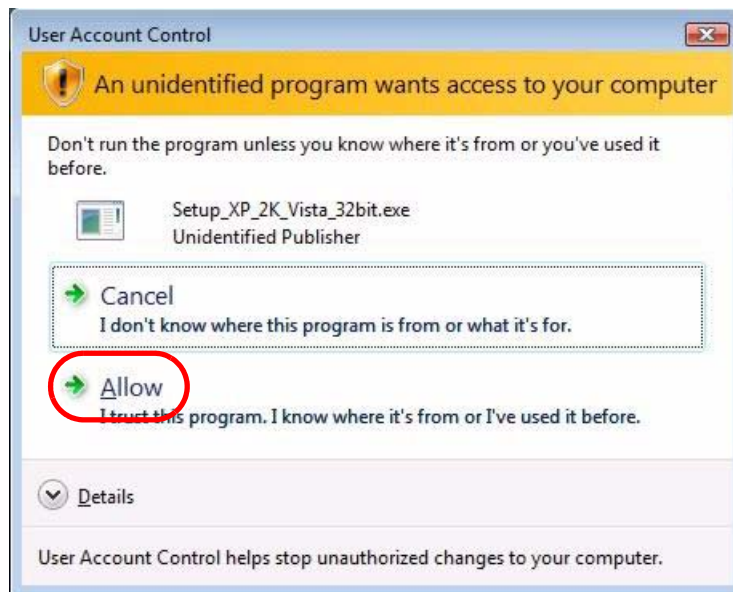
### System Requirements

- Windows 98 (Second Edition), Windows Me (Millennium Edition), Windows 2000, Windows XP or Windows Vista
- An available USB port

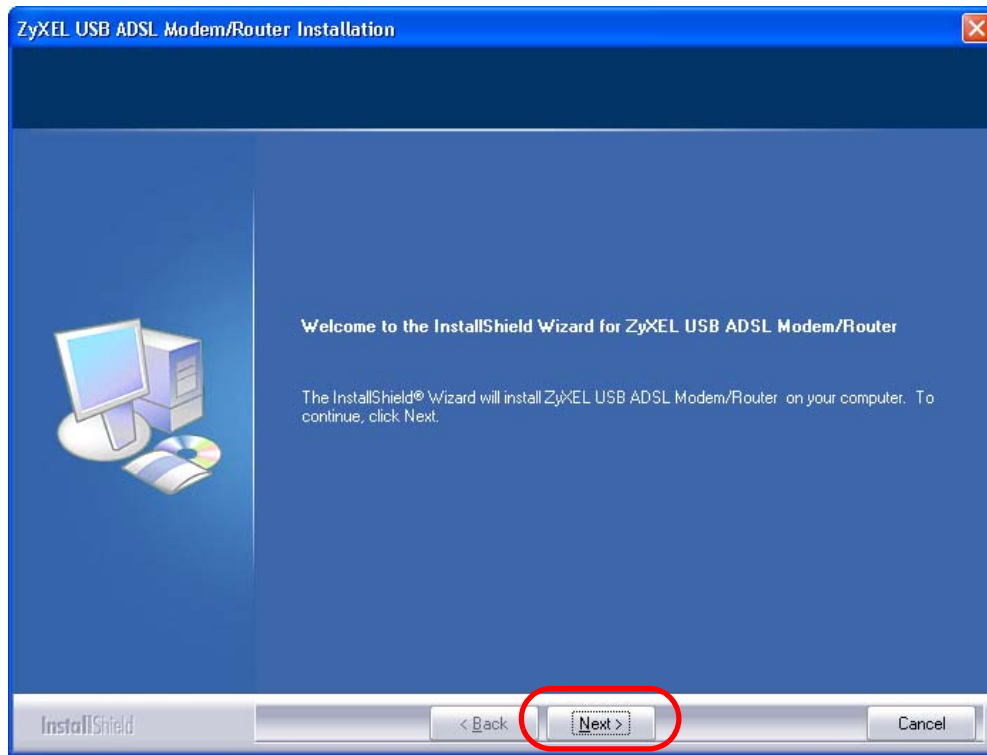
Note: Install the USB driver before you connect the P-660RU-Tx to the USB port.

## 1.7.1 Installing the USB Driver in Windows

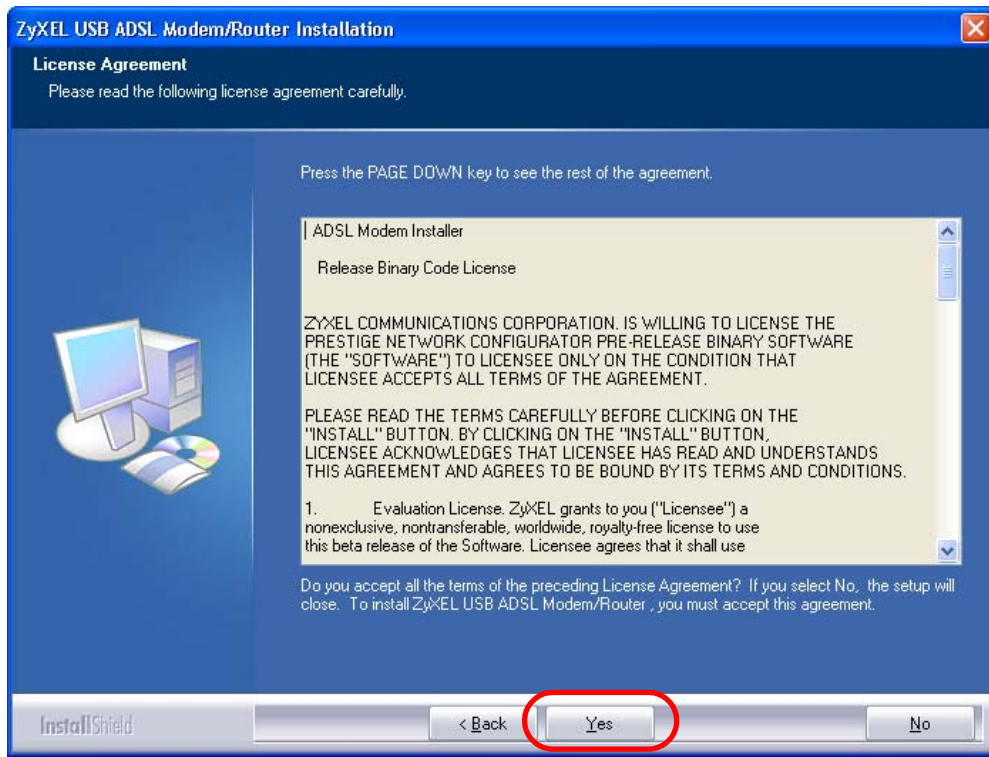
- 1 Save your work and close all applications.
- 2 Insert the included CD. The CD automatically runs and the main screen displays.
- 3 Click the **Setup** icon on the main screen.
- 4 Select the Windows version of your operating system.
- 5 An install warning may appear in the Windows Vista OS. Click **Allow** to continue.



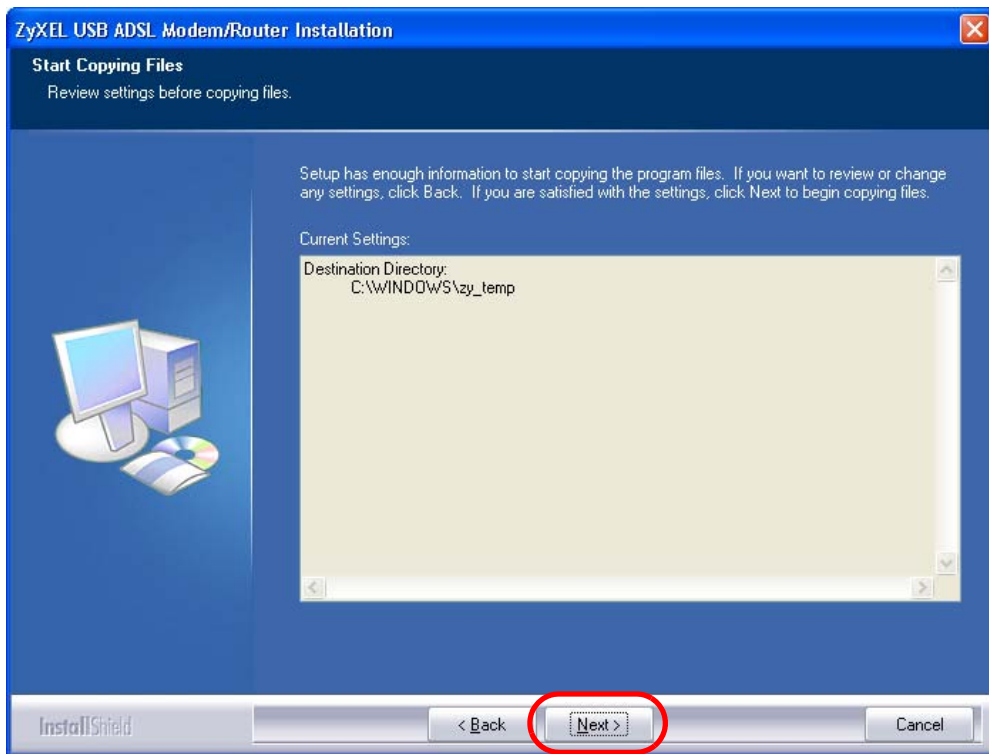
- 6 Click **Next** in the Welcome screen to begin the USB Installation Wizard. Follow the installation prompts. You may need to restart your computer at the end of the installation.



- 7 Click **Yes** to agree to the license agreement.



- 8 A **Start Copying Files** screen displays. Click **Next**.

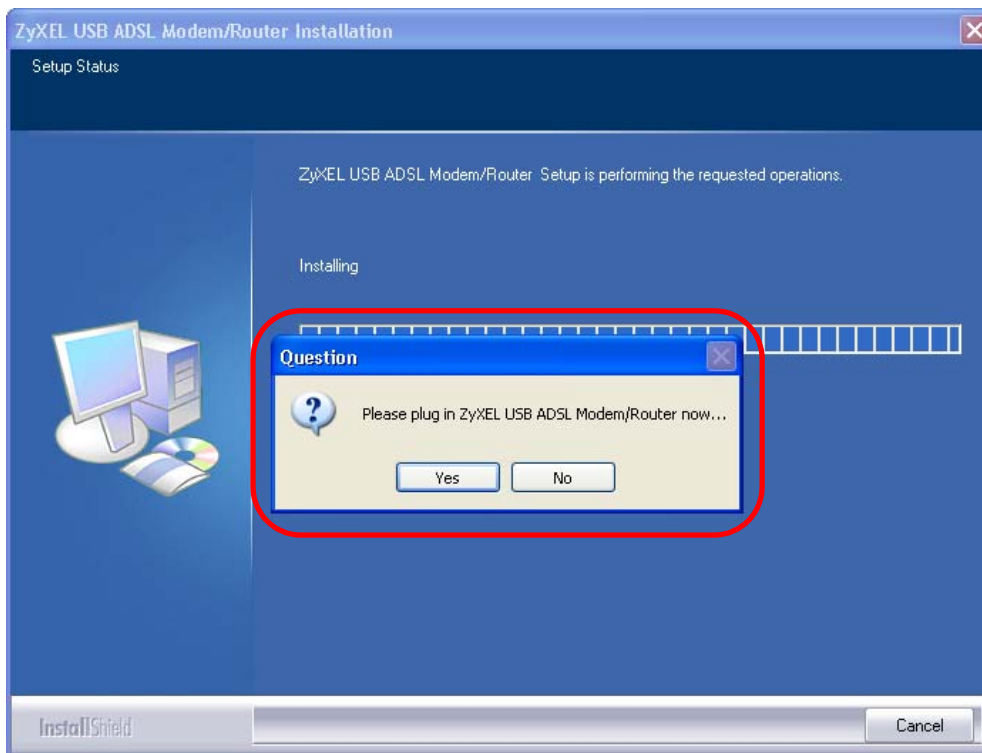




- 9 **Windows 98/Me:** Select **Yes, I want to restart my computer now** and click **OK**.



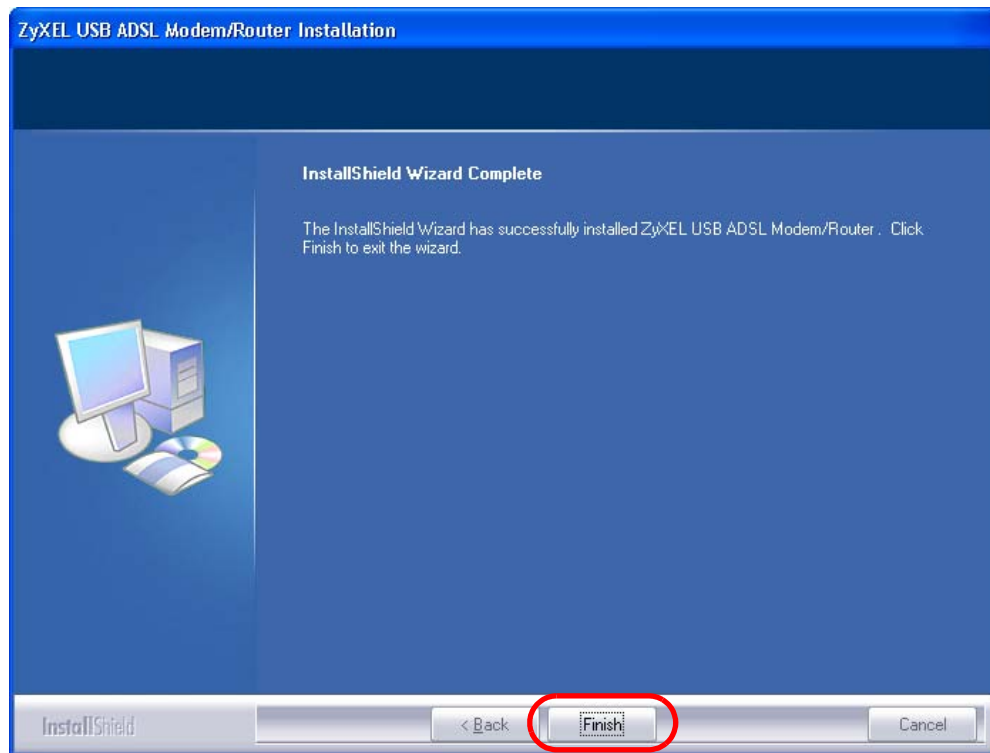
- 10 **Windows 2000/XP:** Connect the P-660RU-Tx to the computer's USB port when prompted. A windows displays indicating that the system has found new hardware.



11 **Windows XP:** If a warning window displays, click **Continue Anyway**.



12 Click **Finish** to complete the installation. Restart the computer if prompted.

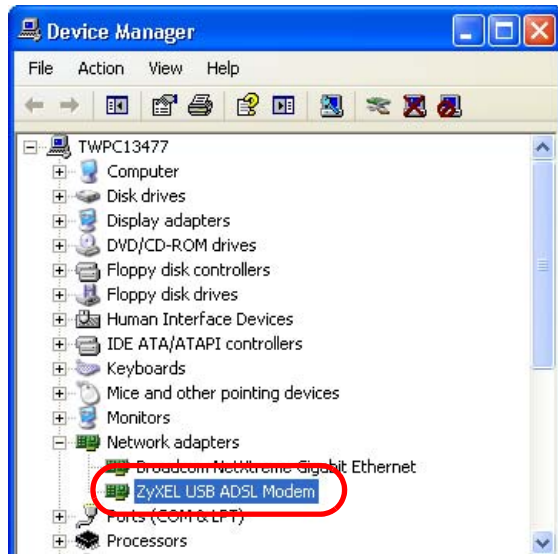


## 1.7.2 Verifying Your USB Installation

Check the status of the P-660RU-Tx in the **Device Manager** window. Click **Start > Settings > Control Panel > System > Hardware** and then click **Device Manager**. (Steps may vary depending on the version of Windows).

Verify the status of the P-660RU-Tx under **Network adapters**. Check that there is no question mark on the device icon for the P-660RU-Tx.

The screen for Windows XP is shown here.





# Introducing the Web Configurator

## 2.1 Overview

The web configurator is an HTML-based management interface that allows easy device setup and management via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

See [Appendix B on page 199](#) if you need to make sure these functions are allowed in Internet Explorer.

### 2.1.1 Accessing the Web Configurator

- 1 Make sure your P-660RU-Tx hardware is properly connected (refer to the Quick Start Guide).
- 2 Launch your web browser.
- 3 Type "192.168.1.1" as the URL.

- 4 A login screen displays. To access the administrative web configurator and manage the P-660RU-Tx, enter the username (**admin** by default) and password (**1234** by default) in the login screen and click **OK**. If you have changed the password, enter your password and click **OK**.

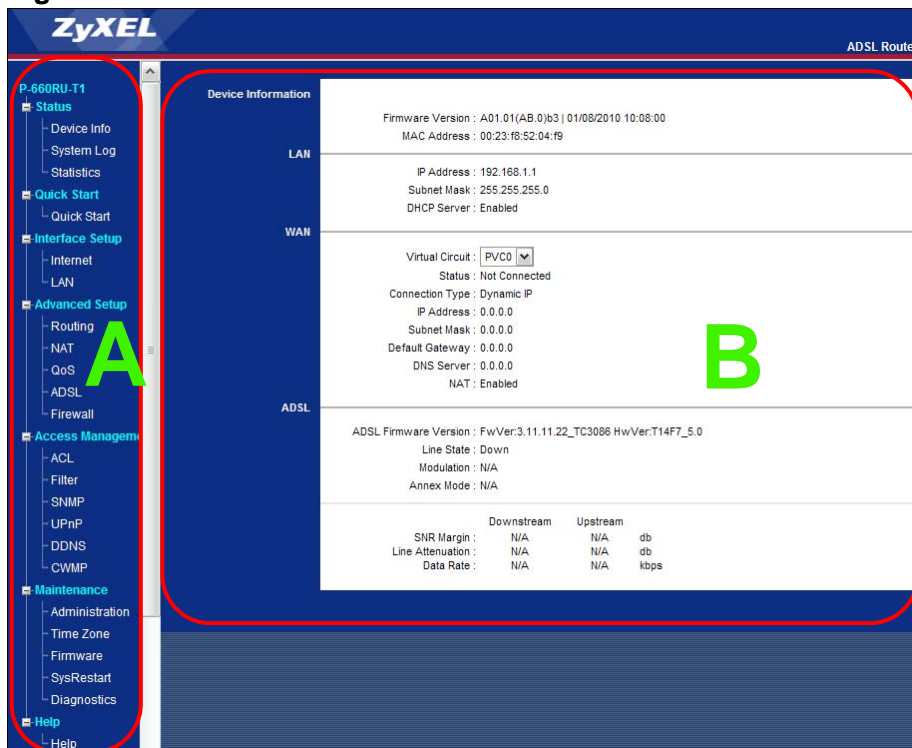
**Figure 3** Login Screen



Note: For security reasons, the P-660RU-Tx automatically logs you out if you do not use the web configurator for five minutes (default). If this happens, log in again.

## 2.2 Web Configurator Main Screen

**Figure 4** Main Screen



As illustrated above, the main screen is divided into these parts:

- **A** - navigation panel
- **B** - main window

## 2.2.1 Navigation Panel

Use the menu items on the navigation panel to open screens to configure P-660RU-Tx features. The following tables describe each menu item.

**Table 2** Navigation Panel Summary

| LINK            | TAB                  | FUNCTION   |
|-----------------|----------------------|--|
| Status          |                      |  |
| Device Info     |                      | This screen shows the P-660RU-Tx's general device and network status information.  |
| System Log      |                      | Use this screen to display your device's logs.   |
| Statistics      |                      | Use this screen to display the statistics of the P-660RU-Tx.   |
| Quick Start     |                      |  |
| Quick Start     |                      | Use this wizard to set up your Internet connection.  |
| Interface Setup |                      |  |
| Internet        | Internet             | Use this screen to configure ISP parameters, WAN IP address assignment and other advanced properties.                        |
|                 | PVC Summary Table    | Use this screen to display your PVC settings.  |
| LAN             | LAN                  | Use this screen to configure LAN TCP/IP and DHCP settings and other advanced properties.                                     |
|                 | DHCP IP Pool Summary | Use this screen to display the IP and MAC addresses of the computers on your LAN.  |
| Advanced Setup  |                      |  |
| Routing         | Routing Table List   | Use this screen to display the static routes on your P-660RU-Tx.   |
|                 | Static Route         | Use this screen to configure IP static routes to tell your device about networks beyond the directly connected remote nodes. |
| NAT             | NAT                  | Use this screen to configure the NAT settings.   |
|                 | DMZ                  | Use this screen to configure the DMZ settings.   |
|                 | Virtual Server       | Use this screen to forward incoming service requests to the server(s) on your local network.                                 |
|                 | IP Address Mapping   | Use this screen to change your P-660RU-Tx's address mapping settings.  |
| QoS             | QoS                  | Use this screen to enable QoS and traffic prioritizing and configure bandwidth management on the WAN.                        |
|                 | QoS Settings Summary | Use this screen to check the QoS rules and actions you configured for the P-660RU-Tx.  |
| ADSL            |                      | Use this screen to configure the ADSL settings on your P-660RU-Tx.   |

**Table 2** Navigation Panel Summary

| LINK              | TAB                | FUNCTION   |
|-------------------|--------------------|--|
| Firewall          |                    | Use this screen to activate/deactivate the firewall and/or SPI on your P-660RU-Tx.                         |
| Access Management |                    |  |
| ACL               |                    | Use this screen to determine which application can access which P-660RU-Tx interface from which computers. |
| Filter            | IP/MAC Filter      | Use this screen to create IP/MAC filter rules.   |
|                   | Application Filter | Use this screen to set the days and times for your device to perform content filtering.                    |
|                   | URL Filter         | Use this screen to allow or deny traffic from certain types of applications.                               |
| SNMP              |                    | Use this screen to configure your P-660RU-Tx's settings for Simple Network Management Protocol management. |
| UPnP              |                    | Use this screen to turn UPnP on or off.  |
| DDNS              |                    | This screen allows you to use a static hostname alias for a dynamic IP address.                            |
| CWMP              |                    | Use this screen to have a management server manage the P-660RU-Tx.   |
| Maintenance       |                    |  |
| Administration    |                    | Use this screen to configure your device's password.   |
| Time Zone         |                    | Use this screen to change your P-660RU-Tx's time and date.   |
| Firmware          |                    | Use this screen to manage configuration files and upload firmware to your device.                          |
| SysRestart        |                    | This screen allows you to reboot the P-660RU-Tx without turning the power off.                             |
| Diagnostics       |                    | Use this screen to test the connections to other devices.  |

## 2.2.2 Main Window

The main window displays information and configuration fields. It is discussed in the rest of this document.

Right after you log in, the **Status** screen is displayed. See [Chapter 3 on page 43](#) for more information about the **Status** screen.



---

# PART II

# Status

---

Device Information (43)

System Logs (47)

Traffic Statistics (49)



# Device Information

## 3.1 Overview

Use the **Device Info** screen to look at the current status of the device, system resources, and interfaces (LAN and WAN).

## 3.2 The Device Info Screen

Use this screen to view the status of the P-660RU-Tx. Click **Status > Device Info** to open the following screen.

**Figure 5** Status > Device Information

| Device Information |  |            |          |
|--------------------|--|------------|----------|
|                    | Firmware Version : A01.01(AB.0)b3   01/08/2010 10:08:00<br>MAC Address : 00:23:f8:52:04:f9   |            |          |
| LAN                | IP Address : 192.168.1.1<br>Subnet Mask : 255.255.255.0<br>DHCP Server : Enabled   |            |          |
| WAN                | Virtual Circuit : <input type="text" value="PVC0"/><br>Status : Not Connected<br>Connection Type : Dynamic IP<br>IP Address : 0.0.0.0<br>Subnet Mask : 0.0.0.0<br>Default Gateway : 0.0.0.0<br>DNS Server : 0.0.0.0<br>NAT : Enabled |            |          |
| ADSL               | ADSL Firmware Version : FwVer:3.11.11.22_TC3086 HwVer:T14F7_5.0<br>Line State : Down<br>Modulation : N/A<br>Annex Mode : N/A   |            |          |
|                    |  | Downstream | Upstream |
|                    | SNR Margin :   | N/A        | N/A db   |
|                    | Line Attenuation :   | N/A        | N/A db   |
|                    | Data Rate :  | N/A        | N/A kbps |

The following table describes the fields in this screen.

**Table 3** Status > Device Information

| LABEL                 | DESCRIPTION   |
|-----------------------|---|
| Device Information    |   |
| Firmware Version      | This is the current version of the firmware inside the device. It also shows the date the firmware version was created.   |
| MAC Address           | This is the MAC (Media Access Control) or Ethernet address unique to your P-660RU-Tx.   |
| LAN                   |   |
| IP Address            | This is the current IP address of the P-660RU-Tx in the LAN.  |
| Subnet Mask           | This is the current subnet mask in the LAN.   |
| DHCP Server           | This field displays what DHCP services the P-660RU-Tx is providing to the LAN. Choices are:<br><br><b>Enabled</b> - The P-660RU-Tx is a DHCP server in the LAN. It can assign IP addresses to other computers in the LAN.<br><br><b>Relay</b> - The P-660RU-Tx acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients.<br><br><b>Disabled</b> - The P-660RU-Tx is not providing any DHCP services to the LAN. |
| WAN                   |   |
| Virtual Circuit       | Use the drop-down list box to select a virtual circuit. The fields below display information about the virtual circuit you choose.  |
| Status                | This is the status of the WAN connection.   |
| Connection Type       | This is the connection type supported by your ISP.  |
| IP Address            | This is the current IP address of the P-660RU-Tx in the WAN, if applicable.   |
| Subnet Mask           | This is the current subnet mask in the WAN, if applicable.  |
| Default Gateway       | This is the IP address of the default gateway, if applicable.   |
| DNS Server            | This is the current DNS server in the WAN, if applicable.   |
| NAT                   | This field displays whether NAT is activated.   |
| ADSL                  |   |
| ADSL Firmware Version | This is the current version of the device's DSL modem code.   |
| Line State            | This is the status of your ADSL connection.   |
| Modulation            | This is the ADSL modulation of your P-660RU-Tx.   |
| Annex Mode            | This is the annex mode of your P-660RU-Tx.  |
| Downstream            | This is the downstream speed of your ZyXEL Device.  |
| Upstream              | This is the upstream speed of your ZyXEL Device.  |

**Table 3** Status > Device Information

| LABEL            | DESCRIPTION  |
|------------------|--|
| SNR Margin       | This is the Signal to Noise Ratio (SNR) margin. SNR represents the ratio of the signal received to the system's noise threshold. The higher the SNR number, the better the line quality. |
| Line Attenuation | This is the difference (in dB) between the power received at the near-end and that transmitted from the far-end.   |
| Data Rate        | This is speed of data transfer on your P-660RU-Tx.   |



# System Logs

## 4.1 Overview

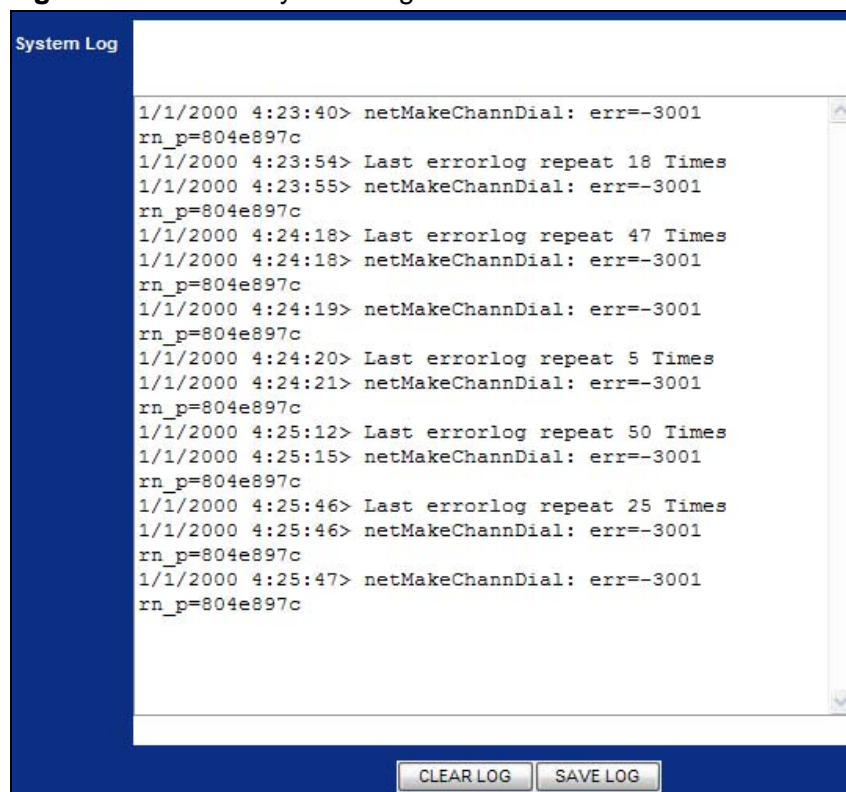
This chapter contains information about viewing the P-660RU-Tx's logs.

A log is a message about an event that occurred on your P-660RU-Tx. For example, when someone logs in to the P-660RU-Tx.

## 4.2 The System Log Screen

Use this screen to see the logs for your P-660RU-Tx. Click **Status > System Log** to open the following screen.

**Figure 6** Status > System Log



The following table describes the fields in this screen.

**Table 4** Status > System Log

| LABEL      | DESCRIPTION  |
|------------|--|
| System Log | This field displays the log messages of your P-660RU-Tx. |
| CLEAR LOG  | Click this to delete all the logs.                       |
| SAVE LOG   | Click this to save the logs in a text file.              |



# Traffic Statistics

## 5.1 Overview

This chapter contains information about viewing traffic statistics of your P-660RU-Tx.

## 5.2 The Statistics Screen

Use this screen to check the traffic statistics of your P-660RU-Tx. Click **Status > Statistics** to open the following screen. The screen varies depending on what type of port you selected in the **Interface** field.

The following screen displays traffic statistics for the Ethernet port.

**Figure 7** Status > Statistics (Ethernet)

| Transmit Statistics       |        | Receive Statistics        |        |
|---------------------------|--------|---------------------------|--------|
| Transmit Frames           | 1013   | Receive Frames            | 2307   |
| Transmit Multicast Frames | 98     | Receive Multicast Frames  | 471    |
| Transmit total Bytes      | 586622 | Receive total Bytes       | 282464 |
| Transmit Collision        | 0      | Receive CRC Errors        | 0      |
| Transmit Error Frames     | 0      | Receive Under-size Frames | 0      |

The following table describes the labels in this screen.

**Table 5** Status > Statistics (Ethernet)

| LABEL                     | DESCRIPTION  |
|---------------------------|--|
| Interface                 | Select <b>Ethernet</b> or <b>ADSL</b> to display traffic statistics on the port. |
| Transmit Statistics       |  |
| Transmit Frames           | This field displays the number of transmitted frames on this port.               |
| Transmit Multicast Frames | This field displays the number of good multicast frames transmitted.             |
| Transmit total Bytes      | This field displays the number of bytes transmitted on this port.                |

**Table 5** Status > Statistics (Ethernet) (continued)

| LABEL                     | DESCRIPTION  |
|---------------------------|--|
| Transmit Collision        | This field displays information on collisions while transmitting frames.   |
| Transmit Error Frames     | This field displays the number of transmitted errors on this port.   |
| Receive Statistics        |  |
| Receive Frames            | This field displays the number of received frames on this port.  |
| Receive Multicast Frames  | This field displays the number of good multicast frames received.  |
| Receive total Bytes       | This field displays the number of bytes received on this port.   |
| Receive CRC errors        | This field displays the number of frames received with Cyclic Redundant Check (CRC) errors.                                  |
| Receive Under-size Frames | This field displays the number of received frames that were under-size (shorter than 60 octets or greater than 1522 octets). |
| REFRESH                   | Click this to update the screen.   |

The following screen displays traffic statistics for the ADSL port.

**Figure 8** Status > Statistics (ADSL)

| Transmit Statistics         |   | Receive Statistics         |   |
|-----------------------------|---|----------------------------|---|
| Transmit total PDUs         | 0 | Receive total PDUs         | 0 |
| Transmit total Error Counts | 0 | Receive total Error Counts | 0 |

The following table describes the labels in this screen.

**Table 6** Status > Statistics (ADSL)

| LABEL                       | DESCRIPTION  |
|-----------------------------|--|
| Transmit Statistics         |  |
| Transmit total PDUs         | This field displays the amount of Protocol Data Units (PDUs) transmitted on this port. |
| Transmit total Error Counts | This field displays the number of error counts transmitted on this port.               |
| Receive Statistics          |  |
| Receive total PDUs          | This field displays the amount of PDUs received on this port.                          |
| Receive total Error Counts  | This field displays the number of error counts received on this port.                  |
| REFRESH                     | Click this to update the screen.   |

# Quick Start Wizard

## 6.1 Overview

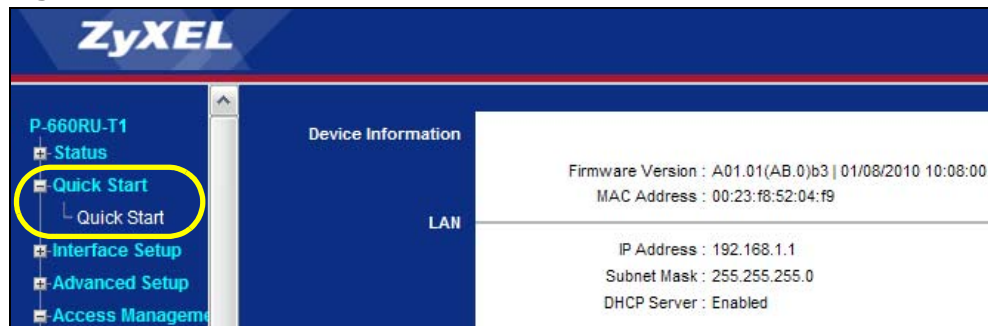
This chapter provides information on the Quick Start Wizard screens. Use the wizard screens to configure your system for Internet access with the information given to you by your ISP.

Note: See the advanced menu chapters for background information on these fields.

## 6.2 Quick Start Wizard

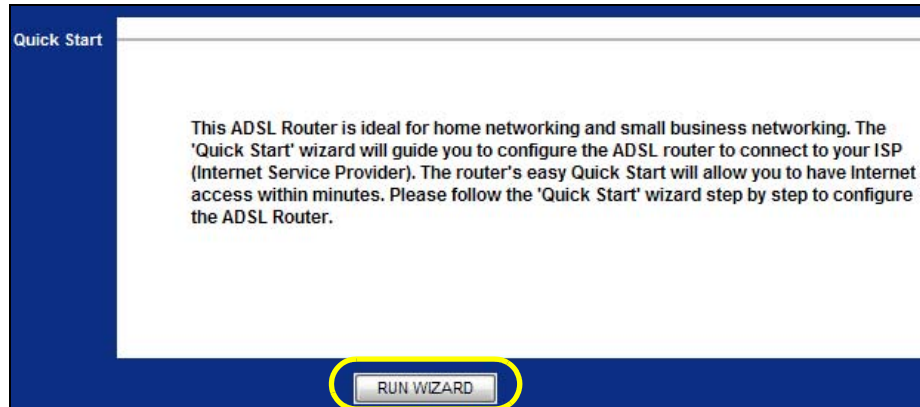
- 1 After you enter the password to access the web configurator, click **Quick Start** > **Quick Start** from the navigation panel to go to the wizard screens.

**Figure 9** Access Quick Start Wizard



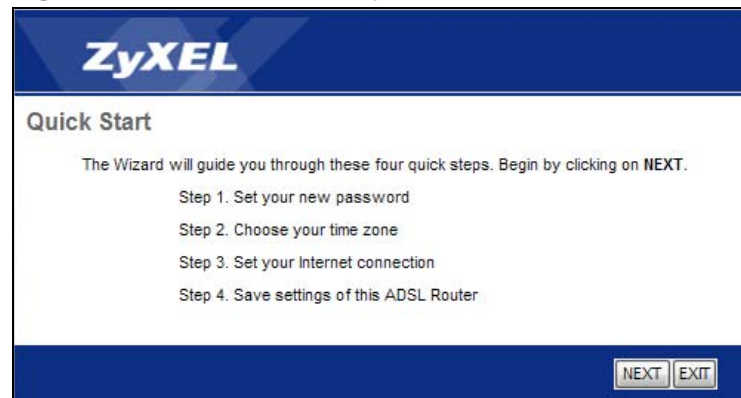
- 2 Click **RUN WIZARD** to configure the system for Internet access.

**Figure 10** Run Wizard



- 3 The following screen summarizes the steps required to configure an Internet connection. Click **NEXT** to begin the setup.

