



# PMG5318-B20A

Wireless N GPON HGU with 4-port GbE Switch

Version 1.00  
Edition 1, 8/2014

## User's Guide

### Default Login Details

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

---

**IMPORTANT!**

**READ CAREFULLY BEFORE USE.**

**KEEP THIS GUIDE FOR FUTURE REFERENCE.**

Screenshots and graphics in this book may differ slightly from your product due to differences in your product firmware or your computer operating system. Every effort has been made to ensure that the information in this manual is accurate.

### **Related Documentation**

- Quick Start Guide

The Quick Start Guide shows how to connect the GPON Device and get up and running right away.

# Table of Contents

|  |           |
|--|-----------|
| <b>Table of Contents .....</b>                     | <b>3</b>  |
| <b>Chapter 1</b>                                   |           |
| <b>Introduction.....</b>                           | <b>9</b>  |
| 1.1 Overview .....                                 | 9         |
| 1.2 Managing the GPON Device .....                 | 9         |
| 1.3 Good Habits for Managing the GPON Device ..... | 9         |
| 1.4 Applications for the GPON Device .....         | 9         |
| 1.4.1 Triple Play .....                            | 10        |
| 1.4.2 Internet Access .....                        | 10        |
| 1.4.3 VoIP Features .....                          | 11        |
| 1.5 LEDs (Lights) .....                            | 11        |
| 1.6 The Reset Button .....                         | 12        |
| 1.6.1 Using the Reset Button .....                 | 12        |
| 1.7 The WPS Button .....                           | 13        |
| 1.7.1 Using the WPS button .....                   | 13        |
| <b>Chapter 2</b>                                   |           |
| <b>The Web Configurator .....</b>                  | <b>15</b> |
| 2.1 Overview .....                                 | 15        |
| 2.1.1 Accessing the Web Configurator .....         | 15        |
| 2.2 Web Configurator Main Screen .....             | 16        |
| 2.2.1 Title Bar .....                              | 16        |
| 2.2.2 Navigation Panel .....                       | 17        |
| 2.2.3 Main Window .....                            | 18        |
| 2.2.4 Status Bar .....                             | 19        |
| <b>Chapter 3</b>                                   |           |
| <b>Status Screens .....</b>                        | <b>21</b> |
| 3.1 Overview .....                                 | 21        |
| 3.2 Status .....                                   | 21        |
| <b>Chapter 4</b>                                   |           |
| <b>WAN .....</b>                                   | <b>25</b> |
| 4.1 Overview .....                                 | 25        |
| 4.1.1 What You Need to Know .....                  | 25        |
| 4.2 Internet Access Setup Status .....             | 26        |
| 4.3 Internet Access Setup .....                    | 26        |
| 4.3.1 WAN Interface Type - PPPoE .....             | 27        |

|  |           |
|--|-----------|
| 4.3.2 WAN Interface Type - IP .....              | 32        |
| 4.3.3 WAN Interface Type - Bridging .....        | 36        |
| 4.3.4 802.1Q VLAN ID - Edit .....                | 37        |
| 4.4 Default Gateway .....                        | 38        |
| <b>Chapter 5</b>                                 |           |
| <b>LAN .....</b>                                 | <b>39</b> |
| 5.1 Overview .....                               | 39        |
| 5.1.1 What You Need to Know .....                | 39        |
| 5.2 The IP and DHCP Screen .....                 | 40        |
| 5.3 Client List .....                            | 41        |
| 5.4 Port Speed .....                             | 42        |
| <b>Chapter 6</b>                                 |           |
| <b>Wireless LAN.....</b>                         | <b>45</b> |
| 6.1 Overview .....                               | 45        |
| 6.1.1 What You Need to Know About Wireless ..... | 45        |
| 6.1.2 Before You Start .....                     | 46        |
| 6.2 The General Screen .....                     | 46        |
| 6.3 The Security Screen .....                    | 47        |
| 6.3.1 No Security .....                          | 48        |
| 6.3.2 WEP Encryption .....                       | 48        |
| 6.3.3 WPA(2)-PSK .....                           | 50        |
| 6.3.4 WPA(2) .....                               | 51        |
| 6.4 The WPS Screen .....                         | 52        |
| 6.5 The WPS Station Screen .....                 | 53        |
| 6.5.1 MAC Filter .....                           | 53        |
| 6.6 The WMM Screen .....                         | 55        |
| 6.7 The Status Screen .....                      | 55        |
| 6.8 The Isolation Screen .....                   | 56        |
| 6.9 Wireless LAN Technical Reference .....       | 57        |
| 6.9.1 Wireless Network Overview .....            | 57        |
| 6.9.2 Additional Wireless Terms .....            | 58        |
| 6.9.3 Wireless Security Overview .....           | 58        |
| 6.9.4 Signal Problems .....                      | 61        |
| 6.9.5 BSS .....                                  | 61        |
| 6.9.6 MBSSID .....                               | 62        |
| 6.9.7 Wireless Distribution System (WDS) .....   | 62        |
| 6.9.8 WiFi Protected Setup (WPS) .....           | 63        |
| <b>Chapter 7</b>                                 |           |
| <b>NAT.....</b>                                  | <b>71</b> |
| 7.1 Overview .....                               | 71        |

|  |           |
|--|-----------|
| 7.1.1 What You Need to Know .....                                | 71        |
| 7.2 Port Forwarding .....  | 73        |
| 7.2.1 Default Server IP Address .....                            | 74        |
| 7.2.2 Port Forwarding: Services and Port Numbers .....           | 74        |
| 7.2.3 Pinging a Device Behind NAT From the WAN (Example) .....   | 74        |
| 7.2.4 Configuring Servers Behind Port Forwarding (Example) ..... | 75        |
| 7.3 Configuring Port Forwarding .....                            | 76        |
| 7.3.1 Port Forwarding Edit .....                                 | 78        |
| <b>Chapter 8</b>   |           |
| <b>Quality of Service (QoS).....</b>                             | <b>79</b> |
| 8.1 Overview .....   | 79        |
| 8.2 The QoS General Screen .....                                 | 79        |
| <b>Chapter 9</b>   |           |
| <b>Voice .....</b>   | <b>81</b> |
| 9.1 Introduction .....   | 81        |
| 9.1.1 What You Need to Know .....                                | 81        |
| 9.2 SIP Service Provider .....                                   | 82        |
| 9.2.1 Dial Plan .....  | 85        |
| 9.3 SIP Account .....  | 87        |
| 9.4 Analog Phone .....   | 90        |
| 9.5 Speed Dial .....   | 90        |
| <b>Chapter 10</b>  |           |
| <b>Phone Usage .....</b>   | <b>93</b> |
| 10.1 Overview .....  | 93        |
| 10.2 Dialing a Telephone Number .....                            | 93        |
| 10.3 Using Speed Dial .....                                      | 93        |
| 10.4 Phone Services Overview .....                               | 93        |
| 10.4.1 The Flash Key .....                                       | 94        |
| 10.4.2 Supplementary Phone Services .....                        | 94        |
| <b>Chapter 11</b>  |           |
| <b>USB Services .....</b>  | <b>97</b> |
| 11.1 Overview .....  | 97        |
| 11.1.1 What You Can Do in this Chapter .....                     | 97        |
| 11.1.2 What You Need To Know .....                               | 97        |
| 11.2 The File Sharing Screen .....                               | 98        |
| 11.2.1 Before You Begin .....                                    | 98        |
| 11.3 Account Management .....                                    | 99        |
| 11.3.1 Add New File Sharing User .....                           | 100       |

|   |            |
|---|------------|
| <b>Chapter 12</b>   |            |
| <b>Remote Management.....</b>                                     | <b>103</b> |
| 12.1 Overview .....   | 103        |
| 12.1.1 What You Need to Know .....                                | 103        |
| 12.2 WWW .....  | 104        |
| 12.3 Telnet .....   | 105        |
| 12.4 FTP .....  | 106        |
| 12.5 SSH .....  | 107        |
| 12.6 ICMP .....   | 108        |
| 12.7 UPnP .....   | 109        |
| 12.7.1 What You Need to Know About UPnP .....                     | 109        |
| 12.7.2 Installing UPnP in Windows Example .....                   | 110        |
| 12.7.3 Using UPnP in Windows XP Example .....                     | 111        |
| 12.8 The TR-069 Screen .....                                      | 115        |
| <b>Chapter 13</b>   |            |
| <b>Static Route.....</b>  | <b>119</b> |
| 13.1 Overview .....   | 119        |
| 13.2 Static Route .....   | 119        |
| 13.2.1 Configuring Static Route .....                             | 120        |
| 13.2.2 Static Route Edit .....                                    | 121        |
| <b>Chapter 14</b>   |            |
| <b>Dynamic DNS .....</b>  | <b>123</b> |
| 14.1 Overview .....   | 123        |
| 14.1.1 What You Need To Know .....                                | 123        |
| 14.2 The Dynamic DNS Screen .....                                 | 124        |
| <b>Chapter 15</b>   |            |
| <b>Firewall .....</b>   | <b>127</b> |
| 15.1 Overview .....   | 127        |
| 15.1.1 What You Can Do in the Firewall Screens .....              | 127        |
| 15.1.2 What You Need to Know About Firewall .....                 | 128        |
| 15.2 The General Screen .....                                     | 130        |
| 15.3 The Rules Screen .....                                       | 131        |
| 15.3.1 The Rules Add Screen .....                                 | 132        |
| 15.3.2 Customized Services .....                                  | 133        |
| 15.3.3 Configuring a Customized Service .....                     | 134        |
| 15.4 Firewall Technical Reference .....                           | 135        |
| 15.4.1 Firewall Rules Overview .....                              | 135        |
| 15.4.2 Guidelines For Enhancing Security With Your Firewall ..... | 136        |
| 15.4.3 Security Considerations .....                              | 136        |

|  |            |
|--|------------|
| <b>Chapter 16</b>                          |            |
| <b>System</b>                              | <b>137</b> |
| 16.1 Overview                              | 137        |
| 16.1.1 What You Need to Know               | 137        |
| 16.2 General Setup                         | 138        |
| 16.3 Time Setting                          | 139        |
| 16.4 SLID                                  | 140        |
| <b>Chapter 17</b>                          |            |
| <b>Logs</b>                                | <b>141</b> |
| 17.1 Overview                              | 141        |
| 17.2 View Log                              | 141        |
| 17.3 Log Settings                          | 142        |
| <b>Chapter 18</b>                          |            |
| <b>Tools</b>                               | <b>145</b> |
| 18.1 Overview                              | 145        |
| 18.1.1 Some Warnings                       | 145        |
| 18.2 Firmware Upgrade                      | 145        |
| 18.3 Configuration                         | 147        |
| 18.3.1 Backup Configuration                | 147        |
| 18.3.2 Restore Configuration               | 147        |
| 18.3.3 Reset to Factory Defaults           | 148        |
| 18.4 Restart                               | 148        |
| <b>Chapter 19</b>                          |            |
| <b>Diagnostic</b>                          | <b>149</b> |
| 19.1 Overview                              | 149        |
| 19.2 General                               | 149        |
| <b>Chapter 20</b>                          |            |
| <b>Troubleshooting</b>                     | <b>151</b> |
| 20.1 Overview                              | 151        |
| 20.2 Power, Hardware Connections, and LEDs | 151        |
| 20.3 GPON Device Access and Login          | 152        |
| 20.4 Internet Access                       | 153        |
| 20.5 Phone Calls and VoIP                  | 154        |
| Appendix A Customer Support                | 155        |
| Appendix B Legal Information               | 161        |
| <b>Index</b>                               | <b>165</b> |





# Introduction

## 1.1 Overview

The PMG5318-B20A combines a fiber optic (GPON) router with a built-in switch. Its voice over IP (VoIP) capabilities allow you to use a traditional analog telephone to make Internet phone calls.

## 1.2 Managing the GPON Device

Use the GPON Device's built-in Web Configurator to manage it. You can connect to it using a web browser such as Firefox 2.0 (and higher) or Internet Explorer 6 (and higher). For details on connecting to it, see the [Section 2.1.1 on page 15](#).

## 1.3 Good Habits for Managing the GPON Device

Do the following things regularly to make the GPON Device more secure and to manage the GPON Device 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 GPON Device to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the GPON Device. You could simply restore your last configuration.

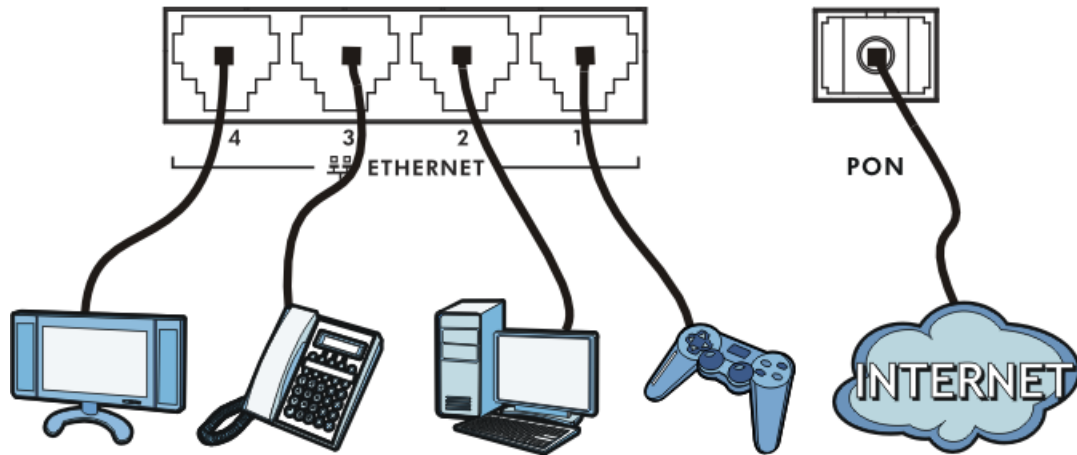
## 1.4 Applications for the GPON Device

Here are some example uses for which the GPON Device is well suited.

### 1.4.1 Triple Play

The ISP may provide “triple play” service to the GPON Device. This allows you to take advantage of such features as broadband Internet access, Voice over IP telephony, and streaming video/audio media, all at the same time with no noticeable loss in bandwidth.

Figure 1 Triple Play Example

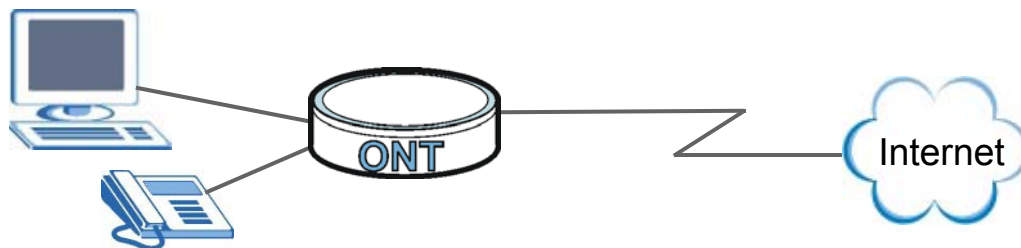


### 1.4.2 Internet Access

Your GPON Device provides shared Internet access by connecting a fiber optic line provided by the ISP to the PON port.

Figure 2 GPON Device's Router Features

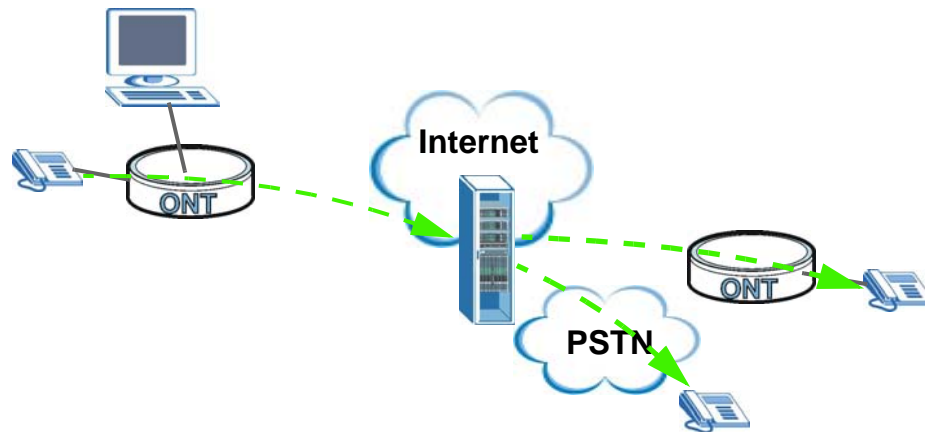
#### LAN



### 1.4.3 VoIP Features

You can register up to 2 SIP (Session Initiation Protocol) accounts and use the GPON Device to make and receive VoIP telephone calls:

**Figure 3** GPON Device's VoIP Features

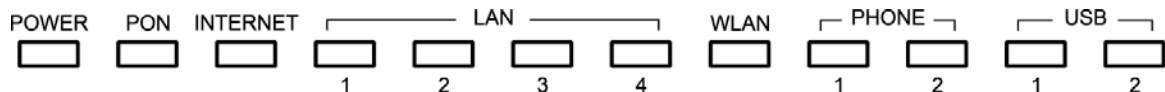


Calls via a VoIP service provider - the GPON Device sends your call to a VoIP service provider's SIP server which forwards your calls to either VoIP or PSTN phones.

## 1.5 LEDs (Lights)

The following graphic displays the labels of the LEDs.

**Figure 4** LEDs on the Top Panel



None of the LEDs are on if the GPON Device is not receiving power.

**Table 1** LED Descriptions

| LED   | COLOR  | STATUS   | DESCRIPTION   |
|-------|--------|----------|---|
| POWER | Green  | On       | The GPON Device is receiving power and ready for use.   |
|       |        | Blinking | The GPON Device is self-testing.  |
|       | Red    | On       | The GPON Device detected an error while self-testing, or there is a device malfunction.   |
|       |        | Off      | The GPON Device is not receiving power and there is no device malfunction.  |
| PON   | Green  | On       | The GPON Device has a PON line connection.  |
|       | Orange | On       | The GPON Device's PON port is physically connected but not registered.  |
|       | Red    | On       | The GPON Device's PON port is not connected. The optical transceiver may have malfunctioned or the fiber cable may not be connected or may be broken or damaged enough to break the PON connection. |

**Table 1** LED Descriptions

| LED       | COLOR  | STATUS   | DESCRIPTION   |
|-----------|--------|----------|---|
| INTERNET  | Green  | On       | The GPON Device has an IP connection but no traffic.  |
|           |        | Blinking | The GPON Device is sending or receiving IP traffic.   |
|           |        | Off      | The GPON Device attempted to make an IP connection but failed.  |
| LAN 1~4   | Orange | On       | The GPON Device has a 1G Ethernet connection with another device (such as a computer) on the Local Area Network (LAN) through this port.      |
|           |        | Blinking | The GPON Device is sending/receiving data to/from the LAN through this port.  |
|           | Green  | On       | The GPON Device has a 10/100M Ethernet connection with another device (such as a computer) on the Local Area Network (LAN) through this port. |
|           |        | Blinking | The GPON Device is sending/receiving data to/from the LAN through this port.  |
|           |        | Off      | The GPON Device does not have an Ethernet connection with the LAN through this port.  |
| WLAN      | Green  | On       | The wireless network is activated.  |
|           |        | Blinking | The GPON Device is communicating with other wireless clients.   |
|           |        | Off      | The wireless network is not activated.  |
|           | Orange | Blinking | The GPON Device is setting up a WPS connection.   |
| PHONE 1~2 | Green  | On       | A SIP account is registered for the phone port.   |
|           |        | Blinking | A telephone connected to the phone port has its receiver off the hook or there is an incoming call.   |
|           |        | Off      | The phone port does not have a SIP account registered.  |
|           | Red    | On       | SIP account registration failed.  |
| USB 1~2   | Green  | On       | The GPON Device recognizes a USB connection through the USB slot.   |
|           |        | Blinking | The GPON Device is sending or receiving data to or from the USB device connected to it.   |
|           |        | Off      | The GPON Device does not detect a USB connection through the USB slot.  |

Refer to [Section 1.5 on page 11](#) 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 the default.

### 1.6.1 Using the Reset Button

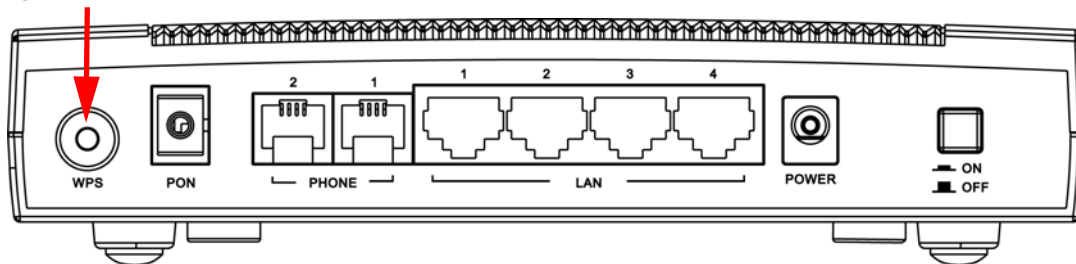
- 1 Make sure the **POWER** LED is on (not blinking).

- 2 To set the device back to the factory default settings, press the **RESET** button for more than 3 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 The WPS Button

You can use the **WPS** button on the back of the device to disable or activate the wireless LAN. You can also use it to activate WPS in order to quickly set up a wireless network with strong security.

**Figure 5** WPS Button



### 1.7.1 Using the WPS button

- 1 Make sure the **POWER** LED is on (not blinking).
- 2 If the wireless LAN of the GPON Device is enabled, the LED light shines green. If not, press the **WPS** button for more than 5 seconds and release it when the LED turns green. If you want to turn it off, press the **WPS** button for 5 seconds again.
- 3 Press the **WPS** button for over 5 seconds and release it. See above for **WPS** button location.
- 4 Press the WPS button on a compatible device within 2 minutes of pressing the button on the GPON Device. The **WLAN** LED should flash in orange while the GPON Device sets up a WPS connection with the other wireless device.
- 5 Once the connection is successfully made, the **WLAN** LED shines green.



# 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 8.0 and later or Firefox 23.0.0 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 GPON Device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

### 2.1.1 Accessing the Web Configurator

- 1 Make sure your GPON Device hardware is properly connected (refer to [Section 1.5 on page 11](#) for details on this).
- 2 Launch your web browser.
- 3 Type the default device address shown on the cover page of this User's Guide as the URL.
- 4 A password screen displays. Enter your password and click **Login**.

**Figure 6** Password Screen



PMG5318-B20A

Welcome to your router Configuration Interface !  
Enter your password and press enter or click "Login"

Username:

 Password:

Login Cancel

Note: For security reasons, the GPON Device automatically logs you out if you do not use the web configurator for an extended period of time. If this happens, log in again.

## 2.2 Web Configurator Main Screen

The main screen is divided into these parts:

**Figure 7** Main Screen

The screenshot shows the ZyXEL web configurator main screen. The interface is divided into four main sections:

- A - Title Bar:** Contains the ZyXEL logo and a Logout icon in the upper right corner.
- B - Navigation Panel:** A vertical sidebar on the left containing menu items: Status, Network, VoIP, Usb Services, Advanced, Security, and Maintenance.
- C - Main Window:** The central area displaying system information. It includes:
  - Device Information:** Host Name (PMG5318-B20A), Model Number (PMG5318-B20A), Firmware Version (V100AANC0).
  - WAN Status:** Mode (+), IP Address, IP Subnet Mask, Default Gateway, First DNS Server, Second DNS Server, Third DNS Server, IPv6 Global Address, IPv6 Link local Address, IPv6 First DNS Server, IPv6 Second DNS Server, IPv6 Third DNS Server.
  - System Status:** System Uptime (0:03:23), CPU Usage (67.53%), Memory Usage (59.79%).
  - Interface Status:** A table showing interface status and rates.
 

| Interface | Status | Rate      |
|-----------|--------|-----------|
| WAN       | Down   | /         |
| LAN1      | Down   | - / -     |
| LAN2      | Down   | - / -     |
| LAN3      | Up     | 1G / Full |
| LAN4      | Down   | - / -     |
  - Registration Status:** A table showing SIP account registration details.
 

| Account | Action                                  | Account Status | Associate Service Provider Name | URI               |
|---------|---|----------------|---------------------------------|-------------------|
| SIP 1   | <input type="button" value="Register"/> | Not Registered | Undefined                       | ChangeMe@ChangeMe |
| SIP 2   | <input type="button" value="Register"/> | In-Active      | Undefined                       | ChangeMe@ChangeMe |
- D - Status Bar:** A horizontal bar at the bottom showing a Message icon and the text 'Ready'.

- **A** - title bar
- **B** - navigation panel
- **C** - main window
- **D** - status bar

### 2.2.1 Title Bar

The title bar provides the **Logout** icon in the upper right corner. Click this icon to log out of the web configurator.





## 2.2.2 Navigation Panel

Use the menu items on the navigation panel to open screens to configure GPON Device features. The following tables describe each menu item.

**Table 2** Navigation Panel Summary

| LINK                | TAB                   | FUNCTION  |
|---------------------|-----------------------|---|
| Status              |                       | This screen shows the GPON Device's general device and network status information. Use this screen to access the statistics and client list.                |
| Network             |                       |   |
| WAN                 | Internet Access Setup | Use this screen to configure ISP parameters, WAN IP address assignment, DNS servers and other advanced properties.  |
|                     | Default Gateway       | Use this screen to configure your GPON Device's default gateway settings.   |
|                     | Multicast Setup       | Use this screen to configure your GPON Device's IGMP settings.  |
| LAN<br>Wireless LAN | IP & DHCP             | Use this screen to configure LAN TCP/IP and DHCP settings, enable Any IP and other advanced properties.   |
|                     | Client List           | Use this screen to look at the IP addresses currently assigned to DHCP clients and the IP addresses reserved for specific MAC addresses.                    |
|                     | Port Speed            | Use this screen to configure your GPON Device's LAN port speed settings.  |
|                     | General               | Use this screen to turn the wireless connection on or off, configure the MAC filter, and make other basic configuration changes.                            |
|                     | Security              | Use this screen to set up wireless security.  |
|                     | WPS                   | Use this screen to enable or disable WPS, generate a security PIN (Personal Identification Number) and see information about the GPON Device's WPS status.  |
|                     | WPS Station           | Use this screen to set up WPS by pressing a button or using a PIN.  |
|                     | MAC Filter            | Use this screen to allow or deny MAC address(es) for specific wireless networks.  |
|                     | WMM                   | Use this screen to enable Wi-Fi MultiMedia (WMM) to ensure quality of service in wireless networks for multimedia applications.                             |
|                     | Status                | Use this screen to view all associated wireless clients and their status.   |
|                     | Isolation             | Use this screen to control whether associated wireless clients can communicate with each other across a different wireless network through the GPON Device. |
| NAT                 | Port Forwarding       | Use this screen to configure port forwarding rules.   |
| QoS                 | General               | Use this screen to enable and configure QoS settings for specific traffic.  |
| VoIP                |                       |   |
| SIP                 | SIP Service Provider  | Use this screen to configure the SIP settings used by the GPON Device when you place calls over the Internet.   |
|                     | SIP Account           | Use this screen to configure your SIP account information.  |
| Phone               | Analog Phone          | Use this screen to set which phone ports use which SIP accounts.  |
| Phone Book          | Speed Dial            | Use this screen to configure speed dial for SIP phone numbers that you call often.  |
| Usb Services        |                       |   |
| File Sharing        | Share Configuration   | Use this screen to enable file sharing via the GPON Device.   |

**Table 2** Navigation Panel Summary

| LINK         | TAB                | FUNCTION  |
|--------------|--------------------|---|
|              | Account Management | Use this screen to configure user accounts to access file shares.   |
| Advanced     |                    |   |
| Remote MGMT  | WWW                | Use this screen to configure through which interface(s) and from which IP address(es) users can use HTTP to manage the GPON Device.   |
|              | Telnet             | Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet to manage the GPON Device. |
|              | FTP                | Use this screen to configure through which interface(s) and from which IP address(es) users can use FTP to access the GPON Device.    |
|              | SSH                | Use this screen to configure Secure SHell (SSH) connections to the GPON Device.   |
|              | ICMP               | Use this screen to set which interfaces respond to PING requests.   |
|              | UPnP               | Use this screen to configure UPnP connections to the GPON Device.   |
|              | TR-069             | Use this screen to configure your ONT to be managed by an ACS.  |
| Static Route |                    | Use this screen to configure the required information for a static route.   |
| Dynamic DNS  |                    | Use this screen to enable DDNS and configure the DDNS settings on the ONT.  |
| Security     |                    |   |
| Firewall     | General            | Use this screen to enable firewall and set the default action that the firewall takes on packets depending on packet direction.       |
|              | Rules              | Use this screen to view the configured firewall rules and add, edit or remove a firewall rule.  |
| Maintenance  |                    |   |
| System       | General            | Use this screen to configure your device's name, management inactivity timeout and password.  |
|              | Time Setting       | Use this screen to change your GPON Device's time and date.   |
|              | SLID               | Use this screen change your GPON Device's Subscriber Location ID (SLID) setting.  |
| Logs         | View Log           | Use this screen to display your device's logs.  |
|              | Log Settings       | Use this screen to select which logs and/or immediate alerts your device is to record. You can also set it to e-mail the logs to you. |
| Tools        | Firmware           | Use this screen to upload firmware to your device.  |
|              | Configuration      | Use this screen to backup and restore your device's configuration (settings) or reset the factory default settings.                   |
|              | Restart            | This screen allows you to reboot the GPON Device without turning the power off.   |
| Diagnostic   | General            | Use this screen to test the connections to other devices.   |

## 2.2.3 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 21](#) for more information about the **Status** screen.

## 2.2.4 Status Bar

Check the status bar when you click **Apply** or **OK** to verify that the configuration has been updated.



# Status Screens

## 3.1 Overview

Use the **Status** screens to look at the current status of the device, system resources, interfaces (LAN and WAN), and SIP accounts. You can also register and unregister SIP accounts.

## 3.2 Status

Click **Status** to access this screen.

**Figure 8** Status

The screenshot displays the Status screen with a 'Refresh Interval: None' dropdown and an 'Apply' button at the top right.

**Device Information**

|                  |              |
|------------------|--------------|
| Host Name        | PMG5318-B20A |
| Model Number     | PMG5318-B20A |
| Firmware Version | V100AANC0    |

**WAN Status**

|                           |       |
|---------------------------|-------|
| + Mode                    | PPPoE |
| - IP Address              |       |
| - IP Subnet Mask          |       |
| - Default Gateway         |       |
| - First DNS Server        |       |
| - Second DNS Server       |       |
| - Third DNS Server        |       |
| - IPv6 Global Address     | ::/64 |
| - IPv6 Link local Address | ::/64 |
| - IPv6 First DNS Server   | ::    |
| - IPv6 Second DNS Server  | ::    |
| - IPv6 Third DNS Server   | ::    |
| + Mode                    | IPOE  |
| - IP Address              |       |
| - IP Subnet Mask          |       |
| - Default Gateway         |       |
| - First DNS Server        |       |
| - Second DNS Server       |       |
| - Third DNS Server        |       |
| - IPv6 Global Address     | ::/64 |
| - IPv6 Link local Address | ::/64 |
| - IPv6 First DNS Server   | ::    |
| - IPv6 Second DNS Server  | ::    |
| - IPv6 Third DNS Server   | ::    |



**LAN Information**

|                     |                   |
|---------------------|-------------------|
| - IP Address        | 192.168.1.1       |
| - IP Subnet Mask    | 255.255.255.0     |
| - MAC Address       | 28:28:5d:51:5a:90 |
| - First DNS Server  | 192.168.1.1       |
| - Second DNS Server | 0.0.0.0           |
| - Third DNS Server  | 0.0.0.0           |

**Transceiver Status**

|                    |                |
|--------------------|----------------|
| - Temperature      | 43.32(Celsius) |
| - Voltage          | 3.33(Volts)    |
| - Bias Current     | 0.00(mA)       |
| - Optical Tx Power | N/A(dBm)       |
| - Optical Rx Power | N/A(dBm)       |

**System Status**

|               |  |
|---------------|--|
| System Uptime | 0:05:45  |
| CPU Usage     |  67.27%   |
| Memory Usage  |  61.03% |

**Interface Status**

| Interface | Status | Rate      |
|-----------|--------|-----------|
| WAN       | Down   | /         |
| LAN1      | Down   | - / -     |
| LAN2      | Down   | - / -     |
| LAN3      | Up     | 1G / Full |
| LAN4      | Down   | - / -     |

**Registration Status**

| Account | Action                                  | Account Status | Associate Service Provider Name | URI               |
|---------|---|----------------|---------------------------------|-------------------|
| SIP 1   | <input type="button" value="Register"/> | Not Registered | Undefined                       | ChangeMe@ChangeMe |
| SIP 2   | <input type="button" value="Register"/> | In-Active      | Undefined                       | ChangeMe@ChangeMe |

Each field is described in the following table.

