

---

**LX220N**

**User Manual**

# Contents

1	Safety Precautions.....	1
2	Overview .....	2
2.1	Packing List.....	2
2.2	Application .....	2
2.3	Features.....	3
2.4	Standards Compatibility and Compliance .....	4
3	Hardware Description and Installation.....	5
3.1	LEDs and Interfaces.....	5
3.2	Hardware Installation.....	8
4	PC Network Configuration and Login.....	10
4.1	PC Network Configuration.....	10
4.2	Logging in to the DSL Router .....	11
5	Web-based Management .....	12
5.1	Setup .....	12
5.1.1	Wizard .....	13
5.1.2	Internet Setup.....	12
5.1.3	Wireless.....	16
5.1.4	Local Network.....	20
5.1.5	Local IPv6 Network.....	24
5.1.6	Time and Date .....	26
5.1.7	Logout .....	27
5.2	Advanced.....	28
5.2.1	Advanced Wireless .....	28
5.2.2	ALG.....	35
5.2.3	Port Forwarding.....	35
5.2.4	DMZ .....	37
5.2.5	SAMBA.....	37
5.2.6	Parental Control.....	39
5.2.7	Filtering Options.....	42
5.2.8	QoS Configuration .....	58
5.2.9	Anti-Attack Settings .....	50
5.2.10	DNS .....	64
5.2.11	Dynamic DNS.....	52
5.2.12	Network Tools.....	54

## LX220N User Manual

5.2.13	Routing.....	64
5.2.14	Schedules .....	83
5.2.15	NAT .....	70
5.2.16	DLNA .....	71
5.2.17	IP Tunnel.....	71
5.2.18	Logout .....	76
5.3	Management .....	77
5.3.1	Global IPv6.....	90
5.3.2	System Management.....	77
5.3.3	Firmware Update .....	79
5.3.4	Access Controls.....	80
5.3.5	Diagnosis.....	85
5.3.6	Log Configuration .....	87
5.4	Status.....	87
5.4.1	Device Info .....	88
5.4.2	Wireless Clients.....	89
5.4.3	DHCP Clients.....	89
5.4.4	IPv6 Status .....	90
5.4.5	Logs .....	90
5.4.6	Statistics .....	91
5.4.7	Route Info.....	93
5.5	Help .....	93
6	Trouble Shooting.....	94
7	FCC Statement .....	94

## 1 Safety Precautions

Take the following instructions to prevent the device from risks and damage caused by fire or electric power.

- Use the type of power marked in the volume label.
- Use the power adapter in the product package.
- Pay attention to the power load of the outlet or prolonged lines. An overburden power outlet or damaged lines or plugs may cause electric shock or fire accidents. Check the power cords regularly. If you find any damage, replace it at once.
- Proper space left for heat dissipation is necessary to avoid damage caused by overheating to the device. The long and thin holes on the device are designed for heat dissipation to ensure that the device works normally. Do not cover these heat dissipation holes.
- Do not put this device close to a heat source or under a high temperature occurs. Keep the device away from direct sunshine.
- Do not put this device close to an overdamp or watery place. Do not spill fluid on this device.
- Do not connect this device to a PC or electronic product unless instructed by our customer engineer or your broadband provider. Wrong connection may cause power or fire risk.
- Do not place this device on an unstable surface or support.

## 2 Overview

The LX220N DSL Router integrates wireless LAN and USB service into one unit. It is designed to provide a simple and cost-effective DSL Internet connection for a private Ethernet and 802.11g/802.11b/802.11n wireless network. The Router combines high-speed DSL Internet connection, IP routing for the LAN, and wireless connectivity in one package.

The Router is easy to install and use. The Router connects to an Ethernet LAN or computers via standard Ethernet ports. The DSL connection is made using ordinary telephone line with standard connectors. Multiple workstations can be networked and connected to the Internet by a single Wide Area Network (WAN) interface and single global IP address. The advanced security enhancements, packet filtering and port redirection, can help protect your network from potentially devastating intrusions by malicious agents from outside your network. Network and Router management is done through the web-based management interface accessed through the local Ethernet using any web browser. You may also enable remote management to enable configuration of the Router via the WAN interface.

### 2.1 Packing List

- 1 x LX220N
- 1 x external splitter
- 1 x power adapter
- 2 x telephone cables (RJ-11, more than 1.8m)
- 1 x Ethernet cable (RJ-45, more than 1.8m)
- 1 x USB cable (USB, more than 1m)
- 1 x user manual
- 1 x quality guarantee card
- 1 x certificate of quality

### 2.2 Application

- Home gateway
- Wireless LAN

- SOHOs
- Small enterprises
- Higher data rate broadband sharing
- Audio and video streaming and transfer
- PC file and application sharing
- Network and online gaming
- USB storage

## 2.3 Features

- User-friendly GUI for web configuration
- Compatible with all standard Internet applications
- Industry standard and interoperable xDSL interface
- Simple web-based status page displays a snapshot of system configuration, and links to the configuration pages
- Downloadable flash software updates
- Support for up to 8 permanent virtual circuits (PVC)
- Support for up to 8 PPPoE sessions
- Support RIP v1 & RIP v2
- WLAN with high-speed data transfer rates, compatible with IEEE 802.11b/g/n
- IP routing and bridging
- Asynchronous transfer mode (ATM) , PTM (Packet Transfer mode), and digital subscriber line (DSL) support
- Point-to-point protocol (PPP)
- Network/port address translation (NAT/PAT)
- Quality of service (QoS)
- Wireless LAN security: WPA, 802.1x, RADIUS client
- Universal plug-and-play(UPnP)
- Web filtering
- Management and control
  - Web-based management (WBM)
  - Command line interface (CLI)
  - TR-069 WAN management protocol
- Remote update
- System statistics and monitoring

- DSL router is targeted at the following platforms: DSL modems, wireless access points and bridge.
- Multicast listener discovery (MLD)
- Digital living network alliance (DLNA)
- Synergy advanced multipurpose bus arbiter (SAMBA)
- Internet group management protocol (IGMP)
- Application layer gateway (ALG)

## **2.4 Standards Compatibility and Compliance**

- Support application level gateway (ALG)
- ITU G.992.1 (G.dmt)
- ITU G.992.2 (G.lite)
- ITU G.994.1 (G.hs)
- ITU G.992.3 (ADSL2)
- ITU G.992.5 (ADSL2+)
- ITU G.993.1 (VDSL)
- ITU G.993.2 (VDSL2)
- ANSI T1.413 Issue 2
- IEEE 802.3
- IEEE 802.3u
- IEEE 802.11b
- IEEE 802.11g
- IEEE 802.11n

## 3 Hardware Description and Installation

### 3.1 LEDs and Interfaces

#### Front Panel





Figure 1 Front panel

The following table describes the indicators on the front panel.

Indicator	Color	Status	Description
Power	Green	On	The device is powered on.
		Off	The device is powered off.
	Red	On	Self-test fails, or failure occurs, or the device is starting.
DSL	Green	On	DSL link is established.
		Slow Blink	The DSL line is attempting to detect signals.
		Fast Blink	Signals have been detected, and the DSL line is attempting to establish link.
Internet	Green	On	Physical layer connection and IP connection is established in routing mode.
		Blink	IP connection is established, and messages are being transmitted.
		Off	IP connection or physical layer link is not established.
	Red	On	IP connection fails.
WAN	Green	On	WAN link is established.
		Blink	Data is being transmitted through a WAN interface.
		Off	WAN link is not established.
LAN 1/2	Green	On	Ethernet link is established.
		Blink	Data is being transmitted through a LAN interface.
		Off	Ethernet link is not established.
WLAN	Green	On	WLAN is enabled.
		Blink	Data is being transmitted by the wireless module.
		Off	WLAN is disabled.
WPS	Green	On	Negotiation is successful under Wi-Fi protected setup.
		Blink	Negotiation is in progress under Wi-Fi protected

Indicator	Color	Status	Description
			Setup.
		Off	Wi-Fi protected setup is disabled.
USB	Green	On	A USB flash disk is connected.
		Blink	Data is being transmitted.
		Off	No USB connection.