**Figure 11** Wizard Summary



- 4 Enter a new password for accessing the web configurator or enter your old one if you don't want to change it. Type the new or old password in both fields and click **NEXT**.

**Figure 12** Password



**ZyXEL**

Quick Start - Password

You may change the admin account password by entering in a new password. Click **NEXT** to continue.

New Password:

Confirmed Password:

BACK NEXT EXIT

- 5 Select the time zone for your location and click **NEXT**.

**Figure 13** Time Zone

- 6 Select the connection type supported by your ISP and click **NEXT**.

**Figure 14** ISP Connection Type

- 7 The next wizard screen varies depending on what connection type you use. Configure the fields and click **NEXT** to continue.

**Figure 15** ISP Connection: Dynamic IP

The following table describes the fields in this screen.

**Table 7** ISP Connection: Dynamic IP

| LABEL           | DESCRIPTION  |
|-----------------|--|
| VPI             | Enter the VPI (Virtual Path Identifier) assigned to you. This field may already be configured. VPI defines a virtual circuit. Refer to the appendix for more information.  |
| VCI             | Enter the VCI (Virtual Channel Identifier) assigned to you. This field may already be configured. VCI defines a virtual circuit. Refer to the appendix for more information.   |
| Connection Type | Select the multiplexing method used by your ISP from the drop-down list box.<br><br>Available options are: <b>1483 Bridged IP LLC</b> , <b>1483 Bridged IP VC-Mux</b> , <b>1483 Routed IP LLC(IPoA)</b> and <b>1483 Routed IP VC-Mux</b> . |
| BACK            | Click this to return to the previous screen without saving.  |
| NEXT            | Click this to continue to the next wizard screen.  |
| EXIT            | Click this to close the wizard screen without saving.  |

**Figure 16** ISP Connection: Static IP Address

**ZyXEL**

**Quick Start - Static IP Address**

Enter the static IP information provided to you by your ISP. Click **NEXT** to continue.

VPI:  (0~255)

VCI:  (1~65535)

IP Address:

Subnet mask:

ISP Gateway:

Connection Type:  ▼

The following table describes the fields in this screen.

**Table 8** ISP Connection: Static IP Address

| LABEL           | DESCRIPTION  |
|-----------------|--|
| VPI             | Enter the VPI assigned to you. This field may already be configured. VPI defines a virtual circuit. Refer to the appendix for more information.  |
| VCI             | Enter the VCI assigned to you. This field may already be configured. VCI defines a virtual circuit. Refer to the appendix for more information.  |
| IP Address      | Type your ISP assigned IP address in this field.   |
| Subnet mask     | Enter a subnet mask in dotted decimal notation.<br>Refer to the appendix to calculate a subnet mask If you are implementing subnetting.  |
| ISP Gateway     | Specify a gateway IP address supplied by your ISP.   |
| Connection Type | Select the multiplexing method used by your ISP from the drop-down list box.<br><br>Available options are: <b>1483 Bridged IP LLC</b> , <b>1483 Bridged IP VC-Mux</b> , <b>1483 Routed IP LLC(IPoA)</b> and <b>1483 Routed IP VC-Mux</b> . |
| BACK            | Click this to return to the previous screen without saving.  |
| NEXT            | Click this to continue to the next wizard screen.  |
| EXIT            | Click this to close the wizard screen without saving.  |

**Figure 17** ISP Connection: PPPoE/PPPoA

**ZyXEL**

**Quick Start - PPPoE/PPPoA**

Enter the PPPoE/PPPoA information provided to you by your ISP. Click **NEXT** to continue.

Username:

Password:

VPI:  (0~255)

VCI:  (1~65535)

Connection Type:  ▼

The following table describes the fields in this screen.

**Table 9** ISP Connection: PPPoE/PPPoA

| LABEL           | DESCRIPTION  |
|-----------------|--|
| Username        | Enter the username exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.               |
| Password        | Enter the password associated with the above username.   |
| VPI             | Enter the VPI assigned to you. This field may already be configured. VPI defines a virtual circuit. Refer to the appendix for more information.  |
| VCI             | Enter the VCI assigned to you. This field may already be configured. VCI defines a virtual circuit. Refer to the appendix for more information.  |
| Connection Type | Select the multiplexing method used by your ISP from the drop-down list box.<br><br>Available options are: <b>PPPoE LLC</b> , <b>PPPoE VC-Mux</b> , <b>PPPoA LLC</b> and <b>PPPoA VC-Mux</b> . |
| BACK            | Click this to return to the previous screen without saving.  |
| NEXT            | Click this to continue to the next wizard screen.  |
| EXIT            | Click this to close the wizard screen without saving.  |

**Figure 18** ISP Connection: Bridge Mode

The following table describes the fields in this screen.

**Table 10** ISP Connection: Bridge Mode

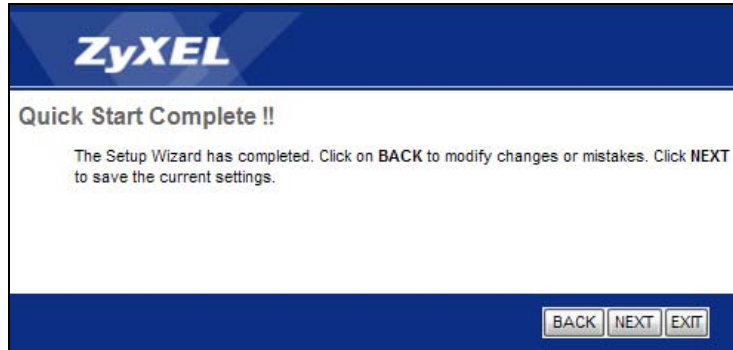
| LABEL           | DESCRIPTION   |
|-----------------|---|
| VPI             | Enter the VPI assigned to you. This field may already be configured. VPI defines a virtual circuit. Refer to the appendix for more information.                           |
| VCI             | Enter the VCI assigned to you. This field may already be configured. VCI defines a virtual circuit. Refer to the appendix for more information.                           |
| Connection Type | Select the multiplexing method used by your ISP from the drop-down list box.<br><br>Available options are: <b>1483 Bridged IP LLC</b> and <b>1483 Bridged IP VC-Mux</b> . |
| BACK            | Click this to return to the previous screen without saving.   |



**Table 10** ISP Connection: Bridge Mode (continued)

| LABEL | DESCRIPTION   |
|-------|---|
| NEXT  | Click this to continue to the next wizard screen.     |
| EXIT  | Click this to close the wizard screen without saving. |

- 8 Click **NEXT** to save your changes and complete the setup.

**Figure 19** Complete Quick Start

- 9 Launch your web browser and navigate to [www.zyxel.com](http://www.zyxel.com). Internet access is just the beginning. Refer to the rest of this guide for more detailed information on the complete range of P-660RU-Tx features. If you cannot access the Internet, open the web configurator again to confirm that the Internet settings you configured in the wizard setup are correct.



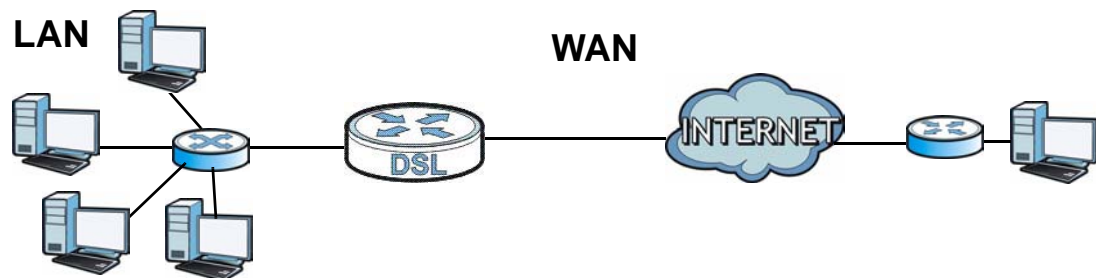
# Internet Setup

## 7.1 Overview

This chapter describes how to configure Wide Area Network (WAN) settings from the **Internet** screens. Use these screens to configure your P-660RU-Tx for Internet access.

A WAN connection is an outside connection to another network or the Internet. It connects your private networks (such as a Local Area Network (LAN) and other networks, so that a computer in one location can communicate with computers in other locations.

**Figure 20** LAN and WAN



### 7.1.1 What You Can Do in the Internet Screens

- Use the **Internet** screen ([Section 7.2 on page 62](#)) to configure the WAN settings on the P-660RU-Tx for Internet access.
- Use the **PVCs Summary** screen ([Section 7.2.5 on page 70](#)) to display a summary table for PVC settings.

### 7.1.2 What You Need to Know About ADSL Internet Access

#### Encapsulation Method

Encapsulation is used to include data from an upper layer protocol into a lower layer protocol. To set up a WAN connection to the Internet, you need to use the same encapsulation method used by your Internet Service Provider (ISP). If your

ISP offers a dial-up Internet connection using PPP over Ethernet (PPPoE) or PPPoA, they should also provide a username and password (and service name) for user authentication.

### **ADSL Terms**

A Permanent Virtual Circuit (PVC) is the connection for your device to the ISP. You need a Virtual Path Identifier (VPI) and a Virtual Channel Identifier (VCI) to identify a PVC. Multiplexing is a way of carrying protocols on a PVC. Your ISP should supply you with all this information.

### **WAN IP Address**

The WAN IP address is an IP address for the P-660RU-Tx, which makes it accessible from an outside network. It is used by the P-660RU-Tx to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the P-660RU-Tx tries to access the Internet.

If your ISP assigns you a static WAN IP address, they should also assign you the subnet mask and DNS server IP address(es) (and a gateway IP address if you use the Ethernet or ENET ENCAP encapsulation method).

### **ATM QoS**

Asynchronous Transfer Mode (ATM) is a LAN and WAN networking technology that provides high-speed data transfer. ATM uses fixed-size packets of information called cells. With ATM, a high QoS (Quality of Service) can be guaranteed. QoS is a service agreement that guarantees certain speed even when the network is congested. ATM QoS is defined by the Peak Cell Rate (PCR), Sustain Cell Rate (SCR) and Maximum Burst Size (MBS).

### **NAT**

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

### **Multicast**

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just one.

## IGMP

Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. There are three versions of IGMP. IGMP version 2 is an improvement over version 1, but IGMP version 1 is still in wide use. IGMP version 3 supports source filtering, reporting or ignoring traffic from specific source address to a particular host on the network.

### Finding Out More

See [Section 7.3 on page 70](#) for technical background information on WAN.

## 7.1.3 Before You Begin

You need to know your Internet access settings such as encapsulation and WAN IP address. Get this information from your ISP.

## 7.2 The Internet Screen

Use this screen to change your P-660RU-Tx's WAN settings. Click **Interface Setup > Internet**. The **Dynamic IP Address** part of this screen differs by the encapsulation you select.

**Figure 21** Interface Setup > Internet

The following table describes the labels in this screen.

**Table 11** Interface Setup > Internet

| LABEL           | DESCRIPTION  |
|-----------------|--|
| ATM VC          |  |
| Virtual Circuit | Select the PVC you want to configure from the drop-down list box.  |
| PVCs Summary    | Click this to display a summary table of the PVC settings on your P-660RU-Tx. See <a href="#">Section 7.2.5 on page 70</a> for more details. |
| Status          | Use this field to enable or disable the PVC.   |
| VPI             | Virtual Path Identifier (VPI) defines a virtual circuit. Refer to the appendix for more information. Enter the VPI assigned to you.          |
| VCI             | Virtual Channel Identifier (VCI) defines a virtual circuit. Enter the VCI assigned to you. Refer to the appendix for more information.       |

**Table 11** Interface Setup > Internet (continued)

| LABEL         | DESCRIPTION   |
|---------------|---|
| QoS           |   |
| ATM QoS       | Select <b>CBR</b> (Continuous Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select <b>UBR</b> (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select <b>rtVBR</b> (real-time Variable Bit Rate) for applications with bursty connections that require closely controlled delay and delay variation. Select <b>nrtVBR</b> (non real-time Variable Bit Rate) for connections that do not require closely controlled delay and delay variation. |
| PCR           | Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR in this field.  |
| SCR           | The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.   |
| MBS           | Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.   |
| Encapsulation | Select the connection type supported by your ISP. The next fields vary depending on what connection type you use. See the following sections for more details.  |
| SAVE          | Click this to save your changes.  |
| DELETE        | Click this to restore the PVC to default settings.  |

## 7.2.1 Dynamic IP Address

In the **Interface Setup > Internet** screen, select **Dynamic IP Address** from the **ISP** field to display the following screen.

**Figure 22** Interface Setup > Internet (Dynamic IP)

The screenshot displays the configuration interface for a Dynamic IP address. The left sidebar is labeled 'Dynamic IP'. The main content area shows the following settings:

- ISP:**  Dynamic IP Address,  Static IP Address,  PPPoA/PPPoE,  Bridge Mode
- Encapsulation:** 1483 Bridged IP LLC (dropdown menu)
- Bridge Interface:**  Activated,  Deactivated
- NAT:** Enable (dropdown menu)
- Default Route:**  Yes,  No
- TCP MTU Option:** TCP MTU(0:default) 0 bytes
- Dynamic Route:** RIP1 (dropdown menu), Direction Both (dropdown menu)
- Multicast:** Disabled (dropdown menu)
- MAC Spoofing:**  Enabled,  Disabled
- MAC Address:** 00:00:00:00:00:00 (text input field)

The following table describes the labels in this screen.

**Table 12** Interface Setup > Internet (Dynamic IP)

| LABEL            | DESCRIPTION  |
|------------------|--|
| Encapsulation    | Select the method of multiplexing used by your ISP from the drop-down list box. Available options are: <b>1483 Bridged IP LLC</b> , <b>1483 Bridged IP VC-Mux</b> , <b>1483 Routed IP LLC(IPoA)</b> and <b>1483 Routed IP VC-Mux</b> .   |
| Bridge Interface | This field is only available when you select <b>1483 Bridged IP LLC</b> or <b>1483 Bridged IP VC-Mux</b> in the <b>Encapsulation</b> field.<br><br>Use this field to enable or disable the bridge mode. Activate the bridge mode when your ISP provides you with more than one IP address and you want the connected computers to get individual IP address from ISP's DHCP server directly.                           |
| NAT              | Use this field to enable or disable Network Address Translation (NAT).   |
| Default Route    | Select <b>Yes</b> to direct traffic not listed in the routing table to the default gateway.<br><br>Select <b>No</b> to drop traffic not listed in the routing table.   |
| TCP MTU Option   | The Maximum Transmission Unit (MTU) defines the size of the largest packet allowed on an interface or connection. Enter the MTU in this field.   |
| Dynamic Route    | RIP (Routing Information Protocol) allows a router to exchange routing information with other routers.<br><br>Select the RIP version from <b>RIP1</b> , <b>RIP2-B</b> and <b>RIP2-M</b> .  |
| Direction        | Use this field to control how much routing information the P-660RU-Tx sends and receives on the subnet.<br><br>Select the RIP direction from <b>None</b> , <b>Both</b> , <b>IN Only</b> and <b>OUT Only</b> .  |
| Multicast        | Multicast packets are sent to a group of computers on the LAN and are an alternative to unicast packets (packets sent to one computer) and broadcast packets (packets sent to every computer).<br><br>IGMP is a network-layer protocol used to establish membership in a multicast group. The P-660RU-Tx supports <b>IGMP v1</b> , <b>IGMP v2</b> and <b>IGMP v3</b> . Select <b>Disabled</b> to turn off the feature. |
| MAC Spoofing     | This field is only available when you select <b>1483 Bridged IP LLC</b> or <b>1483 Bridged IP VC-Mux</b> in the <b>Encapsulation</b> field.<br><br>Select <b>Enable</b> to alter the MAC address that you entered below so that the PVCs on the P-660RU-Tx can establish connections to the network.   |



## 7.2.2 Static IP Address

In the **Interface Setup > Internet** screen, select **Static IP Address** from the **ISP** field to display the following screen.

**Figure 23** Interface Setup > Internet (Static IP)

The following table describes the labels in this screen.

**Table 13** Interface Setup > Internet (Static IP)

| LABEL             | DESCRIPTION  |
|-------------------|--|
| Encapsulation     | Select the method of multiplexing used by your ISP from the drop-down list box. Available options are: <b>1483 Bridged IP LLC</b> , <b>1483 Bridged IP VC-Mux</b> , <b>1483 Routed IP LLC(IPoA)</b> and <b>1483 Routed IP VC-Mux</b> .   |
| Static IP Address | A static IP address is a fixed IP that your ISP gives you. Type your ISP assigned IP address in the field.   |
| IP Subnet Mask    | Enter a subnet mask in dotted decimal notation.  |
| Gateway           | Specify a gateway IP address (supplied by your ISP).   |
| Bridge Interface  | This field is only available when you select <b>1483 Bridged IP LLC</b> or <b>1483 Bridged IP VC-Mux</b> in the <b>Encapsulation</b> field.<br><br>Use this field to enable or disable the bridge mode. Activate the bridge mode when your ISP provides you with more than one IP address and you want the connected computers to get individual IP address from ISP's DHCP server directly. |
| NAT               | Use this field to enable or disable Network Address Translation (NAT).   |
| Default Route     | Select <b>Yes</b> to direct traffic not listed in the routing table to the default gateway. Select <b>No</b> to drop traffic not listed in the routing table.  |

**Table 13** Interface Setup > Internet (Static IP) (continued)

| LABEL          | DESCRIPTION  |
|----------------|--|
| TCP MTU Option | The Maximum Transmission Unit (MTU) defines the size of the largest packet allowed on an interface or connection. Enter the MTU in this field.   |
| Dynamic Route  | RIP (Routing Information Protocol) allows a router to exchange routing information with other routers.<br><br>Select the RIP version from <b>RIP1</b> , <b>RIP2-B</b> and <b>RIP2-M</b> .  |
| Direction      | Use this field to control how much routing information the P-660RU-Tx sends and receives on the subnet.<br><br>Select the RIP direction from <b>None</b> , <b>Both</b> , <b>IN Only</b> and <b>OUT Only</b> .  |
| Multicast      | Multicast packets are sent to a group of computers on the LAN and are an alternative to unicast packets (packets sent to one computer) and broadcast packets (packets sent to every computer).<br><br>IGMP is a network-layer protocol used to establish membership in a multicast group. The P-660RU-Tx supports <b>IGMP v1</b> , <b>IGMP v2</b> and <b>IGMP v3</b> . Select <b>Disabled</b> to turn off the feature. |
| MAC Spoofing   | This field is only available when you select <b>1483 Bridged IP LLC</b> or <b>1483 Bridged IP VC-Mux</b> in the <b>Encapsulation</b> field.<br><br>Select <b>Enable</b> to alter the MAC address that you entered below so that the PVCs on the P-660RU-Tx can establish connections to the network.   |

## 7.2.3 PPPoA/PPPoE

In the **Interface Setup > Internet** screen, select **PPPoA/PPPoE** from the **ISP** field to display the following screen.

**Figure 24** Interface Setup > Internet (PPPoA/PPPoE)

The following table describes the labels in this screen.

**Table 14** Interface Setup > Internet (PPPoA/PPPoE)

| LABEL         | DESCRIPTION  |
|---------------|--|
| PPPoE/PPPoA   |  |
| Servicename   | Type the name of your service in this field.   |
| Username      | Enter the username exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.           |
| Password      | Enter the password associated with the username above.   |
| Encapsulation | Select the method of multiplexing used by your ISP from the drop-down list box. Available options are: <b>PPPoE LLC</b> , <b>PPPoE VC-Mux</b> , <b>PPPoA LLC</b> and <b>PPPoA VC-Mux</b> . |

**Table 14** Interface Setup > Internet (PPPoA/PPPoE) (continued)

| LABEL              | DESCRIPTION  |
|--------------------|--|
| Bridge Interface   | <p>This field is only available when you select <b>PPPoE LLC</b> or <b>PPPoE VC-Mux</b> in the <b>Encapsulation</b> field.</p> <p>Use this field to enable or disable the bridge mode. Activate the bridge mode when your ISP provides you with more than one IP address and you want the connected computers to get individual IP address from ISP's DHCP server directly.</p>  |
| Connection Setting |  |
| Connection         | <p>Select <b>Always On (Recommended)</b> when you want your connection up all the time. The P-660RU-Tx will try to bring up the connection automatically if it is disconnected.</p> <p>Select <b>Connect On-Demand</b> when you don't want the connection up all the time and specify an idle time-out in minutes. The default setting is 0 minute, which means the Internet session will not timeout.</p> <p>Select <b>Connect Manually</b> to establish the connection only when you need it.</p> <p><b>Note:</b> Do not specify an always-on connection unless your telephone company offers flat-rate service or you need a constant connection and the cost is of no concern.</p> |
| TCP MSS Option     | <p>The TCP Maximum Segment Size (MSS) defines the size of the largest packet allowed on an interface or connection. Enter the TCP MSS in this field. In general, the TCP MSS is 1452.</p>  |
| IP Address         |  |
| Get IP Address     | <p>Select the type of IP address provided by your ISP. A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet.</p>  |
| Static IP Address  | <p>Type your ISP assigned IP address in the field.</p>   |
| IP Subnet Mask     | <p>Enter a subnet mask in dotted decimal notation.</p>   |
| Gateway            | <p>Specify a gateway IP address (supplied by your ISP).</p>  |
| NAT                | <p>Use this field to enable or disable Network Address Translation (NAT).</p>  |
| Default Route      | <p>Select <b>Yes</b> to direct traffic not listed in the routing table to the default gateway. Select <b>No</b> to drop traffic not listed in the routing table.</p>   |
| TCP MTU Option     | <p>The Maximum Transmission Unit (MTU) defines the size of the largest packet allowed on an interface or connection. Enter the MTU in this field.</p>  |
| Dynamic Route      | <p>RIP (Routing Information Protocol) allows a router to exchange routing information with other routers.</p> <p>Select the RIP version from <b>RIP1</b>, <b>RIP2-B</b> and <b>RIP2-M</b>.</p>   |
| Direction          | <p>Use this field to control how much routing information the P-660RU-Tx sends and receives on the subnet.</p> <p>Select the RIP direction from <b>None</b>, <b>Both</b>, <b>IN Only</b> and <b>OUT Only</b>.</p>  |

**Table 14** Interface Setup > Internet (PPPoA/PPPoE) (continued)

| LABEL        | DESCRIPTION  |
|--------------|--|
| Multicast    | Multicast packets are sent to a group of computers on the LAN and are an alternative to unicast packets (packets sent to one computer) and broadcast packets (packets sent to every computer).<br><br>IGMP is a network-layer protocol used to establish membership in a multicast group. The P-660RU-Tx supports <b>IGMP v1</b> , <b>IGMP v2</b> and <b>IGMP v3</b> . Select <b>Disabled</b> to turn off the feature. |
| MAC Spoofing | This field is only available when you select <b>1483 Bridged IP LLC</b> or <b>1483 Bridged IP VC-Mux</b> in the <b>Encapsulation</b> field.<br><br>Select <b>Enable</b> to alter the MAC address that you entered below so that the PVCs on the P-660RU-Tx can establish connections to the network.   |

## 7.2.4 Bridge Mode

In the **Interface Setup > Internet** screen, select **Bridge Mode** from the **ISP** field to display the following screen.

**Figure 25** Interface Setup > Internet (Bridge)

The following table describes the labels in this screen.

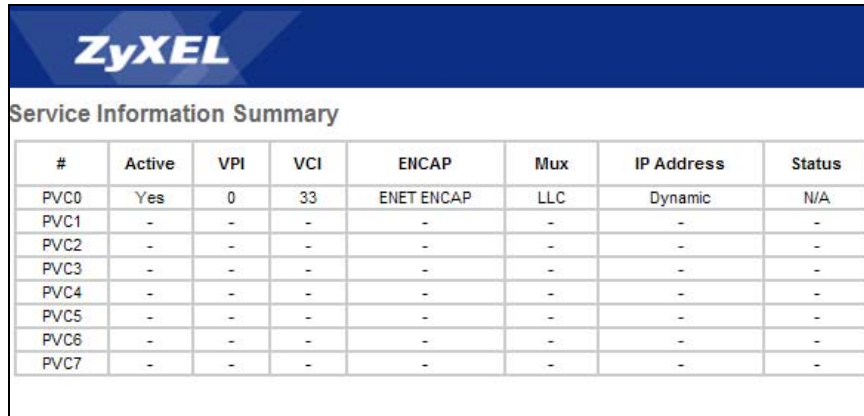
**Table 15** Interface Setup > Internet (Bridge)

| LABEL       | DESCRIPTION   |
|-------------|---|
| Bridge Mode | Select the method of multiplexing used by your ISP from the drop-down list box. Available options are: <b>1483 Bridged IP LLC</b> and <b>1483 Bridged IP VC-Mux</b> . |

## 7.2.5 The PVCs Summary Screen

Use this field to check your PVC settings. In the **Interface Setup > Internet** screen, click **PVCs Summary** in the **Virtual Circuit** field to display the following screen.

**Figure 26** Interface Setup > PVCs Summary



The screenshot shows the ZyXEL logo at the top left. Below it is the title "Service Information Summary". A table lists PVC settings for PVC0 through PVC7. PVC0 is active, while others are inactive. PVC0 uses ENET encapsulation and LLC multiplexing with a dynamic IP address. Other PVCs use default settings.

| #    | Active | VPI | VCI | ENCAP      | Mux | IP Address | Status |
|------|--------|-----|-----|------------|-----|------------|--------|
| PVC0 | Yes    | 0   | 33  | ENET ENCAP | LLC | Dynamic    | N/A    |
| PVC1 | -      | -   | -   | -          | -   | -          | -      |
| PVC2 | -      | -   | -   | -          | -   | -          | -      |
| PVC3 | -      | -   | -   | -          | -   | -          | -      |
| PVC4 | -      | -   | -   | -          | -   | -          | -      |
| PVC5 | -      | -   | -   | -          | -   | -          | -      |
| PVC6 | -      | -   | -   | -          | -   | -          | -      |
| PVC7 | -      | -   | -   | -          | -   | -          | -      |

The following table describes the labels in this screen.

**Table 16** Interface Setup > PVCs Summary

| LABEL      | DESCRIPTION   |
|------------|---|
| #          | This field displays the index number for the corresponding PVC. |
| Active     | This field displays whether the PVC is activated.               |
| VPI        | This field displays the VPI value.                              |
| VCI        | This field displays the VCI value.                              |
| ENCAP      | This field displays the type of encapsulation.                  |
| Mux        | This field displays the multiplexing method.                    |
| IP Address | This field displays the type of IP address.                     |
| Status     | This field displays the connection status of the PVC.           |

## 7.3 WAN Technical Reference

This section provides some technical background information about the topics covered in this chapter.

### 7.3.1 Encapsulation

Be sure to use the encapsulation method required by your ISP. The P-660RU-Tx supports the following methods.

## PPP over Ethernet

The P-660RU-Tx supports Point-to-Point Protocol over Ethernet (PPPoE). PPPoE is an IETF Draft standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The PPPoE option is for a dial-up connection using PPPoE.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example RADIUS).

One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the P-660RU-Tx (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the P-660RU-Tx does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

## PPPoA

PPPoA stands for Point to Point Protocol over ATM Adaptation Layer 5 (AAL5). A PPPoA connection functions like a dial-up Internet connection. The P-660RU-Tx encapsulates the PPP session based on RFC1483 and sends it through an ATM PVC (Permanent Virtual Circuit) to the Internet Service Provider's (ISP) DSLAM (Digital Subscriber Line (DSL) Access Multiplexer). Please refer to RFC 2364 for more information on PPPoA. Refer to RFC 1661 for more information on PPP.

## RFC 1483

RFC 1483 describes two methods for Multiprotocol Encapsulation over ATM Adaptation Layer 5 (AAL5). The first method allows multiplexing of multiple protocols over a single ATM virtual circuit (LLC-based multiplexing) and the second method assumes that each protocol is carried over a separate ATM virtual circuit (VC-based multiplexing). Please refer to RFC 1483 for more detailed information.

## 7.3.2 Multiplexing

There are two conventions to identify what protocols the virtual circuit (VC) is carrying. Be sure to use the multiplexing method required by your ISP.

### **VC-based Multiplexing**

In this case, by prior mutual agreement, each protocol is assigned to a specific virtual circuit; for example, VC1 carries IP, etc. VC-based multiplexing may be dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical.

### **LLC-based Multiplexing**

In this case one VC carries multiple protocols with protocol identifying information being contained in each packet header. Despite the extra bandwidth and processing overhead, this method may be advantageous if it is not practical to have a separate VC for each carried protocol, for example, if charging heavily depends on the number of simultaneous VCs.

## **7.3.3 VPI and VCI**

Be sure to use the correct Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) numbers assigned to you. The valid range for the VPI is 0 to 255 and for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Please see the appendix for more information.

## **7.3.4 IP Address Assignment**

A static IP is a fixed IP that your ISP gives you. A dynamic IP is not fixed; the ISP assigns you a different one each time. However the encapsulation method assigned influences your choices for IP address.

### **IP Assignment with PPPoA or PPPoE Encapsulation**

If you have a dynamic IP, then the **IP Address** and **Gateway IP Address** fields are not applicable (N/A). If you have a static IP, then you only need to fill in the **IP Address** field and not the **Gateway IP Address** field.

### **IP Assignment with RFC 1483 Encapsulation**

In this case the IP address assignment must be static.

## **7.3.5 Always-On Connection (PPP)**

An always-on connection is a dial-up line where the connection is always up regardless of traffic demand. The P-660RU-Tx does two things when you specify an always-on connection. The first is that idle timeout is disabled. The second is that the P-660RU-Tx will try to bring up the connection when turned on and



whenever the connection is down. An always-on connection can be very expensive for obvious reasons.

Do not specify an always-on connection unless your telephone company offers flat-rate service or you need a constant connection and the cost is of no concern.

### 7.3.6 ATM QoS

ATM QoS is an agreement between the carrier and the subscriber to regulate the average rate and fluctuations of data transmission over an ATM network. This agreement helps eliminate congestion, which is important for transmission of real time data such as audio and video connections.

Peak Cell Rate (PCR) is the maximum rate at which the sender can send cells. This parameter may be lower (but not higher) than the maximum line speed. 1 ATM cell is 53 bytes (424 bits), so a maximum speed of 832Kbps gives a maximum PCR of 1962 cells/sec. This rate is not guaranteed because it is dependent on the line speed.

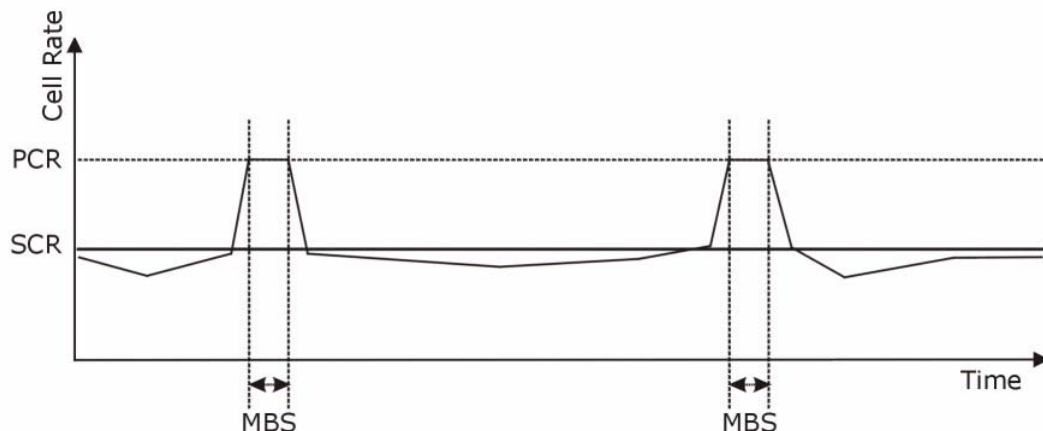
Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

Maximum Burst Size (MBS) is the maximum number of cells that can be sent at the PCR. After MBS is reached, cell rates fall below SCR until cell rate averages to the SCR again. At this time, more cells (up to the MBS) can be sent at the PCR again.

If the PCR, SCR or MBS is set to the default of "0", the system will assign a maximum value that correlates to your upstream line rate.

The following figure illustrates the relationship between PCR, SCR and MBS.

**Figure 27** Example of ATM OoS



## 7.3.7 ATM Traffic Classes

These are the basic ATM traffic classes defined by the ATM Forum Traffic Management 4.0 Specification.

### **Constant Bit Rate (CBR)**

Constant Bit Rate (CBR) provides fixed bandwidth that is always available even if no data is being sent. CBR traffic is generally time-sensitive (doesn't tolerate delay). CBR is used for connections that continuously require a specific amount of bandwidth. A PCR is specified and if traffic exceeds this rate, cells may be dropped. Examples of connections that need CBR would be high-resolution video and voice.

### **Variable Bit Rate (VBR)**

The Variable Bit Rate (VBR) ATM traffic class is used with bursty connections. Connections that use the Variable Bit Rate (VBR) traffic class can be grouped into real time (VBR-RT) or non-real time (VBR-nRT) connections.

The VBR-RT (real-time Variable Bit Rate) type is used with bursty connections that require closely controlled delay and delay variation. It also provides a fixed amount of bandwidth (a PCR is specified) but is only available when data is being sent. An example of an VBR-RT connection would be video conferencing. Video conferencing requires real-time data transfers and the bandwidth requirement varies in proportion to the video image's changing dynamics.

The VBR-nRT (non real-time Variable Bit Rate) type is used with bursty connections that do not require closely controlled delay and delay variation. It is commonly used for "bursty" traffic typical on LANs. PCR and MBS define the burst levels, SCR defines the minimum level. An example of an VBR-nRT connection would be non-time sensitive data file transfers.

### **Unspecified Bit Rate (UBR)**

The Unspecified Bit Rate (UBR) ATM traffic class is for bursty data transfers. However, UBR doesn't guarantee any bandwidth and only delivers traffic when the network has spare bandwidth. An example application is background file transfer.

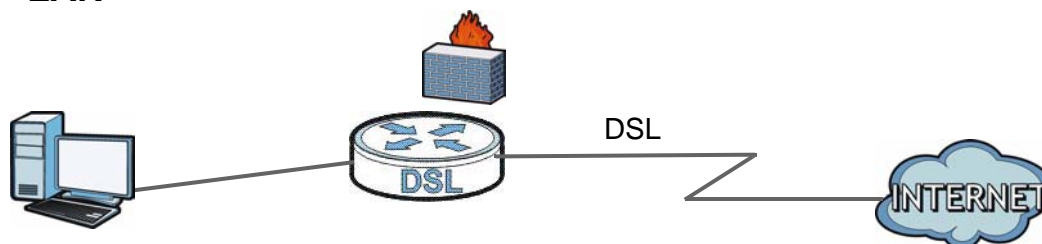
# LAN Setup

## 8.1 Overview

A Local Area Network (LAN) is a shared communication system to which many networking devices are connected. It is usually located in one area such as a building or floor of a building.

Use the LAN screen to help you configure a LAN DHCP server and manage IP addresses.

### LAN



### 8.1.1 What You Can Do in the LAN Screens

- Use the **LAN** screen ([Section 8.2 on page 77](#)) to set the LAN IP address and subnet mask of your ZyXEL device. You can also edit your P-660RU-Tx's RIP, multicast and DHCP settings from this screen.
- Use the **DHCP IP Pool Summary** screen ([Section 8.2.1 on page 79](#)) to check the IP and MAC addresses of the computers on your LAN.

### 8.1.2 What You Need To Know About LAN

#### IP Address

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

## Subnet Mask

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

## DHCP

A DHCP (Dynamic Host Configuration Protocol) server can assign your P-660RU-Tx an IP address, subnet mask, DNS and other routing information when it's turned on.

## RIP

RIP (Routing Information Protocol) allows a router to exchange routing information with other routers.

## Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

## IGMP

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. There are three versions of IGMP. IGMP version 2 is an improvement over version 1, but IGMP version 1 is still in wide use. IGMP version 3 supports source filtering, reporting or ignoring traffic from specific source address to a particular host on the network.

## DNS

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a networking device before you can access it.

## Finding Out More

See [Section 8.3 on page 79](#) for technical background information on LANs.

## 8.2 The LAN Screen

Use this screen to configure your LAN settings. Click **Interface Setup > LAN** to display the following screen.

Follow these steps to configure your LAN settings.

- 1 Enter an IP address into the **IP Address** field. The IP address must be in dotted decimal notation. This will become the IP address of your P-660RU-Tx.
- 2 Enter the IP subnet mask into the **IP Subnet Mask** field. Unless instructed otherwise it is best to leave this alone, the configurator will automatically compute a subnet mask based upon the IP address you entered.
- 3 Click **SAVE** to save your settings.

**Figure 28** Interface Setup > LAN

The following table describes the fields in this screen.