**Table 3** Status

| LABEL                              | DESCRIPTION   |
|------------------------------------|---|
| Device Information                 |   |
| Host Name                          | This field displays the GPON Device system name. It is used for identification. You can change this in the <b>Maintenance &gt; System &gt; General</b> screen's <b>System Name</b> field.   |
| Model Name                         | This is the model name of the GPON Device.  |
| Firmware Version                   | This field displays the current version of the firmware inside the device. It also shows the date the firmware version was created. Click this to go to the screen where you can change it. |
| WAN Status                         | This section displays connection information for each WAN connection configured on the GPON Device.   |
| Mode                               | This is the method of encapsulation used by your service provider for this WAN connection.  |
| IP Address                         | This field displays the IP address of the WAN connection.   |
| IP Subnet Mask                     | This field displays the WAN connection's subnet mask.   |
| Default Gateway                    | This field displays the IP address of the default gateway, if applicable.   |
| First/Second/Third DNS Server      | These are the DNS server IP addresses assigned to the WAN connection.   |
| IPv6 Global Address                | This is the IPv6 global address of the WAN connection.  |
| IPv6 Link local Address            | This is the link-local address assigned to the WAN connection.  |
| IPv6 First/Second/Third DNS Server | These are the IPv6 DNS server IP addresses assigned to the WAN connection.  |
| LAN Information                    |   |
| IP Address                         | This field displays the current IP address of the GPON Device in the LAN. Click this to go to the screen where you can change it.   |
| IP Subnet Mask                     | This field displays the GPON Device's current subnet mask in the LAN.   |
| MAC Address                        | This shows the LAN Ethernet adapter MAC (Media Access Control) address of your GPON Device.   |
| First/Second/Third DNS Server      | These are the DNS server IP addresses the GPON Device passes to the DHCP clients.   |
| Transceiver Status                 |   |
| Temperature                        | This displays the temperature in Celsius. The normal range is 0-70 degrees.   |
| Voltage                            | This displays the voltage in Volts. The normal range is 3.13-3.47 Volts.  |
| Bias Current                       | This displays the bias current in mA. The normal range is 4-50 mA.  |
| Optical Tx Power                   | This displays the optical transmitting power in dBm.  |
| Optical Rx Power                   | This displays the optical receiving power in dBm. The normal range is -28 to -8 dBm.  |
| System Status                      |   |

**Table 3** Status

| LABEL                           | DESCRIPTION   |
|---------------------------------|---|
| System Uptime                   | This field displays how long the GPON Device has been running since it last started up. The GPON Device starts up when you plug it in, when you restart it ( <b>Maintenance &gt; Tools &gt; Restart</b> ), or when you reset it.  |
| CPU Usage                       | This field displays what percentage of the GPON Device's processing ability is currently used. When this percentage is close to 100%, the GPON Device is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications.   |
| Memory Usage                    | This field displays what percentage of the GPON Device's memory is currently used. Usually, this percentage should not increase much. If memory usage does get close to 100%, the GPON Device is probably becoming unstable, and you should restart the device. See <a href="#">Section 18.4 on page 148</a> , or turn it off (unplug the power) for a few seconds.   |
| Interface Status                |   |
| Interface                       | This column identifies the interface on the GPON Device.  |
| Status                          | This field displays <b>Up</b> when the interface has a connection and <b>Down</b> when it does not.   |
| Rate                            | This field displays the connection speed of the WAN interface's PON connection when it is connected. This field displays the connection speed and duplex for a connected LAN interface.   |
| Registration Status             |   |
| Account                         | This column displays each SIP account in the GPON Device.   |
| Action                          | <p>If the SIP account is already registered with the SIP server, the <b>Account Status</b> field displays <b>Registered</b>.</p> <p>Click <b>Unregister</b> to delete the SIP account's registration in the SIP server. This does not cancel your SIP account, but it deletes the mapping between your SIP identity and your IP address or domain name.</p> <p>If the SIP account is not registered with the SIP server, the <b>Account Status</b> field displays <b>Not Registered</b>.</p> <p>Click <b>Register</b> to have the GPON Device attempt to register the SIP account with the SIP server.</p> <p>The button is grayed out if the SIP account is disabled.</p>  |
| Account Status                  | <p>This field displays the current registration status of the SIP account. You have to register SIP accounts with a SIP server to use VoIP.</p> <p><b>Inactive</b> - The SIP account is not active. You can activate it in <b>VoIP &gt; SIP &gt; SIP Account</b>.</p> <p><b>Not Registered</b> - The last time the GPON Device tried to register the SIP account with the SIP server, the attempt failed. Use the <b>Register</b> button to register the account again. The GPON Device automatically tries to register the SIP account when you turn on the GPON Device or when you activate it.</p> <p><b>Registered</b> - The SIP account is already registered with the SIP server. You can use it to make a VoIP call.</p> |
| Associate Service Provider Name | This column displays the service provider name for each SIP account.  |
| URI                             | This field displays the account number and service domain of the SIP account. You can change these in <b>VoIP &gt; SIP &gt; SIP Settings</b> .  |





## 4.1 Overview

This chapter describes how to configure WAN settings. A WAN (Wide Area Network) is an outside connection to another network or the Internet.

### 4.1.1 What You Need to Know

The following terms and concepts may help as you read through the chapter.

#### Encapsulation

Be sure to use the encapsulation method required by the ISP. The GPON Device supports the following methods.

#### PPP over Ethernet

The GPON Device supports PPPoE (Point-to-Point Protocol over Ethernet). 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 GPON Device (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the GPON Device does that part of the task.

#### IP Address Assignment

A static IP is a fixed IP that the ISP provides. A dynamic IP is not fixed; the ISP assigns a different one each time. The Single User Account feature can be enabled or disabled if you have either a dynamic or static IP. However the encapsulation method assigned influences your choices for IP address and ENET ENCAP gateway.

## Multicast and IGMP

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 Management Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data.

## 4.2 Internet Access Setup Status

Use this screen to view your GPON Device's WAN settings. Click **Network > WAN**. Your GPON Device's number and names of default WAN interfaces may vary from this example.

**Figure 9** Internet Access Setup Status

| Interface | Description | Type  | Service Type | Vlan ID | Vlan 802.1p | ICMP     | NAT     | Modify |
|-----------|-------------|-------|--------------|---------|-------------|----------|---------|--------|
| wan1      | PPPoE_ETH   | PPPoE | Data,IPTV    | 10      | 0           | Enabled  | Enabled |        |
| wan2      | IPoE_ETH    | IPoE  | VoIP         | 20      | 0           | Disabled | Enabled |        |

The following table describes the labels in this screen.

**Table 4** Internet Access Setup Status

| LABEL        | DESCRIPTION  |
|--------------|--|
| Interface    | This shows the name of the interface used by this connection.  |
| Description  | This is the service description for traffic using this connection.   |
| Type         | This shows the method of encapsulation used by this connection.  |
| Service Type | This is the service type for traffic using this connection.  |
| Vlan ID      | This shows the VLAN ID assigned to traffic for this connection. This is assigned by the OLT.                                       |
| Vlan 802.1p  | This displays the 802.1P priority level assigned to traffic sent through this connection.  |
| ICMP         | This shows whether the WAN interface will respond to ICMP packets.   |
| NAT          | This shows whether NAT is activated or not for this interface. NAT is not available when the connection uses the bridging service. |
| Modify       | Click the <b>Edit</b> icon to configure the WAN connection.<br>Click the <b>Remove</b> icon to delete the WAN connection.          |
| Add          | Click this to create a new WAN connection.   |

## 4.3 Internet Access Setup

Use these screens to configure your GPON Device's WAN interfaces. Click **Modify** or **Add** in the **Network > WAN > Internet Access Setup** status screen.

The available fields vary in this screen depending on the option (**PPPoE**, **IP**, or **Bridging**) you select in the **WAN interface type** field.

### 4.3.1 WAN Interface Type - PPPoE

Select **PPPoE** as the **WAN interface type** to open the following screen.

**Figure 10** Internet Access Setup - PPPoE

**Internet Access Setup**

**General**

WAN interface type: PPPoE

WAN IP Connection: IPv4 & IPv6

User Name: guest

Password: .....

Service Name:

Authentication Method: AUTO

**Service**

Service Description: PPPoE\_ETH

802.1Q VLAN ID [0-4092]: 10 [Edit](#)

802.1P Priority Method:  Default Pbit  DSCP to Pbit (default Pbit for Non-IP)

WAN service type:  Data  VoIP  Management  IPTV

Enable WAN Connection Limit

Connection Number:

**IGMP Proxy Configuration**

LAN IGMP version: V3

WAN IGMP version: V2

Query Interval: 125

**Connection**

Always-on

Connection Demand Max Idle Timeout: 0 sec

**Feature**

Enable NAT  Enable ICMP  Enable IP Conflict Detection

**IPv4 IP Address**

Obtain an IP Address Automatically

Static IP Address

**IPv4 DNS Server**

First DNS Server: FromISP

Second DNS Server: FromISP

Third DNS Server: FromISP

The screenshot shows a configuration window for IPv6 settings. It is divided into three main sections:

- IPv6 IP Address:** Contains a dropdown for 'Address Configuration Mode' set to 'SLAAC'. Below are input fields for 'Link-Local Address', 'IPv6 Address' (marked as optional), 'Prefix Length' (with a range of 16-64), and 'Default Gateway' (marked as optional).
- IPv6 DNS Server:** Contains three rows for 'First DNS Server', 'Second DNS Server', and 'Third DNS Server'. Each row has a dropdown menu set to 'FromISP' and an adjacent input field.
- IPv6 Router Advertisement Setting:** Contains checkboxes for 'M Flag' and 'O Flag'. Below are input fields for 'Preference', 'Prefix', and 'Prefix Length'.

At the bottom of the window are 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

**Table 5** Internet Access Setup - PPPoE

| LABEL                 | DESCRIPTION  |
|-----------------------|--|
| General               |  |
| WAN interface type    | Select PPPoE as the method of encapsulation used by your ISP from the drop-down list box.  |
| WAN IP Connection     | Select <b>IPv4</b> to have this WAN run IPv4 only.<br>Select <b>IPv6/IPv4</b> to allow this WAN to run IPv4 and IPv6 at the same time.<br>Select <b>IPv6</b> to have this WAN run IPv6 only.   |
| User Name             | Enter the user name exactly as assigned by the ISP. 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 user name above.  |
| Service Name          | Type the name of your PPPoE service here.  |
| Authentication Method | The GPON Device supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure than PAP; however, PAP is readily available on more platforms.<br>Use the drop-down list box to select an authentication protocol for outgoing calls.<br>Options are:<br><b>AUTO</b> - Your GPON Device accepts either CHAP or PAP when requested by this remote node.<br><b>CHAP</b> - Your GPON Device accepts CHAP only.<br><b>PAP</b> - Your GPON Device accepts PAP only. |
| Service               |  |
| Service Description   | Enter a description to identify this WAN interface.  |

**Table 5** Internet Access Setup - PPPoE (continued)

| LABEL                              | DESCRIPTION  |
|------------------------------------|--|
| 802.1Q VLAN ID                     | This shows the VLAN ID assigned to traffic for this connection. Click <b>Edit</b> to open a screen where you can select a different VLAN ID. See <a href="#">Section 4.3.4 on page 37</a> for information on this screen.  |
| 802.1P Priority Method             | Select the 802.1P priority method to be assigned to traffic sent through this connection.  |
| WAN service type                   | If you select <b>PPPoE</b> or <b>IP</b> in the <b>WAN service type</b> field above, select which type of traffic ( <b>Data</b> , <b>VoIP</b> , <b>Management</b> , and/or <b>IPTV</b> ) can use this WAN interface.<br><br>This field displays <b>Bridge</b> if you select <b>Bridge</b> in the <b>WAN service type</b> field above.   |
| Enable WAN Connection Limit        | Select <b>Enable WAN Connection Limit</b> to limit the number of connections for a service type.   |
| Connection Number                  | If you select <b>Enable WAN Connection Limit</b> , you can specify the maximum number of connections. For a low priority service type, you can set this number to a lower value.   |
| IGMP Proxy Configuration           |  |
| LAN IGMP version                   | Select the IGMP version to be used for IGMP messages originating from the LAN.   |
| WAN IGMP version                   | Select the IGMP version to be used for IGMP messages originating from the WAN.   |
| Query Interval                     | Enter the time period in seconds between general queries. A general query is a message sent to learn the multicast reception state of the device attached to the interface.  |
| Connection                         |  |
| Always-on                          | Select <b>Always-on</b> when you want your connection up all the time. The GPON Device will try to bring up the connection automatically if it is disconnected.  |
| Connect Demand                     | Select <b>Connect Demand</b> when you don't want the connection up all the time and specify an idle time-out in the <b>Max Idle Timeout</b> field.   |
| Feature                            |  |
| Enable NAT                         | Select this check box to activate NAT on this connection.  |
| Enable ICMP                        | Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.<br><br>Select this check box to reply to incoming WAN Ping requests. If this is not enabled, the GPON Device will not respond to any incoming Ping requests. |
| Enable IP Conflict Detection       | Select this to have the GPON Device detect if the IP address assigned to this WAN interface conflicts with other WAN IP addresses.   |
| IPv4 IP Address                    |  |
| Obtain an IP Address Automatically | A dynamic IP address is not fixed; the ISP assigns a different one each time you connect to the Internet.<br><br>Select <b>Obtain an IP Address Automatically</b> to get a dynamic IPv4 address for this WAN.  |
| Static IP Address                  | A static IP address is a fixed IP that the ISP provides.<br><br>Select <b>Static IP Address</b> and type the ISP assigned information in the field below.  |
| IPv4 DNS Server                    |  |

**Table 5** Internet Access Setup - PPPoE (continued)

| LABEL   | DESCRIPTION   |
|---|---|
| First DNS Server<br>Second DNS Server<br>Third DNS Server | Select <b>From ISP</b> if the ISP dynamically assigns DNS server information (and the GPON Device's WAN IP address) and you select <b>Obtain an IP Address Automatically</b> .<br><br>Select <b>UserDefined</b> if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right.<br><br>Select <b>None</b> if you do not want to configure DNS servers. You must have another DNS server on your LAN, or else the computers must have their DNS server addresses manually configured. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.   |
| IPv6 IP Address   |   |
| Address Configuration Mode                                | Select <b>DHCP</b> if you want to obtain an IPv6 address from a DHCPv6 server. The IP address assigned by a DHCPv6 server has priority over the IP address automatically generated by the Device using the IPv6 prefix from an RA.<br>Select <b>SLAAC</b> (Stateless address autoconfiguration) to have the Device use the prefix to automatically generate a unique IP address that does not need to be maintained by a DHCP server.<br>Select <b>Auto</b> to have the Device indicate to hosts for IPv6 address generation depending on the M/O (Managed/Other) flag values in the router advertisements sending to hosts. You can configure the M/O flag settings in the <b>IPv6 Router Advertisement Setting</b> section below. |
| Link-Local Address  | This field displays the link-local address the GPON Device generated itself for the WAN.  |
| IPv6 Address  | Enter the IPv6 address assigned by your ISP for this WAN.   |
| Prefix Length   | Enter the address prefix length to specify how many most significant bits in an IPv6 address compose the network address.   |
| Default Gateway   | Enter the IP address of the next-hop gateway. The gateway is a router or switch on the same segment as your GPON Device's interface(s). The gateway helps forward packets to their destinations.  |
| IPv6 DNS Server   |   |
| First DNS Server<br>Second DNS Server<br>Third DNS Server | Select <b>From ISP</b> if the ISP dynamically assigns DNS server information (and the GPON Device's WAN IP address) and you select <b>Obtain an IP Address Automatically</b> .<br><br>Select <b>UserDefined</b> if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right.<br><br>Select <b>None</b> if you do not want to configure DNS servers. You must have another DNS server on your LAN, or else the computers must have their DNS server addresses manually configured. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.   |
| IPv6 Router Advertisement Setting                         | Select this option if you want to have the GPON Device use the IPv6 prefix from the connected router's Router Advertisement (RA) to generate an IPv6 address.   |
| M Flag  | Select this to have the GPON Device indicate to hosts to obtain network settings (such as WAN IP, LAN prefix and DNS settings) through DHCPv6.<br>Clear this to have the GPON Device check O flag.  |
| O Flag  | Select this to have the GPON Device indicate to hosts to obtain DNS information and LAN prefix through DHCPv6.<br>Clear this to have the GPON Device not get information through DHCPv6.  |

**Table 5** Internet Access Setup - PPPoE (continued)

| LABEL         | DESCRIPTION  |
|---------------|--|
| Preference    | This field displays the router preference ( <b>Low</b> , <b>Medium</b> or <b>High</b> ) the gateway assigned to the GPON Device. The GPON Device sends this preference in the router advertisements to tell hosts what preference they should use for the GPON Device. This helps hosts to choose their default router especially when there are multiple IPv6 routers in the network.<br><br>Note: Make sure the hosts also support router preference to make this function work. |
| Prefix        | Enter the IPv6 prefix provided by your ISP.  |
| Prefix Length | Enter the bit number of the IPv6 subnet mask provided by your ISP.   |
| Apply         | Click <b>Apply</b> to save the changes.  |
| Cancel        | Click <b>Cancel</b> to begin configuring this screen afresh.   |

## 4.3.2 WAN Interface Type - IP

Select **IP** as the **WAN interface type** to open the following screen.

**Figure 11** Internet Access Setup - IP

**Internet Access Setup**

**General**

WAN interface type: IP  
WAN IP Connection: IPv4 & IPv6

**ARP Ping**

Enable ARP Ping:

**Service**

Service Description:   
802.1Q VLAN ID [0-4092]: 10 [Edit](#)  
802.1P Priority Method:  Default Pbit  DSCP to Pbit (default Pbit for Non-IP)  
WAN service type:  Data  VoIP  Management  IPTV  
 Enable WAN Connection Limit  
Connection Number:

**IGMP Proxy Configuration**

LAN IGMP version: V3  
WAN IGMP version: V2  
Query Interval: 125

**Feature**

Enable NAT  Enable ICMP  Enable IP Conflict Detection

**IPv4 IP Address**

Obtain an IP Address Automatically  
 Enable DHCP Option 60  
Vendor class Identifier:   
 Enable DHCP Option 61  
 Hexadecimal  
Client Identifier:   
 Enable DHCP Option 125  
 Static IP Address



The following table describes the labels in this screen.

**Table 6** Internet Access Setup - IP

| LABEL                  | DESCRIPTION  |
|------------------------|--|
| General                |  |
| WAN interface type     | Select <b>IP</b> as the method of encapsulation used by your ISP from the drop-down list box.  |
| WAN IP Connection      | Select <b>IPv4</b> to have this WAN run IPv4 only.<br>Select <b>IPv6/IPv4</b> to allow this WAN to run IPv4 and IPv6 at the same time.<br>Select <b>IPv6</b> to have this WAN run IPv6 only.   |
| ARP Ping               |  |
| Enable ARP Ping        | Select this to have the GPON Device send ARP requests to the gateway regularly if the gateway IP might change often. If the GPON Device does not receive the gateway's response, the GPON Device requests a new gateway IP through DHCP. |
| Service                |  |
| Service Description    | Enter a description to identify this WAN interface.  |
| 802.1Q VLAN ID         | This shows the VLAN ID assigned to traffic for this connection. Click <b>Edit</b> to open a screen where you can select a different VLAN ID. See <a href="#">Section 4.3.4 on page 37</a> for information on this screen.                |
| 802.1P Priority Method | Select the 802.1P priority method to be assigned to traffic sent through this connection.  |

**Table 6** Internet Access Setup - IP (continued)

| LABEL                              | DESCRIPTION  |
|------------------------------------|--|
| WAN service type                   | Select which type of traffic ( <b>Data</b> , <b>VoIP</b> , <b>Management</b> , and/or <b>IPTV</b> ) can use this WAN interface.  |
| Enable WAN Connection Limit        | Select <b>Enable WAN Connection Limit</b> to limit the number of connections for a service type.   |
| Connection Number                  | If you select <b>Enable WAN Connection Limit</b> , you can specify the maximum number of connections. For a low priority service type, you can set this number to a lower value.   |
| IGMP Proxy Configuration           |  |
| LAN IGMP version                   | Select the IGMP version to be used for IGMP messages originating from the LAN.   |
| WAN IGMP version                   | Select the IGMP version to be used for IGMP messages originating from the WAN.   |
| Query Interval                     | Enter the time period in seconds between general queries. A general query is a message sent to learn the multicast reception state of the device attached to the interface.  |
| Feature                            |  |
| Enable NAT                         | Select this check box to activate NAT on this connection.  |
| Enable ICMP                        | Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.<br><br>Select this check box to reply to incoming WAN Ping requests. If this is not enabled, the GPON Device will not respond to any incoming Ping requests. |
| Enable IP Conflict Detection       | Select this to have the GPON Device detect if the IP address assigned to this WAN interface conflicts with other WAN IP addresses.   |
| IPv4 IP Address                    |  |
| Obtain an IP Address Automatically | A dynamic IP address is not fixed; the ISP assigns a different one each time you connect to the Internet.<br><br>Select <b>Obtain an IP Address Automatically</b> to get a dynamic IPv4 address for this WAN.  |
|                                    | The following DHCP Option 60, 61, and 125 fields are available only when you select <b>IP</b> in the <b>WAN interface type</b> field above.  |
| Enable DHCP Option 60              | Select this to identify the vendor and functionality of the GPON Device in DHCP requests that the GPON Device sends to a DHCP server when getting a WAN IP address.  |
| Vendor Class Identifier            | Enter the Vendor Class Identifier (Option 60), such as the type of the hardware or firmware.   |
| Enable DHCP Option 61              | Select this to identify the GPON Device in DHCP requests that the GPON Device sends to a DHCP server when getting a WAN IP address.  |
| Client Identifier                  | If <b>Hexadecimal</b> is selected, you can enter the GPON Device's hardware address, that is the MAC address in this field using hexadecimal characters.<br><br>If <b>String</b> is selected, enter a string to identify the GPON Device using alphanumeric characters.  |
| Enable DHCP Option 125             | Select this to add vendor specific information to DHCP requests that the GPON Device sends to a DHCP server when getting a WAN IP address.   |
| Static IP Address                  | A static IP address is a fixed IP that the ISP provides.<br><br>Select <b>Static IP Address</b> and type the ISP assigned information in the field below.  |
| IPv4 DNS Server                    |  |

**Table 6** Internet Access Setup - IP (continued)

| LABEL   | DESCRIPTION  |
|---|--|
| First DNS Server<br>Second DNS Server<br>Third DNS Server | <p>Select <b>From ISP</b> if the ISP dynamically assigns DNS server information (and the GPON Device's WAN IP address) and you select <b>Obtain an IP Address Automatically</b>.</p> <p>Select <b>UserDefined</b> if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right.</p> <p>Select <b>None</b> if you do not want to configure DNS servers. You must have another DNS server on your LAN, or else the computers must have their DNS server addresses manually configured. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.</p>  |
| IPv6 IP Address   |  |
| Address Configuration Mode                                | <p>Select <b>DHCP</b> if you want to obtain an IPv6 address from a DHCPv6 server. The IP address assigned by a DHCPv6 server has priority over the IP address automatically generated by the Device using the IPv6 prefix from an RA.</p> <p>Select <b>SLAAC</b> (Stateless address autoconfiguration) to have the Device use the prefix to automatically generate a unique IP address that does not need to be maintained by a DHCP server.</p> <p>Select <b>Auto</b> to have the Device indicate to hosts for IPv6 address generation depending on the M/O (Managed/Other) flag values in the router advertisements sending to hosts. You can configure the M/O flag settings in the <b>IPv6 Router Advertisement Setting</b> section below.</p> |
| Link-Local Address  | This field displays the link-local address the GPON Device generated itself for the WAN.   |
| IPv6 Address  | Enter the IPv6 address assigned by your ISP for this WAN.  |
| Prefix Length   | Enter the address prefix length to specify how many most significant bits in an IPv6 address compose the network address.  |
| Default Gateway   | Enter the IP address of the next-hop gateway. The gateway is a router or switch on the same segment as your GPON Device's interface(s). The gateway helps forward packets to their destinations.   |
| IPv6 DNS Server   |  |
| First DNS Server<br>Second DNS Server<br>Third DNS Server | <p>Select <b>From ISP</b> if the ISP dynamically assigns DNS server information (and the GPON Device's WAN IP address) and you select <b>Obtain an IP Address Automatically</b>.</p> <p>Select <b>UserDefined</b> if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right.</p> <p>Select <b>None</b> if you do not want to configure DNS servers. You must have another DNS server on your LAN, or else the computers must have their DNS server addresses manually configured. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.</p>  |
| IPv6 Router Advertisement Setting                         | Select this option if you want to have the GPON Device use the IPv6 prefix from the connected router's Router Advertisement (RA) to generate an IPv6 address.  |
| M Flag  | <p>Select this to have the GPON Device indicate to hosts to obtain network settings (such as WAN IP, LAN prefix and DNS settings) through DHCPv6.</p> <p>Clear this to have the GPON Device check O flag.</p>  |
| O Flag  | <p>Select this to have the GPON Device indicate to hosts to obtain DNS information and LAN prefix through DHCPv6.</p> <p>Clear this to have the GPON Device not get information through DHCPv6.</p>  |

**Table 6** Internet Access Setup - IP (continued)

| LABEL         | DESCRIPTION  |
|---------------|--|
| Preference    | This field displays the router preference ( <b>Low</b> , <b>Medium</b> or <b>High</b> ) the gateway assigned to the GPON Device. The GPON Device sends this preference in the router advertisements to tell hosts what preference they should use for the GPON Device. This helps hosts to choose their default router especially when there are multiple IPv6 routers in the network.<br><br>Note: Make sure the hosts also support router preference to make this function work. |
| Prefix        | Enter the IPv6 prefix provided by your ISP.  |
| Prefix Length | Enter the bit number of the IPv6 subnet mask provided by your ISP.   |
| Apply         | Click <b>Apply</b> to save the changes.  |
| Cancel        | Click <b>Cancel</b> to begin configuring this screen afresh.   |

### 4.3.3 WAN Interface Type - Bridging

Select **Bridging** as the **WAN interface type** to open the following screen.

**Figure 12** Internet Access Setup - Bridging

The following table describes the labels in this screen.

**Table 7** Internet Access Setup - Bridging

| LABEL                  | DESCRIPTION   |
|------------------------|---|
| General                |   |
| WAN interface type     | Select <b>Bridging</b> as the method of encapsulation used by your ISP from the drop-down list box.   |
| Bridging LAN ports     | Select one or more LAN or wireless port(s) to bind with this WAN connection. Only the selected ports here can use this WAN connection.  |
| Service                |   |
| Service Description    | Enter a description to identify this WAN interface.   |
| 802.1Q VLAN ID         | This shows the VLAN ID assigned to traffic for this connection. Click <b>Edit</b> to open a screen where you can select a different VLAN ID. See <a href="#">Section 4.3.4 on page 37</a> for information on this screen. |
| 802.1P Priority Method | Select the 802.1P priority method to be assigned to traffic sent through this connection.   |
| WAN service type       | This field displays <b>Bridge</b> .   |

**Table 7** Internet Access Setup - Bridging (continued)

| LABEL  | DESCRIPTION  |
|--------|--|
| Apply  | Click <b>Apply</b> to save the changes.                      |
| Cancel | Click <b>Cancel</b> to begin configuring this screen afresh. |

### 4.3.4 802.1Q VLAN ID - Edit

Use this screen to configure the 802.1Q VLAN ID settings for a WAN interface. Click **Edit** next to **802.1Q VLAN ID** on an **Internet Access Setup** screen.

**Figure 13** 802.1Q VLAN ID - Edit

Vlan Edit

Select a provisioned vlan for wan1: 10

| Provisioned Vlan/Pbit      | Status  |
|----------------------------|---------|
| <input type="radio"/> NONE | disused |
| <input type="radio"/> None | disused |

Apply

The following table describes the labels in this screen.

**Table 8** 802.1Q VLAN ID - Edit

| LABEL                 | DESCRIPTION   |
|-----------------------|---|
| Provisioned VLAN/Pbit | The available VLAN/Pbit values provisioned by the OLT are listed in this column. You can select a VLAN/Pbit to be used by this WAN interface. |
| Status                | This column displays the current status of the respective VLAN/Pbit. It will display if it is in use by a WAN interface, or not in use.       |
| Apply                 | Click <b>Apply</b> to save the changes.   |

## 4.4 Default Gateway

Use this screen to configure your GPON Device's default gateway settings. Click **Network > WAN > Default Gateway**.

**Figure 14** Default Gateway

| WAN Interface                              | WAN Status |
|--|------------|
| <input checked="" type="radio"/> PPPoE_ETH | Down       |
| <input type="radio"/> wan2                 | Down       |

The following table describes the labels in this screen.

**Table 9** Default Gateway

| LABEL         | DESCRIPTION  |
|---------------|--|
| WAN Interface | Select a WAN interface you want to act as the default gateway.                                     |
| WAN Status    | This displays if the interface displayed in the WAN Interface column is <b>Up</b> or <b>Down</b> . |
| Apply         | Click <b>Apply</b> to save the changes.  |
| Cancel        | Click this to restore your previously saved settings.  |

## 5.1 Overview

This chapter describes how to configure LAN settings.

A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is a computer network limited to the immediate area, usually the same building or floor of a building. The LAN screens can help you configure a LAN DHCP server and manage IP addresses.

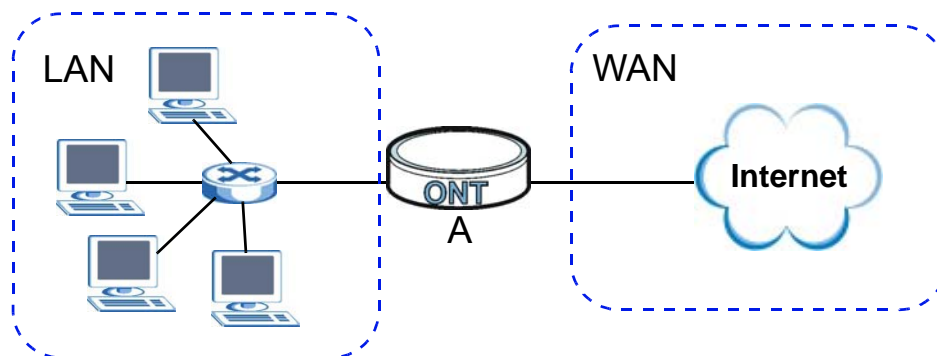
### 5.1.1 What You Need to Know

The following terms and concepts may help as you read through this chapter.

#### LANs, WANs and the GPON Device

The actual physical connection determines whether the GPON Device 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. The figure shows the GPON Device **A**.

**Figure 15** LAN and WAN IP Addresses



## 5.2 The IP and DHCP Screen

Click **Network > LAN** to open the **IP & DHCP** screen. Use this screen to set the Local Area Network IP address and subnet mask of your GPON Device.