## Rear Panel

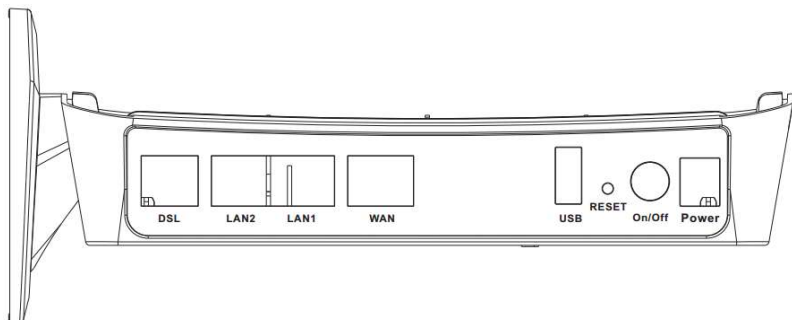


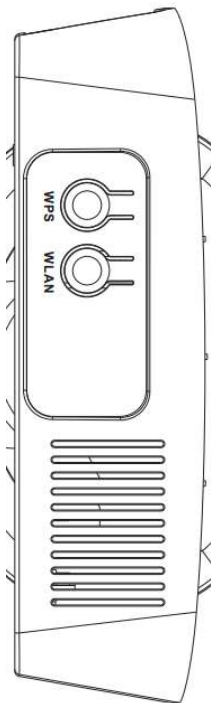
Figure 2 Rear panel

The following table describes the interface of the device.

Interface/Button	Description
DSL	RJ-11 interface connecting to a telephone set through a telephone cable
LAN1/2	Ethernet RJ-45 interfaces connecting to the Ethernet interfaces of computers or Ethernet devices
WAN	Ethernet RJ-45 interfaces connecting to the WAN interfaces.
USB	USB port, for connecting a 3G network card or other USB storage devices.
Reset	Reset to the factory defaults. To restore factory defaults, keep the device powered on and push a paper clip into the hole. Press down the button for more than 5 seconds and then release.
ON/OFF	Push to power on/off the device.

Interface/Button	Description
Power	Interface connecting to the power adapter. The power adapter output is: 12V DC, 1500mA

## Side Panel



Interface/Button	Description
WPS	This button is used for enabling WPS PBC mode. If WPS is enabled, press this button, and then the wireless router starts to accept the negotiation of PBC mode.
WLAN	WLAN switch, for enabling or disabling the WLAN function.

## 3.2 Hardware Installation

- Step 1** Connect the **DSL** port of the device and the **Modem** port of the splitter with a telephone cable. Connect the phone to the **Phone** port of the splitter through a telephone cable. Connect the incoming line to the **Line** port of the splitter.

The splitter has three ports:

- Line: Connect to a wall phone port (RJ-11 jack).
- Modem: Connect to the DSL port of the device.
- Phone: Connect to a telephone set.

**Step 2** Connect a **LAN** port of the device to the network card of the PC through an Ethernet cable (MDI/MDIX).

**Note:**

Use twisted-pair cables to connect the device to a Hub or switch.

**Step 3** Plug one end of the power adapter to the wall outlet and the other end to the **Power** port of the device.

**Connection 1:** Figure 3 displays the application diagram for the connection of the device, PC, splitter and telephone sets, when no telephone set is placed before the splitter.

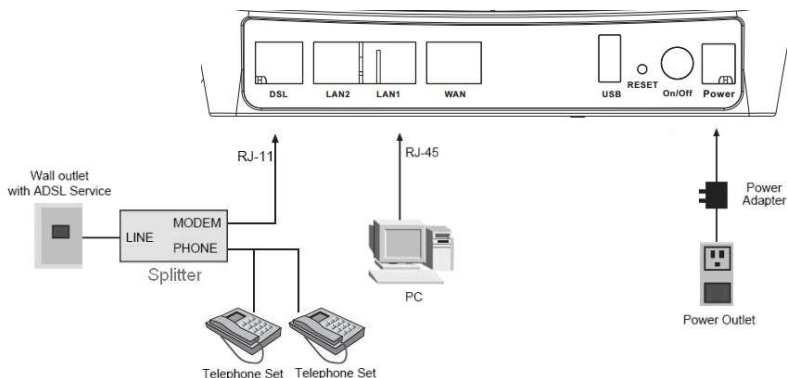


Figure 3 Connection diagram (without telephone sets before the splitter)

As illustrated in the following figure, the splitter is installed close to the device. Installing a telephone directly before the splitter may lead to failure of connection between the device and the central office, or failure of Internet access, or slow connection speed. If you really need to add a telephone set before the splitter, you must add a microfilter before a telephone set. Do not connect several telephones before the splitter or connect several telephones with the microfilter.

## 4 PC Network Configuration and Login

### 4.1 PC Network Configuration

Each network interface on the PC should either be configured with a statically defined IP address and DNS address, or be instructed to automatically obtain an IP address using the network DHCP server. DSL router provides a DHCP server on its LAN and it is recommended to configure your LAN to automatically obtain its IP address and DNS server IP address.

The configuration principle is identical but should be carried out differently on each operating system.

The following displays the **TCP/IP Properties** dialog box on Windows XP.

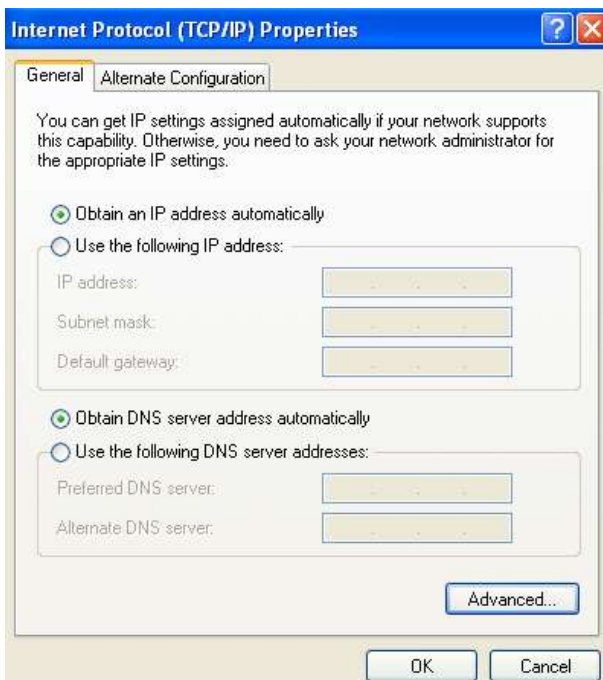


Figure 4 PC Network Configuration

TCP/IP configuration steps for Windows XP are as follows:

**Step 1** Choose Start > Control Panel > Network Connections.

Right-click the Ethernet connection icon and choose **Properties**.

On the **General** tab, select the **Internet Protocol (TCP/IP)** component and click **Properties**. The Internet Protocol (TCP/IP) Properties window appears.

Select the **Obtain an IP address automatically** radio button.

Select the **Obtain DNS server address automatically** radio button.

Click **OK** to save the settings.

## 4.2 Logging in to the DSL Router

To log in to the DSL router, do as follows.

**Step 1** Open a Web browser on your computer.

**Step 2** Enter **http://192.168.1.1** (default IP address of the DSL router) in the address bar. The login page appears.

**Step 3** Enter the user name and the password. The default username and password of the super user are **admin** and **c1@r0**. The username and password of the common user are **Usuario** and **c1@r0**. It is recommended to change these default values after logging in to the DSL router for the first time.

**Step 4** Click **Login** to log in to the Web page.



<b>Language</b>	English ▾
<b>UserName</b>	admin ▾
<b>Password</b>	<input type="text"/>
	<input type="button" value="Login"/>

Copyright © LANIX Systems, Inc.

Figure 5 Logging in to the DSL Router

After logging in to the DSL router as a super user, you can query, configure, and modify all the settings, and diagnose the system.

## 5 Web-based Management

This chapter describes how to use Web-based management of the DSL router, which allows you to configure and control all of DSL router features and system parameters in a user-friendly GUI.

### 5.1 Setup

In the main interface, click **Setup** tab to enter the **Setup** menu as shown in the following figure. The submenus are **Wizard**, **Internet Setup**, **Wireless**, **Local Network**, **Local IPv6 Network**, **Time and Date** and **Logout**.

#### 5.1.1 Internet Setup

Choose **Setup > Internet Setup**. The page shown in the following figure appears. In this page, you can configure the WAN interface of the device.