**Table 17** Interface Setup > LAN

| LABEL           | DESCRIPTION   |
|-----------------|---|
| Router Local IP |   |
| IP Address      | Enter the LAN IP address you want to assign to your P-660RU-Tx in dotted decimal notation, for example, 192.168.1.1 (factory default).  |
| IP Subnet Mask  | Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your P-660RU-Tx automatically computes the subnet mask based on the IP Address you enter, so do not change this field unless you are instructed to do so. |

**Table 17** Interface Setup > LAN

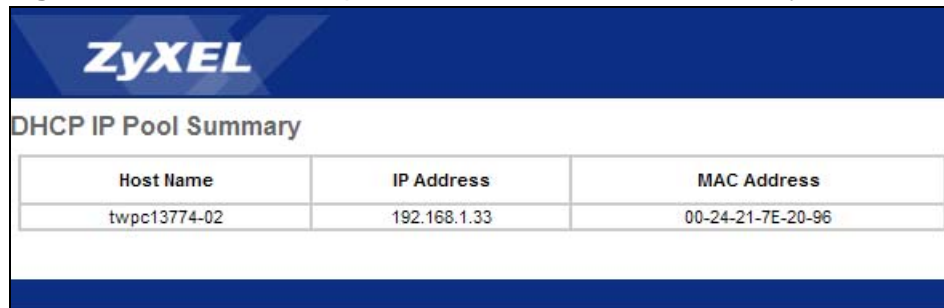
| LABEL                | DESCRIPTION  |
|----------------------|--|
| Dynamic Route        | RIP (Routing Information Protocol) allows a router to exchange routing information with other routers.<br><br>Select the RIP version from <b>RIP1</b> , <b>RIP2-B</b> and <b>RIP2-M</b> .  |
| Direction            | Use this field to control how much routing information the P-660RU-Tx sends and receives on the subnet.<br><br>Select the RIP direction from <b>None</b> , <b>Both</b> , <b>IN Only</b> and <b>OUT Only</b> .  |
| Multicast            | Multicast packets are sent to a group of computers on the LAN and are an alternative to unicast packets (packets sent to one computer) and broadcast packets (packets sent to every computer).<br><br>IGMP is a network-layer protocol used to establish membership in a multicast group. The P-660RU-Tx supports <b>IGMP v1</b> , <b>IGMP v2</b> and <b>IGMP v3</b> . Select <b>Disabled</b> to turn off the feature. |
| DHCP                 |  |
| DHCP                 | If set to <b>Enabled</b> , your P-660RU-Tx can assign IP addresses, an IP default gateway and DNS servers to operating systems that support the DHCP client.<br><br>If set to <b>Disabled</b> , the DHCP server will be disabled.<br><br>If set to <b>Relay</b> , the P-660RU-Tx acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients.                     |
| DHCP Server          |  |
| Starting IP Address  | This field specifies the first of the contiguous addresses in the IP address pool.   |
| Current Pool Summary | Click this to display a summary table for the IP address pool. See <a href="#">Section 8.2.1 on page 79</a> for more details.<br><br>The P-660RU-Tx is pre-configured with a pool of IP addresses for the DHCP clients (DHCP Pool). See the product specifications in the appendices. Do not assign static IP addresses from the DHCP pool to your LAN computers.  |
| IP Pool Count        | This field specifies the size, or count of the IP address pool.  |
| Lease Time           | This is the period of time DHCP-assigned addresses is used.<br><br>DHCP automatically assigns IP addresses to clients when they log in. DHCP centralizes IP address management on central computers that run the DHCP server program. DHCP leases addresses, for a period of time, which means that past addresses are “recycled” and made available for future reassignment to other systems.                         |
| DNS                  |  |
| DNS Relay            | Select <b>Auto Discovered DNS Server Only</b> if your ISP dynamically assigns DNS server information (and the P-660RU-Tx's WAN IP address).<br><br>Select <b>User Discovered DNS Server Only</b> if you have the IP address of a DNS server. You have to specify the primary and secondary DNS servers in the following fields.  |

**Table 17** Interface Setup > LAN

| LABEL                          | DESCRIPTION   |
|--------------------------------|---|
| Primary DNS Server             | Enter the IP address for the primary DNS server.  |
| Secondary DNS Server           | Enter the IP address for the secondary DNS server.  |
| DHCP Server IP for Relay Agent | This field is only available when you select <b>Relay</b> in the <b>DNS Relay</b> field. Enter the IP address of the actual remote DHCP server in this field. |
| SAVE                           | Click this to save your changes.  |
| CANCEL                         | Click this to restore your previously saved settings.   |

## 8.2.1 The DHCP IP Pool Summary Screen

This table allows you to see the IP and Media Access Control (MAC) addresses of individual computers on your LAN. In the **Interface Setup > LAN** screen, click the **Current Pool Summary** button to open the following screen.

**Figure 29** Interface Setup > LAN > DHCP IP Pool Summary


| ZyXEL                |              |                   |
|----------------------|--------------|-------------------|
| DHCP IP Pool Summary |              |                   |
| Host Name            | IP Address   | MAC Address       |
| twpc13774-02         | 192.168.1.33 | 00-24-21-7E-20-96 |

The following table describes the labels in this screen.

**Table 18** Interface Setup > LAN > DHCP IP Pool Summary

| LABEL       | DESCRIPTION  |
|-------------|--|
| Host Name   | This field displays the name of a computer that receives an IP address from the P-660RU-Tx.        |
| IP Address  | This field displays the IP address of a computer that receives an IP address from the P-660RU-Tx.  |
| MAC Address | This field displays the MAC address of a computer that receives an IP address from the P-660RU-Tx. |

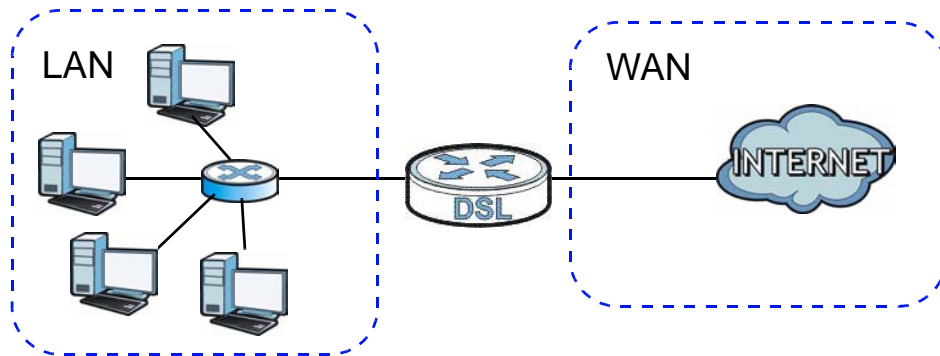
## 8.3 LAN Technical Reference

This section provides some technical background information about the topics covered in this chapter.

### 8.3.1 LANs, WANs and the ZyXEL Device

The actual physical connection determines whether the P-660RU-Tx ports are LAN or WAN ports. There are two separate IP networks, one inside the LAN network and the other outside the WAN network as shown next.

**Figure 30** LAN and WAN IP Addresses



### 8.3.2 DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the P-660RU-Tx as a DHCP server or disable it. When configured as a server, the P-660RU-Tx provides the TCP/IP configuration for the clients. If you turn DHCP service off, you must have another DHCP server on your LAN, or else the computer must be manually configured.

### 8.3.3 DNS Server Addresses

DNS (Domain Name System) maps a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The DNS server addresses you enter when you set up DHCP are passed to the client machines along with the assigned IP address and subnet mask.

There are two ways that an ISP disseminates the DNS server addresses.

- The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the **Primary** and **Secondary DNS Server** fields.



- Some ISPs choose to disseminate the DNS server addresses using the DNS server extensions of IPCP (IP Control Protocol) after the connection is up. If your ISP did not give you explicit DNS servers, chances are the DNS servers are conveyed through IPCP negotiation. The P-660RU-Tx supports the IPCP DNS server extensions through the DNS proxy feature.

If the DHCP is set to **Relay**, the P-660RU-Tx tells the DHCP clients that it itself is the DNS server. When a computer sends a DNS query to the P-660RU-Tx, the P-660RU-Tx acts as a DNS proxy and forwards the query to the real DNS server learned through IPCP and relays the response back to the computer.

Please note that DNS proxy works only when the ISP uses the IPCP DNS server extensions. It does not mean you can leave the DNS servers out of the DHCP setup under all circumstances. If your ISP gives you explicit DNS servers, make sure that you enter their IP addresses.

### 8.3.4 LAN TCP/IP

The P-660RU-Tx has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

#### IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the P-660RU-Tx. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your P-660RU-Tx, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your P-660RU-Tx will compute the subnet mask automatically based on the IP address

that you entered. You don't need to change the subnet mask computed by the P-660RU-Tx unless you are instructed to do otherwise.

### Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet, for example, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

**Note:** Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, "Address Allocation for Private Internets" and RFC 1466, "Guidelines for Management of IP Address Space".

## 8.3.5 RIP Setup

RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. When set to:

- **Both** - the P-660RU-Tx will broadcast its routing table periodically and incorporate the RIP information that it receives.
- **In Only** - the P-660RU-Tx will not send any RIP packets but will accept all RIP packets received.
- **Out Only** - the P-660RU-Tx will send out RIP packets but will not accept any RIP packets received.
- **None** - the P-660RU-Tx will not send any RIP packets and will ignore any RIP packets received.

The **Version** field controls the format and the broadcasting method of the RIP packets that the P-660RU-Tx sends (it recognizes both formats when receiving). RIP-1 is universally supported; but RIP-2 carries more information. RIP-1 is

probably adequate for most networks, unless you have an unusual network topology.

Both RIP-2B and RIP-2M sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting.

### 8.3.6 Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. IGMP version 3 supports source filtering, reporting or ignoring traffic from specific source address to a particular host on the network. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

The P-660RU-Tx supports IGMP version 1 (**IGMP-v1**), IGMP version 2 (**IGMP-v2**) and IGMP version 3 (**IGMP-v3**). At start up, the P-660RU-Tx queries all directly connected networks to gather group membership. After that, the P-660RU-Tx periodically updates this information. IP multicasting can be enabled/disabled on the P-660RU-Tx LAN and/or WAN interfaces in the web configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.



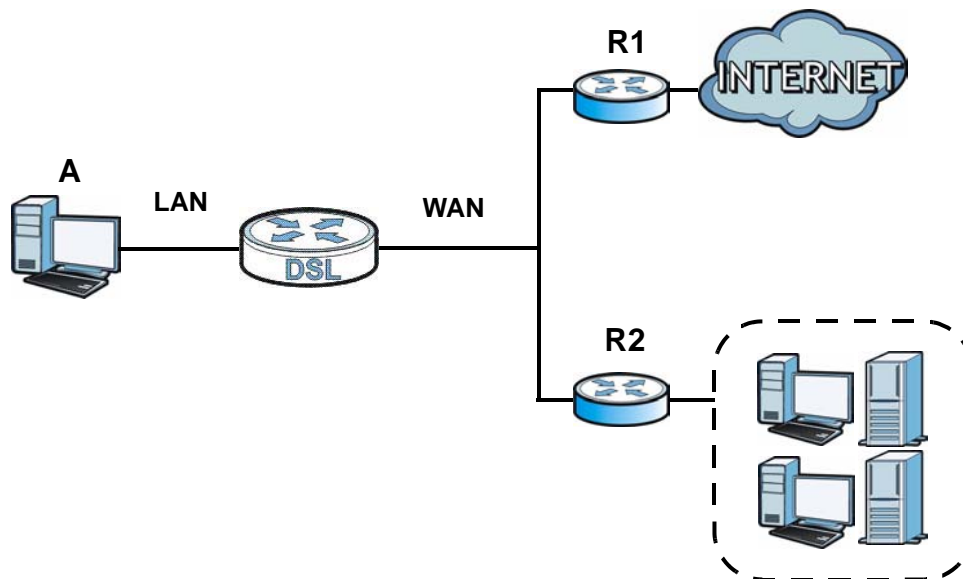
# Static Route

## 9.1 Overview

The P-660RU-Tx usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the P-660RU-Tx send data to devices not reachable through the default gateway, use static routes.

For example, the next figure shows a computer (**A**) connected to the P-660RU-Tx's LAN interface. The P-660RU-Tx routes most traffic from **A** to the Internet through the P-660RU-Tx's default gateway (**R1**). You create one static route to connect to services offered by your ISP behind router **R2**.

**Figure 31** Example of Static Routing Topology



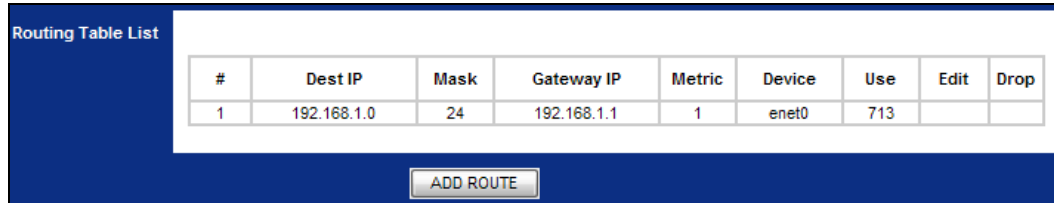
### 9.1.1 What You Can Do in the Static Route Screens

- Use the **Routing Table List** screen ([Section 9.2 on page 86](#)) to view static routes on the P-660RU-Tx.
- Use the **Static Route** screen ([Section 9.2.1 on page 87](#)) to add or edit IP static routes on the P-660RU-Tx.

## 9.2 The Routing Table List Screen

Use this screen to view the static route rules. Click **Advanced Setup > Routing** to display the following screen.

**Figure 32** Advanced Setup > Routing Table List



| # | Dest IP     | Mask | Gateway IP  | Metric | Device | Use | Edit | Drop |
|---|-------------|------|-------------|--------|--------|-----|------|------|
| 1 | 192.168.1.0 | 24   | 192.168.1.1 | 1      | enet0  | 713 |      |      |

The following table describes the labels in this screen.

**Table 19** Advanced Setup > Routing Table List

| LABEL      | DESCRIPTION  |
|------------|--|
| #          | This is the number of an individual static route.  |
| Dest IP    | This parameter specifies the IP network address of the final destination. Routing is always based on network number.   |
| Mask       | This parameter specifies the IP network subnet mask of the final destination.  |
| Gateway IP | This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations. |
| Metric     | This field displays the priority of each route on the P-660RU-Tx.  |
| Device     | This is the name that describes or identifies this route.  |
| Use        | This is the number of times the route was used.  |
| Edit       | Click this to go to the screen where you can set up a static route on the P-660RU-Tx. You cannot edit the default routes.  |
| Drop       | Click this to remove a static route from the P-660RU-Tx. You cannot delete the default routes.   |
| ADD ROUTE  | Click this to add a new static route on the P-660RU-Tx.  |

## 9.2.1 The Static Route Screen

Use this screen to configure the required information for a static route. Select a static route index number and click **Edit**, or click the **ADD ROUTE** button in the **Routing Table List** screen. The screen shown next appears.

**Figure 33** Advanced > Routing > Static Route

The following table describes the labels in this screen.

**Table 20** Advanced > Static Route: Edit

| LABEL                  | DESCRIPTION  |
|------------------------|--|
| Destination IP Address | This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.  |
| IP Subnet Mask         | Enter the IP subnet mask in this field.  |
| Gateway IP Address     | <p>You can set the static route using a gateway IP address or a remote node.</p> <p>Enter the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.</p> <p>Select a remote node from the drop-down list box to set the static route. A remote node is a connection point outside of the local area network. One example of a remote node is your connection to your ISP. See <a href="#">Section 7.2 on page 62</a> for details on configuring a remote node.</p> |
| Metric                 | <p>This field sets this route's priority among the routes the P-660RU-Tx uses.</p> <p>The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".</p>   |

**Table 20** Advanced > Static Route: Edit

| LABEL            | DESCRIPTION  |
|------------------|--|
| Announced in RIP | Routing Information Protocol (RIP) allows a router to exchange routing information with other routers.<br><br>Select <b>Yes</b> to allow RIP to send information about the static route to other routers.<br><br>Select <b>No</b> to prevent RIP from sending information about the static route to other routers. |
| SAVE             | Click this to save your changes.   |
| DELETE           | Click this to remove the static route.   |
| BACK             | Click this to return to the previous screen without saving.  |
| CANCEL           | Click this to restore your previously saved settings.  |



# Network Address Translation (NAT)

## 10.1 Overview

This chapter discusses how to configure NAT on the P-660RU-Tx. NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

### 10.1.1 What You Can Do in the NAT Screens

- Use the **NAT** screen ([Section 10.2 on page 91](#)) to configure the NAT settings.
- Use the **DMZ** screen ([Section 10.3 on page 91](#)) to configure the DMZ settings.
- Use the **Virtual Server** screen ([Section 10.4 on page 92](#)) to forward incoming service requests to the server(s) on your local network.
- Use the **IP Address Mapping** screen ([Section 10.5 on page 95](#)) to change your P-660RU-Tx's address mapping settings.

### 10.1.2 What You Need To Know About NAT

#### Inside/Outside

Inside/outside denotes where a host is located relative to the P-660RU-Tx, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

#### Public/Local

Public/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the public address refers to the IP address of the host when the same packet is traveling in the WAN side.

## NAT

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host.

## Port Forwarding

A port forwarding set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single computer to the outside world.

## Single IP Versus NAT

Single IP is a ZYNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. The P-660RU-Tx also supports multiple IPs to map multiple public IP addresses to multiple private LAN IP addresses of clients or servers using mapping types.

- Choose **Single IP** if you have just one public WAN IP address for your P-660RU-Tx.
- Choose **Multiple IPs** if you have multiple public WAN IP addresses for your P-660RU-Tx.

## Finding Out More

See [Section 10.6 on page 97](#) for advanced technical information on NAT.

## 10.2 The NAT Screen

Use this screen to configure NAT for each PVC. Click **Advanced Setup > NAT** to open the following screen.

**Figure 34** Advanced Setup > NAT



The following table describes the labels in this screen.

**Table 21** Network > NAT > General

| LABEL              | DESCRIPTION  |
|--------------------|--|
| Virtual Circuit    | Select the PVC you want to configure from the drop-down list box.  |
| NAT Status         | This field shows whether NAT is enabled. See <a href="#">Section 7.2 on page 62</a> for more details on activating NAT.  |
| Number of IPs      | Select <b>Single</b> if you have just one public WAN IP address for your P-660RU-Tx.<br><br>Select <b>Multiple</b> if you have multiple public WAN IP addresses for your P-660RU-Tx.                                       |
| DMZ                | Click this to configure the DMZ settings. See <a href="#">Section 10.3 on page 91</a> for more details.  |
| Virtual Server     | Click this to configure port forwarding rules for your P-660RU-Tx. See <a href="#">Section 10.4 on page 92</a> for more details.   |
| IP Address Mapping | This is available only when you select <b>Multiple</b> in the <b>Number of IPs</b> field. Click this to configure address mapping rules for your P-660RU-Tx. See <a href="#">Section 10.5 on page 95</a> for more details. |

## 10.3 The DMZ Screen

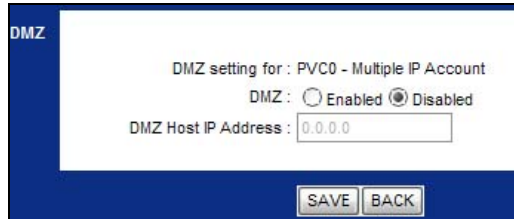
The DeMilitarized Zone (DMZ) provides a way for public servers (Web, e-mail, FTP, etc.) to be visible to the outside world (while still being protected from DoS (Denial of Service) attacks such as SYN flooding and Ping of Death). These public servers can also still be accessed from the secure LAN.

By default the firewall allows traffic between the WAN and the DMZ, traffic from the DMZ to the LAN is denied, and traffic from the LAN to the DMZ is allowed.

Internet users can have access to host servers on the DMZ but no access to the LAN, unless special filter rules allowing access were configured by the administrator or the user is an authorized remote user.

Use this screen to configure a separate independent network from the LAN in which you can put your servers. Click **Advanced Setup > NAT > DMZ** to open the following screen.

**Figure 35** Advanced Setup > NAT > DMZ



The following table describes the labels in this screen.

**Table 22** Advanced Setup > NAT > DMZ

| LABEL               | DESCRIPTION  |
|---------------------|--|
| DMZ setting for     | This field displays the PVC you want to configure.   |
| DMZ                 | Use this field to enable or disable DMZ.   |
| DMZ Host IP Address | Type the IP address for DMZ in dotted decimal notation.<br><br>Note: Make sure the IP addresses of the LAN, WAN and DMZ are on separate subnets. |
| SAVE                | Click this to save your settings.  |
| BACK                | Click this to return to the previous screen without saving.  |

## 10.4 The Virtual Server Screen

LAN computers usually have DHCP-assigned private IP address that cannot be accessed directly from the WAN. Use this screen to allow the P-660RU-Tx to forward traffic to the servers on the LAN.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

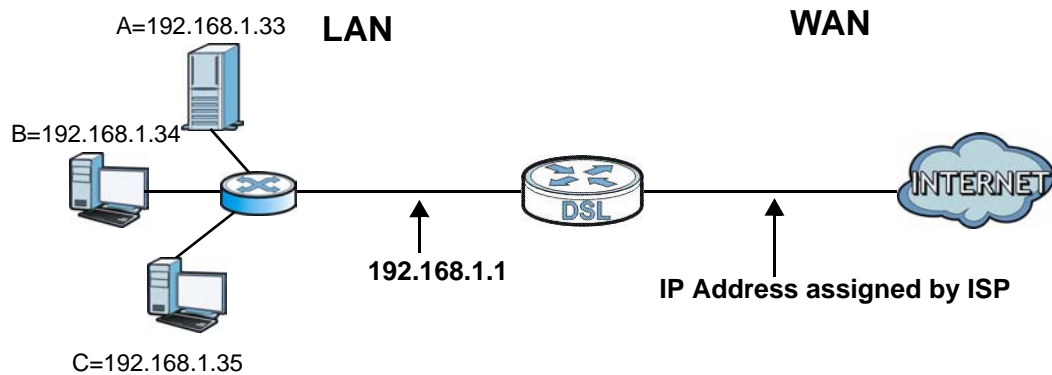
The most often used port numbers and services are shown in [Appendix D on page 219](#). Please refer to RFC 1700 for further information about port numbers.

Note: Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

## 10.4.1 Configuring Servers Behind Port Forwarding (Example)

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

**Figure 36** Multiple Servers Behind NAT Example



The following table summarizes the settings described in the above example.

**Table 23** Multiple Servers Behind NAT Example

|   | SERVICES | PORTS | DEFAULT SERVER IP |
|---|----------|-------|-------------------|
| A | FTP      | 21-22 | 192.168.1.33      |
| B | Telnet   | 23    | 192.168.1.34      |
| C | SMTP     | 25    | 192.168.1.35      |

## 10.4.2 Configuring the Virtual Server Screen

Click **Advanced Setup > NAT > Virtual Server** to open the following screen.

See [Appendix D on page 219](#) for port numbers commonly used for particular services.

**Figure 37** Advanced Setup > NAT > Virtual Server

Virtual Server for: PVC0 - Multiple IP Account

Rule Index: 1

Application: -

Protocol: ALL

Start Port Number: 0

End Port Number: 0

Local IP Address: 0.0.0.0

| Rule | Application | Protocol | Start Port | End Port | Local IP Address |
|------|-------------|----------|------------|----------|------------------|
| 1    | -           | -        | 0          | 0        | 0.0.0.0          |
| 2    | -           | -        | 0          | 0        | 0.0.0.0          |
| 3    | -           | -        | 0          | 0        | 0.0.0.0          |
| 4    | -           | -        | 0          | 0        | 0.0.0.0          |
| 5    | -           | -        | 0          | 0        | 0.0.0.0          |
| 6    | -           | -        | 0          | 0        | 0.0.0.0          |
| 7    | -           | -        | 0          | 0        | 0.0.0.0          |
| 8    | -           | -        | 0          | 0        | 0.0.0.0          |
| 9    | -           | -        | 0          | 0        | 0.0.0.0          |
| 10   | -           | -        | 0          | 0        | 0.0.0.0          |
| 11   | -           | -        | 0          | 0        | 0.0.0.0          |
| 12   | -           | -        | 0          | 0        | 0.0.0.0          |
| 13   | -           | -        | 0          | 0        | 0.0.0.0          |
| 14   | -           | -        | 0          | 0        | 0.0.0.0          |
| 15   | -           | -        | 0          | 0        | 0.0.0.0          |
| 16   | -           | -        | 0          | 0        | 0.0.0.0          |

SAVE DELETE BACK CANCEL

The following table describes the fields in this screen.

**Table 24** Advanced Setup > NAT > Virtual Server

| LABEL              | DESCRIPTION   |
|--------------------|---|
| Virtual Server     |   |
| Virtual Server for | This is the PVC that this virtual server will use.  |
| Rule Index         | Select the rule's index number from the drop-down list box.   |
| Application        | Use the drop-down list box to select the type of server you have on your network. Applications or services are defined by their protocol (TCP or UDP) and port number. For example, TCP port 80 defines web (HTTP) traffic. If you have a web server on your network, you need to forward HTTP applications (TCP port 80) to the server's IP address.<br><br>Choices are: <b>FTP, SSH, TELNET, SMTP, HTTP_Server, POP3, HTTPS, T.120, H.323, PPTP, pcAnywhere, VNC</b> and <b>CUSeeMe</b> . |

**Table 24** Advanced Setup > NAT > Virtual Server

| LABEL                  | DESCRIPTION  |
|------------------------|--|
| Protocol               | Use the drop-down list box to choose the IP port ( <b>ALL</b> , <b>TCP</b> or <b>UDP</b> ) that defines your service.  |
| Start Port Number      | Enter a port number in this field.<br><br>To forward only one port, enter the port number again in the <b>End Port Number</b> field.<br><br>To forward a series of ports, enter the start port number here and the end port number in the <b>End Port Number</b> field.  |
| End Port Number        | Enter a port number in this field.<br><br>To forward only one port, enter the port number again in the <b>Start Port Number</b> field above and then enter it again in this field.<br><br>To forward a series of ports, enter the last port number in a series that begins with the port number in the <b>Start Port Number</b> field above. |
| Local IP Address       | Enter the inside IP address of the server in this field.   |
| Virtual Server Listing |  |
| Rule                   | This is the rule's index number.   |
| Application            | This is a service's name.  |
| Protocol               | This is the IP port.   |
| Start Port             | This is the first port number that identifies a service.   |
| End Port               | This is the last port number that identifies a service.  |
| Local IP Address       | This is the server's IP address.   |
| SAVE                   | Click this to save your changes.   |
| DELETE                 | Click this to remove the rule.   |
| BACK                   | Click this to return to the previous screen without saving.  |
| CANCEL                 | Click this to restore your previously saved settings.  |

## 10.5 The IP Address Mapping Screen

Configure this screen if you have multiple IP addresses from your ISP and you want to map them to private IP addresses on your LAN.

Note: The **Address Mapping** screen is available only when you select **Multiple** for the **Number of IPs** in the **NAT** screen.

Ordering your rules is important because the P-660RU-Tx applies the rules in the order that you specify. When a rule matches the current packet, the P-660RU-Tx takes the corresponding action and the remaining rules are ignored.

Use this screen to change your P-660RU-Tx's address mapping settings. Click **Advanced Setup > NAT > IP Address Mapping** to open the following screen.

**Figure 38** Advanced Setup > NAT > IP Address Mapping

IP Address Mapping

Address Mapping Rule : PVC0

Rule Index : 1

Rule Type : One-to-One

Local Start IP : 0.0.0.0

Local End IP : N/A

Public Start IP : 0.0.0.0 (0.0.0.0 for modem's WAN IP)

Public End IP : N/A

| Rule | Type | Local Start IP | Local End IP | Public Start IP | Public End IP |
|------|------|----------------|--------------|-----------------|---------------|
| 1    | -    | ...            | ...          | ...             | ...           |
| 2    | -    | ...            | ...          | ...             | ...           |
| 3    | -    | ...            | ...          | ...             | ...           |
| 4    | -    | ...            | ...          | ...             | ...           |
| 5    | -    | ...            | ...          | ...             | ...           |
| 6    | -    | ...            | ...          | ...             | ...           |
| 7    | -    | ...            | ...          | ...             | ...           |
| 8    | -    | ...            | ...          | ...             | ...           |

Address Mapping List

SAVE DELETE BACK CANCEL

The following table describes the fields in this screen.

**Table 25** Network > NAT > Address Mapping

| LABEL                | DESCRIPTION   |
|----------------------|---|
| IP Address Mapping   |   |
| Address Mapping Rule | The rules configured in this screen apply to this PVC.  |
| Rule Index           | Select the rule's index number from the drop-down list box.   |
| Rule Type            | <p>Choose the port mapping type from one of the following.</p> <p><b>One-to-One:</b> This mode maps one local IP address to one public IP address. Note that port numbers do not change for one-to-one NAT mapping type.</p> <p><b>Many-to-One:</b> This mode maps multiple local IP addresses to one public IP address. This is equivalent to the <b>Single IP</b> feature that previous ZyXEL routers supported only.</p> <p><b>Many-to-Many Overload:</b> This mode maps multiple local IP addresses to shared public IP addresses.</p> <p><b>Many-to-Many No Overload:</b> This mode maps each local IP address to unique public IP addresses.</p> <p><b>Server:</b> This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.</p> |
| Local Start IP       | This is the starting local IP address. Local IP addresses are <b>N/A</b> for <b>Server</b> port mapping.  |



**Table 25** Network > NAT > Address Mapping (continued)

| LABEL                | DESCRIPTION  |
|----------------------|--|
| Local End IP         | This is the end local IP address. If your rule is for all local IP addresses, then enter 0.0.0.0 as the <b>Local Start IP</b> address and 255.255.255.255 as the <b>Local End IP</b> address.<br><br>This field is <b>N/A</b> for <b>One-to-One</b> and <b>Server</b> mapping types.   |
| Public Start IP      | This is the starting public IP address. Enter 0.0.0.0 here if you have a dynamic IP address from your ISP.   |
| Public End IP        | This is the ending public IP address. This field is <b>N/A</b> for <b>One-to-One</b> , <b>Many-to-One</b> and <b>Server</b> mapping types.   |
| Address Mapping List |  |
| Rule                 | This is the rule's index number.   |
| Type                 | <b>1-1</b> : One-to-One mode maps one local IP address to one public IP address. Note that port numbers do not change for the One-to-One NAT mapping type.<br><br><b>M-1</b> : Many-to-One mode maps multiple local IP addresses to one public IP address. This is equivalent to the <b>Single IP</b> feature that previous ZyXEL routers supported only.<br><br><b>M-M Ov</b> (Overload): Many-to-Many Overload mode maps multiple local IP addresses to shared public IP addresses.<br><br><b>MM No</b> (No Overload): Many-to-Many No Overload mode maps each local IP address to unique public IP addresses.<br><br><b>Server</b> : This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world. |
| Local Start IP       | This is the starting inside local IP address. Local IP addresses are <b>N/A</b> for <b>Server</b> port mapping.  |
| Local End IP         | This is the ending inside local IP address. If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the <b>Local Start IP</b> address and 255.255.255.255 as the <b>Local End IP</b> address. This field is <b>N/A</b> for <b>One-to-one</b> and <b>Server</b> mapping types.   |
| Public Start IP      | This is the starting inside public IP address. Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. You can only do this for <b>Many-to-One</b> and <b>Server</b> mapping types.   |
| Public End IP        | This is the ending inside public IP address. This field is <b>N/A</b> for <b>One-to-one</b> , <b>Many-to-One</b> and <b>Server</b> mapping types.  |
| SAVE                 | Click this to save your changes.   |
| DELETE               | Click this to remove the rule.   |
| BACK                 | Click this to return to the previous screen without saving.  |
| CANCEL               | Click this to restore your previously saved settings.  |

## 10.6 NAT Technical Reference

This section contains more information regarding NAT.

## 10.6.1 NAT Definitions

Inside/outside denotes where a host is located relative to the P-660RU-Tx, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Public/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the public address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while public/local refers to the IP address of a host used in a packet. Thus, an inside local address is the IP address of an inside host in a packet when the packet is still in the local network, while an inside public address is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

**Table 26** NAT Definitions

| ITEM    | DESCRIPTION   |
|---------|---|
| Inside  | This refers to the host on the LAN.   |
| Outside | This refers to the host on the WAN.   |
| Local   | This refers to the packet address (source or destination) as the packet travels on the LAN. |
| Public  | This refers to the packet address (source or destination) as the packet travels on the WAN. |

NAT never changes the IP address (either local or public) of an outside host.

## 10.6.2 What NAT Does

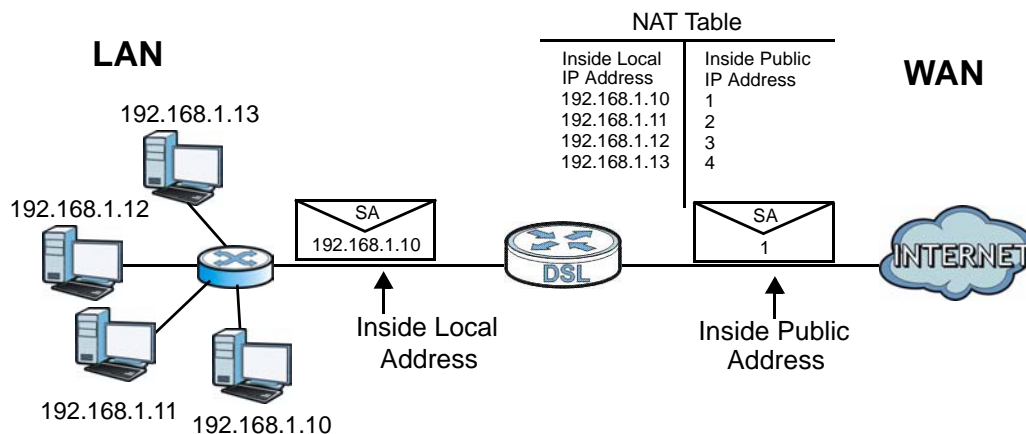
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside public address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside public address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or public) of an outside host is never changed.

The public IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers, NAT offers the additional benefit of firewall protection. With no servers defined, your P-660RU-Tx filters out all incoming inquiries, thus preventing intruders from probing your network.

### 10.6.3 How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the inside local address is the source address on the LAN, and the inside public address is the source address on the WAN. For incoming packets, the inside local address is the destination address on the LAN, and the inside public address is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The P-660RU-Tx keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

**Figure 39** How NAT Works





# Quality of Service (QoS)

## 11.1 Overview

Use the **QoS** screen to set up your P-660RU-Tx to use QoS for traffic management.

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control bandwidth. QoS allows the P-660RU-Tx to group and prioritize application traffic and fine-tune network performance.

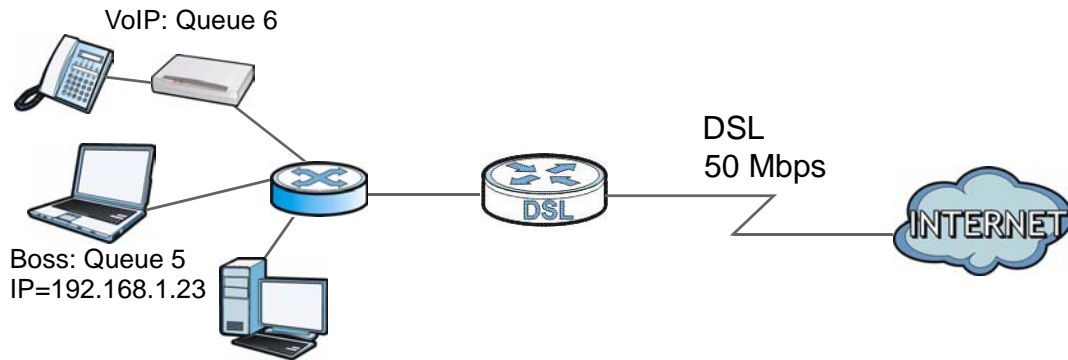
Without QoS, all traffic data are equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical applications such as video-on-demand.

The P-660RU-Tx assigns each packet a priority and then queues the packet accordingly. Packets assigned with a high priority are processed more quickly than those with low priorities if there is congestion, allowing time-sensitive applications to flow more smoothly. Time-sensitive applications include both those that require a low level of latency (delay) and a low level of jitter (variations in delay) such as Voice over IP (VoIP) or Internet gaming, and those for which jitter alone is a problem such as Internet radio or streaming video.

In the following figure, your Internet connection has an upstream transmission speed of 50 Mbps. You configure a classifier to assign the highest priority queue (6) to VoIP traffic from the LAN interface, so that voice traffic would not get delayed when there is network congestion. Traffic from the boss's IP address (192.168.1.23 for example) is mapped to queue 5. Traffic that does not match

these two classes are assigned priority queue based on the internal QoS mapping table on the P-660RU-Tx.

