



ZXHN H108N

Home Gateway

Maintenance Management Manual

Version: V2.1

ZTE CORPORATION
NO. 55, Hi-tech Road South, ShenZhen, P.R.China
Postcode: 518057
Tel: +86-755-26771900
Fax: +86-755-26770801
URL: <http://ensupport.zte.com.cn>
E-mail: support@zte.com.cn

LEGAL INFORMATION

Copyright © 2012 ZTE CORPORATION.

The contents of this document are protected by copyright laws and international treaties. Any reproduction or distribution of this document or any portion of this document, in any form by any means, without the prior written consent of ZTE CORPORATION is prohibited. Additionally, the contents of this document are protected by contractual confidentiality obligations.

All company, brand and product names are trade or service marks, or registered trade or service marks, of ZTE CORPORATION or of their respective owners.

This document is provided “as is”, and all express, implied, or statutory warranties, representations or conditions are disclaimed, including without limitation any implied warranty of merchantability, fitness for a particular purpose, title or non-infringement. ZTE CORPORATION and its licensors shall not be liable for damages resulting from the use of or reliance on the information contained herein.

ZTE CORPORATION or its licensors may have current or pending intellectual property rights or applications covering the subject matter of this document. Except as expressly provided in any written license between ZTE CORPORATION and its licensee, the user of this document shall not acquire any license to the subject matter herein.

ZTE CORPORATION reserves the right to upgrade or make technical change to this product without further notice. Users may visit ZTE technical support website <http://ensupport.zte.com.cn> to inquire related information.

The ultimate right to interpret this product resides in ZTE CORPORATION.

Revision History

Revision No.	Revision Date	Revision Reason
R1.0	2012-11-30	First Edition

Serial Number: SJ-20121120142951-001

Publishing Date: 2012-11-30 (R1.0)

Contents

About This Manual	I
Chapter 1 Overview	1-1
1.1 Product Introduction	1-1
1.2 Product Features.....	1-1
1.3 Technical Specifications.....	1-2
Chapter 2 Configuration Preparations	2-1
2.1 Configuring TCP/IP	2-1
2.2 Logging In to the Device	2-2
Chapter 3 Basic Setup	3-1
3.1 Configuring the Wizard Parameters	3-1
3.2 Configuring the Internet Parameters	3-9
3.3 Wireless Configuration.....	3-17
3.3.1 Configuring Basic Wireless Parameters	3-17
3.3.2 Configuring Wireless Security	3-19
3.4 Configuring the Local Network	3-22
3.5 Configuring the Local IPv6 Network.....	3-29
3.6 Configuring the Time and Date.....	3-31
Chapter 4 Advanced Configuration	4-1
4.1 Advanced Wireless Configuration.....	4-1
4.1.1 Configuring Advanced Parameters	4-1
4.1.2 Configuring MAC Filtering.....	4-3
4.1.3 Configuring Security Parameters.....	4-5
4.1.4 Configuring the WPS	4-8
4.2 Configuring Port Forwarding	4-11
4.3 Configuring the DMZ	4-13
4.4 Configuring the SAMBA Service	4-14
4.5 Configuring the 3G WAN.....	4-15
4.6 Parental Control Configuration	4-17
4.6.1 Blocking Websites	4-17
4.6.2 Configuring MAC Filtering.....	4-19
4.7 Filtering Options Configuration	4-21
4.7.1 Configuring IP Filtering	4-21
4.7.2 Configuring Bridge Filtering.....	4-24

4.8 Qos Configuration	4-26
4.8.1 Configuring QoS Global Options.....	4-26
4.8.2 Configuring QoS Queues.....	4-26
4.8.3 Configuring QoS Classification.....	4-27
4.9 Configuring the Firewall	4-30
4.10 Configuring a DNS	4-31
4.11 Configuring a Dynamic DNS.....	4-32
4.12 Network Tools Configuration.....	4-33
4.12.1 Configuring Port Mapping	4-34
4.12.2 Configuring IGMP Proxy	4-35
4.12.3 Configuring IGMP Snooping.....	4-37
4.12.4 Configuring MLD	4-38
4.12.5 Configuring UPnP.....	4-39
4.12.6 Configuring the ADSL	4-39
4.12.7 Configuring the SNMP	4-40
4.12.8 Configuring the TR-064 Protocol	4-41
4.12.9 Configuring the TR-069 Protocol	4-42
4.12.10 Configuring Certificates.....	4-44
4.12.11 Configuring a Printer	4-46
4.13 Routing Configuration	4-47
4.13.1 Configuring a Static Route	4-47
4.13.2 Configuring an IPv6 Static Route	4-48
4.13.3 Configuring a Policy Route.....	4-49
4.13.4 Configuring the Default Gateway	4-50
4.13.5 Configuring the RIP	4-51
4.13.6 Configuring the RIPng Protocol	4-52
4.14 Configuring Schedules.....	4-53
4.15 Configuring NAT	4-55
4.16 Enabling DLNA	4-56
4.17 IP Tunnel Configuration	4-57
4.17.1 Configuring the 4in6 Tunnel	4-57
4.17.2 Configuring the 6in4 Tunnel	4-59
Chapter 5 System Management and Maintenance	5-1
5.1 Enabling Global IPv6.....	5-1
5.2 Configuring System Management.....	5-2
5.3 Updating the Firmware	5-3
5.4 Access Control Configuration.....	5-3

5.4.1 Managing Users	5-3
5.4.2 Configuring Services	5-5
5.4.3 Enabling IP Address Access Control Mode	5-6
5.5 Diagnosis	5-7
5.5.1 Implementing the DSL Test	5-7
5.5.2 Diagnosing a Trace Route.....	5-8
5.6 Configuring Logs	5-9
Chapter 6 Status Query.....	6-1
6.1 Viewing the Device Information	6-1
6.2 Viewing the Information on Wireless Clients.....	6-2
6.3 Viewing the Information on DHCP Clients	6-3
6.4 Viewing the IPv6 Status	6-3
6.5 Viewing System Logs	6-4
6.6 Viewing the Statistics Information	6-5
6.7 Viewing the IPv4 Route Information.....	6-6
6.8 Viewing the IPv6 Route Information.....	6-6
Glossary	I

About This Manual

Purpose

This manual describes how to configure and maintain the ZXHN H108N.

Intended Audience

This document is intended for:

- Network planning engineers
- Installation debugging engineers
- On-site maintenance engineers
- Network monitoring engineers
- System maintenance engineers
- Data configuration engineers

What Is in This Manual



This manual contains the following chapters:

Chapter	Summary
1, Overview	Describes the product features and technical specifications.
2, Configuration Preparations	Describe the TCP/IP configuration and login procedure.
3, Basic Setup	Describe the internet configuration, wireless configuration, local network configuration, local IPv6 network configuration, time and date configuration.
4, Advanced Configuration	Describe the advanced configuration of wireless, port forwarding, DMZ, SAMBA, 3G WAN, parental control, filtering options, QoS, firewall, DNS, DDNS, network tools, routing, schedules, NAT, DLNA, and IP tunnel.
5, System Management and Maintenance	Describe how to manage and maintain the device.
6, Status Query	Describe how to view the device status.

Conventions

This manual uses the following typographical conventions:

Typeface	Meaning
Italics	Variables in commands. It may also refer to other related manuals and documents.
Bold	Menus, menu options, function names, input fields, option button names, check boxes, drop-down lists, dialog box names, window names, parameters, and commands.

Typeface	Meaning
Constant width	Text that you type, program codes, filenames, directory names, and function names.
[]	Optional parameters.
{ }	Mandatory parameters.
	Separates individual parameters in a series of parameters.
	Danger: indicates an imminently hazardous situation. Failure to comply can result in death or serious injury, equipment damage, or site breakdown.
	Warning: indicates a potentially hazardous situation. Failure to comply can result in serious injury, equipment damage, or interruption of major services.
	Caution: indicates a potentially hazardous situation. Failure to comply can result in moderate injury, equipment damage, or interruption of minor services.
	Note: provides additional information about a certain topic.

Chapter 1

Overview

Table of Contents

Product Introduction	1-1
Product Features.....	1-1
Technical Specifications	1-2

1.1 Product Introduction

The ZXHN H108N is an Asymmetric Digital Subscriber Line ([ADSL](#)) access device that supports multiple line modes for BHS. It has the following features:

- It supports ADSL2/ADSL2+ and is backward compatible to ADSL, and provides auto-negotiation capability for different standards (G.dmt, T1.413 Issue 2) according to the settings on the central office Digital Subscriber Line Access Multiplexer ([DSLAM](#)).
- It provides four 10/100Base-T Ethernet interfaces and one Universal Serial Bus ([USB](#)) 2.0 Host interface.
- It supports Institute of Electrical and Electronics Engineers ([IEEE](#)) 802.11 b/g/n Wi-Fi interfaces.
- It provides broadband connection to the Internet by using high-speed ADSL connection.
- It provides secure wireless encryption modes and firewall to protect network security, and supports remote network management through TR-069 and Web Graphical User Interface ([GUI](#)).

1.2 Product Features

The ZXHN H108N has the following features:

- Supports G.dmt, T1.413, ADSL2, READSL2, and ADSL2+.
- Provides the 10/100BaseT Ethernet interface (MDI/MDIX).
- Supports [IEEE](#) 802.11 b/g/n.
- Supports [USB](#) 2.0 Host.
- Supports Bridge or Router mode.
- Provides high reliability, easy to operate, low power consumption.
- Supports Network Address Translation ([NAT](#)) and Port Address Translation ([PAT](#)).
- Supports the TR069 protocol.
- Supports configuration through web pages.
- Supports the Dynamic Host Configuration Protocol ([DHCP](#)) server.
- Supports virtual server.

- Supports configuration file backup to the local computer and uploading the saved file to the ZXHN H108N.
- Supports a wide input voltage range, which can reach 100V-240V (base on the linear power supply).

1.3 Technical Specifications

Table 1-1 lists the ZXHN H108N technical specifications.

Table 1-1 Technical Specifications

Item	Specification
Dimensions	140 mm (width) × 38 mm (height) × 186 mm (depth) (ZXHN H108N case) 155 mm (width) × 90 mm (height) × 275 mm (depth)
Weight	256 g (not including the attachment and power supply) 715 g (including attachment and power supply)
Input voltage	100 V–240 V AC 50/60Hz
Rated voltage	12 V DC
Rated current	1 A
Working temperature	0°C–40°C
Working humidity	20%–90%
Storage temperature	–40°C to 60°C

Chapter 2

Configuration Preparations

Table of Contents

Configuring TCP/IP	2-1
Logging In to the Device	2-2

2.1 Configuring TCP/IP

This procedure describes how to configure **TCP/IP**.

Context

The computer address needs to be configured in the same network segment as the ZXHN H108N address so that the ZXHN H108N device can access the ZXHN H108N.

The default network settings for the ZXHN H108N are as follows:

- IP address: 192.168.1.33
- Subnet mask: 255.255.255.0
- Default gateway: 192.168.1.1

Steps

1. Configure TCP/IP.
 - a. In the **Local Area Connection Properties** dialog box, select **Internet Protocol (TCP/IP)**.
 - b. Click **Properties**. The **Internet Protocol (TCP/IP) Properties** dialog box is displayed.
 - c. Select **Use the following IP address**. Set **IP address**, **Subnet mask**, and **Default gateway**. For example, set the IP address to 192.168.1.33, the subnet mask to 255.255.255.0, and the default gateway to 192.168.1.1.
 - d. Click **OK**.



Note:

The settings may change with the network requirements.

2. Check the TCP/IP settings.

Use the **Ping** command to check the connection between the computer and ZXHN H108N.

If the computer fails to ping the ZXHN H108N, verify the following:

- The Ethernet cable between the ZXHN H108N and the computer is correctly connected.
- The ZXHN H108N is powered on.
- The network adapter driver is correctly installed on the computer.
- The TCP/IP settings on the computer are correctly configured.

– End of Steps –

2.2 Logging In to the Device

You can configure the ZXHN H108N through web pages.

Prerequisite

The ZXHN H108N is properly connected and the computer is correctly configured.

Context

Web pages provide different configuration permissions for different users. For the user permissions, refer to [Table 2-1](#).

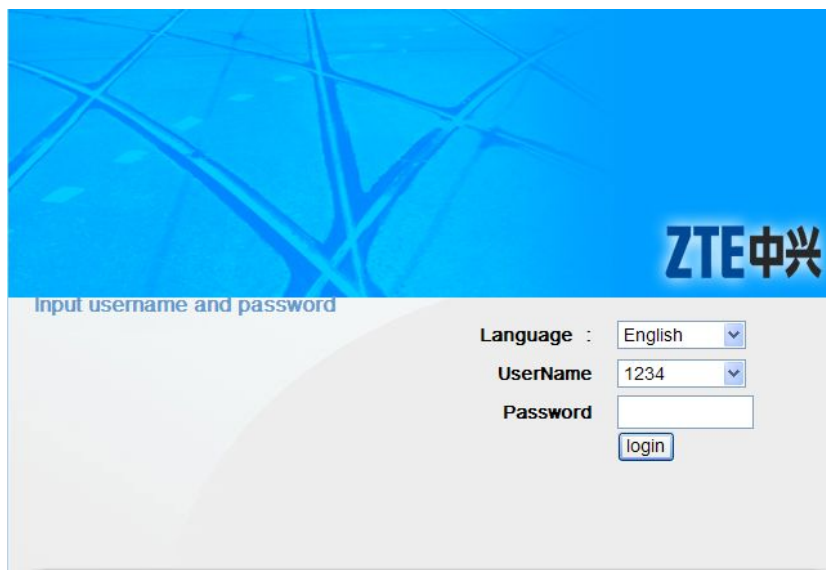
Table 2-1 User Permissions

Role	User Name/Password	Permission
Administrator	1234/1234	Has all the configuration permissions on the web pages.
Common users	user/user	Have the permission of viewing some configurations.

Steps

1. Open the web browser.
2. In the address bar, enter `http://192.168.1.1:8000`, which is the default IP address of the ZXHN H108N, and then press **Enter**. The login page is displayed, see [Figure 2-1](#).

Figure 2-1 Login Page



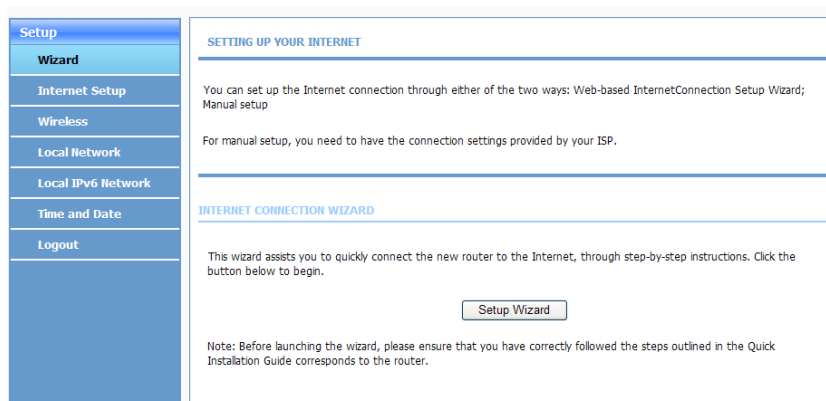
3. From the **Language** list, select a language. From the **UserName** list, select a user name. In the **Password** text box, enter the password.

**Note:**

The default user name and password for the administrator are both 1234.

4. Click **login**. The ZXHN H108N home page is displayed, see [Figure 2-2](#).

Figure 2-2 ZXHN H108N Web Page



– End of Steps –

This page intentionally left blank.

Chapter 3

Basic Setup

Table of Contents

Configuring the Wizard Parameters.....	3-1
Configuring the Internet Parameters.....	3-9
Wireless Configuration	3-17
Configuring the Local Network.....	3-22
Configuring the Local IPv6 Network.....	3-29
Configuring the Time and Date	3-31

3.1 Configuring the Wizard Parameters

If you configure a router for the first time, you can click **Setup Wizard** for the configuration guidance.

Context

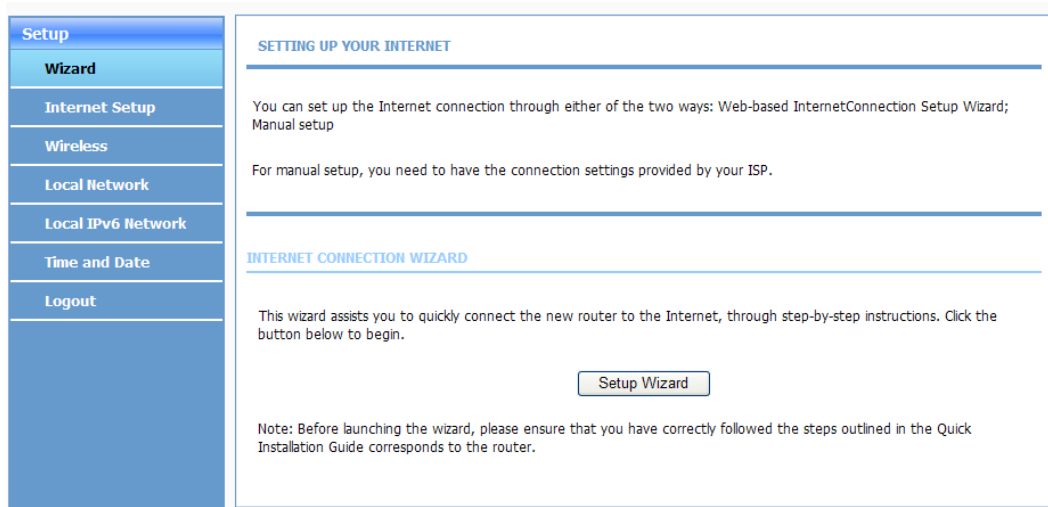
The ZXHN H108N supports the following Internet connection modes:

- Point to Point Protocol over Ethernet ([PPPoE](#))
- Point to Point Protocol over ATM ([PPPoA](#))
- Dynamic IP address
- Static IP address
- Bridge

Steps

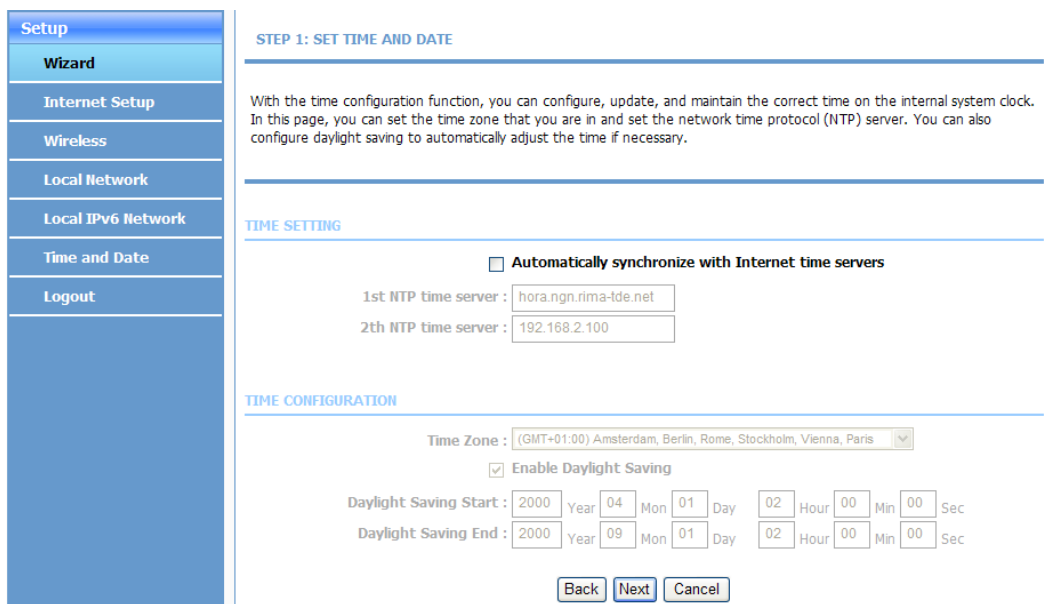
1. Select **Setup > Wizard**. The **SETTING UP YOUR INTERNET** page is displayed, see [Figure 3-1](#).

Figure 3-1 SETTING UP YOUR INTERNET Page



2. Click **Setup Wizard**. The **WELCOME TO SETUP WIZARD** page is displayed.
3. Click **Next**. The **STEP 1: SET TIME AND DATE** page is displayed, see [Figure 3-2](#).

Figure 3-2 SET TIME AND DATE Page



4. (Optional) Configure the time and date parameters. For a description of the parameters, refer to [Table 3-1](#).

Table 3-1 Parameter Descriptions for Time and Date Configuration

Parameter	Description
Automatically synchronize with Internet time server	Automatically synchronizes with the Internet time server.
1st NTP time server	Primary time server address.
2nd NTP time server	Secondary time server address.

Parameter	Description
Current Local Time	–
Time Zone	Time zone.
Enable Daylight Saving	Whether to enable the daylight saving function.
Daylight Saving Start	Starting time of the daylight saving period.
Daylight Saving End	Ending time of the daylight saving period.

5. Click **Next**. The **STEP 2: SETUP INTERNET CONNECTION** page is displayed, see [Figure 3-3](#).

Figure 3-3 SETUP INTERNET CONNECTION Page

6. Configure the network connection parameters.
- **PPPoE**
From the **Protocol** list, select **PPPoE**. Configure the network connection parameters, see [Figure 3-4](#).

Figure 3-4 SETUP INTERNET CONNECTION Page-PPPoE

STEP 2: SETUP INTERNET CONNECTION

Please select your ISP (Internet Service Provider) from the list below.

Protocol:

Encapsulation Mode:

VPI: (0-255)

VCI: (32-65535)

Search Available PVC:

PPPOE/PPPOA

Please enter the user name and password provided by your Internet service provider (ISP). Note that the information is case-sensitive. Click "Next" to continue.

Username:

Password:

Confirm Password:

For a description of the connection parameters, refer to [Table 3-2](#).

Table 3-2 PPPoE Connection Parameter Descriptions

Parameter	Description
Protocol	→ PPPoE → PPPoA → Dynamic IP → Static IP → Bridge
Encapsulation Mode	→ VC-Mux → LLC
VPI	Virtual path identifier.
VCI	Virtual channel identifier, 16 bits, indicating a virtual channel in a virtual path. A VPI and a VCI are used together to indicate a virtual connection.
Search Available PVC	To search for available PVCs, click Scan .
Username	User name provided by the Internet Service Provider (ISP).
Password/Confirm Password	User password provided by the ISP.

- PPPoA

From the **Protocol** list, select **PPPoA**. Configure the network connection parameters. For a description of the connection parameters, refer to [Table 3-2](#).

- Dynamic IP

From the **Protocol** list, select **Dynamic IP**. Configure the network connection parameters, see [Figure 3-5](#).

Figure 3-5 Configuring Dynamic IP Network Connection—Dynamic IP

STEP 2: SETUP INTERNET CONNECTION

Please select your ISP (Internet Service Provider) from the list below.

Protocol:

Encapsulation Mode:

VPI: (0-255)

VCI: (32-65535)

Search Available PVC:

For a description of the connection parameters, refer to [Table 3-2](#).

- Static IP

From the **Protocol** lists, select **Static IP**. Configure the network connection parameters, see [Figure 3-6](#).

Figure 3-6 Configuring Static IP Network Connection—Static IP

STEP 2: SETUP INTERNET CONNECTION

Please select your ISP (Internet Service Provider) from the list below.

Protocol :

Encapsulation Mode:

VPI : (0-255)

VCI : (32-65535)

Search Available PVC :

STATIC IP

You have selected Static IP Internet connection. Please enter the appropriate information as provided by your ISP.

To guarantee the performance of the auto PVC scan feature, please enter the information of VPI/VCI numbers if your ISP has provided it.

Click Next to continue.