**INTERNET SETUP**

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

Default GateWay Mode  Auto  Manual

Default Wan Mode  DSL  ETHERNET

**DSL CONFIG**

	VPI/VCI	VLAN ID	ENCAP	Service Name	Protocol	State	Status	V4 Default Gateway	V6 Default Gateway	Action
<input type="radio"/>	0/32	0	LLC	D_PPPoE_0_1	PPPoE	1		<input type="radio"/>	-	-
<input type="radio"/>	0/45	0	LLC	D_PPPoE_0_2	PPPoE	1		<input type="radio"/>	-	-

**ETHERNET CONFIG**

VLAN ID	Service Name	Protocol	State	Status	V4 Default Gateway	V6 Default Gateway	Action

Click **Add** in “INTERNET SETUP”. The page shown in the following figure appears.



## INTERNET SETUP

This screen allows you to configure an WAN connection.

## DSL MODE CONFIGURATION

DSL Mode : ATM ▾

## ATM PVC CONFIGURATION

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

## CONNECTION TYPE

Protocol : Bridging ▾  
 Bridge Accel. :   
 Encapsulation Mode : LLC ▾  
 802.1Q VLAN ID : 0 (0 = disable, 1 - 4094)  
 Enable Service :   
 Service Name : D\_Bridging\_0\_3

Apply Cancel

The following table describes the parameters in this page.

Field	Description
DSL Mode	You can select <b>ATM</b> or <b>PTM</b> .
PVC Settings	<b>VPI</b> : The virtual path between two points in an ATM network, and its valid value is from <b>0</b> to <b>255</b> . <b>VCI</b> : The virtual channel between two points in an ATM network, ranging from <b>32</b> to <b>65535</b> (0 to 31 is reserved for local management of ATM traffic).
Service	You can select from the drop-down list.

Field	Description
Category	<div style="border: 1px solid black; padding: 5px;">           UBR With PCR <span style="float: right;">▼</span>            UBR Without PCR  <b>UBR With PCR</b>            CBR            Non Realtime VBR            Realtime VBR         </div>
Protocol	<p>You can select from the drop-down list.</p> <div style="border: 1px solid black; padding: 5px;">           Bridging <span style="float: right;">▼</span>            PPP over ATM (PPPoA)            PPP over Ethernet (PPPoE)            MAC Encapsulation Routing (MER)            IP over ATM (IPoA)  <b>Bridging</b> </div>
Encapsulation Mode	Select the method of encapsulation provided by your ISP. You can select <b>LLC</b> or <b>VCMUX</b> .

Click **Apply**, the page shown in the following figure appears.

## DSL CONFIG

	VPI/VCI	VLAN ID	ENCAP	Service Name	Protocol	State	Status	V4 Default Gateway	V6 Default Gateway	Action
<input type="radio"/>	0/32	0	LLC	D_PPPoE_0_1	PPPoE	1		<input type="radio"/>	-	-
<input type="radio"/>	0/45	0	LLC	D_PPPoE_0_2	PPPoE	1		<input type="radio"/>	-	-

## ETHERNET CONFIG

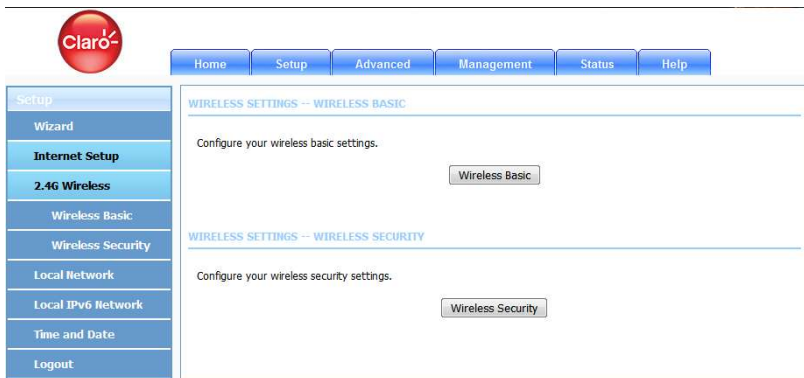
VLAN ID	Service Name	Protocol	State	Status	V4 Default Gateway	V6 Default Gateway	Action
---------	--------------	----------	-------	--------	--------------------	--------------------	--------

To manage the existing WAN connections, select a connection from the list, and then click **Edit** or **Delete**.

## 5.1.2 Wireless

This section describes the wireless LAN and basic configuration. A wireless LAN can be as simple as two computers with wireless LAN cards communicating in a peer-to-peer network or as complex as a number of computers with wireless LAN cards communicating through access points which bridge network traffic to wired LAN.

Choose **Setup** > **Wireless**. The **Wireless** page shown in the following figure appears.



### 5.1.2.1 Wireless Basic

In the **Wireless** page, click **Wireless Basic**. The page shown in the following figure appears. In this page, you can configure the parameters of wireless LAN clients that may connect to the device.

## WIRELESS BASIC CONFIGURATION

Enable Wireless :

AP Isolate :

SSID :

Visibility Status :  Visible  Invisible

Continent/Country :

802.11 Mode :

Band Width :

Wireless Channel :

The following table describes the parameters in this page.

Field	Description
Enable Wireless	Select this to turn Wi-Fi on.
AP Isolate	Select this to turn AP isolation on.
Wireless Network Name (SSID)	The Wireless Network Name is a unique name that identifies a network. All devices on a network must share the same wireless network name in order to communicate on the network. If you decide to change the wireless network name from the default setting, enter your new wireless network name in this field.
Visibility Status	You can select <b>Visible</b> or <b>Invisible</b> .
Country	Select the country from the drop-down list.
802.11 Mode	Select the appropriate 802.11 mode based on the wireless clients in your network. The drop-down menu options are <b>802.11b only</b> , <b>802.11g only</b> , <b>802.11n only</b> , <b>Mixed 802.11b/g</b> , <b>Mixed 802.11n/g</b> and <b>Mixed 802.11b/g/n</b> .
Band Width	Select the appropriate band as <b>20M</b> , <b>40M Plus</b> , or <b>40M Minus</b> from the pull-down menu.
Wireless Channel	Select the wireless channel from the pull-down menu. It is different for different country.
Transmission	Select the transmission rate for the network. The rate

Field	Description
Rate	of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select <b>Auto</b> to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client. The default is <b>Auto</b> .

Click **Apply** to save the settings.

### 5.1.2.2 Wireless Security

In the **Wireless** page, click **Wireless Security**. The page shown in the following figure appears. Wireless security is vital to your network to protect the wireless communication among wireless stations, access points and wired network.

#### Note:

Enable Wireless before configuring the wireless security settings in this page.  
Refer to 5.1.2.1 Wireless Basic.

When the Security Mode is set as **WEP**, the following figure appears.

WIRELESS SECURITY MODE

---

Wireless Security Mode : WEP

---

WEP

---

WEP Key Length : 64 bit ( length applies to all keys )

Default Tx Key : 1

WEP Key Format : HEX (10 characters)

WEP Key1 : 1111111111

WEP Key2 :

WEP Key3 :

WEP Key4 :

Authentication : Open

Apply Cancel

The following table describes the parameters of this page.

Field	Description
WEP Key Length	Choose the WEP key length. You can choose <b>64-bit</b> or <b>128-bit</b> .
Default Tx Key	Choose the index of WEP Key. You can choose <b>Key 1, 2, 3</b> or <b>4</b> .
WEP Key Format	<ul style="list-style-type: none"> <li>When <b>64-bit</b> key length is selected, you can choose <b>ASCII (5 characters)</b> or <b>HEX (10 characters)</b>.</li> <li>When <b>128-bit</b> key length is selected, you can choose <b>ASCII (13 characters)</b> or <b>HEX (26 characters)</b>.</li> </ul>
WEP Key 1/2/3/4	The Encryption keys are used to encrypt the data. Both the modem and wireless stations must use the same encryption key for data transmission. The default key 1 is <b>1111111111</b> .
Authentication	Choose an authentication mode.

Click **Apply** to save the settings.

When the Security Mode is set as **WPA2 only** or **WPA/WPA2 Mixed**, the following figure appears.