**Figure 40** QoS Example



### 11.1.1 What You Can Do in the QoS Screens

- Use the **QoS** screen ([Section 11.2 on page 103](#)) to configure QoS settings on the P-660RU-Tx.
- Use the **QoS Settings Summary** screen ([Section 11.2.1 on page 105](#)) to check the summary of QoS rules and actions you configured for the P-660RU-Tx.

### 11.1.2 What You Need to Know About QoS

#### 802.1p

QoS is used to prioritize source-to-destination traffic flows. All packets in the same flow are given the same priority. 802.1p is a way of managing traffic in a network by grouping similar types of traffic together and treating each type as a class. You can use 802.1p to give different priorities to different packet types.

#### Tagging and Marking

In a QoS class, you can configure whether to add or change the DiffServ Code Point (DSCP) value, IEEE 802.1p priority level and VLAN ID number in a matched packet. When the packet passes through a compatible network, the networking device, such as a backbone switch, can provide specific treatment or service based on the tag or marker.

#### Finding Out More

See [Section 11.3 on page 106](#) for advanced technical information on QoS.

## 11.2 The QoS Screen

Use this screen to enable or disable QoS and have the P-660RU-Tx assign priority levels to traffic according to the port range, IEEE 802.1p priority level and/or IP precedence.

Click **Advanced Setup > QoS** to open the screen as shown next.

**Figure 41** Advanced Setup > QoS

**Quality of Service**

QoS :  Activated  Deactivated  
 Summary : [QoS Settings Summary](#)

**Rule**

Rule Index : 1  
 Active :  Activated  Deactivated  
 Application : SIP  
 Physical Ports :  USB  Enet1  
 Destination MAC :  
 IP : 224.0.0.0  
 Mask : 240.0.0.0  
 Port Range : 5060 ~ 5060  
 Source MAC :  
 IP :  
 Mask :  
 Port Range : ~  
 Protocol ID : UDP  
 Vlan ID Range : ~  
 IPP/DS Field :  IPP/TOS  DSCP  
 IP Precedence Range : ~  
 Type of Service :  
 DSCP Range : (Value Range: 0 ~ 63)  
 802.1p : ~

**Action**

IPP/DS Field :  IPP/TOS  DSCP  
 IP Precedence Remarking :  
 Type of Service Remarking :  
 DSCP Remarking : (Value Range: 0 ~ 63)  
 802.1p Remarking : 5  
 Queue # : Highest

[ADD](#) [DELETE](#) [CANCEL](#)

The following table describes the labels in this screen.

**Table 27** Advanced Setup > QoS

| LABEL               | DESCRIPTION   |
|---------------------|---|
| Quality of Service  |   |
| QoS                 | Use this field to activate QoS to improve your network performance.<br><br>You can give priority to traffic that the P-660RU-Tx forwards out through the WAN interface. Give high priority to voice and video to make them run more smoothly. Similarly, give low priority to many large file downloads so that they do not reduce the quality of other applications. |
| Summary             | Click this to open a summary table showing the QoS settings. See <a href="#">Section 11.2.1 on page 105</a> for more details.   |
| Rule                |   |
| Rule Index          | Select the rule's index number from the drop-down list box.   |
| Active              | Use this field to enable or disable the rule.   |
| Application         | Select an application from the drop-down list box. The <b>Destination Port Range</b> and <b>Protocol ID</b> fields may change depending on the type of applications you choose.   |
| Physical Ports      | Select <b>Enet1</b> to apply the rule to the Ethernet port or select <b>USB</b> to apply the rule to the USB port.  |
| Destination MAC     | Type a destination MAC address here. QoS is then applied to traffic containing this destination MAC address. Leave it blank to apply the rule to all MAC addresses.   |
| IP                  | Enter a destination IP address in dotted decimal notation. QoS is then applied to traffic containing this destination IP address. A blank destination IP address means any destination IP address.  |
| Mask                | Enter a destination subnet mask here.   |
| Port Range          | Either use the default value set by the application you choose, or enter the port number to which the rule should be applied.   |
| Source MAC          | Type a source MAC address here. QoS is then applied to traffic containing this source MAC address. Leave it blank to apply the rule to all MAC addresses.   |
| IP                  | Enter a source IP address in dotted decimal notation. QoS is then applied to traffic containing this source IP address. A blank source IP address means any source IP address.  |
| Mask                | Enter a source subnet mask here.  |
| Port Range          | Enter the port number to which the rule should be applied. 0 means any source port number. See <a href="#">Appendix D on page 219</a> for some common services and port numbers.  |
| Protocol ID         | Select an IP protocol type from the drop-down list box.   |
| Vlan ID Range       | Enter the source VLAN ID in this field.   |
| IPP/DS Field        | Select <b>IPP/TOS</b> to specify an IP precedence range and type of services.<br><br>Select <b>DSCP</b> to specify a DiffServ Code Point (DSCP) range.  |
| IP Precedence Range | Select a range from 0 to 7 for IP precedence. Zero is the lowest priority and seven is the highest.   |



**Table 27** Advanced Setup > QoS

| LABEL                     | DESCRIPTION   |
|---------------------------|---|
| Type of Service           | Select a type of service from the drop-down list box.<br>Available options are: <b>Normal service</b> , <b>Minimize delay</b> , <b>Maximize throughput</b> , <b>Maximize reliability</b> and <b>Minimize monetary cost</b> .                        |
| DSCP Range                | Specify a DSCP number between 0 and 63 in this field.   |
| 802.1p                    | Select a priority level (0 to 7) from the drop-down list box.   |
| Action                    |   |
| IPP/DS Field              | Select <b>IPP/TOS</b> to specify an IP precedence range and type of services.<br>Select <b>DSCP</b> to specify a DiffServ Code Point (DSCP) range.  |
| IP Precedence Remarking   | Select from 0 to 7 to re-assign IP precedence to matched traffic. Zero is the lowest priority and seven is the highest.   |
| Type of Service Remarking | Select a type of service to re-assign the priority level to matched traffic.<br>Available options are: <b>Normal service</b> , <b>Minimize delay</b> , <b>Maximize throughput</b> , <b>Maximize reliability</b> and <b>Minimize monetary cost</b> . |
| DSCP Remarking            | Specify a DSCP number between 0 and 63 to re-assign the priority level to matched traffic.  |
| 802.1p Remarking          | Select a priority level (0 to 7) to re-assign the priority level to matched traffic.  |
| Queue #                   | Specify a <b>Low</b> , <b>Medium</b> , <b>High</b> or <b>Highest</b> queue tag to matched traffic. Traffic assigned to a higher queue gets through faster while traffic in lower queues is dropped when there is network congestion.                |
| ADD                       | Click this to add the rule.   |
| DELETE                    | Click this to remove the rule.  |
| CANCEL                    | Click this to restore previously saved settings.  |

## 11.2.1 The QoS Settings Summary Screen

Use this screen to display a summary of rules and actions configured for the P-660RU-Tx. In the **Advanced > QoS** screen, click the **QoS Settings Summary** button to open the following screen.

**Figure 42** Advanced Setup > QoS > QoS Settings Summary

| QoS Settings Summary |        |                |   |  |             |         |                   |        |                                |                     |         |
|----------------------|--------|----------------|---|--|-------------|---------|-------------------|--------|--------------------------------|---------------------|---------|
| Rules                |        |                |   |  |             |         |                   |        | Actions                        |                     |         |
| #                    | Active | Physical Ports | Destination<br>MAC<br>IP/Mask<br>Port Range | Source<br>MAC<br>IP/Mask<br>Port Range | Protocol ID | VLAN ID | IPP/TOS<br>(DSCP) | 802.1p | IPP/TOS<br>(DSCP)<br>Remarking | 802.1p<br>Remarking | Queue # |
| 1                    | Y      | e1,            | 224.0.0.0/4<br>5060-5060                    | -<br>-                                 | UDP         | <br>-   | -/<br>-           | <br>-  | -/<br>-                        | 5                   | HH      |

e: ethernet, u: usb, NS: Normal service, MD: Minimize delay, MT: Maximize throughput, MR: Maximize reliability, MC: Minimize monetary cost, HH: Highest, H: High, M: Medium, L: Low.

The following table describes the labels in this screen.

**Table 28** Advanced Setup > QoS > QoS Settings Summary

| LABEL                                   | DESCRIPTION   |
|---|---|
| Rules                                   |   |
| #                                       | This is the rule's index number.  |
| Active                                  | This shows whether the rule is enabled or disabled.                                       |
| Physical Ports                          | This is the physical port associated with the rule.                                       |
| Destination MAC and IP/Mask Port Ranges | This is the port range for destination MAC address and IP address.                        |
| Source MAC and IP/Mask Port Ranges      | This is the port range for source MAC address and IP address.                             |
| Protocol ID                             | This is the protocol ID associated with the rule.   |
| VLAN ID                                 | This is the VLAN ID associated with the rule.   |
| IPP/TOS (DSCP)                          | This shows the IPP/TOS or DSCP settings.  |
| 802.1p                                  | This is the 802.1p priority level.  |
| Actions                                 |   |
| IPP/TOS (DSCP) Remarking                | The P-660RU-Tx re-assigns the priority values specified in this field to matched traffic. |
| 802.1p Remarking                        | The P-660RU-Tx re-assigns the priority levels specified in this field to matched traffic. |
| Queue #                                 | The P-660RU-Tx assigns the queue level specified in this field to matched traffic.        |

## 11.3 QoS Technical Reference

This section provides some technical background information about the topics covered in this chapter.

### 11.3.1 IEEE 802.1p

IEEE 802.1p specifies the user priority field and defines up to eight separate traffic types. The following table describes the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p).

**Table 29** IEEE 802.1p Priority Level and Traffic Type

| PRIORITY LEVEL | TRAFFIC TYPE   |
|----------------|--|
| Level 7        | Typically used for network control traffic such as router configuration messages.                            |
| Level 6        | Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay). |

**Table 29** IEEE 802.1p Priority Level and Traffic Type

| PRIORITY LEVEL | TRAFFIC TYPE  |
|----------------|---|
| Level 5        | Typically used for video that consumes high bandwidth and is sensitive to jitter.   |
| Level 4        | Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.  |
| Level 3        | Typically used for “excellent effort” or better than best effort and would include important business traffic that can tolerate some delay.                   |
| Level 2        | This is for “spare bandwidth”.  |
| Level 1        | This is typically used for non-critical “background” traffic such as bulk transfers that are allowed but that should not affect other applications and users. |
| Level 0        | Typically used for best-effort traffic.   |

### 11.3.2 IP Precedence

Similar to IEEE 802.1p prioritization at layer-2, you can use IP precedence to prioritize packets in a layer-3 network. IP precedence uses three bits of the eight-bit ToS (Type of Service) field in the IP header. There are eight classes of services (ranging from zero to seven) in IP precedence. Zero is the lowest priority level and seven is the highest.

### 11.3.3 Automatic Priority Queue Assignment

If you enable QoS on the P-660RU-Tx, the P-660RU-Tx can automatically base on the IEEE 802.1p priority level, IP precedence and/or packet length to assign priority to traffic which does not match a class.

The following table shows you the internal layer-2 and layer-3 QoS mapping on the P-660RU-Tx. On the P-660RU-Tx, traffic assigned to higher priority queues gets through faster while traffic in lower index queues is dropped if the network is congested.

**Table 30** Internal Layer2 and Layer3 QoS Mapping

| PRIORITY QUEUE | LAYER 2                                       | LAYER 3             |        |                         |
|----------------|---|---------------------|--------|-------------------------|
|                | IEEE 802.1P USER PRIORITY (ETHERNET PRIORITY) | TOS (IP PRECEDENCE) | DSCP   | IP PACKET LENGTH (BYTE) |
| 0              | 1   | 0                   | 000000 |                         |
| 1              | 2   |                     |        |                         |
| 2              | 0   | 0                   | 000000 | >1100                   |

**Table 30** Internal Layer2 and Layer3 QoS Mapping

| PRIORITY QUEUE | LAYER 2                                       | LAYER 3             |                                      |                         |
|----------------|---|---------------------|--------------------------------------|-------------------------|
|                | IEEE 802.1P USER PRIORITY (ETHERNET PRIORITY) | TOS (IP PRECEDENCE) | DSCP                                 | IP PACKET LENGTH (BYTE) |
| 3              | 3   | 1                   | 001110<br>001100<br>001010<br>001000 | 250~1100                |
| 4              | 4   | 2                   | 010110<br>010100<br>010010<br>010000 |                         |
| 5              | 5   | 3                   | 011110<br>011100<br>011010<br>011000 | <250                    |
| 6              | 6   | 4                   | 100110<br>100100<br>100010<br>100000 |                         |
|                |   | 5                   | 101110<br>101000                     |                         |
| 7              | 7   | 6                   | 110000                               |                         |
|                |   | 7                   | 111000                               |                         |

## 12.1 Overview

This chapter contains information about configuring the ADSL settings for your P-660RU-Tx.

## 12.2 The ADSL Screen

Use this screen to select the ADSL mode and type for your P-660RU-Tx. Click **Advanced Setup > ADSL** to open the following screen.

**Figure 43** Advanced Setup > ADSL

The following table describes the labels in this screen.

**Table 31** Advanced Setup > ADSL

| LABEL     | DESCRIPTION   |
|-----------|---|
| ADSL Mode | Select the mode supported by your ISP.<br><br>Use <b>Auto Sync-Up</b> if you are not sure which mode to choose from. The P-660RU-Tx dynamically diagnoses the mode supported by the ISP and selects the best compatible one for your connection.<br><br>Other options are <b>ADSL2+</b> , <b>ADSL2</b> , <b>G.DMT</b> , <b>T1.413</b> and <b>G.lite</b> . |

**Table 31** Advanced Setup > ADSL (continued)

| LABEL     | DESCRIPTION   |
|-----------|---|
| ADSL Type | Select the type supported by your ISP.<br>Available options are <b>ANNEX A</b> , <b>ANNEX A/L</b> , <b>ANNEX M</b> and <b>ANNEX A/L/M</b> . |
| SAVE      | Click this to save your changes.  |

## 13.1 Overview

This chapter shows you how to enable the P-660RU-Tx firewall. Use the firewall to protect your P-660RU-Tx and network from attacks by hackers on the Internet and control access to it. By default the firewall:

- allows traffic that originates from your LAN computers to go to all other networks.
- blocks traffic that originates on other networks from going to the LAN.
- blocks SYN and port scanner attacks.

By default, the P-660RU-Tx blocks DDOS, LAND and Ping of Death attacks whether the firewall is enabled or disabled.

### 13.1.1 What You Can Do in the Firewall Screens

Use the **Firewall** screen ([Section 13.2 on page 112](#)) to enable firewall and/or SPI on the P-660RU-Tx.

### 13.1.2 What You Need to Know About Firewall

#### SYN Attack

A SYN attack floods a targeted system with a series of SYN packets. Each packet causes the targeted system to issue a SYN-ACK response. While the targeted system waits for the ACK that follows the SYN-ACK, it queues up all outstanding SYN-ACK responses on a backlog queue. SYN-ACKs are moved off the queue only when an ACK comes back or when an internal timer terminates the three-way handshake. Once the queue is full, the system will ignore all incoming SYN requests, making the system unavailable for legitimate users.

#### DoS

Denials of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a

device or network so users no longer have access to network resources. The ZyXEL Device is pre-configured to automatically detect and thwart all known DoS attacks.

## DDoS

A DDoS attack is one in which multiple compromised systems attack a single target, thereby causing denial of service for users of the targeted system.

## LAND Attack

In a LAND attack, hackers flood SYN packets into the network with a spoofed source IP address of the target system. This makes it appear as if the host computer sent the packets to itself, making the system unavailable while the target system tries to respond to itself.

## Ping of Death

Ping of Death uses a "ping" utility to create and send an IP packet that exceeds the maximum 65,536 bytes of data allowed by the IP specification. This may cause systems to crash, hang or reboot.

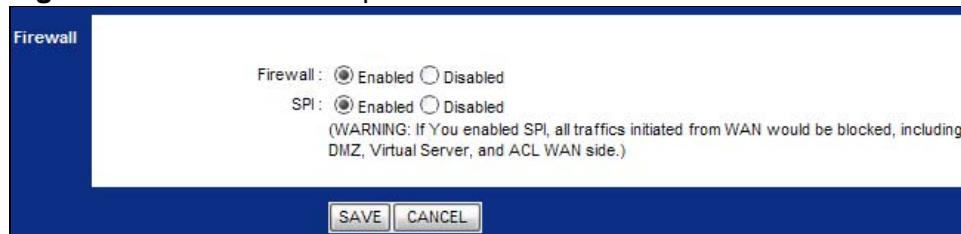
## SPI

Stateful Packet Inspection (SPI) tracks each connection crossing the firewall and makes sure it is valid. Filtering decisions are based not only on rules but also context. For example, traffic from the WAN may only be allowed to cross the firewall in response to a request from the LAN.

## 13.2 The Firewall Screen

Use this screen to enable firewall and/or SPI. Click **Advanced Setup > Firewall** to display the following screen.

**Figure 44** Advanced Setup > Firewall





The following table describes the labels in this screen.

**Table 32** Advanced > Firewall

| LABEL    | DESCRIPTION  |
|----------|--|
| Firewall | Use this field to enable or disable firewall on your P-660RU-Tx. |
| SPI      | Use this field to enable or disable SPI on your P-660RU-Tx.      |
| SAVE     | Click this to save your changes.                                 |
| CANCEL   | Click this to restore your previously saved settings.            |

**Enabling SPI blocks all traffic initiated from the WAN side, including the DMZ, virtual server and ACL on the WAN side.**



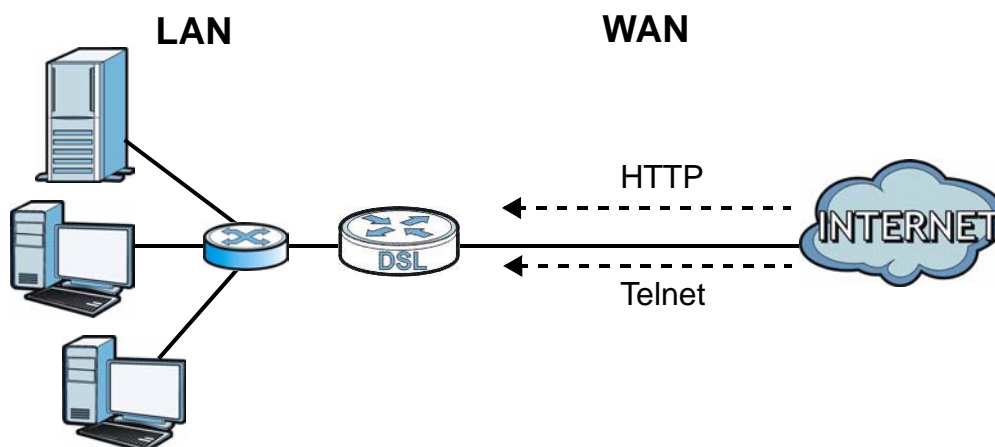
# Access Control

## 14.1 Access Control Overview

Access Control allows you to determine which application can access which P-660RU-Tx interface from which computers.

The following figure shows access to the P-660RU-Tx from the WAN being limited to HTTP (web) and Telnet only.

**Figure 45** Access Control



### 14.1.1 The Access Control Setup Screen

Use this screen to configure from where and how users may access the P-660RU-Tx.

### 14.1.2 Access Control Interfaces

You may manage your P-660RU-Tx via:

- **WAN**
- **LAN**
- **Both** (LAN and WAN)

### 14.1.3 System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The P-660RU-Tx automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling.

### 14.1.4 Configuring the Access Control Setup Screen

Click **Access Management > ACL** to open the following screen.

**Figure 46** Access Management > ACL

The screenshot shows the 'Access Control Setup' screen. On the left is a blue sidebar with three sections: 'Access Control Setup', 'Access Control Editing', and 'Access Control Listing'. The main content area is white and contains the following controls:

- Access Control Setup:** 'ACL:  Activated  Deactivated'
- Access Control Editing:**
  - 'ACL Rule Index: 1' (dropdown menu)
  - 'Active:  Yes  No'
  - 'Secure IP Address: 0.0.0.0 ~ 0.0.0.0 (0.0.0.0 ~ 0.0.0.0 means all IPs)'
  - 'Application: Web' (dropdown menu)
  - 'Interface: Both' (dropdown menu)
- Access Control Listing:** A table with columns: Index, Active, Secure IP Address, Application, Interface.
- Buttons:** 'SAVE', 'DELETE', 'CANCEL' at the bottom.

The following table describes the fields in this screen.

**Table 33** Access Management > ACL

| LABEL                  | DESCRIPTION   |
|------------------------|---|
| Access Control Setup   |   |
| ACL                    | Select <b>Activated</b> to enable access control on the P-660RU-Tx or select <b>Deactivated</b> to disable it.  |
| Access Control Editing |   |
| ACL Rule Index         | Select an index rule number in order to edit or delete it.  |
| Active                 | Select <b>Yes</b> to enable this active control rule or <b>No</b> to disable it.  |
| Secure IP Address      | Enter the range of IP addresses of computers that are allowed to access the device. 0.0.0.0 ~ 0.0.0.0 means that any computer can access the P-660RU-Tx. If you want just one computer to be able to access the P-660RU-Tx, then enter its IP address in both fields. |

**Table 33** Access Management > ACL (continued)

| LABEL                  | DESCRIPTION   |
|------------------------|---|
| Application            | <p>Select the service through which the computer can access the device.</p> <ul style="list-style-type: none"> <li>• If you want to allow a user to connect to the P-660RU-Tx using the web configurator, select <b>Web</b>.</li> <li>• If you want to allow a user to connect to the P-660RU-Tx using Telnet, select <b>Telnet</b>.</li> <li>• If you want to allow a user to upload firmware to the P-660RU-Tx, select <b>FTP</b>.</li> <li>• If you want to allow an administrator to send SNMP commands, select <b>SNMP</b>.</li> <li>• If you want to allow a user to find the P-660RU-Tx on the network (for troubleshooting purposes, for example), select <b>Ping</b>.</li> <li>• Select <b>ALL</b> to allow access for all services. You cannot select a combination of services.</li> </ul> |
| Interface              | <p>Select the port through which you can access the device. Select <b>Both</b> for access via either port. If you configure 0.0.0.0 ~ 0.0.0.0 <b>Secure IP Address</b>, <b>ALL</b> services and <b>WAN</b> interface, you will not be able to access the device at all from the LAN unless you configure another rule for LAN access.</p>   |
| Access Control Listing | <p>The summary table displays the configured parameters for the selected rule.</p>  |
| SAVE                   | <p>Click this so save your changes.</p>   |
| DELETE                 | <p>Select an access control rule index number and click this to remove it.</p>  |
| CANCEL                 | <p>Click this to restore your previously saved settings.</p>  |



## 15.1 Overview

This chapter introduces three types of filters supported by the P-660RU-Tx. You can configure rules to restrict traffic by IP addresses, MAC addresses, application types and/or URLs.

### 15.1.1 What You Can Do in the Filter Screens

- Use the **IP/MAC Filter** screen ([Section 15.2 on page 120](#)) to create IP/MAC filter rules.
- Use the **Application Filter** screen ([Section 15.3 on page 122](#)) to allow or deny traffic from certain types of applications.
- Use the **URL Filter** screen ([Section 15.4 on page 123](#)) to block access to web sites.

### 15.1.2 What You Need to Know About Filtering

#### IP/MAC Filter Structure

An IP/MAC filter set consists of one or more filter rules. The P-660RU-Tx allows you to configure up to twelve filter sets with six rules in each set, for a total of 72 filter rules in the system.

#### URL

The URL (Uniform Resource Locator) identifies and helps locates resources on a network. On the Internet the URL is the web address that you type in the address bar of your Internet browser, for example “<http://www.zyxel.com>”.

## 15.2 The IP/MAC Filter Screen

Use this screen to create and apply IP/MAC filters. Click **Access Management > Filter** and select **IP/MAC Filter** in the **Filter Type Selection** field. The screen appears as shown.

**Figure 47** Access Management > Filter (IP/MAC)

The screenshot shows the configuration interface for IP/MAC filters. It includes sections for setting the filter type, filter set index, interface, direction, rule index, rule type, active status, source/destination IP addresses, subnet masks, port numbers, protocol, and rule unmatched action. A table at the bottom displays the current filter set configuration.

| # | Active | Src Address/Mask | Dest IP/Mask | Src Port | Dest Port | Protocol | Unmatched |
|---|--------|------------------|--------------|----------|-----------|----------|-----------|
| 1 | -      | -                | -            | -        | -         | -        | -         |
| 2 | -      | -                | -            | -        | -         | -        | -         |
| 3 | -      | -                | -            | -        | -         | -        | -         |
| 4 | -      | -                | -            | -        | -         | -        | -         |
| 5 | -      | -                | -            | -        | -         | -        | -         |
| 6 | -      | -                | -            | -        | -         | -        | -         |

The following table describes the labels in this screen.

**Table 34** Access Management > Filter (IP/MAC)

| LABEL                     | DESCRIPTION   |
|---------------------------|---|
| Filter Type               |   |
| Filter Type Selection     | Select the filter type from the drop-down list box.<br>Available options are <b>IP/MAC Filter</b> , <b>Application Filter</b> and <b>URL Filter</b> . |
| IP/MAC Filter Set Editing |   |
| IP/MAC Filter Set Index   | Select the index number of the filter set.  |
| Interface                 | Select the PVC to which to apply the filter.  |



**Table 34** Access Management > Filter (IP/MAC) (continued)

| LABEL                      | DESCRIPTION   |
|----------------------------|---|
| Direction                  | Apply the filter to <b>Both</b> , <b>Incoming</b> or <b>Outgoing</b> traffic direction.   |
| IP/MAC Filter Rule Editing |   |
| IP/MAC Filter Rule Index   | Select the index number of the filter rule.   |
| Rule Type                  | Select <b>IP</b> or <b>MAC</b> type to configure the rule.<br>Use the <b>IP Filter</b> to block traffic by IP addresses.<br>Use the <b>MAC Filter</b> to block traffic by MAC address.          |
| Active                     | Use this field to enable or disable the rule.   |
| Source IP Address          | Enter the source IP address of the packets you wish to filter. This field is ignored if it is 0.0.0.0.  |
| Subnet Mask                | Enter the IP subnet mask for the source IP address  |
| Port Number                | Enter the source port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.  |
| Destination IP Address     | Enter the destination IP address of the packets you wish to filter. This field is ignored if it is 0.0.0.0.   |
| Subnet Mask                | Enter the IP subnet mask for the destination IP address.  |
| Port Number                | Enter the destination port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.   |
| Protocol                   | Select <b>ICMP</b> , <b>TCP</b> or <b>UDP</b> for the upper layer protocol.   |
| MAC Address                | This field is only available when you select <b>MAC</b> in the <b>Rule Type</b> field.<br>Enter the MAC address of the packets you wish to filter.  |
| Rule Unmatched             | Select the action for a packet not matching the rule.<br>Select <b>Forward</b> to forward traffic immediately and skip checking the remaining rules. Select <b>Next</b> to check the next rule. |
| IP Filter Listing          |   |
| IP Filter Set Index        | Select the index number of the filter set from the drop-down list box.  |
| Interface                  | This is the interface that the filter set applies to.   |
| Direction                  | The filter set applies to this traffic direction.   |
| #                          | This is the index number of the rule in a filter set.   |
| Active                     | This field shows whether the rule is activated.   |
| Src Address/Mask           | This is the source IP address and subnet mask when you select <b>IP</b> as the rule type.<br>This is the MAC address when you select <b>MAC</b> as the rule type.                               |
| Dest IP/Mask               | This is the destination IP address and subnet mask.   |
| Src Port                   | This is the source port number.   |
| Dest Port                  | This is the destination port number.  |

**Table 34** Access Management > Filter (IP/MAC) (continued)

| LABEL     | DESCRIPTION  |
|-----------|--|
| Protocol  | This is the upper layer protocol.  |
| Unmatched | When a packet doesn't match the rule, this is the action the P-660RU-Tx takes on the packet. |
| SAVE      | Click this to save your changes.   |
| DELETE    | Click this to remove the filter rule.  |
| CANCEL    | Click this to restore your previously saved settings.  |

## 15.3 The Application Filter Screen

Use this screen to allow or deny traffic for certain types of applications. The application filter provides a convenient way to manage the use of various applications on the network.

Click **Access Management > Filter** and select **Application Filter** in the **Filter Type Selection** field. The screen appears as shown.

**Figure 48** Access Management > Filter (Application)

The following table describes the labels in this screen.

**Table 35** Access Management > Filter (Application)

| LABEL                      | DESCRIPTION   |
|----------------------------|---|
| Application Filter Editing |   |
| Application Filter         | Use this field to enable or disable the application filter.           |
| ICQ                        | Use this field to allow or deny ICQ traffic.                          |
| MSN                        | Use this field to allow or deny MSN traffic.                          |
| YMSG                       | Use this field to allow or deny Yahoo Messenger traffic.              |
| Real Audio/Video           | Use this field to allow or deny transferring RealPlayer format files. |

**Table 35** Access Management > Filter (Application) (continued)

| LABEL  | DESCRIPTION   |
|--------|---|
| SAVE   | Click this to save your changes.                      |
| CANCEL | Click this to restore your previously saved settings. |

## 15.4 The URL Filter Screen

Use this screen to block websites by URL. Click **Access Management > Filter** and select **URL Filter** in the **Filter Type Selection** field. The screen appears as shown.

**Figure 49** Access Management > Filter (URL)

| Index | URL |
|-------|-----|
| 1     |     |
| 2     |     |
| 3     |     |
| 4     |     |
| 5     |     |
| 6     |     |
| 7     |     |
| 8     |     |
| 9     |     |
| 10    |     |
| 11    |     |
| 12    |     |
| 13    |     |
| 14    |     |
| 15    |     |
| 16    |     |

The following table describes the labels in this screen.

**Table 36** Access Management > Filter (URL)

| LABEL              | DESCRIPTION   |
|--------------------|---|
| URL Filter Editing |   |
| Active             | Use this field to enable or disable the URL filter. |
| URL Index          | Select the index number of the filter.              |
| URL                | Enter the URL for the P-660RU-Tx to block.          |
| URL Filter Listing |   |

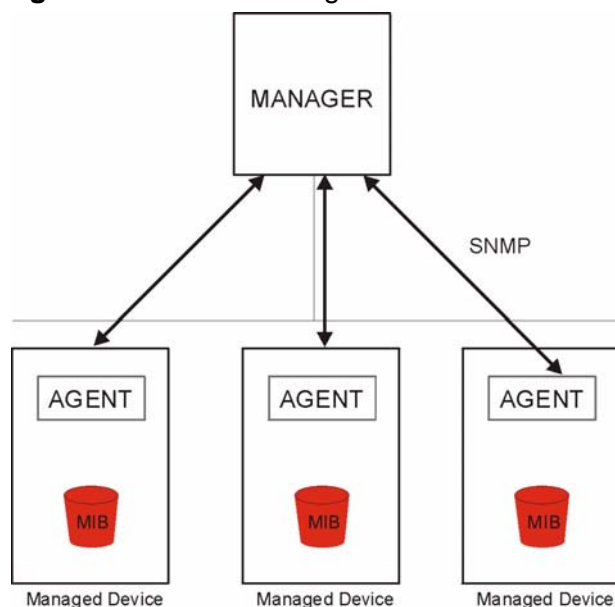
**Table 36** Access Management > Filter (URL) (continued)

| LABEL  | DESCRIPTION  |
|--------|--|
| Index  | This is the index number of the filter rule.                 |
| URL    | This is the URL you have configured the P-660RU-Tx to block. |
| SAVE   | Click this to save your changes.                             |
| DELETE | Click this to remove the filter rule.                        |
| CANCEL | Click this to restore your previously saved settings.        |

## 16.1 Overview

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your P-660RU-Tx supports SNMP agent functionality, which allows a manager station to manage and monitor the P-660RU-Tx through the network. The P-660RU-Tx supports SNMP version one (SNMPv1) and version two (SNMPv2). The next figure illustrates an SNMP management operation.

**Figure 50** SNMP Management Model



An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the P-660RU-Tx). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- Set - Allows the manager to set values for object variables within an agent.

### 16.1.1 Supported MIBs

The P-660RU-Tx supports MIB II, which is defined in RFC-1213 and RFC-1215. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance.

## 16.2 The SNMP Screen

Use this screen to change your P-660RU-Tx's SNMP settings. Click **Access Management > SNMP** to display the following screen.

**Figure 51** Access Management > SNMP

The following table describes the labels in this screen.

**Table 37** Access Management > SNMP

| LABEL         | DESCRIPTION  |
|---------------|--|
| Get Community | Enter the <b>Get Community</b> , which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests. |
| Set Community | Enter the <b>Set community</b> , which is the password for incoming Set requests from the management station. The default is public and allows all requests.                 |
| SAVE          | Click this to save your changes.   |

# Universal Plug-and-Play (UPnP)

## 17.1 Overview

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

### 17.1.1 What You Can Do in the UPnP Screen

Use the **UPnP** screen ([Section 17.2 on page 128](#)) to enable UPnP on the P-660RU-Tx and allow UPnP-enabled applications to automatically configure the P-660RU-Tx.

### 17.1.2 What You Need to Know About UPnP

#### Identifying UPnP Devices

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

#### NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

See the NAT chapter for more information on NAT.

### Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

When a UPnP device joins a network, it announces its presence with a multicast message. For security reasons, the P-660RU-Tx allows multicast messages on the LAN only.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

### UPnP and ZyXEL

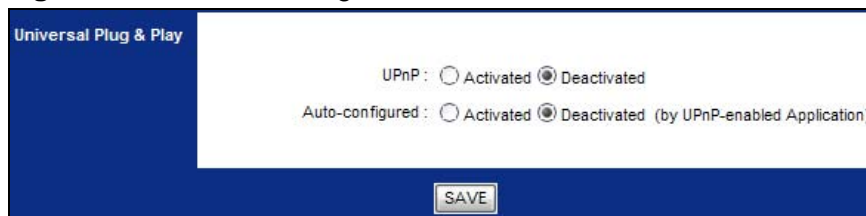
ZyXEL has achieved UPnP certification from the Universal Plug and Play Forum UPnP™ Implementers Corp. (UIC). ZyXEL's UPnP implementation supports Internet Gateway Device (IGD) 1.0.

See the following sections for examples of installing and using UPnP.

## 17.2 The UPnP Screen

Use the following screen to configure the UPnP settings on your P-660RU-Tx. Click **Access Management > UPnP** to display the screen shown next.

**Figure 52** Access Management > UPnP





The following table describes the fields in this screen.

**Table 38** Access Management > UPnP

| LABEL           | DESCRIPTION  |
|-----------------|--|
| UPnP            | Use this field to enable or disable UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the P-660RU-Tx's IP address (although you must still enter the password to access the web configurator).  |
| Auto-configured | Use this field to allow or disable UPnP-enabled applications to automatically configure the P-660RU-Tx so that they can communicate through the P-660RU-Tx, for example by using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application. |
| SAVE            | Click this to save your changes.   |

## 17.3 Installing UPnP in Windows Example

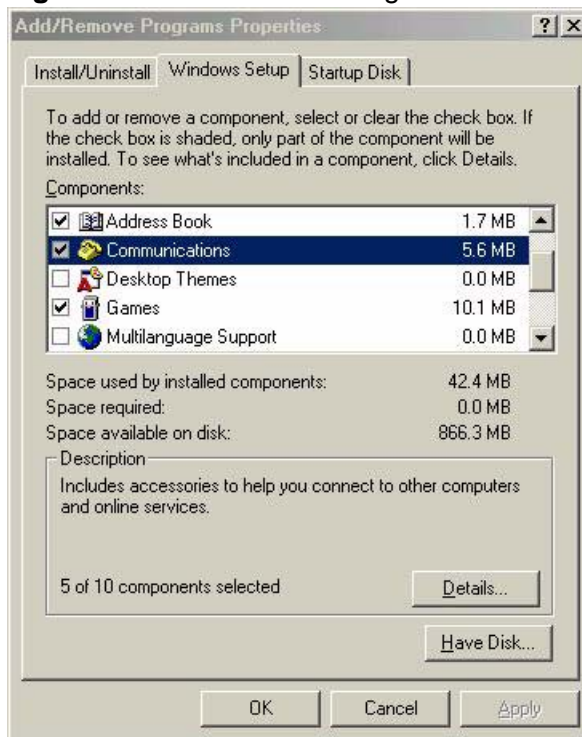
This section shows how to install UPnP in Windows Me and Windows XP.

### Installing UPnP in Windows Me

Follow the steps below to install the UPnP in Windows Me.