**Figure 16** LAN & DHCP

The screenshot shows the 'IP & DHCP' configuration screen. It has three tabs: 'IP & DHCP' (selected), 'Client List', and 'Port Speed'. The main content is organized into three sections:

- LAN TCP/IP:** Contains two text input fields: 'IP Address' with the value '192.168.1.1' and 'IP Subnet Mask' with the value '255.255.255.0'.
- DHCP Setup:** Contains a dropdown menu for 'DHCP' set to 'Server', an 'IP Pool Starting Address' field with '192.168.1.2', a 'Pool Size' field with '253', a 'DHCP Lease Time' field with '14400' and 'seconds' next to it, and a checkbox for 'Enable DHCP Option 43' which is unchecked. Below it is a 'Vendor specific information' text input field.
- DNS Server:** Contains three rows for 'First DNS Server', 'Second DNS Server', and 'Third DNS Server'. Each row has a dropdown menu (set to 'DNS Relay', 'FromISP', and 'FromISP' respectively) and a text input field (with values '192.168.1.1', '0.0.0.0', and '0.0.0.0').

At the bottom of the screen are two buttons: 'Apply' and 'Cancel'.

The following table describes the fields in this screen.

**Table 10** IP & DHCP

| LABEL                    | DESCRIPTION  |
|--------------------------|--|
| LAN TCP/IP               |  |
| IP Address               | Enter the LAN IP address you want to assign to your GPON Device 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 GPON Device 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.   |
| DHCP Setup               |  |
| DHCP                     | Select whether to have the GPON Device act as a DHCP <b>Server</b> .<br><br>Select <b>Server</b> to have the GPON Device assign IP addresses and provide subnet mask, gateway, and DNS server information to the network. The GPON Device is the DHCP server for the network.<br><br>Otherwise, select <b>Disable</b> to not have the GPON Device provide any DHCP services. The DHCP server will be disabled. |
| IP Pool Starting Address | This field specifies the first of the contiguous addresses in the IP address pool.   |



**Table 10** IP & DHCP (continued)

| LABEL                 | DESCRIPTION  |
|-----------------------|--|
| Pool Size             | This field specifies the size, or count of the IP address pool.  |
| DHCP Lease Time       | This field specifies the lease time in seconds of the IP address assigned by the DHCP server.  |
| Enable DHCP option 43 | Select this and type the <b>Vender specific information</b> you want the GPON Device to add in the DHCP Offer packets. The information is used, for example, for configuring an ACS's (Auto Configuration Server) URL.   |
| DNS Server            |  |
| First DNS Server      | Select <b>From ISP</b> if the ISP dynamically assigns DNS server information (and the GPON Device's WAN IP address).   |
| Second DNS Server     | Select <b>UserDefined</b> if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right.   |
| Third DNS Server      | Select <b>DNS Relay</b> to have the GPON Device act as a DNS proxy only when the ISP uses IPCP DNS server extensions. The GPON Device's LAN IP address displays in the field to the right (read-only). The GPON Device tells the DHCP clients on the LAN that the GPON Device itself is the DNS server. When a computer on the LAN sends a DNS query to the GPON Device, the GPON Device forwards the query to the real DNS server learned through IPCP and relays the response back to the computer.<br><br>Select <b>None</b> if you do not want to configure DNS servers. You must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured. If you do not configure a DNS server, you must know the IP address of a computer in order to access it. |
| Apply                 | Click <b>Apply</b> to save your changes back to the GPON Device.   |
| Cancel                | Click <b>Cancel</b> to begin configuring this screen afresh.   |

## 5.3 Client List

Use this screen to look at the IP addresses currently assigned to DHCP clients and the IP addresses reserved for specific MAC addresses. Click **Network > LAN > Client List**.

This table allows you to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:AO:C5:00:00:02.

**Figure 17** Client List

| # | Status | HostName | Interface Type | IP Address  | MAC Address       | Remaining LeaseTime | Res...                   |
|---|--------|----------|----------------|-------------|-------------------|---------------------|--------------------------|
| 1 |        | pc01     | -              | 192.168.1.2 | 00:24:21:7c:f8:44 | 2:32:52             | <input type="checkbox"/> |

The following table describes the labels in this screen.

**Table 11** Client List

| LABEL                | DESCRIPTION  |
|----------------------|--|
| IP Address           | Enter the IP address that you want to assign to the computer on your LAN with the MAC address that you will also specify.  |
| MAC Address          | Enter the MAC address of a computer on your LAN.   |
| Add                  | Click <b>Add</b> to add a static DHCP entry.   |
| #                    | This is the index number of the static IP table entry (row).   |
| Status               | This field displays whether the client is connected to the GPON Device.  |
| Host Name            | This field displays the computer host name.  |
| Interface Type       | This field displays if the client is connected through ethernet or wireless.   |
| IP Address           | This field displays the IP address relative to the # field listed above.   |
| MAC Address          | The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation).<br><br>A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address. |
| Remaining Lease Time | This field displays the remaining time for this DHCP lease.  |
| Reserve              | Select the check box in the heading row to automatically select all check boxes or select the check box(es) in each entry to have the GPON Device always assign the selected entry(ies)'s IP address(es) to the corresponding MAC address(es) (and host name(s)). You can select up to 128 entries in this table.  |
| Apply                | Click <b>Apply</b> to save your changes back to the GPON Device.   |
| Cancel               | Click <b>Cancel</b> to begin configuring this screen afresh.   |
| Refresh              | Click <b>Refresh</b> to reload the DHCP table.   |

## 5.4 Port Speed

Use this screen to configure your GPON Device's LAN port speed settings. Click **Network > LAN > Port Speed**.

**Figure 18** Port Speed

The screenshot shows the 'LAN Port Speed Setting' configuration window. At the top, there are tabs for 'IP & DHCP', 'Client List', and 'Port Speed'. The main content area contains a table with the following data:

| LAN Port | Speed           | Duplex |
|----------|-----------------|--------|
| Port 1   | Autonegotiation | Auto   |
| Port 2   | Autonegotiation | Auto   |
| Port 3   | Autonegotiation | Auto   |
| Port 4   | Autonegotiation | Auto   |

Below the table, there are two buttons: 'Apply' and 'Cancel'.

The following table describes the labels in this screen.

**Table 12** Port Speed

| LABEL    | DESCRIPTION   |
|----------|---|
| LAN Port | This column displays the LAN port number.   |
| Speed    | Select <b>Autonegotiation</b> to have the GPON Device automatically use 1G, 100M or 10M depending on the device connected to the port. You can also manually select one of these speeds.          |
| Duplex   | Select <b>Auto</b> to have the GPON Device automatically use full or half duplex depending on the device connected to the port. You can also manually select a <b>Full</b> or <b>Half</b> duplex. |
| Apply    | Click <b>Apply</b> to save the changes.   |
| Cancel   | Click this to restore your previously saved settings.   |



# Wireless LAN

## 6.1 Overview

This chapter describes how to perform tasks related to setting up and optimizing your wireless network, including the following.

- Turning the wireless connection on or off.
- Configuring a name, wireless channel and security for the network.
- Using WiFi Protected Setup (WPS) to configure your wireless network.
- Setting up multiple wireless networks.
- Using a MAC (Media Access Control) address filter to restrict access to the wireless network.
- Performing other performance-related wireless tasks.

### 6.1.1 What You Need to Know About Wireless

#### Wireless Basics

“Wireless” is essentially radio communication. In the same way that walkie-talkie radios send and receive information over the airwaves, wireless networking devices exchange information with one another. A wireless networking device is just like a radio that lets your computer exchange information with radios attached to other computers. Like walkie-talkies, most wireless networking devices operate at radio frequency bands that are open to the public and do not require a license to use. However, wireless networking is different from that of most traditional radio communications in that there are a number of wireless networking standards available with different methods of data encryption.

#### SSID

Each network must have a name, referred to as the SSID - “Service Set Identifier”. The “service set” is the network, so the “service set identifier” is the network’s name. This helps you identify your wireless network when wireless networks’ coverage areas overlap and you have a variety of networks to choose from.

#### MAC Address Filter

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address consists of twelve hexadecimal characters (0-9, and A to F), and it is usually written in the following format: “0A:A0:00:BB:CC:DD”.

The MAC address filter controls access to the wireless network. You can use the MAC address of each wireless client to allow or deny access to the wireless network.

## Finding Out More

See [Section 6.9 on page 57](#) for advanced technical information on wireless networks.

### 6.1.2 Before You Start

Before you start using these screens, ask yourself the following questions. See [Section 6.1.1 on page 45](#) if some of the terms used here are not familiar to you.

- What wireless standards do the other wireless devices in your network support (IEEE 802.11g, for example)? What is the most appropriate standard to use?
- What security options do the other wireless devices in your network support (WPA-PSK, for example)? What is the strongest security option supported by all the devices in your network?
- Do the other wireless devices in your network support WPS (Wi-Fi Protected Setup)? If so, you can set up a well-secured network very easily.

Even if some of your devices support WPS and some do not, you can use WPS to set up your network and then add the non-WPS devices manually, although this is somewhat more complicated to do.

- What advanced options do you want to configure, if any? If you want to configure advanced options such as Quality of Service, ensure that you know precisely what you want to do. If you do not want to configure advanced options, leave them as they are.

## 6.2 The General Screen

Use this screen to configure the wireless settings of your GPON Device. Click **Network > Wireless LAN** to open the **General** screen.

**Figure 19** Network > Wireless LAN > General

The screenshot shows the configuration interface for the wireless LAN. The 'General' tab is selected. The 'Wireless Setup' section includes:
 

- Enable Wireless LAN
- Enable MultiSSID
- SSID: ZYXEL\_5A90
- Hide SSID
- Power Level: High
- Auto Channel Selection
- Channel Selection: Channel-13

 The 'Wireless Advanced Setup' section includes:
 

- 802.11 Mode: 802.11 B/G/N MHz

 A note is present: **NOTE:** If you set mode to 802.11 N mixed mode, it will not be 802.11 N mode when security is WEP / WPA / WPA-PSK. There are 'Apply' and 'Cancel' buttons at the bottom.

The following table describes the labels in this screen.

**Table 13** Network > Wireless LAN > General

| LABEL  | DESCRIPTION   |
|--|---|
| Wireless Setup   |   |
| Enable Wireless LAN  | Click the check box to activate wireless LAN.   |
| Enable MultiSSID   | Select this to enable Multi SSID (Service Set IDentity) to have the have the GPON Device broadcast several Basic Service Sets (BSSs) simultaneously.  |
| SSID   | <p>The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN.</p> <p><b>Note:</b> If you are configuring the GPON Device from a computer connected to the wireless LAN and you change the GPON Device's SSID or any wireless security settings, you will lose your wireless connection when you press <b>Apply</b> to confirm. You must then change the wireless settings of your computer to match the GPON Device's new settings.</p>   |
| Hide SSID  | Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.  |
| Power Level  | Select the wireless transmission power ( <b>High, Medium, Low</b> ) of the GPON Device. If there is a high density of wireless APs in an area, decrease the power level to reduce interference with other APs.  |
| Channel Selection  | Set the operating channel manually by selecting a channel from the <b>Channel Selection</b> list or use <b>Auto Channel Select</b> to have it automatically configured.   |
| Wireless Advanced Setup  |   |
| Click <b>Advanced</b> or <b>Basic</b> to display or hide this section. |   |
| 802.11 Mode  | <p>Select <b>802.11 B Only</b> to allow only IEEE 802.11b compliant WLAN devices to associate with the GPON Device.</p> <p>Select <b>802.11 G Only</b> to allow only IEEE 802.11g compliant WLAN devices to associate with the GPON Device.</p> <p>Select <b>802.11 N Only</b> to allow only IEEE 802.11n compliant WLAN devices to associate with the GPON Device.</p> <p>Select <b>802.11 B/G</b> to allow either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the GPON Device. The transmission rate of your GPON Device might be reduced.</p> <p>Select <b>802.11 B/G/N</b> to allow IEEE 802.11b, IEEE 802.11g or IEEE802.11n compliant WLAN devices to associate with the GPON Device. The transmission rate of your GPON Device might be reduced.</p> |
| Apply  | Click this to save your changes.  |
| Cancel   | Click this to restore your previously saved settings.   |

## 6.3 The Security Screen

Use this screen to configure the wireless security settings of your GPON Device. Click **Network > Wireless LAN > Security** to open the **Security** screen.

### 6.3.1 No Security

In the **Network > Wireless LAN > Security** screen, select **No Security** from the **Security Mode** list to allow wireless devices to communicate with the GPON Device without any data encryption or authentication.

Note: If you do not enable any wireless security on your GPON Device, your network is accessible to any wireless networking device that is within range.

**Figure 20** Network > Wireless LAN > Security: No Security

The following table describes the labels in this screen.

**Table 14** Network > Wireless LAN > Security: No Security

| LABEL         | DESCRIPTION  |
|---------------|--|
| SSID Select   | Select the SSID for which you are configuring security settings. |
| Security Mode | Choose <b>No Security</b> from the drop-down list box.           |

### 6.3.2 WEP Encryption

Use this screen to configure and enable WEP encryption. Click **Network > Wireless LAN > Security** to display the **Security** screen. Select **Static WEP** from the **Security Mode** list.



Note: WEP is extremely insecure. Its encryption can be broken by an attacker, using widely-available software. It is strongly recommended that you use a more effective security mechanism. Use the strongest security mechanism that all the wireless devices in your network support. For example, use WPA-PSK or WPA2-PSK if all your wireless devices support it. If your wireless devices support nothing stronger than WEP, use the highest encryption level available.

**Figure 21** Network > Wireless LAN > Security: Static WEP

General **Security** WPS WPS Station MAC Filter WMM Status Isolation

SSID Select

Security Mode

Authentication mode  Open  Shared

Passphrase

WEP Key

**NOTE:**  
 The different WEP key lengths configure different strength security, 40/64-bit, or 128-bit respectively. Your wireless client must match the security strength set on the router.  
 -Please type exactly 5, or 13 characters.  
 or  
 -Please type exactly 10, or 26 characters using only the numbers 0-9 and the letters 'a-f' or 'A-F'.

The following table describes the wireless LAN security labels in this screen.

**Table 15** Network > Wireless LAN > Security: Static WEP

| LABEL         | DESCRIPTION  |
|---------------|--|
| SSID Select   | Select the SSID for which you are configuring security settings.   |
| Security Mode | Choose <b>Static WEP</b> from the drop-down list box.  |
| Passphrase    | Enter a passphrase (up to 32 printable characters) and click <b>Generate</b> . The GPON Device automatically generates a WEP key.  |
| WEP Key       | The WEP key is used to encrypt data. Both the GPON Device and the wireless stations must use the same WEP key for data transmission.<br><br>If you want to manually set the WEP key, enter any 5 or 13 characters (ASCII string) or 10 or 26 hexadecimal characters ("0-9", "A-F") for a 64-bit or 128-bit WEP key respectively. |

### 6.3.3 WPA(2)-PSK

Use this screen to configure and enable WPA(2)-PSK authentication. Click **Network > Wireless LAN > Security** to display the **Security** screen. Select **WPA-PSK** or **WPA2-PSK** from the **Security Mode** list.

**Figure 22** Network > Wireless LAN > Security: WPA(2)-PSK

The screenshot shows the 'Security' tab of the configuration interface. The 'Security Mode' is set to 'WPA2-PSK'. The 'WPA Compatible' checkbox is unchecked. The 'Encrypt Mode' is set to 'AES'. The 'Pre-Shared Key' field contains 'WACJW3NE97'. The 'Group Key Update' is set to 'Enable' with a radio button selected. The 'Group Key Update Timer' is set to '3600 (seconds)'. There are 'Apply' and 'Cancel' buttons at the bottom right.

The following table describes the wireless LAN security labels in this screen.

**Table 16** Network > Wireless LAN > Security: WPA(2)-PSK

| LABEL                      | DESCRIPTION   |
|----------------------------|---|
| SSID Select                | Select the SSID for which you are configuring security settings.  |
| Security Mode              | Choose <b>WPA-PSK</b> or <b>WPA2-PSK</b> from the drop-down list box.   |
| WPA Compatible             | This check box is available only when you select <b>WPA2-PSK</b> in the <b>Security Mode</b> field.<br><br>Select the check box to have both WPA-PSK wireless clients be able to communicate with the GPON Device even when the GPON Device is using WPA2-PSK.  |
| Pre-Shared Key             | The encryption mechanisms used for <b>WPA(2)</b> and <b>WPA(2)-PSK</b> are the same. The only difference between the two is that <b>WPA(2)-PSK</b> uses a simple common password, instead of user-specific credentials.<br><br>Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols). |
| WPA Group Key Update Timer | The <b>Group Key Update Timer</b> is the rate at which the AP (if using <b>WPA(2)-PSK</b> key management) sends a new group key out to all clients. The re-keying process is the WPA(2) equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis.                                |

### 6.3.4 WPA(2)

Use this screen to configure and enable WPA(2) authentication. Click **Network > Wireless LAN > Security** to display the **Security** screen. Select **WPA or WPA2** from the **Security Mode** list.

**Figure 23** Network > Wireless LAN > Security: WPA(2)

The following table describes the wireless LAN security labels in this screen.

**Table 17** Network > Wireless LAN > Security: WPA(2)

| LABEL                  | DESCRIPTION  |
|------------------------|--|
| SSID Select            | Select the SSID for which you are configuring security settings.   |
| Security Mode          | Choose <b>WPA</b> or <b>WPA2</b> from the drop-down list box.  |
| WPA Compatible         | This check box is available only when you select <b>WPA2</b> in the <b>Security Mode</b> field.<br><br>Select the check box to have both WPA wireless clients be able to communicate with the GPON Device even when the GPON Device is using WPA2.   |
| Authentication Server  |  |
| IP Address             | Enter the IP address of the external authentication server in dotted decimal notation.   |
| Port Number            | Enter the port number of the external authentication server. The default port number is <b>1812</b> .<br><br>You need not change this value unless your network administrator instructs you to do so with additional information.  |
| Shared Secret          | Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the GPON Device.<br><br>The key must be the same on the external authentication server and your GPON Device. The key is not sent over the network.  |
| Group Key Update Timer | The <b>Group Key Update Timer</b> is the rate at which the <b>RADIUS</b> server (if using WPA(2) key management) sends a new group key out to all clients. The re-keying process is the WPA(2) equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. The GPON Device default is <b>1800</b> seconds (30 minutes). |

## 6.4 The WPS Screen

Use this screen to configure WiFi Protected Setup (WPS) on your GPON Device.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Set up each WPS connection between two devices. Both devices must support WPS.

Click **Network > Wireless LAN > WPS**. The following screen displays.

**Figure 24** Network > Wireless LAN > WPS

The following table describes the labels in this screen.

**Table 18** Network > Wireless LAN > WPS

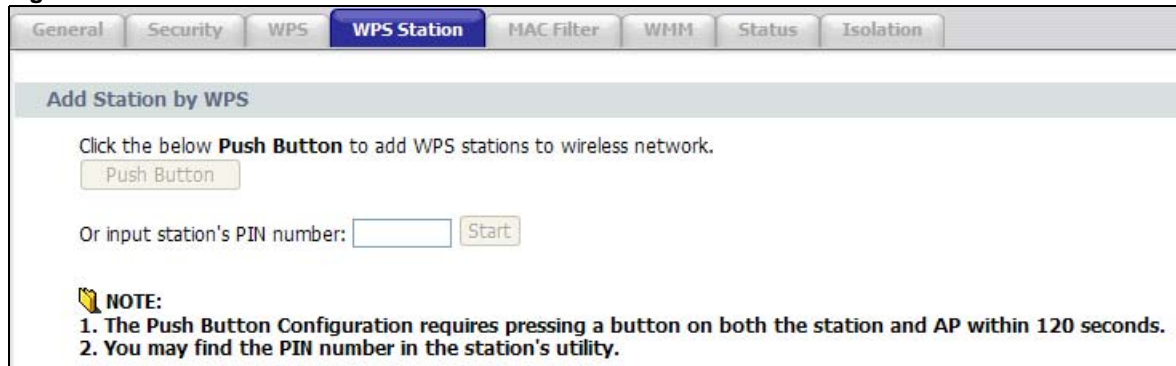
| LABEL      | DESCRIPTION   |
|------------|---|
| WPS Setup  |   |
| Enable WPS | Select the check box to activate WPS on the GPON Device.  |
| PIN Number | The PIN of the GPON Device is shown here. Enter this PIN in the configuration utility of the device you want to connect to using WPS.<br><br>The PIN is not necessary when you use WPS push-button method.<br><br>Click the <b>Generate</b> button to have the Device create a new PIN.   |
| WPS Status | This displays <b>Configured</b> when the GPON Device has connected to a wireless network using WPS or <b>Enable WPS</b> is selected and wireless or wireless security settings have been changed. The current wireless and wireless security settings also appear in the screen.<br><br>This displays <b>Unconfigured</b> if WPS is disabled and there is no wireless or wireless security changes on the GPON Device or you click <b>Release</b> to remove the configured wireless and wireless security settings. |
| Release    | This button is available when the WPS status is <b>Configured</b> .<br><br>Click this button to remove all configured wireless and wireless security settings for WPS connections on the GPON Device.   |
| Apply      | Click this to save your changes.  |
| Cancel     | Click this to restore your previously saved settings.   |

## 6.5 The WPS Station Screen

Use this screen to set up a WPS wireless network using either Push Button Configuration (PBC) or PIN Configuration.

Click **Network > Wireless LAN > WPS Station**. The following screen displays.

**Figure 25** Network > Wireless LAN > WPS Station



**Add Station by WPS**

Click the below **Push Button** to add WPS stations to wireless network.

Or input station's PIN number:

**NOTE:**

1. The **Push Button Configuration** requires pressing a button on both the station and AP within 120 seconds.
2. You may find the **PIN** number in the station's utility.

The following table describes the labels in this screen.

**Table 19** Network > Wireless LAN > WPS Station

| LABEL                         | DESCRIPTION  |
|-------------------------------|--|
| Push Button                   | Click this to add another WPS-enabled wireless device (within wireless range of the GPON Device) to your wireless network. This button may either be a physical button on the outside of device, or a menu button similar to the <b>Push Button</b> on this screen.<br><br>Note: You must press the other wireless device's WPS button within two minutes of pressing this button.                     |
| Or input station's PIN number | Enter the PIN of the device that you are setting up a WPS connection with and click <b>Start</b> to authenticate and add the wireless device to your wireless network.<br><br>You can find the PIN either on the outside of the device, or by checking the device's settings.<br><br>Note: You must also activate WPS on that device within two minutes to have it present its PIN to the GPON Device. |

### 6.5.1 MAC Filter

Use this screen to change your GPON Device's MAC filter settings.

Click **Network > Wireless LAN > MAC Filter**. The following screen displays.

**Figure 26** Network > Wireless LAN > MAC Filter

The following table describes the labels in this screen.

**Table 20** Network > Wireless LAN > MAC Filter

| LABEL             | DESCRIPTION   |
|-------------------|---|
| Filter Action     | Define the MAC filter action for all SSIDs' MAC addresses listed in the <b>MAC Address</b> table below.<br>Select <b>Deny</b> to block access to the GPON Device. MAC addresses not listed can access the GPON Device.<br>Select <b>Allow</b> to permit access to the GPON Device. MAC addresses not listed cannot access to the GPON Device. |
| SSID Select       | Select the SSID for which you want to configure MAC filter settings.  |
| Enable MAC Filter | Select the check box to enable MAC address filtering for the selected SSID.   |
| #                 | This is the index number of the MAC address.  |
| MAC Address       | Enter the MAC addresses of the wireless devices that are allowed access to the GPON Device in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.  |

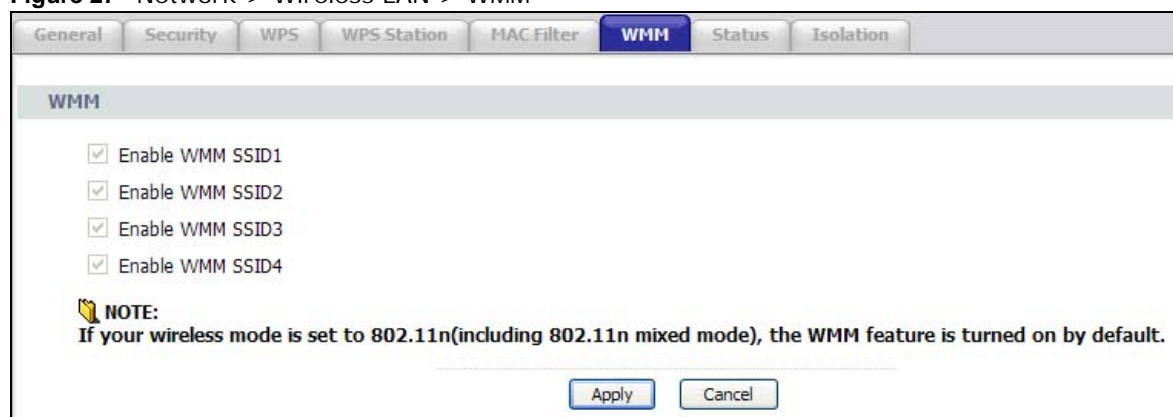
**Table 20** Network > Wireless LAN > MAC Filter

| LABEL  | DESCRIPTION   |
|--------|---|
| Apply  | Click this to save your changes.                      |
| Cancel | Click this to restore your previously saved settings. |

## 6.6 The WMM Screen

Use this screen to enable or disable Wi-Fi MultiMedia (WMM) wireless networks for multimedia applications.

Click **Network > Wireless LAN > WMM**. The following screen displays.

**Figure 27** Network > Wireless LAN > WMM

The following table describes the labels in this screen.

**Table 21** Network > Wireless LAN > WMM

| LABEL              | DESCRIPTION  |
|--------------------|--|
| Enable WMM SSID1-4 | This enables the Device to automatically give a service a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (Wifi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly. |
| Apply              | Click this to save your changes.   |
| Cancel             | Click this to restore your previously saved settings.  |

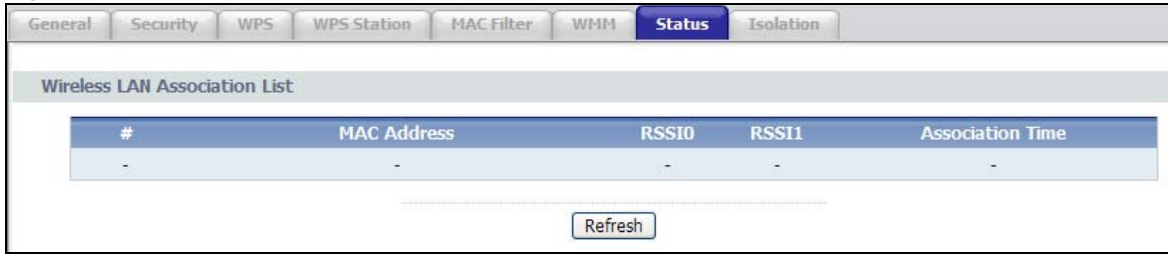
## 6.7 The Status Screen

Use this screen to view the status of wireless connections to the GPON Device.



Click **Network > Wireless LAN > Status**. The following screen displays.

**Figure 28** Network > Wireless LAN > Status



The following table describes the labels in this screen.

**Table 22** Network > Wireless LAN > Status

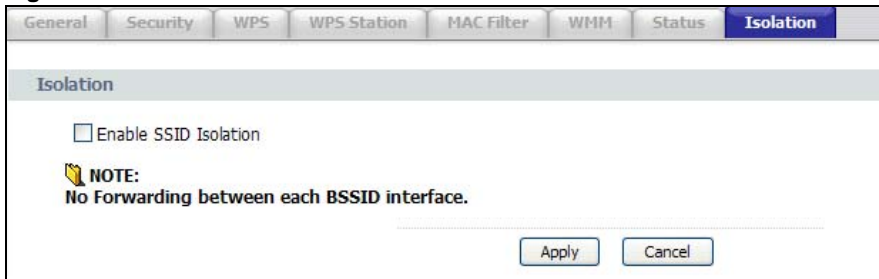
| LABEL            | DESCRIPTION   |
|------------------|---|
| #                | This field displays the index number of the wireless client.  |
| MAC Address      | This field displays the MAC address for the wireless adapter of the wireless client.  |
| RSSI0-1          | This field displays the Received Signal Strength Indication (RSSI), which is an overall measurement of radio signal strength. A higher RSSI level indicates a stronger signal. An RSSI displays for each of the GPON Device's antennae. |
| Association Time | This field displays the length of time the wireless client has been connected.  |
| Refresh          | Click this to update the information in the table.  |

## 6.8 The Isolation Screen

Use this screen to enable/disable SSID isolation.

Click **Network > Wireless LAN > Isolation**. The following screen displays.

**Figure 29** Network > Wireless LAN > Isolation



The following table describes the labels in this screen.

**Table 23** Network > Wireless LAN > Isolation

| LABEL                 | DESCRIPTION   |
|-----------------------|---|
| Enable SSID Isolation | Select this to keep the wireless clients in an SSID from directly communicating with wireless clients in other SSIDs through the GPON Device. |
| Apply                 | Click this to save your changes.  |
| Cancel                | Click this to restore your previously saved settings.   |



## 6.9 Wireless LAN Technical Reference

This section discusses wireless LANs in depth. For more information, see the appendix.

### 6.9.1 Wireless Network Overview

Wireless networks consist of wireless clients, access points and bridges.

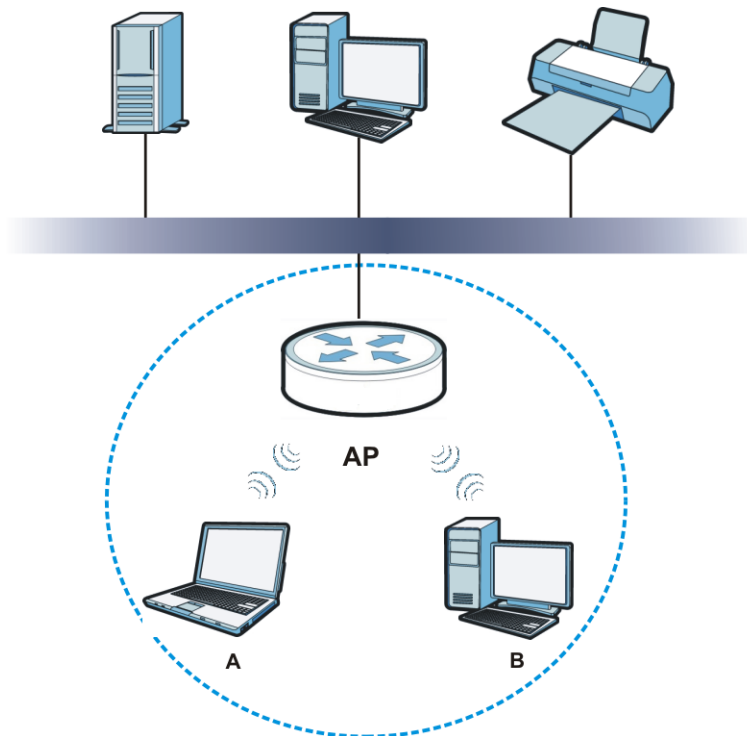
- A wireless client is a radio connected to a user's computer.
- An access point is a radio with a wired connection to a network, which can connect with numerous wireless clients and let them access the network.
- A bridge is a radio that relays communications between access points and wireless clients, extending a network's range.

Traditionally, a wireless network operates in one of two ways.

- An "infrastructure" type of network has one or more access points and one or more wireless clients. The wireless clients connect to the access points.
- An "ad-hoc" type of network is one in which there is no access point. Wireless clients connect to one another in order to exchange information.

The following figure provides an example of a wireless network.

**Figure 30** Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** use the access point (**AP**) to interact with the other devices (such as the printer) or with the Internet. Your GPON Device is the AP.

Every wireless network must follow these basic guidelines.

- Every device in the same wireless network must use the same SSID.  
The SSID is the name of the wireless network. It stands for Service Set IDentifier.
- If two wireless networks overlap, they should use a different channel.  
Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.
- Every device in the same wireless network must use security compatible with the AP.  
Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

## Radio Channels

In the radio spectrum, there are certain frequency bands allocated for unlicensed, civilian use. For the purposes of wireless networking, these bands are divided into numerous channels. This allows a variety of networks to exist in the same place without interfering with one another. When you create a network, you must select a channel to use.