#### WIRELESS SECURITY MODE

Wireless Security Mode : WPA2 only

#### WPA2 ONLY

WPA Mode : Personal

Encryption Mode : AES

Group Key Update Interval : 100 (60 - 65535)

#### PRE-SHARED KEY

Pre-Shared Key : ifajlejf (ASCII < 64, HEX = 64)

Apply Cancel

The following table describes the parameters in this page.

Field	Description
Wireless Security Mode	<p>Configure the wireless encryption mode. You can choose <b>None</b>, <b>WEP</b>, <b>WPA2 Only</b> or <b>WPA /WPA2 Mixed</b>.</p> <ul style="list-style-type: none"> <li>● Wired equivalent privacy (WEP) encrypts data frames before transmitting over the wireless network.</li> <li>● WPA2 is a subset of the IEEE802.11i security specification draft.</li> <li>● WPA/WPA2 Mixed is the collection of WPA and WPA2 encryption modes. The wireless client establishes the connection between the modem through WPA or WPA2.</li> </ul> <p>Key differences between WPA and WEP are user authentication and improved data encryption.</p>
WPA Mode	<ul style="list-style-type: none"> <li>● Select <b>Personal</b>, and then enter the pre-shared key in the <b>Pre-Shared Key</b> field.</li> <li>● Select <b>Enterprise</b>, and then enter the port, IP address, and password of the Radius server. You need to enter the password provided by the Radius server when the wireless client connects the modem.</li> </ul> <p>If the encryption is set to <b>WEP</b>, the modem uses 802.1 X authentication, which is Radius authentication.</p>
Encryption Mode	<p>When <b>WPA /WPA2 Mixed</b> is selected, you can select WPA encryption as <b>AES</b>, <b>TKIP</b> or <b>Both</b>.</p>
Group Key Update Interval	<p>When WPA encryption is applied, messages sent are encrypted with a password. For higher security, WPA password is updated periodically. This value is the update interval of the WPA password.</p>

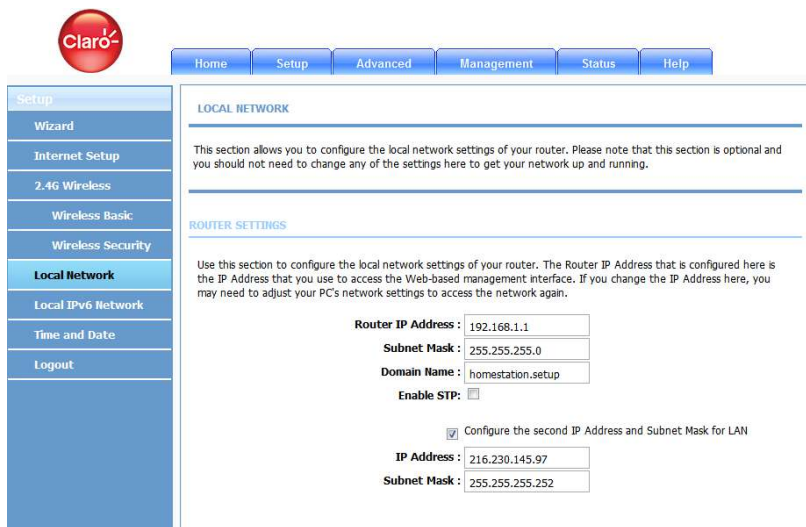
### 5.1.3 Local Network

You can configure the LAN IP address according to the actual application. The preset IP address is 192.168.1.1. You can use the default settings and DHCP

service to manage the IP settings for the private network. The IP address of the device is the base address used for DHCP. To use the device for DHCP on your LAN, the IP address pool used for DHCP must be compatible with the IP address of the device. The IP address available in the DHCP IP address pool changes automatically if you change the IP address of the device.

You can also enable the secondary LAN IP address. The two LAN IP addresses must be in different networks.

Choose **Setup > Local Network**. The **Local Network** page shown in the following figure appears.



The screenshot shows the Claro LX220N web interface. At the top left is the Claro logo. A navigation bar contains buttons for Home, Setup, Advanced, Management, Status, and Help. On the left is a vertical menu with options: Setup, Wizard, Internet Setup, 2.4G Wireless, Wireless Basic, Wireless Security, **Local Network** (highlighted), Local IPv6 Network, Time and Date, and Logout. The main content area is titled 'LOCAL NETWORK'. It contains a paragraph: 'This section allows you to configure the local network settings of your router. Please note that this section is optional and you should not need to change any of the settings here to get your network up and running.' Below this is a section titled 'ROUTER SETTINGS'. It includes a paragraph: 'Use this section to configure the local network settings of your router. The Router IP Address that is configured here is the IP Address that you use to access the Web-based management interface. If you change the IP Address here, you may need to adjust your PC's network settings to access the network again.' The settings are as follows:

Router IP Address :	192.168.1.1
Subnet Mask :	255.255.255.0
Domain Name :	homestation_setup
Enable STP:	<input type="checkbox"/>
<input checked="" type="checkbox"/> Configure the second IP Address and Subnet Mask for LAN	
IP Address :	216.230.145.97
Subnet Mask :	255.255.255.252

By default, **Enable DHCP Server** is selected for the Ethernet LAN interface of the device. DHCP service supplies IP settings to workstations configured to automatically obtain IP settings from a PC connected to the device through the Ethernet port. When the device is used for DHCP, it becomes the default gateway for DHCP clients connected to it. If you change the IP address of the device, you must also change the range of IP addresses in the pool used for DHCP on the LAN. The IP address pool can contain up to 253 IP addresses.



Configure the second IP Address and Subnet Mask for LAN

**IP Address :**   
**Subnet Mask :**

This page is used to configure the DHCP Server and DHCP Relay Settings. The **HCP Lease Time** is at least **600** seconds and without upper limit; **-1** means unrestricted lease time.

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

**Enable DHCP Relay :**   
**Relay IP Address :**

Use this section to 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 Lease Time :**  (seconds [time not allowed less than

600s])

Click **Apply** to save the settings.

The **DHCP Client Class List** section is shown as below.

## DHCP CLIENT CLASS LIST

Client Class	Min Address	Max Address	DNS Address
--------------	-------------	-------------	-------------

Click **Add**, the page shown in the following figure appears.

### ADD DHCP CLIENT CLASS(OPTIONAL)

**Client Class Name :**   
**Min IP Address :**   
**Max IP Address :**   
**DNS Address :**

The **DHCP Cond Option** section is shown as below. Here you can specify the reply message (option **240~245**) the modem sends to the client. After **DHCP CLIENT CLASS** is configured, you can configure **DHCP COND OPTION**.

## DHCP CONDITIONAL OPTION

Status	Client Class Name	Option Code	Option Value
--------	-------------------	-------------	--------------

Click **Add** to add DHCP option as shown in the following figure.

## ADD DHCP OPTION(OPTIONAL)

Conditional Option Enable :

Conditional Option Client Class :

Conditional Option Tag :

Conditional Option Value :

Only when this function is enabled, the modem returns the content below to the client.

The **Cond Option Client Class** is the client class name of DHCP Cond Option. The **Cond Option Tag** is a part of the value in the message sent by the modem to the client. It is between **240** and **245**.

The **Cond Option Value** is a value in the message sent by the modem to the client. This value can be specified at random.

After setting, click **Apply** to save the settings.

In the **Local Network** page, you can assign IP addresses on the LAN to specific individual computers based on their MAC addresses.

## DHCP RESERVATIONS LIST

Status	Computer Name	MAC Address	IP Address
--------	---------------	-------------	------------

Click **Add** to add static DHCP (optional). The page shown in the following figure appears.

## ADD DHCP RESERVATION (OPTIONAL)

Enable :

Computer Name :

IP Address :

MAC Address :

Apply Cancel

Select **Enable** to reserve the IP address for the designated PC with the configured MAC address. The **Computer Name** helps you to recognize the PC with the MAC address, for example, Father's Laptop. Click **Apply** to save the settings.

After the DHCP reservation is saved, the DHCP reservations list displays the configuration.

The **NUMBER OF DYNAMIC DHCP CLIENTS** page shows the current DHCP clients (PC or Laptop) connected to the device and the detailed information of the connected computer(s).