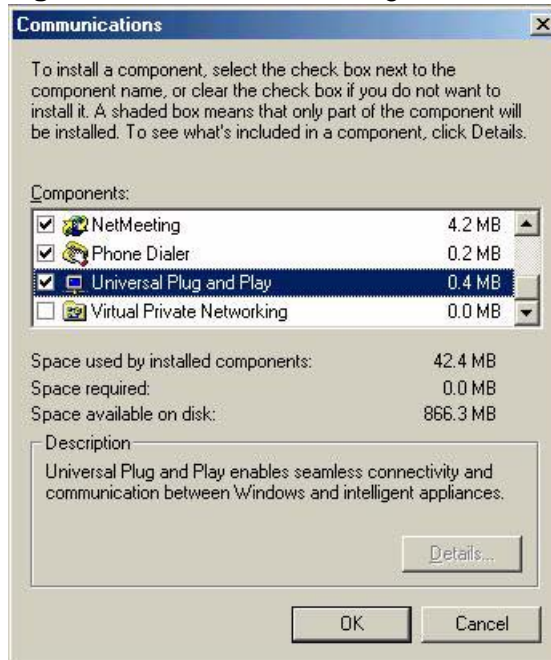
- 1 Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.
- 2 Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.

**Figure 53** Add/Remove Programs: Windows Setup: Communication



- 3 In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.

**Figure 54** Add/Remove Programs: Windows Setup: Communication: Components



- 4 Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.
- 5 Restart the computer when prompted.

### Installing UPnP in Windows XP

Follow the steps below to install the UPnP in Windows XP.

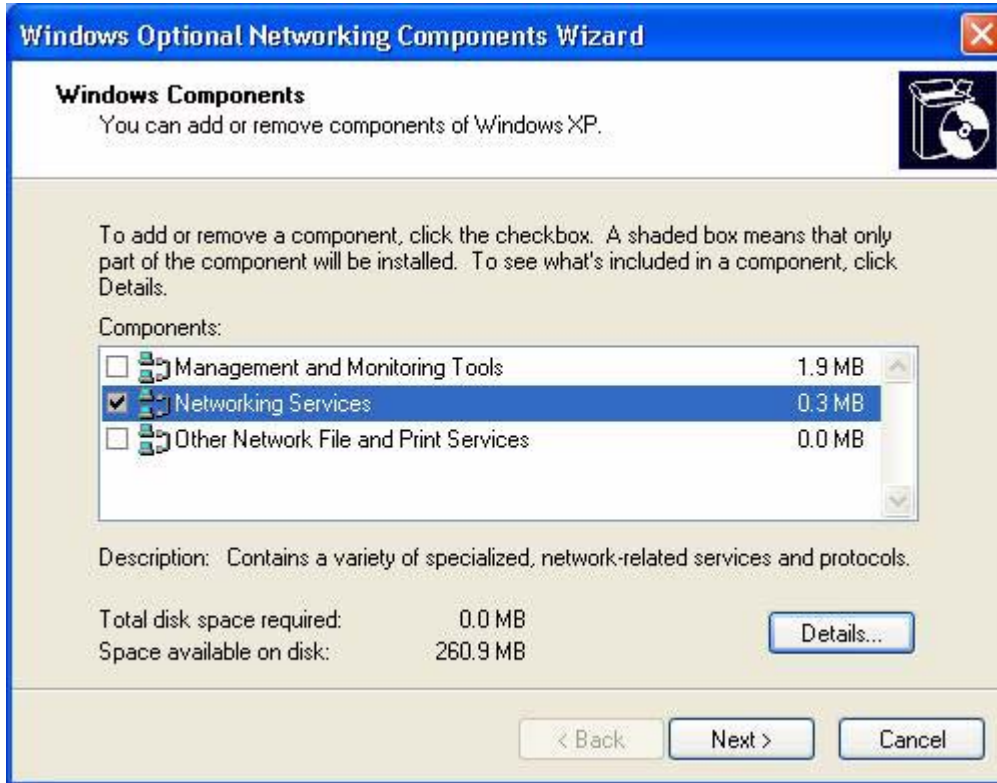
- 1 Click **Start** and **Control Panel**.
- 2 Double-click **Network Connections**.
- 3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ....**

**Figure 55** Network Connections



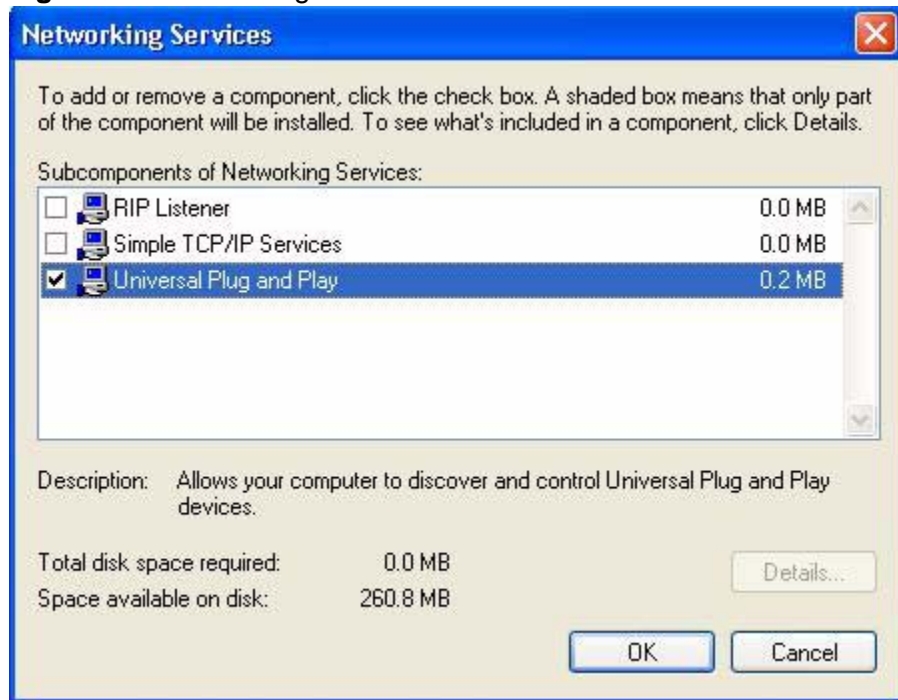
- 4 The **Windows Optional Networking Components Wizard** window displays. Select **Networking Service** in the **Components** selection box and click **Details**.

**Figure 56** Windows Optional Networking Components Wizard



- 5 In the **Networking Services** window, select the **Universal Plug and Play** check box.

**Figure 57** Networking Services



- 6 Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.

## 17.4 Using UPnP in Windows XP Example

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the P-660RU-Tx.

Make sure the computer is connected to a LAN port of the P-660RU-Tx. Turn on your computer and the P-660RU-Tx.

### Auto-discover Your UPnP-enabled Network Device

- 1 Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.

- 2 Right-click the icon and select **Properties**.

**Figure 58** Network Connections



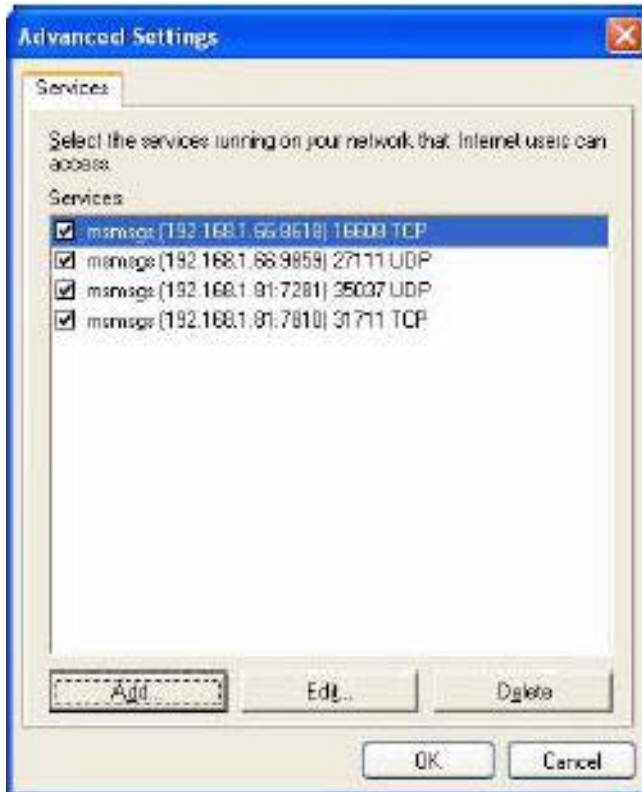
- 3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.

**Figure 59** Internet Connection Properties

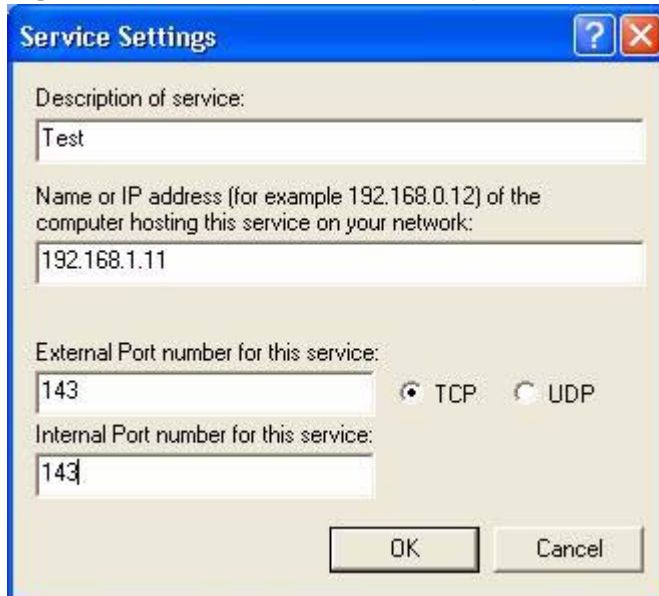


- 4 You may edit or delete the port mappings or click **Add** to manually add port mappings.

**Figure 60** Internet Connection Properties: Advanced Settings



**Figure 61** Internet Connection Properties: Advanced Settings: Add



- 5 When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.



- 6 Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray.

**Figure 62** System Tray Icon



- 7 Double-click on the icon to display your current Internet connection status.

**Figure 63** Internet Connection Status



### Web Configurator Easy Access

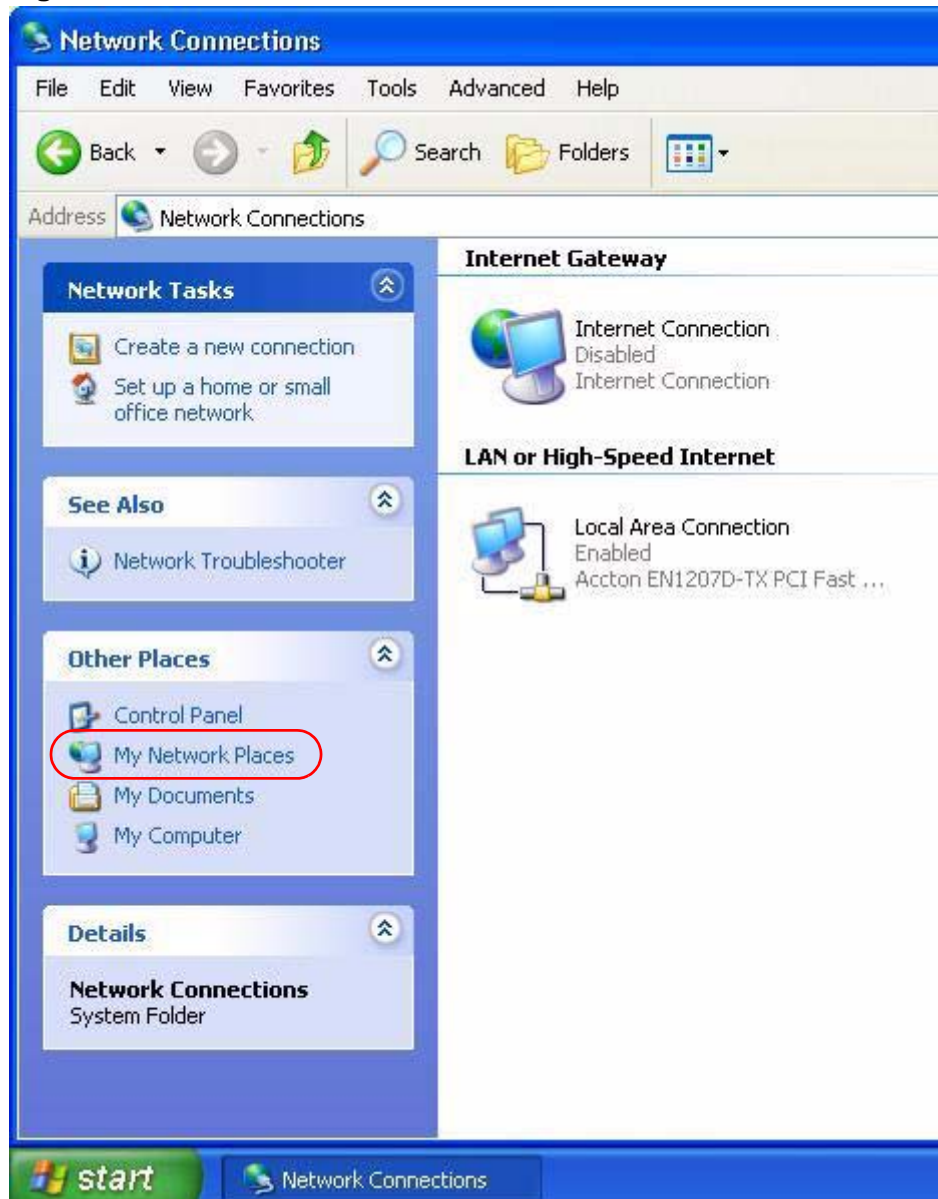
With UPnP, you can access the web-based configurator on the P-660RU-Tx without finding out the IP address of the P-660RU-Tx first. This comes helpful if you do not know the IP address of the P-660RU-Tx.

Follow the steps below to access the web configurator.

- 1 Click **Start** and then **Control Panel**.
- 2 Double-click **Network Connections**.

- 3 Select **My Network Places** under **Other Places**.

**Figure 64** Network Connections



- 4 An icon with the description for each UPnP-enabled device displays under **Local Network**.

- 5 Right-click on the icon for your P-660RU-Tx and select **Invoke**. The web configurator login screen displays.

**Figure 65** Network Connections: My Network Places



- 6 Right-click on the icon for your P-660RU-Tx and select **Properties**. A properties window displays with basic information about the P-660RU-Tx.

**Figure 66** Network Connections: My Network Places: Properties: Example





# Dynamic DNS Setup

## 18.1 Overview

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with [www.dyndns.org](http://www.dyndns.org). This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

### 18.1.1 What You Can Do in the DDNS Screen

Use the **Dynamic DNS** screen ([Section 18.2 on page 142](#)) to enable DDNS and configure the DDNS settings on the P-660RU-Tx.

### 18.1.2 What You Need To Know About DDNS

#### DYNDNS Wildcard

Enabling the wildcard feature for your host causes \*.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

If you have a private WAN IP address, then you cannot use Dynamic DNS.

## 18.2 The Dynamic DNS Screen

Use this screen to change your P-660RU-Tx's DDNS. Click **Access Management > DDNS**. The screen appears as shown.

**Figure 67** Access Management > DDNS

The following table describes the fields in this screen.

**Table 39** Advanced > Dynamic DNS

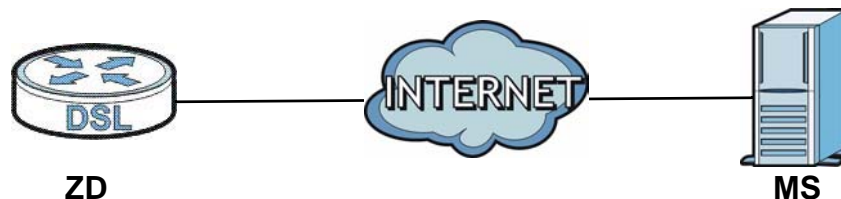
| LABEL            | DESCRIPTION  |
|------------------|--|
| Dynamic DNS      | Use this field to enable or disable dynamic DNS.                               |
| Service Provider | This is the name of your Dynamic DNS service provider.                         |
| My Host Name     | Type the domain name assigned to your P-660RU-Tx by your Dynamic DNS provider. |
| E-mail Address   | Type your e-mail address.  |
| Username         | Type your username.  |
| Password         | Type the password assigned to you.   |
| Wildcard support | Use this field to enable or disable DynDNS Wildcard.                           |
| SAVE             | Click this to save your changes.   |

## 19.1 Overview

The P-660RU-Tx supports TR-069 Amendment 1 (CPE WAN Management Protocol Release 2.0) and TR-069 Amendment 2 (CPE WAN Management Protocol v1.1, Release 3.0).

TR-069 is a protocol that defines how your P-660RU-Tx (**ZD**) can be managed via a management server (**MS**) such as ZyXEL's Vantage Access.

**Figure 68** LAN and WAN



An administrator can use a management server to remotely set up the ZyXEL device, modify settings, perform firmware upgrades as well as monitor and diagnose the ZyXEL device.

In order to use CWMP, you need to configure the following steps:

- 1 Activate CWMP
- 2 Specify the URL, username and password.
- 3 Activate periodic inform and specify an interval value.

## 19.2 The CWMP Setup Screen

Use this screen to configure your P-660RU-Tx to be managed by a management server. Click **Access Management** > **CWMP** to display the following screen.

**Figure 69** Access Management > CWMP

The following table describes the fields in this screen.

**Table 40** Access Management > CWMP

| LINK               | DESCRIPTION  |
|--------------------|--|
| CWMP Setup         |  |
| CWMP               | Select <b>Activated</b> to allow the P-660RU-Tx to be managed by a management server or select <b>Deactivated</b> to not allow the P-660RU-Tx to be managed by a management server.  |
| Login ACS          | Configure this part of the screen to log into the management server.   |
| URL                | Type the IP address or domain name of the management server. If the P-660RU-Tx is behind a NAT router that assigns it a private IP address, you will have to configure a NAT port forwarding rule on the NAT router.   |
| User Name          | The user name is used to authenticate the P-660RU-Tx when making a connection to the management server. This user name on the management server and the P-660RU-Tx must be the same. Type a user name of up to 255 printable characters found on an English-language keyboard. Spaces and characters such as @#\$%^&*()_+ are allowed. |
| Password           | The password is used to authenticate the P-660RU-Tx when making a connection to the management server. This password on the management server and the P-660RU-Tx must be the same. Type a password of up to 255 printable characters found on an English-language keyboard.  |
| Connection Request | Use this part of the screen to allow the management server to connect to the P-660RU-Tx after a successful login.  |
| Path               | Type the IP address or domain name of the P-660RU-Tx. The management server uses this path to verify the P-660RU-Tx.   |



**Table 40** Access Management > CWMP (continued)

| LINK            | DESCRIPTION   |
|-----------------|---|
| Port            | The default port for access to the P-660RU-Tx from the management server is the HTTP port, port 80. If you change it, make sure it does not conflict with another port on your network and it is recommended to use a port number above 1024 (not a commonly used port). The management server should use this port to connect to the P-660RU-Tx. You may need to alter your NAT port forwarding rules if they were already configured. |
| UserName        | The user name is used to authenticate the management server when connecting to the P-660RU-Tx. Type a user name of up to 255 printable characters found on an English-language keyboard. Spaces and characters such as @#\$%^&*()_+ are allowed.  |
| Password        | The password is used to authenticate the management server when connecting to the P-660RU-Tx. Type a password of up to 255 printable characters found on an English-language keyboard. Spaces are not allowed.  |
| Periodic Inform | Select <b>Activated</b> to have the P-660RU-Tx periodically send information to the management server (recommended if CWMP is enabled) or select <b>Deactivated</b> to not have the P-660RU-Tx periodically send information to the management server   |
| Interval        | The interval is the duration in seconds for which the P-660RU-Tx must attempt to connect with the management server to send information and check for configuration updates. Enter a value between 1 and 86400 seconds.   |
| SAVE            | Click this to save your changes.  |
| CANCEL          | Click this to restore your previously saved settings.   |



# Administrator Settings

## 20.1 Overview

This chapter shows you how to change the system password.

## 20.2 The Administrator Screen

Use this screen to set a new password for your P-660RU-Tx. Click **Maintenance > Administration** to open the following screen.

**Figure 70** Maintenance > Administration

The screenshot shows a web interface titled 'Administrator'. It features a blue sidebar on the left. The main content area has a white background with the following elements: 'Username : admin', 'New Password :' followed by a text input field, 'Confirm Password :' followed by another text input field, and two buttons labeled 'SAVE' and 'CANCEL' at the bottom.

The following table describes the labels in this screen.

**Table 41** Maintenance > Administration

| LABEL            | DESCRIPTION  |
|------------------|--|
| New Password     | Type your new password (up to 30 characters). Note that as you type a password, the screen displays a (*) for each character you type. After you change the password, use the new password to access the P-660RU-Tx. |
| Confirm Password | Type the new password again for confirmation.  |
| SAVE             | Click this to save your changes.   |
| CANCEL           | Click this to restore your previously saved settings.  |



## Time Zone

### 21.1 Overview

This chapter contains information about configuring your P-660RU-Tx's time settings.

### 21.2 The Time Zone Screen

Use this screen to configure the P-660RU-Tx's time based on your local time zone. To change your P-660RU-Tx's time and date, click **Maintenance > Time Zone**. The screen appears as shown.

**Figure 71** Maintenance > Time Zone

The following table describes the fields in this screen.

**Table 42** Maintenance > Time Zone

| LABEL                | DESCRIPTION   |
|----------------------|---|
| Time Zone            |   |
| Current Date/Time    | This field displays the date and time of your P-660RU-Tx. |
| Time Synchronization |   |

**Table 42** Maintenance > Time Zone (continued)

| LABEL                 | DESCRIPTION  |
|-----------------------|--|
| Synchronize time with | <p>Select <b>NTP Server automatically</b> to have the P-660RU-Tx get the time and date from the time server. The NTP server displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.</p> <p>Select <b>PC's Clock</b> to have the P-660RU-Tx synchronize the time with your PC.</p> <p>Select <b>Manually</b> to enter the time and date manually.</p> |
| Time Zone             | Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).   |
| Daylight Saving       | <p>Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.</p> <p>Select <b>Enabled</b> if you use Daylight Saving Time.</p>   |
| NTP Server Address    | Enter the IP address or URL (up to 20 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information.   |
| Date                  | This field is only available when you want to set the time and date manually. Enter the date in this field.  |
| Time                  | This field is only available when you want to set the time and date manually. Enter the time in this field.  |
| SAVE                  | Click this to save your changes.   |
| CANCEL                | Click this to restore your previously saved settings.  |

# Firmware

## 22.1 Overview

This chapter explains how to upload new firmware and manage configuration files.

Use the instructions in this chapter to change the device's configuration file or upgrade its firmware. After you configure your device, you can backup the configuration file to a computer. That way if you later misconfigure the device, you can upload the backed up configuration file to return to your previous settings. You can alternately upload the factory default configuration file if you want to return the device to the original default settings. The firmware determines the device's available features and functionality. You can download new firmware releases from your nearest ZyXEL FTP site (or [www.zyxel.com](http://www.zyxel.com)) to use to upgrade your device's performance.

**Only use firmware for your device's specific model. Refer to the label on the bottom of your P-660RU-Tx.**

### 22.1.1 What You Need To Know About Firmware

#### Filename Conventions

The configuration file (often called the romfile or rom-0) contains the factory default settings in the menus such as password, DHCP Setup, TCP/IP Setup, etc. It arrives from ZyXEL with a "rom" filename extension. Once you have customized the P-660RU-Tx's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (ZyXEL Network Operating System sometimes referred to as the "ras" file) is the system firmware and has a "bin" filename extension. Find this firmware at [www.zyxel.com](http://www.zyxel.com). With many FTP and TFTP clients, the filenames are similar to those seen next.

```
ftp> put firmware.bin ras
```

This is a sample FTP session showing the transfer of the computer file "firmware.bin" to the P-660RU-Tx.

```
ftp> get rom-0 config.cfg
```

This is a sample FTP session saving the current configuration to the computer file "config.cfg".

If your (T)FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the P-660RU-Tx only recognizes "rom-0" and "ras". Be sure you keep unaltered copies of both files for later use.

The following table is a summary. Please note that the internal filename refers to the filename on the P-660RU-Tx and the external filename refers to the filename not on the P-660RU-Tx, that is, on your computer, local network or FTP site and so the name (but not the extension) may vary. After uploading new firmware, see the **Status** screen to confirm that you have uploaded the correct firmware version.

**Table 43** Filename Conventions

| FILE TYPE          | INTERNAL NAME | EXTERNAL NAME  | DESCRIPTION |
|--------------------|---------------|--|-------------|
| Configuration File | Rom-0         | This is the configuration filename on the P-660RU-Tx. Uploading the rom-0 file replaces the entire ROM file system, including your P-660RU-Tx configurations, system-related data (including the default password), the error log and the trace log. | *.rom       |
| Firmware           | Ras           | This is the generic name for the ZYNOS firmware on the P-660RU-Tx.   | *.bin       |

### FTP Restrictions

FTP will not work when:

- 1 You have disabled the FTP service in the **Remote Management** screen.
- 2 The IP you entered in the Secured Client IP field does not match the client IP. If it does not match, the device will disallow the FTP session.

## 22.1.2 Before You Begin

Make sure the FTP service has not been disabled in the Remote Management screen.



## 22.1.3 Firmware and Configuration Files Examples

This section contains examples about managing configuration files and uploading firmware to your P-660RU-Tx.

### Using FTP to Restore Configuration

This example shows you how to restore a previously saved configuration. Note that this function erases the current configuration before restoring a previous backup configuration; please do not attempt to restore unless you have a backup configuration file stored on disk.

FTP is the preferred method for restoring your current computer configuration to your device since FTP is faster. Please note that you must wait for the system to automatically restart after the file transfer is complete.

**Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE your device. When the Restore Configuration process is complete, the device automatically restarts.**

### Restore Using FTP Session Example

**Figure 72** Restore Using FTP Session Example

```
ftp> put config.rom rom-0
200 Port command okay
150 Opening data connection for STOR rom-0
226 File received OK
221 Goodbye for writing flash
ftp: 16384 bytes sent in 0.06Seconds 273.07Kbytes/sec.
ftp>quit
```

Refer to [Section 22.1.1 on page 151](#) to read about configurations that disallow TFTP and FTP over WAN.

### FTP and TFTP Firmware and Configuration File Uploads

These examples show you how to upload firmware and configuration files.

**Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE your device.**

FTP is the preferred method for uploading the firmware and configuration. To use this feature, your computer must have an FTP client. The following sections give examples of how to upload the firmware and the configuration files.

## FTP File Upload Command from the DOS Prompt Example

- 1 Launch the FTP client on your computer.
- 2 Enter "open", followed by a space and the IP address of your device.
- 3 Press [ENTER] when prompted for a username.
- 4 Enter your password as requested (the default is "1234").
- 5 Enter "bin" to set transfer mode to binary.
- 6 Use "put" to transfer files from the computer to the device, for example, "put firmware.bin ras" transfers the firmware on your computer (firmware.bin) to the device and renames it "ras". Similarly, "put config.rom rom-0" transfers the configuration file on your computer (config.rom) to the device and renames it "rom-0". Likewise "get rom-0 config.rom" transfers the configuration file on the device to your computer and renames it "config.rom." See earlier in this chapter for more information on filename conventions.
- 7 Enter "quit" to exit the ftp prompt.

## FTP Session Example of Firmware File Upload

**Figure 73** FTP Session Example of Firmware File Upload

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 1103936 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

More commands (found in GUI-based FTP clients) are listed in this chapter.

Refer to [Section 22.1.1 on page 151](#) to read about configurations that disallow TFTP and FTP over WAN.

## TFTP File Upload

The device also supports the uploading of firmware files using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To transfer the firmware and the configuration file, follow the procedure shown next.

- 1 Use telnet from your computer to connect to the device and log in. Because TFTP does not have any security checks, the device records the IP address of the telnet client and accepts TFTP requests only from this address.
- 2 Enter the command "sys stdio 0" to disable the management idle timeout, so the TFTP transfer will not be interrupted. Enter "command sys stdio 5" to restore the five-minute management idle timeout (default) when the file transfer is complete.
- 3 Launch the TFTP client on your computer and connect to the device. Set the transfer mode to binary before starting data transfer.
- 4 Use the TFTP client (see the example below) to transfer files between the device and the computer. The file name for the firmware is "ras".

Note that the telnet connection must be active and the device in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use "get" to transfer from the device to the computer, "put" the other way around, and "binary" to set binary transfer mode.

### TFTP Upload Command Example

The following is an example TFTP command:

```
tftp [-i] host put firmware.bin ras
```

Where "i" specifies binary image transfer mode (use this mode when transferring binary files), "host" is the device's IP address, "put" transfers the file source on the computer (firmware.bin – name of the firmware on the computer) to the file destination on the remote host (ras - name of the firmware on the device).

Commands that you may see in GUI-based TFTP clients are listed earlier in this chapter.

### Using the FTP Commands to Back Up Configuration

- 1 Launch the FTP client on your computer.
- 2 Enter "open", followed by a space and the IP address of your P-660RU-Tx.
- 3 Press [ENTER] when prompted for a username.
- 4 Enter your password as requested (the default is "1234").

- 5 Enter "bin" to set transfer mode to binary.
- 6 Use "get" to transfer files from the P-660RU-Tx to the computer, for example, "get rom-0 config.rom" transfers the configuration file on the P-660RU-Tx to your computer and renames it "config.rom". See earlier in this chapter for more information on filename conventions.
- 7 Enter "quit" to exit the ftp prompt.

### FTP Command Configuration Backup Example

This figure gives an example of using FTP commands from the DOS command prompt to save your device's configuration onto your computer.

**Figure 74** FTP Session Example

```

331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> get rom-0 zyxel.rom
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 16384 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit

```

### Configuration Backup Using GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

**Table 44** General Commands for GUI-based FTP Clients

| COMMAND                  | DESCRIPTION   |
|--------------------------|---|
| Host Address             | Enter the address of the host server.   |
| Login Type               | Anonymous.<br><br>This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option.<br><br>Normal.<br><br>The server requires a unique User ID and Password to login. |
| Transfer Type            | Transfer files in either ASCII (plain text format) or in binary mode.   |
| Initial Remote Directory | Specify the default remote directory (path).  |
| Initial Local Directory  | Specify the default local directory (path).   |

## 22.2 The Firmware Screen

Use this screen to manage configuration files and upload firmware to your P-660RU-Tx.

### Firmware Upgrade

Follow the instructions in this screen to upload firmware to your P-660RU-Tx. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot. See [Section 22.1.3 on page 153](#) for upgrading firmware using FTP/TFTP commands.

**Do NOT turn off the P-660RU-Tx while firmware upload is in progress!**

### Romfile Backup

Romfile backup allows you to back up (save) the P-660RU-Tx's current configuration to a file on your computer. Once your P-660RU-Tx is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Maintenance > Firmware** to open the following screen.

**Figure 75** Maintenance > Firmware

The following table describes the labels in this screen.

**Table 45** Maintenance > Firmware

| LABEL                    | DESCRIPTION  |
|--------------------------|--|
| Current Firmware Version | This is the present firmware version and the date created.   |
| New Firmware Location    | Click <b>Browse...</b> to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them. |

**Table 45** Maintenance > Firmware (continued)

| LABEL                | DESCRIPTION  |
|----------------------|--|
| New Romfile Location | This allows you to upload a new or previously saved configuration file from your computer to your P-660RU-Tx.<br><br>Click <b>Browse...</b> to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them. |
| Romfile Backup       | Click this to save the P-660RU-Tx's current configuration to your computer.  |
| UPGRADE              | Click this to begin the upload process.  |

# System Restart

## 23.1 Overview

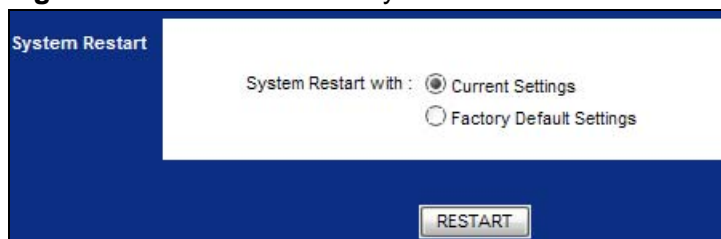
This chapter shows you how to restart your P-660RU-Tx.

## 23.2 The System Restart Screen

System restart allows you to reboot the P-660RU-Tx remotely without turning the power off. You may need to do this if the P-660RU-Tx hangs, for example.

Click **Maintenance** > **SysRestart** to open the following screen.

**Figure 76** Maintenance > System Restart



The following table describes the labels in this screen.

**Table 46** Maintenance > System Restart

| LABEL               | DESCRIPTION  |
|---------------------|--|
| System Restart with | Select <b>Current Settings</b> to keep your configuration settings after the P-660RU-Tx reboots. This does not affect the P-660RU-Tx's configuration.<br><br>Select <b>Factory Default Settings</b> to clear all user-defined configuration information and return the P-660RU-Tx to its factory defaults. |
| RESTART             | Click this to reboot the P-660RU-Tx.   |





# Diagnostic

## 24.1 Overview

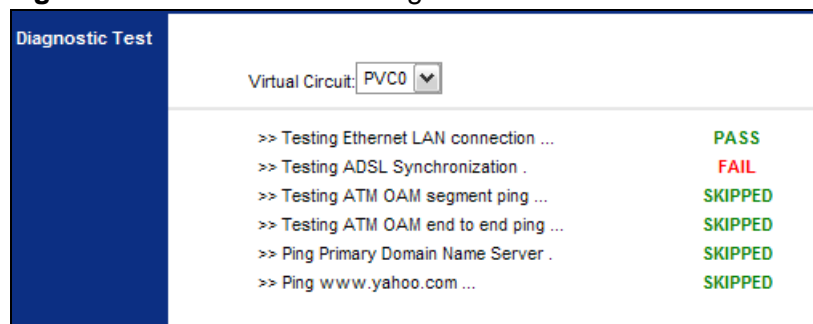
These read-only screens display information to help you identify problems with the P-660RU-Tx.

## 24.2 The Diagnostic Screen

Use this screen to test your connection and ping an IP address. Select the virtual circuit you want to check from the drop-down list box.

Click **Maintenance > Diagnostic** to open the screen shown next.

**Figure 77** Maintenance > Diagnostic





# Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- [Power, Hardware Connections, and LEDs](#)
- [P-660RU-Tx Access and Login](#)
- [Internet Access](#)

## 25.1 Power, Hardware Connections, and LEDs

---

The P-660RU-Tx does not turn on. None of the LEDs turn on.

---

- 1 Make sure the P-660RU-Tx is turned on.
- 2 Make sure you are using the power adaptor or cord included with the P-660RU-Tx.
- 3 Make sure the power adaptor or cord is connected to the P-660RU-Tx and plugged in to an appropriate power source. Make sure the power source is turned on.
- 4 Turn the P-660RU-Tx off and on.
- 5 If the problem continues, contact the vendor.

---

One of the LEDs does not behave as expected.

---

- 1 Make sure you understand the normal behavior of the LED. See [Section 1.5 on page 28](#).
- 2 Check the hardware connections. See the Quick Start Guide.

- 3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.
- 4 Turn the P-660RU-Tx off and on.
- 5 If the problem continues, contact the vendor.

## 25.2 P-660RU-Tx Access and Login

---

### I forgot the IP address for the P-660RU-Tx.

---

- 1 The default IP address is **192.168.1.1**.
- 2 If you changed the IP address and have forgotten it, you might get the IP address of the P-660RU-Tx by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the P-660RU-Tx (it depends on the network), so enter this IP address in your Internet browser.
- 3 If this does not work, you have to reset the device to its factory defaults. See [Section 1.6 on page 29](#).

---

### I forgot the password.

---

- 1 The default password is **1234**.
- 2 If this does not work, you have to reset the device to its factory defaults. See [Section 1.6 on page 29](#).

---

### I cannot see or access the **Login** screen in the web configurator.

---

- 1 Make sure you are using the correct IP address.
  - The default IP address is **192.168.1.1**.
  - If you changed the IP address ([Section 8.2 on page 77](#)), use the new IP address.

- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for [I forgot the IP address for the P-660RU-Tx](#).
- 2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.
  - 3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled. See [Appendix B on page 199](#).
  - 4 If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See [Appendix A on page 175](#). Your P-660RU-Tx is a DHCP server by default.
    - If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the P-660RU-Tx. See [Appendix A on page 175](#).
  - 5 Reset the device to its factory defaults, and try to access the P-660RU-Tx with the default IP address. See [Section 1.6 on page 29](#).
  - 6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

### Advanced Suggestions

- Try to access the P-660RU-Tx using another service, such as Telnet. If you can access the P-660RU-Tx, check the remote management settings and firewall rules to find out why the P-660RU-Tx does not respond to HTTP.
- If your computer is connected to the **WAN** port, use a computer that is connected to a **ETHERNET** port.