IP Address :

Subnet Mask :

Default Gateway :

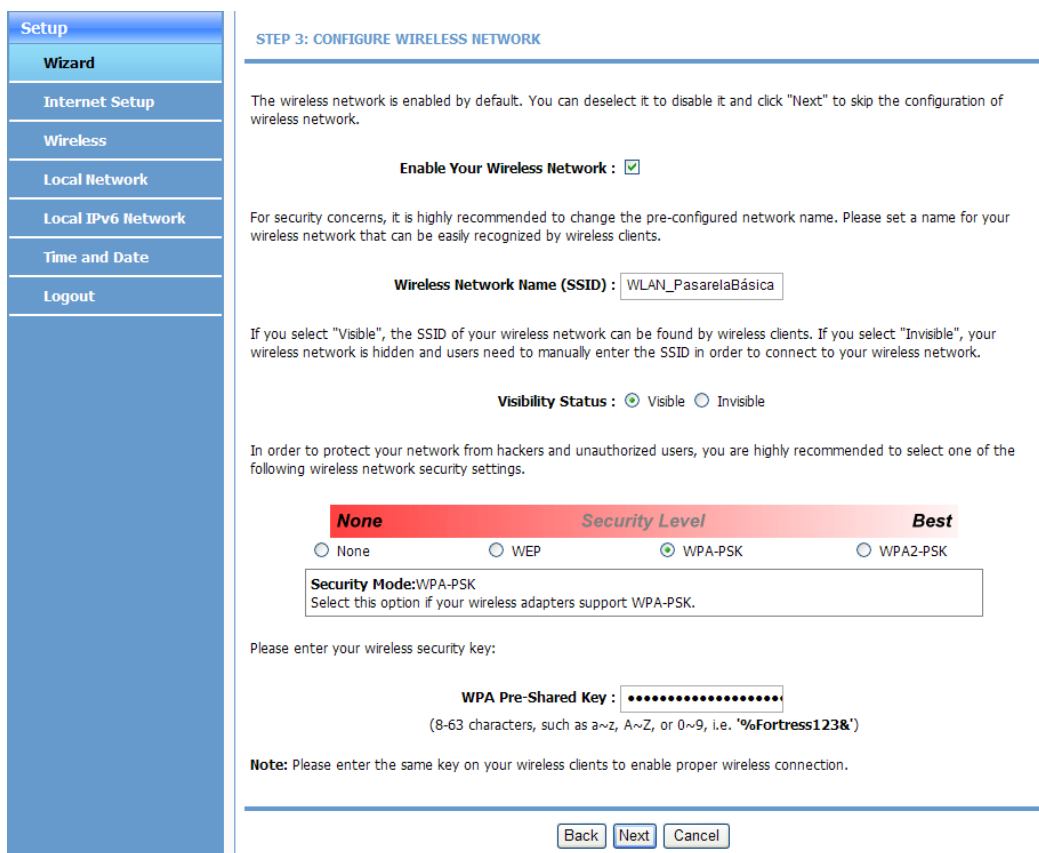
Primary DNS Server :

- Bridge

From the **Protocol** lists, select **Bridge**. Configure the network connection parameters. For a description of the connection parameters, refer to [Table 3-2](#).

7. Click **Next**. The **STEP3: CONFIGURE WIRELESS NETWORK** page is displayed, see [Figure 3-7](#).

Figure 3-7 CONFIGURE WIRELESS NETWORK Page



8. Configure the wireless network parameters.

For a description of the wireless network parameters, refer to [Table 3-3](#).

Table 3-3 Wireless Network Parameter Descriptions

Parameter	Description
Enable Your Wireless Network	The wireless network is enabled by default. You can clear the check box to disable it and click Next to skip the configuration of the wireless network.
Wireless Network Name (SSID)	For security purpose, it is recommended to change the pre-configured network name.
Visibility Status	If Visibility Status is set to Visible , the SSID of the wireless network can be found by wireless clients. If Visibility Status is Invisible , the wireless network is hidden and users need to manually enter the SSID in order to connect to the wireless network.

Parameter	Description
Security Level	<ul style="list-style-type: none"> ● None No security level is enabled. ● WEP Wireless adapters only support WEP and do not support WPA. ● WPA-PSK Wireless adapters support WPA-PSK. ● WPA2-PSK Wireless adapters support WPA2-PSK.
WEP Key/WPA Pre-Shared Key/WPA2 Pre-Shared Key	The key should be the same as that on the wireless client for proper wireless connections.

- Click **Next**. The **STEP4: COMPLETED AND RESTART** page is displayed, see [Figure 3-8](#).

Figure 3-8 COMPLETED AND RESTART Page

STEP 4: COMPLETED AND RESTART

The setup is complete. Click "Back" to review or modify the settings.

If the Internet connection does not work, try the Setup Wizard again with alternative settings, or use manual setup instead if you have the Internet connection details provided by your ISP.

SETUP SUMMARY

The following shows a detailed summary of your settings. Please print this page out or write the information on a piece of paper, and save it, so you can correctly configure the settings on your wireless client adapters later based on the information in this page.

Time Settings :	1
NTP Server 1 :	hora.ngn.rima-tde.net
NTP Server 2 :	192.168.2.100
Time Zone :	CET
Daylight Saving Time :	1
VPI / VCI :	8/35
Protocol :	PPPoE
Connection Type :	LLC
Username :	user
Password :	****
Wireless Network Name (SSID) :	SSID1
Visibility Status :	1
Encryption :	WPA
Pre-Shared Key :	*****
WEP Key :	

- Click **Apply**.
– End of Steps –

3.2 Configuring the Internet Parameters

You can configure an Asynchronous Transfer Mode (ATM) PVC identifier (VPI/VCI) and select a service category.

Steps

1. Select **Setup > Internet Setup**. The **INTERNET SETUP** page is displayed, see [Figure 3-9](#).

Figure 3-9 INTERNET SETUP Page

The screenshot shows the 'INTERNET SETUP' page. On the left is a navigation menu with 'Internet Setup' selected. The main content area has a title 'INTERNET SETUP' and instructions: 'Choose "Add", "Edit", or "Delete" to configure WAN interfaces.' Below this is a section titled 'WAN SETUP' containing a table with the following data:

	VPI/VCI	VLAN ID	ENCAP	Service Name	Protocol	State	Status	Backup3G	Action
<input type="checkbox"/>	8/35	0	LLC	PVC:8/35	IPoA	1	Disconnected	0	-
<input type="checkbox"/>	8/36	0	LLC	PVC:8/36	PPPoE	1	Disconnected	1	Connect

Below the table are buttons for 'Add', 'Edit', and 'Delete'.

2. Click **Add**. The configuration page for a new Internet connection is displayed, see [Figure 3-10](#).

Figure 3-10 INTERNET SETUP Page—New Internet Connection Configuration

The screenshot shows the 'INTERNET SETUP' page for a new connection. The navigation menu is on the left. The main content area has a title 'INTERNET SETUP' and instructions: 'In this page, you can configure an ATM PVC identifier (VPI and VCI) and select a service category.' Below this is a section titled 'ATM PVC CONFIGURATION' with the following fields:

- VPI: 0 (0-255)
- VCI: 35 (32-65535)
- Service Category: UBR With PCR (dropdown)
- Peak Cell Rate: 0 (cells/s)
- Sustainable Cell Rate: 0 (cells/s)
- Maximum Burst Size: 0 (cells)

Below this is a section titled 'CONNECTION TYPE' with the following fields:

- Protocol: Bridging (dropdown)
- Encapsulation Mode: LLC (dropdown)
- 802.1Q VLAN ID: 0 (0 = disable, 1 - 4094)
- Priority: 0 (0 - 7)
- Enable QinQ:
- Firewall Enable:
- Enable Proxy Arp:

At the bottom are buttons for 'Apply' and 'Cancel'.

3. In the **ATM PVC CONFIGURATION** area, configure the parameters. For a description of the parameters, refer to [Table 3-4](#).

Table 3-4 Parameter Descriptions for ATM PVC Configuration

Parameter	Description
VPI	Virtual path identifier
VCI	Virtual channel identifier, 16 bits, indicating a virtual channel in a virtual path A VPI and a VCI are used together to indicate a virtual connection.
Service Category	Service type in the ATM QoS configuration for uplink traffic control. Five service types are supported: <ul style="list-style-type: none"> ● UBR Without PCR ● UBR With PCR ● CBR ● Non Realtime VBR ● Realtime VBR
Peak Cell Rate	QoS threshold value
Sustainable Cell Rate	Sustainable cell rate
Maximum Burst Size	Maximum burst size

4. Configure the connection type parameters.

The ZXHN H108N supports five types of protocols.

- PPP over ATM (PPPoA)
 - i. From the **Protocol** list, select **PPP over ATM (PPPoA)**. Configure the connection type parameters of the PPPoA protocol.

Figure 3-11 CONNECTION TYPE Area–PPPoA

CONNECTION TYPE

Protocol: PPP over ATM (PPPoA)

Encapsulation Mode: LLC

802.1Q VLAN ID: 0 (0 = disable, 1 - 4094)

Priority: 0 (0 - 7)

Enable QinQ:

Firewall Enable:

Enable Proxy Arp

For a description of the PPPoA connection type parameters, refer to [Table 3-5](#).

Table 3-5 Parameter Descriptions for the PPPoA Connection Type

Parameter	Description
Protocol	Connection protocol
Encapsulation Mode	Encapsulation type of IP packets: → VCMUX → LLC
Firewall Enable	Whether to enable the firewall

- ii. Configure the PPP parameters of the PPPoA protocol.

Figure 3-12 PPP USERNAME AND PASSWORD Area–PPPoA

PPP USERNAME AND PASSWORD

PPP Username :

PPP Password :

Confirm PPP Password :

Authentication Method : AUTO

Dial-up mode : AlwaysOn

Inactivity Timeout : 100 (Seconds [0-65535])

MRU Size : 1492 (576~1492)

MTU Size : 1400 (576~1492)

Keep Alive :

Lcp Echo Interval (sec) : 30

Lcp Echo Failure : 5

Use Static IP Address :

IP Address :

Enable NAT :

NAT Type : Full Cone Nat

Enable WAN Service :

Service Name : pppoa_0_35_0_6_Internet_

For a description of the PPP parameters, refer to [Table 3-6](#).

Table 3-6 PPP Parameter Descriptions

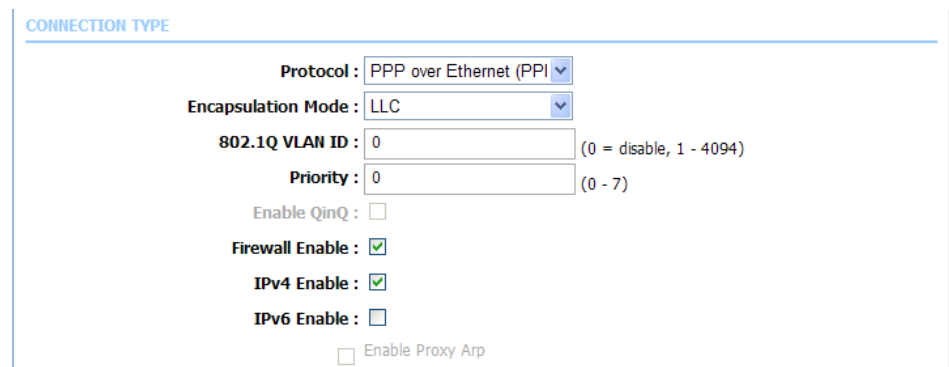
Parameter	Description
PPP Username	PPPoE/PPPoA user name, which is provided by the ISP.
PPP Password/Confirm PPP Password	PPPoE/PPPoA user password, which is provided by the ISP.
Authentication Method	Authentication method, including AUTO, PAP, CHAP, and MS-CHAP. By default, it is AUTO.

Parameter	Description
Dial-up mode	Dial-up mode, including the following: <ul style="list-style-type: none"> → AlwaysOn: When the configuration is complete, the system gets online automatically and keeps online. → OnDemand: If there is no data flow in the connection channel during the inactivity timeout period, the connection is interrupted automatically. If there are data flows during the inactivity timeout period, the connection is recovered automatically. → Manual: The subscriber gets online through manual dial-up accordingly.
Inactivity Timeout	If there is no data flow in the connection channel during the inactivity timeout period, the connection is interrupted automatically. If there are data flows during the inactivity timeout period, the connection is recovered automatically.
MRU Size	Maximum receive unit size.
MTU Size	Maximum transfer unit size.
Keep Alive	Sends Keep Alive packets to the NE periodically.
Lcp Echo Interval (sec)	Interval of sending the Echo Request packet.
Lcp Echo Failure	If a packet is not responded to during this time period, the packet is considered failed.
Use Static IP Address	Uses the static IP address.
IP Address	Static IP address.
Enable NAT	When multiple computers in a Local Area Network (LAN) share one IP address to access the Internet, Network Address Translation (NAT) is used to translate each private network address to the public network address of the Wide Area Network (WAN) port.
NAT Type	<ul style="list-style-type: none"> → Symmetric Nat → Full Cone Nat
Enable WAN Service	Whether to enable the WAN service. If the WAN service is not enabled, the WAN link cannot obtain an IP address.
Service Name	WAN link name.

iii. Select **Backup 3G Enable**, see [Figure 3-13](#).

Figure 3-13 3G CONNECTION BACKUP SETTINGS Area

- PPP over Ethernet (PPPoE)
 - i. From the **Protocol** list, select **PPP over Ethernet (PPPoE)** . Configure the connection type parameters of the PPPoE protocol, see [Figure 3-14](#).

Figure 3-14 CONNECTION TYPE Area-PPPoE

For a description of the PPPoE connection type parameters, refer to [Table 3-7](#).

Table 3-7 Parameter Descriptions for the PPPoE Connection Type

Parameter	Description
Protocol	Connection protocol
Encapsulation Mode	Encapsulation type of the IP packets → VCMUX → LLC
802.1Q VLAN ID	VLAN ID
Priority	802.1P priority
Firewall Enable	Whether to enable the firewall
IPv4 Enable	Whether to enable Internet Protocol version 4 (IPv4)
IPv6 Enable	Whether to enable Internet Protocol version 6 (IPv6)

- ii. Configure the PPP parameters of the PPPoE protocol.
For a description of the PPP parameters, refer to [Table 3-6](#).
 - iii. Select **Backup 3G Enable**, see [Figure 3-13](#).
- MAC Encapsulation Routing (MER)

- i. From the **Protocol** list, select **MAC Encapsulation Routing (MER)**. Configure the connection type parameters of the MER protocol, see [Figure 3-15](#).

Figure 3-15 CONNECTION TYPE Area–MER

The screenshot shows the 'CONNECTION TYPE' configuration page for the MER protocol. The fields are as follows:

- Protocol: MAC Encapsulation Ro
- Encapsulation Mode: LLC
- 802.1Q VLAN ID: 0 (0 = disable, 1 - 4094)
- Priority: 0 (0 - 7)
- Enable QinQ:
- Firewall Enable:
- IPv4 Enable:
- IPv6 Enable:
- Enable Proxy Arp:

For a description of the MER connection type parameters, refer to [Table 3-8](#).

Table 3-8 Parameter Descriptions for the MER Connection Type

Parameter	Description
Protocol	Connection protocol
Encapsulation Mode	Encapsulation type of IP packets: → VCMUX → LLC
802.1Q VLAN ID	VLAN ID
Priority	802.1P priority
Firewall Enable	Whether to enable the firewall
IPv4 Enable	Whether to enable IPv4
IPv6 Enable	Whether to enable IPv6
Enable Proxy Arp	Whether to enable proxy Whether to enable ARP

- ii. In the **WAN IP SETTINGS** area, configure the WAN IP address parameters, see [Figure 3-16](#).

Figure 3-16 WAN IP SETTINGS Area

WAN IP SETTINGS

Obtain address automatically
 Use the following address :

WAN IP Address :
 WAN Subnet Mask :
 Default gateway :
 Preferred DNS server :
 Alternate DNS server :

Enable NAT :
 NAT Type :

Enable WAN Service :
 Service Name :

For a description of the parameters, refer to [Table 3-9](#).

Table 3-9 Parameter Descriptions for the WAN IP Settings

Parameter	Description
Obtain address automatically	Obtains the IP address automatically.
Use the following address	Uses the static IP address.
WAN IP Address	WAN IP address.
WAN Subnet Mask	Subnet mask.
Default gateway	Default gateway.
Preferred DNS server	Primary Domain Name Server (DNS) server address.
Alternate DNS server	Secondary DNS server address.
Enable NAT	When multiple computers in a LAN share one IP address to access the Internet, NAT is used to translate each private network address to the public network address of the WAN port.
NAT Type	→ Symmetric Nat → Full Cone Nat
Enable WAN Service	Whether to enable the WAN service. If the WAN service is not enabled, the WAN link cannot obtain an IP address.
Service Name	WAN link name.

iii. Select **Backup 3G Enable**, see [Figure 3-13](#).

- IP over ATM (IPoA)
 - i. From the **Protocol** list, select **IP over ATM (IPoA)**. Configure the connection type parameters of the IPoA protocol, see [Figure 3-17](#).

Figure 3-17 CONNECTION TYPE Area–IPoA

The screenshot shows the 'CONNECTION TYPE' configuration window. The 'Protocol' dropdown is set to 'IP over ATM (IPoA)'. The 'Encapsulation Mode' dropdown is set to 'LLC'. The '802.1Q VLAN ID' text box contains '0' with a note '(0 = disable, 1 - 4094)'. The 'Priority' text box contains '0' with a note '(0 - 7)'. There are three checkboxes: 'Enable QinQ' (unchecked), 'Firewall Enable' (checked), and 'Enable Proxy Arp' (unchecked).

For a description of the IPoA connection type parameters, refer to [Table 3-5](#).

- ii. In the **WAN IP SETTINGS** area, configure the WAN IP address parameters, see [Figure 3-16](#).
For a description of the WAN IP address parameters, refer to [Table 3-9](#).
- iii. Select **Backup 3G Enable**, see [Figure 3-13](#).

- Bridging

From the **Protocol** list, select **Bridging**. Configure the connection type parameters of the Bridging protocol, see [Figure 3-18](#).

Figure 3-18 CONNECTION TYPE Area–Bridging

The screenshot shows the 'CONNECTION TYPE' configuration window. The 'Protocol' dropdown is set to 'Bridging'. The 'Encapsulation Mode' dropdown is set to 'LLC'. The '802.1Q VLAN ID' text box contains '0' with a note '(0 = disable, 1 - 4094)'. The 'Priority' text box contains '0' with a note '(0 - 7)'. There are three checkboxes: 'Enable QinQ' (unchecked), 'Firewall Enable' (checked), and 'Enable Proxy Arp' (unchecked). At the bottom, there are 'Apply' and 'Cancel' buttons.

For a description of the Bridging connection type parameters, refer to [Table 3-10](#).

Table 3-10 Parameter Descriptions for the Bridging Connection Type

Parameter	Description
Protocol	Connection protocol

Parameter	Description
Encapsulation Mode	Encapsulation type of the IP packets: → VCMUX → LLC
802.1Q VLAN ID	VLAN ID
Priority	802.1P priority
Enable QinQ	Whether to enable QinQ
Firewall Enable	Whether to enable the firewall
Enable Proxy Arp	Whether to enable proxy ARP

5. Click **Apply**.
6. (Optional) To modify the network connection configurations, click **Edit**.
7. (Optional) To delete the network connection configurations, click **Delete**.

– End of Steps –

3.3 Wireless Configuration

Wireless configuration includes the following:

- Wireless basic configuration
- Wireless security configuration

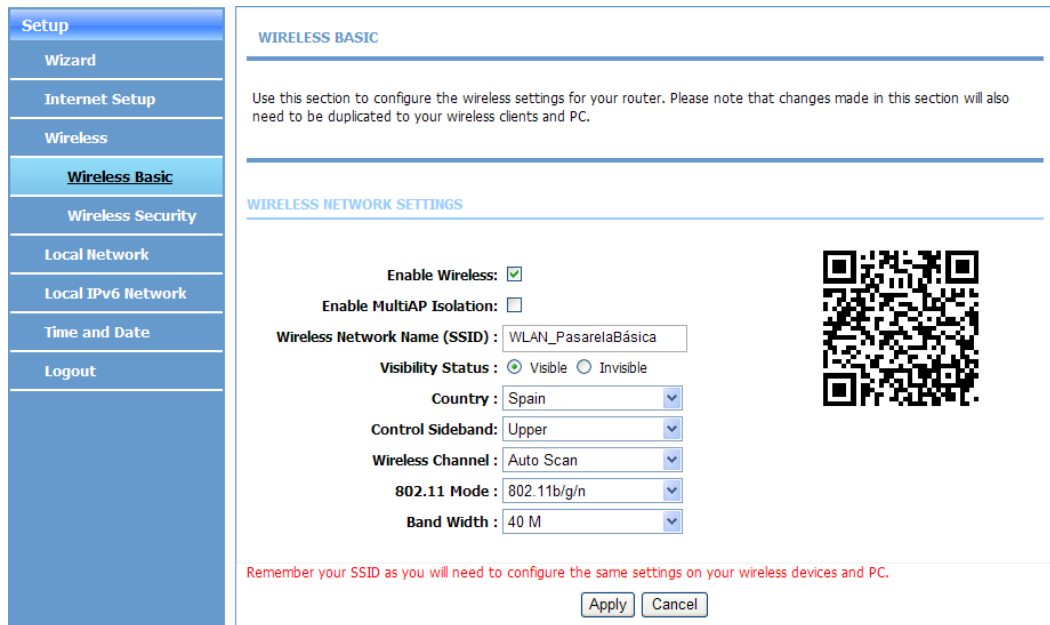
3.3.1 Configuring Basic Wireless Parameters

This procedure describes how to configure basic wireless parameters.

Steps

1. Select **Setup > Wireless > Wireless Basic**. The **WIRELESS BASIC** page is displayed, see [Figure 3-19](#).

Figure 3-19 WIRELESS BASIC Page



2. Configure the wireless basic parameters. For a description of the parameters, refer to Table 3-11.

Table 3-11 Wireless Basic Parameter Descriptions

Parameter	Description
Enable Wireless	Whether to enable wireless
Enable MultiAP Isolation	Whether to enable isolation between multiple SSIDs
Wireless Network Name (SSID)	SSID name
Visibility Status	<ul style="list-style-type: none"> ● Visible ● Invisible
Country	Country or region
Control Sideband	<ul style="list-style-type: none"> ● Upper ● Lower
Wireless Channel	Wireless channel, with the default of Auto Scan
802.11 Mode	<ul style="list-style-type: none"> ● 802.11b ● 802.11g ● 802.11n ● 802.11b/g ● 802.11n/g ● 802.11b/g/n
Band Width	<ul style="list-style-type: none"> ● 20M ● 40M ● 20M/40M

3. Click **Apply**.
– End of Steps –

3.3.2 Configuring Wireless Security

The ZXHN H108N supports three wireless security modes, including Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and WPA2. WEP is the basic wireless encryption standard. WPA and WPA2 provide higher levels of security.

None Security Mode

1. Select **Setup > Wireless > Wireless Security**. The **WIRELESS SECURITY** page is displayed, see [Figure 3-20](#).

Figure 3-20 WIRELESS SECURITY Page

WIRELESS SECURITY

In this page, you can configure the wireless security settings for the router. Please note that changes made in this page must also be duplicated to your wireless clients and PC.

WIRELESS SECURITY MODE

To protect your privacy, you can configure wireless security features. The device supports 3 wireless security modes including: WEP, WPA, and WPA2. WEP is the original wireless encryption standard. WPA and WPA2 provide higher levels of security.

Security Mode:

WPA Encryption:

WPA

Select **WPA** or **WPA2** to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. The strongest cipher that the client supports is used. For the highest security, select **WPA2 Only**. This mode uses AES (CCMP) cipher and legacy stations are not allowed to access with WPA security. For maximum compatibility, select **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance, select **WPA2 Only** (which uses AES cipher).

WPA-PSK does not require an authentication server. The WPA option requires an external RADIUS server.

WPA Mode:

Group Key Update Interval:

PRE-SHARED KEY

Pre-Shared Key:

Remember your SSID and the security key as you will need to configure the same settings on your wireless devices and PC.

2. From the **Security Mode** list, select **None**.
3. Click **Apply**.

WEP Security Mode

1. Select **Setup > Wireless > Wireless Security**. The **WIRELESS SECURITY** page is displayed.
2. From the **Security Mode** list, select **WEP**, see [Figure 3-21](#).

Figure 3-21 WEP Parameter Configuration Area

WIRELESS SECURITY MODE

To protect your privacy, you can configure wireless security features. The device supports 3 wireless security modes including: WEP, WPA, and WPA2. WEP is the original wireless encryption standard. WPA and WPA2 provide higher levels of security.