## NUMBER OF DYNAMIC DHCP CLIENTS : 0

Computer Name	MAC Address	IP Address	Expire Time
---------------	-------------	------------	-------------

## 5.1.4 Local IPv6 Network

You can configure the LAN IPv6 address according to the actual application. The preset IPv6 address is fe80::1. You can use the default settings and DHCPv6 service to manage the IPv6 settings for the private network. The IPv6 address of the device is the base address used for DHCPv6. To use the device for DHCPv6 on your LAN, the IPv6 address pool used for DHCPv6 must be compatible with the IPv6 address of the device. The IPv6 address available in the DHCP IPv6 address pool changes automatically if you change the IPv6 address of the device.

Choose **Setup > Local IPv6 Network**. The page shown in the following figure appears. In this page, you can configure a static LAN IPv6 address, enable or disable DHCPv6 server and RADVD, and configure site prefix.

Setup	<b>IPv6 LAN SETTINGS</b>
Wizard	Note: Stateful DHCPv6 is supported after the IPv6 address 16-bit. For example: Interface ID range from 1 to ffff, IPv6 address range from 2111:123:123:123:1 to 2111:123:123:123:ffff.
Internet Setup	<b>STATIC LAN IPV6 ADDRESS CONFIGURATION</b>
2.4G Wireless	IPv6 Address : fe80::21e:3ff:febe:3f2
Wireless Basic	<b>DHCPV6 CONFIGURATION</b>
Wireless Security	Enable DHCPv6 Server : <input checked="" type="checkbox"/>
Local Network	LAN Address Config Mode : <input checked="" type="radio"/> Stateless <input type="radio"/> Stateful
<b>Local IPv6 Network</b>	Start Interface ID : 1
Time and Date	End Interface ID : ff
Logout	DHCPv6 Lease Time : 14400
	Use the following DNS server addresses.
	IPv6 DNS Mode : <input checked="" type="radio"/>
	Static DNS Servers : <input type="radio"/>
	Static IPv6 DNS Servers : 2111:3c:123:0:c:135:9a
	<b>UNIQUE LOCAL ADDRESSES CONFIGURATION</b>
	Enable RADVD : <input checked="" type="checkbox"/>
	RADVD DNSLL : <input type="text"/>
	ULA mode : <input type="radio"/> From WAN <input type="radio"/> Statically Configure <input checked="" type="radio"/> BOTH
	Address : fd80::1/64 (e.g: fd80::1/64)
	Site Prefix : fd80::/64 (e.g: fd80::/64)
	Preferred Life Time : 14400
	Valid Life Time : 86400
	Apply Cancel

The following table describes the parameters in this page.

Field	Description
IPv6 Interface Address	The IPv6 address of link local gateway on the LAN side.
Enable DHCPv6 Server	Choose to enable DHCPv6 server.
LAN address config mode	Choose an IPv6 address mode. <b>Stateless</b> refers to stateless address auto-configuration (SLAAC) mode, and <b>Stateful</b> refers to dynamic host configuration protocol (DHCP) mode.
Start/ End	IPv6 address pool range.

Field	Description
Interface ID	
DHCPv6 Lease Time	IPv6 lease time.
Get DNS Servers from WAN	You can choose to get the IPv6 DNS server address from the WAN side.
Static DNS Servers	You can manually set the IPv6 DNS server address.
Static IPv6 DNS Servers	Input an IPv6 DNS server address.
Enable RADVD	The router advertisement daemon (RADVD) is run by Linux or BSD systems acting as IPv6 routers. It sends router advertisement messages, specified by RFC2461, to a local Ethernet LAN periodically and when requested by a node sending a router solicitation message. These messages are required for IPv6 stateless auto-configuration.
Auto get prefix from WAN	You can choose to get an IPv6 prefix from the WAN automatically.
WAN interface	You can choose to get an IPv6 prefix from the selected WAN connection.
Static	You can choose to specify an IPv6 prefix.
Site Prefix	Input an IPv6 prefix.

After finishing setting, click the **Apply** button to apply the settings.

## 5.1.5 Time and Date

Choose **Setup > Time and Date**. The page shown in the following figure appears.

The screenshot shows the configuration interface for the LX220N device. On the left is a navigation menu with the following items: Setup, Wizard, Internet Setup, 2.4G Wireless, Wireless Basic, **Wireless Security**, Local Network, Local IPv6 Network, **Time and Date**, and Logout. The main content area is titled "TIME AND DATE" and contains the following sections:

- TIME AND DATE**: A header section with a sub-header "TIME AND DATE". Below it is a paragraph: "The Time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone that you are in and set the NTP (Network Time Protocol) Server. Daylight Saving can also be configured to automatically adjust the time when needed."
- TIME SETTING**: A section containing a checked checkbox labeled "Automatically synchronize with Internet time servers". Below this are three input fields:
  - 1st NTP time server: gt.pool.ntp.org
  - 2nd NTP time server: www.pool.ntp.org
  - 3rd NTP time server: (empty)
- TIME CONFIGURATION**: A section containing:
  - Current Local Time: 2016-12-09 04:27
  - Time Zone: (GMT+01:00) Amsterdam, Berlin, Rome, Stockholm, Vienna, Paris (dropdown menu)
  - Enable Daylight Saving: checked checkbox
  - Daylight Saving Start: 03 Mon 11 Day 02 Hour 00 Min 00 Sec
  - Daylight Saving End: 11 Mon 04 Day 02 Hour 00 Min 00 Sec
  - Buttons: Apply, Cancel

In the **Time and Date** page, you can configure, update, and maintain the correct time on the internal system clock. You can set the time zone that you are in and the network time protocol (NTP) server. You can also configure daylight saving to automatically adjust the time when needed.

Select **Automatically synchronize with Internet time servers**.

Select the specific time server and the time zone from the corresponding drop-down lists.

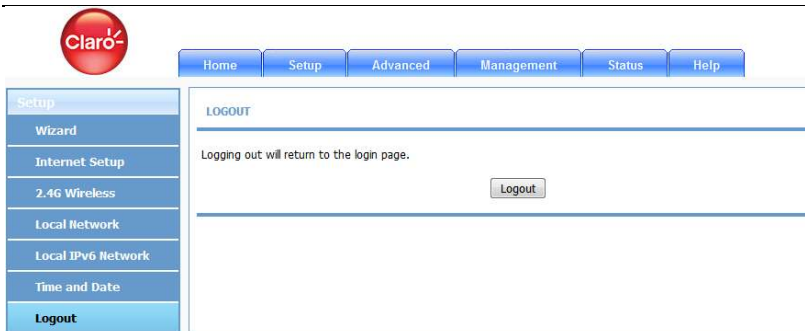
Select **Automatically adjust clock for daylight saving changes** if necessary.

Set the daylight as you want.

Click **Apply** to save the settings.

## 5.1.6 Logout

Choose **Setup > Logout**. The page shown in the following figure appears. In this page, you can log out of the configuration page.



## 5.2 Advanced

This section includes advanced features for network management, security and administrative tools to manage the device. You can view status and other information used to examine performance and troubleshoot.

In the main interface, click **Advanced** tab to enter the **Advanced** menu as shown in the following figure. The submenus are **2.4G Advanced Wireless**, **ALG**, **Port Forwarding**, **DMZ**, **SAMBA**, **Parental Control**, **Filtering Options**, **QoS Configuration**, **Anti-Attack Settings**, **DNS**, **Dynamic DNS**, **Network Tools**, **Routing**, **Schedules**, **NAT**, **DLNA**, **IP Tunnel** and **Logout**.

### 5.2.1 Advanced Wireless

It is suggested not to change the defaults, as incorrect settings may reduce the performance of your wireless radio. The default settings provide the best wireless radio performance in most environments.

Choose **Advanced** > **Advanced Wireless**. The page shown in the following figure appears.