---

I can see the [Login](#) screen, but I cannot log in to the P-660RU-Tx.

---

- 1 Make sure you have entered the password correctly. The default password is **1234**. The field is case-sensitive, so make sure [Caps Lock] is not on.
- 2 You cannot log in to the web configurator while someone is using Telnet to access the P-660RU-Tx. Log out of the P-660RU-Tx in the other session, or ask the person who is logged in to log out.
- 3 Turn the P-660RU-Tx off and on.
- 4 If this does not work, you have to reset the device to its factory defaults. See [Section 1.6 on page 29](#).

---

### I cannot Telnet to the P-660RU-Tx.

---

See the troubleshooting suggestions for [I cannot see or access the Login screen in the web configurator](#). Ignore the suggestions about your browser.

---

### I cannot use FTP to upload / download the configuration file. / I cannot use FTP to upload new firmware.

---

See the troubleshooting suggestions for [I cannot see or access the Login screen in the web configurator](#). Ignore the suggestions about your browser.

## 25.3 Internet Access

---

### I cannot access the Internet.

---

- 1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and [Section 1.5 on page 28](#).
- 2 Make sure you entered your ISP account information correctly in the wizard. These fields are case-sensitive, so make sure [Caps Lock] is not on.
- 3 If you are trying to access the Internet wirelessly, make sure the wireless settings in the wireless client are the same as the settings in the AP.
- 4 Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
- 5 If the problem continues, contact your ISP.

---

### I cannot access the Internet anymore. I had access to the Internet (with the P-660RU-Tx), but my Internet connection is not available anymore.

---

- 1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and [Section 1.5 on page 28](#).

- 2 Turn the P-660RU-Tx off and on.
- 3 If the problem continues, contact your ISP.

---

### The Internet connection is slow or intermittent.

---

- 1 There might be a lot of traffic on the network. Look at the LEDs, and check [Section 1.5 on page 28](#). If the P-660RU-Tx is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
- 2 Check the signal strength. If the signal strength is low, try moving your computer closer to the P-660RU-Tx if possible, and look around to see if there are any devices that might be interfering with the wireless network (for example, microwaves, other wireless networks, and so on).
- 3 Turn the P-660RU-Tx off and on.
- 4 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

#### **Advanced Suggestions**

- Check the settings for QoS. If it is disabled, you might consider activating it. If it is enabled, you might consider raising or lowering the priority for some applications.





# Product Specifications

The following tables summarize the P-660RU-Tx's hardware and firmware features.

## 26.1 Hardware Specifications

**Table 47** Hardware Specifications

|                       |  |
|-----------------------|--|
| Dimensions            | (110 W) x (107 D) x (36 H) mm                                      |
| Weight                | 165 g  |
| Power Specification   | 5V DC 1A Switching   |
| LAN Ethernet Port     | 1 auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet port |
| ADSL Port             | 1 RJ-11 FXS POTS port  |
| USB Port              | 1 USB 1.1 port   |
| RESET Button          | Restores factory defaults  |
| Operation Temperature | 0° C ~ 40° C   |
| Storage Temperature   | -20° ~ 60° C   |
| Operation Humidity    | 20% ~ 85% RH   |
| Storage Humidity      | 20% ~ 90% RH   |

## 26.2 Firmware Specifications

**Table 48** Firmware Specifications

|                     |                         |
|---------------------|-------------------------|
| Default IP Address  | 192.168.1.1             |
| Default Subnet Mask | 255.255.255.0 (24 bits) |
| Default Username    | admin                   |
| Default Password    | 1234                    |

**Table 48** Firmware Specifications (continued)

|  |  |
|--|--|
| DHCP Server IP Pool                        | 192.168.1.32 to 192.168.1.64   |
| Device Management                          | Use the web configurator to easily configure the rich range of features on the P-660RU-Tx.   |
| Firmware Upgrade                           | Download new firmware (when available) from the ZyXEL web site and use the web configurator, an FTP or a TFTP tool to put it on the P-660RU-Tx.<br><br><b>Note: Only upload firmware for your specific model!</b>  |
| Configuration Backup & Restoration         | Make a copy of the P-660RU-Tx's configuration. You can put it back on the P-660RU-Tx later if you decide to revert back to an earlier configuration.   |
| Network Address Translation (NAT)          | Each computer on your network must have its own unique IP address. Use NAT to convert your public IP address(es) to multiple private IP addresses for the computers on your network.   |
| Port Forwarding                            | If you have a server (mail or web server for example) on your network, you can use this feature to let people access it from the Internet.   |
| DHCP (Dynamic Host Configuration Protocol) | Use this feature to have the P-660RU-Tx assign IP addresses, an IP default gateway and DNS servers to computers on your network. Your device can also act as a surrogate DHCP server (DHCP Relay) where it relays IP address assignment from the actual real DHCP server to the clients. |
| Dynamic DNS Support                        | With Dynamic DNS (Domain Name System) support, you can use a fixed URL, <a href="http://www.zyxel.com">www.zyxel.com</a> for example, with a dynamic IP address. You must register for this service with a Dynamic DNS service provider.   |
| IP Multicast                               | IP multicast is used to send traffic to a specific group of computers. The P-660RU-Tx supports versions 1 and 2 of IGMP (Internet Group Management Protocol) used to join multicast groups (see RFC 2236).   |
| Time and Date                              | Get the current time and date from an external server when you turn on your P-660RU-Tx. You can also set the time manually. These dates and times are then used in logs.   |
| Logs                                       | Use logs for troubleshooting.  |
| Universal Plug and Play (UPnP)             | A UPnP-enabled device can dynamically join a network, obtain an IP address and convey its capabilities to other devices on the network.  |
| Firewall                                   | Your device has a stateful inspection firewall with DoS (Denial of Service) protection. By default, when the firewall is activated, all incoming traffic from the WAN to the LAN is blocked unless it is initiated from the LAN.   |
| IP/MAC Address Filters                     | Your device's packet filtering function allows added network security and management.  |
| Application Filter                         | Application filter allows you to block instant messaging programs.   |
| URL Filter                                 | URL filter allows you to block access to Internet web sites that contain key words (that you specify) in the URL.  |
| QoS (Quality of Service)                   | You can efficiently manage traffic on your network by reserving bandwidth and giving priority to certain types of traffic and/or to particular computers.  |

**Table 48** Firmware Specifications (continued)

|   |  |
|---|--|
| Remote Management                                 | This allows you to decide whether a service (HTTP or FTP traffic for example) from a computer on a network (LAN or WAN for example) can access the P-660RU-Tx.   |
| PPPoE Support (RFC2516)                           | PPPoE (Point-to-Point Protocol over Ethernet) emulates a dial-up connection. It allows your ISP to use their existing network configuration with newer broadband technologies such as ADSL. The PPPoE driver on your device is transparent to the computers on the LAN, which see only Ethernet and are not aware of PPPoE thus saving you from having to manage PPPoE clients on individual computers.  |
| Other PPPoE Features                              | PPPoE idle time out<br>PPPoE dial on demand  |
| Multiple PVC (Permanent Virtual Circuits) Support | Your device supports up to 8 Permanent Virtual Circuits (PVCs).  |
| ADSL Standards                                    | ANSI T1.413, Issue 2; G.dmt (G.992.1); G.lite (G.992.2)<br>ADSL2 G.dmt.bis (G.992.3)<br>ADSL2 G.lite.bis (G.992.4)<br>ADSL2+ (G.992.5)<br>Reach-Extended ADSL (RE ADSL)<br>SRA (Seamless Rate Adaptation)<br>Auto-negotiating rate adaptation<br>ADSL physical connection ATM AAL5 (ATM Adaptation Layer type 5)<br>Multi-protocol over AAL5 (RFC2684/1483)<br>PPP over ATM AAL5 (RFC2364)<br>PPP over Ethernet for DSL connection (RFC2516)<br>VC-based and LLC-based multiplexing<br>I.610 F4/F5 OAM<br>Annex A/B/I/J/L/M<br>TR-067/TR-100 |

**Table 48** Firmware Specifications (continued)

|                        |   |
|------------------------|---|
| Other Protocol Support | PPP (Point-to-Point Protocol) link layer protocol<br>IP routing<br>Transparent bridging for unsupported network layer protocols<br>RIP I/RIP II<br>ICMP<br>ATM QoS<br>SNMP v1 and v2c with MIB II support (RFC 1213)<br>IP Multicasting IGMP v1, v2 and v3<br>IGMP Proxy  |
| Management             | Embedded Web Configurator<br>CLI (Command Line Interpreter)<br>SNMP v1 & v2c with MIB II<br>Embedded FTP/TFTP Server for firmware upgrade and configuration file backup and restore<br>Telnet for remote management<br>Remote Management Control: Telnet, FTP, Web, SNMP and DNS.<br>Remote Firmware Upgrade<br>Syslog<br>TR-069<br>F4/F5 OAM |

The following list, which is not exhaustive, illustrates the standards supported in the P-660RU-Tx.

**Table 49** Standards Supported

| STANDARD | DESCRIPTION   |
|----------|---|
| RFC 867  | Daytime Protocol  |
| RFC 868  | Time Protocol.  |
| RFC 1058 | RIP-1 (Routing Information Protocol)                    |
| RFC 1112 | IGMP v1   |
| RFC 1157 | SNMPv1: Simple Network Management Protocol version 1    |
| RFC 1305 | Network Time Protocol (NTP version 3)                   |
| RFC 1441 | SNMPv2 Simple Network Management Protocol version 2     |
| RFC 1483 | Multiprotocol Encapsulation over ATM Adaptation Layer 5 |
| RFC 1631 | IP Network Address Translator (NAT)                     |
| RFC 1661 | The Point-to-Point Protocol (PPP)                       |
| RFC 1723 | RIP-2 (Routing Information Protocol)                    |
| RFC 1901 | SNMPv2c Simple Network Management Protocol version 2c   |

**Table 49** Standards Supported (continued)

| STANDARD                 | DESCRIPTION  |
|--------------------------|--|
| RFC 2236                 | Internet Group Management Protocol, Version 2.   |
| RFC 2364                 | PPP over AAL5 (PPP over ATM over ADSL)   |
| RFC 2408                 | Internet Security Association and Key Management Protocol (ISAKMP)   |
| RFC 2516                 | A Method for Transmitting PPP Over Ethernet (PPPoE)  |
| RFC 2684                 | Multiprotocol Encapsulation over ATM Adaptation Layer 5.   |
| RFC 2766                 | Network Address Translation - Protocol   |
| ANSI T1.413, Issue 2     | Asymmetric Digital Subscriber Line (ADSL) standard.  |
| G dmt(G.992.1)           | G.992.1 Asymmetrical Digital Subscriber Line (ADSL) Transceivers   |
| ITU G.992.1 (G.DMT)      | ITU standard for ADSL using discrete multitone modulation.   |
| ITU G.992.2 (G. Lite)    | ITU standard for ADSL using discrete multitone modulation.   |
| ITU G.992.3 (G.dmt.bis)  | ITU standard (also referred to as ADSL2) that extends the capability of basic ADSL in data rates.                              |
| ITU G.992.4 (G.lite.bis) | ITU standard (also referred to as ADSL2) that extends the capability of basic ADSL in data rates.                              |
| ITU G.992.5 (ADSL2+)     | ITU standard (also referred to as ADSL2+) that extends the capability of basic ADSL by doubling the number of downstream bits. |
| Microsoft PPTP           | MS PPTP (Microsoft's implementation of Point to Point Tunneling Protocol)  |
| MBM v2                   | Media Bandwidth Management v2  |
| RFC 2383                 | ST2+ over ATM Protocol Specification - UNI 3.1 Version   |
| TR-069                   | TR-069 DSL Forum Standard for CPE Wan Management.  |
| 1.363.5                  | Compliant AAL5 SAR (Segmentation And Re-assembly)  |

## 26.3 Power Adaptor Specifications

**Table 50** P-660RU-Tx Series Power Adaptor Specifications

| NORTH AMERICAN PLUG STANDARDS |                              |
|-------------------------------|------------------------------|
| AC Power Adapter Model        | 5V DC US Switching           |
| Input Power                   | AC 100-240Volts, 50/60Hz     |
| Output Power                  | DC 5Volts/1.0A               |
| Power Consumption             | 5 Watt max                   |
| Safety Standards              | ANSI/UL 60950-1, CSA 60950-1 |

**Table 50** P-660RU-Tx Series Power Adaptor Specifications (continued)

|                                      |                          |
|--------------------------------------|--------------------------|
| <b>EUROPEAN PLUG STANDARDS</b>       |                          |
| AC Power Adapter Model               | 5V DC EU Switching       |
| Input Power                          | AC 100-240Volts, 50/60Hz |
| Output Power                         | DC 5Volts/1.0A           |
| Power Consumption                    | 5 Watt max               |
| Safety Standards                     | CE, GS or TUV, EN60950-1 |
| <b>UNITED KINGDOM PLUG STANDARDS</b> |                          |
| AC Power Adapter Model               | 5V DC UK Switching       |
| Input Power                          | AC 100-240Volts, 50/60Hz |
| Output Power                         | DC 5Volts/1.0A           |
| Power Consumption                    | 5 Watt max               |
| Safety Standards                     | CE, GS or TUV, EN60950-1 |

# Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP/Vista, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

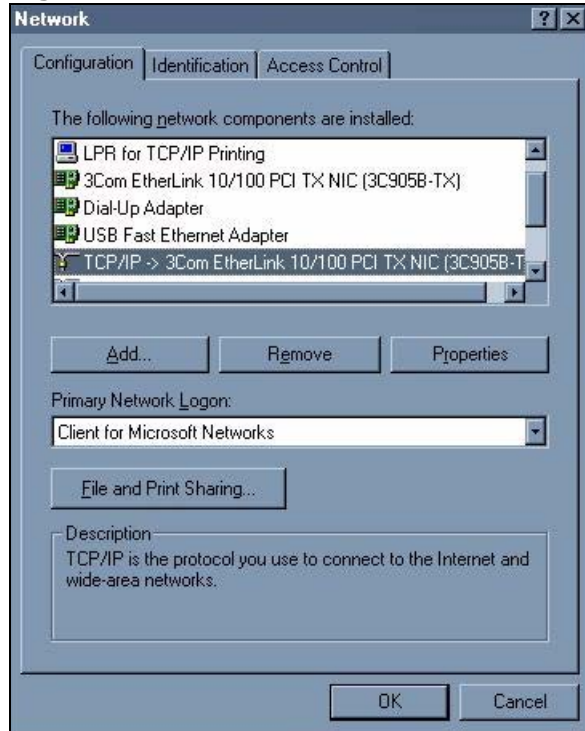
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the P-660RU-Tx's LAN port.

## Windows 95/98/Me

Click **Start, Settings, Control Panel** and double-click the **Network** icon to open the **Network** window.

**Figure 78** Windows 95/98/Me: Network: Configuration



### Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

- 1 In the **Network** window, click **Add**.
- 2 Select **Adapter** and then click **Add**.
- 3 Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

- 1 In the **Network** window, click **Add**.
- 2 Select **Protocol** and then click **Add**.



- 3 Select **Microsoft** from the list of **manufacturers**.
- 4 Select **TCP/IP** from the list of network protocols and then click **OK**.

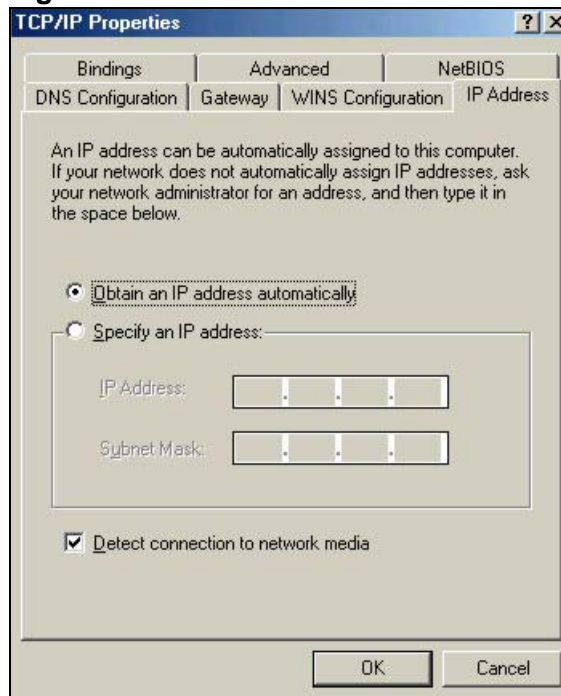
If you need Client for Microsoft Networks:

- 1 Click **Add**.
- 2 Select **Client** and then click **Add**.
- 3 Select **Microsoft** from the list of manufacturers.
- 4 Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.
- 5 Restart your computer so the changes you made take effect.

## Configuring

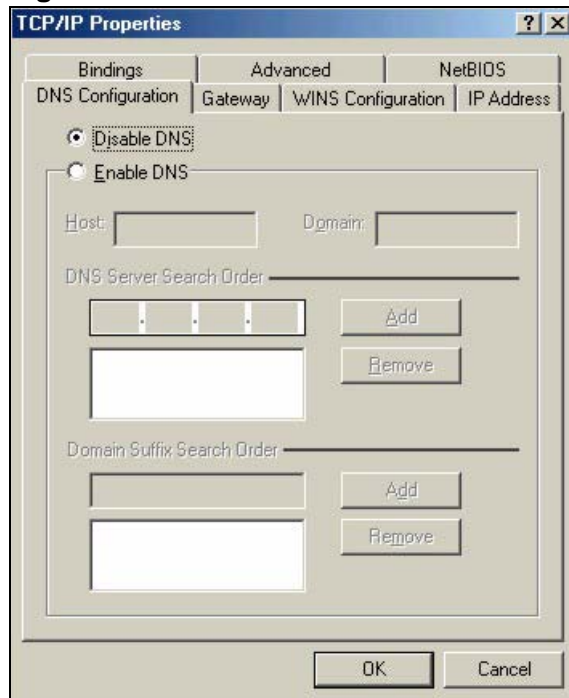
- 1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**
- 2 Click the **IP Address** tab.
  - If your IP address is dynamic, select **Obtain an IP address automatically**.
  - If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

**Figure 79** Windows 95/98/Me: TCP/IP Properties: IP Address



- 3 Click the **DNS** Configuration tab.
  - If you do not know your DNS information, select **Disable DNS**.
  - If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

**Figure 80** Windows 95/98/Me: TCP/IP Properties: DNS Configuration



- 4 Click the **Gateway** tab.
  - If you do not know your gateway's IP address, remove previously installed gateways.
  - If you have a gateway IP address, type it in the **New gateway field** and click **Add**.
- 5 Click **OK** to save and close the **TCP/IP Properties** window.
- 6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.
- 7 Turn on your P-660RU-Tx and restart your computer when prompted.

## Verifying Settings

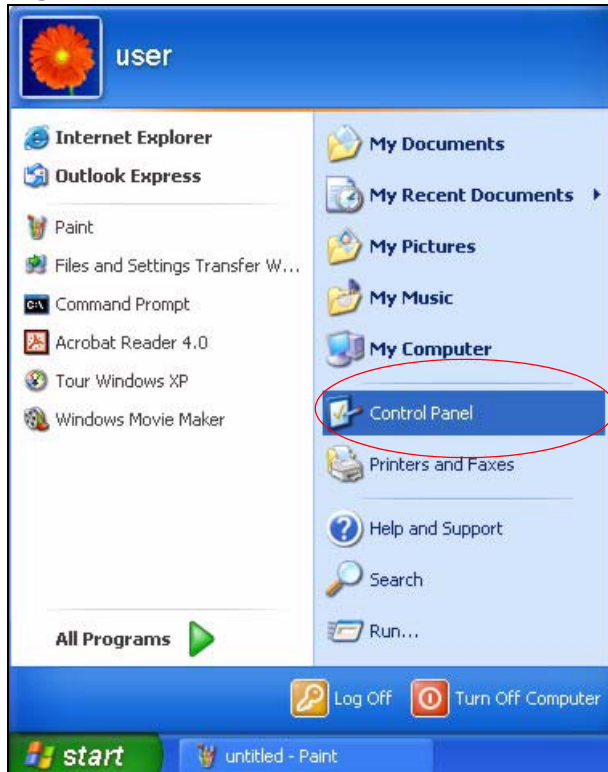
- 1 Click **Start** and then **Run**.
- 2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.
- 3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

## Windows 2000/NT/XP

The following example figures use the default Windows XP GUI theme.

- 1 Click **start** (**Start** in Windows 2000/NT), **Settings**, **Control Panel**.

**Figure 81** Windows XP: Start Menu



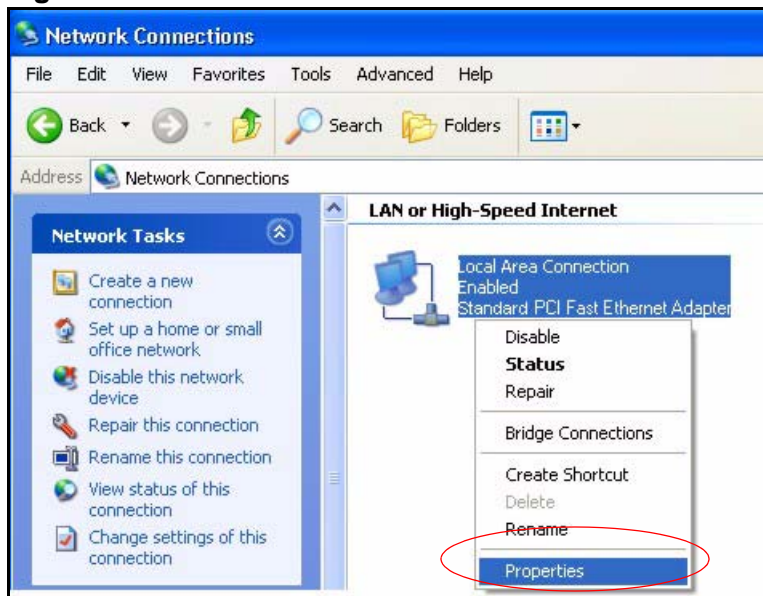
- 2 In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).

**Figure 82** Windows XP: Control Panel



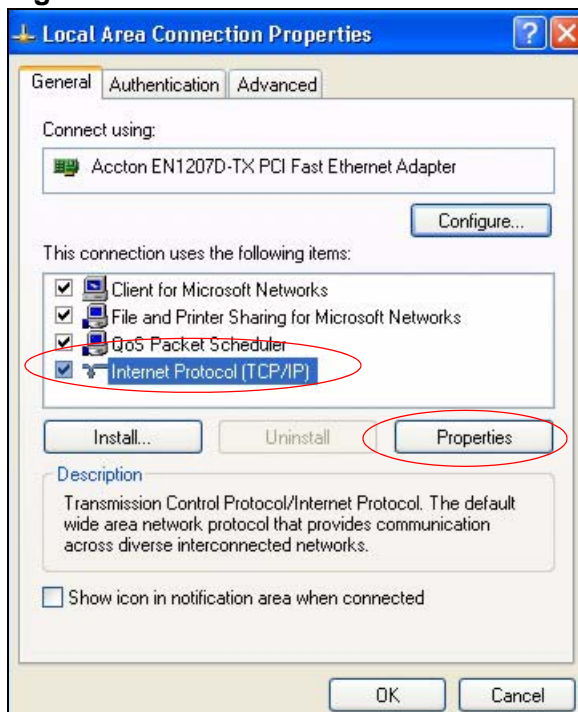
- 3 Right-click **Local Area Connection** and then click **Properties**.

**Figure 83** Windows XP: Control Panel: Network Connections: Properties



- 4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and then click **Properties**.

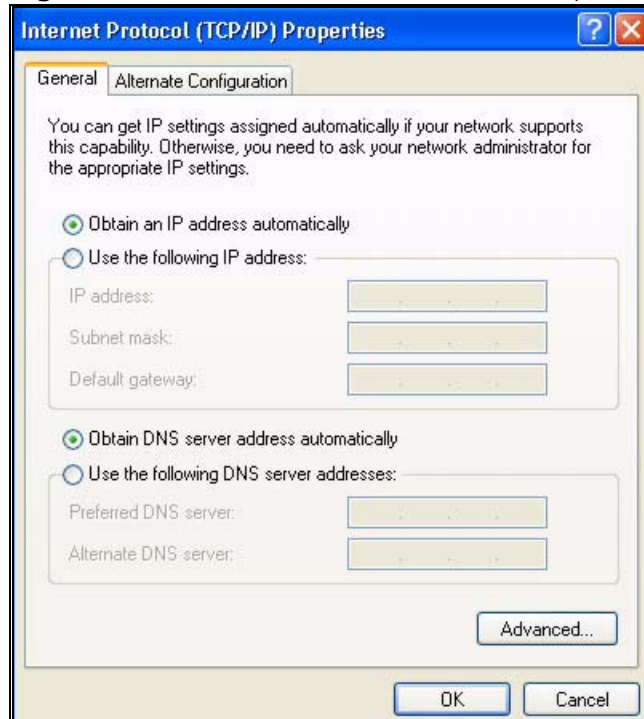
**Figure 84** Windows XP: Local Area Connection Properties



- 5 The **Internet Protocol TCP/IP Properties** window opens (the **General** tab in Windows XP).

- If you have a dynamic IP address click **Obtain an IP address automatically**.
- If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.
- Click **Advanced**.

**Figure 85** Windows XP: Internet Protocol (TCP/IP) Properties



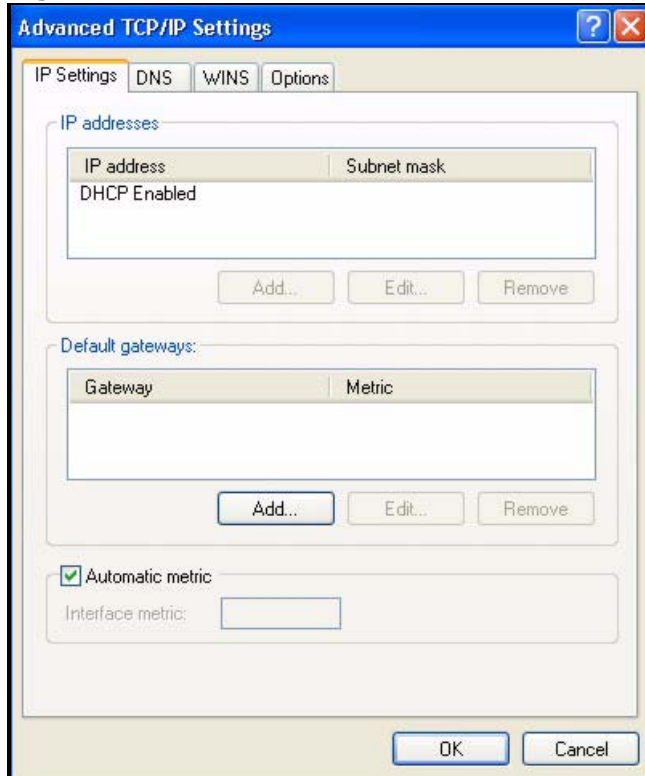
- 6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.

- Click **OK** when finished.

**Figure 86** Windows XP: Advanced TCP/IP Properties

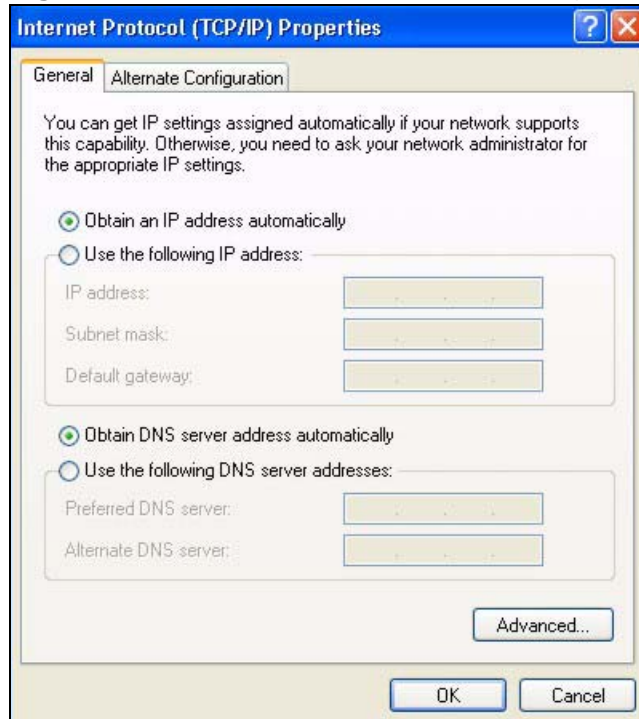


**7** In the **Internet Protocol TCP/IP Properties** window (the **General** tab in Windows XP):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

**Figure 87** Windows XP: Internet Protocol (TCP/IP) Properties



- 8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
- 9 Click **Close** (**OK** in Windows 2000/NT) to close the **Local Area Connection Properties** window.
- 10 Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).
- 11 Turn on your P-660RU-Tx and restart your computer (if prompted).

## Verifying Settings

- 1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.
- 2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

## Windows Vista

This section shows screens from Windows Vista Enterprise Version 6.0.



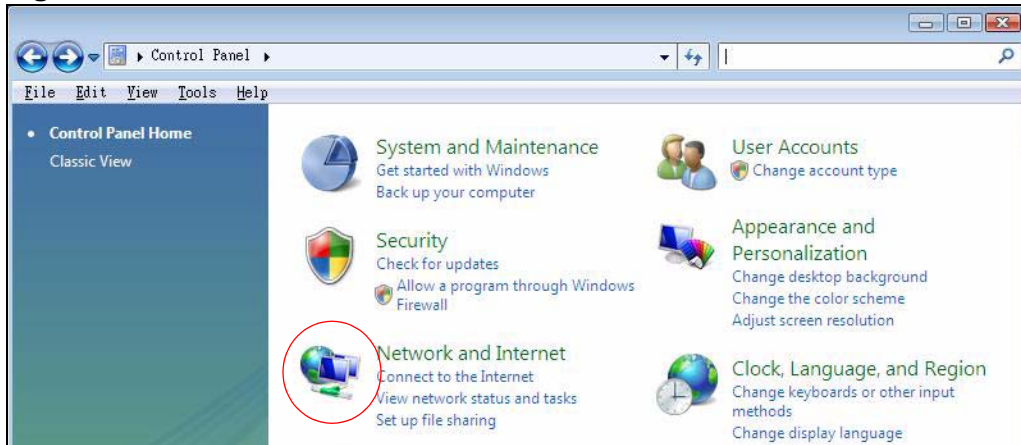
- 1 Click the **Start** icon, **Control Panel**.

**Figure 88** Windows Vista: Start Menu



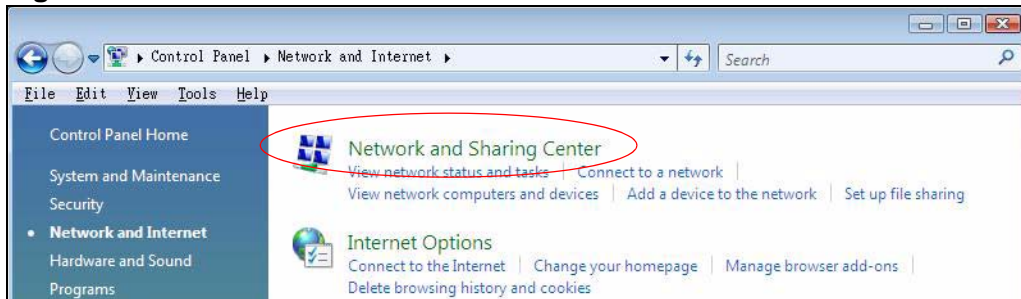
- 2 In the **Control Panel**, double-click **Network and Internet**.

**Figure 89** Windows Vista: Control Panel



- 3 Click **Network and Sharing Center**.

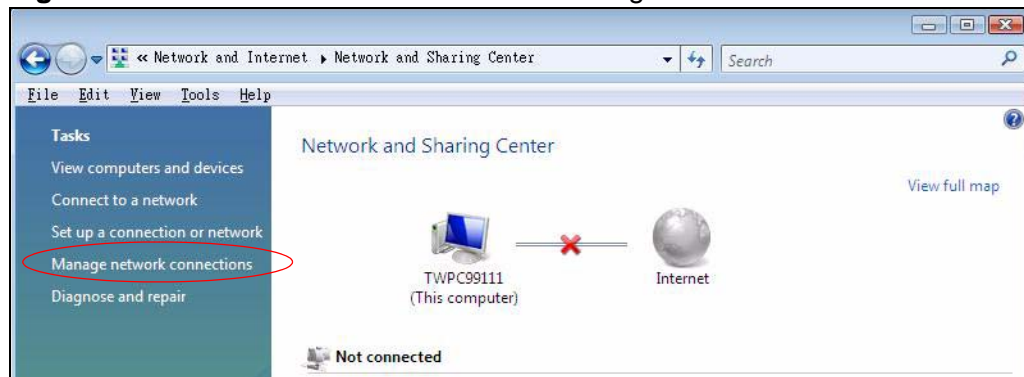
**Figure 90** Windows Vista: Network And Internet





4 Click **Manage network connections**.

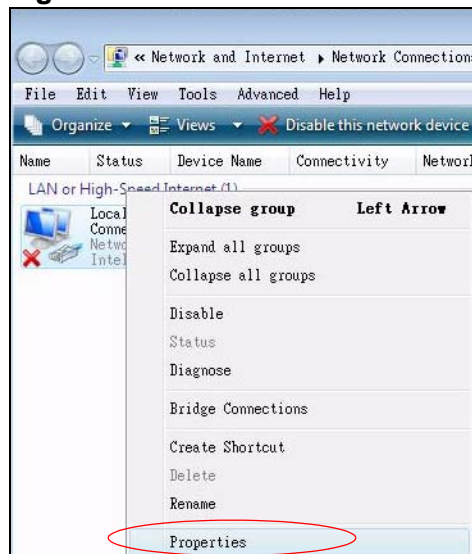
**Figure 91** Windows Vista: Network and Sharing Center



5 Right-click **Local Area Connection** and then click **Properties**.

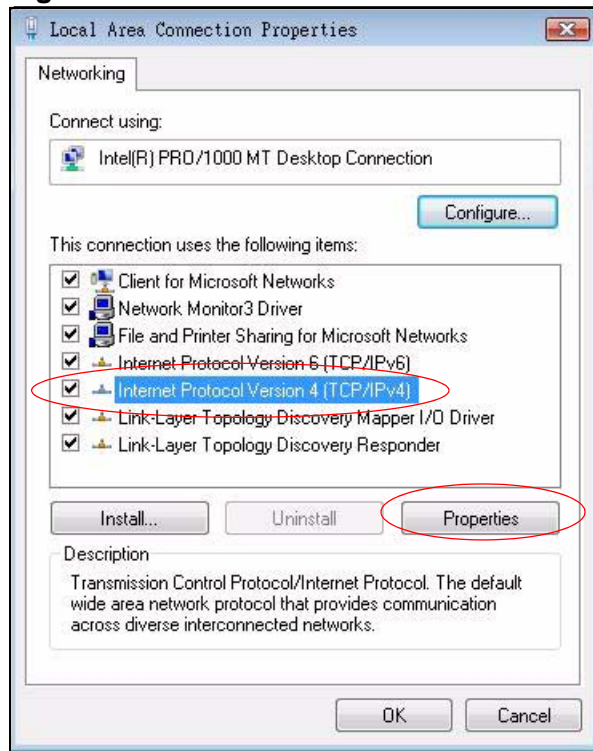
Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

**Figure 92** Windows Vista: Network and Sharing Center



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

**Figure 93** Windows Vista: Local Area Connection Properties

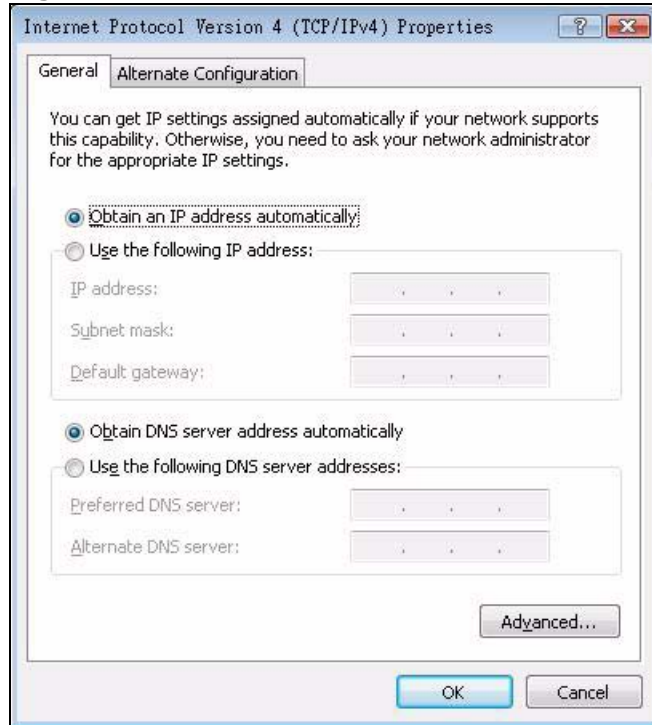


- 7 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens (the **General** tab).