Security Mode :

WEP

If you select WEP, the device operates **ONLY** in **Legacy Wireless mode (802.11B/G)**.

WEP is the wireless encryption standard. To use it, you must enter the same key(s) on the router and the wireless stations. A 64-bit key consists of 10 hexadecimal digits and a 128-bit key consists of 26 hexadecimal digits. A hexadecimal digit is a number from 0 to 9 or a letter from A to F. For the most secure use of WEP, set the authentication type to "Shared Key".

You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. A maximum of 5 text characters can be entered for 64 bit keys, and a maximum of 13 characters for 128 bit keys.

WEP Key Length :

Choose WEP Key :

WEP Key1 :

WEP Key2 :

WEP Key3 :

WEP Key4 :

Authentication :

Remember your SSID and the security key as you will need to configure the same settings on your wireless devices and PC.

3. Configure the WEP parameters. For a description of the parameters, refer to [Table 3-12](#).

Table 3-12 WEP Parameter Descriptions

Parameter	Description
WEP Key Length	<ul style="list-style-type: none"> ● 64 bits (10 hex digits or 5 characters) ● 128 bits (26 hex digits or 13 characters)
Choose WEP Key	WEP provides four keys, which are from WEP Key1 to WEP Key4
WEP Key1/WEP Key2/WEP Key3/WEP Key4	WEP provides four keys, which are from WEP Key1 to WEP Key4

Parameter	Description
Authentication	<ul style="list-style-type: none"> ● Open ● Share Key

4. Click **Apply**.

Auto (WPA or WPA2) Security Mode

1. Select **Setup > Wireless > Wireless Security**. The **WIRELESS SECURITY** page is displayed.
2. From the **Security Mode** list, select **Auto (WPA or WPA2)**.
3. From the **WPA Encryption** list, select **AES** or **TKIP+AES**.
4. Perform one of the following operations:
 - From the **WPA Mode** list, select **Auto (WPA or WPA2)-PSK**, see [Figure 3-22](#).

Figure 3-22 WPA and Pre-Shared Key Parameter Configuration Area

WPA

Select **WPA** or **WPA2** to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. The strongest cipher that the client supports is used. For the highest security, select **WPA2 Only**. This mode uses AES (CCMP) cipher and legacy stations are not allowed to access with WPA security. For maximum compatibility, select **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance, select **WPA2 Only** (which uses AES cipher).

WPA-PSK does not require an authentication server. The WPA option requires an external RADIUS server.

WPA Mode :

Group Key Update Interval :

PRE-SHARED KEY

Pre-Shared Key :

Remember your SSID and the security key as you will need to configure the same settings on your wireless devices and PC.

Configure the WPA and Pre-Shared Key parameters. For a description of the parameters, refer to [Table 3-13](#).

Table 3-13 WPA and Pre-Shared Key Parameter Descriptions

Parameter	Description
Group Key Update Interval	Interval of updating the group key
Pre-Shared Key	Password used to connect to the client

- From the **WPA Mode** list, select **Auto(WPA or WPA2)-Enterprise**, see [Figure 3-23](#).

Figure 3-23 WPA and EAP (802.1x) Parameter Configuration Area

WPA

Select **WPA** or **WPA2** to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. The strongest cipher that the client supports is used. For the highest security, select **WPA2 Only**. This mode uses AES (CCMP) cipher and legacy stations are not allowed to access with WPA security. For maximum compatibility, select **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance, select **WPA2 Only** (which uses AES cipher).

WPA-PSK does not require an authentication server. The WPA option requires an external RADIUS server.

WPA Mode :

Group Key Update Interval :

EAP (802.1X)

When WPA enterprise is enabled, the router uses EAP (802.1x) to authenticate clients via a remote RADIUS server.

RADIUS server IP Address :

RADIUS server Port :

RADIUS server Shared Secret :

Remember your SSID and the security key as you will need to configure the same settings on your wireless devices and PC.

Configure the WPA and EAP (802.1x) parameters. For a description of the parameters, refer to [Table 3-14](#).

Table 3-14 WPA and EAP (802.1x) Parameter Descriptions

Parameter	Description
Group Key Update Interval	Interval of updating the group key
RADIUS server IP Address	802.1x server address
RADIUS server Port	802.1x server port number
RADIUS server Shared Secret	802.1x wireless authentication password

- Click **Apply**.

WPA2 Only or WPA Only Security Mode

The configuration methods for **WPA2 only** and **WPA only** are the same as that for **Auto (WPA or WPA2)**.

3.4 Configuring the Local Network

This procedure describes how to configure the local network settings of the router.

Steps

1. Select **Setup > Local Network**. The **LOCAL NETWORK** page is displayed, see [Figure 3-24](#).

Figure 3-24 LOCAL NETWORK Page

Setup

Wizard

Internet Setup

Wireless

Local Network

Local IPv6 Network

Time and Date

Logout

LOCAL NETWORK

In this page, you can configure the local network settings of your router. Please note that settings in this page are optional and you need not change any of the settings in this page to get your network up and running.

ROUTER SETTINGS

The IP address of the router configured in this page is the one you use to access the Web management interface. If you change the IP address in this page, you need to adjust the network settings of your PC to access the network.

Router IP Address :
Subnet Mask :
Domain Name :
 Enable Proxy Arp

Configure the second IP Address and Subnet Mask for LAN

IP Address :
Subnet Mask :

DHCP SETTINGS (OPTIONAL)

Use this section to configure the DHCP Relay for your network.

Enable DHCP Relay

Relay IP Address :

In this page, you can configure the built-in DHCP server to assign IP addresses to the computers on your network.

Enable DHCP Server

DHCP IP Address Range : to
 DHCP IP Mask :
 DHCP Router IP :
DHCP Lease Time : (seconds)

Use the following DNS server addresses:

Enable static DNS

Preferred DNS server :
 Alternate DNS server :

Enable DNS Relay

Use this section to configure the DHCP Server in lan port individual:

- LAN Port1
- LAN Port2
- LAN Port3
- LAN Port4
- WLAN Port1
- WLAN Port2
- WLAN Port3
- WLAN Port4

DHCP CLIENT CLASS LIST

Client Class	Min Address	Max Address	DNS Address
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>			

DHCP COND OPTION

Status	Client Class Name	Option Code	Option Value
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>			

DHCP RESERVATIONS LIST

Status	Computer Name	MAC Address	IP Address
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>			

NUMBER OF DYNAMIC DHCP CLIENTS : 1

Computer Name	MAC Address	IP Address	Expire Time
ZTE-20050515BIY	00:21:97:df:6b:2a	192.168.1.33	36341

- In the **ROUTER SETTINGS** area, configure the parameters, see [Figure 3-25](#).

Figure 3-25 ROUTER SETTINGS Area

ROUTER SETTINGS

The IP address of the router configured in this page is the one you use to access the Web management interface. If you change the IP address in this page, you need to adjust the network settings of your PC to access the network.

Router IP Address :

Subnet Mask :

Domain Name :

Enable Proxy Arp

Configure the second IP Address and Subnet Mask for LAN

IP Address :

Subnet Mask :

For a description of the router settings parameters, refer to [Table 3-15](#).

Table 3-15 Router Settings Parameter Descriptions

Parameter	Description
Router IP Address	Modem management IP address
Subnet Mask	Subnet mask
Domain Name	Domain name
Enable Proxy Arp	Whether to enable ARP proxy
Configure the second IP Address and Subnet Mask for LAN	Secondary management IP address of the gateway

- (Optional) In the **DHCP SETTINGS (OPTIONAL)** area, configure the parameters, see [Figure 3-26](#).

Figure 3-26 DHCP SETTINGS Area**DHCP SETTINGS (OPTIONAL)**

Use this section to configure the DHCP Relay for your network.

Enable DHCP Relay

Relay IP Address :

In this page, you can configure the built-in DHCP server to assign IP addresses to the computers on your network.

Enable DHCP Server

DHCP IP Address Range : to

DHCP IP Mask :

DHCP Router IP :

DHCP Lease Time : (seconds)

Use the following DNS server addresses:

Enable static DNS

Preferred DNS server :

Alternate DNS server :

Enable DNS Relay

Use this section to configure the DHCP Server in lan port individual:

LAN Port1

LAN Port2

LAN Port3

LAN Port4

WLAN Port1

WLAN Port2

WLAN Port3

WLAN Port4

For a description of the Dynamic Host Configuration Protocol (DHCP) settings parameters, refer to [Table 3-16](#).

Table 3-16 DHCP Settings Parameter Descriptions

Parameter	Description
Enable DHCP Relay	Whether to enable DHCP relay
Relay IP Address	Relay server address
Enable DHCP Server	Whether to enable DHCP server
DHCP IP Address Range	DHCP IP address distribution range
DHCP IP Mask	Subnet mask of the DHCP IP address
DHCP Router IP	DHCP gateway address
DHCP Lease Time	DHCP address leasing time
Enable static DNS	Whether to enable static Domain Name Server (DNS) address

Parameter	Description
Preferred DNS server	Primary DNS address
Alternate DNS server	Secondary DNS address
Enable DNS Relay	Whether to enable DNS relay
LAN Port1–LAN Port4	LAN ports that the DHCP server belongs to
WLAN Port1–WLAN Port1	

4. Click **Apply**.
5. (Optional) Add a DHCP client class.
 - a. In the **DHCP CLIENT CLASS LIST** area, click **Add**, see [Figure 3-27](#).

Figure 3-27 ADD DHCP CLIENT CLASS Area

DHCP CLIENT CLASS LIST

	Client Class	Min Address	Max Address	DNS Address
<input type="checkbox"/>	192.168.1.44	192.168.1.44	192.168.1.54	192.168.1.1

Add Edit Delete

ADD DHCP CLIENT CLASS(OPTIONAL)

Client Class Name :

Min IP Address :

Max IP Address :

DNS Address :

Apply Cancel

Configure the DHCP client class parameters. For a description of the parameters, refer to [Table 3-17](#).

Table 3-17 DHCP Client Class Parameter Descriptions

Parameter	Description
Client Class Name	Client class name
Min IP Address	Minimum IP address
Max IP Address	Maximum IP address
DNS Address	DNS address

- b. Click **Apply**.
6. (Optional) Add a DHCP Cond Option.
 - a. In the **DHCP COND OPTION** area, click **Add**, see [Figure 3-28](#).

Figure 3-28 ADD DHCP COND OPTION Area

DHCP COND OPTION

	Status	Client Class Name	Option Code	Option Value
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>				

ADD DHCP OPTION(OPTIONAL)

Cond Option enable:

Cond Option Client Class:

Cond Option Tag:

Cond Option Value:

Configure the DHCP Cond Option parameters. For a description of the parameters, refer to [Table 3-18](#).

Table 3-18 DHCP Cond Option Parameter Descriptions

Parameter	Description
Cond Option enable	Whether to enable DHCP Cond Option
Cond Option Client Class	Client class of DHCP Cond Option
Cond Option Tag	Value range: 240–245
Cond Option Value	Value carried by the CPE, which can be specified as required

- b. Click **Apply**.
- 7. (Optional) Add a DHCP reserved address.
 - a. In the **DHCP RESERVATION LIST** area, click **Add**, see [Figure 3-29](#).

Figure 3-29 ADD DHCP RESERVATION Area

DHCP RESERVATIONS LIST

	Status	Computer Name	MAC Address	IP Address
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>				

ADD DHCP RESERVATION (OPTIONAL)

Enable :

Computer Name :

IP Address :

MAC Address :

Configure the DHCP reserved address parameters. For a description of the parameters, refer to [Table 3-19](#).

Table 3-19 DHCP Reservation Parameter Descriptions

Parameter	Description
Enable	Whether to enable DHCP address reservation
Computer Name	Computer name
IP Address	Reserved IP address
MAC Address	Corresponding MAC address

b. Click **Apply**.

– End of Steps –

3.5 Configuring the Local IPv6 Network

This procedure describes how to configure the local network settings of the router.

Steps

1. Select **Setup > Local IPv6 Network**. The **IPV6 LAND SETTINGS** page is displayed, see [Figure 3-30](#).

Figure 3-30 IPV6 LAND SETTINGS Page

2. Configure the local IPv6 network parameters. For a description of the parameters, refer to Table 3-20.

Table 3-20 Local IPv6 Network Parameter Descriptions

Parameter	Description
IPv6 Interface Address	IPv6 interface address.
Enable DHCPv6 Server	Whether to enable the IPV6 DHCP server.
LAN address config mode	LAN address configuration mode.
Start Interface ID	Starting port number of the address segment.
End Interface ID	Ending port number of the address segment.
DHCPv6 Lease Time	Lease time of the DHCPv6 address.
Get DNS Servers from WAN	Obtains the DNS server from the WAN.
Static DNS Servers	Static DNS server.
Static IPv6 DNS Servers	Static IPv6 DNS server.
Enable RADVD	Whether to enable RADVD.

Parameter	Description
Auto get prefix from WAN	Obtains WAN prefix automatically.
Static	Whether to enable static prefix.
Site Prefix	Static prefix.

- Click **Apply**.

– End of Steps –

3.6 Configuring the Time and Date

This procedure describes how to configure the time zone, Network Time Protocol (NTP) server, and daylight saving.

Steps

- Select **Setup > Time and Date**. The **TIME AND DATE** page is displayed, see [Figure 3-31](#).

Figure 3-31 TIME AND DATE Page

- Configure the time and date parameters. For a description of the parameters, refer to [Table 3-21](#).

Table 3-21 Time and Date Parameter Descriptions

Parameter	Description
Automatically synchronize with Internet time server	Whether to synchronize with the Internet time server automatically
Primary NTP time server	Primary time server address

Parameter	Description
Secondary NTP time server	Secondary time server address
Current Local Time	Current local time
Time Zone	Time zone
Automatically adjust clock for daylight saving changes	Whether to adjust time according to the daylight saving time

3. Click **Apply**.

– End of Steps –

Chapter 4

Advanced Configuration

Table of Contents

Advanced Wireless Configuration.....	4-1
Configuring Port Forwarding.....	4-11
Configuring the DMZ.....	4-13
Configuring the SAMBA Service.....	4-14
Configuring the 3G WAN.....	4-15
Parental Control Configuration.....	4-17
Filtering Options Configuration.....	4-21
Qos Configuration.....	4-26
Configuring the Firewall.....	4-30
Configuring a DNS.....	4-31
Configuring a Dynamic DNS.....	4-32
Network Tools Configuration.....	4-33
Routing Configuration.....	4-47
Configuring Schedules.....	4-53
Configuring NAT.....	4-55
Enabling DLNA.....	4-56
IP Tunnel Configuration.....	4-57

4.1 Advanced Wireless Configuration

Advanced wireless configuration includes the configuration of the following:

- Advanced settings
- MAC filtering
- Security settings
- WPS settings

4.1.1 Configuring Advanced Parameters

This procedure describes how to configure the advanced parameters of the wireless LAN interface.

Steps

1. Select **Advanced > Advanced Wireless > Advanced Settings**. The **ADVANCED SETTINGS** page is displayed, see [Figure 4-1](#).

Figure 4-1 ADVANCED SETTINGS Page

Advanced

Advanced Wireless

Advanced Settings

MAC Filtering

Security Settings

WPS Settings

Port Forwarding

DMZ

SAMBA

3G WAN Configuration

Parental Control

Filtering Options

QoS Configuration

Firewall Settings

DHIS

Dynamic DHIS

Network Tools

Routing

Schedules

NAT

DLNA

IP Tunnel

Logout

ADVANCED SETTINGS

These options are for users who wish to change the behavior of their 802.11g wireless radio from the standard setting. It is not recommended to modify these settings from the factory defaults. Incorrect settings may affect your wireless performance. The default settings usually provide the best wireless performance in most environments.

ADVANCED WIRELESS SETTINGS

Transmission Rate : ▼

Multicast Rate : ▼

Transmit Power : ▼

Beacon Period : (20 ~ 1000)

RTS Threshold : (256 ~ 2346)

Fragmentation Threshold : (256 ~ 2346)

DTIM Interval : (1 ~ 255)

Preamble Type : ▼

SSID

Enable Wireless :

Wireless Network Name (SSID) :

Visibility Status : Visible Invisible

User Isolation : ▼

WMM Advertise : ▼

Max Clients : (1 ~ 32)

GUEST/VIRTUAL ACCESS POINT-1

Enable Wireless Guest Network :

Guest SSID :

Visibility Status : Visible Invisible

User Isolation : ▼

WMM Advertise : ▼

Max Clients : (1 ~ 32)

GUEST/VIRTUAL ACCESS POINT-2

Enable Wireless Guest Network :

Guest SSID :

Visibility Status : Visible Invisible

User Isolation : ▼

WMM Advertise : ▼

Max Clients : (1 ~ 32)

GUEST/VIRTUAL ACCESS POINT-3

Enable Wireless Guest Network :

Guest SSID :

Visibility Status : Visible Invisible

User Isolation : ▼

WMM Advertise : ▼

Max Clients : (1 ~ 32)

- Configure the advanced parameters. For a description of the parameters, refer to Table 4-1.

Table 4-1 Advanced Settings Parameter Descriptions

Parameter	Description
Transmission Rate	Packet transmission rate on the wireless network
Multicast Rate	Multicast rate: <ul style="list-style-type: none"> ● Lower ● Higher
Transmit Power	Transmission power percentage of a wireless router, including 20%, 40%, 60%, 80%, and 100%
Beacon Period	Time period (sent with the beacon) before sending the beacon again, which can be adjusted in milliseconds (ms)
RTS Threshold	Maximum number of packets that can be transmitted on the router
Fragmentation Threshold	Fragmentation threshold, which helps to improve the performance of network transmission on the Radio Frequency (RF) interference
DTIM Interval	Wake-up interval of clients in power saving mode
Preamble Type	Length of the Cyclic Redundancy Check (CRC) block for communication between the router and wireless clients <ul style="list-style-type: none"> ● long ● short
Enable Wireless/Enable Wireless Guest Network	Whether to enable SSID or guest SSID
Wireless Network Name (SSID)/Guest SSID	SSID name or guest SSID name
Visibility Status	<ul style="list-style-type: none"> ● Visible ● Invisible
User Isolation	<ul style="list-style-type: none"> ● Off ● On
WMM Advertise	Whether to enable WMM
Max Clients	Maximum number of clients that can be connected

3. Click **Apply**.

– End of Steps –

4.1.2 Configuring MAC Filtering

This procedure describes how to configure MAC filtering, to permit or deny the device with a specified MAC address to access the ZXHN H108N.

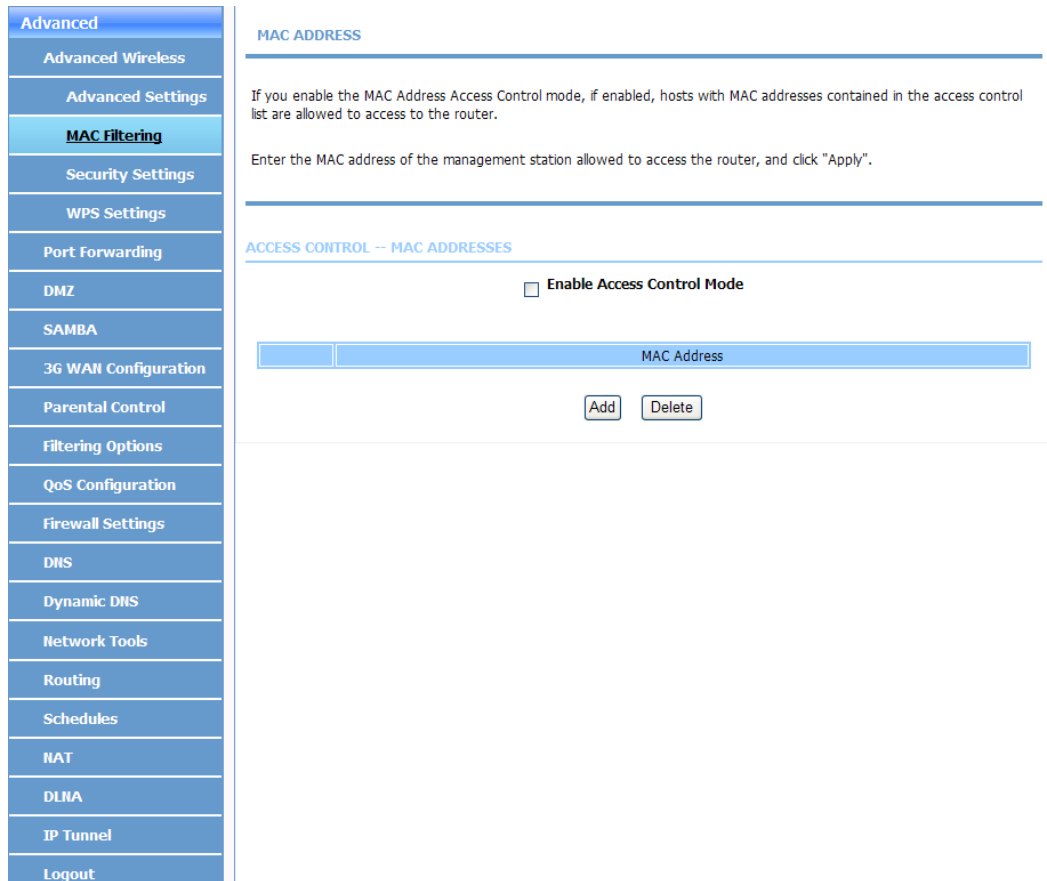
Context

MAC filtering is effective only for the user-side LAN, that is, upstream data flows.

Steps

1. Select **Advanced > Advanced Wireless > MAC Filtering**. The **MAC ADDRESS** page is displayed, see [Figure 4-2](#).

Figure 4-2 MAC ADDRESS Page



2. Click **Add**. Configure the MAC filtering parameters. For a description of the MAC filtering parameters, refer to [Table 4-2](#).

Table 4-2 MAC Filtering Parameter Descriptions

Parameter	Description
Enable Access Control Mode	Whether to enable access control mode
MAC Address	MAC address that needs to be filtered

3. Click **Apply**.
4. (Optional) To delete a MAC filtering item, select it and click **Delete**.

– End of Steps –

4.1.3 Configuring Security Parameters

The ZXHN H108N supports three wireless security modes, including Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and WPA2. WEP is the basic wireless encryption standard. WPA and WPA2 provide higher levels of security.

None Security Mode

1. Select **Advanced > Advanced Wireless > Security Settings**. The **WIRELESS SECURITY** page is displayed, see [Figure 4-3](#).

Figure 4-3 WIRELESS SECURITY Page

Advanced

- Advanced Wireless
- Advanced Settings
- MAC Filtering
- Security Settings**
- WPS Settings
- Port Forwarding
- DMZ
- SAMBA
- 3G WAN Configuration
- Parental Control
- Filtering Options
- QoS Configuration
- Firewall Settings
- DHIS
- Dynamic DHIS
- Network Tools
- Routing
- Schedules
- WAT
- DLIA
- IP Tunnel
- Logout

WIRELESS SECURITY

In this page, you can configure the wireless security settings for the router. Please note that changes made in this page must also be duplicated to your wireless clients and PC.

WIRELESS SSID

Select SSID : WLAN_PasarelaBásic

WIRELESS SECURITY MODE

To protect your privacy, you can configure wireless security features. The device supports 3 wireless security modes including: WEP, WPA, and WPA2. WEP is the original wireless encryption standard. WPA and WPA2 provide higher levels of security.

Security Mode : WPA only

WPA Encryption : TKIP+AES

WPA

Select **WPA** or **WPA2** to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. The strongest cipher that the client supports is used. For the highest security, select **WPA2 Only**. This mode uses AES (CCMP) cipher and legacy stations are not allowed to access with WPA2 security. For maximum compatibility, select **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance, select **WPA2 Only** (which uses AES cipher).

WPA-PSK does not require an authentication server. The WPA option requires an external RADIUS server.

WPA Mode : WPA-PSK

Group Key Update Interval : 0

PRE-SHARED KEY

Pre-Shared Key :

Remember your SSID and the security key as you will need to configure the same settings on your wireless devices and PC.

Apply Cancel

2. From the **Select SSID** list, select an SSID.
3. From the **Security Mode** list, select **None**.
4. Click **Apply**.