Advanced	ADVANCED WIRELESS -- ADVANCED SETTINGS
<b>2.4G Advanced Wireless</b>	
Advanced Settings	Allows you to configure advanced features of the wireless LAN interface. <a href="#">Advanced Settings</a>
MAC Filtering	ADVANCED WIRELESS -- MAC FILTERING
Security Settings	Allows you to configure wireless firewall by denying or allowing designated MAC addresses. <a href="#">MAC Filtering</a>
WPS Settings	ADVANCED WIRELESS -- SECURITY SETTINGS
WDS Settings	Allows you to configure security features of the wireless LAN interface. <a href="#">Security Settings</a>
ALG	ADVANCED WIRELESS -- WPS SETTING
Port Forwarding	Allows you to configure wireless WPS. <a href="#">WPS Setting</a>
Porttrigger	ADVANCED WIRELESS -- WDS SETTING
DMZ	Allows you to configure wireless WDS. <a href="#">WDS Setting</a>
SAMBA	
Parental Control	
Filtering Options	
QoS	
Anti-Attack Settings	
Dynamic DNS	
Network Tools	
Routing	
NAT	
DLNA	
IPsec	
IP Tunnel	
VPII	

### 5.2.1.1 Advanced Settings

Select **Advanced Settings**. The page shown in the following figure appears.





Home	Setup	Advanced	Management	Status	Help
------	-------	----------	------------	--------	------

Advanced

**2.4G Advanced Wireless**

**Advanced Settings**

MAC Filtering

Security Settings

WPS Settings

WDS Settings

ALG

Port Forwarding

Porttrigger

DMZ

SAMBA

Parental Control

Filtering Options

QoS

Anti-Attack Settings

Dynamic DNS

Network Tools

Routing

NAT

DLNA

IPsec

IP Tunnel

VPI

**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.

---

**WIRELESS ENABLE**

Enable Wireless :

---

**ADVANCED WIRELESS SETTINGS**

Transmit Power : 100% ▾

Beacon Period : 100 (20 ~ 1023)

RTS Threshold : 2346 (1 ~ 2347)

Fragmentation Threshold : 2346 (256 ~ 2346)

DTIM Interval : 10 (1 ~ 255)

Preamble Type : long ▾

---

**SSID**

SSID : CLARO\_be3f2f

Visibility Status :  Visible  Invisible

User Isolation : Off ▾

Disable WMM Advertise : On ▾

Max Clients : 16 (1 ~ 32)

---

**GUEST/VIRTUAL ACCESS POINT-1**

Enable :

Guest SSID : CLARO\_AP2

Visibility Status :  Visible  Invisible

**Wireless Network Name (SSID):** The Wireless Network Name is a unique name that identifies a network. All devices on a network must share the same wireless network name in order to communicate on the network. If you decide to change the wireless network name from the default setting, enter your new wireless network name in this field.

These settings are only for more technically advanced users who have sufficient knowledge about wireless LAN. Do not change these settings unless you know the effect of changes on the device.

Click **Apply** to save the settings.

### 5.2.1.2 MAC Filtering

Select **MAC Filtering**. The page shown in the following figure appears.

#### ACCESS CONTROL – MAC ADDRESSES

Wireless SSID : CLARO\_be3f2f ▾  
 Access Control Mode : Disable ▾

#### WLAN FILTER LIST

Mac	Comment	Operation
<input type="button" value="Add"/>		

MAC address access control permits access to this route from hosts with MAC addresses contained in the WLAN Filter List.

Choose a wireless SSID, select an access control mode, and then click **Add** to add a MAC Address as shown in the following figure. Click **Apply** to finish. After adding a filter, you can edit or delete it.

#### ACCESS CONTROL – MAC ADDRESSES

Wireless SSID : CLARO\_be3f2f ▾  
 Access Control Mode : Disable ▾

#### WLAN FILTER LIST

Mac	Comment	Operation
<input type="button" value="Add"/>		

#### INCOMING MAC FILTER

MAC :  (xx:xx:xx:xx:xx:xx)  
 Comment :

### 5.2.1.3 Security Settings

Select **Security Settings**. The VAP Configuration page appears.

## WIRELESS SECURITY

## WIRELESS SSID

Select SSID : CLARO\_be3f2f ▾

## WIRELESS SECURITY

Security Mode : WPA2 only ▾

## WPA2 ONLY

WPA Mode : Personal ▾

Encryption Mode : AES ▾

Group Key Update Interval : 100 (60 - 65535)

## PRE-SHARED KEY

Pre-Shared Key : lfajlejf (ASCII &lt; 64, HEX = 64)

Submit

Refresh

Select the SSID that you want to configure from the drop-down list. Select the encryption type from the **Work Mode** drop-down list. You can select **None**, **WEP**, **WPA2 Only** or **WPA/WPA2 Mixed**. The default mode is **None**. If you select **WEP**, the page shown in the following figure appears.

## WIRELESS SECURITY

Security Mode : WEP ▾

## ENABLED WEP

Encryption Strength 64 bit ( length applies to all keys ) ▾

Choose WEP Key 1 ▾

Key Type HEX (10 characters) ▾

WEP Key1 : 1111111111

WEP Key2 :

WEP Key3 :

WEP Key4 :

Authentication Open ▾

Submit

Refresh

If you select **WPA2 Only** or **WPA/WPA2 Mixed**, the page shown in the following figure appears.

### WIRELESS SECURITY

---

Security Mode : WPA2 only ▾

### WPA2 ONLY

---

WPA Mode : Personal ▾

Encryption Mode : AES ▾

Group Key Update Interval : 100 (60 - 65535)

### PRE-SHARED KEY

---

Pre-Shared Key : lfajlejf (ASCII < 64, HEX = 64)

Submit

Refresh

Click **Submit** to save the settings. For detailed configuration, you may refer to 5.1.2.2 Wireless Security.

### 5.2.1.4 WPS Settings

Select **WPS Settings**. This page is used to config WPS settings.

#### Note:

To configure WPS, the WLAN security mode must be WPA-PSK or WPA2-PSK mode.

## WPS

The WPS condition must be WPA-PSK or WPA2-PSK security mode, and the SSID should be broadcasted.

**Wireless SSID :** CLARO\_be3f2f

**WPA Mode :** WPA2-PSK

**Pre-Shared Key :** \*\*\*\*\*

## WI-FI PROTECTED SETUP CONFIG

Enabled WPS :

Push Button :

Select Mode :  ▼

AP PIN : 12345670

Trigger AP PIN:

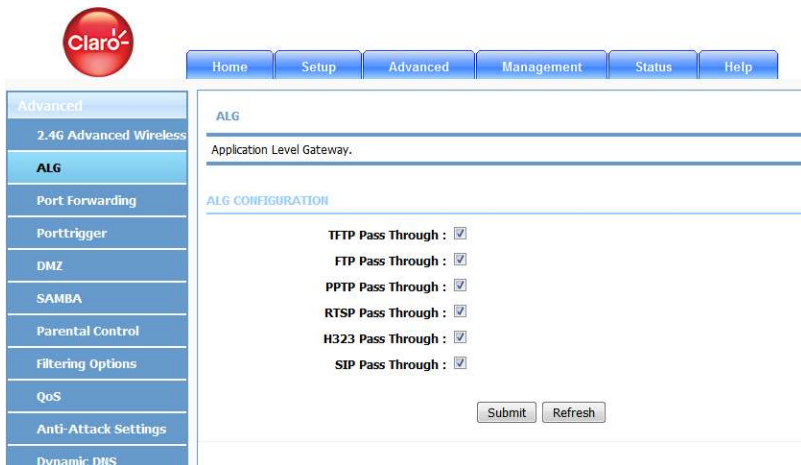
WPS Session Status :

The following table describes the parameters of this page.

Field	Description
Wireless SSID	Select one SSID of the CPE.
Enabled WPS	Choose to enable WPS function to set the following parameters.
PBC	In this way, the router generates PIN. Click this button, the router will generate a PIN, and meanwhile press the WPS button on the wireless client. The wireless client automatically establishes connection with the router under encryption mode without inputting the key.
PIN	In this way, the wireless client generates PIN. Enter PIN of the wireless client in the <b>Input Station PIN</b> field, and then click <b>PIN</b> to establish the connection.
WPS Session Status	Display the session status.

## 5.2.2 ALG


Choose **Advanced** > **ALG**. The page shown in the following figure appears. In this page, you can enable passthrough of TFTP, FTP, PPTP, RTSP, L2TP, H323, SIP and IPSEC.



## 5.2.3 Port Forwarding

This function is used to open ports in your device and redirect data through those ports to a single PC on your network (WAN-to-LAN traffic). It allows remote users to access services on your LAN, such as FTP for file transfers or SMTP and POP3 for e-mail. The device accepts remote requests for these services at your global IP address. It uses the specified TCP or UDP protocol and port number, and redirects these requests to the server on your LAN with the LAN IP address you specify. Note that the specified private IP address must be within the available range of the subnet where the device is in.