Since the available unlicensed spectrum varies from one country to another, the number of available channels also varies.

## 6.9.2 Additional Wireless Terms

The following table describes some wireless network terms and acronyms used in the GPON Device's Web Configurator.

**Table 24** Additional Wireless Terms

| TERM                    | DESCRIPTION   |
|-------------------------|---|
| RTS/CTS Threshold       | In a wireless network which covers a large area, wireless devices are sometimes not aware of each other's presence. This may cause them to send information to the AP at the same time and result in information colliding and not getting through.<br><br>By setting this value lower than the default value, the wireless devices must sometimes get permission to send information to the GPON Device. The lower the value, the more often the devices must get permission.<br><br>If this value is greater than the fragmentation threshold value (see below), then wireless devices never have to get permission to send information to the GPON Device. |
| Preamble                | A preamble affects the timing in your wireless network. There are two preamble modes: long and short. If a device uses a different preamble mode than the GPON Device does, it cannot communicate with the GPON Device.   |
| Authentication          | The process of verifying whether a wireless device is allowed to use the wireless network.  |
| Fragmentation Threshold | A small fragmentation threshold is recommended for busy networks, while a larger threshold provides faster performance if the network is not very busy.   |

## 6.9.3 Wireless Security Overview

By their nature, radio communications are simple to intercept. For wireless data networks, this means that anyone within range of a wireless network without security can not only read the data passing over the airwaves, but also join the network. Once an unauthorized person has access to

the network, he or she can steal information or introduce malware (malicious software) intended to compromise the network. For these reasons, a variety of security systems have been developed to ensure that only authorized people can use a wireless data network, or understand the data carried on it.

These security standards do two things. First, they authenticate. This means that only people presenting the right credentials (often a username and password, or a “key” phrase) can access the network. Second, they encrypt. This means that the information sent over the air is encoded. Only people with the code key can understand the information, and only people who have been authenticated are given the code key.

These security standards vary in effectiveness. Some can be broken, such as the old Wired Equivalent Protocol (WEP). Using WEP is better than using no security at all, but it will not keep a determined attacker out. Other security standards are secure in themselves but can be broken if a user does not use them properly. For example, the WPA-PSK security standard is very secure if you use a long key which is difficult for an attacker’s software to guess - for example, a twenty-letter long string of apparently random numbers and letters - but it is not very secure if you use a short key which is very easy to guess - for example, a three-letter word from the dictionary.

Because of the damage that can be done by a malicious attacker, it’s not just people who have sensitive information on their network who should use security. Everybody who uses any wireless network should ensure that effective security is in place.

A good way to come up with effective security keys, passwords and so on is to use obscure information that you personally will easily remember, and to enter it in a way that appears random and does not include real words. For example, if your mother owns a 1970 Dodge Challenger and her favorite movie is Vanishing Point (which you know was made in 1971) you could use “70dodchal71vanpoi” as your security key.

The following sections introduce different types of wireless security you can set up in the wireless network.

### 6.9.3.1 SSID

Normally, the GPON Device acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the GPON Device does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized wireless devices to get the SSID. In addition, unauthorized wireless devices can still see the information that is sent in the wireless network.

### 6.9.3.2 MAC Address Filter

Every device that can use a wireless network has a unique identification number, called a MAC address.<sup>1</sup> A MAC address is usually written using twelve hexadecimal characters<sup>2</sup>; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each device in the wireless network, see the device’s User’s Guide or other documentation.

- 
1. Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.
  2. Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

You can use the MAC address filter to tell the GPON Device which devices are allowed or not allowed to use the wireless network. If a device is allowed to use the wireless network, it still has to have the correct information (SSID, channel, and security). If a device is not allowed to use the wireless network, it does not matter if it has the correct information.

This type of security does not protect the information that is sent in the wireless network. Furthermore, there are ways for unauthorized wireless devices to get the MAC address of an authorized device. Then, they can use that MAC address to use the wireless network.

### 6.9.3.3 User Authentication

Authentication is the process of verifying whether a wireless device is allowed to use the wireless network. You can make every user log in to the wireless network before using it. However, every device in the wireless network has to support IEEE 802.1x to do this.

For wireless networks, you can store the user names and passwords for each user in a RADIUS server. This is a server used in businesses more than in homes. If you do not have a RADIUS server, you cannot set up user names and passwords for your users.

Unauthorized wireless devices can still see the information that is sent in the wireless network, even if they cannot use the wireless network. Furthermore, there are ways for unauthorized wireless users to get a valid user name and password. Then, they can use that user name and password to use the wireless network.

### 6.9.3.4 Encryption

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

The types of encryption you can choose depend on the type of authentication. (See [Section 6.9.3.3 on page 60](#) for information about this.)

**Table 25** Types of Encryption for Each Type of Authentication

|                   | NO AUTHENTICATION | RADIUS SERVER |
|-------------------|-------------------|---------------|
| Weakest<br>↑<br>↓ | No Security       | WPA           |
|                   | Static WEP        |               |
|                   | WPA-PSK           |               |
| Strongest         | WPA2-PSK          | WPA2          |

For example, if the wireless network has a RADIUS server, you can choose **WPA** or **WPA2**. If users do not log in to the wireless network, you can choose no encryption, **Static WEP**, **WPA-PSK**, or **WPA2-PSK**.

Usually, you should set up the strongest encryption that every device in the wireless network supports. For example, suppose you have a wireless network with the GPON Device and you do not have a RADIUS server. Therefore, there is no authentication. Suppose the wireless network has two devices. Device A only supports WEP, and device B supports WEP and WPA-PSK. Therefore, you should set up **Static WEP** in the wireless network.

Note: It is recommended that wireless networks use **WPA-PSK**, **WPA**, or stronger encryption. The other types of encryption are better than none at all, but it is still possible for unauthorized wireless devices to figure out the original information pretty quickly.

When you select **WPA2** or **WPA2-PSK** in your GPON Device, you can also select an option (**WPA compatible**) to support WPA as well. In this case, if some of the devices support WPA and some support WPA2, you should set up **WPA2-PSK** or **WPA2** (depending on the type of wireless network login) and select the **WPA compatible** option in the GPON Device.

Many types of encryption use a key to protect the information in the wireless network. The longer the key, the stronger the encryption. Every device in the wireless network must have the same key.

## 6.9.4 Signal Problems

Because wireless networks are radio networks, their signals are subject to limitations of distance, interference and absorption.

Problems with distance occur when the two radios are too far apart. Problems with interference occur when other radio waves interrupt the data signal. Interference may come from other radio transmissions, such as military or air traffic control communications, or from machines that are coincidental emitters such as electric motors or microwaves. Problems with absorption occur when physical objects (such as thick walls) are between the two radios, muffling the signal.

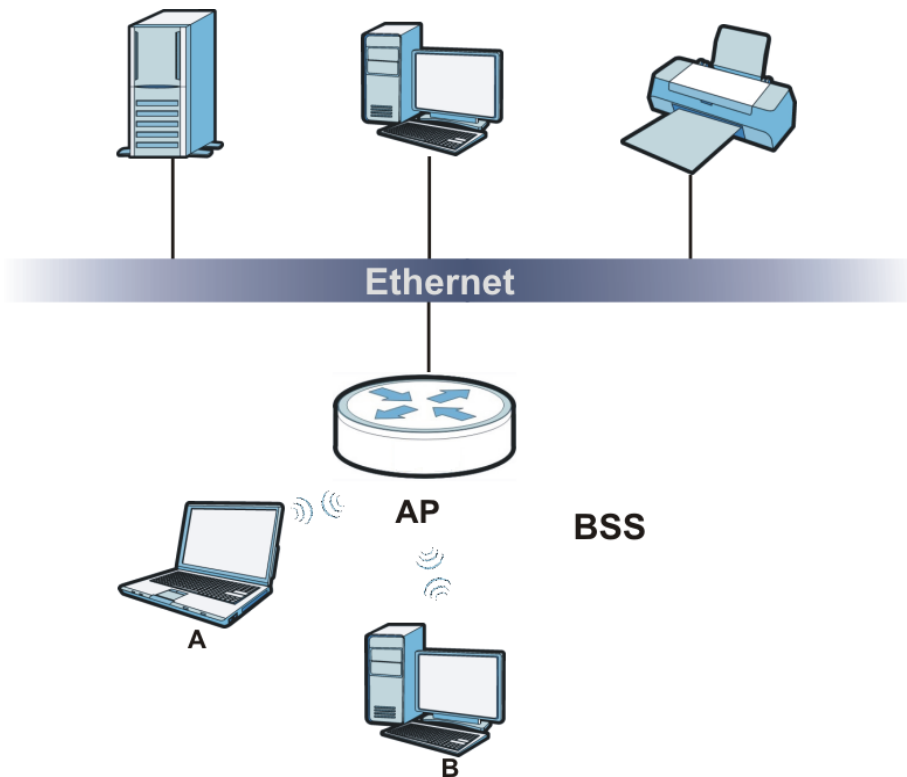
## 6.9.5 BSS

A Basic Service Set (BSS) exists when all communications between wireless stations or between a wireless station and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless stations in the BSS. When Intra-BSS traffic blocking is disabled, wireless station A and B can access the wired network and communicate with each other.

When Intra-BSS traffic blocking is enabled, wireless station A and B can still access the wired network but cannot communicate with each other.

**Figure 31** Basic Service set



## 6.9.6 MBSSID

Traditionally, you need to use different APs to configure different Basic Service Sets (BSSs). As well as the cost of buying extra APs, there is also the possibility of channel interference. The GPON Device's MBSSID (Multiple Basic Service Set IDentifier) function allows you to use one access point to provide several BSSs simultaneously. You can then assign varying QoS priorities and/or security modes to different SSIDs.

Wireless devices can use different BSSIDs to associate with the same AP.

### 6.9.6.1 Notes on Multiple BSSs

- A maximum of eight BSSs are allowed on one AP simultaneously.
- You must use different keys for different BSSs. If two wireless devices have different BSSIDs (they are in different BSSs), but have the same keys, they may hear each other's communications (but not communicate with each other).
- MBSSID should not replace but rather be used in conjunction with 802.1x security.

## 6.9.7 Wireless Distribution System (WDS)

The GPON Device can act as a wireless network bridge and establish WDS (Wireless Distribution System) links with other APs. You need to know the MAC addresses of the APs you want to link to.

Once the security settings of peer sides match one another, the connection between devices is made.

At the time of writing, WDS security is compatible with other ZyXEL access points only. Refer to your other access point's documentation for details.

The following figure illustrates how WDS link works between APs. Notebook computer **A** is a wireless client connecting to access point **AP 1**. **AP 1** has no wired Internet connection, but it can establish a WDS link with access point **AP 2**, which has a wired Internet connection. When **AP 1** has a WDS link with **AP 2**, the notebook computer can access the Internet through **AP 2**.

**Figure 32** WDS Link Example



## 6.9.8 WiFi Protected Setup (WPS)

Your GPON Device supports WiFi Protected Setup (WPS), which is an easy way to set up a secure wireless network. WPS is an industry standard specification, defined by the WiFi Alliance.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Each WPS connection works between two devices. Both devices must support WPS (check each device's documentation to make sure).

Depending on the devices you have, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (a unique Personal Identification Number that allows one device to authenticate the other) in each of the two devices. When WPS is activated on a device, it has two minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves.

### 6.9.8.1 Push Button Configuration

WPS Push Button Configuration (PBC) is initiated by pressing a button on each WPS-enabled device, and allowing them to connect automatically. You do not need to enter any information.

Not every WPS-enabled device has a physical WPS button. Some may have a WPS PBC button in their configuration utilities instead of or in addition to the physical button.

Take the following steps to set up WPS using the button.

- 1 Ensure that the two devices you want to set up are within wireless range of one another.
- 2 Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this - for the GPON Device, see [Section 6.5 on page 53](#)).
- 3 Press the button on one of the devices (it doesn't matter which). For the GPON Device you must press the WPS button for more than five seconds.

- 4 Within two minutes, press the button on the other device. The registrar sends the network name (SSID) and security key through an secure connection to the enrollee.

If you need to make sure that WPS worked, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

### 6.9.8.2 PIN Configuration

Each WPS-enabled device has its own PIN (Personal Identification Number). This may either be static (it cannot be changed) or dynamic (in some devices you can generate a new PIN by clicking on a button in the configuration interface).

Use the PIN method instead of the push-button configuration (PBC) method if you want to ensure that the connection is established between the devices you specify, not just the first two devices to activate WPS in range of each other. However, you need to log into the configuration interfaces of both devices to use the PIN method.

When you use the PIN method, you must enter the PIN from one device (usually the wireless client) into the second device (usually the Access Point or wireless router). Then, when WPS is activated on the first device, it presents its PIN to the second device. If the PIN matches, one device sends the network and security information to the other, allowing it to join the network.

Take the following steps to set up a WPS connection between an access point or wireless router (referred to here as the AP) and a client device using the PIN method.

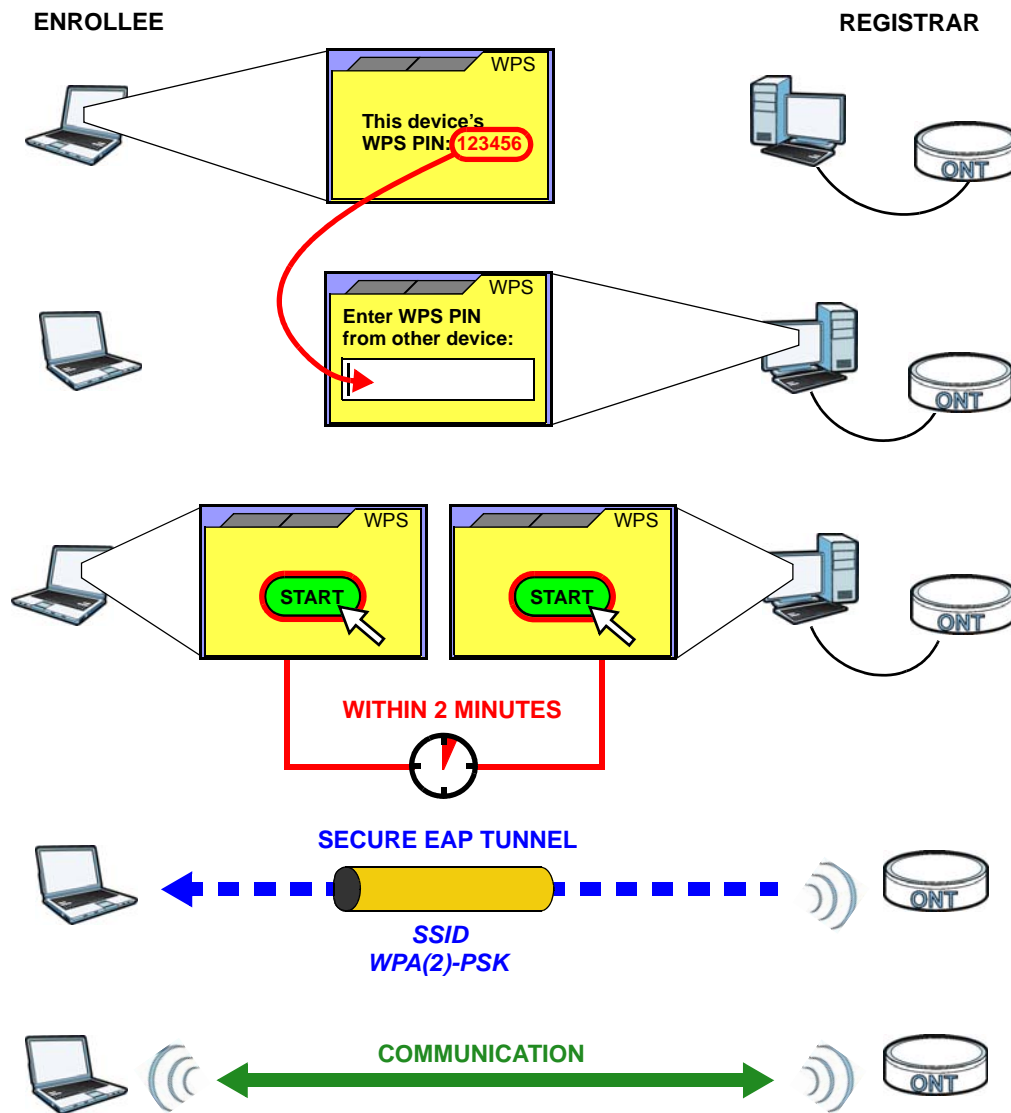
- 1 Ensure WPS is enabled on both devices.
- 2 Access the WPS section of the AP's configuration interface. See the device's User's Guide for how to do this.
- 3 Look for the client's WPS PIN; it will be displayed either on the device, or in the WPS section of the client's configuration interface (see the device's User's Guide for how to find the WPS PIN - for the GPON Device, see [Section 6.4 on page 52](#)).
- 4 Enter the client's PIN in the AP's configuration interface.
- 5 If the client device's configuration interface has an area for entering another device's PIN, you can either enter the client's PIN in the AP, or enter the AP's PIN in the client - it does not matter which.
- 6 Start WPS on both devices within two minutes.
- 7 Use the configuration utility to activate WPS, not the push-button on the device itself.
- 8 On a computer connected to the wireless client, try to connect to the Internet. If you can connect, WPS was successful.

If you cannot connect, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.



The following figure shows a WPS-enabled wireless client (installed in a notebook computer) connecting to the WPS-enabled AP via the PIN method.

**Figure 33** Example WPS Process: PIN Method

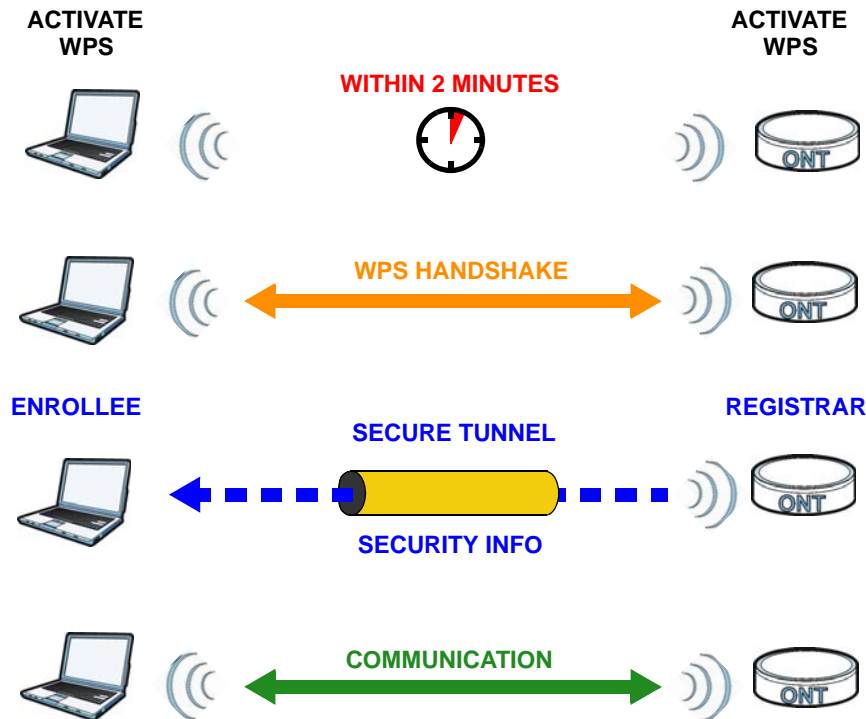


### 6.9.8.3 How WPS Works

When two WPS-enabled devices connect, each device must assume a specific role. One device acts as the registrar (the device that supplies network and security settings) and the other device acts as the enrollee (the device that receives network and security settings). The registrar creates a secure EAP (Extensible Authentication Protocol) tunnel and sends the network name (SSID) and the WPA-PSK or WPA2-PSK pre-shared key to the enrollee. Whether WPA-PSK or WPA2-PSK is used depends on the standards supported by the devices. If the registrar is already part of a network, it sends the existing information. If not, it generates the SSID and WPA(2)-PSK randomly.

The following figure shows a WPS-enabled client (installed in a notebook computer) connecting to a WPS-enabled access point.

**Figure 34** How WPS works



The roles of registrar and enrollee last only as long as the WPS setup process is active (two minutes). The next time you use WPS, a different device can be the registrar if necessary.

The WPS connection process is like a handshake; only two devices participate in each WPS transaction. If you want to add more devices you should repeat the process with one of the existing networked devices and the new device.

Note that the access point (AP) is not always the registrar, and the wireless client is not always the enrollee. All WPS-certified APs can be a registrar, and so can some WPS-enabled wireless clients.

By default, a WPS device is “unconfigured”. This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is unconfigured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled device has connected to another device using WPS, it becomes “configured”. A configured wireless client can still act as enrollee or registrar in subsequent WPS connections, but a configured access point can no longer act as enrollee. It will be the registrar in all subsequent WPS connections in which it is involved. If you want a configured AP to act as an enrollee, you must reset it to its factory defaults.

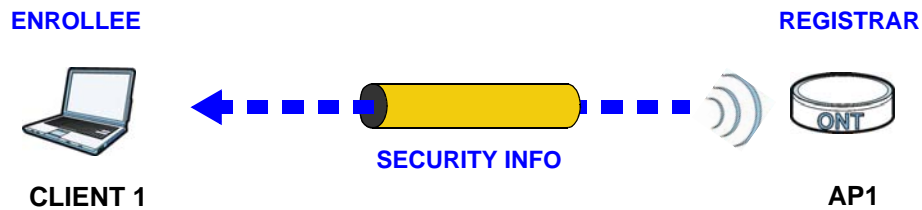
#### 6.9.8.4 Example WPS Network Setup

This section shows how security settings are distributed in an example WPS setup.

The following figure shows an example network. In step **1**, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1**

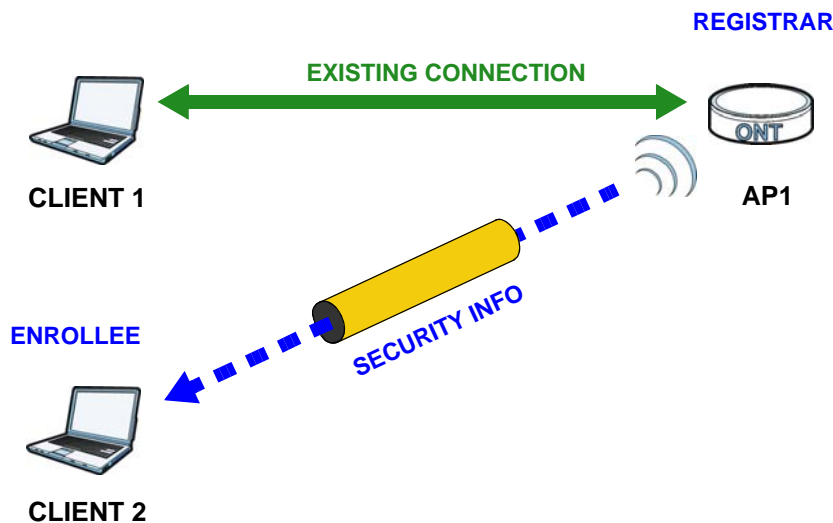
is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information to set up the network, since it is unconfigured and has no existing information.

**Figure 35** WPS: Example Network Step 1



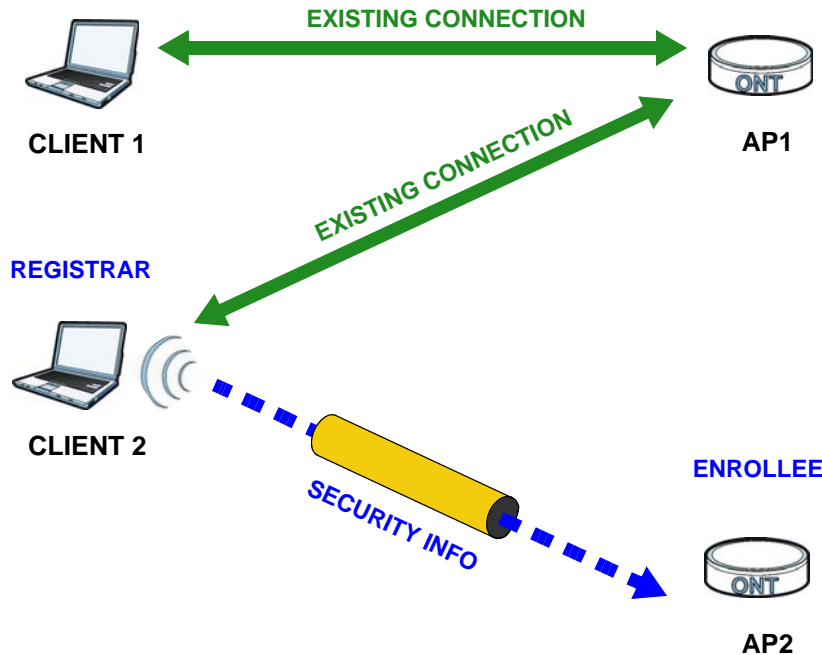
In step 2, you add another wireless client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the registrar, since it is configured (it already has security information for the network). **AP1** supplies the existing security information to **Client 2**.

**Figure 36** WPS: Example Network Step 2



In step 3, you add another access point (**AP2**) to your network. **AP2** is out of range of **AP1**, so you cannot use **AP1** for the WPS handshake with the new access point. However, you know that **Client 2** supports the registrar function, so you use it to perform the WPS handshake instead.

**Figure 37** WPS: Example Network Step 3



### 6.9.8.5 Limitations of WPS

WPS has some limitations of which you should be aware.

- WPS works in Infrastructure networks only (where an AP and a wireless client communicate). It does not work in Ad-Hoc networks (where there is no AP).
- When you use WPS, it works between two devices only. You cannot enroll multiple devices simultaneously, you must enroll one after the other.

For instance, if you have two enrollees and one registrar you must set up the first enrollee (by pressing the WPS button on the registrar and the first enrollee, for example), then check that it successfully enrolled, then set up the second device in the same way.

- WPS works only with other WPS-enabled devices. However, you can still add non-WPS devices to a network you already set up using WPS.

WPS works by automatically issuing a randomly-generated WPA-PSK or WPA2-PSK pre-shared key from the registrar device to the enrollee devices. Whether the network uses WPA-PSK or WPA2-PSK depends on the device. You can check the configuration interface of the registrar device to discover the key the network is using (if the device supports this feature). Then, you can enter the key into the non-WPS device and join the network as normal (the non-WPS device must also support WPA-PSK or WPA2-PSK).

- When you use the PBC method, there is a short period (from the moment you press the button on one device to the moment you press the button on the other device) when any WPS-enabled device could join the network. This is because the registrar has no way of identifying the “correct” enrollee, and cannot differentiate between your enrollee and a rogue device. This is a possible way for a hacker to gain access to a network.

You can easily check to see if this has happened. WPS works between only two devices simultaneously, so if another device has enrolled your device will be unable to enroll, and will not have access to the network. If this happens, open the access point’s configuration interface and look at the list of associated clients (usually displayed by MAC address). It does not matter if the access point is the WPS registrar, the enrollee, or was not involved in the WPS handshake; a rogue device must still associate with the access point to gain access to the network. Check the MAC addresses of your wireless clients (usually printed on a label on the bottom of the device). If there is an unknown MAC address you can remove it or reset the AP.



## 7.1 Overview

This chapter discusses how to configure NAT on the GPON Device.

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.

### 7.1.1 What You Need to Know

The following terms and concepts may help as you read through this chapter.

#### 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 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. Note that the IP address (either local or global) of an outside host is never changed.

#### NAT Definitions

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

Global/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 global 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 global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) 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. |

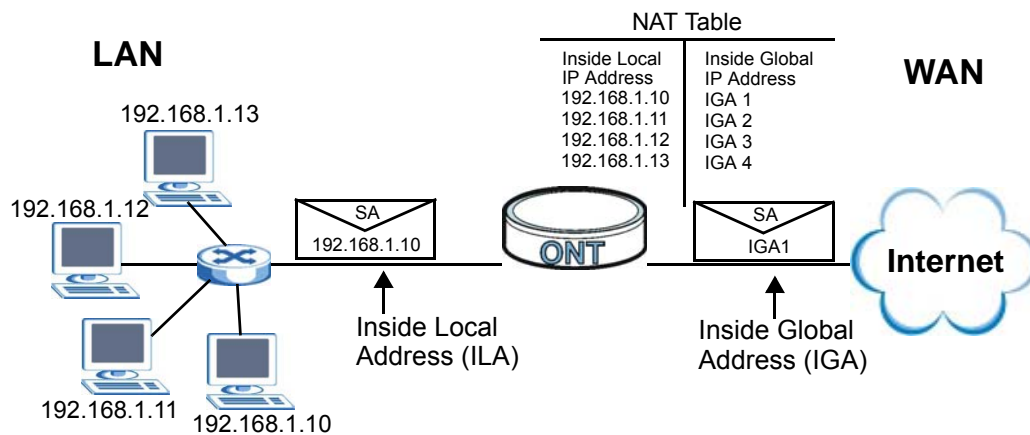
**Table 26** NAT Definitions (continued)

| ITEM   | DESCRIPTION   |
|--------|---|
| Local  | This refers to the packet address (source or destination) as the packet travels on the LAN. |
| Global | 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 global) of an outside host.

## How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA 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 in each packet and then forwards it to the Internet. The GPON Device keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

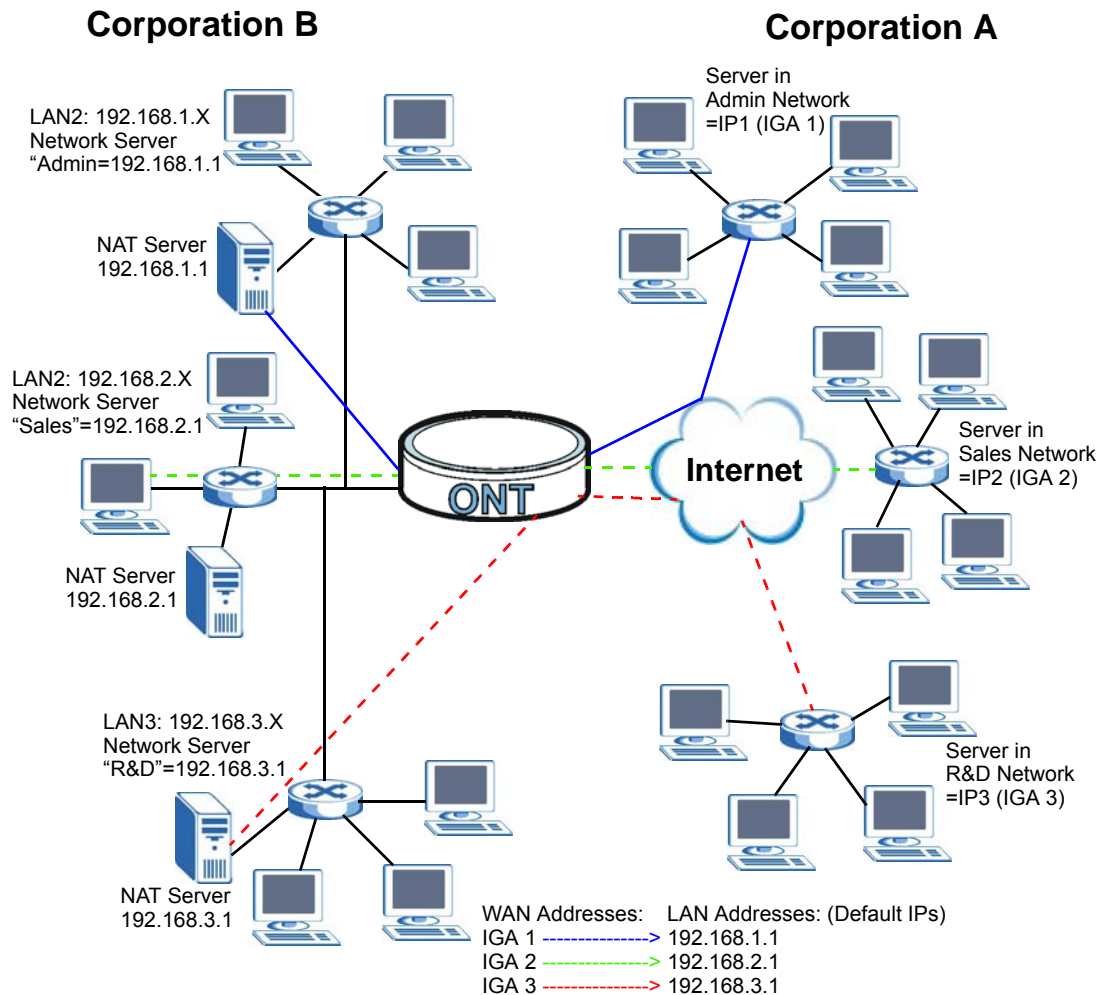
**Figure 38** How NAT Works



## NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP alias) behind the GPON Device can communicate with three distinct WAN networks.