WEP Security Mode

1. Select **Advanced > Advanced Wireless > Security Settings**. The **WIRELESS SECURITY** page is displayed.
2. From the **Select SSID** list, select an SSID.
3. From the **Security Mode** list, select **WEP**, see [Figure 4-4](#).

Figure 4-4 WEP Parameter Configuration Area

WIRELESS SECURITY MODE

To protect your privacy, you can configure wireless security features. The device supports 3 wireless security modes including: WEP, WPA, and WPA2. WEP is the original wireless encryption standard. WPA and WPA2 provide higher levels of security.

Security Mode :

WEP

If you select WEP, the device operates **ONLY** in **Legacy Wireless mode (802.11B/G)**.

WEP is the wireless encryption standard. To use it, you must enter the same key(s) on the router and the wireless stations. A 64-bit key consists of 10 hexadecimal digits and a 128-bit key consists of 26 hexadecimal digits. A hexadecimal digit is a number from 0 to 9 or a letter from A to F. For the most secure use of WEP, set the authentication type to "Shared Key".

You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. A maximum of 5 text characters can be entered for 64 bit keys, and a maximum of 13 characters for 128 bit keys.

WEP Key Length :

Choose WEP Key :

WEP Key1 :

WEP Key2 :

WEP Key3 :

WEP Key4 :

Authentication :

Remember your SSID and the security key as you will need to configure the same settings on your wireless devices and PC.

Configure the WEP parameters. For a description of the parameters, refer to [Table 4-3](#).

Table 4-3 WEP Parameter Descriptions

Parameter	Description
WEP Key Length	<ul style="list-style-type: none"> ● 64 bits (10 hex digits or 5 characters) ● 128 bits (26 hex digits or 13 characters)
Choose WEP Key	WEP provides four keys, which are from WEP Key1 to WEP Key4

Parameter	Description
WEP Key1/WEP Key2/WEP Key3/WEP Key4	WEP provides four keys, which are from WEP Key1 to WEP Key4
Authentication	<ul style="list-style-type: none"> ● Open ● Share Key

4. Click **Apply**.

Auto (WPA or WPA2) Security Mode

1. Select **Advanced > Advanced Wireless > Security Settings**. The **WIRELESS SECURITY** page is displayed.
2. From the **Select SSID** list, select an SSID.
3. From the **Security Mode** list, select **Auto (WPA or WPA2)**.
4. From the **WPA Encryption** list, select **AES** or **TKIP+AES**.
5. Perform one of the following operations:
 - From the **WPA Mode** list, select **Auto (WPA or WPA2)-PSK**, see [Figure 4-5](#).

Figure 4-5 WPA and Pre-Shared Key Parameter Configuration Area

WPA

Select **WPA** or **WPA2** to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. The strongest cipher that the client supports is used. For the highest security, select **WPA2 Only**. This mode uses AES (CCMP) cipher and legacy stations are not allowed to access with WPA security. For maximum compatibility, select **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance, select **WPA2 Only** (which uses AES cipher).

WPA-PSK does not require an authentication server. The WPA option requires an external RADIUS server.

WPA Mode :

Group Key Update Interval :

PRE-SHARED KEY

Pre-Shared Key :

Remember your SSID and the security key as you will need to configure the same settings on your wireless devices and PC.

Configure the WPA and Pre-Shared Key parameters. For a description of the parameters, refer to [Table 4-4](#).

Table 4-4 WPA and Pre-Shared Key Parameter Descriptions

Parameter	Description
Group Key Update Interval	Interval of updating the group key
Pre-Shared Key	Password used to connect to the client

- From the **WPA Mode** list, select **Auto(WPA or WPA2)-Enterprise**, see [Figure 4-6](#).

Figure 4-6 WPA and EAP (802.1x) Parameter Configuration Area

WPA

Select **WPA** or **WPA2** to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. The strongest cipher that the client supports is used. For the highest security, select **WPA2 Only**. This mode uses AES (CCMP) cipher and legacy stations are not allowed to access with WPA security. For maximum compatibility, select **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance, select **WPA2 Only** (which uses AES cipher).

WPA-PSK does not require an authentication server. The WPA option requires an external RADIUS server.

WPA Mode :

Group Key Update Interval :

EAP (802.1X)

When WPA enterprise is enabled, the router uses EAP (802.1x) to authenticate clients via a remote RADIUS server.

RADIUS server IP Address :

RADIUS server Port :

RADIUS server Shared Secret :

Remember your SSID and the security key as you will need to configure the same settings on your wireless devices and PC.

Configure the WPA and EAP (802.1x) parameters. For a description of the parameters, refer to [Table 4-5](#).

Table 4-5 WPA and EAP (802.1x) Parameter Descriptions

Parameter	Description
Group Key Update Interval	Interval of updating the group key
RADIUS server IP Address	802.1x server address
RADIUS server Port	802.1x server port number
RADIUS server Shared Secret	802.1x wireless authentication password

6. Click **Apply**.

WPA2 Only or WPA Only Security Mode

The configuration methods for **WPA2 only** and **WPA only** are the same as that for **Auto (WPA or WPA2)**.

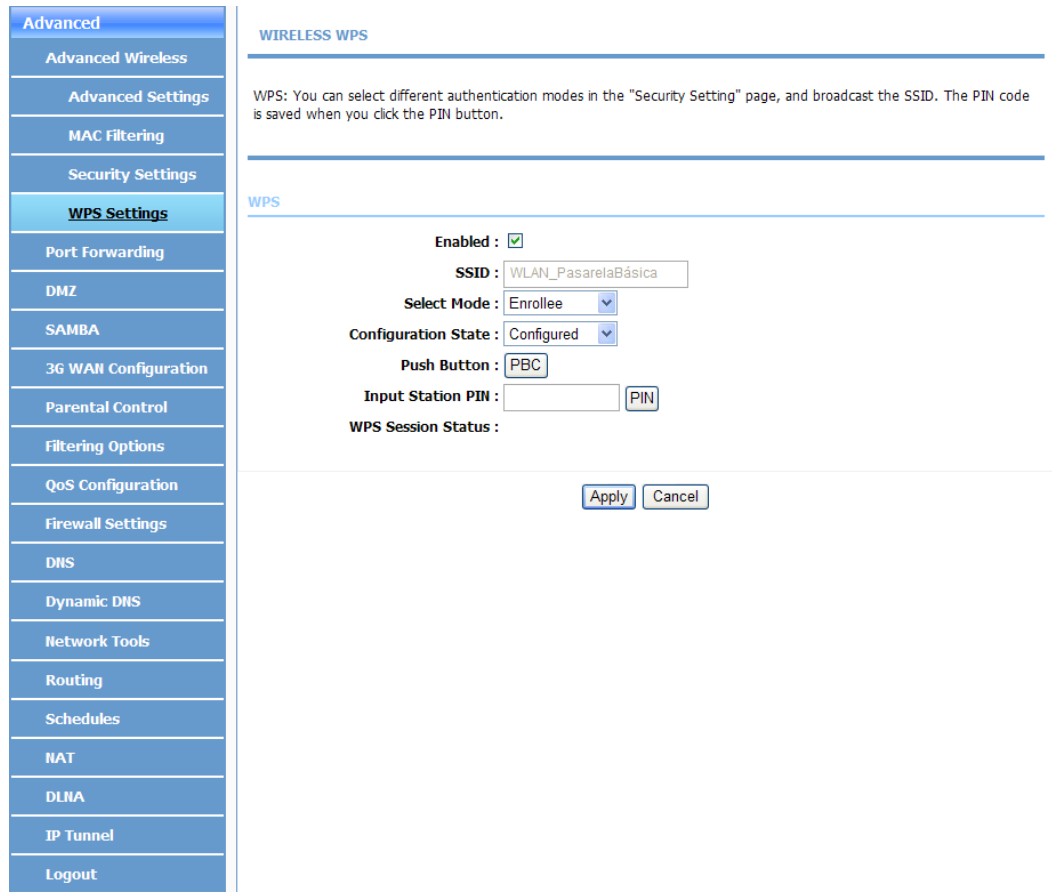
4.1.4 Configuring the WPS

This procedure describes how to configure the Wireless Priority Service (**WPS**).

Enrollee Mode

1. Select **Advanced > Advanced Wireless > WPS Settings**. The **WIRELESS WPS** page is displayed, see [Figure 4-7](#).

Figure 4-7 WIRELESS WPS Page



2. Select **Enable**. From the **Select Mode** list, select **Enrollee**.
3. Configure the WPS parameters. For a description of the WPS parameters, refer to [Table 4-6](#).

Table 4-6 WPS Parameter Descriptions (Enrollee Mode)

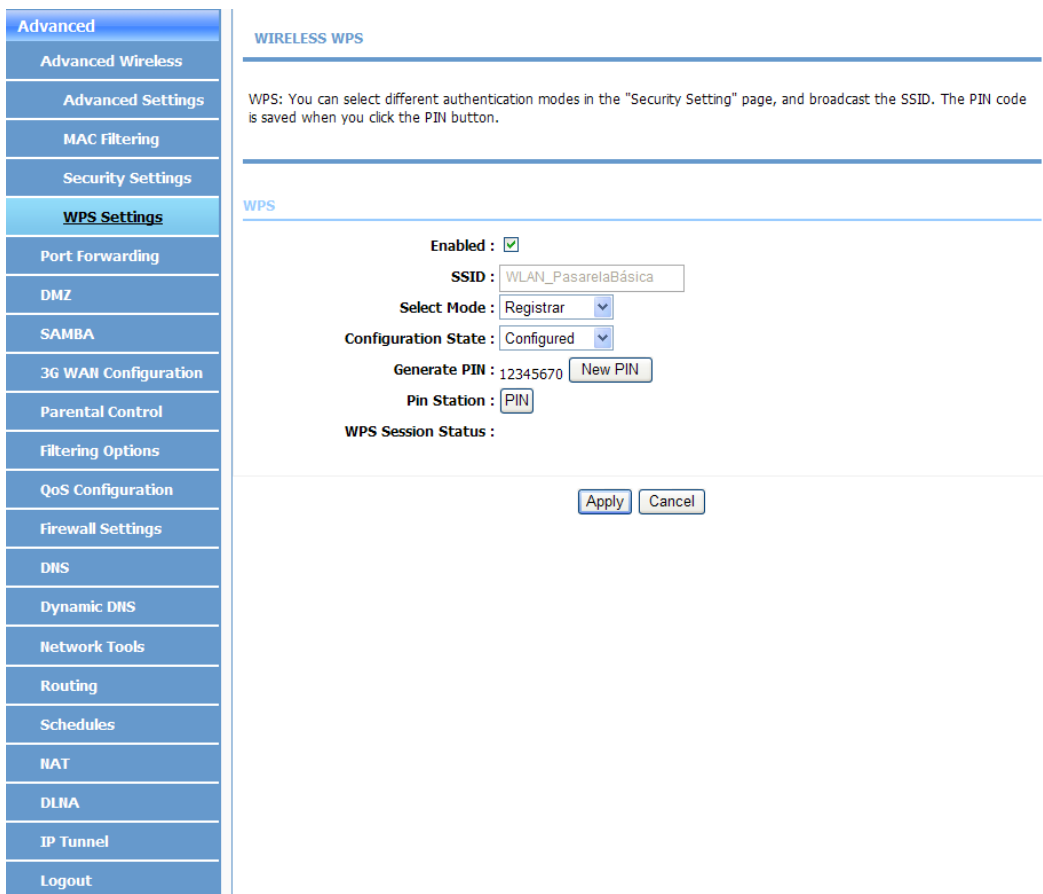
Parameter	Description
Configuration State	Configuration state
Push Button	Whether to enable the WPS function
Input Station PIN	To save the Personal Identification Number (PIN) code by clicking PIN
WPS Session Status	WPS status

4. Click **Apply**.

Registrar Mode

1. Select **Advanced > Advanced Wireless > WPS Settings**. The **WIRELESS WPS** page is displayed.
2. Select **Enable**. From the **Select Mode** list, select **Registrar**, see [Figure 4-8](#).

Figure 4-8 WIRELESS WPS Page–Registrar Mode



3. Configure the WPS parameters. For a description of the WPS parameters, refer to [Table 4-7](#).

Table 4-7 WPS Parameter Descriptions (Registrar Mode)

Parameter	Description
Configuration State	Configuration state
Generate PIN	To generate a new PIN code by clicking New PIN
Pin Station	PIN code connection
WPS Session Status	WPS status

4. Click **Apply**.

4.2 Configuring Port Forwarding

This procedure describes how to enable multiple ports (by selecting multiple ports or specifying a port range) on a router and forward data through these ports to a single computer in the network.

Context

Port forwarding is used to forward the incoming traffic from the WAN side to the internal server with a private IP address at the LAN side. The internal port is required only when the external port needs to be converted to a different port number that is used by the server at the LAN side. A maximum of 80 entries can be configured.

Steps

1. Select **Advanced > Port Forwarding**. The **PORT FORWARDING** page is displayed, see [Figure 4-9](#).

Figure 4-9 PORT FORWARDING Page

PORT FORWARDING

Port Forwarding allows you to direct incoming traffic from the WAN side (identified by protocol and external port) to the internal server with a private IP address on the LAN side. The internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum of 80 entries can be configured.

Select the service name, and enter the server IP address and click "Apply" to forward IP packets for this service to the specified server. Note: Modifying the **Internal Port Start** or **Internal Port End** is not recommended. If the **External Port Start** or the **External Port End** changes, the **Internal Port Start** or **Internal Port End** automatically changes accordingly.

PORT FORWARDING SETUP

	Server Name	Wan Connection	External Port Start/End	Protocol	Internal Port Start/End	Server IP Address	Schedule Rule	Remote IP
<input type="checkbox"/>		PVC:8/36	1000/1000	tcp	1000/1000	192.168.1.150	Always	
<input type="checkbox"/>		PVC:8/36	3000/3000	tcp	3000/3000	192.168.1.100	Always	
<input type="checkbox"/>		PVC:8/36	3500/4000	tcp	3500/4000	192.168.1.100	Always	
<input type="checkbox"/>		PVC:8/36	1500/2000	tcp	1500/2000	192.168.1.150	Always	

2. Click **Add**, see [Figure 4-10](#).

Figure 4-10 PORT FORWARDING Page—Adding a Port Forwarding Configuration Item

PORT FORWARDING SETUP

Remaining number of entries that can be configured: 76

WAN Connection(s): PVC:8/36

Server Name:

Select a Service: (Click to Select)

Custom Server:

Schedule: always [View Available Schedules](#)

Server IP Address(Host Name): 192.168.1.

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Remote Ip
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	<input type="text"/>

Configure the port forwarding parameters. For a description of the port forwarding parameters, refer to [Table 4-8](#).

Table 4-8 Port Forwarding Parameter Descriptions

Parameter	Description
WAN Connection	WAN connection type, which can be configured by selecting Setup > Internet Setup .
Server Name	Select Select a Service , and then select a service from the drop-down list. Select Custom Server , and then enter the server name in the text box.
Schedule	<ul style="list-style-type: none"> ● Always ● Never ● Click View Available Schedules, that is, select Advanced > Schedule to configure other options.

Parameter	Description
Server IP Address(Host Name)	IP address or host name of the server.
External Port Start/End	External port range.
Protocol	Protocol of the permitted packets.
Internal Port Start/End	Internal port range.
Remote Ip	Remote IP address.

3. Click **Apply**.
4. (Optional) To edit the port forwarding configuration, click **Edit**.
5. (Optional) To delete the port forwarding configuration, click **Delete**.

– End of Steps –

4.3 Configuring the DMZ

The ZXHN H108N forwards the IP packets that do not belong to any applications configured in the port forwarding list, from WAN to the Demilitarized Zone (DMZ) host. This procedure describes how to configure the DMZ parameters.

Steps

1. Select **Advanced > DMZ**. The **DMZ** page is displayed, see [Figure 4-11](#).

Figure 4-11 DMZ Page

2. Configure the DMZ parameters. For a description of the DMZ parameters, refer to [Table 4-9](#).

Table 4-9 DMZ Parameter Descriptions

Parameter	Description
WAN Connection	WAN connection type, which can be configured by selecting Setup > Internet Setup .
Enable DMZ	Whether to enable DMZ.
DMZ Host IP Address	IP address of the LAN host that provides the DMZ service.

- Click **Apply**.
– End of Steps –

4.4 Configuring the SAMBA Service

SAMBA service is used to provide the file share service to the users at the LAN side.

Steps

- Select **Advanced > SAMBA**. The **SAMBA** page is displayed, see [Figure 4-12](#).

Figure 4-12 SAMBA Page

- Configure the SAMBA parameters. For a description of the SAMBA parameters, refer to [Table 4-10](#).

Table 4-10 SAMBA Parameter Descriptions

Parameter	Description
Enable SAMBA	Whether to enable SAMBA
Workgroup	Group name
Netbios Name	Network Basic Input/Output System (BIOS) name

Parameter	Description
SMB User Name	–
New SMB password/Retype new SMB password	Connection password
Enable USB Storage	Whether to enable USB storage connection
Enable Anonymous Access	Whether to enable anonymous access

- Click **Apply**.

– End of Steps –

4.5 Configuring the 3G WAN

This procedure describes how to configure The 3rd Generation Mobile Communications (3G) WAN.

Steps

- Select **Advanced > 3G WAN Configuration**. The **3G WAN Configuration** page is displayed, see [Figure 4-13](#).

Figure 4-13 3G WAN Configuration Page

Choose "Add", "Edit", or "Delete" to configure 3G WAN interfaces.

When you want to edit the 3G configuration, please ensure the 3G is in disconnection status at first.

3G Status: NoDongle
Inform: NO USB CARD

Service Name	Protocol	State	Status	Default Gateway	Action
ppp3g	PPPo3G	1	Disconnected	<input type="checkbox"/>	dial

Add Edit Delete Pin Manage DongleInfo

- Click **Edit**, see [Figure 4-14](#).

Figure 4-14 3G INTERNET SETUP Area

3G INTERNET SETUP

This screen allows you to configure a 3G Internet connection.

3G USB SETUP

Enable 3G Service :

Account :

Password :

Dial_Number :

Net Type : ▼

APN :

OnDemand :

Inactivity Timeout : (Seconds [0-65535])

Backup delay time : (Seconds [0-600])

Recovery delay time : (Seconds [0-600])

Initialization Delay time : (If too small, some 3g dongle will be unsupported)

Mode Switch Delay time : (If too small, some 3g dongle will be unsupported)

BackupMechanism : ▼

Checking IP address:

Timeout (in sec.):

Period time (in sec.):

Fail Tolerance:

Configure the 3G WAN parameters. For a description of the parameters, refer to [Table 4-11](#).

Table 4-11 3G WAN Parameter Descriptions

Parameter	Description
Enable 3G Service	Whether to enable the 3G service.
Account	User account.
Password	User password.
Dial_Number	3G dial-up number.
Net Type	<ul style="list-style-type: none"> ● Auto ● EVDO ● WCDMA ● TD-SCDMA
APN	Access Point Name (APN), defined by the carrier.
OnDemand	Dial-up on demand.

Parameter	Description
Inactivity Timeout	Disconnects automatically when there is no data flow in the specified timeout period.
BackupMechanism	<ul style="list-style-type: none">• DSL• IP Check
Checking IP address	This parameter needs to be configured when BackupMechanism is set to IP Check .
Fail Tolerance	Default: 1.

3. Click **Apply**.

– End of Steps –

4.6 Parental Control Configuration

Parental control configuration includes the following:

- Blocking websites
- Configuring MAC filtering

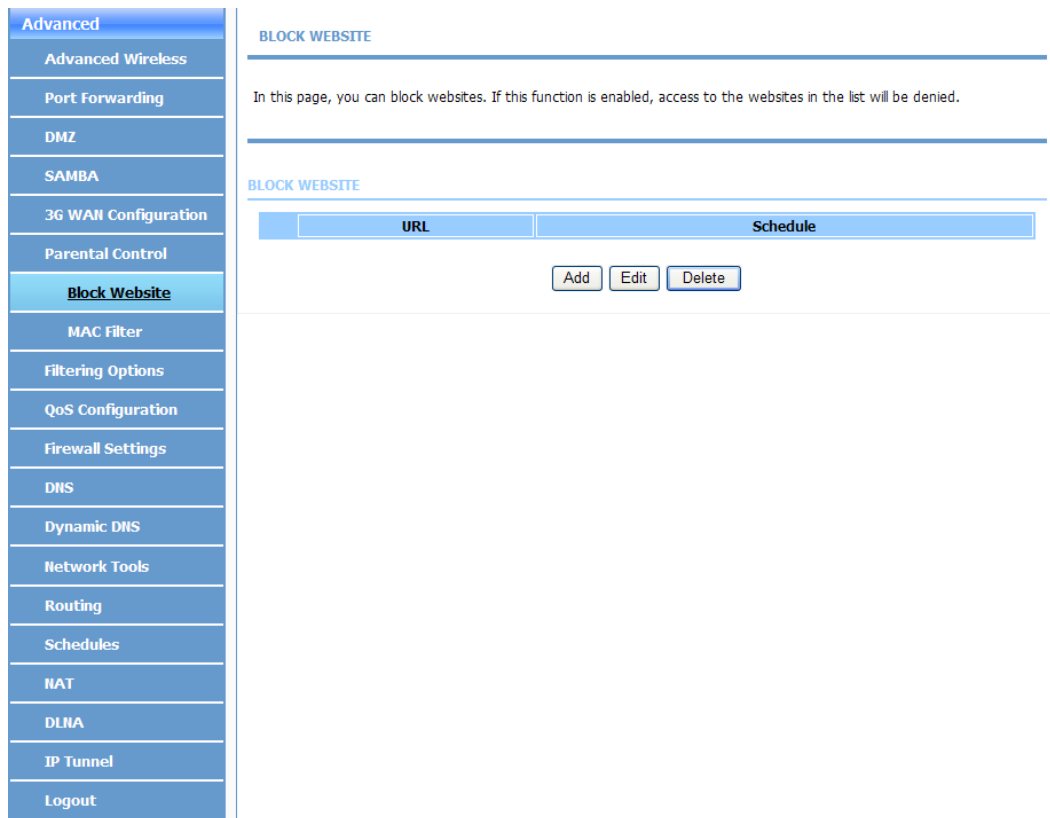
4.6.1 Blocking Websites

This procedure describes how to block certain websites.

Steps

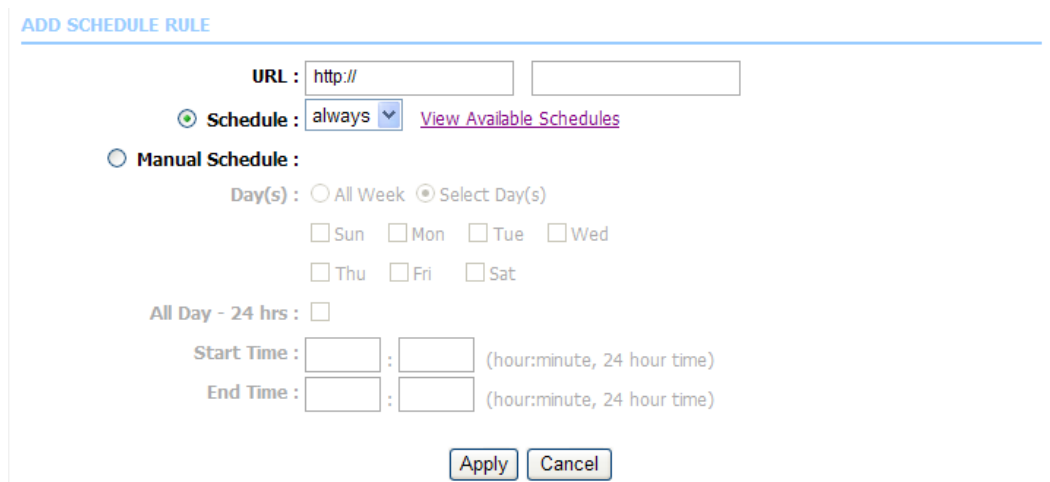
1. Select **Advanced > Parental Control > Block Website**. The **Block Website** page is displayed, see [Figure 4-15](#).