- If you have a dynamic IP address click **Obtain an IP address automatically**.
- If you have a static IP address click **Use the following IP address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.

- Click **Advanced**.

**Figure 94** Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties



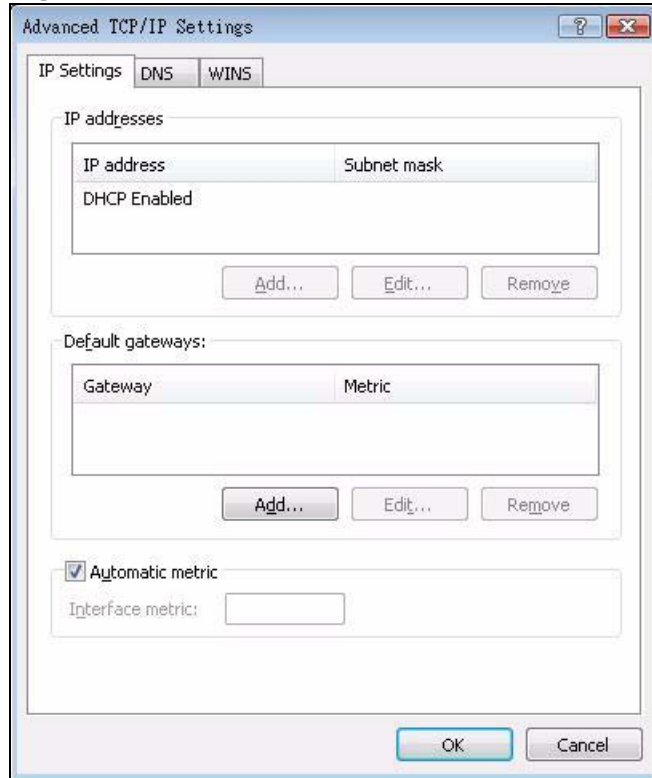
- 8 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.

- Click **OK** when finished.

**Figure 95** Windows Vista: Advanced TCP/IP Properties

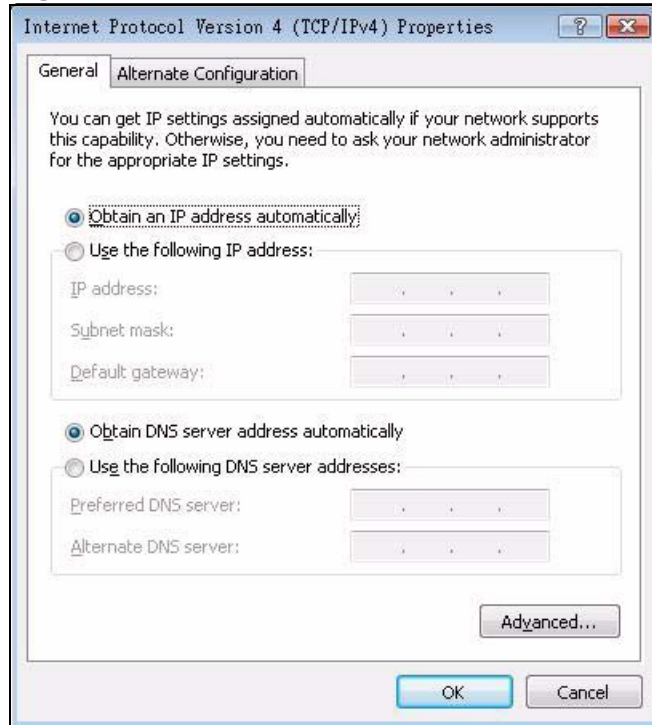


**9** In the **Internet Protocol Version 4 (TCP/IPv4) Properties** window, (the **General** tab):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

**Figure 96** Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties



- 10 Click **OK** to close the **Internet Protocol Version 4 (TCP/IPv4) Properties** window.
- 11 Click **Close** to close the **Local Area Connection Properties** window.
- 12 Close the **Network Connections** window.
- 13 Turn on your P-660RU-Tx and restart your computer (if prompted).

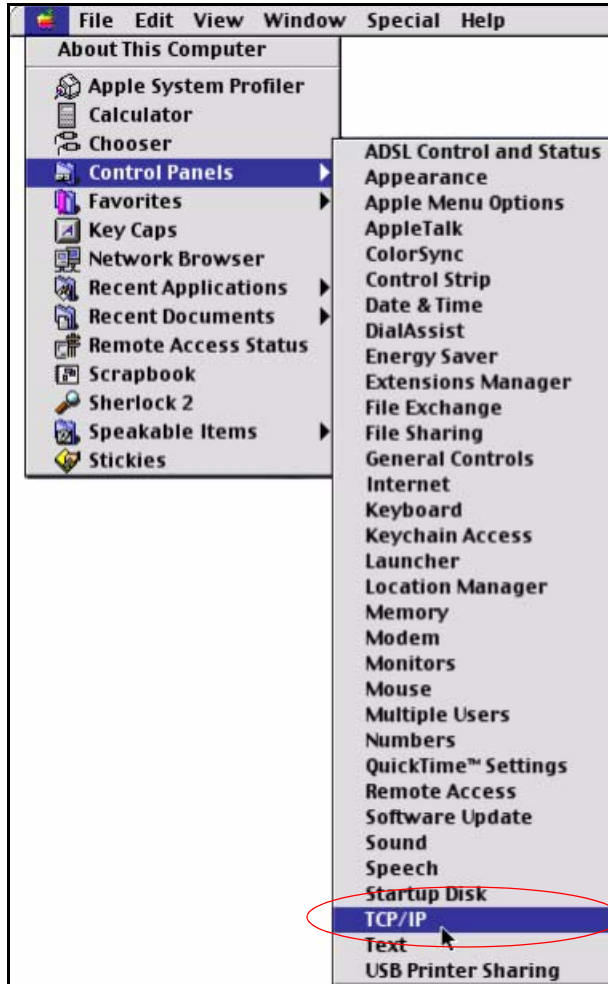
## Verifying Settings

- 1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.
- 2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

## Macintosh OS 8/9

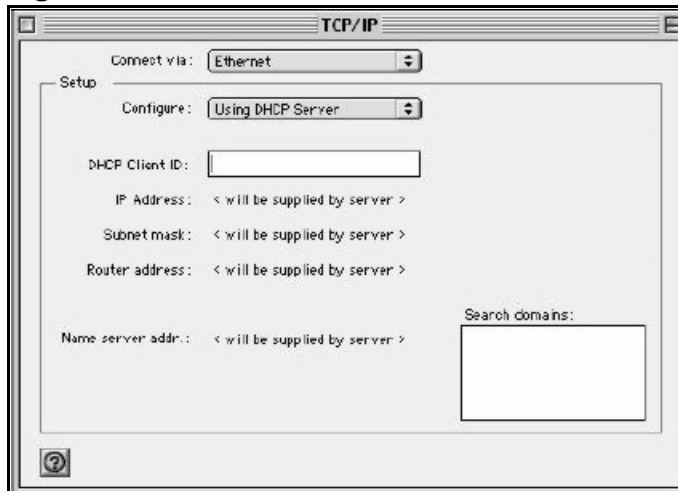
- 1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

**Figure 97** Macintosh OS 8/9: Apple Menu



- 2 Select **Ethernet built-in** from the **Connect via** list.

**Figure 98** Macintosh OS 8/9: TCP/IP



- 3 For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.
- 4 For statically assigned settings, do the following:
  - From the **Configure** box, select **Manually**.
  - Type your IP address in the **IP Address** box.
  - Type your subnet mask in the **Subnet mask** box.
  - Type the IP address of your P-660RU-Tx in the **Router address** box.
- 5 Close the **TCP/IP Control Panel**.
- 6 Click **Save** if prompted, to save changes to your configuration.
- 7 Turn on your P-660RU-Tx and restart your computer (if prompted).

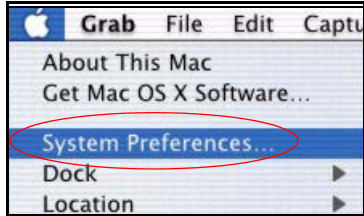
## Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

## Macintosh OS X

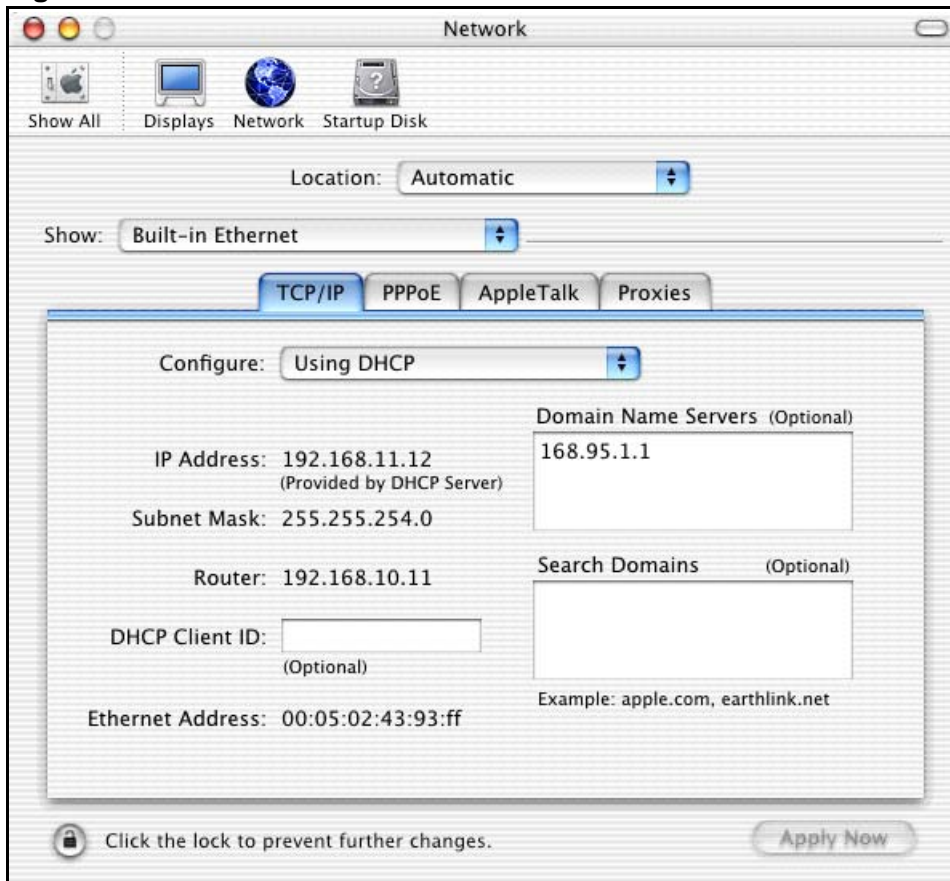
- 1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

**Figure 99** Macintosh OS X: Apple Menu



- 2 Click **Network** in the icon bar.
  - Select **Automatic** from the **Location** list.
  - Select **Built-in Ethernet** from the **Show** list.
  - Click the **TCP/IP** tab.
- 3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

**Figure 100** Macintosh OS X: Network



- 4 For statically assigned settings, do the following:



- From the **Configure** box, select **Manually**.
  - Type your IP address in the **IP Address** box.
  - Type your subnet mask in the **Subnet mask** box.
  - Type the IP address of your P-660RU-Tx in the **Router address** box.
- 5 Click **Apply Now** and close the window.
  - 6 Turn on your P-660RU-Tx and restart your computer (if prompted).

## Verifying Settings

Check your TCP/IP properties in the **Network** window.

## Linux

This section shows you how to configure your computer's TCP/IP settings in Red Hat Linux 9.0. Procedure, screens and file location may vary depending on your Linux distribution and release version.

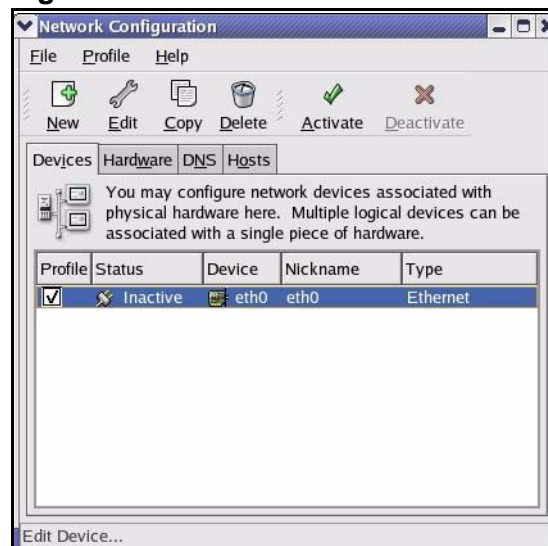
Note: Make sure you are logged in as the root administrator.

## Using the K Desktop Environment (KDE)

Follow the steps below to configure your computer IP address using the KDE.

- 1 Click the Red Hat button (located on the bottom left corner), select **System Setting** and click **Network**.

**Figure 101** Red Hat 9.0: KDE: Network Configuration: Devices



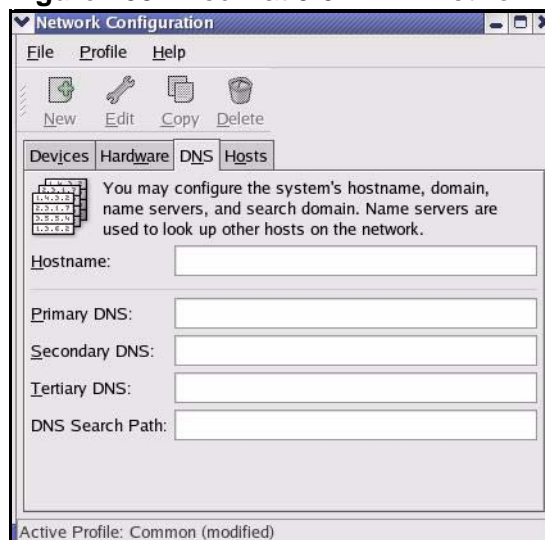
- 2 Double-click on the profile of the network card you wish to configure. The **Ethernet Device General** screen displays as shown.

**Figure 102** Red Hat 9.0: KDE: Ethernet Device: General



- If you have a dynamic IP address, click **Automatically obtain IP address settings with** and select **dhcp** from the drop down list.
  - If you have a static IP address, click **Statically set IP Addresses** and fill in the **Address**, **Subnet mask**, and **Default Gateway Address** fields.
- 3 Click **OK** to save the changes and close the **Ethernet Device General** screen.
  - 4 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Configuration** screen. Enter the DNS server information in the fields provided.

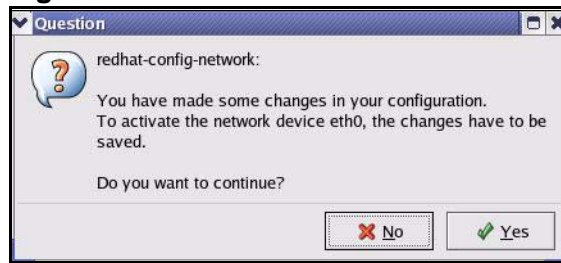
**Figure 103** Red Hat 9.0: KDE: Network Configuration: DNS



- 5 Click the **Devices** tab.

- Click the **Activate** button to apply the changes. The following screen displays. Click **Yes to save the changes in all screens**.

**Figure 104** Red Hat 9.0: KDE: Network Configuration: Activate



- After the network card restart process is complete, make sure the **Status** is **Active** in the **Network Configuration** screen.

## Using Configuration Files

Follow the steps below to edit the network configuration files and set your computer IP address.

- Assuming that you have only one network card on the computer, locate the `ifconfig-eth0` configuration file (where `eth0` is the name of the Ethernet card). Open the configuration file with any plain text editor.
  - If you have a dynamic IP address, enter **dhcp** in the `BOOTPROTO=` field. The following figure shows an example.

**Figure 105** Red Hat 9.0: Dynamic IP Address Setting in `ifconfig-eth0`

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- If you have a static IP address, enter **static** in the `BOOTPROTO=` field. Type `IPADDR=` followed by the IP address (in dotted decimal notation) and type `NETMASK=` followed by the subnet mask. The following example shows an example where the static IP address is 192.168.1.10 and the subnet mask is 255.255.255.0.

**Figure 106** Red Hat 9.0: Static IP Address Setting in `ifconfig-eth0`

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.10
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- 2 If you know your DNS server IP address(es), enter the DNS server information in the `resolv.conf` file in the `/etc` directory. The following figure shows an example where two DNS server IP addresses are specified.

**Figure 107** Red Hat 9.0: DNS Settings in `resolv.conf`

```
nameserver 172.23.5.1
nameserver 172.23.5.2
```

- 3 After you edit and save the configuration files, you must restart the network card. Enter `./network restart` in the `/etc/rc.d/init.d` directory. The following figure shows an example.

**Figure 108** Red Hat 9.0: Restart Ethernet Card

```
[root@localhost init.d]# network restart

Shutting down interface eth0:           [OK]
Shutting down loopback interface:       [OK]
Setting network parameters:             [OK]
Bringing up loopback interface:         [OK]
Bringing up interface eth0:             [OK]
```

## Verifying Settings

Enter `ifconfig` in a terminal screen to check your TCP/IP properties.

**Figure 109** Red Hat 9.0: Checking TCP/IP Properties

```
[root@localhost]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:BA:72:5B:44
          inet addr:172.23.19.129  Bcast:172.23.19.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:717 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:730412 (713.2 Kb)  TX bytes:1570 (1.5 Kb)
          Interrupt:10 Base address:0x1000
[root@localhost]#
```



# Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Note: Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

## Internet Explorer Pop-up Blockers

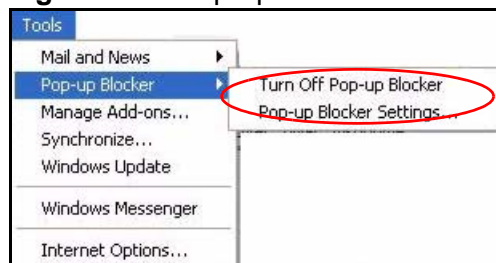
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

### Disable Pop-up Blockers

- 1 In Internet Explorer, select **Tools, Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

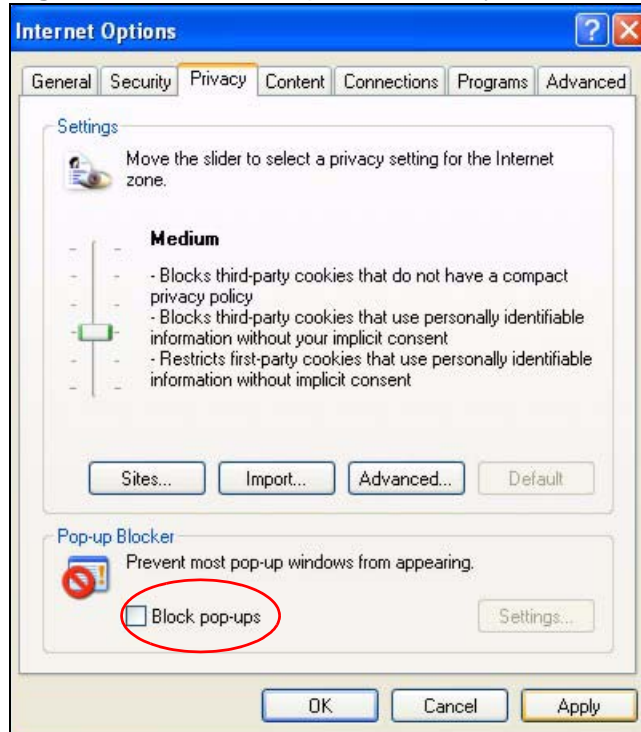
**Figure 110** Pop-up Blocker



You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

- 1 In Internet Explorer, select **Tools, Internet Options, Privacy**.
- 2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

**Figure 111** Internet Options: Privacy



- 3 Click **Apply** to save this setting.

### Enable Pop-up Blockers with Exceptions

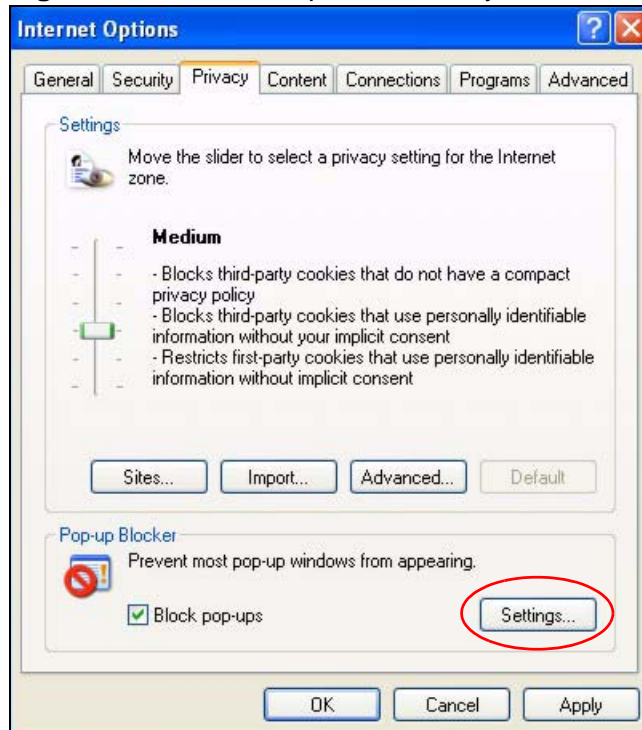
Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

- 1 In Internet Explorer, select **Tools, Internet Options** and then the **Privacy** tab.



- 2 Select **Settings...** to open the **Pop-up Blocker Settings** screen.

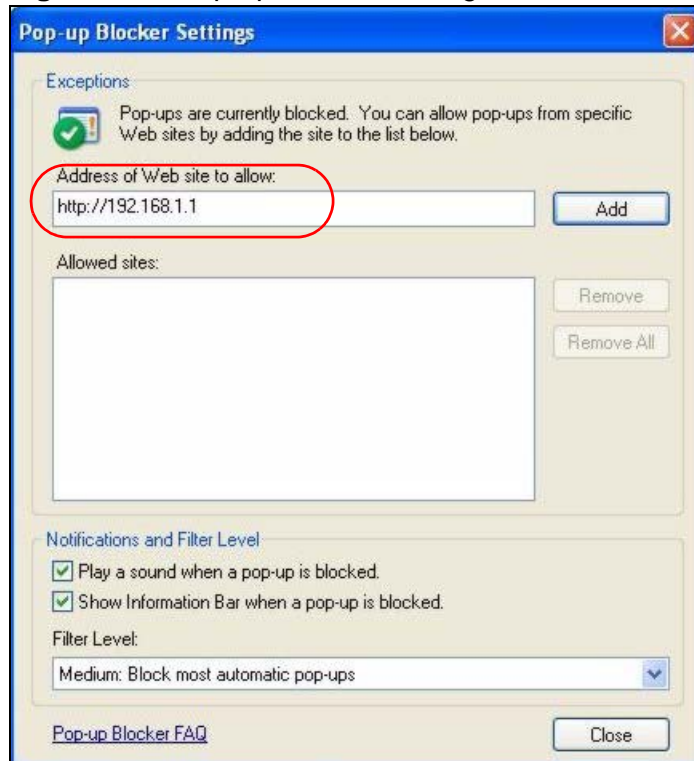
**Figure 112** Internet Options: Privacy



- 3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.167.1.

- 4 Click **Add** to move the IP address to the list of **Allowed sites**.

**Figure 113** Pop-up Blocker Settings



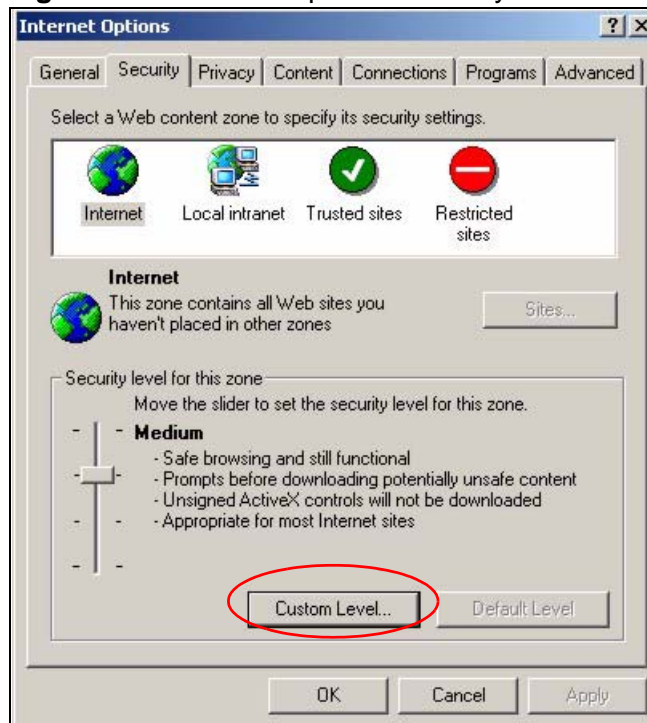
- 5 Click **Close** to return to the **Privacy** screen.
- 6 Click **Apply** to save this setting.

## JavaScripts

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

- 1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

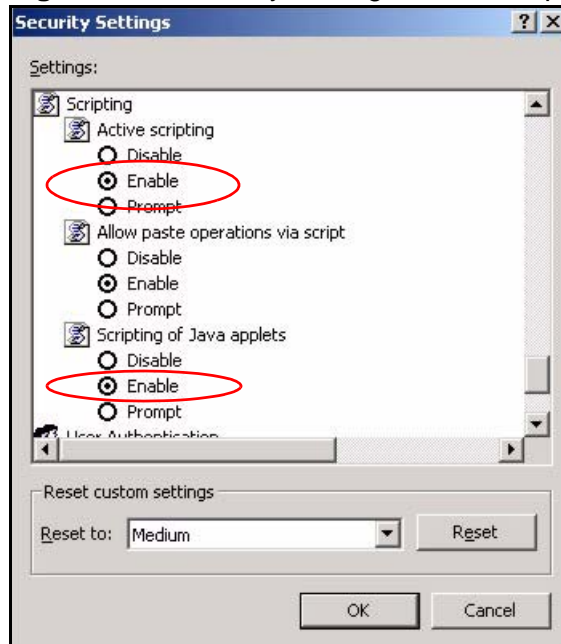
**Figure 114** Internet Options: Security



- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Scripting**.
- 4 Under **Active scripting** make sure that **Enable** is selected (the default).
- 5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

- 6 Click **OK** to close the window.

**Figure 115** Security Settings - Java Scripting

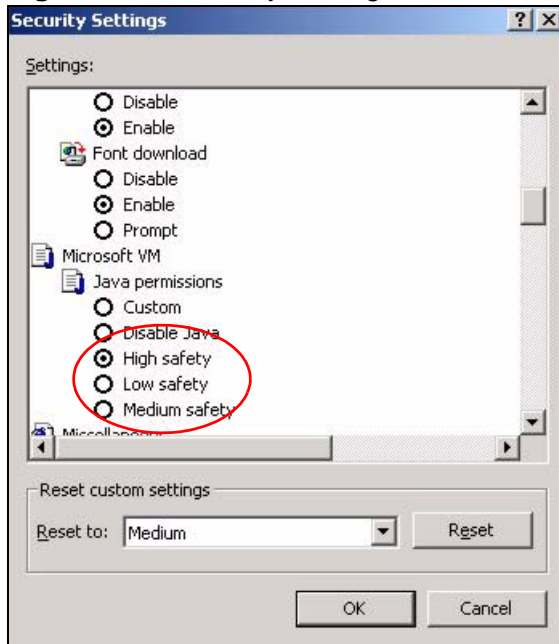


## Java Permissions

- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Security** tab.
- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Microsoft VM**.
- 4 Under **Java permissions** make sure that a safety level is selected.

- 5 Click **OK** to close the window.

**Figure 116** Security Settings - Java

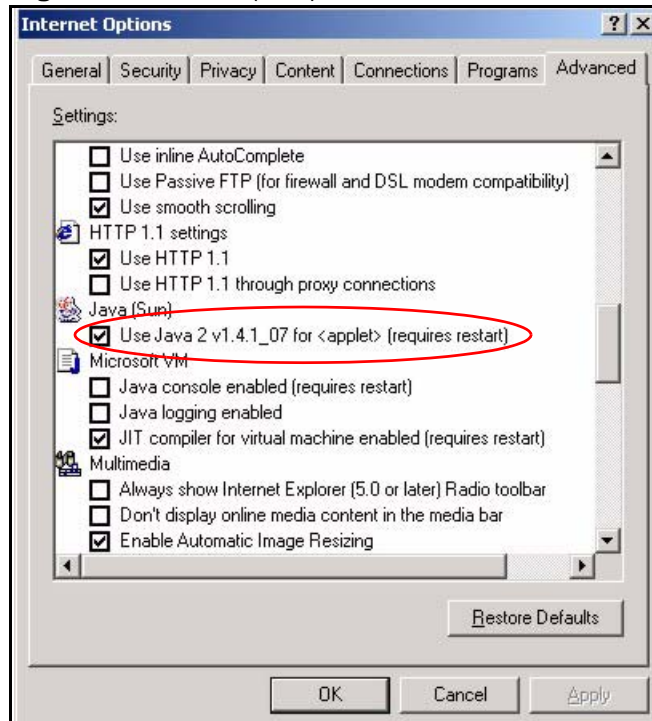


## JAVA (Sun)

- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Advanced** tab.
- 2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

- 3 Click **OK** to close the window.

**Figure 117** Java (Sun)

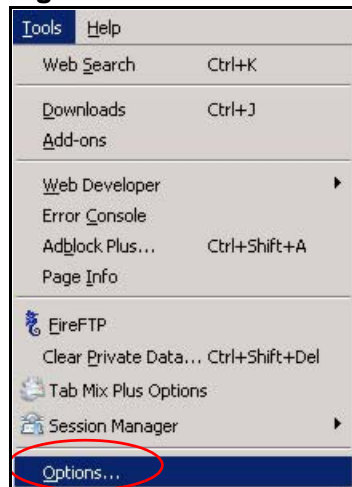


## Mozilla Firefox

Mozilla Firefox 2.0 screens are used here. Screens for other versions may vary.

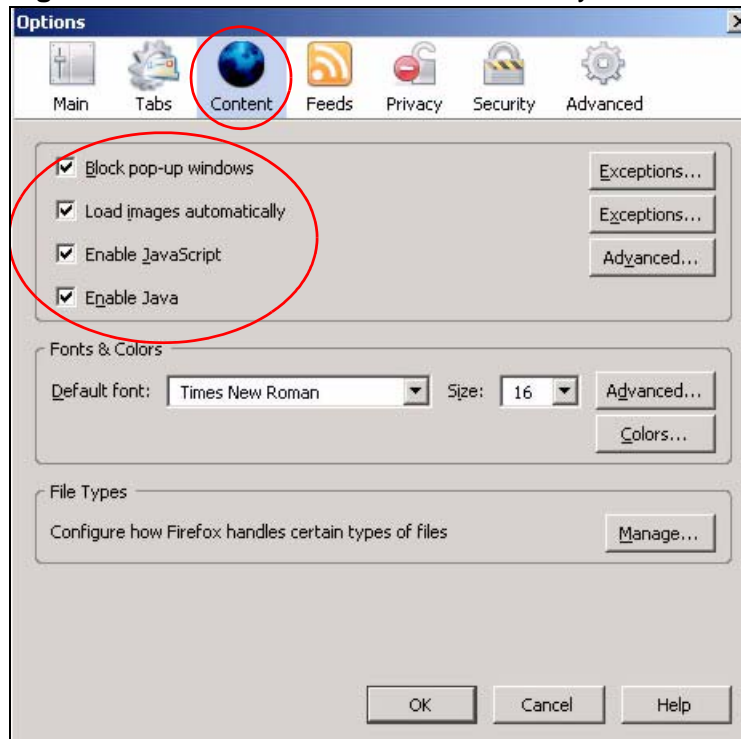
You can enable Java, Javascripts and pop-ups in one screen. Click **Tools**, then click **Options** in the screen that appears.

**Figure 118** Mozilla Firefox: Tools > Options



Click **Content** to show the screen below. Select the check boxes as shown in the following screen.

**Figure 119** Mozilla Firefox Content Security







# IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

## Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

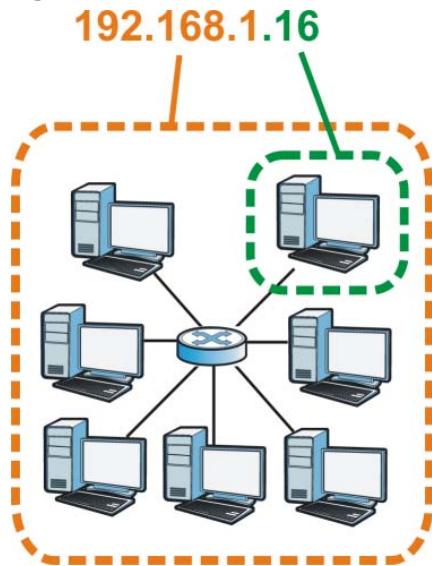
## Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

**Figure 120** Network Number and Host ID



How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

## Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term “subnet” is short for “sub-network”.

A subnet mask has 32 bits. If a bit in the subnet mask is a “1” then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is “0” then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

**Table 51** Subnet Masks

|                      | <b>1ST<br/>OCTET:</b><br><b>(192)</b> | <b>2ND<br/>OCTET:</b><br><b>(168)</b> | <b>3RD<br/>OCTET:</b><br><b>(1)</b> | <b>4TH<br/>OCTET</b><br><b>(2)</b> |
|----------------------|---------------------------------------|---------------------------------------|-------------------------------------|------------------------------------|
| IP Address (Binary)  | 11000000                              | 10101000                              | 00000001                            | 00000010                           |
| Subnet Mask (Binary) | <b>11111111</b>                       | <b>11111111</b>                       | <b>11111111</b>                     | 00000000                           |
| Network Number       | <b>11000000</b>                       | <b>10101000</b>                       | <b>00000001</b>                     |                                    |
| Host ID              |                                       |                                       |                                     | 00000010                           |

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a “1” value). For example, an “8-bit mask” means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

**Table 52** Subnet Masks

|             | BINARY    |           |           |           | DECIMAL         |
|-------------|-----------|-----------|-----------|-----------|-----------------|
|             | 1ST OCTET | 2ND OCTET | 3RD OCTET | 4TH OCTET |                 |
| 8-bit mask  | 11111111  | 00000000  | 00000000  | 00000000  | 255.0.0.0       |
| 16-bit mask | 11111111  | 11111111  | 00000000  | 00000000  | 255.255.0.0     |
| 24-bit mask | 11111111  | 11111111  | 11111111  | 00000000  | 255.255.255.0   |
| 29-bit mask | 11111111  | 11111111  | 11111111  | 11111000  | 255.255.255.248 |

## Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

**Table 53** Maximum Host Numbers

| SUBNET MASK |                 | HOST ID SIZE |              | MAXIMUM NUMBER OF HOSTS |
|-------------|-----------------|--------------|--------------|-------------------------|
| 8 bits      | 255.0.0.0       | 24 bits      | $2^{24} - 2$ | 16777214                |
| 16 bits     | 255.255.0.0     | 16 bits      | $2^{16} - 2$ | 65534                   |
| 24 bits     | 255.255.255.0   | 8 bits       | $2^8 - 2$    | 254                     |
| 29 bits     | 255.255.255.248 | 3 bits       | $2^3 - 2$    | 6                       |

## Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a "/" followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

**Table 54** Alternative Subnet Mask Notation

| SUBNET MASK     | ALTERNATIVE NOTATION | LAST OCTET (BINARY) | LAST OCTET (DECIMAL) |
|-----------------|----------------------|---------------------|----------------------|
| 255.255.255.0   | /24                  | 0000 0000           | 0                    |
| 255.255.255.128 | /25                  | 1000 0000           | 128                  |
| 255.255.255.192 | /26                  | 1100 0000           | 192                  |
| 255.255.255.224 | /27                  | 1110 0000           | 224                  |
| 255.255.255.240 | /28                  | 1111 0000           | 240                  |
| 255.255.255.248 | /29                  | 1111 1000           | 248                  |
| 255.255.255.252 | /30                  | 1111 1100           | 252                  |

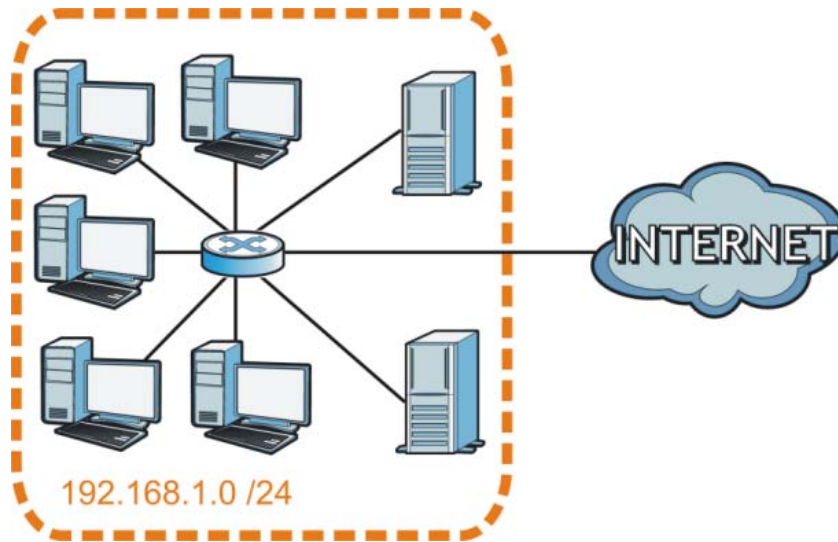
## Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of  $2^8 - 2$  or 254 possible hosts.