**Figure 39** NAT Application With IP Alias



## 7.2 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.

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.

Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. The 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 the ISP.

The basic rules of port forwarding are:

- If NAT is enabled, you must configure a port forwarding rule if you want traffic on the WAN to find computers on the LAN.
- A port forwarding rule can only forward TCP and UDP traffic.
- If NAT is disabled, the GPON Device will route packets based on the information in the NAT routing table.

## 7.2.1 Default Server IP Address

You can assign a default server IP address to which the GPON Device can forward traffic for all protocols, such as TCP, UDP, ICMP (ping), ESP, and so on, that do not match an existing port forwarding rule.

Note: If you do not assign a **Default Server** IP address, the GPON Device discards all packets received for ports that are not specified in a port forwarding rule or in the remote management setup.

## 7.2.2 Port Forwarding: Services and Port Numbers

Use the **Port Forwarding** screen to forward incoming service requests to the server(s) on your local network.

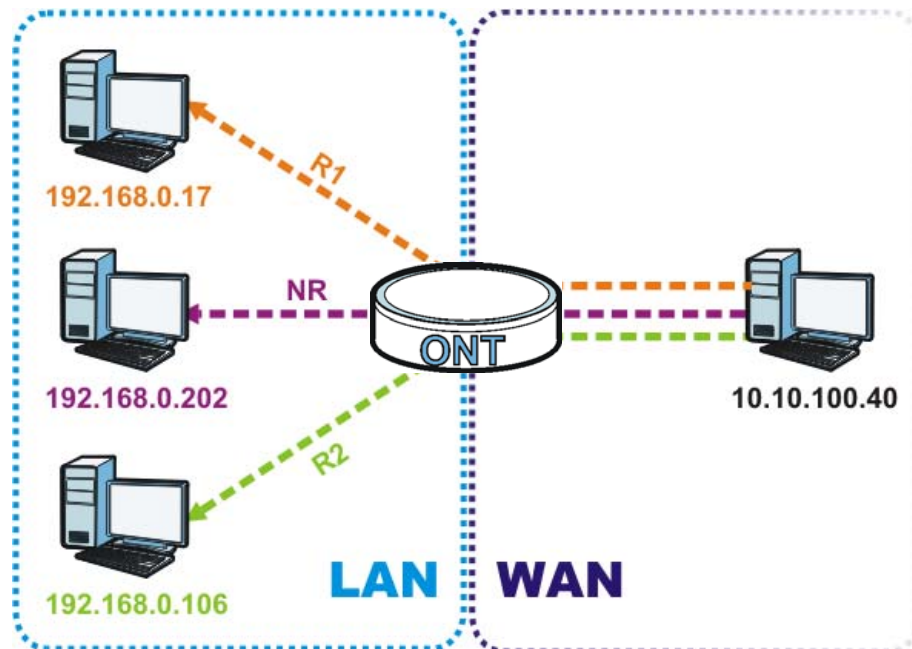
## 7.2.3 Pinging a Device Behind NAT From the WAN (Example)

Imagine that you want to ping a device on the LAN behind your GPON Device from a remote location on the WAN while NAT is enabled.

You cannot create a port forwarding rule for ping because ping uses the ICMP protocol; port forwarding can only handle the TCP and UDP protocols.

However, you can assign one of the computers on your LAN with a default server IP address. This allows it to receive all traffic that is not specifically routed by a port forwarding rule, including ping.

**Figure 40** Pinging a Device Behind NAT



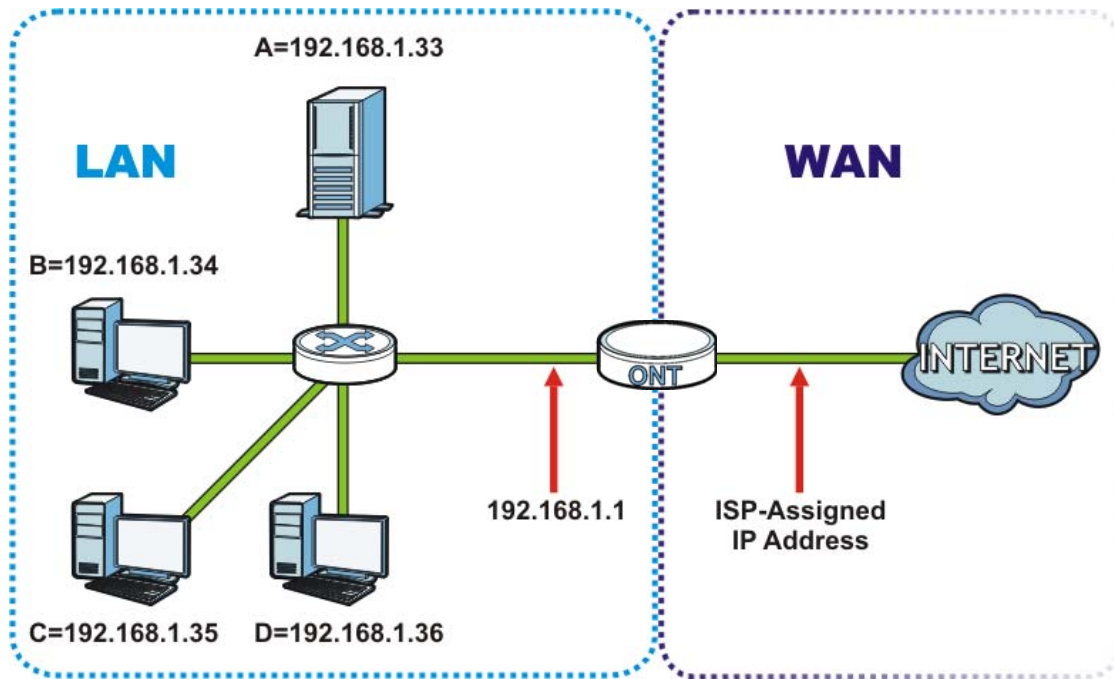
If you want to assign the IP address 192.168.0.202 as your “catch-all” category, for example, you can designate it as the GPON Device’s default server. Port forwarding rule 1 (**R1**) sends all TCP/UDP traffic that matches the rule to 192.168.0.17 while port forwarding rule 2 (**R2**) sends TCP/UDP traffic that matches to 192.168.0.106. Everything else (**NR**) goes to 192.168.0.202. For details on assigning a default server IP address, see [Section 7.3 on page 76](#).

## 7.2.4 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 41** Multiple Servers Behind NAT Example



## 7.3 Configuring Port Forwarding

Click **Network > NAT > Port Forwarding** to open the following screen.

**Figure 42** Port Forwarding

The screenshot shows the 'Port Forwarding' configuration interface. At the top, there's a 'Default Server Setup' section with a 'Default Server Address' input field. Below that is the 'Port Forwarding' section, which includes a 'Service Name' dropdown menu currently set to 'HTTP', and a 'Server IP Address' input field with an 'Add' button next to it. A table with the following columns is displayed: '#', 'Active', 'Service Name', 'Start Port', 'End Port', 'Protocol', 'Server IP Address', and 'Modify'. Below the table, there is a 'NOTE' icon and text: 'NOTE: You may also need to create a [Firewall](#) rule'. At the bottom of the screen, there are 'Apply' and 'Cancel' buttons.

The following table describes the fields in this screen.

**Table 27** Port Forwarding

| LABEL                  | DESCRIPTION   |
|------------------------|---|
| Default Server Setup   |   |
| Default Server Address | Enter an internal IP address to which the GPON Device forwards incoming packets if the GPON Device cannot find a rule matched in the table below. Leave this field blank to have the GPON Device not forward packets that do not match a rule.  |
| Port Forwarding        |   |
| Service Name           | Select a pre-defined service ( <b>HTTP, FTP, TELNET, HTTPS</b> ) from the drop-down list box. The pre-defined service port number(s) and protocol will display in the <b>Start port, End port</b> and <b>Protocol</b> fields of the table below after you click <b>Add</b> .<br><br>Otherwise, select <b>User Define</b> to open the <b>Rule Setup</b> screen where you can manually enter the port number(s) and select the IP protocol. |
| Server IP Address      | Enter the IP address of the server for the specified service.   |
| Add                    | Click this button to add a rule to the table below.   |
| #                      | This is the rule index number (read-only).  |
| Active                 | This field indicates whether the rule is active or not.<br><br>Clear the check box to disable the rule. Select the check box to enable it.  |
| Service Name           | This field displays the name of the service used by the packets for this virtual server.  |
| Start Port             | This is the first internal or external port number that identifies a service.   |
| End Port               | This is the last internal or external port number that identifies a service.  |
| Protocol               | This field displays the corresponding IP protocol ( <b>TCP, UDP</b> or <b>TCP/UDP</b> ) for the service.  |
| Server IP Address      | This field displays the inside IP address of the server.  |
| Modify                 | Click the <b>Edit</b> icon to go to the screen where you can edit the port forwarding rule.<br><br>Click the <b>Remove</b> icon to delete an existing port forwarding rule. Note that subsequent rules move up by one when you take this action.  |
| Apply                  | Click <b>Apply</b> to save your changes back to the GPON Device.  |
| Reset                  | Click <b>Reset</b> to return to the previous configuration.   |

## 7.3.1 Port Forwarding Edit

Use this screen to modify a port forwarding rule. Click an **Edit** icon next to a pre-defined port forwarding service rule in the **Network > NAT > Port Forwarding** screen to open the following screen.

**Figure 43** Port Forwarding Edit

The screenshot shows a web-based configuration interface for editing a port forwarding rule. The title is 'Rule Setup'. There is a checked checkbox for 'Active'. Below it are several input fields: 'Service Name' with the value 'HTTP', 'Start Port' with '80', 'End Port' which is empty, 'Server IP Address' with '192.168.10.100', and 'Protocol' with a dropdown menu showing 'TCP'. At the bottom right, there are three buttons: 'Back', 'Apply', and 'Cancel'.

The following table describes the fields in this screen.

**Table 28** Port Forwarding Edit

| LABEL             | DESCRIPTION  |
|-------------------|--|
| Active            | This field indicates whether the rule is active or not.<br>Clear the check box to disable the rule. Select the check box to enable it.                             |
| Service Name      | This field displays the name of the service used by the packets for this virtual server.   |
| Start Port        | This is the first internal or external port number that identifies a service.  |
| End Port          | This is the last internal or external port number that identifies a service.   |
| Server IP Address | This field displays the inside IP address of the server.   |
| Protocol          | This field displays the corresponding IP protocol ( <b>TCP</b> , <b>UDP</b> or <b>TCP/UDP</b> ) for the service. Select another protocol if you want to change it. |
| Back              | Click <b>Back</b> to ignore unsaved changes you made on this screen and go back to the previous screen.  |
| Apply             | Click <b>Apply</b> to save your changes back to the GPON Device.   |
| Cancel            | Click <b>Cancel</b> to return to the previous configuration.   |

# Quality of Service (QoS)

## 8.1 Overview

Use the **QoS** screen to set up your GPON Device to use QoS for traffic management.

## 8.2 The QoS General Screen

Use this screen to enable or disable QoS and configure the QoS settings for services.

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

**Figure 44** Network > QoS > General

| Service Configuration |         |        |
|-----------------------|---------|--------|
| VoIP/SIP              | DSCP 46 | Pbit 2 |
| VoIP/RTP              | DSCP 46 | Pbit 2 |
| RTSP                  | DSCP 26 | Pbit 5 |
| IGMP                  | DSCP 24 | Pbit 4 |
| TR069                 | DSCP 48 | Pbit 6 |

The following table describes the labels in this screen.

**Table 29** Network > QoS > General

| LABEL                 | DESCRIPTION  |
|-----------------------|--|
| Enable QoS            | Use this field to turn on QoS to improve your network performance.   |
| Service Configuration | Use this section to configure the DSCP and priority bit settings for VoIP/SIP, VoIP/RTP, RTSP, IGMP, and TR069 traffic.            |
| DSCP                  | This is the DSCP number (0~63) added to traffic of this classifier.  |
| Pbit                  | This is the IEEE 802.1p priority level (0~7) assigned to traffic of this classifier. The lower the number the higher the priority. |
| Apply                 | Click this to save your changes.   |
| Cancel                | Click this to restore your previously saved settings.  |





## 9.1 Introduction

This chapter provides background information on VoIP and SIP and explains how to configure your device's voice settings.

VoIP is the sending of voice signals over Internet Protocol. This allows you to make phone calls and send faxes over the Internet at a fraction of the cost of using the traditional circuit-switched telephone network. You can also use servers to run telephone service applications like PBX services and voice mail. Internet Telephony Service Provider (ITSP) companies provide VoIP service.

Circuit-switched telephone networks require 64 kilobits per second (Kbps) in each direction to handle a telephone call. VoIP can use advanced voice coding techniques with compression to reduce the required bandwidth.

### 9.1.1 What You Need to Know

The following terms and concepts may help as you read through this chapter.

#### SIP

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet.

SIP signaling is separate from the media for which it handles sessions. The media that is exchanged during the session can use a different path from that of the signaling. SIP handles telephone calls and can interface with traditional circuit-switched telephone networks.

#### SIP Identities

A SIP account uses an identity (sometimes referred to as a SIP address). A complete SIP identity is called a SIP URI (Uniform Resource Identifier). A SIP account's URI identifies the SIP account in a way similar to the way an e-mail address identifies an e-mail account. The format of a SIP identity is SIP-Number@SIP-Service-Domain.

#### SIP Number

The SIP number is the part of the SIP URI that comes before the "@" symbol. A SIP number can use letters like in an e-mail address (johndoe@your-ITSP.com for example) or numbers like a telephone number (1122334455@VoIP-provider.com for example).

## SIP Service Domain

The SIP service domain of the VoIP service provider is the domain name in a SIP URI. For example, if the SIP address is [1122334455@VoIP-provider.com](mailto:1122334455@VoIP-provider.com), then “VoIP-provider.com” is the SIP service domain.

## 9.2 SIP Service Provider

Use this screen to maintain basic information about each SIP account. Your VoIP service provider (the company that lets you make phone calls over the Internet) should provide this. You can also enable and disable each SIP account. To access this screen, click **VoIP > SIP**.

**Figure 45** VoIP > SIP > SIP Service Provider

| SIP Service Provider                           |                                     | SIP Account |
|--|-------------------------------------|-------------|
| <b>General</b>                                 |                                     |             |
| <input type="checkbox"/> Active                |                                     |             |
| SIP Service Provider Name                      | Undefined                           |             |
| SIP Server Address                             | ChangeMe                            |             |
| SIP Server Port                                | 5060 (1025-65535)                   |             |
| REGISTER Server Address                        | ChangeMe                            |             |
| REGISTER Server Port                           | 5060 (1025-65535)                   |             |
| SIP Service Domain                             | ChangeMe                            |             |
| SIP Local Port                                 | 5060 (1025-65535)                   |             |
| <b>Timer Setting</b>                           |                                     |             |
| Registration Period                            | 3600 (20-65535) second, 0 = Disable |             |
| Register Expires                               | 3600 (90-65535) second              |             |
| Register Re-send Timer                         | 180 (1-65535) second                |             |
| Session Expires                                | 180 (90-3600) second                |             |
| Min-SE   | 90 (90-1800) second                 |             |
| <b>DSCP Tag</b>                                |                                     |             |
| SIP DSCP Priority Setting                      | 46 (0-63)                           |             |
| RTP DSCP Priority Setting                      | 46 (0-63)                           |             |
| <b>RTP Port Range</b>                          |                                     |             |
| Start Port                                     | 50000 (1025-65535)                  |             |
| End Port                                       | 65535 (1025-65535)                  |             |
| <b>Outbound Proxy</b>                          |                                     |             |
| <input type="checkbox"/> Active Outbound Proxy |                                     |             |
| Outbound Proxy Address                         |                                     |             |
| Outbound Proxy Port                            | 5060 (1025-65535)                   |             |

**SIP Transport Method**

SIP Transport Method Selection: UDP

---

**Dialing Interval**

Dialing Interval Selection: 3 Second

---

**DTMF Method**

DTMF Method Selection: RFC 2833

---

**FAX Option**

G.711 FaxPassthrough
  T.38 Fax Relay

---

**Dialing Plan**

| Dialing Plan | Rule List    | Comment |
|--------------|--------------|---------|
| X.T          | Rule[1]:Pass |         |

Current Length:3/256      Amount:1      [? Help](#)

| Rules                 | Symbol      | Description  |
|-----------------------|-------------|--|
| Multiple Rule         |             | Multiple rules use " " to separate each other.   |
| Any one numeric digit | x           | Allow user to input any numeric digit (0~9), one 'x' means one digit   |
| A subset of keys      | [ ]         | Allow user to input a range of digits, eg: [ 1-3] or [148]   |
| Repeat                | .           | Allow user to input a repeatable digit (above 0 times). Eg: (12.) means 1, 12, 122, 1222 is allowable.                       |
| Append                | <:123>      | Append '123' digits in the place of the rule.  |
| Remove                | <123:>      | Remove '123' digits in the place of the rule.  |
| Replace               | <123:456>   | Replace '123' digits to '456' digits in the place of the rule.   |
| Block                 | !           | Type '!' at the end of the rule, to block the number which matches the rule.   |
| Immediate Dial        | @           | Type '@' at the end of the rule, once the input dial number reaches and matches the rule, dial out immediately./td>          |
| Gateway               | =gw0=,=gw3= | Type one of these at the end of the rule, the number matches the rule will be transfer to the gateway (0: FXS port; 3: SIP). |

[Basic](#)

Each field is described in the following table.

**Table 30** VoIP > SIP > SIP Service Provider

| LABEL                 | DESCRIPTION   |
|-----------------------|---|
| General               |   |
| Active                | Select this to use this service provider profile for SIP phone calls.   |
| Service Provider Name | Enter your SIP service provider's name, using up to 64 printable English-keyboard characters.   |
| SIP Server Address    | Enter the IP address or domain name of the SIP server provided by your VoIP service provider. You can use up to 256 printable English keyboard characters. It does not matter whether the SIP server is a proxy, redirect or register server. |

**Table 30** VoIP > SIP > SIP Service Provider (continued)

| LABEL                     | DESCRIPTION   |
|---------------------------|---|
| SIP Server Port           | Enter the SIP server's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.  |
| REGISTER Server Address   | Enter the IP address or domain name of the SIP register server, if your VoIP service provider gave you one. Otherwise, enter the same address you entered in the <b>SIP Server Address</b> field. You can use up to 256 printable English keyboard characters.  |
| REGISTER Server Port      | Enter the SIP register server's listening port number, if your VoIP service provider gave you one. Otherwise, enter the same port number you entered in the <b>SIP Server Port</b> field.   |
| SIP Service Domain        | Enter the SIP service domain name or the SIP server's IP address. In the full SIP URI, this is the part after the @ symbol. You can use up to 256 printable English keyboard characters.  |
| SIP Local Port            | Enter the GPON Device's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.   |
| Apply                     | Click this to save your changes.  |
| Cancel                    | Click this to exit the screen without saving any changes.   |
| Advanced Setup            | Click this to display the following advanced settings for this SIP account.   |
| Timer Settings            |   |
| Registration Period       | Enter the number of seconds allocated for the GPON Device to register with a SIP service.   |
| Register Expires          | Enter the number of seconds your SIP account is registered with the SIP register server before the registration is downgraded to 'inactive' and all SIP functions for the account are blocked. The GPON Device automatically tries to re-register your SIP account when one-half of this time has passed. (The SIP register server might have a different expiration, which takes priority over this setting.)  |
| Register Re-send Timer    | Enter the number of seconds the GPON Device waits before it tries again to register the SIP account, if the first try failed or if there is no response.  |
| Session Expires           | Enter the number of seconds the SIP server waits for a 'keep alive' signal from the GPON Device before disconnecting the call. The keep alive signal is periodically sent from the GPON Device during a call as long as the connection between it and the server remains constant. If interference happens somewhere along the line, or the connection is unexpectedly terminated, then the SIP server uses this setting as a timer to automatically disconnect the call.   |
| Min-SE                    | Enter the minimum number of seconds the GPON Device accepts for a session expiration time when it receives a request to start a SIP session. If the request has a shorter time, the GPON Device rejects it.   |
| DSCP Tag                  |   |
| SIP DSCP Priority Setting | Enter the DSCP (DiffServ Code Point) number for SIP message transmissions. The Device creates Class of Service (CoS) priority tags with this number to SIP traffic that it transmits.   |
| RTP DSCP Priority Setting | Enter the DSCP (DiffServ Code Point) number for RTP voice transmissions. The Device creates Class of Service (CoS) priority tags with this number to RTP traffic that it transmits.   |
| RTP Port Range            |   |
| Start Port<br>End Port    | <p>Enter the listening port number(s) for RTP traffic, if your VoIP service provider gave you this information. Otherwise, keep the default values.</p> <p>To enter one port number, enter the port number in the <b>Start Port</b> and <b>End Port</b> fields.</p> <p>To enter a range of ports,</p> <ul style="list-style-type: none"> <li>• enter the port number at the beginning of the range in the <b>Start Port</b> field</li> <li>• enter the port number at the end of the range in the <b>End Port</b> field.</li> </ul> |

**Table 30** VoIP > SIP > SIP Service Provider (continued)

| LABEL                          | DESCRIPTION  |
|--------------------------------|--|
| Outbound Proxy                 |  |
| Active Outbound Proxy          | Select this if the service provider has a SIP outbound server to handle voice calls. This allows the GPON Device to work with any type of NAT router and eliminates the need for STUN or a SIP ALG. Turn off any SIP ALG on a NAT router in front of the GPON Device to keep it from retranslating the IP address (since this is already handled by the outbound proxy server.   |
| Outbound Proxy Address         | Enter the IP address or domain name of the SIP outbound proxy server.  |
| Outbound Proxy Port            | Enter the outbound proxy server's listening port, if your VoIP service provider gave you one. Otherwise, keep the default value.   |
| SIP Transport Method           |  |
| SIP Transport Method Selection | Select the transport layer protocol <b>UDP</b> or <b>TCP</b> (usually UDP) used for SIP.   |
| Dialing Interval Selection     |  |
| Dialing Interval Selection     | Select the number of seconds the GPON Device waits before placing a dialed call.   |
| DTMF Method                    |  |
| DTMF Method Selection          | Control how the GPON Device handles the alphanumeric keypad tones. You should use the same mode the VoIP service provider uses.<br><br><b>RFC 2833</b> - send the DTMF tones in RTP packets<br><br><b>InBand</b> - send the DTMF tones in the voice data stream. This method works best when you are using a codec that does not use compression. Codecs that use compression can distort the tones.<br><br><b>SIP INFO</b> - send the DTMF tones in SIP messages. |
| Fax Option                     |  |
| G.711 FaxPassthrough           | Select this option to send and receive fax messages over the network or Internet using VoIP. By encoding fax data as audio data, faxes may be susceptible to packet loss and other errors. However, as this standard is considerably older than T.38, it is more compatible with older or obsolete systems.  |
| T.38 Fax Relay                 | Select this option to send and received fax messages over the network or Internet using IP. This is the standard fax transmission protocol for sending faxes over networks rather than phone lines.  |
| Dialing Plan                   |  |
| Dialing Plan                   | Create dialing plan rules here. See <a href="#">Section 9.2.1 on page 85</a> for more information. Click the <b>Help</b> icon to display guidelines for creating dialing plan rules.   |
| Apply                          | Click this to save your changes.   |
| Cancel                         | Click this to exit the screen without saving any changes.  |
| Basic                          | Click this to hide the advanced settings on this screen.   |

## 9.2.1 Dial Plan

A dial plan defines the dialing patterns, such as the length and range of the digits for a telephone number. It also includes country codes, access codes, area codes, local numbers, long distance numbers or international call prefixes. For example, the dial plan ([2-9]xxxxxx) does not allow a local number which begins with 1 or 0.

Without a dial plan, users have to manually enter the whole callee's number and wait for the specified dialing interval to time out or press a terminator key (usually the pound key on the phone keypad) before the GPON Device makes the call.

The GPON Device initializes a call when the dialed number matches any one of the rules in the dial plan. Dial plan rules follow these conventions:

- Rules are separated by the | (bar) symbol.
- "x" stands for a wildcard and can be any digit from 0 to 9.
- A subset of keys is in a square bracket []. Ranges are allowed.  
For example, [359] means a number matching this rule can be 3, 5 or 9. [26-8\*] means a number matching this rule can be 2, 6, 7, 8 or \*.
- The dot "." appended to a digit allows the digit to be ignored or repeated multiple times. Any digit (0-9, \*, #) after the dot will be ignored.  
For example, (01.) means a number matching this rule can be 0, 01, 0111, 01111, and so on.
- <dialed-number:translated-number> indicates the number after the colon replaces the number before the colon in an angle bracket <>. For example,  
(<:1212> xxxxxxx) means the GPON Device automatically prefixes the translated-number "1212" to the number you dialed before making the call. This can be used for local calls in the US.  
(<9:> xxx xxxxxxx) means the GPON Device automatically removes the specified prefix "9" from the number you dialed before making the call. This is always used for making outside calls from an office.  
(xx<123:456>xxxx) means the GPON Device automatically translates "123" to "456" in the number you dialed before making the call.
- Calls with a number followed by the exclamation mark "!" will be dropped.
- Calls with a number followed by the termination character "@" will be made immediately. Any digit (0-9, \*, #) after the @ character will be ignored.
- Gateway: Type "=gw0=" or "=gw3=" at the end of the rule. If the number matches the call will be transferred to a gateway (0: FXS port; 3: SIP).

In this example dial plan (0 | [49]11 | 1 [2-9]xx xxxxxxx | 1 947 xxxxxxx !), you can dial "0" to call the local operator, call 411 or 911, or make a long distance call with an area code starting from 2 to 9 in the US. The calls with the area code 947 will be dropped.

# 9.3 SIP Account

Use this screen to set up your basic SIP account information. Click **VoIP > SIP > SIP Account** to display this screen.

Figure 46 VoIP > SIP > SIP Account

The screenshot shows the 'SIP Account' configuration page. At the top, there are two tabs: 'SIP Service Provider' and 'SIP Account'. The page is organized into several sections:

- Service Provider Selection:** A dropdown menu for 'Service Provider Selection' with the value '[1]:Undefined'.
- SIP Account Selection:** A dropdown menu for 'SIP Account Selection' with the value '[1][Line:1]:ChangeMe'.
- General:** A checked checkbox for 'Active SIP Account' and a text input field for 'Number' containing 'ChangeMe'.
- Authentication:** Text input fields for 'User Name' (containing 'ChangeMe') and 'Password' (masked with dots).
- Voice Feature:** Dropdown menus for 'Speaking Volume' and 'Listening Volume' (both set to 'Middle'), and checkboxes for 'Active G.168 (Echo Cancellation)' (checked) and 'Active VAD' (unchecked).
- Audio Codecs Setting:** A table for codec configuration. The 'Disabled Codec (s)' column is empty. The 'Priority Enabled Codec(s)' column contains a list: G.711ALaw(64.0 Kbps), G.711MuLaw(64.0 Kbps), G.723.1(6.3 Kbps), and G.726(32.0 Kbps). There are 'UP' and 'DOWN' buttons to the right of the list.
- CAUTION:** A warning icon and text: 'G.711 FaxPassthrough is not workable when "Enabled codec(s)" without G.711ALaw and G.711 MuLaw.'
- Call Feature:** Checked checkboxes for 'Active Caller ID', 'Active Call Transfer', and 'Active Call Waiting'. A text input field for 'Call Waiting Reject Timer' is set to '20' with '(0-180)Second' next to it.

Active Unconditional Forward 
  
 Active Busy Forward 
  
 Active No Answer Forward 
  
 No Answer Ring Count  (3-180)second(s)

**⚠ CAUTION:**  
 If you enable [Unconditional Forward], [Busy Forward] and [No Answer] will be ignored.

[Basic](#)

Each field is described in the following table.

**Table 31** VoIP > SIP > SIP Account

| LABEL                            | DESCRIPTION   |
|----------------------------------|---|
| SIP Account Selection            |   |
| SIP Account Selection            | Select the SIP account you want to see in this screen. If you change this field, the screen automatically refreshes.  |
| General                          |   |
| Active SIP Account               | Select this if you want the GPON Device to use this account. Clear it if you do not want the GPON Device to use this account.   |
| Number                           | Enter your SIP number. In the full SIP URI, this is the part before the @ symbol. You can use up to 32 printable English keyboard characters.   |
| Authentication                   |   |
| User Name                        | Enter the user name for registering this SIP account, exactly as it was given to you. You can use up to 128 printable English keyboard characters.  |
| Password                         | Enter the user name for registering this SIP account, exactly as it was given to you. You can use up to 128 printable English keyboard characters.  |
| Apply                            | Click this to save your changes.  |
| Cancel                           | Click this to exit the screen without saving any changes.   |
| Advanced                         | Click this to display the following advanced settings for this SIP account.   |
| Voice Feature                    |   |
| Speaking Volume                  | Adjust the incoming ( <b>Listening</b> ) volume. The options are: <ul style="list-style-type: none"> <li>• <b>Minimum</b>, which decreases the volume</li> <li>• <b>Middle</b>, which makes no adjustments</li> <li>• <b>Maximum</b>, which increases the volume</li> </ul> |
| Listening Volume                 | Adjust the outgoing ( <b>Speaking</b> ) volume. The options are: <ul style="list-style-type: none"> <li>• <b>Minimum</b>, which decreases the volume</li> <li>• <b>Middle</b>, which makes no adjustments</li> <li>• <b>Maximum</b>, which increases the volume</li> </ul>  |
| Active G.168 (Echo Cancellation) | Select this if you want to eliminate the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.   |
| Active VAD                       | Select this if the GPON Device should transmit smaller packets when you are not speaking. This reduces the bandwidth used.  |



**Table 31** VoIP > SIP > SIP Account (continued)

| LABEL                        | DESCRIPTION  |
|------------------------------|--|
| Audio Codecs Setting         |  |
| Disabled Codec(s)            | This field lists codecs the GPON Device will not use. Click the left facing arrow to move codecs from the Enabled Codec(s) list to this list. Or click the right facing arrow to move a codec to the Enabled Codec(s) list.  |
| Priority                     | This field lists the priority in which the GPON Device will attempt to use each codec in the Enabled Codec(s) list.  |
| Enabled Codec(s)             | <p>This field lists the codecs the GPON Device will use. Click the left facing arrow to move codecs to the Disabled Codec(s) list. Or click the right facing arrow to move a codec to the Enabled Codec(s) list. Codec options include:</p> <p>G.711 provides high voice quality but requires more bandwidth (64 kbps).</p> <ul style="list-style-type: none"> <li>• <b>G.711ALaw</b> is typically used in Europe.</li> <li>• <b>G.711MuLaw</b> is typically used in North America and Japan.</li> </ul> <p>The GPON Device must use the same codec as the peer. When two SIP devices start a SIP session, they must agree on a codec.</p> |
| Call Feature                 |  |
| Active Caller ID             | Select this to enable call transfer on the GPON Device. This allows you to transfer an incoming call (that you have answered) to another phone.  |
| Active Call Transfer         | Select this to enable call transfer on the GPON Device. This allows you to transfer an incoming call (that you have answered) to another phone.  |
| Active Call Waiting          | Select this to enable call waiting on the GPON Device. This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.  |
| Call Waiting Reject Timer    | Enter the number of seconds for call waiting to stay engaged before disconnecting the caller.  |
| Active Unconditional Forward | Select this, then enter a phone number to which incoming calls are forwarded.  |
| Active Busy Forward          | <p>Select this if you want the GPON Device to forward incoming calls to the specified phone number if the phone port is busy.</p> <p>Specify the phone number in the field on the right.</p> <p>If you have call waiting, the incoming call is forwarded to the specified phone number if you reject or ignore the second incoming call.</p>   |
| Active No Answer Forward     | Select this, then enter a phone number to which calls are forwarded when the phone is not answered.  |
| No Answer Ring Count         | Enter the number of rings the GPON Device waits before forwarding unanswered calls.  |
| Apply                        | Click this to save your changes.   |
| Cancel                       | Click this to exit the screen without saving any changes.  |
| Basic                        | Click this to hide the advanced settings on this screen.   |

## 9.4 Analog Phone

Use this screen to link the GPON Device's analog phone ports with one or more SIP accounts to handle outgoing and incoming calls. Click **VoIP > Phone**. The following screen displays.