Choose **Advanced** > **Port Forwarding**. The page shown in the following figure appears.



Home Setup **Advanced** Management Status Help

Advanced

- 2.4G Advanced Wireless
- ALG
- Port Forwarding**
- Porttrigger
- DMZ
- SAMBA
- Parental Control
- Filtering Options
- QoS
- Anti-Attack Settings

### 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 16 entries can be configured for each WAN connection.

Select the service name, and enter the server IP address and click "Apply" to forward IP packets for this service to the specified server.

#### PORT FORWARDING SETUP

Server Name	Wan Connection	External Port Start/End	Protocol	Internal Port	Server IP Address	Schedule Rule	Remote IP
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>							

Click **Add** to add a virtual server.

#### PORT FORWARDING SETUP

WAN Connection(s): D\_PPPoE\_0\_1 ▾

Server Name:

Schedule: always ▾

Server IP Address(Host Name): 192.168.1.

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

enter a name in the **Server Name** field.

Enter an IP address in the **Server IP Address** field to appoint the corresponding PC to receive forwarded packets.

Click **Apply** to save the settings. The page shown in the following figure appears. A virtual server is added.

## 5.2.4 DMZ

Since some applications are not compatible with NAT, the device supports the use of a DMZ IP address for a single host on the LAN. This IP address is not protected by NAT and it is visible to agents on the Internet with the correct type of software. Note that any client PC in the DMZ is exposed to various types of security risks. If you use the DMZ, take measures (such as client-based virus protection) to protect the remaining client PCs on your LAN from possible contamination through DMZ.

Choose **Advanced > DMZ**. The page shown in the following figure appears.

The screenshot shows the Claro DSL Router web interface. At the top left is the Claro logo. A navigation bar contains buttons for Home, Setup, Advanced, Management, Status, and Help. A left sidebar lists menu items: Advanced, 2.4G Advanced Wireless, ALG, Port Forwarding, Porttrigger, DMZ (highlighted), SAMBA, Parental Control, Filtering Options, QoS, Anti-Attack Settings, and Dynamic DNS. The main content area is titled 'DMZ' and contains the following text:

The DSL Router will forward IP packets from the WAN that do not belong to any of the applications configured in the Port Forwarding table to the DMZ host computer.

Enter the computer's IP address and click "Apply" to activate the DMZ host.

Clear the IP address field and click "Apply" to deactivate the DMZ host.

---

**DMZ HOST**

WAN Connection : D\_PPpoe\_0\_1

Enable DMZ :

DMZ Host IP Address :

Buttons: Apply, Cancel

Choose to enable DMZ, input a DMZ host ip address or Select a IP from list, and click then **Apply** to save the settings.

## 5.2.5 SAMBA

Select **Advanced > SAMBA**. The page shown in the following figure appears.



**SAMBAs**

configure for Samba.

---

**SAMBA SERVER**

**Enable SAMBA :**

**Workgroup :**

**Netbios Name :**

modify the password for user root:

**New SMB password :**

**Retype new SMB password :**

**Enable USB Storage :**

**Enable Anonymous Access :**

The following table describes the parameters of this page.

Field	Description
Enable SAMBA	Select the check box to enable the samba service
Workgroup	Enter the name of your local area network (LAN).
Netbios Name	Enter your netbios name which is an identifier used by netbios services running on a computer.
New SMB password	Enter your samba password for user root.
Retype new SMB password	Reconfirm your samba password here.
Enable USB Storage	Select the check box to support USB storage.
Enable Anonymous Access	Select the check box to allow anonymous users access.

## 5.2.6 Parental Control

Choose **Advanced > Parental Control**. The **Parent Control** page shown in the following figure appears.

The screenshot displays the web interface for parental control. At the top left is the Claro logo. A navigation bar contains buttons for Home, Setup, Advanced, Management, Status, and Help. The left sidebar lists various settings, with 'Parental Control' highlighted. The main content area is titled 'PARENTAL CONTROL - WEBSITE FILTER' and contains the text: 'This is a blocking function for website addresses, if this function is enabled, access to the website addresses in the list will be denied.' Below this text is a button labeled 'Website Filter'. The second section is titled 'PARENTAL CONTROL - MAC FILTER' and contains the text: 'Uses MAC address to implement filtering.' Below this text is a button labeled 'MAC Filter'.

This page provides two useful tools for restricting the Internet access. **Website Filter** allows you to quickly create a list of all websites that you wish to stop users from accessing. **MAC Filter** allows you to control when clients or PCs connected to the device are allowed to access the Internet.

### 5.2.6.1 Website Filter

In the **Parental Control** page, click **Website Filter**. The page shown in the following figure appears.

## WEBSITE FILTER

Create a list of websites that you would like the devices on your network to be allowed or denied access to.

## WEBSITE FILTER

Access Control Mode : Deny ▼



## WEBSITE FILTER LIST

URL	Schedule
-----	----------




Click **Add**. The page shown in the following figure appears.

## WEBSITE FILTER LIST

URL	Schedule
-----	----------




## ADD SCHEDULE RULE

URL :

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)



Enter the website in the **URL** field. Select the **Schedule** from the drop-down list, or select **Manual Schedule** and select the corresponding time and days.

Click **Apply** to add the website to the **WEBSITE FILTER** table. The page shown in the following figure appears.


## WEBSITE FILTER

Access Control Mode : Deny ▾

Submit

Cancel

## WEBSITE FILTER LIST

	URL	Schedule
	www.xxx....	Sun,Mon,Tue,Wed,Thu,Fri,Sat, time 00:00 00:00

Add

Edit

Delete

## 5.2.6.2 MAC Filter

In the **Parental Control** page, click **MAC Filter**. The page shown in the following figure appears.

## BLOCK MAC ADDRESS

Time of Day Restrictions -- A maximum of 16 entries can be configured

This page adds a time of day restriction to a special LAN device connected to the router. The "Current PC's MAC Address" automatically displays the MAC address of the LAN device where the browser is running. To restrict another LAN device, click the "Other MAC Address" button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows-based PC, open a command prompt window and type "ipconfig /all".


## Mac Filtering Global Policy:

- Black List** --Allow all packets but **DENY** those matching any of specific rules listed
- White List** --Deny all packets but **ALLOW** those matching any of specific rules listed

Apply

Cancel

## BLOCK MAC ADDRESS--BLACKLIST

	Username	MAC	Schedule
			

Add

Edit

Delete

Choose **BLACK\_LIST** or **WHITE\_LIST**, and then click **Add**. The page shown in the following figure appears.

## ADD SCHEDULE RULE

User Name :

Current PC's MACAddress :

Other MAC Address :

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)

Enter the use name and MAC address and select the corresponding time and days. Click **Apply** to add the MAC address to the **BLOCK MAC ADDRESS Table**. The page shown in the following figure appears.

## BLOCK MAC ADDRESS--BLACKLIST

	Username	MAC	Schedule
	test	00:22:33:44:4c:22	Sun,Mon,Tue,Wed,Thu,Fri,Sat, time 00:00 00:00

## 5.2.7 Filtering Options

Choose **Advanced > Filtering Options**. The **Filtering Options** page shown in the following figure appears.

Claro

Home Setup Advanced Management Status Help

Advanced

2.4G Advanced Wireless

ALG

Port Forwarding

Porttrigger

DMZ

SAMBA

Parental Control

**Filtering Options**

IPv4 Filtering

IPv6 Filtering

Bridge Filtering

QoS

Anti-Attack Settings

FILTERING OPTIONS – IPV4 FILTERING

Uses IPv4 address to implement filtering.

IPv4 Filtering

FILTERING OPTIONS – IPV6 FILTERING

Uses IPv6 address to implement filtering.

IPv6 Filtering

FILTERING OPTIONS – BRIDGE FILTERING

Bridge Filtering is only effective on ATM PVCs configured in Bridge mode. It is MAC layer filter

Bridge Filtering

### 5.2.7.1 IPv4 Filtering

In the **Filtering Options** page, click **IPv4 Filtering**. The page shown in the following figure appears. In this page, you may configure IPv4 firewall function.

**Note:**

The settings are applicable only when IP filter is enabled.