Figure 4-15 BLOCK WEBSITE Page



2. Click **Add**, see Figure 4-16.

Figure 4-16 ADD SCHEDULE RULE Area



Configure the website blocking parameters. For a description of the parameters, refer to Table 4-12.

Table 4-12 Website Blocking Parameter Descriptions

Parameter	Description
URL	Uniform resource locator

Parameter	Description
Schedule/Manual Schedule	Self-defined time period

3. Click **Apply**.
4. (Optional) To edit the website blocking configuration, click **Edit**.
5. (Optional) To delete the website blocking configuration, click **Delete**.

– End of Steps –

4.6.2 Configuring MAC Filtering

This procedure describes how to configure MAC filtering, to permit or deny the device with a specified MAC address to access the ZXHN H108N.

Context

MAC filtering is effective only for the user-side LAN, that is, upstream data flows.

Steps

1. Select **Advanced > Parental Control > MAC Filter**. The **MAC FILTER** page is displayed.
2. Select **BLACK_LIST** or **WHITE_LIST**. Configure the MAC filtering global policy.
3. Click **Add**, see [Figure 4-17](#).

Figure 4-17 Add Schedule Rule Area

MAC Filtering Global Policy:

BLACK_LIST --Allow all packets but **DENY** MAC addresses that match a rule in the list
 WHITE_LIST --Deny all packets but **ALLOW** MAC addresses that match a rule in the list

BLOCK MAC ADDRESS--BLACKLIST

Username	MAC	Schedule

ADD SCHEDULE RULE

User Name :

Current PC's MACAddress :

Other MAC Address :

Schedule : [View Available Schedules](#)

Manual Schedule :
 Day(s) : All Week Select Day(s)
 Sun Mon Tue Wed
 Thu Fri Sat

All Day - 24 hrs :

Start Time : : (hour:minute, 24 hour time)
End Time : : (hour:minute, 24 hour time)

Configure the schedule rule parameters. For a description of the parameters, refer to Table 4-13.

Table 4-13 Schedule Rule Parameter Descriptions

Parameter	Description
User Name	User name
Current PC's MACAddress/Other MAC Address	<p>Current PC's MAC Address displays the MAC address of the LAN device where the browser is running.</p> <p>To filter another LAN device, select Other MAC Address and enter the MAC address of that LAN device.</p> <p>To obtain the MAC address of a Windows-based PC, open the command line interface and enter ipconfig /all.</p>
Schedule/Manual Schedule	Customized time period

4. Click **Apply**.
5. (Optional) To edit a MAC filtering item, select it and click **Edit**.

6. (Optional) To delete a MAC filtering item, select it and click **Delete**.
- End of Steps –

4.7 Filtering Options Configuration

Filtering options configuration includes the following:

- IP filtering
- Bridge filtering

4.7.1 Configuring IP Filtering

This procedure describes how to configure IP filtering to permit or deny a device with the specified IP address to access the ZXHN H108N.

Steps

1. Select **Advanced > Filtering Options > IP Filtering**. The **IP FILTER** page is displayed, see [Figure 4-18](#).

Figure 4-18 IP FILTER Page

IP FILTER

In this page, you can specify a filter name and at least one condition to create a filter for identify incoming IP traffic. All the specified conditions take effect simultaneously. Click "Apply" to save the filter and enable it.

FIREWALL

Name	Interface	In/Out	Default action	Bytes	Pkts	Local/Forward
<input type="button" value="Add Filter"/> <input type="button" value="Edit Filter"/> <input type="button" value="Delete Filter"/>						

RULE

Enabled	Protocol	IP Version Type	Action	RejectType	IcmpType	OrigIP/ Mask	OrigPort	DestIP/ Mask	DestPort	Bytes	Pkts
<input type="button" value="Add Rule"/> <input type="button" value="Edit Rule"/> <input type="button" value="Delete Rule"/>											

2. Click **Add Filter**, see [Figure 4-19](#).

Figure 4-19 Filtering Configuration Area

FIREWALL

Name	Interface	In/Out	Default action	Bytes	Pkts	Local/Forward
------	-----------	--------	----------------	-------	------	---------------

Add Filter Edit Filter Delete Filter

FILTER INFO

Name:

Interface: LAN

In/Out: In

Default action: Permit

Local/Forward: Local

Apply Cancel

Configure the IP filtering parameters. For a description of the parameters, refer to Table 4-14.

Table 4-14 IP Filtering Parameter Descriptions

Parameter	Description
Name	Rule name
Interface	Interface type
In/Out	Data flow direction
Default action	Default action, which is permit or deny
Local/Forward	Forwarding or saving in the local disk

3. Click **Apply**.
4. Click **Add Rule**, see [Figure 4-20](#).

Figure 4-20 Rule Information Configuration Area

RULE INFO

Notes:
 1.When Protocol is 'ICMP',one of IcmpType to be selected;
 2.When Action is 'Reject',one of RejectType to be selected;
 3.When the "IP Version Type" is Ipv4,Please enter the IPv4 address and mask of the corresponding;
 4.When the "IP Version Type" is Ipv6,Please enter the IPv6 address and prefix length of the corresponding;

Enabled:

Protocol: ALL

IP Version Type: IPv4

Action: Permit

ALG: Enable

DSCP:

Packet Length: - (1~65535)

SOURCE SETTING

IP Address:

PrefixLength/Mask:

DESTINATION SETTING

FQDN Enabled

IP Address:

PrefixLength/Mask:

Configure the rule parameters. For a description of the parameters, refer to [Table 4-15](#).

Table 4-15 Rule Information Parameter Descriptions

Parameter	Description
Enabled	Whether to enable the rule
Protocol	Protocol type
IP Version Type	IPv4 or IPv6
Action	Permit or deny
ALG	Whether to enable the Application Level Gateway (ALG) function
DSCP	Differentiated services code point
Packet Length	Packet length
IP Address	Source IP address
PrefixLength/Mask	Prefix length and mask
FQDN Enabled	Fully qualified domain name, which is the host name and full path
IP Address	Destination IP address
PrefixLength/Mask	Prefix length and mask

5. Click **Apply**.
 6. (Optional) Perform the following operations as required:
 - To edit an IP filtering item, select it and click **Edit Filter**.
 - To delete an IP filtering item, select it and click **Delete Filter**.
 - To edit an IP filtering rule item, select it and click **Edit Rule**.
 - To delete an IP filtering rule item, select it and click **Delete Rule**.
- End of Steps –

4.7.2 Configuring Bridge Filtering

Bridge filtering is also known as MAC address filtering. You can forward or deny incoming traffic based on the source or destination MAC address. Bridge filtering works with interfaces that are configured as bridges.

Context

Bridge Filtering is effective only on the Asynchronous Transfer Mode (ATM) Permanent Virtual Channels (PVCs) that are configured in Bridge mode.

- ALLOW: All the MAC-layer frames can be transmitted.
- DENY: All the MAC-layer frames except those matching a configured rule cannot be transmitted.

Steps

1. Select **Advanced > Filtering Options > Bridge Filtering**. The **BRIDGE FILTERING** page is displayed, see [Figure 4-21](#).

Figure 4-21 BRIDGE FILTERING Page

BRIDGE FILTERING

Bridge Filtering is effective only on ATM PVCs configured in Bridge mode. ALLOW means that all MAC layer frames can be transmitted. DENY means that all MAC layer frames except those matching a rule in the following list can not be transmitted.

Specify at least one condition to create a filter for identify the MAC layer frames. If you specify several conditions, all of them take effect simultaneously. Click "Apply" to save the filter and enable it.

WARNING: Changing from one global policy to another automatically REMOVES all the existing rules. You will need to create new rules for the new policy.

Bridge Filtering Global Policy:
 ALLOW all packets but **DENY** MAC addresses that match a rule in the list
 DENY all packets but **ALLOW** MAC addresses that match a rule in the list

Apply Cancel

DISPLAY LIST

VPI/VCI	protocol	DMAC	SMAC	Prio	vlanID	DIR	TIME
Add Edit Delete							

2. Select **ALLOW** or **DENY**. Configure the bridge filtering global policy.
3. Click **Apply**.
4. Click **Add**, see Figure 4-22. Configure the bridge filtering parameters.

Figure 4-22 Bridge Filtering Configuration Area

ADD BRIDGE FILTER

Protocol Type: (Click to Select) ▼

Destination MAC Address:

Source MAC Address:

User Priority: (0-7)

vlanID: (0-4095)

Frame Direction: WAN=>LAN ▼

Time schedule: always ▼ [View Available Schedules](#)

Wan interface: select all interfaces ▼

Apply Cancel

5. Click **Apply**.
6. (Optional) To edit a bridge filtering item, select it and click **Edit**.
7. (Optional) To delete a bridge filtering item, select it and click **Delete**.

– End of Steps –

4.8 Qos Configuration

Qos Configuration includes the following:

- QoS global options configuration
- QoS queue configuration
- QoS classification configuration

4.8.1 Configuring QoS Global Options

This procedure describes how to enable or disable the queuing operation.

Steps

1. Select **Advanced > QoS Configuration > QoS Global Options**. The **QoS GLOBAL CONFIGURATION** page is displayed, see [Figure 4-23](#).

Figure 4-23 QoS GLOBAL CONFIGURATION Page

Advanced	QoS GLOBAL CONFIGURATION
Advanced Wireless	Enable Queuing Operation <input checked="" type="checkbox"/>
Port Forwarding	<input type="button" value="Submit"/> <input type="button" value="Refresh"/>
DMZ	
SAMBA	
3G WAN Configuration	
Parental Control	
Filtering Options	
QoS Configuration	
QoS Global Options	
QoS Queue Config	
QoS Classification	
Firewall Settings	
DNS	
Dynamic DNS	
Network Tools	
Routing	
Schedules	
NAT	
DLNA	
IP Tunnel	

2. Select **Enable Queuing Operation**.
3. Click **Submit**.

– End of Steps –

4.8.2 Configuring QoS Queues

This procedure describes how to configure Quality of Service (QoS) Queues.

Steps

1. Select **Advanced > QoS Configuration > QoS Queue Config**. The **QoS GLOBAL CONFIGURATION** page is displayed, see [Figure 4-24](#).

Figure 4-24 QoS GLOBAL CONFIGURATION Page

QoS GLOBAL CONFIGURATION

Enable

Upstream Bandwidth Kbps (0 means no limit bandwidth)

Scheduling Strategy (Note: Scheduling change would clear the queue configuration)

Enable DSCP/TC Mark

Enable 802.1P Mark

UPSTREAM QUEUE CONFIGURATION

Number	Name	Enable	Precedence	Egress Interface	Operation
1	UP_Q_3	<input checked="" type="checkbox"/>	<input type="text" value="1"/>	<input type="text" value="WAN"/>	<input type="button" value="Delete"/>
2	UP_Q_4	<input checked="" type="checkbox"/>	<input type="text" value="2"/>	<input type="text" value="WAN"/>	<input type="button" value="Delete"/>
3	UP_Q_5	<input checked="" type="checkbox"/>	<input type="text" value="3"/>	<input type="text" value="WAN"/>	<input type="button" value="Delete"/>
4	UP_Q_6	<input checked="" type="checkbox"/>	<input type="text" value="4"/>	<input type="text" value="WAN"/>	<input type="button" value="Delete"/>

2. Configure the QoS global parameters, and then click **Add Queue**.
3. Modify a record in the **Upstream Queue Configuration** list. For a description of the parameters, refer to [Table 4-16](#).

Table 4-16 Upstream Queue Configuration Parameter Descriptions

Parameter	Description
Enable	Whether to enable the upstream queue
Precedence	Queue priority
Egress Interface	WAN-side interface

4. Click **Submit**.

– End of Steps –

4.8.3 Configuring QoS Classification

This procedure describes how to configure the QoS classification rules.

Context

QoS is a network security mechanism, which is used to solve the problems such as network delay and congestion.

Steps

1. Select **Advanced > QoS Configuration > QoS Classification**. The **QOS CLASSIFY CONFIG** page is displayed, see [Figure 4-25](#).

Figure 4-25 QOS CLASSIFY CONFIG Page

QOS CLASSIFY CONFIG

LIST

Classify Number	Enable	Classify Condition	Classify Mark	Classify Queue	Operation
1	1	Source/Destination MAC address : / Ethernet Type : IPv4 VLANID : -1 802.1P : -1 Source/Destination IP address : /81.47.224.0 Source/Destination Mask : /255.255.252.0 DSCP value : Do not mark Protocol Type : UDP Source port range : -1--1 Destination port range : -1--1	802.1P: -1 DSCP:	UP_Q_3	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
2	1	Source/Destination MAC address : / Ethernet Type : IPv4 VLANID : -1 802.1P : -1 Source/Destination IP address : /80.58.63.192 Source/Destination Mask : /255.255.255.192 DSCP value : Do not mark Protocol Type : Do not match Source port range : -1--1 Destination port range : -1--1	802.1P: -1 DSCP:	UP_Q_3	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

2. Configure the QoS classification parameters, and then click **Add Classification Rule**. The **QOS FLOW CLASSIFICATION CONFIGURATION** page is displayed, see [Figure 4-26](#).

Figure 4-26 QOS FLOW CLASSIFICATION CONFIGURATION Page

Advanced

Advanced Wireless

Port Forwarding

DMZ

SAMBAA

3G WAN Configuration

Parental Control

Filtering Options

QoS Configuration

 QoS Global Options

 QoS Queue Config

QoS Classification

 Firewall Settings

 DNS

 Dynamic DNS

 Network Tools

 Routing

 Schedules

 NAT

 DLIA

 IP Tunnel

 Logout

QOS FLOW CLASSIFICATION CONFIGURATION

Enable

CLASSIFY CONDITIONS

Ip Protocol Type: IPv4

Input Interface: LAN

Source MAC address:

Source MAC mask:

802.1P: Not Match

Source IPv4 address:

Source subnet mask:

Destination IPv4 address:

Destination subnet mask:

DSCP Check: Not Match

Protocol Type: Not Match

Source port range: -

Destination port range: -

CLASSIFICATION MATCH RESULT

Classify Queue: Unbound

DSCP Mark: Not Mark

For a description of the QoS flow classification parameters, refer to [Table 4-17](#).

Table 4-17 QoS Flow Classification Parameter Descriptions

Parameter	Description
Enable	Whether to enable the rule
Ip Protocol Type	IP protocol type
Input Interface	Input interface
Source MAC address	Source MAC address
Source MAC mask	MAC address mask, which can be null
802.1P	802.1P priority
Source IPv4 address	Source IP address
Source subnet mask	Source subnet mask
Destination IPv4 address	Destination IP address
Destination subnet mask	Destination subnet mask
DSCP Check	DSCP value
Protocol Type	Protocol type

Parameter	Description
Source port range	Source port range
Destination port range	Destination port range
Classify Queue	Queue classification
DSCP Mark	DSCP remarking

3. Click **Submit**.
 4. (Optional) To edit a QoS classification configuration item, select it and click **Edit**.
 5. (Optional) To delete a QoS classification configuration item, select it and click **Delete**.
- End of Steps –

4.9 Configuring the Firewall

This procedure describes how to configure the firewall to enhance network security.

Steps

1. Select **Advanced > Firewall Settings**. The **Firewall Settings** page is displayed, see [Figure 4-27](#).

Figure 4-27 FIREWALL SETTINGS Page

The screenshot displays the 'FIREWALL SETTINGS' page. On the left is a navigation menu with 'Firewall Settings' highlighted. The main area is titled 'FIREWALL SETTINGS' and includes a note: 'Click "Apply" to take the changes in effect immediately.' Below this is the 'FIREWALL CONFIGURATION' section, which contains the following settings:

- Enable Attack Prevent
- Icmp Echo
- Fraggle
- Echo Chargen
- IP Land
- Port Scan
- TCP Flags: Set "SYN FIN"
- TCP Flags: Set "SYN RST"
- TCP Flags: Set "FIN RST"
- TCP Flags: Set "ACK FIN"
- TCP Flags: Set "ACK PSH"
- TCP Flags: Set "ACK URG"
- TCP DoS :
- TCP DoS Max Rate: (packets/second)

At the bottom right of the configuration area are 'Apply' and 'Cancel' buttons.

2. Select the check boxes to enable the protection functions as required.
3. Click **Apply**.

– End of Steps –

4.10 Configuring a DNS

This procedure describes how to configure a Domain Name Server (DNS).

Context

DNS is a server that translates a [URL](#) or domain name to the corresponding IP address. The Internet is based on an IP address, and the alphabetical URL or domain name is easier to remember.

Steps

1. Select **Advanced > DNS**. The **DNS** page is displayed, see [Figure 4-28](#).

Figure 4-28 DNS Page

2. Configure the DNS parameters. For a description of the DNS parameters, refer to [Table 4-18](#).

Table 4-18 DNS Parameter Descriptions

Parameter	Description
Wan Connection	WAN connection type
Primary DNS server	Primary DNS
Secondary DNS server	Secondary DNS

3. Click **Apply**.

– End of Steps –

4.11 Configuring a Dynamic DNS

This procedure describes how to configure a dynamic DNS. The host with a dynamic IP address can then provide the domain name service.

Context

Dynamic Domain Name Server (**DDNS**) enables a server (such as Web, FTP, game server) to be a host by using a domain name (www.xxx.com) and a dynamic IP address assigned by the broadband Internet Service Provider (**ISP**). When the DDNS service is enabled, a computer can access a server by entering the host name of the server rather than the IP address.

Steps

1. Select **Advanced > Dynamic DNS**. The **DYNAMIC DNS** page is displayed, see [Figure 4-29](#).

Figure 4-29 DYNAMIC DNS Page

The screenshot shows the 'Dynamic DNS' configuration page. On the left is a navigation menu with 'Dynamic DNS' highlighted. The main content area is titled 'DYNAMIC DNS' and contains the following text:

The dynamic DNS (DDNS) feature enables you to host a server (such as Web, FTP, game server) using a domain name that you have purchased (www.xxx.com) with the dynamic (changing) IP address assigned by the broadband Internet service provider. Using a DDNS service, your friends can enter your host name to connect to your game server without knowing your IP address.

Below the text is a table with the following columns: Hostname, Username, Service, and Interface. Below the table are three buttons: Add, Edit, and Delete.

2. Click **Add**, see [Figure 4-30](#).

Figure 4-30 ADD DYNAMIC DNS Area

Configure the DDNS parameters. For a description of the parameters, refer to [Table 4-19](#).

Table 4-19 DDNS Parameter Descriptions

Parameter	Description
DDNS provider	DDNS service provider
Hostname	Fully qualified host name, such as myhost.mydomain.net
Interface	WAN-side interface PVC
Username	User name provided by the ISP
Password	Password provided by the ISP
HashKey	Hash key

3. Click **Apply**.
4. (Optional) To edit a DDNS configuration item, select it and click **Edit**.
5. (Optional) To delete a DDNS configuration item, select it and click **Delete**.

– End of Steps –

4.12 Network Tools Configuration

Network tools include the following:

- Port mapping
- IGMP proxy
- IGMP snooping
- MLD
- UPnP
- ADSL
- SNMP
- TR-064 protocol
- TR-069 protocol
- Certificates
- Printer

4.12.1 Configuring Port Mapping

This procedure describes how to configure port mapping.

Context

Port mapping refers to map multiple ports to a PVC and bridge groups. Each group works as an independent network.

A maximum of five port mapping items can be configured.

Steps

1. Select **Advanced > Network Tools > Port Mapping**. The **PORT MAPPING** page is displayed, see [Figure 4-31](#).

Figure 4-31 PORT MAPPING Page

PORT MAPPING

Port Mapping -- A maximum 5 entries can be configured

Port mapping supports mapping multiple ports to PVC and bridging groups. Each group serves as an independent network. Before using this feature, you must click "Add" and create mapping groups with appropriate LAN and WAN interfaces. If you select a group and click "Delete", the group is removed and the interfaces that are used to be in that group are automatically added to the Default group.

PORT MAPPING SETUP

Group Name	Interfaces
<input type="checkbox"/> Lan1	ethernet1, ethernet2, ethernet3, ethernet4, wlan0, wlan0-vap0, wlan0-vap1, ...

Add Edit Delete

2. Click **Add**, see [Figure 4-32](#). Configure the port mapping parameters.

Figure 4-32 ADD PORT MAPPING Area

ADD PORT MAPPING

To create a mapping group, do as follows:

1. Enter the group name, select interfaces from the available interface list and use the arrow button to add them to the grouped interface list, to create the required port mapping. Note that the group name must be unique.
2. Click "Apply" to take the changes into effect immediately.

PORT MAPPING CONFIGURATION

Group Name:

Grouped Interfaces		Available Interfaces
	<input type="button" value="→"/> <input type="button" value="←"/>	ethernet1 ethernet2 ethernet3 ethernet4 wlan0 wlan0-vap0 wlan0-vap1 wlan0-vap2
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

3. Click **Apply**.
4. (Optional) To edit a port mapping item, select it and click **Edit**.
5. (Optional) To delete a port mapping item, select it and click **Delete**.

– End of Steps –

4.12.2 Configuring IGMP Proxy

This procedure describes how to configure Internet Group Management Protocol (IGMP) proxy.

Context

The ZXHN H108N supports IGMP packet processing through IGMP proxy.

Steps

1. Select **Advanced > Network Tools > IGMP Proxy**. The **IGMP PROXY** page is displayed, see [Figure 4-33](#).

Figure 4-33 IGMP PROXY Page

- Advanced
- Advanced Wireless
- Port Forwarding
- DMZ
- SAMBA
- 3G WAN Configuration
- Parental Control
- Filtering Options
- QoS Configuration
- Firewall Settings
- DNS
- Dynamic DNS
- Network Tools
- Port Mapping
- IGMP Proxy**
- IGMP Snooping
- MLD Configuration
- UPnP
- ADSL
- SNMP
- TR-064
- TR-069
- Certificates
- Printer

IGMP PROXY

IGMP proxy enables the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. The system acts as a proxy for its hosts when you enable it by:

1. Enabling IGMP proxy on a WAN interface (upstream), which connects to a router running IGMP.
2. Enabling IGMP on a LAN interface (downstream), which connects to its host.

IGMP PROXY CONFIGURATION

Enable IGMP Proxy

PVC:8/36
 PVC:8/35

IGMP Version : (v)

Port Binding : (v)

Enable PassThrough :

Enable FastLeaving :

General Query Interval : (seconds)

General Query Response Interval : (*100 milliseconds)

Group Query Interval : (seconds)

Group Query Response Interval : (*100 milliseconds)

Group Query Count :

Last Member Query Interval : (seconds)

Last Member Query Count :

IGMP TABLE

Group Address	Interface	State
<input type="button" value="Refresh"/>		

2. Configure the IGMP proxy parameters. For a description of the parameters, refer to Table 4-20.

Table 4-20 IGMP Proxy Parameter Descriptions

Parameter	Description
Enable IGMP Proxy	Whether to enable IGMP proxy.
IGMP Version	IGMP version.
Port Binding	Port binding.
Enable PassThrough	By default, it is enabled.
Enable FastLeaving	By default, it is enabled.
General Query Interval	By default, it is 150 seconds.
General Query Response Interval	By default, it is 20 ms.
Group Query Interval	By default, it is 325 seconds.
Group Query Response Interval	By default, it is 20 ms.
Group Query Count	By default, it is 3.
Last Member Query Interval	By default, it is 1 second.

Parameter	Description
Last Member Query Count	By default, it is 1 second.

3. Click **Apply**.

– End of Steps –

4.12.3 Configuring IGMP Snooping

This procedure describes how to configure IGMP snooping.

Steps

1. Select **Advanced > Network Tools > IGMP Snooping**. The **IGMP** page is displayed, see [Figure 4-34](#).

Figure 4-34 IGMP Page

2. Configure the IGMP snooping parameters. For a description of the parameters, refer to [Table 4-21](#).

Table 4-21 IGMP Snooping Parameter Descriptions

Parameter	Description
Enabled	Whether to enable IGMP snooping
LastMemberQueryInterval	Default: 200000
HostTimeout	Default: 3000000
MrouterTimeout	Default: 1
LeaveTimeout	Default: 0

Parameter	Description
MaxGroups	Default: 100

- Click **Apply**.
- End of Steps –

4.12.4 Configuring MLD

This procedure describes how to configure Multicast Listener Discovery (MLD).