**Figure 47** VoIP > Phone > Analog Phone

Each field is described in the following table.

**Table 32** VoIP > Phone > Analog Phone

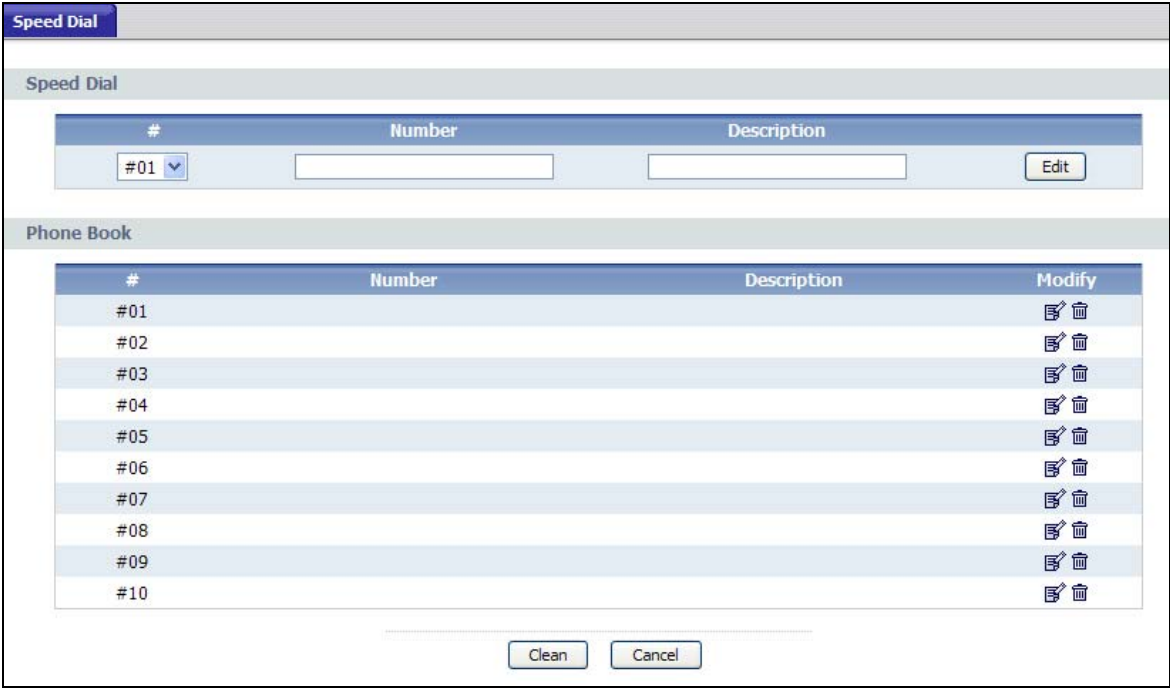
| LABEL                | DESCRIPTION  |
|----------------------|--|
| Phone Port Selection |  |
| Phone Port Selection | Select a phone port to configure on this screen.   |
| Phone to SIP Account |  |
| SIP Account          | This indicates the SIP account mapping to the phone port for both incoming and outgoing calls. Select <b>None</b> to disable the phone port so you cannot receive and make calls through the phone port. |
| SIP Number           | This indicates the SIP account's number. You can click it to open the <b>SIP Account</b> screen, where you can change it.  |
| Service Provider     | This indicates the service provider used by this SIP account.  |
| SIP Account Status   | This indicates whether the account is active or not. Click it to open the <b>SIP Account</b> screen, where you can change the status.  |
| Apply                | Click this to save your changes.   |
| Cancel               | Click this to exit the screen without saving any changes.  |

## 9.5 Speed Dial

Speed dial provides shortcuts for dialing frequently used (VoIP) phone numbers. You also have to create speed-dial entries if you want to call SIP numbers that contain letters. Once you have configured a speed dial rule, you can use a shortcut (the speed dial number, #01 for example) on your phone's keypad to call the phone number.

Use this screen to add, edit, or remove speed-dial numbers for outgoing calls. To access this screen, click **VoIP > Phone Book > Speed Dial**.

**Figure 48** VoIP > Phone Book > Speed Dial



Each field is described in the following table.

**Table 33** VoIP > Phone Book > Speed Dial

| LABEL                 | DESCRIPTION  |
|-----------------------|--|
| Speed Dial            | Use this section to create or edit speed-dial entries.   |
| #                     | Select the speed-dial number you want to use for this phone number.  |
| Number                | Enter the SIP number you want the GPON Device to call when you dial the speed-dial number.   |
| Description           | Enter a description for this speed dial number. You can use up to 128 alphanumeric characters.   |
| Add                   | Click this to use the information in the <b>Speed Dial</b> section to update the <b>Speed Dial Phone Book</b> section.   |
| Speed Dial Phone Book | Use this section to look at all the speed-dial entries and to erase them.  |
| #                     | This field displays the speed-dial number you should dial to use this entry.   |
| Number                | This field displays the SIP number the GPON Device calls when you dial the speed-dial number.  |
| Destination           | This field is blank, if the speed-dial entry uses one of your SIP accounts. Otherwise, this field shows the IP address or domain name of the SIP server or other party. (This field corresponds with the <b>Type</b> field in the <b>Speed Dial</b> section.)              |
| Modify                | Use this field to edit or erase the speed-dial entry.<br><br>Click the <b>Edit</b> icon to copy the information for this speed-dial entry into the <b>Speed Dial</b> section, where you can change it.<br><br>Click the <b>Remove</b> icon to erase this speed-dial entry. |

**Table 33** VoIP > Phone Book > Speed Dial (continued)

| LABEL  | DESCRIPTION   |
|--------|---|
| Clear  | Click this to erase all the speed-dial entries.                       |
| Cancel | Click this to set every field in this screen to its last-saved value. |

# Phone Usage

## 10.1 Overview

This chapter describes how to use a phone connected to your GPON Device for basic tasks.

Note: Not all service providers support all features.

## 10.2 Dialing a Telephone Number

The **PHONE** LED turns green when your SIP account is registered. Dial a SIP number like "12345" on your phone's keypad.

Use speed dial entries (see [Section 9.5 on page 90](#)) for SIP numbers that use letters. Dial the speed dial entry on your telephone's keypad.

Use your VoIP service provider's dialing plan to call regular telephone numbers.

## 10.3 Using Speed Dial

After configuring the speed dial entry and adding it to the phonebook, press the speed dial entry's key combination on your phone's keypad.

## 10.4 Phone Services Overview

Supplementary services such as call hold, call waiting, call transfer, etc. are generally available from your VoIP service provider. The GPON Device supports the following services:

- Call Hold
- Call Waiting
- Making a Second Call
- Call Transfer
- Call Forwarding
- Internal Calls

Note: To take full advantage of the supplementary phone services available through the GPON Device's phone port, you may need to subscribe to the services from your VoIP service provider.

## 10.4.1 The Flash Key

Flashing means to press the hook for a short period of time (a few hundred milliseconds) before releasing it. On newer telephones, there should be a "flash" key (button) that generates the signal electronically. If the flash key is not available, you can tap (press and immediately release) the hook by hand to achieve the same effect. However, using the flash key is preferred since the timing is much more precise. With manual tapping, if the duration is too long, it may be interpreted as hanging up by the GPON Device.

You can invoke all the supplementary services by using the flash key.

## 10.4.2 Supplementary Phone Services

This section describes how to use supplementary phone services. Commands for supplementary services are listed in the table below.

After pressing the flash key, if you do not issue the sub-command before the default sub-command timeout (2 seconds) expires or issue an invalid sub-command, the current operation will be aborted.

**Table 34** Flash Key Commands

| COMMAND | SUB-COMMAND | DESCRIPTION  |
|---------|-------------|--|
| Flash   |             | Put a current call on hold to place a second call.<br>Switch back to the call (if there is no second call).  |
| Flash   | 0           | Drop the call presently on hold or reject an incoming call which is waiting for answer.  |
| Flash   | 1           | Disconnect the current phone connection and answer the first incoming call.  |
| Flash   | 2           | 1. Switch back and forth between two calls.<br>2. Put a current call on hold to answer an on-hold call or the second incoming call.<br>3. Separate the current three-way conference call into two individual calls (one is on-line, the other is on hold). |
| Flash   | 3           | Merge the first call which was placed on hold into the second call and start a 3-way conference call.  |

### 10.4.2.1 Call Hold

Call hold allows you to put a call (**A**) on hold by pressing the flash key.

If you have another call, press the flash key and then "1" or "2" (depending on whether it is the first or second incoming call) to switch back and forth between caller **A** and **B** by putting either one on hold.

Press the flash key and then "0" to disconnect the call presently on hold and keep the current call on line.

If you hang up the phone but a caller is still on hold, there will be a remind ring.

### 10.4.2.2 Call Waiting

This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.

If there is a second call to a telephone number, you will hear a call waiting tone. Take one of the following actions.

- Pick up the second call and put the first call on hold.  
Press the flash key and then press "2".
- Reject the second call.  
Press the flash key and then press "0".
- Put the second call on hold and answer the first call.  
Press the flash key and then "1". You can then press the flash key and then "2" to answer the second call but put the first call on hold.

### 10.4.2.3 Call Transfer

Do the following to transfer an incoming call (that you have answered) to another phone.

- 1 Answer the incoming call.
- 2 Press the flash key to put the caller on hold.
- 3 Dial the number of the intended callee.
- 4 Hang up the call after it starts ringing or is answered. The GPON Device puts the caller through to the callee.





# USB Services

## 11.1 Overview

The GPON Device has two USB ports used to share files via a USB memory stick or a USB hard drive.

### 11.1.1 What You Can Do in this Chapter

- Use the **File Sharing** screen to configure a file-sharing server ([Section 11.2 on page 98](#)).
- Use the **Account Management** screen to configure user accounts ([Section 11.3 on page 99](#)).

### 11.1.2 What You Need To Know

The following terms and concepts may help as you read this chapter.

#### Workgroup name

This is the name given to a set of computers that are connected on a network and share resources such as a printer or files. Windows automatically assigns the workgroup name when you set up a network.

#### Shares

When settings are set to default, each USB device connected to the GPON Device is given a folder, called a “share”. If a USB hard drive connected to the GPON Device has more than one partition, then each partition will be allocated a share. You can also configure a “share” to be a sub-folder or file on the USB device.

#### File Systems

A file system is a way of storing and organizing files on your hard drive and storage device. Often different operating systems such as Windows or Linux have different file systems. The file sharing feature on your GPON Device supports File Allocation Table (FAT) and FAT32.

#### Common Internet File System

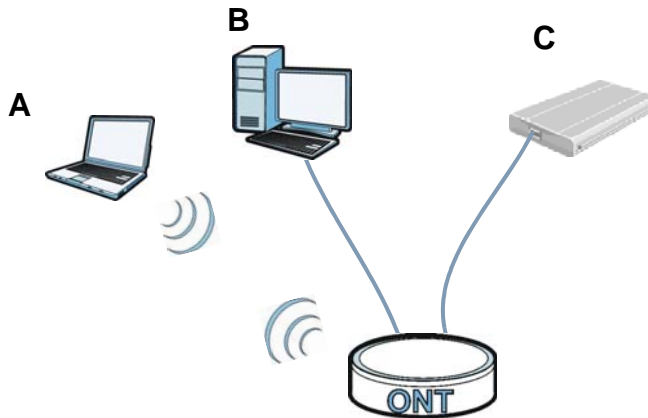
The GPON Device uses Common Internet File System (CIFS) protocol for its file sharing functions. CIFS compatible computers can access the USB file storage devices connected to the GPON Device. CIFS protocol is supported on Microsoft Windows, Linux Samba and other operating systems (refer to your systems specifications for CIFS compatibility).

## 11.2 The File Sharing Screen

You can share files on a USB memory stick or hard drive connected to your GPON Device with users on your network.

The following figure is an overview of the GPON Device's file server feature. Computers **A** and **B** can access files on a USB device (**C**) which is connected to the GPON Device.

**Figure 49** File Sharing Overview



---

The GPON Device will not be able to join the workgroup if your local area network has restrictions set up that do not allow devices to join a workgroup. In this case, contact your network administrator.

---

### 11.2.1 Before You Begin

Make sure the GPON Device is connected to your network and turned on.

- 1 Connect the USB device to one of the GPON Device's USB port. Make sure the GPON Device is connected to your network.
- 2 The GPON Device detects the USB device and makes its contents available for browsing. If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source that is on.

Note: If your USB device cannot be detected by the GPON Device, see the troubleshooting for suggestions.

Use this screen to set up file sharing using the GPON Device. To access this screen, Click **Usb Services > File Sharing**.

**Figure 50** Usb Services > File Sharing

Each field is described in the following table.

**Table 35** Usb Services > File Sharing

| LABEL                              | DESCRIPTION   |
|------------------------------------|---|
| Enable File Sharing Services (SMB) | Select this to activate file sharing through the GPON Device.   |
| Host Name                          | This field shows the configured host name of the GPON Device.   |
| Workgroup Name                     | You can add the GPON Device to an existing or new workgroup on your network. Enter the name of the workgroup which your GPON Device automatically joins.<br><br>You can set the GPON Device's workgroup name to be exactly the same as the workgroup name to which your computer belongs.<br><br>Note: The GPON Device will not be able to join the workgroup if your local area network has restrictions set up that do not allow devices to join a workgroup. In this case, contact your network administrator. |
| Apply                              | Click this to save your changes to the GPON Device.   |
| Cancel                             | Click this to set every field in this screen to its last-saved value.   |

## 11.3 Account Management

Click **Usb Services > File Sharing > Account Management** to view and configure file sharing user accounts on the GPON Device.

**Figure 51** Usb Services > File Sharing > Account Management

Each field is described in the following table.

**Table 36** Usb Services > File Sharing > Account Management

| LABEL     | DESCRIPTION   |
|-----------|---|
| Add       | Click this to set up a file-sharing account. Before you can share files you need a user account.  |
| Active    | This field displays whether a user account is activated or not. Select the check box to enable the account. Clear the check box to disable the account.   |
| Status    | This field displays the status of the user account.   |
| User Name | This field displays the name of the user account.   |
| Modify    | Click the <b>Edit</b> icon to modify the user account.<br><br>Click the <b>Remove</b> icon to remove the user account from the list. Note that you cannot remove the default superuser account. |
| Apply     | Click this to save your changes to the GPON Device.   |
| Cancel    | Click this to set every field in this screen to its last-saved value.   |

### 11.3.1 Add New File Sharing User

In the **Account Management** screen, click the **Add** button or an **Edit** icon next to a user account to create a new user or configure the existing user on the GPON Device.

**Figure 52** Account Management: Add

**Figure 53** Account Management: Edit

Each field is described in the following table.

**Table 37** Account Management: Add/Edit

| LABEL               | DESCRIPTION  |
|---------------------|--|
| User Name           | Enter a user name that will be allowed to access shares. You can enter up to 16 characters. Only letters and numbers allowed.<br><br>This field is greyed-out when you are editing a user account. |
| New Password        | Enter the password used to access the share. You must enter 5 to 15 characters. Only letters and numbers are allowed. The password is case sensitive.  |
| Retype New Password | Retype the password that you entered above.  |

**Table 37** Account Management: Add/Edit

| LABEL  | DESCRIPTION   |
|--------|---|
| Apply  | Click this to save your changes to the GPON Device.                   |
| Cancel | Click this to set every field in this screen to its last-saved value. |



# Remote Management

## 12.1 Overview

This chapter provides information on configuring remote management.

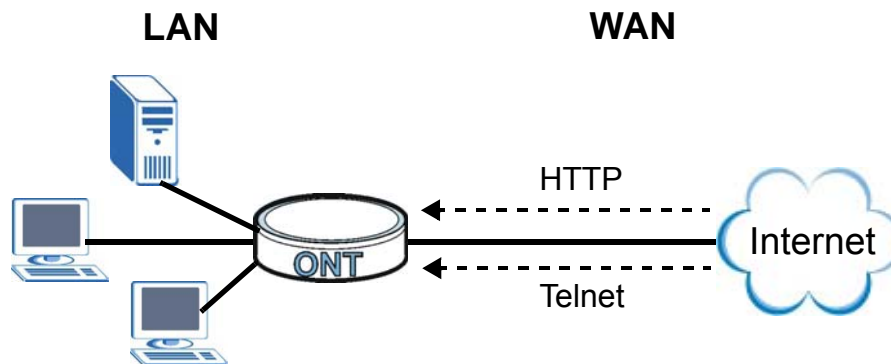
### 12.1.1 What You Need to Know

The following terms and concepts may help as you read through this chapter.

Remote management allows you to determine which services/protocols can access which GPON Device interface (if any) from which computers.

The following figure shows remote management of the GPON Device coming in from the WAN.

**Figure 54** Remote Management From the WAN



You may manage your GPON Device from a remote location via:

- Internet (WAN only)
- ALL (LAN and WAN)
- LAN only,
- None (Disable).

To disable remote management of a service, select **Disable** in the corresponding **Access Status** field.

You may only have one remote management session running at a time. The GPON Device automatically disconnects a remote management session of lower priority when another remote management session of higher priority starts. The priorities for the different types of remote management sessions are: Telnet and WWW.

## Remote Management Limitations

Remote management does not work when:

You have not enabled that service on the interface in the corresponding remote management screen.

- You have disabled that service in one of the remote management screens.
- The IP address in the **Secured Client IP** field does not match the client IP address. If it does not match, the GPON Device will disconnect the session immediately.
- There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.

## Remote Management and NAT

When NAT is enabled:

- Use the GPON Device's WAN IP address when configuring from the WAN.
- Use the GPON Device's LAN IP address when configuring from the LAN.

## System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The GPON Device 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.

## 12.2 WWW

You can manage your GPON Device from over the Web. To change your GPON Device's World Wide Web settings, click **Advanced** > **Remote MGMT** to display the **WWW** screen.

**Figure 55** Remote Management: WWW

The screenshot shows the 'WWW' configuration page. At the top, there are navigation tabs: WWW, Telnet, FTP, SSH, ICMP, UPnP, and TR-069. The 'WWW' tab is selected. Below the tabs, the page title is 'WWW'. The configuration area includes:
 

- 'Access Status' with a dropdown menu currently showing 'LAN / WLAN'.
- 'Secured Client IP' with two radio buttons: 'All' (which is selected) and 'Selected' (which is unselected), followed by an empty text input field.
- A note icon (hand with lightning bolt) followed by the text: 'NOTE : You may also need to create a [Firewall rule](#)'.
- At the bottom right, there are two buttons: 'Apply' and 'Cancel'.



The following table describes the labels in this screen.

**Table 38** Remote Management: WWW

| LABEL             | DESCRIPTION   |
|-------------------|---|
| Access Status     | Select the interface(s) through which a computer may access the GPON Device using this service.<br><br>Note: <b>WAN</b> refers to traffic from the Management WAN interface. Traffic from other WAN interfaces will be dropped.   |
| Secured Client IP | A secured client is a "trusted" computer that is allowed to communicate with the GPON Device using this service.<br><br>Select <b>All</b> to allow any computer to access the GPON Device using this service.<br><br>Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the GPON Device using this service. |
| Apply             | Click <b>Apply</b> to save your settings back to the GPON Device.   |
| Cancel            | Click <b>Cancel</b> to begin configuring this screen afresh.  |

## 12.3 Telnet

You can use Telnet to access the GPON Device's command line interface. Specify which interfaces allow Telnet access and from which IP address the access can come.

Click **Advanced > Remote MGMT > Telnet** tab to display the screen as shown.

**Figure 56** Remote Management: Telnet

The screenshot shows the 'Telnet' configuration screen. At the top, there are tabs for 'WWW', 'Telnet', 'FTP', 'SSH', 'ICMP', 'UPnP', and 'TR-069'. The 'Telnet' tab is active. Below the tabs, the 'Telnet' section is displayed. It includes the following elements:

- Access Status:** A dropdown menu currently showing 'LAN / WLAN'.
- Secured Client IP:** Two radio buttons: 'All' (which is selected) and 'Selected' (which is unselected). To the right of the 'Selected' radio button is an empty text input field.
- NOTE:** A yellow note icon followed by the text: 'NOTE : You may also need to create a [Firewall rule](#)'.
- Buttons:** 'Apply' and 'Cancel' buttons located at the bottom right of the configuration area.

The following table describes the labels in this screen.

**Table 39** Remote Management: Telnet

| LABEL             | DESCRIPTION   |
|-------------------|---|
| Access Status     | Select the interface(s) through which a computer may access the GPON Device using this service.<br><br>Note: <b>WAN</b> refers to traffic from the Management WAN interface. Traffic from other WAN interfaces will be dropped.   |
| Secured Client IP | A secured client is a “trusted” computer that is allowed to communicate with the GPON Device using this service.<br><br>Select <b>All</b> to allow any computer to access the GPON Device using this service.<br><br>Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the GPON Device using this service. |
| Apply             | Click <b>Apply</b> to save your customized settings and exit this screen.   |
| Cancel            | Click <b>Cancel</b> to begin configuring this screen afresh.  |

## 12.4 FTP

You can use FTP (File Transfer Protocol) to upload and download the GPON Device’s firmware and configuration files, please see the User’s Guide chapter on firmware and configuration file maintenance for details. To use this feature, your computer must have an FTP client.

To change your GPON Device’s FTP settings, click **Advanced > Remote MGMT > FTP**. The screen appears as shown. Use this screen to specify which interfaces allow FTP access and from which IP address the access can come.

**Figure 57** Remote Management: FTP

The following table describes the labels in this screen.

**Table 40** Remote Management: FTP

| LABEL             | DESCRIPTION   |
|-------------------|---|
| Access Status     | Select the interface(s) through which a computer may access the GPON Device using this service.<br><br>Note: <b>WAN</b> refers to traffic from the Management WAN interface. Traffic from other WAN interfaces will be dropped.   |
| Secured Client IP | A secured client is a "trusted" computer that is allowed to communicate with the GPON Device using this service.<br><br>Select <b>All</b> to allow any computer to access the GPON Device using this service.<br><br>Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the GPON Device using this service. |
| Apply             | Click <b>Apply</b> to save your customized settings and exit this screen.   |
| Cancel            | Click <b>Cancel</b> to begin configuring this screen afresh.  |

## 12.5 SSH

Use SSH (Secure SHell) to create a secure channel between two devices for data exchange, such as for VPN.

Click **Advanced > Remote MGMT > SSH** to display this screen.

**Figure 58** Remote Management: SSH

WWW Telnet FTP **SSH** ICMP UPnP TR-069

SSH

Access Status LAN / WLAN

Secured Client IP  All  Selected

**NOTE :**  
You may also need to create a [Firewall rule](#)

Apply Cancel

The following table describes the labels in this screen.

**Table 41** Remote Management: SSH

| LABEL             | DESCRIPTION   |
|-------------------|---|
| Access Status     | Select the interface(s) through which a computer may access the GPON Device using this service.<br><br><b>Note: WAN</b> refers to traffic from the Management WAN interface. Traffic from other WAN interfaces will be dropped.   |
| Secured Client IP | A secured client is a "trusted" computer that is allowed to send SSH queries to the GPON Device.<br><br>Select <b>All</b> to allow any computer to send SSH queries to the GPON Device.<br><br>Choose <b>Selected</b> to just allow the computer with the IP address that you specify to send SSH queries to the GPON Device. |
| Apply             | Click <b>Apply</b> to save your customized settings and exit this screen.   |
| Cancel            | Click <b>Cancel</b> to begin configuring this screen afresh.  |

## 12.6 ICMP

To change your GPON Device's security settings, click **Advanced > Remote MGMT > ICMP**. The screen appears as shown.

If an outside user attempts to probe an unsupported port on your GPON Device, an ICMP response packet is automatically returned. This allows the outside user to know the GPON Device exists. Your GPON Device supports anti-probing, which prevents the ICMP response packet from being sent. This keeps outsiders from discovering your GPON Device when unsupported ports are probed.

**Figure 59** Remote Management: ICMP



The following table describes the labels in this screen.

**Table 42** Remote Management: ICMP

| LABEL              | DESCRIPTION  |
|--------------------|--|
| Respond to Ping on | The GPON Device will not respond to any incoming ping requests when <b>Disable</b> is selected. Select <b>LAN/WLAN</b> to reply to incoming LAN and wireless LAN ping requests. Select <b>WAN</b> to reply to incoming WAN ping requests. Otherwise select <b>LAN &amp; WAN</b> to reply to both incoming LAN and WAN ping requests. |
| Apply              | Click this to save your changes.   |
| Cancel             | Click this to restore your previously saved settings.  |

## 12.7 UPnP

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.

### 12.7.1 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 GPON Device 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.

Click **Advanced > Remote MGMT > UPnP** to display this screen.

**Figure 60** Remote Management: UPnP



The following table describes the labels in this screen.

**Table 43** Remote Management: UPnP

| LABEL         | DESCRIPTION   |
|---------------|---|
| Access Status | Select the interface(s) through which a computer may access the GPON Device using UPnP.<br>Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the GPON Device's IP address (although you must still enter the password to access the web configurator). |
| Apply         | Click <b>Apply</b> to save your customized settings and exit this screen.   |
| Cancel        | Click <b>Cancel</b> to begin configuring this screen afresh.  |

## 12.7.2 Installing UPnP in Windows Example

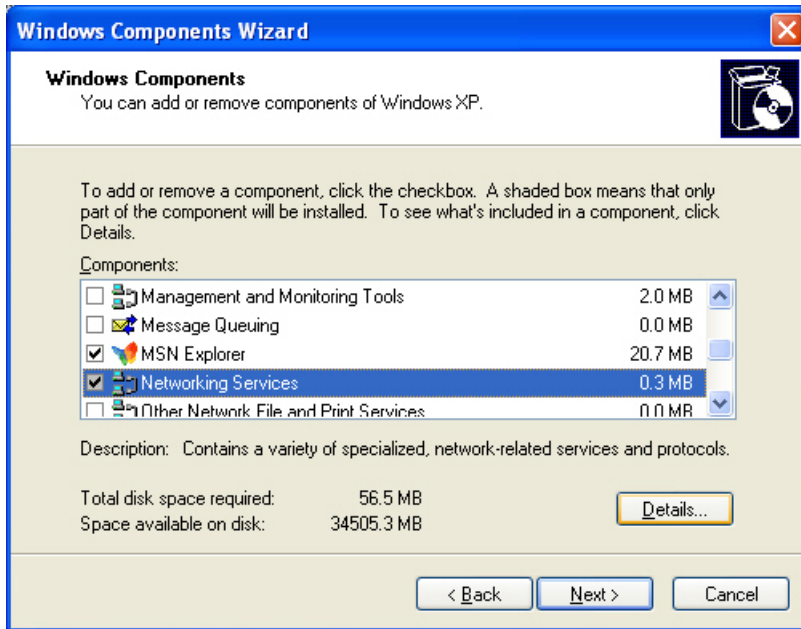
This section shows how to install UPnP in Windows XP.

### Installing UPnP in Windows XP

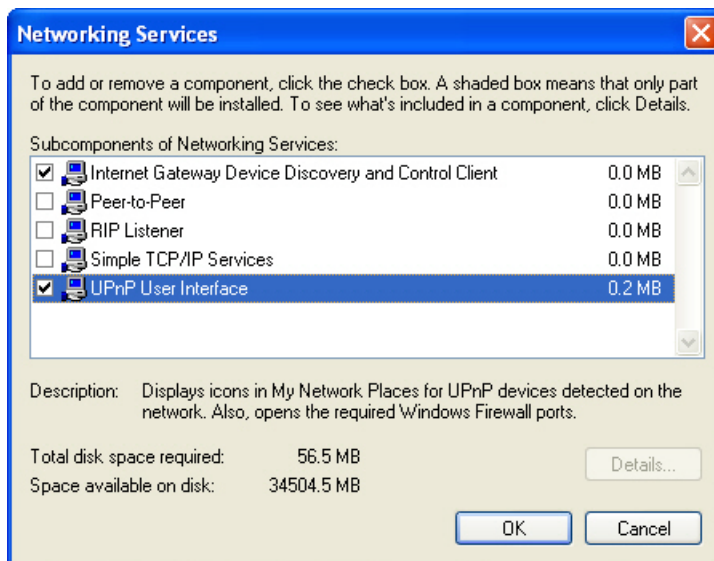
Follow the steps below to install the UPnP in Windows XP.

- 1 Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.

- Click **Add/Remove Windows Components**. Scroll down the bar until you see **Networking Services**. Select it and then click **Details**.



- In the **Networking Services** window, select the **Internet Gateway Device Discovery and Control Client** and **Universal Plug and Play** check boxes.



- Click **OK** to go back to the **Windows Components Wizard** window and click **Next**.
- Click **Finish**.

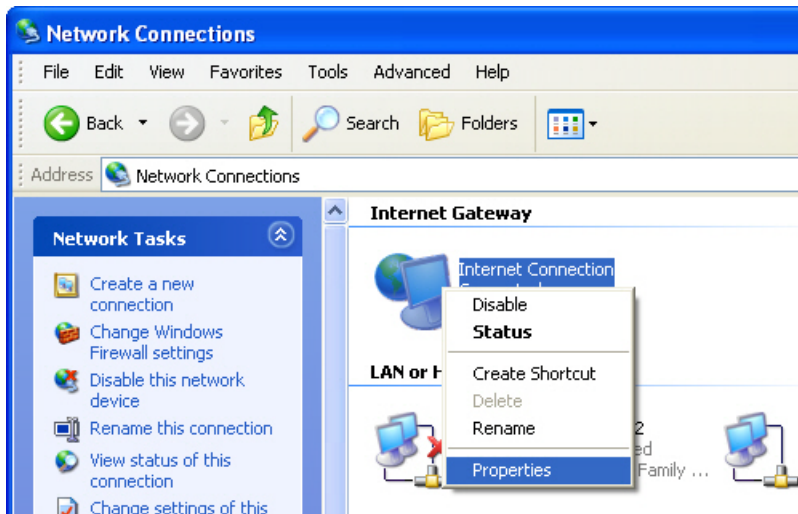
### 12.7.3 Using UPnP in Windows XP Example

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 GPON Device.