The following figure shows the company network before subnetting.

**Figure 121** Subnetting Example: Before Subnetting

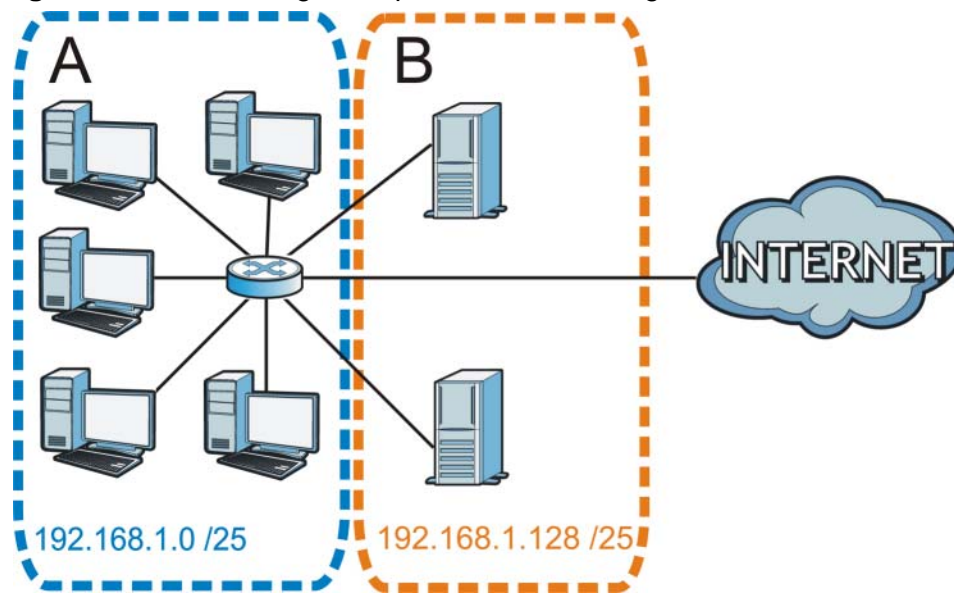


You can “borrow” one of the host ID bits to divide the network  $192.168.1.0$  into two separate sub-networks. The subnet mask is now 25 bits ( $255.255.255.128$  or  $/25$ ).

The “borrowed” host ID bit can have a value of either 0 or 1, allowing two subnets;  $192.168.1.0 /25$  and  $192.168.1.128 /25$ .

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

**Figure 122** Subnetting Example: After Subnetting



In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of  $2^7 - 2$  or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

## Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.11000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving  $2^6 - 2$  or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

**Table 55** Subnet 1

| IP/SUBNET MASK                     | NETWORK NUMBER                | LAST OCTET BIT VALUE |
|------------------------------------|-------------------------------|----------------------|
| IP Address (Decimal)               | 192.168.1.                    | 0                    |
| IP Address (Binary)                | 11000000.10101000.00000001.   | 00000000             |
| Subnet Mask (Binary)               | 11111111.11111111.11111111.   | 11000000             |
| Subnet Address:<br>192.168.1.0     | Lowest Host ID: 192.168.1.1   |                      |
| Broadcast Address:<br>192.168.1.63 | Highest Host ID: 192.168.1.62 |                      |

**Table 56** Subnet 2

| IP/SUBNET MASK                      | NETWORK NUMBER                 | LAST OCTET BIT VALUE |
|-------------------------------------|--------------------------------|----------------------|
| IP Address                          | 192.168.1.                     | 64                   |
| IP Address (Binary)                 | 11000000.10101000.00000001.    | 01000000             |
| Subnet Mask (Binary)                | 11111111.11111111.11111111.    | 11000000             |
| Subnet Address:<br>192.168.1.64     | Lowest Host ID: 192.168.1.65   |                      |
| Broadcast Address:<br>192.168.1.127 | Highest Host ID: 192.168.1.126 |                      |

**Table 57** Subnet 3

| IP/SUBNET MASK                      | NETWORK NUMBER                 | LAST OCTET BIT VALUE |
|-------------------------------------|--------------------------------|----------------------|
| IP Address                          | 192.168.1.                     | 128                  |
| IP Address (Binary)                 | 11000000.10101000.00000001.    | <b>10000000</b>      |
| Subnet Mask (Binary)                | 11111111.11111111.11111111.    | <b>11000000</b>      |
| Subnet Address:<br>192.168.1.128    | Lowest Host ID: 192.168.1.129  |                      |
| Broadcast Address:<br>192.168.1.191 | Highest Host ID: 192.168.1.190 |                      |

**Table 58** Subnet 4

| IP/SUBNET MASK                      | NETWORK NUMBER                 | LAST OCTET BIT VALUE |
|-------------------------------------|--------------------------------|----------------------|
| IP Address                          | 192.168.1.                     | 192                  |
| IP Address (Binary)                 | 11000000.10101000.00000001.    | <b>11000000</b>      |
| Subnet Mask (Binary)                | 11111111.11111111.11111111.    | <b>11000000</b>      |
| Subnet Address:<br>192.168.1.192    | Lowest Host ID: 192.168.1.193  |                      |
| Broadcast Address:<br>192.168.1.255 | Highest Host ID: 192.168.1.254 |                      |

## Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

**Table 59** Eight Subnets

| SUBNET | SUBNET ADDRESS | FIRST ADDRESS | LAST ADDRESS | BROADCAST ADDRESS |
|--------|----------------|---------------|--------------|-------------------|
| 1      | 0              | 1             | 30           | 31                |
| 2      | 32             | 33            | 62           | 63                |
| 3      | 64             | 65            | 94           | 95                |
| 4      | 96             | 97            | 126          | 127               |
| 5      | 128            | 129           | 158          | 159               |
| 6      | 160            | 161           | 190          | 191               |
| 7      | 192            | 193           | 222          | 223               |
| 8      | 224            | 225           | 254          | 255               |

## Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

**Table 60** 24-bit Network Number Subnet Planning

| NO. "BORROWED" HOST BITS | SUBNET MASK           | NO. SUBNETS | NO. HOSTS PER SUBNET |
|--------------------------|-----------------------|-------------|----------------------|
| 1                        | 255.255.255.128 (/25) | 2           | 126                  |
| 2                        | 255.255.255.192 (/26) | 4           | 62                   |
| 3                        | 255.255.255.224 (/27) | 8           | 30                   |
| 4                        | 255.255.255.240 (/28) | 16          | 14                   |
| 5                        | 255.255.255.248 (/29) | 32          | 6                    |
| 6                        | 255.255.255.252 (/30) | 64          | 2                    |
| 7                        | 255.255.255.254 (/31) | 128         | 1                    |

The following table is a summary for subnet planning on a network with a 16-bit network number.

**Table 61** 16-bit Network Number Subnet Planning

| NO. "BORROWED" HOST BITS | SUBNET MASK           | NO. SUBNETS | NO. HOSTS PER SUBNET |
|--------------------------|-----------------------|-------------|----------------------|
| 1                        | 255.255.128.0 (/17)   | 2           | 32766                |
| 2                        | 255.255.192.0 (/18)   | 4           | 16382                |
| 3                        | 255.255.224.0 (/19)   | 8           | 8190                 |
| 4                        | 255.255.240.0 (/20)   | 16          | 4094                 |
| 5                        | 255.255.248.0 (/21)   | 32          | 2046                 |
| 6                        | 255.255.252.0 (/22)   | 64          | 1022                 |
| 7                        | 255.255.254.0 (/23)   | 128         | 510                  |
| 8                        | 255.255.255.0 (/24)   | 256         | 254                  |
| 9                        | 255.255.255.128 (/25) | 512         | 126                  |
| 10                       | 255.255.255.192 (/26) | 1024        | 62                   |
| 11                       | 255.255.255.224 (/27) | 2048        | 30                   |
| 12                       | 255.255.255.240 (/28) | 4096        | 14                   |
| 13                       | 255.255.255.248 (/29) | 8192        | 6                    |
| 14                       | 255.255.255.252 (/30) | 16384       | 2                    |
| 15                       | 255.255.255.254 (/31) | 32768       | 1                    |

## Configuring IP Addresses

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP



addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the P-660RU-Tx.

Once you have decided on the network number, pick an IP address for your P-660RU-Tx that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your P-660RU-Tx will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the P-660RU-Tx unless you are instructed to do otherwise.

## Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, *Address Allocation for Private Internets* and RFC 1466, *Guidelines for Management of IP Address Space*.



## Services

The following table lists some commonly-used services and their associated protocols and port numbers.

- **Name:** This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol:** This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s):** This value depends on the **Protocol**.
  - If the **Protocol** is **TCP, UDP, or TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description:** This is a brief explanation of the applications that use this service or the situations in which this service is used.

**Table 62** Examples of Services

| NAME                  | PROTOCOL           | PORT(S)       | DESCRIPTION  |
|-----------------------|--------------------|---------------|--|
| AH<br>(IPSEC_TUNNEL)  | User-Defined       | 51            | The IPSEC AH (Authentication Header) tunneling protocol uses this service.   |
| AIM                   | TCP                | 5190          | AOL's Internet Messenger service.  |
| AUTH                  | TCP                | 113           | Authentication protocol used by some servers.  |
| BGP                   | TCP                | 179           | Border Gateway Protocol.   |
| BOOTP_CLIENT          | UDP                | 68            | DHCP Client.   |
| BOOTP_SERVER          | UDP                | 67            | DHCP Server.   |
| CU-SEEME              | TCP/UDP<br>TCP/UDP | 7648<br>24032 | A popular videoconferencing solution from White Pines Software.  |
| DNS                   | TCP/UDP            | 53            | Domain Name Server, a service that matches web names (for instance <a href="http://www.zyxel.com">www.zyxel.com</a> ) to IP numbers. |
| ESP<br>(IPSEC_TUNNEL) | User-Defined       | 50            | The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.  |
| FINGER                | TCP                | 79            | Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.                                    |

**Table 62** Examples of Services (continued)

| NAME             | PROTOCOL     | PORT(S) | DESCRIPTION  |
|------------------|--------------|---------|--|
| FTP              | TCP          | 20      | File Transfer Protocol, a program to enable fast transfer of files, including large files that may not be possible by e-mail.          |
|                  | TCP          | 21      |  |
| H.323            | TCP          | 1720    | NetMeeting uses this protocol.   |
| HTTP             | TCP          | 80      | Hyper Text Transfer Protocol - a client/server protocol for the world wide web.  |
| HTTPS            | TCP          | 443     | HTTPS is a secured http session often used in e-commerce.  |
| ICMP             | User-Defined | 1       | Internet Control Message Protocol is often used for diagnostic purposes.   |
| ICQ              | UDP          | 4000    | This is a popular Internet chat program.   |
| IGMP (MULTICAST) | User-Defined | 2       | Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.   |
| IKE              | UDP          | 500     | The Internet Key Exchange algorithm is used for key distribution and management.   |
| IMAP4            | TCP          | 143     | The Internet Message Access Protocol is used for e-mail.   |
| IMAP4S           | TCP          | 993     | This is a more secure version of IMAP4 that runs over SSL.   |
| IRC              | TCP/UDP      | 6667    | This is another popular Internet chat program.   |
| MSN Messenger    | TCP          | 1863    | Microsoft Networks' messenger service uses this protocol.  |
| NetBIOS          | TCP/UDP      | 137     | The Network Basic Input/Output System is used for communication between computers in a LAN.  |
|                  | TCP/UDP      | 138     |  |
|                  | TCP/UDP      | 139     |  |
|                  | TCP/UDP      | 445     |  |
| NEW-ICQ          | TCP          | 5190    | An Internet chat program.  |
| NEWS             | TCP          | 144     | A protocol for news groups.  |
| NFS              | UDP          | 2049    | Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments. |
| NNTP             | TCP          | 119     | Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.  |
| PING             | User-Defined | 1       | Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.              |

**Table 62** Examples of Services (continued)

| NAME              | PROTOCOL     | PORT(S) | DESCRIPTION   |
|-------------------|--------------|---------|---|
| POP3              | TCP          | 110     | Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).   |
| POP3S             | TCP          | 995     | This is a more secure version of POP3 that runs over SSL.   |
| PPTP              | TCP          | 1723    | Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.  |
| PPTP_TUNNEL (GRE) | User-Defined | 47      | PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.  |
| RCMD              | TCP          | 512     | Remote Command Service.   |
| REAL_AUDIO        | TCP          | 7070    | A streaming audio service that enables real time sound over the web.  |
| REXEC             | TCP          | 514     | Remote Execution Daemon.  |
| RLOGIN            | TCP          | 513     | Remote Login.   |
| ROADRUNNER        | TCP/UDP      | 1026    | This is an ISP that provides services mainly for cable modems.  |
| RTELNET           | TCP          | 107     | Remote Telnet.  |
| RTSP              | TCP/UDP      | 554     | The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.   |
| SFTP              | TCP          | 115     | The Simple File Transfer Protocol is an old way of transferring files between computers.  |
| SMTP              | TCP          | 25      | Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.                           |
| SMTPS             | TCP          | 465     | This is a more secure version of SMTP that runs over SSL.   |
| SNMP              | TCP/UDP      | 161     | Simple Network Management Program.  |
| SNMP-TRAPS        | TCP/UDP      | 162     | Traps for use with the SNMP (RFC: 1215).  |
| SQL-NET           | TCP          | 1521    | Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers. |

**Table 62** Examples of Services (continued)

| NAME       | PROTOCOL   | PORT(S)                  | DESCRIPTION  |
|------------|------------|--------------------------|--|
| SSDP       | UDP        | 1900                     | The Simple Service Discovery Protocol supports Universal Plug-and-Play (UPnP).   |
| SSH        | TCP/UDP    | 22                       | Secure Shell Remote Login Program.   |
| STRM WORKS | UDP        | 1558                     | Stream Works Protocol.   |
| SYSLOG     | UDP        | 514                      | Syslog allows you to send system logs to a UNIX server.  |
| TACACS     | UDP        | 49                       | Login Host Protocol used for (Terminal Access Controller Access Control System).   |
| TELNET     | TCP        | 23                       | Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems. |
| TFTP       | UDP        | 69                       | Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).                                |
| VDOLIVE    | TCP<br>UDP | 7000<br>user-<br>defined | A videoconferencing solution. The UDP port number is specified in the application.   |

# Legal Information

## Copyright

Copyright © 2010 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

## Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Your use of the P-660RU-Tx is subject to the terms and conditions of any related service providers.

## Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

## Certifications

### Viewing Certifications

- 1 Go to <http://www.zyxel.com>.

- 2 Select your product on the ZyXEL home page to go to that product's page.
- 3 Select the certification you wish to view from this page.

## ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

### Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

### Registration

Register your product online to receive e-mail notices of firmware upgrades and information at [www.zyxel.com](http://www.zyxel.com) for global products, or at [www.us.zyxel.com](http://www.us.zyxel.com) for North American products.



# Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device. Regional offices are listed below (see also [http://www.zyxel.com/web/contact\\_us.php](http://www.zyxel.com/web/contact_us.php)). Please have the following information ready when you contact an office.

## Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

“+” is the (prefix) number you dial to make an international telephone call.

## Corporate Headquarters (Worldwide)

- Support E-mail: [support@zyxel.com.tw](mailto:support@zyxel.com.tw)
- Sales E-mail: [sales@zyxel.com.tw](mailto:sales@zyxel.com.tw)
- Telephone: +886-3-578-3942
- Fax: +886-3-578-2439
- Web: [www.zyxel.com](http://www.zyxel.com)
- Regular Mail: ZyXEL Communications Corp., 6 Innovation Road II, Science Park, Hsinchu 300, Taiwan

## China - ZyXEL Communications (Beijing) Corp.

- Support E-mail: [cso.zycn@zyxel.cn](mailto:cso.zycn@zyxel.cn)
- Sales E-mail: [sales@zyxel.cn](mailto:sales@zyxel.cn)
- Telephone: +86-010-82800646
- Fax: +86-010-82800587
- Address: 902, Unit B, Horizon Building, No.6, Zhichun Str, Haidian District, Beijing
- Web: <http://www.zyxel.cn>

### **China - ZyXEL Communications (Shanghai) Corp.**

- Support E-mail: [cs0.zycn@zyxel.cn](mailto:cs0.zycn@zyxel.cn)
- Sales E-mail: [sales@zyxel.cn](mailto:sales@zyxel.cn)
- Telephone: +86-021-61199055
- Fax: +86-021-52069033
- Address: 1005F, ShengGao International Tower, No.137 XianXia Rd., Shanghai
- Web: <http://www.zyxel.cn>

### **Costa Rica**

- Support E-mail: [soporte@zyxel.co.cr](mailto:soporte@zyxel.co.cr)
- Sales E-mail: [sales@zyxel.co.cr](mailto:sales@zyxel.co.cr)
- Telephone: +506-2017878
- Fax: +506-2015098
- Web: [www.zyxel.co.cr](http://www.zyxel.co.cr)
- Regular Mail: ZyXEL Costa Rica, Plaza Roble Escazú, Etapa El Patio, Tercer Piso, San José, Costa Rica

### **Czech Republic**

- E-mail: [info@cz.zyxel.com](mailto:info@cz.zyxel.com)
- Telephone: +420-241-091-350
- Fax: +420-241-091-359
- Web: [www.zyxel.cz](http://www.zyxel.cz)
- Regular Mail: ZyXEL Communications, Czech s.r.o., Modranská 621, 143 01 Praha 4 - Modrany, Česká Republika

### **Denmark**

- Support E-mail: [support@zyxel.dk](mailto:support@zyxel.dk)
- Sales E-mail: [sales@zyxel.dk](mailto:sales@zyxel.dk)
- Telephone: +45-39-55-07-00
- Fax: +45-39-55-07-07
- Web: [www.zyxel.dk](http://www.zyxel.dk)
- Regular Mail: ZyXEL Communications A/S, Columbusvej, 2860 Soeborg, Denmark

### **Finland**

- Support E-mail: [support@zyxel.fi](mailto:support@zyxel.fi)
- Sales E-mail: [sales@zyxel.fi](mailto:sales@zyxel.fi)
- Telephone: +358-9-4780-8411

- Fax: +358-9-4780-8448
- Web: [www.zyxel.fi](http://www.zyxel.fi)
- Regular Mail: ZyXEL Communications Oy, Malminkaari 10, 00700 Helsinki, Finland

### **France**

- E-mail: [info@zyxel.fr](mailto:info@zyxel.fr)
- Telephone: +33-4-72-52-97-97
- Fax: +33-4-72-52-19-20
- Web: [www.zyxel.fr](http://www.zyxel.fr)
- Regular Mail: ZyXEL France, 1 rue des Vergers, Bat. 1 / C, 69760 Limonest, France

### **Germany**

- Support E-mail: [support@zyxel.de](mailto:support@zyxel.de)
- Sales E-mail: [sales@zyxel.de](mailto:sales@zyxel.de)
- Telephone: +49-2405-6909-69
- Fax: +49-2405-6909-99
- Web: [www.zyxel.de](http://www.zyxel.de)
- Regular Mail: ZyXEL Deutschland GmbH., Adenauerstr. 20/A2 D-52146, Wuerselen, Germany

### **Hungary**

- Support E-mail: [support@zyxel.hu](mailto:support@zyxel.hu)
- Sales E-mail: [info@zyxel.hu](mailto:info@zyxel.hu)
- Telephone: +36-1-3361649
- Fax: +36-1-3259100
- Web: [www.zyxel.hu](http://www.zyxel.hu)
- Regular Mail: ZyXEL Hungary, 48, Zoldlomb Str., H-1025, Budapest, Hungary

### **India**

- Support E-mail: [support@zyxel.in](mailto:support@zyxel.in)
- Sales E-mail: [sales@zyxel.in](mailto:sales@zyxel.in)
- Telephone: +91-11-30888144 to +91-11-30888153
- Fax: +91-11-30888149, +91-11-26810715
- Web: <http://www.zyxel.in>
- Regular Mail: India - ZyXEL Technology India Pvt Ltd., II-Floor, F2/9 Okhla Phase -1, New Delhi 110020, India

## Japan

- Support E-mail: support@zyxel.co.jp
- Sales E-mail: zyp@zyxel.co.jp
- Telephone: +81-3-6847-3700
- Fax: +81-3-6847-3705
- Web: www.zyxel.co.jp
- Regular Mail: ZyXEL Japan, 3F, Office T&U, 1-10-10 Higashi-Gotanda, Shinagawa-ku, Tokyo 141-0022, Japan

## Kazakhstan

- Support: <http://zyxel.kz/support>
- Sales E-mail: sales@zyxel.kz
- Telephone: +7-3272-590-698
- Fax: +7-3272-590-689
- Web: www.zyxel.kz
- Regular Mail: ZyXEL Kazakhstan, 43 Dostyk Ave., Office 414, Dostyk Business Centre, 050010 Almaty, Republic of Kazakhstan

## Malaysia

- Support E-mail: support@zyxel.com.my
- Sales E-mail: sales@zyxel.com.my
- Telephone: +603-8076-9933
- Fax: +603-8076-9833
- Web: <http://www.zyxel.com.my>
- Regular Mail: ZyXEL Malaysia Sdn Bhd., 1-02 & 1-03, Jalan Kenari 17F, Bandar Puchong Jaya, 47100 Puchong, Selangor Darul Ehsan, Malaysia

## North America

- Support E-mail: support@zyxel.com
- Support Telephone: +1-800-978-7222
- Sales E-mail: sales@zyxel.com
- Sales Telephone: +1-714-632-0882
- Fax: +1-714-632-0858
- Web: www.zyxel.com
- Regular Mail: ZyXEL Communications Inc., 1130 N. Miller St., Anaheim, CA 92806-2001, U.S.A.

## Norway

- Support E-mail: support@zyxel.no

- Sales E-mail: sales@zyxel.no
- Telephone: +47-22-80-61-80
- Fax: +47-22-80-61-81
- Web: www.zyxel.no
- Regular Mail: ZyXEL Communications A/S, Nils Hansens vei 13, 0667 Oslo, Norway

### **Poland**

- E-mail: info@pl.zyxel.com
- Telephone: +48-22-333 8250
- Fax: +48-22-333 8251
- Web: www.pl.zyxel.com
- Regular Mail: ZyXEL Communications, ul. Okrzei 1A, 03-715 Warszawa, Poland

### **Russia**

- Support: <http://zyxel.ru/support>
- Sales E-mail: sales@zyxel.ru
- Telephone: +7-095-542-89-29
- Fax: +7-095-542-89-25
- Web: www.zyxel.ru
- Regular Mail: ZyXEL Russia, Ostrovityanova 37a Str., Moscow 117279, Russia

### **Singapore**

- Support E-mail: support@zyxel.com.sg
- Sales E-mail: sales@zyxel.com.sg
- Telephone: +65-6899-6678
- Fax: +65-6899-8887
- Web: <http://www.zyxel.com.sg>
- Regular Mail: ZyXEL Singapore Pte Ltd., No. 2 International Business Park, The Strategy #03-28, Singapore 609930

### **Spain**

- Support E-mail: support@zyxel.es
- Sales E-mail: sales@zyxel.es
- Telephone: +34-902-195-420
- Fax: +34-913-005-345
- Web: www.zyxel.es
- Regular Mail: ZyXEL Communications, Arte, 21 5ª planta, 28033 Madrid, Spain

## **Sweden**

- Support E-mail: support@zyxel.se
- Sales E-mail: sales@zyxel.se
- Telephone: +46-31-744-7700
- Fax: +46-31-744-7701
- Web: www.zyxel.se
- Regular Mail: ZyXEL Communications A/S, Sjöporten 4, 41764 Göteborg, Sweden

## **Taiwan**

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-2-27399889
- Fax: +886-2-27353220
- Web: <http://www.zyxel.com.tw>
- Address: Room B, 21F., No.333, Sec. 2, Dunhua S. Rd., Da-an District, Taipei

## **Thailand**

- Support E-mail: support@zyxel.co.th
- Sales E-mail: sales@zyxel.co.th
- Telephone: +662-831-5315
- Fax: +662-831-5395
- Web: <http://www.zyxel.co.th>
- Regular Mail: ZyXEL Thailand Co., Ltd., 1/1 Moo 2, Ratchaphruk Road, Bangrak-Noi, Muang, Nonthaburi 11000, Thailand.

## **Turkey**

- Support E-mail: cso@zyxel.com.tr
- Telephone: +90 212 222 55 22
- Fax: +90-212-220-2526
- Web: <http://www.zyxel.com.tr>
- Address: Kaptanpasa Mahallesi Piyalepasa Bulvari Ortadogu Plaza N: 14/13 K: 6 Okmeydani/Sisli Istanbul/Turkey

## **Ukraine**

- Support E-mail: support@ua.zyxel.com
- Sales E-mail: sales@ua.zyxel.com
- Telephone: +380-44-247-69-78

- Fax: +380-44-494-49-32
- Web: [www.ua.zyxel.com](http://www.ua.zyxel.com)
- Regular Mail: ZyXEL Ukraine, 13, Pimonenko Str., Kiev 04050, Ukraine

### **United Kingdom**

- Support E-mail: [support@zyxel.co.uk](mailto:support@zyxel.co.uk)
- Sales E-mail: [sales@zyxel.co.uk](mailto:sales@zyxel.co.uk)
- Telephone: +44-1344-303044, 0845 122 0301 (UK only)
- Fax: +44-1344-303034
- Web: [www.zyxel.co.uk](http://www.zyxel.co.uk)
- Regular Mail: ZyXEL Communications UK Ltd., 11 The Courtyard, Eastern Road, Bracknell, Berkshire RG12 2XB, United Kingdom (UK)





# Index

## Numerics

802.1p [105](#), [106](#)

## A

access control [115](#)  
  activation [116](#)  
  configuration [116](#)  
  service type [117](#)  
activation  
  access control [116](#)  
  CWMP [144](#)  
  DHCP [78](#)  
  DMZ [92](#)  
  dynamic DNS [142](#)  
  DYNDNS wildcard [142](#)  
  firewalls [112](#)  
  QoS [103](#), [104](#)  
  SPI [113](#)  
  UPnP [129](#)  
address mapping [95](#)  
  types [96](#), [97](#)  
ADSL [109](#)  
  status [44](#)  
always-on connection [68](#), [72](#)  
application filter [122](#)  
ATM QoS [60](#), [63](#), [73](#), [74](#)  
  MBS [63](#)  
  PCR [63](#)  
  SCR [63](#)

## B

backup  
  configuration [155](#), [156](#), [157](#)  
broadcast [60](#)

## C

CBR [63](#), [74](#)  
CLI [25](#)  
Command Line Interface, see CLI  
configuration  
  access control [116](#)  
  backup [155](#), [156](#), [157](#)  
  CWMP [144](#)  
  DHCP [78](#)  
  file [151](#)  
  firewalls [112](#)  
  IP precedence [104](#)  
  IP/MAC filter [121](#)  
  LAN [77](#)  
  port forwarding [94](#)  
  restoring [153](#)  
  SNMP [126](#)  
  static route [87](#)  
  WAN [62](#)  
connection  
  always-on [72](#)  
CPE WAN Management Protocol, see CWMP  
CWMP [143](#)  
  activation [144](#)  
  configuration [144](#)

## D

DDoS [112](#)  
DeMilitarized Zone, see DMZ  
Denials of Service, see DoS  
device information [43](#)  
  ADSL [44](#)  
  LAN [44](#)  
  WAN [44](#)  
DHCP [76](#), [78](#), [80](#)  
diagnostic [161](#)  
DiffServ Code Point, see DSCP  
DMZ [91](#)

- activation [92](#)
- DNS [76, 80](#)
- Domain Name System, see DNS
- DoS [111](#)
- driver installation
  - verification [34](#)
- driver installation, USB [30](#)
- DSCP [104](#)
- dynamic DNS [141](#)
  - activation [142](#)
  - wildcard [141](#)
    - activation [142](#)
- Dynamic Host Configuration Protocol, see DHCP
- DYNDNS wildcard [141](#)
  - activation [142](#)

## E

- encapsulation [59](#)
  - PPPoA [67, 71](#)
  - PPPoE [67, 71](#)
  - RFC 1483 [71](#)

## F

- filters [119](#)
  - application [122](#)
  - IP/MAC [120](#)
    - structure [119](#)
  - IP/MAC filter
    - configuration [121](#)
  - URL [119, 123](#)
- firewalls [111](#)
  - configuration [112](#)
  - DDoS [112](#)
  - DoS [111](#)
  - LAND attack [112](#)
  - Ping of Death [112](#)
  - SYN attack [111](#)
- firmware [151](#)
  - upgrading [153](#)
- forwarding ports [90, 92](#)
  - configuration [94](#)
  - example [93](#)

- FTP [25](#)
  - backing up configuration [155](#)
  - limitations [152](#)
  - restoring configuration [153](#)
  - upgrading firmware [153, 154](#)

## I

- IGMP [61, 76, 83](#)
- Internet [59](#)
  - ADSL [109](#)
  - always-on connection [68, 72](#)
  - ATM QoS [60, 63, 73, 74](#)
  - encapsulation [59](#)
  - IGMP [61](#)
  - IP address [60, 65, 68, 72](#)
  - MAC spoofing [64, 66, 69](#)
  - MTU [64, 66, 68](#)
  - multicast [60, 64, 66, 69](#)
  - multiplexing [64, 65, 67, 69, 71](#)
  - RIP [64, 66](#)
  - RIP Routing Information Protocol, see RIP
  - setup [62](#)
  - TCP MSS [68](#)
  - VCI [62, 72](#)
  - VPI [62, 72](#)
- Internet Group Multicast Protocol, see IGMP
- IP address [60, 65, 68, 72, 75, 81](#)
  - ping [161](#)
  - private [82](#)
- IP precedence [105, 107](#)
  - configuration [104](#)
- IP/MAC filter [120](#)
  - configuration [121](#)
  - structure [119](#)

## L

- LAN [75](#)
  - configuration [77](#)
  - DHCP [76, 78, 80](#)
  - DNS [76, 80](#)
  - IGMP [76, 83](#)
  - IP address [75, 81](#)
  - multicast [76, 78, 83](#)

- RIP [76, 82](#)
  - status [44](#)
  - subnet mask [76, 81](#)
- LAND attack [112](#)
- LEDs [28](#)
- limitations
  - FTP [152](#)
- Local Area Network, see LAN
- login [37](#)
  - passwords [38, 147](#)
- logs [47](#)

## M

- MAC spoofing [64, 66, 69](#)
- mapping address [95](#)
  - types [96, 97](#)
- Maximum Burst Size, see MBS
- Maximum Transmission Unit, see MTU
- MBS [63, 73](#)
- metric [87](#)
- MTU [64, 66, 68](#)
- multicast [60, 64, 66, 69, 76, 78, 83](#)
  - IGMP [61](#)
- multiplexing [64, 65, 67, 69, 71](#)
  - LLC-based [72](#)
  - VC-based [72](#)

## N

- NAT [89, 90, 98](#)
  - address mapping [95](#)
    - types [96, 97](#)
  - DMZ [91](#)
  - example [99](#)
  - global [98](#)
  - inside [98](#)
  - local [98](#)
  - outside [98](#)
  - port forwarding [90, 92](#)
    - configuration [94](#)
    - example [93](#)
  - status [91](#)
  - SUA [90, 91](#)

- virtual server [92](#)
  - example [93](#)
- Network Address Translation, see NAT
- notation, subnet mask [212](#)

## P

- passwords [38, 147](#)
  - users [147](#)
- PCR [63, 73](#)
- Peak Cell Rate, see PCR
- Permanent Virtual Circuit, see PVC
- Ping of Death [112](#)
- port forwarding [90, 92](#)
  - configuration [94](#)
  - example [93](#)
- PPPoA [67, 71](#)
- PPPoE [67, 71](#)
- private IP address [82](#)
- PVC [60](#)

## Q

- QoS [101](#)
  - 802.1p [105, 106](#)
  - activation [103, 104](#)
  - DSCP [104](#)
  - example [101](#)
  - IP precedence [105, 107](#)
  - priority queue [107](#)
- Quality of Service, see QoS

## R

- related documentation [3](#)
- remote management
  - SNMP [125](#)
  - system timeout [116](#)
- reset [29](#)
- restart [159](#)
- restoring configuration [153](#)
- restrictions

FTP [152](#)  
RFC 1483 [71](#)  
RIP [64](#), [66](#), [68](#), [76](#), [78](#), [82](#)  
Routing Information Protocol, see RIP

## S

safety warnings [8](#)  
SCR [63](#), [73](#)  
Security Parameter Index, see SPI  
setup  
  access control [116](#)  
  DHCP [78](#)  
  firewalls [112](#)  
  IP precedenceQoS  
    IP precedence [104](#)  
  IP/MAC filter [121](#)  
  LAN [77](#)  
  port forwarding [94](#)  
  static route [87](#)  
  USB port [30](#)  
  WAN [62](#)  
Simple Network Management Protocol, see SNMP  
Single User Account, see SUA  
SNMP [26](#), [125](#)  
  configuration [126](#)  
SPI [112](#)  
  activation [113](#)  
static route [85](#)  
  configuration [87](#)  
  example [85](#)  
  metric [87](#)  
status [39](#), [43](#)  
  ADSL [44](#)  
  LAN [44](#)  
  NAT [91](#)  
  traffic statistics [49](#)  
  WAN [44](#)  
SUA [90](#), [91](#)  
subnet mask [76](#), [81](#), [210](#)  
  notation [212](#)  
subnetting [212](#)  
Sustain Cell Rate, see SCR  
SYN attack [111](#)

syntax conventions [6](#)  
system  
  backing up configuration [156](#)  
  backup configuration [155](#)  
  firmware [151](#)  
    upgrading [153](#)  
  LED [28](#)  
  login [37](#)  
  logs [47](#)  
  passwords [38](#), [147](#)  
    users [147](#)  
  reset [29](#)  
  restoring configuration [153](#)  
  status [39](#), [43](#)  
    ADSL [44](#)  
    LAN [44](#)  
    WAN [44](#)  
  time [149](#)  
  traffic statistics [49](#)

## T

TCP Maximum Segment Size, see TCP MSS  
TCP MSS [68](#)  
TFTP  
  upgrading firmware [154](#)  
time [149](#)  
TR-069 [26](#)  
traffic statistics [49](#)

## U

UBR [63](#), [74](#)  
unicast [60](#)  
Universal Plug and Play, see UPnP  
upgrading firmware [153](#)  
UPnP [127](#)  
  activation [129](#)  
  cautions [128](#)  
  example [130](#)  
  installation [130](#)  
  NAT traversal [127](#)  
URL [119](#)  
URL filter [123](#)

- URL [119](#)
- USB port [29](#)
  - driver installation [30](#)
  - verifying driver installation [34](#)

## V

- VBR [74](#)
- VBR-nRT [63, 74](#)
- VBR-RT [63, 74](#)
- VCI [62, 72](#)
- verifying USB driver installation [34](#)
- Virtual Channel Identifier, see VCI
- Virtual Path Identifier, see VPI
- virtual server [92](#)
  - example [93](#)
- VPI [62, 72](#)

## W

- WAN [59](#)
  - ADSL [109](#)
  - always-on connection [68, 72](#)
  - ATM QoS [60, 63, 73, 74](#)
  - encapsulation [59](#)
  - IGMP [61](#)
  - IP address [60, 65, 68, 72](#)
  - MAC spoofing [64, 66, 69](#)
  - MTU [64, 66, 68](#)
  - multicast [60, 64, 66, 69](#)
  - multiplexing [64, 65, 67, 69, 71](#)
  - RIP [64, 66, 68, 78](#)
  - setup [62](#)
  - status [44](#)
  - TCP MSS [68](#)
  - VCI [62, 72](#)
  - VPI [62, 72](#)
- web configurator [25, 37](#)
  - login [37](#)
  - passwords [38](#)
- Wide Area Network, see WAN
- wizard [51](#)