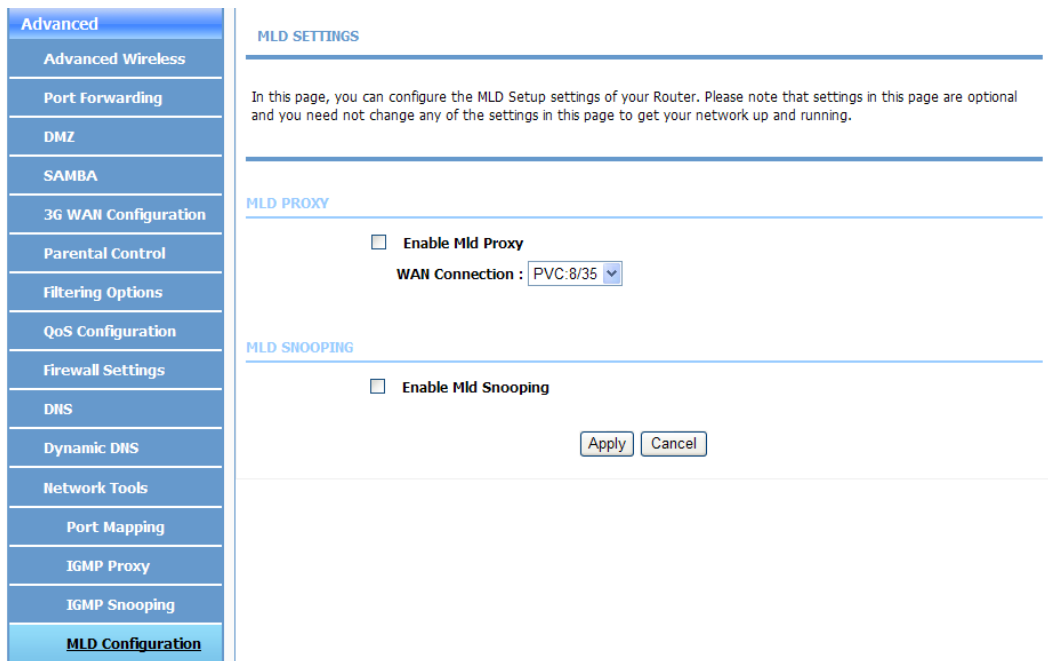
Context

The settings in this page are optional.

Steps

- Select **Advanced > Network Tools > MLD Configuration**. The **MLD SETTINGS** page is displayed, see [Figure 4-35](#).

Figure 4-35 MLD SETTINGS Page



- Configure the MLD parameters. For a description of the parameters, refer to [Table 4-22](#).

Table 4-22 MLD Parameter Descriptions

Parameter	Description
Enable Mld Proxy	Whether to enable MLD proxy
WAN Connection	WAN connection

Parameter	Description
Enable Mld Snooping	Whether to enable multicast snooping

- Click **Apply**.

– End of Steps –

4.12.5 Configuring UPnP

This procedure describes how to configure Universal Plug and Play (UPnP).

Context

UPnP is a set of networking protocols that provides compatibility among networking devices, software, and peripherals.

After UPnP is configured, a device can be dynamically added to a network to obtain an IP address, announcing its functions and knowing the functions of the other devices.

Steps

- Select **Advanced > Network Tools > UPnP**. The **UPnP** page is displayed.
- Configure the UPnP parameters. For a description of the parameters, refer to [Table 4-23](#).

Table 4-23 UPnP Parameter Descriptions

Parameter	Description
Enable UPnP	Whether to enable the UPnP function
WAN Connection	WAN-side interface
LAN Connection	LAN-side interface

- Click **Apply**.

– End of Steps –

4.12.6 Configuring the ADSL

This procedure describes how to configure the Asymmetric Digital Subscriber Line (ADSL) settings of the ZXHN H108N.

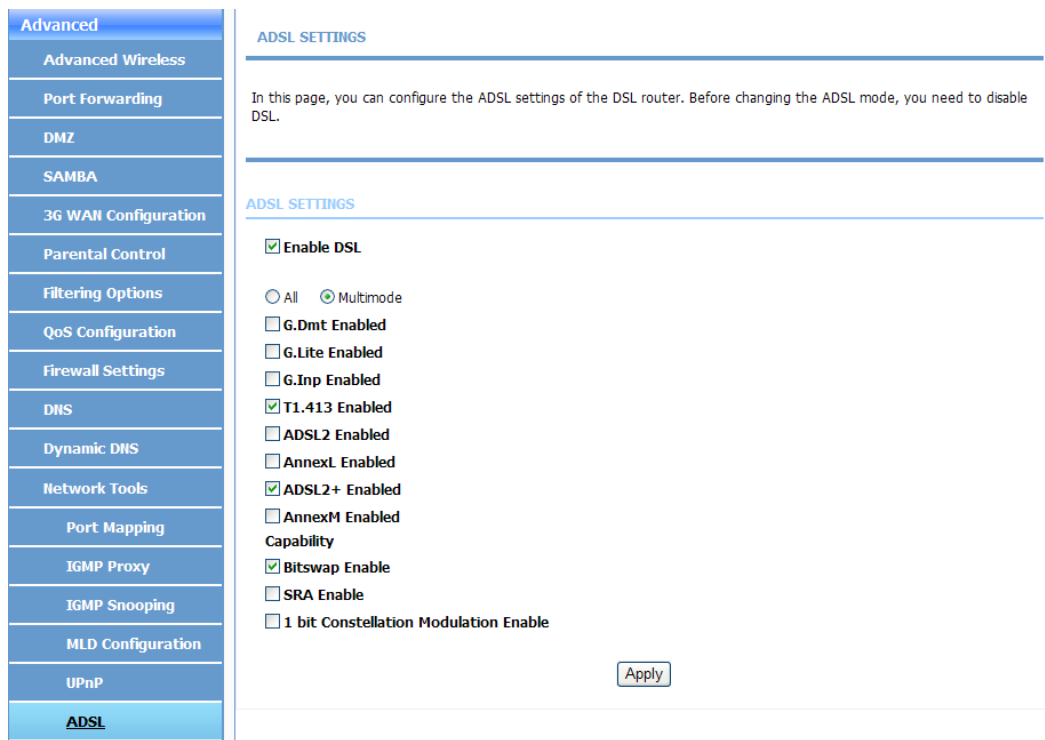
Context

Before changing the ADSL mode, you need to disable Digital Subscriber Line (DSL).

Steps

- Select **Advanced > Network Tools > ADSL**. The **ADSL SETTINGS** page is displayed, see [Figure 4-36](#).

Figure 4-36 ADSL SETTINGS Page



2. Select the check boxes to enable the ADSL functions as required.
3. Click **Apply**.

– End of Steps –

4.12.7 Configuring the SNMP

This procedure describes how to configure the Simple Network Management Protocol (SNMP) protocol.

Steps

1. Select **Advanced > Network Tools > SNMP**. The **SNMP CONFIGURATION** page is displayed, see [Figure 4-37](#).

Figure 4-37 SNMP CONFIGURATION Page

2. Configure the SNMP parameters. For a description of the parameters, refer to [Table 4-24](#).

Table 4-24 SNMP Parameter Descriptions

Parameter	Description
Enable SNMP Agent	Whether to enable SNMP agent
Read Community	Default: public
Set Community	Default: private
Trap Manager IP	Management IP address of the trap server
Trap Community	Trap server Community
Trap Version	Trap server version

3. Click **Apply**.

– End of Steps –

4.12.8 Configuring the TR-064 Protocol

This procedure describes how to configure the TR-064 protocol.

Steps

1. Select **Advanced > Network Tools > TR-064**. The **TR-064 CONFIGURATION** page is displayed, see [Figure 4-38](#).

Figure 4-38 TR-064 CONFIGURATION Page

Advanced	TR064 CONFIGURATION
Advanced Wireless	This page is used to configure the TR064 protocol.
Port Forwarding	
DMZ	
SAMBA	TR064 CONFIGURATION
3G WAN Configuration	<input type="checkbox"/> Enable TR064
Parental Control	Apply Cancel
Filtering Options	
QoS Configuration	
Firewall Settings	
DNS	
Dynamic DNS	
Network Tools	
Port Mapping	
IGMP Proxy	
IGMP Snooping	
MLD Configuration	
UPnP	
ADSL	
SNMP	
TR-064	

2. Select **Enable TR064**.
3. Click **Apply**.

– End of Steps –

4.12.9 Configuring the TR-069 Protocol

This procedure describes how to configure the TR-069 protocol.

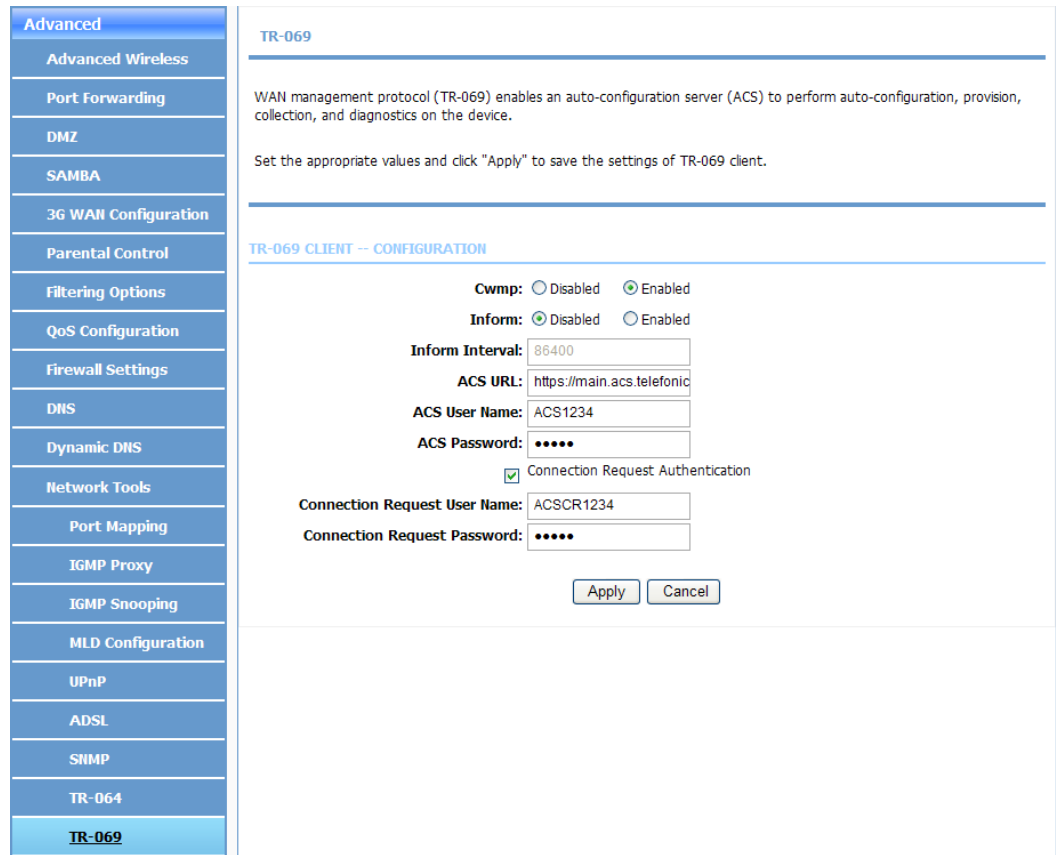
Context

TR-069 is a WAN management protocol. As a bidirectional [SOAP/HTTP](#) based protocol, it provides communication between an ADSL router and an auto configuration server.

Steps

1. Select **Advanced > Network Tools > TR-069**. The **TR-069** page is displayed, see [Figure 4-39](#).

Figure 4-39 TR-069 Page



2. Configure the TR-069 protocol parameters. For a description of the parameters, refer to Table 4-25.

Table 4-25 TR-069 Parameter Descriptions

Parameter	Description
Cwmp	Whether to enable remote access control
Inform	Whether to enable inform packet announcement
Inform Interval	Periodic informing interval
ACS URL	NMS server URL
ACS User Name/ACS Password	User name and password for the device to access the NMS server
Connection Request Authentication	Whether to enable connection request authentication
Connection Request User Name/Connection Request Password	User name and password for the NMS server to access the device

3. Click **Apply**.

– End of Steps –

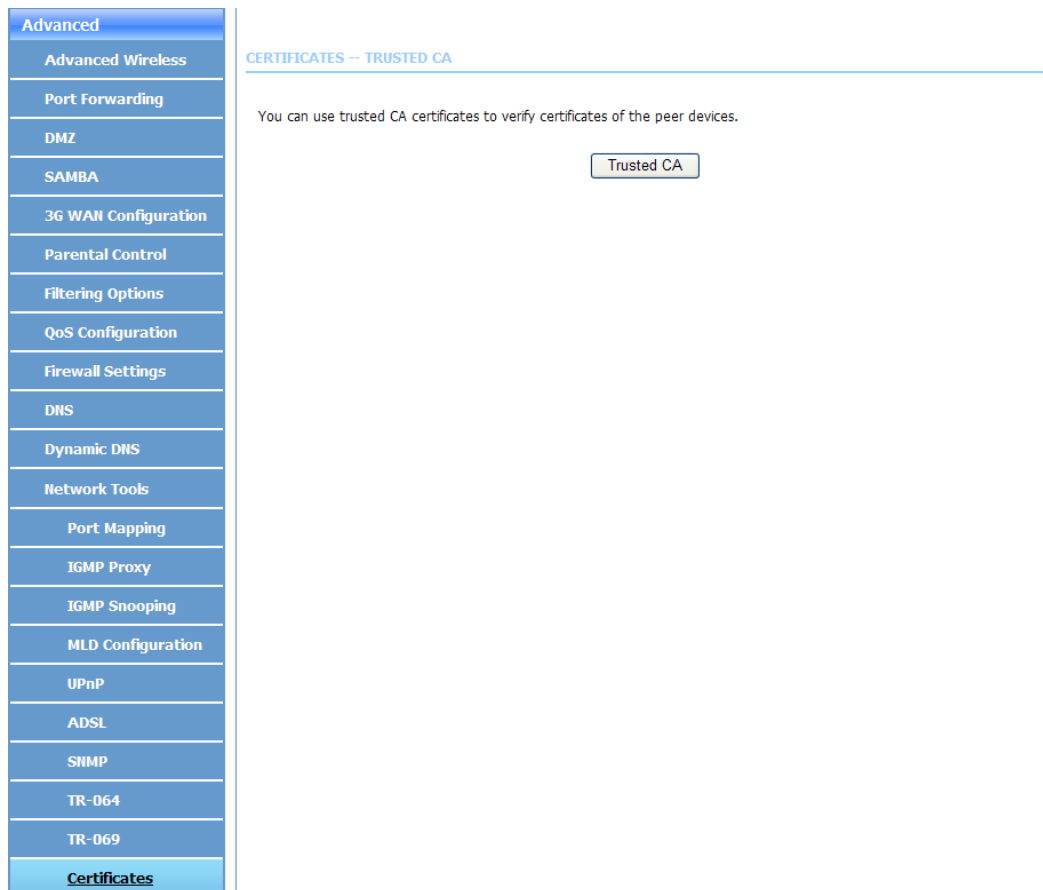
4.12.10 Configuring Certificates

This procedure describes how to configure Certificate Authentication (CA) certificates.

Steps

1. Select **Advanced > Network Tools > Certificates**. The **CERTIFICATES-TRUSTED CA** page is displayed, see [Figure 4-40](#).

Figure 4-40 CERTIFICATES-TRUSTED CA Page



2. Click **Trusted CA**. The trusted CA configuration area is displayed, see [Figure 4-41](#).

Figure 4-41 Certificates–Trusted CA Configuration Area

CERTIFICATES -- TRUSTED CA

In this page, you can add, view, or remove certificates. You can use the CA certificates function to verify certificates of the peer devices. Note: 1. Only one certificate can be saved. 2. You must synchronize your time before using this function.

TRUSTED CA (CERTIFICATE AUTHORITY) CERTIFICATES

Name	Subject	Type	Action
------	---------	------	--------

3. Click **Input Certificate**. The **IMPORT CA CERTIFICATE** area is displayed, see [Figure 4-42](#).

Figure 4-42 TRUSTED CA CERTIFICATES Page–IMPORT CA CERTIFICATE

TRUSTED CA CERTIFICATES

Enter the certificate name and paste the contents.

IMPORT CA CERTIFICATE

Certificate Name:

Certificate:

```
-----BEGIN CERTIFICATE-----
<Insert certificate here>
-----END CERTIFICATE-----
```

4. In the **Certificate Name** text box, enter the certificate name. In the **Certificate** text box, enter the certificate content.

- Click **Apply**.
– End of Steps –

4.12.11 Configuring a Printer

This procedure describes how to configure a printer.

Steps

- Select **Advanced > Network Tools > Printer**. The **PRINT SERVER SETTINGS** page is displayed, see [Figure 4-43](#).

Figure 4-43 PRINT SERVER SETTINGS Page

- Configure the printer parameters. For a description of the parameters, refer to [Table 4-26](#).

Table 4-26 Printer Parameter Descriptions

Parameter	Description
Enable	Whether to enable the printer
Printer Name	Printer name

3. Click **Apply**.

– End of Steps –

4.13 Routing Configuration

4.13.1 Configuring a Static Route

This procedure describes how to configure a static route.

Steps

1. Select **Advanced > Routing > Static Route**. The **STATIC ROUTE** page is displayed, see [Figure 4-44](#).

Figure 4-44 STATIC ROUTE Page

2. Click **Add**. The **STATIC ROUTE ADD** area is displayed, see [Figure 4-45](#).

Figure 4-45 STATIC ROUTE ADD Area

Configure the static route parameters. For a description of the parameters, refer to [Table 4-27](#).

Table 4-27 Static Route Parameter Descriptions

Parameter	Description
Destination Network Address	Destination network address
Subnet Mask	Subnet mask
Use Interface	Broadband connection used for static route forwarding

3. Click **Apply**.
 4. (Optional) To edit a static route, select it and click **Edit**.
 5. (Optional) To delete a static route, select it and click **Delete**.
- End of Steps –

4.13.2 Configuring an IPv6 Static Route

This procedure describes how to configure an IPv6 static route.

Steps

1. Select **Advanced > Routing > IPv6 Static Route**. The **IPV6 STATIC ROUTE** page is displayed, see [Figure 4-46](#).

Figure 4-46 IPV6 STATIC ROUTE Page



2. Click **Add**. The **IPV6 STATIC ROUTE ADD** area is displayed, see [Figure 4-47](#).

Figure 4-47 IPv6 STATIC ROUTE ADD Area

The screenshot shows a configuration window titled "IPv6 STATIC ROUTE ADD". It contains the following elements:

- Enable:** A checkbox that is currently unchecked.
- Destination Network Address:** A text input field that is empty.
- Use Interface:** A dropdown menu with "PVC:8/35" selected.
- Buttons:** "Apply" and "cancel" buttons at the bottom right.

Configure the IPv6 static route parameters. For a description of the parameters, refer to [Table 4-28](#).

Table 4-28 IPv6 Static Route Parameter Descriptions

Parameter	Description
Enable	Whether to enable the IPv6 static route function
Destination Network Address	Destination network address
Use Interface	Broadband connection used for static route forwarding

3. Click **Apply**.
4. (Optional) To edit an IPv6 static route, select it and click **Edit**.
5. (Optional) To delete an IPv6 static route, select it and click **Delete**.

– End of Steps –

4.13.3 Configuring a Policy Route

This procedure describes how to configure a policy route.

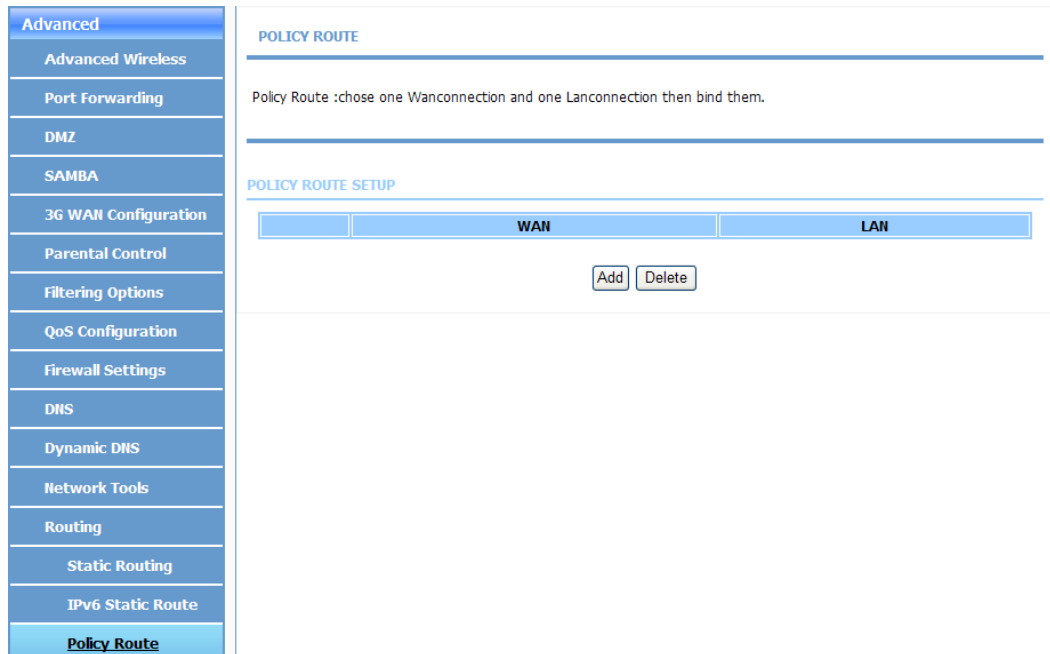
Context

A policy route is a routing rule that enables packets to be forwarded based on the specified policy.

Steps

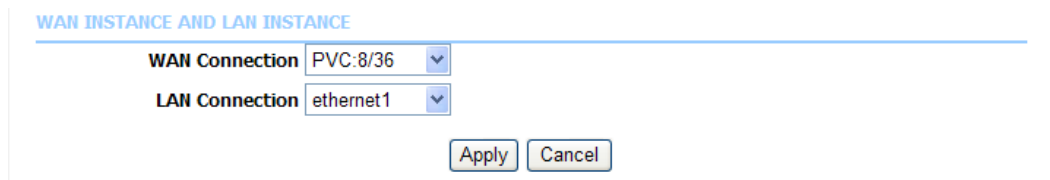
1. Select **Advanced > Routing > Policy Route**. The **POLICY ROUTE** page is displayed, see [Figure 4-48](#).

Figure 4-48 POLICY ROUTE Page



2. Click **Add**. The **WAN INSTANCE AND LAN INSTANCE** area is displayed, see Figure 4-49.

Figure 4-49 WAN INSTANCE AND LAN INSTANCE Area



Configure the policy route parameters. For a description of the parameters, refer to Table 4-29.

Table 4-29 Policy Route Parameter Descriptions

Parameter	Description
WAN Connection	WAN interface corresponding to the route
LAN Connection	LAN interface corresponding to the route

3. Click **Apply**.
4. (Optional) To delete a policy route, select it and click **Delete**.

– End of Steps –

4.13.4 Configuring the Default Gateway

This procedure describes how to configure the default gateway.

Steps

1. Select **Advanced > Routing > Default Gateway**. The **DEFAULT GATEWAY** page is displayed, see [Figure 4-50](#).

Figure 4-50 DEFAULT GATEWAY Page

2. From the **Assigned the Default Gateway** list, select the default IPv4 gateway. From the **Assigned the IPv6 Default Gateway** list, select the default IPv6 gateway.
3. Click **Apply**.

– End of Steps –

4.13.5 Configuring the RIP

This procedure describes how to configure the Routing Information Protocol ([RIP](#)).