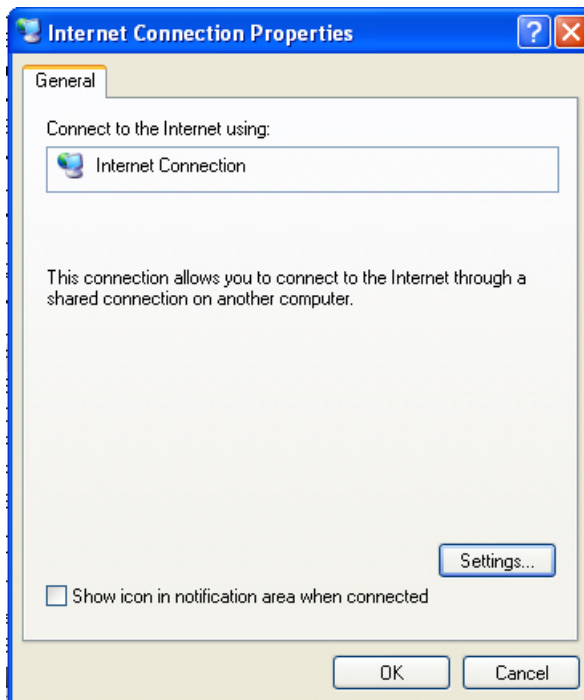
Make sure the computer is connected to a LAN port of the GPON Device. Turn on your computer and the GPON Device.

## 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**.

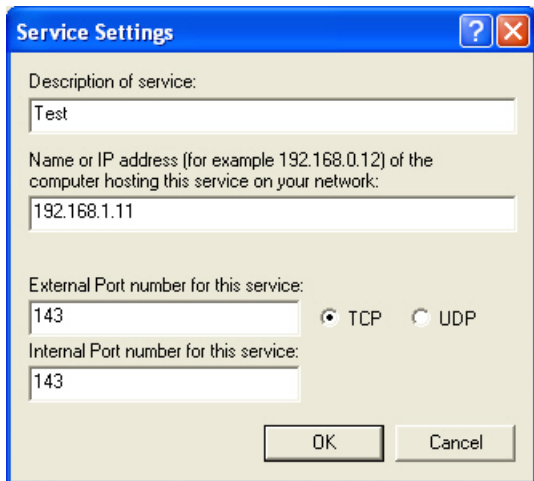
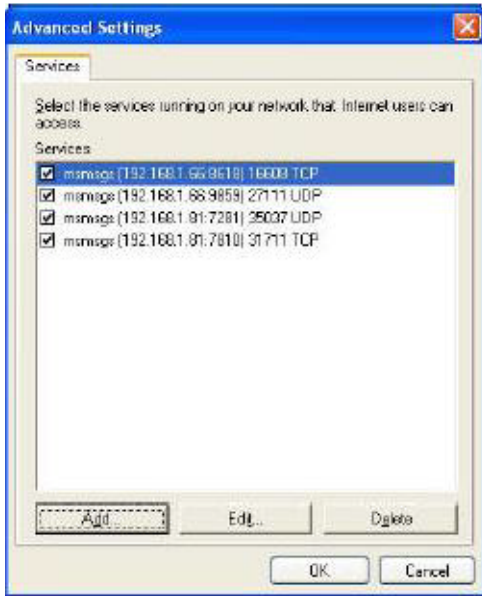


- 3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.

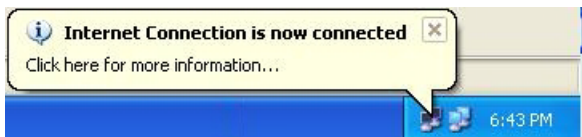




- 4 You may edit or delete the port mappings or click **Add** to manually add port mappings.



- 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.



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

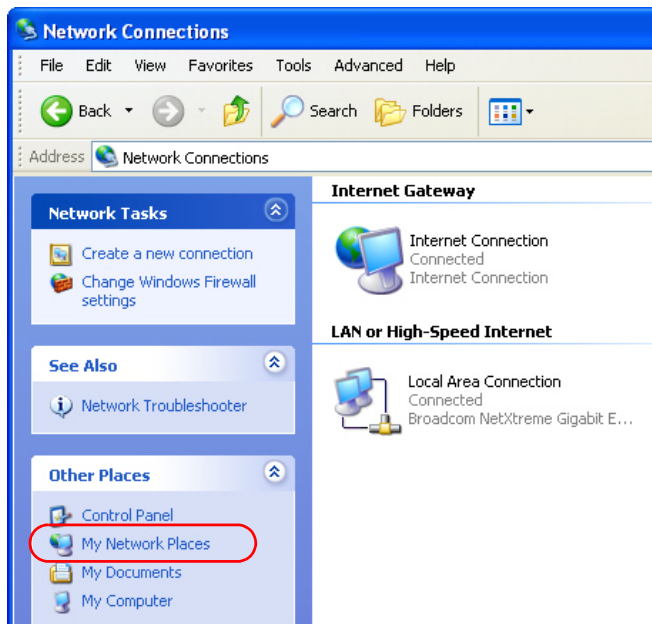


### Web Configurator Easy Access

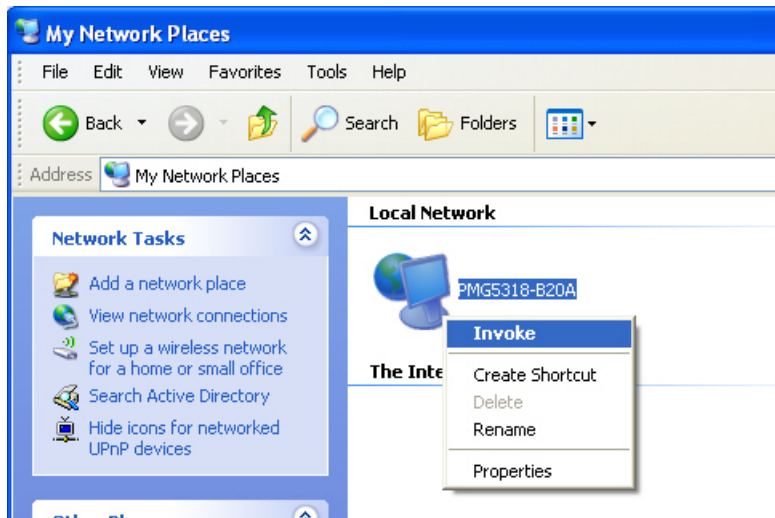
With UPnP, you can access the web-based configurator on the GPON Device without finding out the IP address of the GPON Device first. This comes helpful if you do not know the IP address of the GPON Device.

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**.



- 4 An icon with the description for each UPnP-enabled device displays under **Local Network**.
- 5 Right-click on the icon for your GPON Device and select **Invoke**. The web configurator login screen displays.



## 12.8 The TR-069 Screen

TR-069 defines how Customer Premise Equipment (CPE), for example your GPON Device, can be managed over the WAN by an Auto Configuration Server (ACS). TR-069 is based on sending Remote Procedure Calls (RPCs) between an ACS and a client device. RPCs are sent in Extensible Markup Language (XML) format over HTTP or HTTPS.

An administrator can use an ACS to remotely set up the GPON Device, modify settings, perform firmware upgrades as well as monitor and diagnose the GPON Device. You have enable the device to be managed by the ACS and specify the ACS IP address or domain name and username and password.

Click **Advanced > Remote MGMT > TR-069** to open the following screen. Use this screen to configure your GPON Device to be managed by an ACS.

**Figure 61** Remote Management: TR-069

The following table describes the fields in this screen.

**Table 44** Remote Management: TR-069

| LABEL                        | DESCRIPTION  |
|------------------------------|--|
| Active                       | Select this to activate remote management via TR-069 on the WAN.   |
| ACS URL                      | Enter the URL or IP address of the auto-configuration server.  |
| User Name                    | Enter the TR-069 user name for authentication with the auto-configuration server.  |
| Password                     | Enter the TR-069 password for authentication with the auto-configuration server.   |
| Connection Request URL       | This shows the connection request URL.<br>The ACS can use this URL to make a connection request to the GPON Device.                                    |
| Connection Request User Name | Enter the connection request user name.<br>When the ACS makes a connection request to the GPON Device, this user name is used to authenticate the ACS. |
| Connection Request Password  | Enter the connection request password.<br>When the ACS makes a connection request to the GPON Device, this password is used to authenticate the ACS.   |
| PeriodicInform Enable        | Select this to have the GPON Device periodically send information to the auto-configuration server.  |
| PeriodicInform Interval      | Enter the time interval (in seconds) at which the GPON Device sends information to the auto-configuration server.                                      |
| PeriodicInform Time Enable   | Select this to have the GPON Device send information to the auto-configuration server at a specified time.   |
| PeriodicInform Time          | Enter the date and time at which the GPON Device sends information to the auto-configuration server. For specifying time, the 24 hour format is used.  |
| Apply/Save                   | Click this button to save your changes back to the GPON Device.  |
| Cancel                       | Click <b>Cancel</b> to begin configuring this screen afresh.   |





## Static Route

### 13.1 Overview

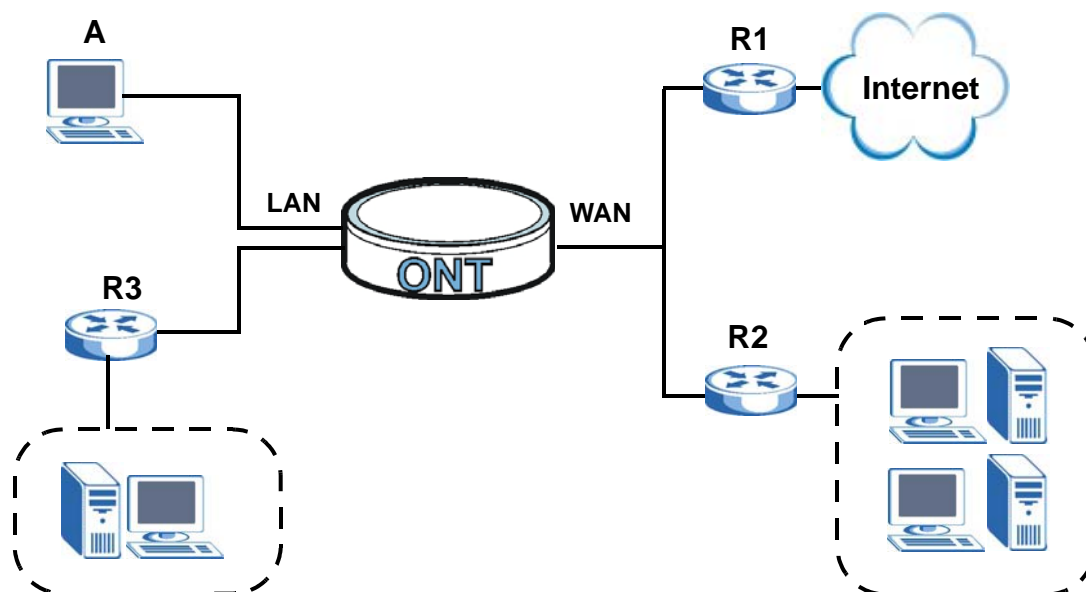
This chapter shows you how to configure static routes for your GPON Device.

### 13.2 Static Route

The GPON Device usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the GPON Device 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 GPON Device's LAN interface. The GPON Device routes most traffic from **A** to the Internet through the GPON Device's default gateway (**R1**). You create one static route to connect to services offered by the ISP behind router **R2**. You create another static route to communicate with a separate network behind a router **R3** connected to the LAN.

**Figure 62** Example of Static Routing Topology



## 13.2.1 Configuring Static Route

Click **Advanced > Static Route** to open the **Static Route** screen.

**Figure 63** Static Route

| #  | Active                   | Name | Destination | Netmask | Gateway | Modify |
|----|--------------------------|------|-------------|---------|---------|--------|
| 1  | <input type="checkbox"/> |      |             |         |         |        |
| 2  | <input type="checkbox"/> |      |             |         |         |        |
| 3  | <input type="checkbox"/> |      |             |         |         |        |
| 4  | <input type="checkbox"/> |      |             |         |         |        |
| 5  | <input type="checkbox"/> |      |             |         |         |        |
| 6  | <input type="checkbox"/> |      |             |         |         |        |
| 7  | <input type="checkbox"/> |      |             |         |         |        |
| 8  | <input type="checkbox"/> |      |             |         |         |        |
| 9  | <input type="checkbox"/> |      |             |         |         |        |
| 10 | <input type="checkbox"/> |      |             |         |         |        |
| 11 | <input type="checkbox"/> |      |             |         |         |        |
| 12 | <input type="checkbox"/> |      |             |         |         |        |
| 13 | <input type="checkbox"/> |      |             |         |         |        |
| 14 | <input type="checkbox"/> |      |             |         |         |        |
| 15 | <input type="checkbox"/> |      |             |         |         |        |
| 16 | <input type="checkbox"/> |      |             |         |         |        |

The following table describes the labels in this screen.

**Table 45** Static Route

| LABEL       | DESCRIPTION  |
|-------------|--|
| #           | This is the number of an individual static route.  |
| Active      | This field indicates whether the rule is active or not.<br>Clear the check box to disable the rule. Select the check box to enable it.   |
| Name        | This is the name that describes or identifies this route.  |
| Destination | This parameter specifies the IP network address of the final destination. Routing is always based on network number.   |
| Netmask     | This parameter specifies the IP network subnet mask of the final destination.  |
| Gateway     | 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.   |
| Modify      | Click the Edit icon to go to the screen where you can set up a static route on the GPON Device.<br>Click the Remove icon to remove a static route from the GPON Device. A window displays asking you to confirm that you want to delete the route. |



**Table 45** Static Route (continued)

| LABEL  | DESCRIPTION   |
|--------|---|
| Apply  | Click this to apply your changes to the GPON Device.        |
| Cancel | Click this to return to the previously saved configuration. |

## 13.2.2 Static Route Edit

Select a static route index number and click **Edit**. The screen shown next appears. Use this screen to configure the required information for a static route.

**Figure 64** Static Route Edit

The following table describes the labels in this screen.

**Table 46** Static Route Edit

| LABEL                  | DESCRIPTION   |
|------------------------|---|
| Active                 | This field allows you to activate/deactivate this static route.   |
| Route Name             | Enter the name of the IP static route. Leave this field blank to delete this static route.  |
| 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 here.  |
| Gateway IP Address     | 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.  |
| Back                   | Click <b>Back</b> to return to the previous screen without saving.  |
| Apply                  | Click <b>Apply</b> to save your changes back to the GPON Device.  |
| Cancel                 | Click <b>Cancel</b> to begin configuring this screen afresh.  |



# Dynamic DNS

## 14.1 Overview

This chapter discusses how to configure your GPON Device to use Dynamic DNS.

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 applications such as NetMeeting and CU-SeeMe). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dns.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.

### 14.1.1 What You Need To Know

#### 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](http://www.yourhost.dyndns.org) and still reach your hostname.

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

## 14.2 The Dynamic DNS Screen

Use this screen to enable DDNS and configure the DDNS settings on the GPON Device. To change your GPON Device's DDNS, click **Advanced > Dynamic DNS**. The screen appears as shown.

**Figure 65** Advanced > Dynamic DNS

The following table describes the fields in this screen.

**Table 47** Advanced > Dynamic DNS

| LABEL                     | DESCRIPTION   |
|---------------------------|---|
| Dynamic DNS Configuration |   |
| Active Dynamic DNS        | Select this check box to use dynamic DNS.   |
| Service Provider          | Select the name of your Dynamic DNS service provider.   |
| Dynamic DNS Type          | Select the type of service that you are registered for from your Dynamic DNS service provider.  |
| Host Name                 | Type the domain name assigned to your GPON Device by your Dynamic DNS provider.<br>You can specify up to two host names in the field separated by a comma (",").  |
| User Name                 | Type your user name.  |
| Password                  | Type the password assigned to you.  |
| Enable Wildcard Option    | Select the check box to enable DynDNS Wildcard.<br><br>This option is only available with a DynDNS account. Enable the wildcard feature to alias subdomains to be aliased to the same IP address as your (dynamic) domain name. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname. |
| IP Address Update Policy  |   |
| Use WAN IP Address        | Select this option to update the IP address of the host name(s) to the WAN IP address.  |

**Table 47** Advanced > Dynamic DNS (continued)

| LABEL                                     | DESCRIPTION   |
|---|---|
| Dynamic DNS server auto detect IP Address | Select this option only when there are one or more NAT routers between the GPON Device and the DDNS server. This feature has the DDNS server automatically detect and use the IP address of the NAT router that has a public IP address.<br><br>Note: The DDNS server may not be able to detect the proper IP address if there is an HTTP proxy server between the GPON Device and the DDNS server. |
| Use specified IP Address                  | Type the IP address of the host name(s). Use this if you have a static IP address.  |
| Apply                                     | Click <b>Apply</b> to save your changes.  |
| Cancel                                    | Click <b>Cancel</b> to restore your previously saved settings.  |



## 15.1 Overview

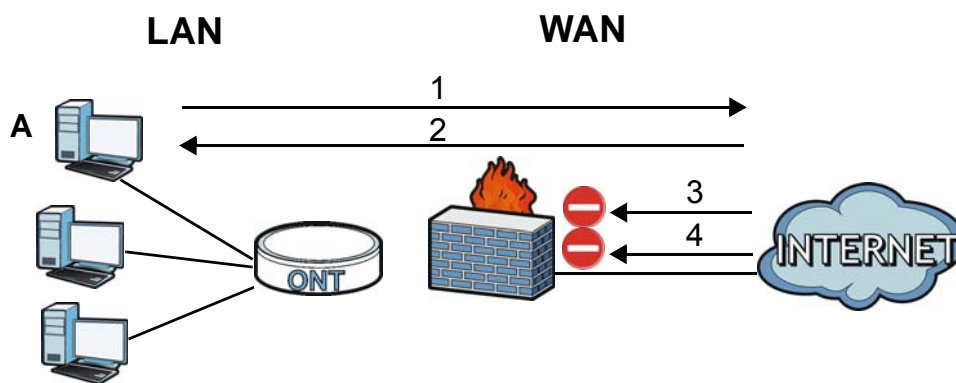
This chapter shows you how to enable the GPON Device firewall. Use the firewall to protect your GPON Device and network from attacks by hackers on the Internet and control access to it. The firewall:

- 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 GPON Device blocks DDOS, LAND and Ping of Death attacks whether the firewall is enabled or disabled.

The following figure illustrates the firewall action. User **A** can initiate an IM (Instant Messaging) session from the LAN to the WAN (1). Return traffic for this session is also allowed (2). However other traffic initiated from the WAN is blocked (3 and 4).

**Figure 66** Default Firewall Action



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

- Use the **General** screen ([Section 15.2 on page 130](#)) to enable firewall and set the default action that the firewall takes on packets depending on packet direction.
- Use the **Rules** screen ([Section 15.3 on page 131](#)) to view the configured firewall rules and add, edit or remove a firewall rule.

## 15.1.2 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 GPON Device is pre-configured to automatically detect and thwart all known DoS attacks.

### DDoS

A Distributed DoS (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 Local Area Network Denial (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.

### RFC 4890 SPEC Traffic

RFC 4890 specifies the filtering policies for ICMPv6 messages. This is important for protecting against security threats including DoS, probing, redirection attacks and renumbering attacks that can be carried out through ICMPv6. Since ICMPv6 error messages are critical for establishing and maintaining communications, filtering policy focuses on ICMPv6 informational messages.



## Anti-Probing

If an outside user attempts to probe an unsupported port on your GPON Device, an ICMP response packet is automatically returned. This allows the outside user to know the GPON Device exists. The GPON Device supports anti-probing, which prevents the ICMP response packet from being sent. This keeps outsiders from discovering your GPON Device when unsupported ports are probed.

## ICMP

Internet Control Message Protocol (ICMP) is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.

## DoS Thresholds

For DoS attacks, the GPON Device uses thresholds to determine when to drop sessions that do not become fully established. These thresholds apply globally to all sessions. You can use the default threshold values, or you can change them to values more suitable to your security requirements.

## 15.2 The General Screen

Use this screen to enable firewall and set the default action that the firewall takes on packets depending on packet direction. Click **Security > Firewall** to display the following screen.

Note: When configuring the firewall, **WAN** refers to traffic passing through the WAN interface set as the default gateway. To check which interface this is click **Network > WAN > Default Gateway**.

**Figure 67** Security > Firewall

| Packet Direction | Default Action | Log                      |
|------------------|----------------|--------------------------|
| LAN to WAN       | Permit         | <input type="checkbox"/> |
| WAN to LAN       | Drop           | <input type="checkbox"/> |

The following table describes the labels in this screen.

**Table 48** Security > Firewall

| LABEL  | DESCRIPTION  |
|--|--|
| Active Firewall  | Select this to enable the firewall feature.  |
| Reject to response the request for unauthorized services | If you select this, the GPON Device will not send an ICMP response packet when unsupported services are requested. Therefore, an outside user will not be able to determine the ONT exists.  |
| Packet Direction   | This is the direction of travel of packets ( <b>LAN to WAN, WAN to LAN</b> ).<br><br>Firewall rules are grouped based on the direction of travel of packets to which they apply. For example, <b>LAN to WAN</b> means packets traveling from a computer/subnet on the LAN to the WAN.  |
| Default Action   | Use the drop-down list boxes to select the default action that the firewall is to take on packets that are traveling in the selected direction and do not match any of the firewall rules.<br><br>Select <b>Drop</b> to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender.<br><br>Select <b>Reject</b> to deny the packets and send a TCP reset packet (for a TCP packet) or an ICMP destination-unreachable message (for a UDP packet) to the sender.<br><br>Select <b>Permit</b> to allow the passage of the packets. |
| Apply  | Click this to save your changes.   |
| Cancel   | Click this to restore your previously saved settings.  |

## 15.3 The Rules Screen

Click **Security > Firewall > Rules** to display the following screen. This screen displays a list of the configured firewall rules. Note the order in which the rules are listed.

Note: The ordering of your rules is very important as rules are applied in turn.

**Figure 68** Security > Firewall > Rules

The following table describes the labels in this screen.

**Table 49** Security > Firewall > Rules

| LABEL                               | DESCRIPTION   |
|-------------------------------------|---|
| Packet Direction                    | Use the drop-down list box to select a direction of travel of packets for which you want to configure firewall rules.   |
| Create a new rule after rule number | Select an index number and click <b>Add</b> to add a new firewall rule after the selected index number. For example, if you select "6", your new rule becomes number 7 and the previous rule 7 (if there is one) becomes rule 8.  |
|                                     | The following read-only fields summarize the rules you have created that apply to traffic traveling in the selected packet direction. The firewall rules that you configure (summarized below) take priority over the general firewall action settings in the <b>General</b> screen.                    |
| #                                   | This is your firewall rule number. The ordering of your rules is important as rules are applied in turn.  |
| Active                              | This field displays whether a firewall is turned on or not. Select the check box to enable the rule. Clear the check box to disable the rule.   |
| Source IP                           | This column displays the source addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to <b>Any</b> .  |
| Destination IP                      | This column displays the destination addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to <b>Any</b> .   |
| Service                             | This column displays the services to which this firewall rule applies.  |
| Action                              | This field displays whether the firewall silently discards packets ( <b>Drop</b> ), discards packets and sends a TCP reset packet or an ICMP destination-unreachable message to the sender ( <b>Reject</b> ) or allows the passage of packets ( <b>Permit</b> ).  |
| Log                                 | This field displays if a log for packets that match the rule is created or not.   |
| Modify                              | Click the Edit icon to go to the screen where you can edit the rule.<br><br>Click the Remove icon to delete an existing firewall rule. A window displays asking you to confirm that you want to delete the firewall rule. Note that subsequent firewall rules move up by one when you take this action. |

**Table 49** Security > Firewall > Rules

| LABEL  | DESCRIPTION   |
|--------|---|
| Order  | Click the Move icon to display the <b>Move the rule to</b> field. Type a number in the <b>Move the rule to</b> field and click the <b>Move</b> button to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering. |
| Apply  | Click this to save your changes.  |
| Cancel | Click this to restore your previously saved settings.   |

### 15.3.1 The Rules Add Screen

Use this screen to configure firewall rules. In the **Rules** screen, select an index number and click **Add** or click a rule's **Edit** icon to display this screen and refer to the following table for information on the labels.

**Figure 69** Security > Firewall > Rules > Add

**Add Rule 1**

Active     Log

Action for Matched Packets: Permit

**Source Address**

Address Type: Any Address

Start IP Address:

End IP Address:

Subnet Mask:

**Destination Address**

Address Type: Any Address

Start IP Address:

End IP Address:

Subnet Mask:

**Service**

Available Services: ANY

[Edit Customized Services](#)

Back Apply Cancel

The following table describes the labels in this screen.

**Table 50** Security > Firewall > Rules > Add

| LABEL                      | DESCRIPTION  |
|----------------------------|--|
| Active                     | Select this option to enable this firewall rule.   |
| Action for Matched Packet  | Use the drop-down list box to select whether to discard ( <b>Drop</b> ), deny and send an ICMP destination-unreachable message to the sender of ( <b>Reject</b> ) or allow the passage of ( <b>Permit</b> ) packets that match this rule.  |
| IP Version Type            | Select the IP version, <b>IPv4</b> or <b>IPv6</b> , to apply this firewall rule to.  |
| Log                        | This field determines if a log for packets that match the rule is created or not.  |
| Source/Destination Address |  |
| Address Type               | Do you want your rule to apply to packets with a particular (single) IP, a range of IP addresses (for instance, 192.168.1.10 to 192.169.1.50), a subnet or any IP address? Select an option from the drop-down list box that includes: <b>Single Address</b> , <b>Range Address</b> , <b>Subnet Address</b> and <b>Any Address</b> . |
| Start IP Address           | Enter the single IP address or the starting IP address in a range here.  |
| End IP Address             | Enter the ending IP address in a range here.   |
| Subnet Mask                | Enter the subnet mask here, if applicable.   |
| Services                   |  |
| Available                  | Select a service from the <b>Available Services</b> box.   |
| Edit Customized Service    | Click the <b>Edit Customized Services</b> link to bring up the screen that you use to configure a new custom service that is not in the predefined list of services.   |
| Apply                      | Click this to save your changes.   |
| Cancel                     | Click this to restore your previously saved settings.  |

## 15.3.2 Customized Services

Configure customized services and port numbers not predefined by the GPON Device. For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) website. Click the **Edit Customized Services** link while editing a firewall rule to configure a custom service port. This displays the following screen.

**Figure 70** Security > Firewall > Rules: Edit: Edit Customized Services

| No. | Name | Protocol | Port |
|-----|------|----------|------|
| 1   |      |          |      |
| 2   |      |          |      |
| 3   |      |          |      |
| 4   |      |          |      |
| 16  |      |          |      |

Back

The following table describes the labels in this screen.

**Table 51** Security > Firewall > Rules: Edit: Edit Customized Services

| LABEL    | DESCRIPTION  |
|----------|--|
| No.      | This is the number of your customized port.  |
| Name     | This is the name of your customized service.   |
| Protocol | This shows the IP protocol ( <b>TCP</b> or <b>UDP</b> ) that defines your customized service.                |
| Port     | This is the port number or range that defines your customized service.                                       |
| Modify   | Click this to go to the <b>Firewall Customized Services Config</b> screen to edit a customized service.      |
| Add      | Click this to go to the <b>Firewall Customized Services Config</b> screen to configure a customized service. |
| Back     | Click this to return to the <b>Firewall Edit Rule</b> screen.  |

### 15.3.3 Configuring a Customized Service

Use this screen to add a customized rule or edit an existing rule. Click a rule number in the **Firewall Customized Services** screen to display the following screen.

**Figure 71** Security > Firewall > Rules: Edit: Edit Customized Services: Config

The following table describes the labels in this screen.

**Table 52** Security > Firewall > Rules: Edit: Edit Customized Services: Config

| LABEL              | DESCRIPTION   |
|--------------------|---|
| Config             |   |
| Service Name       | Type a unique name for your custom port.  |
| Service Type       | Choose the IP port ( <b>TCP</b> or <b>UDP</b> ) that defines your customized port from the drop down list box.                    |
| Port Configuration |   |
| Type               | Click <b>Single</b> to specify one port only or <b>Port Range</b> to specify a span of ports that define your customized service. |
| Port Number        | Type a single port number or the range of port numbers that define your customized service.                                       |
| Back               | Click this to return to the previous screen without saving.   |
| Apply              | Click this to save your changes.  |

**Table 52** Security > Firewall > Rules: Edit: Edit Customized Services: Config

| LABEL  | DESCRIPTION   |
|--------|---|
| Cancel | Click this to restore your previously saved settings. |
| Delete | Click this to delete the current rule.                |

## 15.4 Firewall Technical Reference

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

### 15.4.1 Firewall Rules Overview

Your customized rules take precedence and override the GPON Device's default settings. The GPON Device checks the source IP address, destination IP address and IP protocol type of network traffic against the firewall rules (in the order you list them). When the traffic matches a rule, the GPON Device takes the action specified in the rule.

Firewall rules are grouped based on the direction of travel of packets to which they apply:

- WAN to LAN
- LAN to WAN

Note: The LAN includes both the LAN port and the WLAN.

By default, the GPON Device's stateful packet inspection allows packets traveling in the following directions:

- LAN to WAN  
These rules specify which computers on the LAN can access which computers or services on the WAN.

By default, the GPON Device's stateful packet inspection drops packets traveling in the following directions:

- WAN to LAN  
These rules specify which computers on the WAN can access which computers or services on the LAN.

Note: You also need to configure NAT port forwarding (or full featured NAT address mapping rules) to allow computers on the WAN to access devices on the LAN.

You may define additional rules and sets or modify existing ones but please exercise extreme caution in doing so.

For example, you may create rules to:

- Block certain types of traffic, such as IRC (Internet Relay Chat), from the LAN to the Internet.
- Allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN.

- Allow everyone except your competitors to access a web server.
- Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

These custom rules work by comparing the source IP address, destination IP address and IP protocol type of network traffic to rules set by the administrator. Your customized rules take precedence and override the GPON Device's default rules.

## 15.4.2 Guidelines For Enhancing Security With Your Firewall

- 6 Change the default password via web configurator.
- 7 Think about access control before you connect to the network in any way.
- 8 Limit who can access your router.
- 9 Don't enable any local service (such as telnet or FTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.
- 10 For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.
- 11 Protect against IP spoofing by making sure the firewall is active.
- 12 Keep the firewall in a secured (locked) room.

## 15.4.3 Security Considerations

Note: Incorrectly configuring the firewall may block valid access or introduce security risks to the GPON Device and your protected network. Use caution when creating or deleting firewall rules and test your rules after you configure them.

Consider these security ramifications before creating a rule:

- 1 Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC is blocked, are there users that require this service?
- 2 Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?
- 3 Does a rule that allows Internet users access to resources on the LAN create a security vulnerability? For example, if FTP ports (TCP 20, 21) are allowed from the Internet to the LAN, Internet users may be able to connect to computers with running FTP servers.
- 4 Does this rule conflict with any existing rules?

Once these questions have been answered, adding rules is simply a matter of entering the information into the correct fields in the web configurator screens.



## 16.1 Overview

Use this screen to configure the GPON Device's time and date settings.

### 16.1.1 What You Need to Know

The following terms and concepts may help as you read through this chapter.

#### General Setup and System Name

**General Setup** contains administrative and system-related information. **System Name** is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

- In Windows 2000, click **Start > Settings > Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the **System Name**.
- In Windows XP, click **Start > My Computer > View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the GPON Device **System Name**.

## 16.2 General Setup

Use this screen to configure the GPON Device's system name, inactivity timer, and password. Click **Maintenance > System** to open the **General** screen.

**Figure 72** System > General

The following table describes the labels in this screen.

**Table 53** System > General Setup

| LABEL                          | DESCRIPTION   |
|--------------------------------|---|
| General Setup                  |   |
| System Name                    | Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.  |
| Administrator Inactivity Timer | Type how many minutes a management session (either via the web configurator or telnet) can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended). |
| Password                       |   |
| Old Password                   | Type the default password or the existing password you use to access the system in this field.  |
| New Password                   | Type your new system 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 GPON Device.  |
| Retype to Confirm              | Type the new password again for confirmation.   |
| Apply                          | Click <b>Apply</b> to save your changes back to the GPON Device.  |
| Cancel                         | Click <b>Cancel</b> to begin configuring this screen afresh.  |

## 16.3 Time Setting

To change your GPON Device's time and date, click **Maintenance > System > Time Setting**. The screen appears as shown. Use this screen to configure the GPON Device's time based on your local time zone.

**Figure 73** System > Time Setting

The following table describes the fields in this screen.