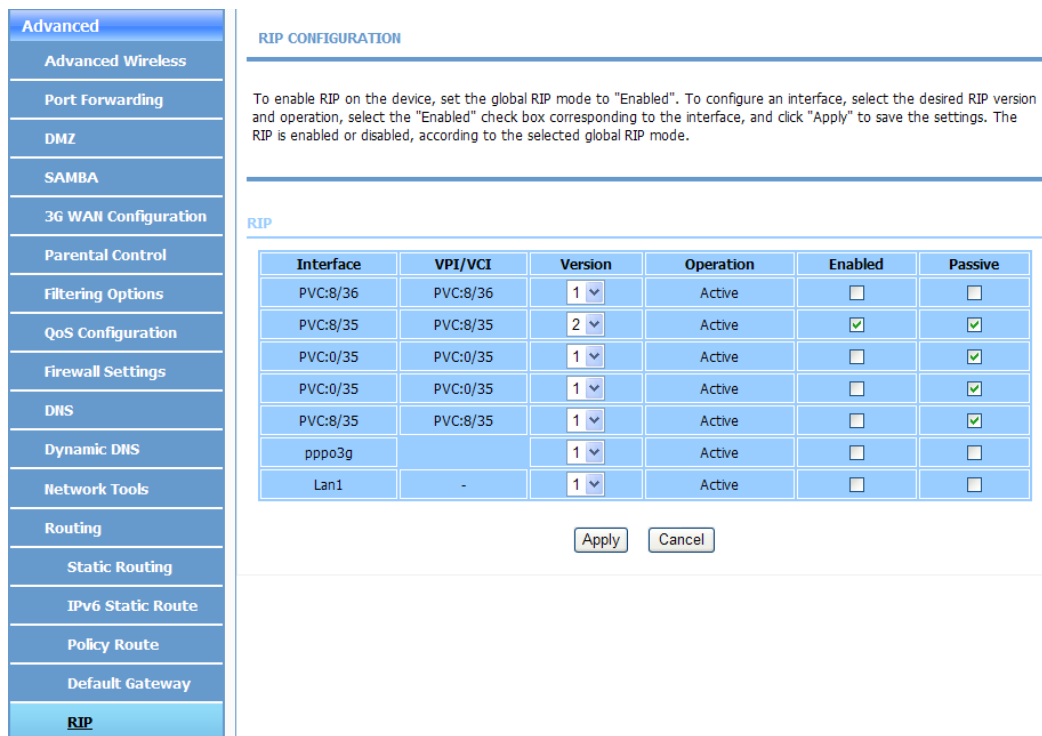
Context

The RIP is a dynamic routing protocol based on the distance-vector algorithm, exchanging routing information through User Datagram Protocol ([UDP](#)) packets. The RIP has its own routing algorithm, and can automatically adapt to network topology changes. It has higher requirements than the static routing, and occupies more network resources.

Steps

1. Select **Advanced > Routing > RIP**. The **RIP CONFIGURATION** page is displayed, see [Figure 4-51](#).

Figure 4-51 RIP CONFIGURATION Page



- In the **RIP** area, configure the RIP parameters. For a description of the parameters, refer to [Table 4-30](#).

Table 4-30 RIP Parameter Descriptions

Parameter	Description
Interface	WAN interface
VPI/VCI	VPI or VCI corresponding to the WAN interface
Version	RIP version
Operation	Operation status

- Click **Apply**.
– End of Steps –

4.13.6 Configuring the RIPng Protocol

This procedure describes how to configure the Routing Information Protocol next generation (RIPng)

Steps

- Select **Advanced > Routing > RIPng**. The **RIPNG CONFIGURATION** page is displayed, see [Figure 4-52](#).

Figure 4-52 RIPNG CONFIGURATION Page

RIPNG CONFIGURATION

To enable RIP for IPv6 (RIPng) on the interface, select the corresponding "Enabled" check box and click "Apply" to save the settings. The RIPng is enabled or disabled accordingly.

RIPNG

Interface	VPI/VCI	Enabled
PVC:8/35	PVC:8/35	<input type="checkbox"/>
ppp03g		<input type="checkbox"/>

Apply Cancel

- In the **RIPNG** list, select **Enable**.
- Click **Apply**.

– End of Steps –

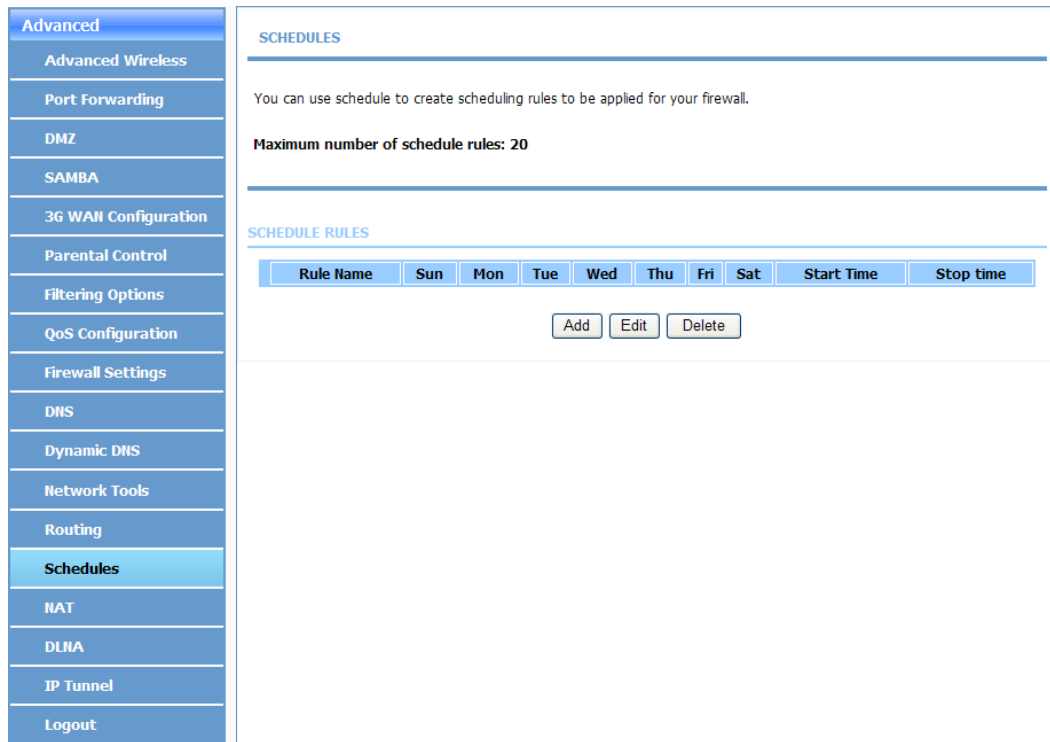
4.14 Configuring Schedules

This procedure describes how to configure schedules, which can be used to create scheduling rules.

Steps

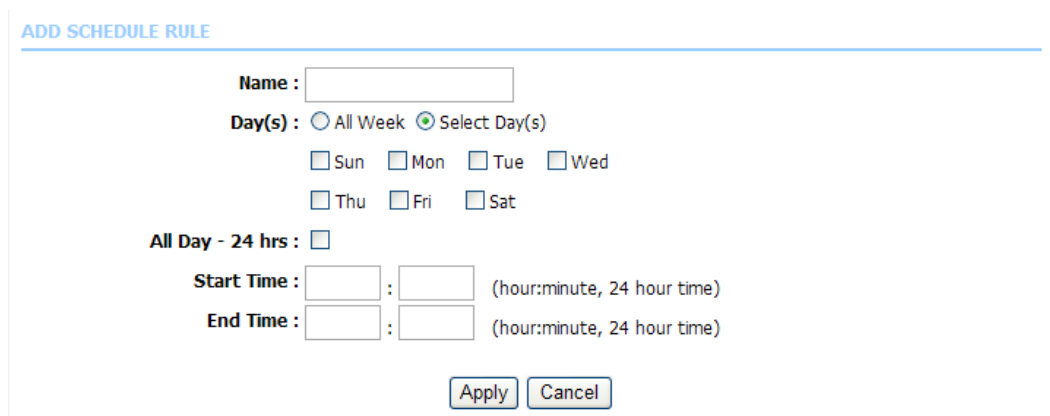
- Select **Advanced > Schedules**. The **SCHEDULES** page is displayed, see [Figure 4-53](#).

Figure 4-53 SCHEDULES Page



2. Click **Add**. The **ADD SCHEDULE RULE** area is displayed, see Figure 4-54.

Figure 4-54 ADD SCHEDULE RULE Area



Configure the schedule parameters. For a description of the parameters, refer to Table 4-31.

Table 4-31 Schedule Parameter Descriptions

Parameter	Description
Name	Schedule name, such as Weekday rule .
Day(s)	Select the check boxes corresponding to the desired days or select All Week to select the whole week.
All Day-24 hrs	The schedule takes effect for the whole day of the selected day(s).

Parameter	Description
Start Time	Starting time of the period that the schedule is effective. This parameter needs to be configured when All Day is not selected.
End Time	Ending time of the period that the schedule is effective. This parameter needs to be configured when All Day is not selected.

3. Click **Apply**.
4. (Optional) To edit a schedule, select it and click **Edit**.
5. (Optional) To delete a schedule, select it and click **Delete**.

– End of Steps –

4.15 Configuring NAT

This procedure describes how to configure Network Address Translation (NAT).

Context

NAT allows the hosts within a private network to transparently access the hosts in the external network. Sessions are uni-directional and outbound from the private network.

Steps

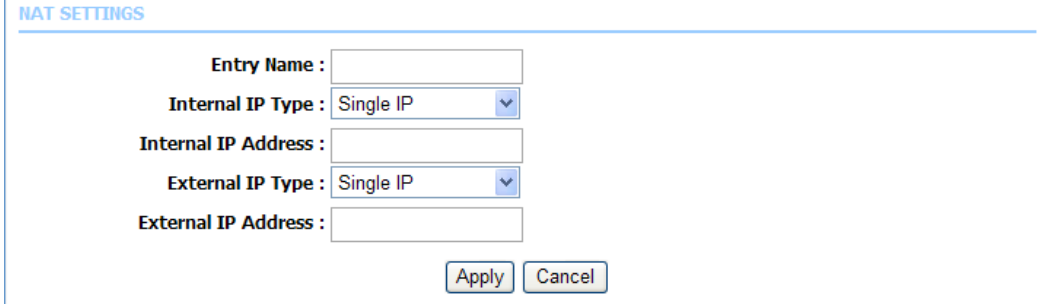
1. Select **Advanced > NAT**. The **NAT** page is displayed, see [Figure 4-55](#).

Figure 4-55 NAT Page

The screenshot shows the NAT configuration page. On the left is a navigation menu with the following items: Advanced, Advanced Wireless, Port Forwarding, DMZ, SAMBA, 3G WAN Configuration, Parental Control, Filtering Options, QoS Configuration, Firewall Settings, DNS, Dynamic DNS, Network Tools, Routing, Schedules, **NAT**, DLNA, IP Tunnel, and Logout. The main content area is titled 'NAT' and contains the following text: 'Traditional NAT would allow hosts within a private network to transparently access hosts in the external network, in most cases. In a traditional NAT, sessions are uni-directional, outbound from the private network. Sessions in the opposite direction may be allowed on an exceptional basis using static address maps for pre-selected hosts.' Below this text is a section titled 'NAT TABLES' which contains a table with three columns: 'Name', 'Internal IP Address', and 'External IP Address'. At the bottom of this section are three buttons: 'Add', 'Edit', and 'Delete'.

2. Click **Add**. The **NAT SETTINGS** area is displayed, see [Figure 4-56](#).

Figure 4-56 NAT SETTINGS Area



The screenshot shows a web interface for NAT settings. The title is "NAT SETTINGS". Below the title, there are five rows of configuration options:

- Entry Name :
- Internal IP Type : (dropdown menu)
- Internal IP Address :
- External IP Type : (dropdown menu)
- External IP Address :

At the bottom right, there are two buttons: "Apply" and "Cancel".

3. Configure the NAT parameters.
4. Click **Apply**.
5. (Optional) To edit an NAT item, select it and click **Edit**.
6. (Optional) To delete an NAT item, select it and click **Delete**.

– End of Steps –

4.16 Enabling DLNA

This procedure describes how to enable Digital Living Network Alliance ([DLNA](#)).

Steps

1. Select **Advanced > DLNA**. The **DLNA** page is displayed, see [Figure 4-57](#).

Figure 4-57 DLNA Page

The screenshot shows a web interface for configuring DLNA. On the left is a vertical menu with the following items: Advanced, Advanced Wireless, Port Forwarding, DMZ, SAMBA, 3G WAN Configuration, Parental Control, Filtering Options, QoS Configuration, Firewall Settings, DNS, Dynamic DNS, Network Tools, Routing, Schedules, NAT, **DLNA**, IP Tunnel, and Logout. The 'DLNA' item is highlighted. The main content area is titled 'DLNA' and contains the text 'You can enable or disable DLNA.' Below this is a section titled 'DLNA SETTING' which includes a checkbox labeled 'Enable DLNA :'. The checkbox is currently unchecked. At the bottom right of this section are two buttons: 'Apply' and 'Cancel'.

2. Select **Enable DLNA**.
 3. Click **Apply**.
- End of Steps –

4.17 IP Tunnel Configuration

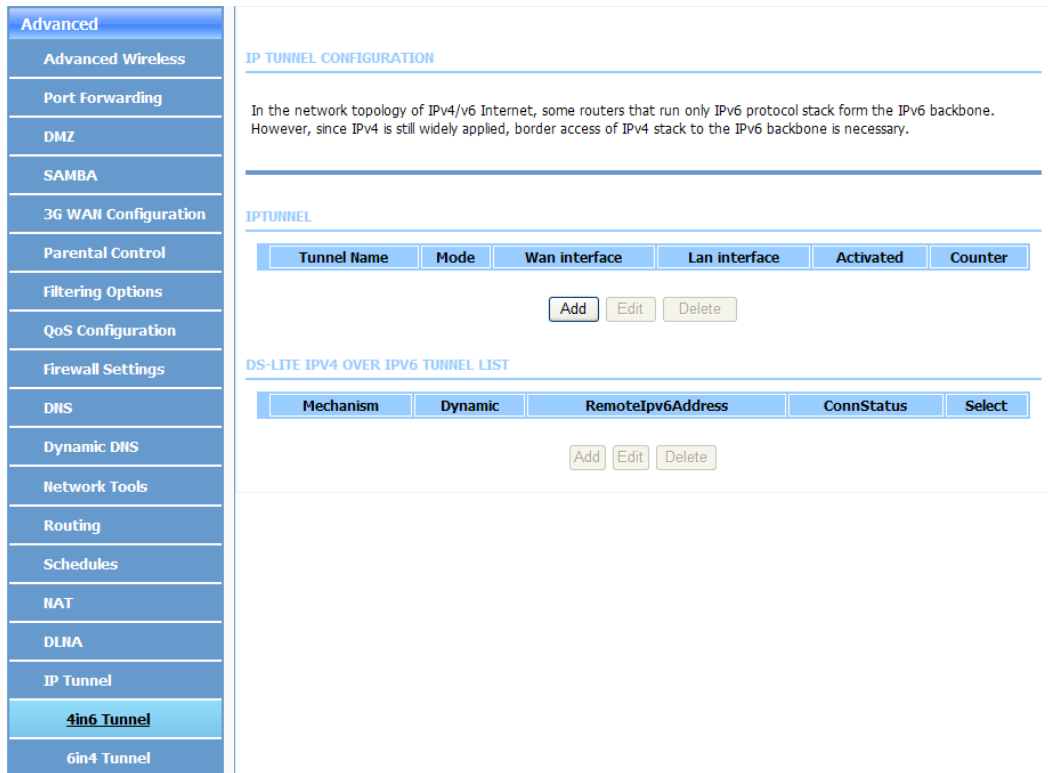
4.17.1 Configuring the 4in6 Tunnel

This procedure describes how to configure the 4in6 Tunnel.

Steps

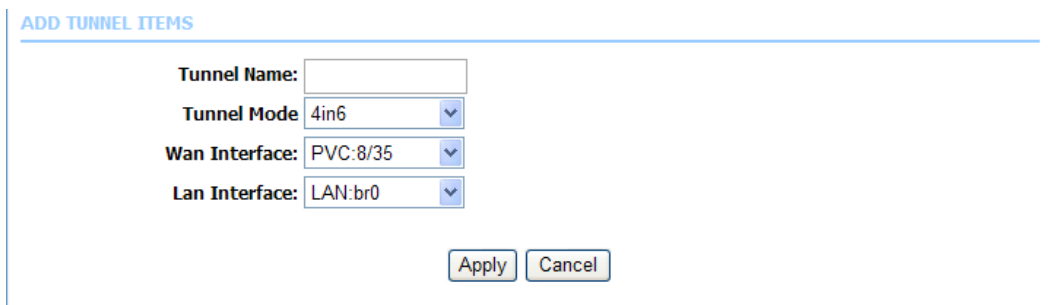
1. Select **Advanced > IP Tunnel > 4in6 Tunnel**. The **IP TUNNEL CONFIGURATION** page is displayed, see [Figure 4-58](#).

Figure 4-58 IP TUNNEL CONFIGURATION Page



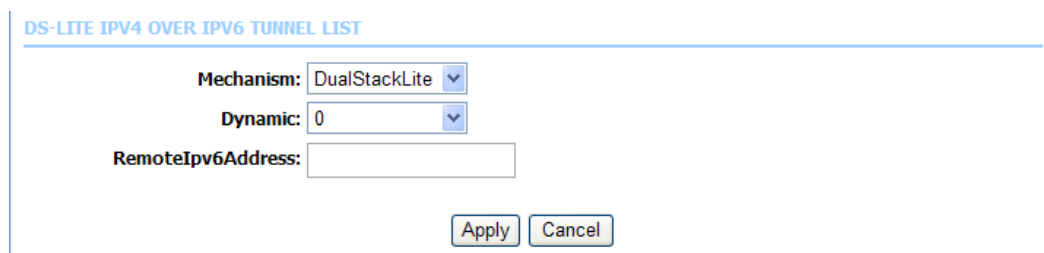
2. Click **Add** below the **IP Tunnel** table. The **ADD TUNNEL ITEMS** area is displayed, see Figure 4-59.

Figure 4-59 ADD TUNNEL ITEMS Area



3. Configure the tunnel parameters.
4. Click **Apply**.
5. Click **Add** below the **DS-Lite IPv4 over IPv6 Tunnel List** table. The **DS-LITE IPV4 OVER IPV6 TUNNEL LIST** area is displayed, see Figure 4-60.

Figure 4-60 DS-LITE IPV4 OVER IPV6 TUNNEL LIST Area



DS-LITE IPV4 OVER IPV6 TUNNEL LIST

Mechanism: DualStackLite

Dynamic: 0

RemoteIpv6Address:

Apply Cancel

6. Configure the parameters of the DS-Lite IPv4 over IPv6 tunnel.
 7. Click **Apply**.
 8. (Optional) Perform the following operation as required:
 - To delete a tunnel, click **Delete** below the **IP Tunnel** table.
 - To edit a tunnel, click **Edit** below the **IP Tunnel** table.
 - To delete a DS-Lite IPv4 over IPv6 tunnel, click **Delete** below the **DS-Lite IPv4 over IPv6 Tunnel List** table.
 - To edit a DS-Lite IPv4 over IPv6 tunnel, click **Edit** below the **DS-Lite IPv4 over IPv6 Tunnel List** table.
- End of Steps –

4.17.2 Configuring the 6in4 Tunnel

This procedure describes how to configure the 6in4 tunnel.

Steps

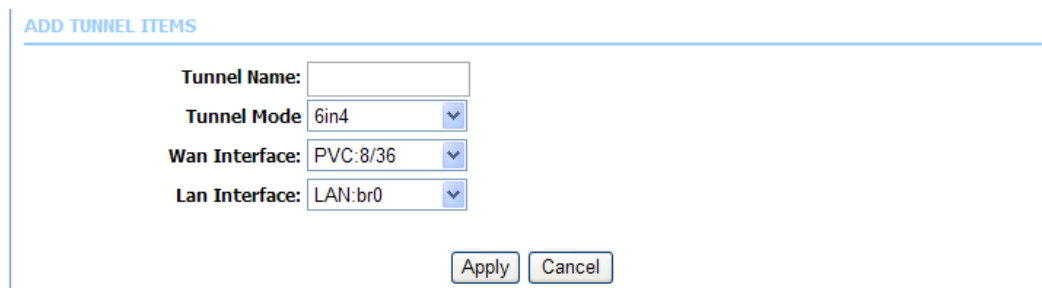
1. Select **Advanced > IP Tunnel > 6in4 Tunnel**. The **IP TUNNEL CONFIGURATION** page is displayed, see [Figure 4-61](#).

Figure 4-61 IP TUNNEL CONFIGURATION Page



- Click **Add** below the **IP Tunnel** table. The **ADD TUNNEL ITEMS** area is displayed, see Figure 4-62.

Figure 4-62 ADD TUNNEL ITEMS Area



- Configure the tunnel parameters.
- Click **Apply**.
- Click **Add** below the **IPv6 Rapid Deployment** table. The **IPv6 RAPID DEPLOYMENT LIST** area is displayed, see Figure 4-63.

Figure 4-63 IPV6 RAPID DEPLOYMENT LIST Area

IPV6 RAPID DEPLOYMENT LIST

Mechanism: Ipv6RapidDeplc

Dynamic: 0

IPv4MaskLen:

Prefix:

BorderRelayAddress:

Apply Cancel

6. Configure the parameters of IPv6 rapid deployment.
7. Click **Apply**.
8. (Optional) Perform the following operation as required:
 - To delete a tunnel, click **Delete** below the **IP Tunnel** table.
 - To edit a tunnel, click **Edit** below the **IP Tunnel** table.
 - To delete an IPv6 rapid deployment item, click **Delete** below the **IPv6 Rapid Deployment** table.
 - To edit an IPv6 rapid deployment item, click **Edit** below the **IPv6 Rapid Deployment** table.

– End of Steps –

This page intentionally left blank.

Chapter 5

System Management and Maintenance

Table of Contents

Enabling Global IPv6.....	5-1
Configuring System Management.....	5-2
Updating the Firmware	5-3
Access Control Configuration	5-3
Diagnosis	5-7
Configuring Logs.....	5-9

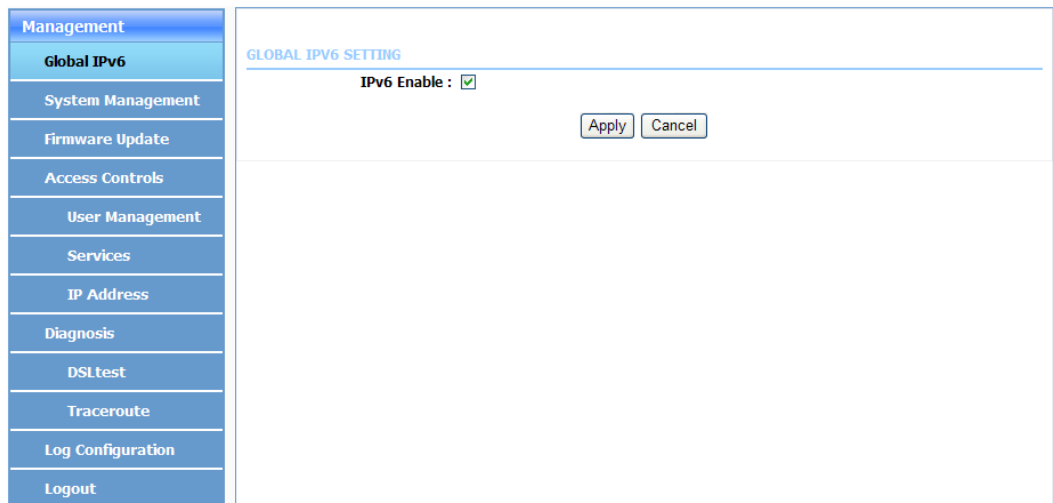
5.1 Enabling Global IPv6

This procedure describes how to enable global IPv6.

Steps

1. Select **Management > Global IPv6**. The **GLOBAL IPV6 SETTING** page is displayed, see Figure 5-1.

Figure 5-1 GLOBAL IPV6 SETTING Page



2. Select **IPv6 Enable**.
3. Click **Apply**.

– End of Steps –

5.2 Configuring System Management

This procedure describes how to reboot the ZXHN H108N device, back up the configuration file of the ZXHN H108N, upgrade the ZXHN H108N, and restore the factory default settings.

Steps

1. Select **Management > System Management**. The **System Management** page is displayed, see [Figure 5-2](#).

Figure 5-2 System Management Page

The screenshot shows the 'System Management' page with a left-hand navigation menu and a main content area. The navigation menu includes: Management, Global IPv6, System Management (highlighted), Firmware Update, Access Controls, Diagnosis, Log Configuration, and Logout. The main content area is titled 'SYSTEM -- REBOOT' and contains a 'Reboot' button. Below this is 'SYSTEM -- BACKUP SETTINGS' with a 'Backup Setting' button. Next is 'SYSTEM -- UPDATE SETTINGS' with a 'Settings File Name' input field, a 'Browse...' button, and an 'Update Setting' button. Finally, 'SYSTEM -- RESTORE DEFAULT SETTINGS' has a 'Restore Default Setting' button.

2. Perform the following operation as required:
 - To reboot the ZXHN H108N, click **Reboot**.
 - To back up the configuration file of the ZXHN H108N, click **Backup Setting**.
 - To upgrade the ZXHN H108N, click **Browse** to select a configuration file, and then click **Update Setting**.
 - To restore the factory default settings, click **Restore Default Setting**.

– End of Steps –

5.3 Updating the Firmware

This procedure describes how to import a firmware image file.

Prerequisite

A firmware image update file has been obtained from the ISP.

Steps

1. Select **Management > Firmware Update**. The **FIRMAWRE UPDATE** page is displayed, see [Figure 5-3](#).

Figure 5-3 FIRMAWRE UPDATE

The screenshot shows the 'FIRMAWRE UPDATE' page. On the left is a navigation menu with the following items: Management, Global IPv6, System Management, **Firmware Update**, Access Controls, Diagnosis, Log Configuration, and Logout. The main content area is titled 'FIRMAWRE UPDATE' and contains the following text:

Step 1: Obtain an updated firmware image file from your ISP.

Step 2: Enter the directory of the image file in the following field or click "Browse" to select the image file.

Step 3: Click "Update Firmware" to upload the new image file.

Note: The update process takes about 2 minutes. The DSL router automatically reboots after the update. Please DO NOT power off the router during the update.

Below the instructions, the current firmware version is 2.1.0 and the date is 08/03/2012-19:38:48. There is a 'Select File:' text box followed by a 'Browse...' button. Below that is a 'Clear Config:' checkbox. At the bottom right is an 'Update Firmware' button.

2. Click **Browse** to select a firmware image update file.
3. Click **Firmware Update**.

– End of Steps –

5.4 Access Control Configuration

Access control configuration includes the following:

- User management
- Service configuration
- IP address configuration

5.4.1 Managing Users

This procedure describes user management.

Context

For user permissions, refer to [Table 5-1](#).

Table 5-1 User Permissions

Role	User Name/Password	Permission
Administrator	1234/1234	Can configure all the parameters on the web pages.
Common users	user/user	Can only view some configurations on the web pages.

Steps

1. Select **Management > Access Controls > User Management**. The **ACCOUNT PASSWORD** page is displayed, see [Figure 5-4](#).

Figure 5-4 ACCOUNT PASSWORD Page

2. Configure user parameters. For a description of the parameters, refer to [Table 5-2](#).

Table 5-2 User Parameter Descriptions

Parameter	Description
Username	<ul style="list-style-type: none"> ● 1234 ● user ● support
New Username	Customized user name

Parameter	Description
Current Password	Default user names and passwords: <ul style="list-style-type: none"> ● 1234/1234 ● user/user ● support/support
New Password	Customized user password
Confirm Password	Confirmed password

3. Click **Apply**.
4. In the **Web Idle Timeout** text box, enter the idle timeout time. For a description of the parameter, refer to [Table 5-3](#).

Table 5-3 Web Idle Timeout Parameter Descriptions

Parameter	Description
Web Idle Timeout	Timeout time for logging in to the web site. Default: 29 minutes If a user does not perform any operations during this time, the user logs out of the system.

5. Click **Apply**.

– End of Steps –

5.4.2 Configuring Services

This procedure describes how to configure a service control list to enable or disable services.

Steps

1. Select **Management > Access Controls > Services**. The **SERVICES** page is displayed, see [Figure 5-5](#).

Figure 5-5 SERVICES Page



- From the **Select WAN Connections** list, select a WAN connection.
- In the service list, select the corresponding check boxes of **LAN** and **WAN**, and configure the parameters of **WAN Access Source Host(IP / Mask) :(Dst Port)**.
- Click **Apply**.

– End of Steps –

5.4.3 Enabling IP Address Access Control Mode

This procedure describes how to enable IP address access control mode.

Context

If IP address access control mode is enabled, the IP addresses contained in the access control list can access the local management services. If access control mode is disabled, the system does not validate the IP addresses of incoming packets. Services are the system applications listed in the service control list.

Steps

- Select **Management > Access Controls > IP Address**. The **IP ADDRESS** page is displayed, see [Figure 5-6](#).

Figure 5-6 IP ADDRESS Page

Management

- Global IPv6
- System Management
- Firmware Update
- Access Controls
- User Management
- Services
- IP Address**
- Diagnosis
- Log Configuration
- Logout

IP ADDRESS

If you enable the IP Address Access Control mode, IP addresses contained in the Access Control List can access the local management services. If the Access Control mode is disabled, the system does not validate IP addresses of incoming packets. Services are the system applications listed in the Service Control List.

Enter the IP address of the management station allowed to access the local management services, and click "Apply".

ACCESS CONTROL -- IP ADDRESSES

Enable Access Control Mode

IP

2. Click **Add**. In the **IP Address** text box, enter an IP address.
3. Click **Apply**.
4. Select **Enable Access Control Mode**.

– End of Steps –

5.5 Diagnosis

5.5.1 Implementing the DSL Test

This procedure describes how to implement the Digital Subscriber Line (**DSL**) test.

Steps

1. Select **Management > Diagnostics > DSLtest**. The **DIAGNOSTICS** page is displayed, see [Figure 5-7](#).

Figure 5-7 DIAGNOSTICS Page

Management

- Global IPv6
- System Management
- Firmware Update
- Access Controls
- Diagnosis
- DSLtest**
- Traceroute
- Log Configuration
- Logout

DIAGNOSTICS

The DSL router can test your DSL connection through the following test items. If a test item displays "Fail", click "Run Diagnostic Test" again to confirm the fail state.

WAN Connection PVC:8/36

2. From the **WAN Connection** list, select a WAN connection.

3. Click **Run Diagnostic Test**.

– End of Steps –

5.5.2 Diagnosing a Trace Route

This procedure describes how to diagnose a trace route.

Steps

1. Select **Management > Diagnostics > Traceroute**. The **TRACEROUTE DIAGNOSIS** page is displayed, see [Figure 5-8](#).

Figure 5-8 TRACEROUTE DIAGNOSIS Page

2. Configure the trace route diagnosis parameters, and then click **Traceroute**.

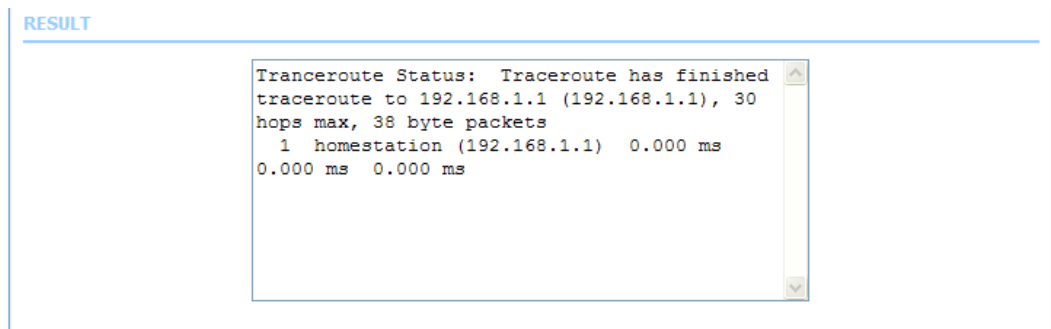
For a description of the trace route diagnosis parameters, refer to [Table 5-4](#).

Table 5-4 Parameter Descriptions for Trace Route Diagnosis

Parameter	Description
Host	Host IP address
Max TTL	Maximum Time To Live
Wait times	Waiting time

The result of trace route diagnosis is displayed in the **Result** text box, see [Figure 5-9](#).

Figure 5-9 Trace Route Diagnosis Result



– End of Steps –

5.6 Configuring Logs

This procedure describes how to configure logs.

Prerequisite

The time of the modem has been set in **Setup > Time and Date**.

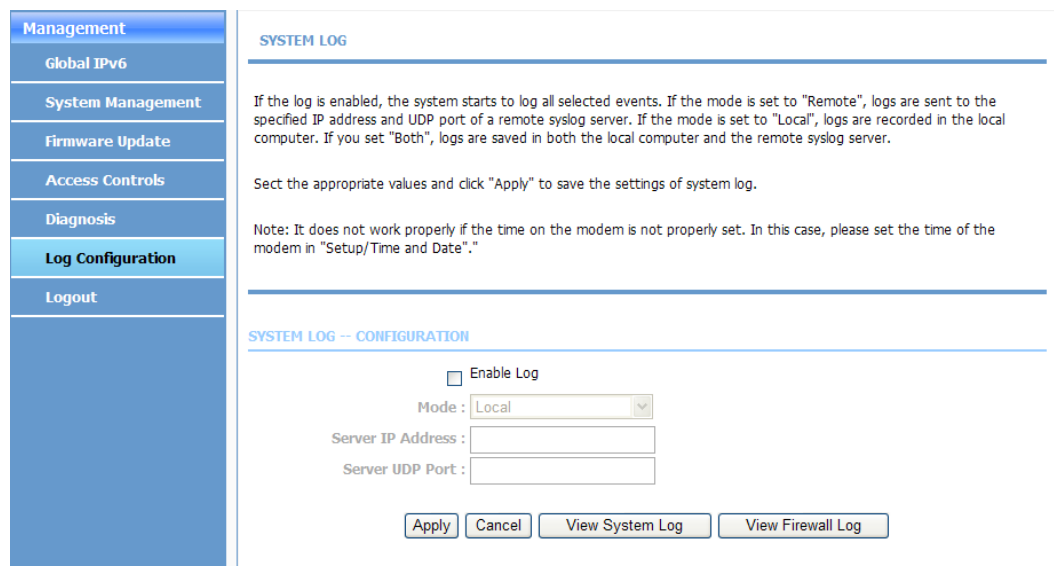
Context

If the log function is enabled, the ZXHN H108N records all the selected events.

Steps

1. Select **Management > Log Configuration**. The **SYSTEM LOG** page is displayed, see [Figure 5-10](#).

Figure 5-10 SYSTEM LOG Page



2. Configure the log parameters. For a description of the parameters, refer to [Table 5-5](#).

Table 5-5 Log Configuration Parameter Descriptions

Parameter	Description
Enable Log	Whether to enable the log function.
Mode	Log mode: <ul style="list-style-type: none">● Local Logs are recorded in the local computer.● Remote Logs are sent to a remote syslog server with the specified IP address and UDP port.● Both Logs are saved in both the local computer and the remote syslog server.
Server IP Address	Server IP address, which needs to be configured when Mode is set to Remote .
Server UDP Port	Server UDP port, which needs to be configured when Mode is set to Remote .

3. Click **Apply**.
4. (Optional) To view the system logs, click **View System Log**.
5. (Optional) To view the firewall logs, click **View Firewall Log**.

– End of Steps –

Chapter 6

Status Query

Table of Contents

Viewing the Device Information	6-1
Viewing the Information on Wireless Clients	6-2
Viewing the Information on DHCP Clients.....	6-3
Viewing the IPv6 Status.....	6-3
Viewing System Logs	6-4
Viewing the Statistics Information	6-5
Viewing the IPv4 Route Information.....	6-6
Viewing the IPv6 Route Information.....	6-6

6.1 Viewing the Device Information

This procedure describes how to view the ZXHN H108N device information.

1. Select **Status > Device Info**. The **DEVICE INFO** page is displayed, see [Figure 6-1](#).

Figure 6-1 DEVICE INFO Page

Status

Device Info

Wireless Clients

DHCP Clients

IPv6 Status

Logs

Statistics

Route Info

IPv6 Route Info

Logout

DEVICE INFO

It indicates the current status of all the connections.

SYSTEM INFO

Modem Name :	H108N
Serial Number :	001FA4915A18
Time and Date :	2012-05-23 01:01:24
HardwareVersion :	ZXHN H108N R1A
SoftwareVersion :	ZXHN H108NV2.1.0d_ERU_BHS
Firmware Version :	2.1.0
Double memory bank :	Double image up to date
System Up Time :	00:01:36

INTERNET INFO

Internet Connection Status : PVC:8/36 ▾

Internet Connection Status:	Disconnected
Wan service type:	Internet_TR069
Default Gateway:	
Preferred DNS Server:	
Alternate DNS Server:	
Downstream Line Rate (Kbps):	0
Upstream Line Rate (Kbps):	0
Data Time Counter (Second):	

Enabled WAN Connections :

VPI/VCI	Service Name	Protocol	IGMP	QoS	IP Address
PVC:8/36	PVC:8/36	PPPOE	Disable	Disable	
	ppp03g	PPPOE	Disable	Disable	
PVC:8/35	PVC:8/35	IPoA	Enable	Disable	172.26.208.12

WIRELESS INFO

select wireless : WLAN_PasarelaBásica ▾

MAC Address:	f8:3fa4:91:5a:21
Status:	Enable
Network Name (SSID):	WLAN_PasarelaBásica
Visibility:	Visible
Security Mode:	WPA

LOCAL NETWORK INFO

MAC Address:	00:1fa4:91:5a:18
IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
DHCP Server:	Enable

6.2 Viewing the Information on Wireless Clients

This procedure describes how to view the information on wireless clients.

Steps

1. Select **Status > Wireless Clients**. The **WIRELESS CLIENTS** page is displayed, see [Figure 6-2](#).

Figure 6-2 WIRELESS CLIENTS Page

2. Click **Refresh** to refresh the information.

– End of Steps –

6.3 Viewing the Information on DHCP Clients

This procedure describes how to view the information on DHCP clients.

Steps

1. Select **Status > DHCP Clients**. The **DHCP CLIENTS** page is displayed, see [Figure 6-3](#).

Figure 6-3 DHCP CLIENTS Page

Hostname	MAC Address	IP Address	Expires In
ZTE-20050515BIY	00:21:97:df:6b:2a	192.168.1.33	43081

2. Click **Refresh** to refresh the information.

– End of Steps –

6.4 Viewing the IPv6 Status

This procedure describes how to view the IPv6 status.

Steps

1. Select **Status > IPv6 Status**. The **IPV6 STATUS** page is displayed, see [Figure 6-4](#).

Figure 6-4 IPV6 STATUS Page

IPV6 STATUS	
In this section you can see the information for the IPv6 Connection.	
IPV6 CONNECTION	
Wan Connection :	PVC:0/35
Connection Type :	DHCP
IPv6 Address/Prefix Len :	
Gateway :	
Pri Dns :	
Sec Dns :	
Prefix Info :	
Status :	Disconnected

2. Click **Refresh** to refresh the information.

– End of Steps –

6.5 Viewing System Logs

This procedure describes how to view system logs.

Steps

1. Select **Status > Logs**. The **LOGS** page is displayed, see [Figure 6-5](#).

Figure 6-5 LOGS Page

```

Manufacturer: ZTE
ProductClass: H108N
SerialNumber: 001FA4915A18
IP: 192.168.1.1
HWVer: ZXHN H108N R1A
SNVer: ZXHN H108NV2.1.0d_ERU_BHS
    
```

2. Click **Refresh** to refresh the information.

– End of Steps –

6.6 Viewing the Statistics Information

This procedure describes how to view the statistics information.

1. Select **Status > Statistics**. The **DEVICE INFO** page is displayed, see [Figure 6-6](#).

Figure 6-6 DEVICE INFO Page

Status

- Device Info
- Wireless Clients
- DHCP Clients
- IPv6 Status
- Logs
- Statistics**
- Route Info
- IPv6 Route Info
- Logout

DEVICE INFO

It indicates the current status of all the connections.

LOCAL NETWORK & WIRELESS

interface	Received				Transmitted			
	Bytes	Pkts	Errs	Rx drop	Bytes	Pkts	Errs	Tx drop
LAN4	864697	9674	0	0	2770980	5520	0	0
WLAN_PasarelaBásica	8523032	89626	0	0	9544910	24875	0	0

INTERNET

Service	VPI/VCI	Protocol	Received				Transmitted				
			Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops	
PVC:8/36	PVC:8/36	PPPOE									
PVC:8/35	PVC:8/35	IPoA	0	0	0	0	156	3	0	0	
PVC:0/35	PVC:0/35	BRIDGE									
PVC:0/35	PVC:0/35	DHCP									
PVC:0/35	PVC:0/35	PPPoA									
ppp03g		PPPOE									

ADSL

Mode:	0	
Type:	0	
DSL Driver Version:	07-27-12 ver 4924c727 2windingX	
Line Coding:	Enable	
Status:	ACTIVATING.	
Up Time:		
	Downstream	Upstream
SNR Margin (0.1dB):	0	0
Attenuation (0.1dB):	0	0
Output Power (dBm):	0.0	0.0
Attainable Rate (Kbps):	0	0
Rate (Kbps):	0	0
D (interleave depth):	0	0
Delay (msec):	0	0
Data Counter:	0 <input type="button" value="Clear"/>	0 <input type="button" value="Clear"/>
HEC Errors:	0	0
OCD Errors:	0	0
LCD Errors:	0	0
CRC Errors:	0	0
FEC Errors:	0	0
Total ES	0	0
Total Frames	0	510

6.7 Viewing the IPv4 Route Information

This procedure describes how to view the IPv4 route information.

1. Select **Status > Route Info**. The **ROUTE INFO** page is displayed, see [Figure 6-7](#).

Figure 6-7 ROUTE INFO Page

Status	<p>ROUTE INFO</p> <hr/> <p>Flags: U - up, I - reject, G - gateway, H - host, R - reinstate D - dynamic (redirect), M - modified (redirect).</p> <hr/> <p>DEVICE INFO -- ROUTE</p> <table border="1"> <thead> <tr> <th>Destination</th> <th>Gateway</th> <th>Subnet Mask</th> <th>Flags</th> <th>Metric</th> <th>Service</th> <th>Interface</th> </tr> </thead> <tbody> <tr> <td>10.167.64.80</td> <td>0.0.0.0</td> <td>255.255.255.248</td> <td>U</td> <td>0</td> <td>0</td> <td>br0</td> </tr> <tr> <td>192.168.1.0</td> <td>0.0.0.0</td> <td>255.255.255.0</td> <td>U</td> <td>0</td> <td>0</td> <td>br0</td> </tr> </tbody> </table>	Destination	Gateway	Subnet Mask	Flags	Metric	Service	Interface	10.167.64.80	0.0.0.0	255.255.255.248	U	0	0	br0	192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	br0
Destination		Gateway	Subnet Mask	Flags	Metric	Service	Interface															
10.167.64.80		0.0.0.0	255.255.255.248	U	0	0	br0															
192.168.1.0		0.0.0.0	255.255.255.0	U	0	0	br0															
Device Info																						
Wireless Clients																						
DHCP Clients																						
IPv6 Status																						
Logs																						
Statistics																						
Route Info																						
IPv6 Route Info																						
Logout																						

6.8 Viewing the IPv6 Route Information

This procedure describes how to view the IPv6 route information.

1. Select **Status > IPv6 Route Info**. The **IPv6 ROUTE INFO** page is displayed, see [Figure 6-8](#).

Figure 6-8 IPV6 ROUTE INFO Page

Status	<p>IPV6 ROUTE INFO</p> <hr/> <p>Flags: U - up, I - reject, G - gateway, H - host, R - reinstate D - dynamic (redirect), M - modified (redirect).</p> <hr/> <p>DEVICE INFO -- IPV6 ROUTE</p> <table border="1"> <thead> <tr> <th>Destination</th> <th>NextHop</th> <th>Flags</th> <th>Metric</th> <th>Ref</th> <th>Use</th> <th>Iface</th> </tr> </thead> <tbody> <tr> <td>fe80::/64</td> <td>::</td> <td>U</td> <td>256</td> <td>0</td> <td>0</td> <td>br0</td> </tr> <tr> <td>::1/128</td> <td>::</td> <td>U</td> <td>0</td> <td>1517</td> <td>1</td> <td>lo</td> </tr> <tr> <td>fe80::/128</td> <td>::</td> <td>U</td> <td>0</td> <td>0</td> <td>1</td> <td>lo</td> </tr> <tr> <td>fe80::1/128</td> <td>::</td> <td>U</td> <td>0</td> <td>0</td> <td>1</td> <td>lo</td> </tr> <tr> <td>ff02::1/128</td> <td>ff02::1</td> <td>UC</td> <td>0</td> <td>478</td> <td>0</td> <td>br0</td> </tr> <tr> <td>ff00::/8</td> <td>::</td> <td>U</td> <td>256</td> <td>0</td> <td>0</td> <td>br0</td> </tr> </tbody> </table>	Destination	NextHop	Flags	Metric	Ref	Use	Iface	fe80::/64	::	U	256	0	0	br0	::1/128	::	U	0	1517	1	lo	fe80::/128	::	U	0	0	1	lo	fe80::1/128	::	U	0	0	1	lo	ff02::1/128	ff02::1	UC	0	478	0	br0	ff00::/8	::	U	256	0	0	br0
Destination		NextHop	Flags	Metric	Ref	Use	Iface																																											
fe80::/64		::	U	256	0	0	br0																																											
::1/128		::	U	0	1517	1	lo																																											
fe80::/128		::	U	0	0	1	lo																																											
fe80::1/128		::	U	0	0	1	lo																																											
ff02::1/128		ff02::1	UC	0	478	0	br0																																											
ff00::/8		::	U	256	0	0	br0																																											
Device Info																																																		
Wireless Clients																																																		
DHCP Clients																																																		
IPv6 Status																																																		
Logs																																																		
Statistics																																																		
Route Info																																																		
IPv6 Route Info																																																		
Logout																																																		

Glossary

3G

- The 3rd Generation Mobile Communications

AC

- Alternating Current

ADSL

- Asymmetric Digital Subscriber Line

ALG

- Application Level Gateway

APN

- Access Point Name

ATM

- Asynchronous Transfer Mode

BIOS

- Basic Input/Output System

CA

- Certificate Authentication

CHAP

- Challenge Handshake Authentication Protocol

CRC

- Cyclic Redundancy Check

DC

- Direct Current

DDNS

- Dynamic Domain Name Server

DHCP

- Dynamic Host Configuration Protocol

DLNA

- Digital Living Network Alliance

DMZ

- Demilitarized Zone

DNS

- Domain Name Server

DSL

- Digital Subscriber Line

DSLAM

- Digital Subscriber Line Access Multiplexer

GUI

- Graphical User Interface

HTTP

- Hypertext Transfer Protocol

IEEE

- Institute of Electrical and Electronics Engineers

IGMP

- Internet Group Management Protocol

IP

- Internet Protocol

IPv4

- Internet Protocol version 4

IPv6

- Internet Protocol Version 6

ISP

- Internet Service Provider

LAN

- Local Area Network

LLC

- Logic Link Control

MLD

- Multicast Listener Discovery

NAT

- Network Address Translation

NMS

- Network Management System

NTP

- Network Time Protocol

PAP

- Password Authentication Protocol

PAT

- Port Address Translation

PIN

- Personal Identification Number

PPPoA

- Point to Point Protocol over ATM

PPPoE

- Point to Point Protocol over Ethernet

PVC

- Permanent Virtual Channel

QoS

- Quality of Service

RF

- Radio Frequency

RIP

- Routing Information Protocol

RIPng

- Routing Information Protocol next generation

SNMP

- Simple Network Management Protocol

SOAP

- Simple Object Access Protocol

TCP

- Transfer Control Protocol

UDP

- User Datagram Protocol

UPnP

- Universal Plug and Play

URL

- Uniform Resource Locator

USB

- Universal Serial Bus

VLAN

- Virtual Local Area Network

WAN

- Wide Area Network

WEP

- Wired Equivalent Privacy

WLAN

- Wireless Local Area Network

WPA

- Wi-Fi Protected Access

WPS

- Wireless Priority Service