**Table 54** System > Time Setting

| LABEL                | DESCRIPTION   |
|----------------------|---|
| Current Time         |   |
| Current Time         | This field displays the time of your GPON Device.<br>Each time you reload this page, the GPON Device synchronizes the time with the time server.                                |
| Current Date         | This field displays the date of your GPON Device.<br>Each time you reload this page, the GPON Device synchronizes the date with the time server.                                |
| Time and Date Setup  |   |
| Get from Time Server | Select this radio button to have the GPON Device get the time and date from the time server you specified below.  |
| Time Protocol        | Indicates that the GPON Device uses the NTP format, which displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.                                 |
| Time Server Address  | Enter the IP address or URL (up to 20 extended ASCII characters in length) of your time server. Check with the ISP/network administrator if you are unsure of this information. |
| Apply                | Click <b>Apply</b> to save your changes back to the GPON Device.  |
| Cancel               | Click <b>Cancel</b> to begin configuring this screen afresh.  |

## 16.4 SLID

To change your GPON Device's Subscriber Location ID (SLID) setting, click **Maintenance > System > SLID**. The screen appears as shown.

**Figure 74** System > SLID

The following table describes the fields in this screen.

**Table 55** System > SLID

| LABEL       | DESCRIPTION   |
|-------------|---|
| Enable SLID | Select this to enable use of SLID.  |
| SLID Value  | Enter the SLID used for gaining access to the service provider's network. |
| Apply       | Click <b>Apply</b> to save your changes back to the GPON Device.          |
| Cancel      | Click <b>Cancel</b> to begin configuring this screen afresh.              |

## 17.1 Overview

This chapter contains information about configuring general log settings and viewing the GPON Device's logs.

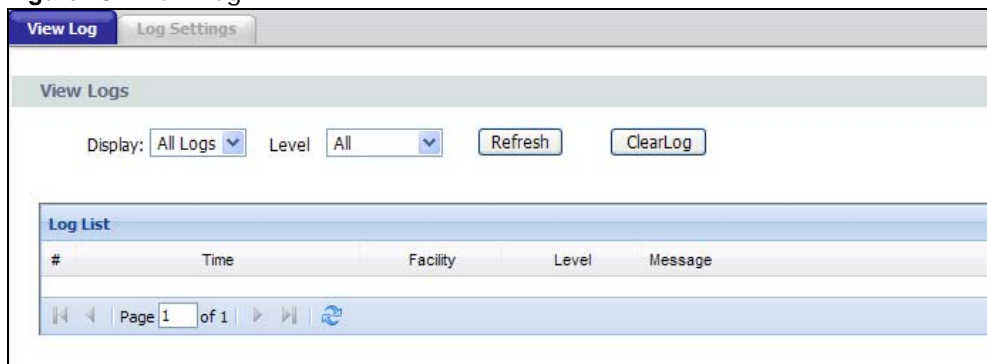
The web configurator allows you to choose which categories of events and/or alerts to have the GPON Device log and then display the logs or have the GPON Device send them to an administrator (as e-mail) or to a syslog server.

## 17.2 View Log

Click **Maintenance > Logs** to open the **View Log** screen. Use this screen to see the logs for the categories that you selected in the **Log Settings** screen (see [Section 17.3 on page 142](#)).

Log entries in red indicate alerts. The log wraps around and deletes the old entries after it fills. Click a column heading to sort the entries. A triangle indicates ascending or descending sort order.

**Figure 75** View Log



The following table describes the fields in this screen.

**Table 56** View Log

| LABEL     | DESCRIPTION   |
|-----------|---|
| Display   | The categories that you select in the <b>Log Settings</b> screen display in the drop-down list box.<br>Select a category of logs to view; select <b>All Logs</b> to view logs from all of the log categories that you selected in the <b>Log Settings</b> page. |
| Refresh   | Click <b>Refresh</b> to renew the log screen.   |
| Clear Log | Click <b>Clear Log</b> to delete all the logs.  |
| #         | This field is a sequential value and is not associated with a specific entry.   |

**Table 56** View Log

| LABEL    | DESCRIPTION  |
|----------|--|
| Time     | This field displays the time the log was recorded.   |
| Facility | This indicates the type of connection to the GPON Device.<br>Facility types are as follows: <ul style="list-style-type: none"> <li>• <b>tr069</b> - This indicates a log from an external auto-configuration server.</li> <li>• <b>ntpclient</b> - This indicates a log from the ntpclient.</li> <li>• <b>login</b> - This indicates a message from the Web Configurator login information.</li> <li>• <b>dhcp</b> - This indicates a log message from the device's DHCP server.</li> <li>• <b>dnsmasq</b> - This indicates a log message from the device's DNS forwarder.</li> <li>• <b>pppoe</b> - This indicates a log message from the device's Point-to-Point Protocol daemon.</li> <li>• <b>kernel</b> - This indicates a log message related to the device's Central Processing Unit (CPU), memory, and I/O ports.</li> <li>• <b>OMCI</b> - This indicates a log message about the GPON OMCI Protocol daemon.</li> <li>• <b>VoIP</b> - This indicates a log a message from the SIP server.</li> </ul> |
| Level    | This indicates the log severity.   |
| Message  | This field states the reason for the log.  |
| First    | Click this to cycle to the first page of logs.   |
| Previous | Click this to cycle to the previous page of logs.  |
| Page     | This indicates which page you are on, out of how many. You can enter a page number here and press [Enter] to jump directly to that page.   |
| Next     | Click this to cycle to the next page of logs.  |
| Last     | Click this to cycle to the last page of logs   |
| Refresh  | Click this to refresh the logs screen.   |

## 17.3 Log Settings

Use this screen to configure which logs to display on the **View Logs** screen (see [Chapter 17 on page 141](#)). Click **Maintenance > Logs > Log Settings**.

**Figure 76** Log Settings

The screenshot shows the 'Log Settings' interface. At the top, there are two tabs: 'View Log' and 'Log Settings'. Below the tabs is a section titled 'Active Log'. Under this section, there are seven checkboxes arranged in three columns: WAN Connection, Network Service, Attacks, System Maintenance, VOIP, and TR-069. The PON checkbox is not visible. At the bottom right of the screen, there are two buttons: 'Apply' and 'Cancel'.

The following table describes the fields in this screen.

**Table 57** Log Settings

| LABEL      | DESCRIPTION   |
|------------|---|
| Active Log |   |
| [Log Type] | Select the type of log you want to be displayed on the <b>View Logs</b> screen. |
| Apply      | Click <b>Apply</b> to save your customized settings and exit this screen.       |
| Cancel     | Click <b>Cancel</b> to return to the previously saved settings.                 |





## 18.1 Overview

This chapter explains how to upload new firmware, manage configuration files and restart your GPON Device.

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.

### 18.1.1 Some Warnings

The following are some friendly reminders about your device:

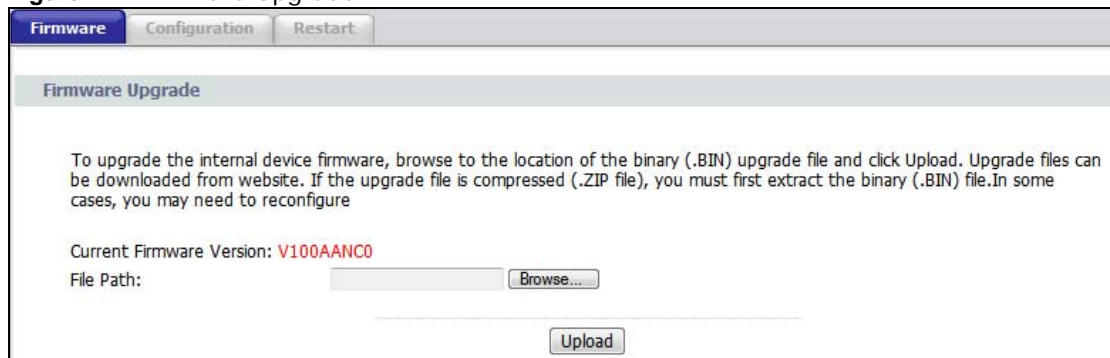
**Do NOT turn off the GPON Device while a firmware upload is in progress!**

**Only use firmware for your device's specific model. Refer to the label on the bottom of your GPON Device.**

## 18.2 Firmware Upgrade

Click **Maintenance > Tools** to open the **Firmware** screen. Follow the instructions in this screen to upload firmware to your GPON Device. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

**Figure 77** Firmware Upgrade



The screenshot shows a web interface for the 'Firmware Upgrade' screen. At the top, there are three tabs: 'Firmware' (selected), 'Configuration', and 'Restart'. Below the tabs is a header 'Firmware Upgrade'. The main content area contains the following text: 'To upgrade the internal device firmware, browse to the location of the binary (.BIN) upgrade file and click Upload. Upgrade files can be downloaded from website. If the upgrade file is compressed (.ZIP file), you must first extract the binary (.BIN) file. In some cases, you may need to reconfigure'. Below this text, it says 'Current Firmware Version: V100AANC0'. There is a 'File Path:' label followed by a text input field and a 'Browse...' button. At the bottom of the form is an 'Upload' button.

The following table describes the labels in this screen.

**Table 58** Firmware Upgrade

| LABEL                    | DESCRIPTION  |
|--------------------------|--|
| Current Firmware Version | This is the present Firmware version and the date created.   |
| File Path                | Type in the location of the file you want to upload in this field or click <b>Browse ...</b> to find it.   |
| Browse...                | 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. |
| Upload                   | Click <b>Upload</b> to begin the upload process. This process may take up to two minutes.  |

After you see the **Firmware Upload in Progress** screen, wait three minutes before logging into the GPON Device again.

The GPON Device automatically restarts in this time causing a temporary network disconnect.

After two minutes, log in again and check your new firmware version in the **Status** screen.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **Firmware** screen.

## 18.3 Configuration

Click **Maintenance > Tools > Configuration**. Information related to factory defaults, backup configuration, and restoring configuration appears in this screen, as shown next.

**Figure 78** Configuration

The screenshot shows a web interface with three main sections:

- Backup Configuration:** Contains the instruction "Click **Backup** to save the current configuration as a file to your computer." and a **Backup** button.
- Restore Configuration:** Contains the instruction "To upload a previously saved configuration file from your computer to the device, enter the file name and path or click **Browse**, then click **Upload**." Below this is a "File Path:" label, a text input field, a **Browse...** button, and an **Upload** button.
- Reset to Factory Default Settings:** Contains the instruction "Click **Reset** to clear all customized configuration settings and restore the device to its factory-default settings." Below this is a list of settings: "The following settings will be used after you click the **Reset** button:", "Password: 1234", and "LAN IP: 192.168.1.1". A **Reset** button is at the bottom.

### 18.3.1 Backup Configuration

Backup Configuration allows you to back up (save) the GPON Device's current configuration to a file on your computer. Once your GPON Device 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 **Backup** to save the GPON Device's current configuration to your computer.

### 18.3.2 Restore Configuration

Restore Configuration allows you to upload a new or previously saved configuration file from your computer to your GPON Device.

**Table 59** Restore Configuration

| LABEL     | DESCRIPTION   |
|-----------|---|
| File Path | Type in the location of the file you want to upload in this field or click <b>Browse ...</b> to find it.  |
| Browse... | 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. |
| Upload    | Click <b>Upload</b> to begin the upload process.  |

After you see a “restore configuration successful” screen, you must then wait one minute before logging into the GPON Device again.

The GPON Device automatically restarts in this time causing a temporary network disconnect.

If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (10.0.0.138).

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **Configuration** screen.

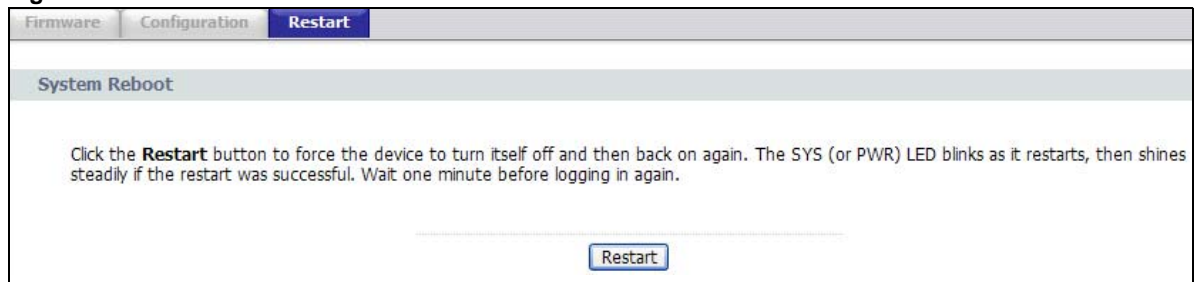
### 18.3.3 Reset to Factory Defaults

Click the **Reset** button to clear all user-entered configuration information and return the GPON Device to its factory defaults. You can also press the **RESET** button on the rear panel to reset the factory defaults of your GPON Device.

## 18.4 Restart

System restart allows you to reboot the GPON Device without turning the power off. Click **Maintenance > Tools > Restart**. Click **Restart** to have the GPON Device reboot. This does not affect the GPON Device's configuration.

**Figure 79** Restart Screen



## Diagnostic

### 19.1 Overview

This read-only screen displays information to help you identify problems with the GPON Device.

### 19.2 General

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

**Figure 80** Diagnostic > General

The screenshot shows a web interface titled "General". It displays the results of a ping command to 192.168.1.2. The output is as follows:

```

PING 192.168.1.2 (192.168.1.2): 56 data bytes
64 bytes from 192.168.1.2: seq=0 ttl=128 time=0.530 ms
64 bytes from 192.168.1.2: seq=1 ttl=128 time=0.443 ms
64 bytes from 192.168.1.2: seq=2 ttl=128 time=0.500 ms
64 bytes from 192.168.1.2: seq=3 ttl=128 time=2.680 ms
64 bytes from 192.168.1.2: seq=4 ttl=128 time=2.713 ms

--- 192.168.1.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.443/1.373/2.713 ms
  
```

Below the output, there is a section labeled "TCP/IP" with an "Address" input field and a "Ping" button.

The following table describes the fields in this screen.

**Table 60** Diagnostic > General

| LABEL          | DESCRIPTION  |
|----------------|--|
| TCP/IP Address | Type the IP address of a computer that you want to ping in order to test a connection. |
| Ping           | Click this button to ping the IP address that you entered from the GPON Device.        |



# Troubleshooting

## 20.1 Overview

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](#)
- [GPON Device Access and Login](#)
- [Internet Access](#)
- [Phone Calls and VoIP](#)

## 20.2 Power, Hardware Connections, and LEDs

---

The GPON Device does not turn on. None of the LEDs turn on.

---

- 1 Make sure the GPON Device is turned on.
- 2 Make sure you are using the power adaptor or cord included with the GPON Device.
- 3 Make sure the power adaptor or cord is connected to the GPON Device and plugged in to an appropriate power source. Make sure the power source is turned on.
- 4 Turn the GPON Device 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. The **PON** LED turns red if the optical transceiver has malfunctioned or the fiber cable is not connected or is broken or damaged enough to break the PON connection. See [Section 1.5 on page 11](#).
- 2 Check the hardware connections. See [Section 1.5 on page 11](#).
- 3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.

- 4 Turn the GPON Device off and on.
- 5 If the problem continues, contact the vendor.

## 20.3 GPON Device Access and Login

---

I forgot the IP address for the GPON Device.

---

- 1 The default IP address is 192.168.1.1.
- 2 If you changed the IP address and have forgotten it, reset the GPON Device to its factory defaults. See [Section 1.6 on page 12](#).

---

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, 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 GPON Device](#).
- 2 Check the hardware connections, and make sure the LEDs are behaving as expected. See [Section 1.5 on page 11](#).
- 3 Make sure your Internet browser does not block pop-up windows and has Javascript and Java enabled.
- 4 Reset the device to its factory defaults, and try to access the GPON Device with the default IP address. See [Section 1.6 on page 12](#).
- 5 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

---

I can see the **Login** screen, but I cannot log in to the GPON Device.

---

- 1 Make sure you have entered the user name and password correctly. The default user name is **admin**. These fields are 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 GPON Device. Log out of the GPON Device in the other session, or ask the person who is logged in to log out.



- 3 Turn the GPON Device off and on.
- 4 If this does not work, you have to reset the device to its factory defaults. See [Section 20.2 on page 151](#).

## 20.4 Internet Access

---

### I cannot access the Internet.

---

- 1 Check the hardware connections, and make sure the LEDs are behaving as expected.  
The **PON** LED turns red if the optical transceiver has malfunctioned or the fiber cable is not connected or is broken or damaged enough to break the PON connection.  
The **PON** LED turns orange if the GPON Device's PON port is physically connected but not registered. If the service provider gave you an SLID to use, make sure you entered the SLID correctly (see [Section 16.4 on page 140](#)). It is case-sensitive, so make sure [Caps Lock] is not on.  
See [Section 1.5 on page 11](#) for details about the other LEDs.
- 2 Make sure you entered the ISP account information correctly in the wizard. These fields are case-sensitive, so make sure [Caps Lock] is not on.
- 3 Disconnect all the cables from your device, and follow the directions in [Section 1.5 on page 11](#) again.
- 4 If the problem continues, contact the ISP.

---

### I cannot access the Internet anymore. I had access to the Internet (with the GPON Device), but my Internet connection is not available anymore.

---

- 1 Check the hardware connections, and make sure the LEDs are behaving as expected. The **PON** LED turns red if the optical transceiver has malfunctioned or the fiber cable is not connected or is broken or damaged enough to break the PON connection. See [Section 1.5 on page 11](#) for details about the other LEDs.
- 2 Turn the GPON Device off and on.
- 3 If the problem continues, contact the 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 11](#). If the GPON Device is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
- 2 Turn the GPON Device off and on.
- 3 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

## 20.5 Phone Calls and VoIP

---

The telephone port won't work or the telephone lacks a dial tone.

---

- 1 Check the telephone connections and telephone wire.

---

I can access the Internet, but cannot make VoIP calls.

---

- 1 The **PHONE** light should come on. Make sure that your telephone is connected to the **PHONE** port.
- 2 You can also check the VoIP status in the **Status** screen.
- 3 If the VoIP settings are correct, use speed dial to make calls. If you can make a call using speed dial, there may be something wrong with the SIP server, contact your VoIP service provider.

# 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 websites are listed below (see also [http://www.zyxel.com/about\\_zyxel/zyxel\\_worldwide.shtml](http://www.zyxel.com/about_zyxel/zyxel_worldwide.shtml)). 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.

## Corporate Headquarters (Worldwide)

### Taiwan

- ZyXEL Communications Corporation
- <http://www.zyxel.com>

## Asia

### China

- ZyXEL Communications (Shanghai) Corp.
- ZyXEL Communications (Beijing) Corp.
- ZyXEL Communications (Tianjin) Corp.
- <http://www.zyxel.cn>

### India

- ZyXEL Technology India Pvt Ltd
- <http://www.zyxel.in>

### Kazakhstan

- ZyXEL Kazakhstan
- <http://www.zyxel.kz>

### **Korea**

- ZyXEL Korea Corp.
- <http://www.zyxel.kr>

### **Malaysia**

- ZyXEL Malaysia Sdn Bhd.
- <http://www.zyxel.com.my>

### **Pakistan**

- ZyXEL Pakistan (Pvt.) Ltd.
- <http://www.zyxel.com.pk>

### **Philippines**

- ZyXEL Philippines
- <http://www.zyxel.com.ph>

### **Singapore**

- ZyXEL Singapore Pte Ltd.
- <http://www.zyxel.com.sg>

### **Taiwan**

- ZyXEL Communications Corporation
- <http://www.zyxel.com>

### **Thailand**

- ZyXEL Thailand Co., Ltd
- <http://www.zyxel.co.th>

### **Vietnam**

- ZyXEL Communications Corporation-Vietnam Office
- <http://www.zyxel.com/vn/vi>

## **Europe**

### **Austria**

- ZyXEL Deutschland GmbH
- <http://www.zyxel.de>

### **Belarus**

- ZyXEL BY
- <http://www.zyxel.by>

**Belgium**

- ZyXEL Communications B.V.
- <http://www.zyxel.com/be/nl/>

**Bulgaria**

- ZyXEL България
- <http://www.zyxel.com/bg/bg/>

**Czech**

- ZyXEL Communications Czech s.r.o
- <http://www.zyxel.cz>

**Denmark**

- ZyXEL Communications A/S
- <http://www.zyxel.dk>

**Estonia**

- ZyXEL Estonia
- <http://www.zyxel.com/ee/et/>

**Finland**

- ZyXEL Communications
- <http://www.zyxel.fi>

**France**

- ZyXEL France
- <http://www.zyxel.fr>

**Germany**

- ZyXEL Deutschland GmbH
- <http://www.zyxel.de>

**Hungary**

- ZyXEL Hungary & SEE
- <http://www.zyxel.hu>

**Latvia**

- ZyXEL Latvia
- <http://www.zyxel.com/lv/lv/homepage.shtml>

## **Lithuania**

- ZyXEL Lithuania
- <http://www.zyxel.com/lt/lt/homepage.shtml>

## **Netherlands**

- ZyXEL Benelux
- <http://www.zyxel.nl>

## **Norway**

- ZyXEL Communications
- <http://www.zyxel.no>

## **Poland**

- ZyXEL Communications Poland
- <http://www.zyxel.pl>

## **Romania**

- ZyXEL Romania
- <http://www.zyxel.com/ro/ro>

## **Russia**

- ZyXEL Russia
- <http://www.zyxel.ru>

## **Slovakia**

- ZyXEL Communications Czech s.r.o. organizacna zlozka
- <http://www.zyxel.sk>

## **Spain**

- ZyXEL Spain
- <http://www.zyxel.es>

## **Sweden**

- ZyXEL Communications
- <http://www.zyxel.se>

## **Switzerland**

- Studerus AG
- <http://www.zyxel.ch/>

**Turkey**

- ZyXEL Turkey A.S.
- <http://www.zyxel.com.tr>

**UK**

- ZyXEL Communications UK Ltd.
- <http://www.zyxel.co.uk>

**Ukraine**

- ZyXEL Ukraine
- <http://www.ua.zyxel.com>

**Latin America****Argentina**

- ZyXEL Communication Corporation
- <http://www.zyxel.com/ec/es/>

**Ecuador**

- ZyXEL Communication Corporation
- <http://www.zyxel.com/ec/es/>

**Middle East****Egypt**

- ZyXEL Communication Corporation
- <http://www.zyxel.com/homepage.shtml>

**Middle East**

- ZyXEL Communication Corporation
- <http://www.zyxel.com/homepage.shtml>

**North America****USA**

- ZyXEL Communications, Inc. - North America Headquarters
- <http://www.us.zyxel.com/>

## Oceania

### Australia

- ZyXEL Communications Corporation
- <http://www.zyxel.com/au/en/>

## Africa

### South Africa

- Nology (Pty) Ltd.
- <http://www.zyxel.co.za>



# Legal Information

## Copyright

Copyright © 2014 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.

## Trademarks

Trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

## Certifications

### Federal Communications Commission (FCC) Interference Statement

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

## Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

## Viewing Certifications

Go to <http://www.zyxel.com> to view this product's documentation and certifications.

## ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies

by region. Check with your vendor and/or the authorized ZyXEL local distributor for details about the Warranty Period of this product. 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 your vendor. You may also refer to the warranty policy for the region in which you bought the device at [http://www.zyxel.com/web/support\\_warranty\\_info.php](http://www.zyxel.com/web/support_warranty_info.php).

#### **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.

### **Open Source Licenses**

This product contains in part some free software distributed under GPL license terms and/or GPL like licenses. Open source licenses are provided with the firmware package. You can download the latest firmware at [www.zyxel.com](http://www.zyxel.com). If you cannot find it there, contact your vendor or ZyXEL Technical Support at [support@zyxel.com.tw](mailto:support@zyxel.com.tw). To obtain the source code covered under those Licenses, please contact your vendor or ZyXEL Technical Support at [support@zyxel.com.tw](mailto:support@zyxel.com.tw).

### **Safety Warnings**

- To avoid possible eye injury, do NOT look into an operating fiber-optic module's connector.
- 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 it 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.
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.
- This product is for indoor use only (utilisation intérieure exclusivement).

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.



"PRODUCT COMPLIES WITH 21 CFR 1040.10 AND 1040.11"

"PRODUIT CONFORME SELON 21CFR 1040.10 ET 1040.11"

CLASS 1 LASER PRODUCT

APPAREIL À LASER DE CLASSE 1



# Index

## A

- ACS [115](#)
- activation
  - MAC address filter [54](#)
  - QoS [79](#)
  - UPnP [110](#)
  - wireless LAN [47](#)
  - WPS [52](#)
- anti-probing [129](#)
- applications
  - Internet access [10](#)
- authentication [58, 60](#)
  - RADIUS server [60](#)
- Auto Configuration Server, see ACS [115](#)

## B

- backup [147](#)
- Basic Service Set, see BSS
- blinking LEDs [11](#)
- BSS [61](#)
  - example [62](#)

## C

- call transfer [95](#)
- certifications [161](#)
  - notices [161](#)
  - viewing [161](#)
- channel, wireless LAN [58](#)
- configuration
  - wireless LAN [46, 47](#)
- contact information [155](#)
- copyright [161](#)
- CTS threshold [58](#)
- customer support [155](#)
- customized services [133, 134](#)

## D

- data fragment threshold [58](#)
- DDoS [128](#)
- default [148](#)
- default LAN IP address [15](#)
- Denials of Service, see DoS
- DHCP [123](#)
- diagnostic [149](#)
- disclaimer [161](#)
- DNS [107, 109](#)
- DoS [128](#)
  - thresholds [129](#)
- dynamic DNS [123](#)
- DYNDNS wildcard [123](#)

## E

- encapsulation [25](#)
  - PPP over Ethernet [25](#)
- encryption [60](#)
  - WEP [48](#)
    - key [49](#)
  - WPA-PSK [50, 51](#)
    - pre-shared key [50](#)

## F

- FCC interference statement [161](#)
- File Sharing [98](#)
- filters
  - MAC address [53, 59](#)
    - activation [54](#)
- firewalls [127](#)
  - actions [133](#)
  - address types [133](#)
  - anti-probing [129](#)
  - customized services [133, 134](#)

- DDoS [128](#)
- default action [130](#)
- DoS [128](#)
  - thresholds [129](#)
- ICMP [129](#)
- LAND attack [128](#)
- logs [131](#), [133](#)
- packet direction [130](#)
- Ping of Death [128](#)
- rules [135](#)
- security [136](#)
- SYN attack [128](#)
- firmware
  - upload [145](#)
  - upload error [146](#)
- flash key [94](#)
- flashing [94](#)
- fragmentation threshold [58](#)
- FTP [73](#)

## G

- general setup [137](#)

## H

- host [138](#)
- HTTP (Hypertext Transfer Protocol) [145](#)

## I

- ICMP [108](#), [129](#)
- IGMP [26](#)
- Internet access [10](#)
- Internet Control Message Protocol, see ICMP
- IP address [74](#)
- IP address assignment [25](#)
- IP pool [40](#), [41](#)

## L

- LAN setup [25](#), [39](#)
- LAND attack [128](#)
- limitations
  - wireless LAN [61](#)
  - WPS [68](#)
- log out [15](#)
- log out (automatic) [15](#)
- logs [141](#)
  - firewalls [131](#), [133](#)

## M

- MAC address [54](#)
  - filter [45](#), [53](#), [59](#)
- MAC address filter
  - activation [54](#)
- managing the device
  - good habits [9](#)
- MBSSID [62](#)
- multicast [26](#)
- multimedia [81](#)
- Multiple BSS, see MBSSID

## N

- NAT [76](#)
  - application [73](#)
  - definitions [71](#)
  - how it works [72](#)
  - remote management [104](#)
  - what it does [71](#)
- NAT (Network Address Translation) [71](#)
- non-proxy calls [90](#)

## P

- packet direction [130](#)
- PBC [63](#)
- phone book

- speed dial [90](#)
- PIN, WPS [53, 64](#)
  - example [65](#)
- Ping of Death [128](#)
- ports [11](#)
- PPPoE [25](#)
  - benefits [25](#)
- PPPoE (Point-to-Point Protocol over Ethernet) [25](#)
- preamble [58](#)
- pre-shared key [50](#)
- probing, firewalls [129](#)
- product registration [162](#)
- push button [13, 53](#)
- Push Button Configuration, see PBC
- push button, WPS [63](#)

## Q

- QoS [79](#)
  - activation [79](#)
- Quality of Service, see QoS
- Quick Start Guide [2](#)

## R

- RADIUS server [60](#)
- registration
  - product [162](#)
- related documentation [2](#)
- remote management
  - ICMP [108](#)
  - NAT [104](#)
  - Telnet [105](#)
  - TR-069 [115](#)
- remote management limitations [104](#)
- Remote Procedure Calls, see RPCs [115](#)
- resetting your device [12](#)
- restore [147](#)
- RFC 1631 [71](#)
- router features [10](#)
- RPPCs [115](#)
- RTS threshold [58](#)

## S

- security
  - network [136](#)
  - wireless LAN [58](#)
- Security Parameter Index, see SPI
- server [139](#)
- Service Set Identifier, see SSID
- services [74](#)
- Session Initiation Protocol [81](#)
- setup
  - wireless LAN [46, 47](#)
- SIP [81](#)
- SIP account [81](#)
- SIP identities [81](#)
- SIP number [81](#)
- SIP service domain [82](#)
- SIP URI [81](#)
- speed dial [90, 93](#)
- SPI [128](#)
- SSID [45, 47, 59](#)
  - MBSSID [62](#)
- static route [119](#)
- status
  - WPS [52](#)
- status indicators [11](#)
- SUA vs NAT [73](#)
- supplementary services [93](#)
- SYN attack [128](#)
- system name [138](#)
- system timeout [104](#)

## T

- Telnet [105](#)
- thresholds
  - data fragment [58](#)
  - DoS [129](#)
  - RTS/CTS [58](#)
- TR-069 [115](#)
  - ACS setup [115](#)
- trademarks [161](#)

**U**

Uniform Resource Identifier [81](#)  
Universal Plug and Play, see UPnP  
UPnP [109](#)  
    activation [110](#)  
    cautions [109](#)  
    example [110](#)  
    installation [110](#)  
    NAT traversal [109](#)

**V**

VoIP [81](#)  
VoIP features [11](#)

**W**

WAN (Wide Area Network) [25](#)  
warranty [161](#)  
    note [162](#)  
WDS [62](#)  
    example [63](#)  
Web Configurator [15](#)  
WEP [48, 60](#)  
    key [49](#)  
WiFi Protected Setup, see WPS  
wireless LAN [45, 57](#)  
    activation [47](#)  
    authentication [58, 60](#)  
    BSS [61](#)  
        example [62](#)  
    channel [58](#)  
    configuration [46, 47](#)  
    encryption [60](#)  
    example [57](#)  
    fragmentation threshold [58](#)  
    limitations [61](#)  
    MAC address filter [45, 53, 54, 59](#)  
    MBSSID [62](#)  
    preamble [58](#)  
    RADIUS server [60](#)  
    RTS/CTS threshold [58](#)  
    security [58](#)

SSID [45, 47, 59](#)  
WDS [62](#)  
    example [63](#)  
WEP [48, 60](#)  
    key [49](#)  
WPA [61](#)  
WPA-PSK [50, 51, 61](#)  
    pre-shared key [50](#)  
WPS [52, 63, 65](#)  
    activation [52](#)  
    adding stations [53](#)  
    example [66](#)  
    limitations [68](#)  
    PIN [53, 64](#)  
    push button [13, 53, 63](#)  
    status [52](#)  
WPA [61](#)  
WPA-PSK [50, 51, 61](#)  
    pre-shared key [50](#)  
WPS [52, 63, 65](#)  
    activation [52](#)  
    adding stations [53](#)  
    example [66](#)  
    limitations [68](#)  
    PIN [53, 64](#)  
        example [65](#)  
    push button [13, 53, 63](#)  
    status [52](#)