## IPFILTER

Enable IP Filter

Enable SPI

Security Level

## FILTER MODEL

WAN --> LAN  White  Black

LAN --> WAN  White  Black

## ADD IP FILTER RULES

Choose

NO.	Enable	IP/Port(source)	IP/Port(destiantion)	Protocol	Description	Device Name

Select a security level, choose a filter direction, and then click **Add a rule** to display the following figure.

## IP FILTER CONFIGURATION

Connection :

Enable :

Protocol :

Source IP :

Source Mask :

Source Port :  -

Destination IP :

Destination Mask :

Destination Port :  -

Description :

The following table describes the parameters of this page.

Field	Description
Connection	Choose an IPv4 WAN connection.
Enable	Tick in the box to enable a filter rule.
Protocol	Choose a protocol corresponding to the rule. You may choose <b>TCP</b> , <b>UDP</b> , <b>ICMP</b> or <b>TCP/UDP</b> .
Source/ Destination IP	Original/ destination IP address.
Source/ Destination Mask	Original/ destination mask.
Source/Destination Port	Original/ end port, which is the original port range.
Description	You can describe this IPv4 filter rule.

After setting the parameters, click **Submit**. The page shown in the following figure appears. You can also click **Edit** or **Delete** to manage the rule.

#### IPFILTER

Enable IP Filter   
 Enable SPI   
 Security Level

#### FILTER MODEL

WAN --> LAN  White  Black  
 LAN --> WAN  White  Black

#### ADD IP FILTER RULES

Choose

	NO.	Enable	IP/Port(source)	IP/Port(destination)	Protocol	Description	Device Name
<input checked="" type="radio"/>	1	1	/	/	TCP		D_PPPE_0_1



### 5.2.7.2 IPv6 Filtering

In the **Filtering Options** page, click **IPv6 Filtering**. The page shown in the following figure appears. In this page, you may configure IPv6 firewall function.

**Note:**

The settings are applicable only when the firewall is enabled.

#### IPv6 FILTER CONFIGURATION

Enable IP Filter

Enable SPI

Security Level

#### FILTER MODEL

WAN --> LAN  White  Black

LAN --> WAN  White  Black

#### ADD IP FILTER RULES

Choose

NO.	Enable	IP/Port(source)	IP/Port(destiantion)	Protocol	Description	Device Name
<input type="button" value="Edit"/> <input type="button" value="Delete"/>						

Select a security level, choose a filter direction, and then click **Add a rule** to display the following figure.

Connection :   
 Enable :   
 Protocol : TCP   
 Source IP :   
 Source Prefix Length :   
 Source Port :  -   
 Destination IP :   
 Destination Prefix Length :   
 Destination Port :  -   
 Description :

The following table describes the parameters of this page.

Field	Description
Connection	Choose an IPv6 WAN connection.
Enable	Tick in the box to enable a firewall rule.
Protocol	Choose a protocol corresponding to the rule. You may choose <b>TCP</b> , <b>UDP</b> , <b>ICMPv6</b> or <b>TCP/UDP</b> .
Source/ Destination IP	Original/ destination IP address
Source prefix length	Original/ destination mask
Source/Destination Port	Original/ end port, which is the original port range
Description	You can describe this IPv6 filter rule.

After setting the parameters, click **Submit**. The page shown in the following figure appears. You can also click **Edit** or **Delete** to manage the rule.

## IPV6 FILTER CONFIGURATION

Enable IP Filter   
 Enable SPI   
 Security Level

## FILTER MODEL

WAN --> LAN  White  Black  
 LAN --> WAN  White  Black

## ADD IP FILTER RULES

Choose

	NO.	Enable	IP/Port(source)	IP/Port(destination)	Protocol	Description	Device Name
<input checked="" type="radio"/>	1	1	/	/	TCP		D_PPpOE_0_1

### 5.2.7.3 Bridge Filtering

In the **Filtering Options** page, click **Bridge Filtering**. The page shown in the following figure appears. This page is used to configure bridge parameters. In this page, you can change the settings or view some information of the bridge and its attached ports.

## BRIDGE FILTERING

Bridge Filtering is only effective on ATM PVCs configured in Bridge mode. ALLOW means that all MAC layer frames will be ALLOWED except those matching with any of the specified rules in the following table. DENY means that all MAC layer frames will be DENIED except those matching with any of the specified rules in the following table.

Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click "Apply" to save and activate the filter.

**WARNING : Changing from one global policy to another will cause all defined rules to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.**

## Bridge Filtering Global Policy:

- ALLOW** all packets but **DENY** those matching any of specific rules listed
- DENY** all packets but **ALLOW** those matching any of specific rules listed

Apply Cancel

## DISPLAY LIST

Interface	protocol	DMAC	SMAC	Prio	vlanID	DIR	TIME
-----------	----------	------	------	------	--------	-----	------

Add Edit Delete

As instructed in the page, choose a bridge filtering global policy as **ALLOW** or **DENY**, and then Click **Add** to add a bridge filter. The page shown in the following figure appears.

## 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 ▾

Wan interface: select all interface ▾

Apply Cancel

The following table describes the parameters of this page.

Field	Description
-------	-------------

Field	Description
Protocol Type	Choose a third-layer protocol type for bridge filtering from the drop-down list. You may choose <b>PPPoE</b> , <b>IPv4</b> , <b>IPv6</b> , <b>AppleTalk</b> , <b>IPX</b> or <b>NetBEUI</b> .
Destination MAC Address	The MAC address of sendee of the message
Source MAC Address	The MAC address of sender of the message
User priority	Vlan priority.
VlanID	Vlan ID of a message.
Frame Direction	Choose the sending direction as <b>WAN to LAN</b> or <b>LAN to WAN</b> .
Time schedule	Choose the filtering strategy as <b>always</b> or <b>never</b> .
Wan interface	Set an effective interface for the bridge filtering rule.

Click **Apply** to save the settings.

## 5.2.8 Anti-Attack Settings

Choose **Advanced > Anti-Attack Settings**. The **Anti-Attack Configuration** page shown in the following figure appears.

## ANTI-ATTACK

### Anti Attack

Enable Anti-Attack

Enable Attack Log

## INDIVIDUAL PROTECTION SWITCH

- Enable SYN Attack Protection, Max SYN Connections Per Second:  
50  (Peer/Second)
- Enable Attack Protection Function of Fragglen
- Enable Attack Protection Function of Echo Chargen
- Enable Attack Protection Function of IP Land
- Enable Protection of Anti PortScan

## ANTI INVALID PACKETS SWITCH

- TCP Flags: Set "SYN FIN"
- TCP Flags: Set "SYN RST"
- TCP Flags: Set "FIN RST"
- TCP Flags: Unset "ACK", Set "FIN"
- TCP Flags: Unset "ACK", Set "PSH"
- TCP Flags: Unset "ACK", Set "URG"
- TCP Flags: Unset "SYN ACK FIN RST URG PSH"
- TCP Flags: Set "SYN ACK FIN RST URG PSH"
- TCP Flags: Unset "PSH", Set "SYN ACK FIN RST URG"
- TCP Flags: Unset "SYN ACK RST URG PSH", Set "FIN"
- TCP Flags: Unset "SYN ACK RST", Set "FIN URG PSH"

Submit

Refresh

A denial-of-service (DoS) attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service.

Port scan protection is designed to block attempts to discover vulnerable ports or services that might be exploited in an attack from the WAN.

Click **Submit** to save the settings.

## 5.2.9 Dynamic DNS

The device supports dynamic domain name service (DDNS). The dynamic DNS service allows a dynamic public IP address to be associated with a static host name in any of the many domains, and allows access to a specified host from various locations on the Internet. Click a hyperlinked URL in the form of `hostname.dyndns.org` and allow remote access to a host. Many ISPs assign public IP addresses using DHCP, so locating a specific host on the LAN using the standard DNS is difficult. For example, if you are running a public web server or VPN server on your LAN, DDNS ensures that the host can be located from the Internet even if the public IP address changes. DDNS requires that an account be set up with one of the supported DDNS service providers (DynDNS.org, 3322.org and freedns.afraid.org).

Choose **Advanced > Dynamic DNS**. The page shown in the following figure appears.



The screenshot shows the web interface of the device. At the top left is the 'Claro' logo. A navigation bar contains tabs for 'Home', 'Setup', 'Advanced', 'Management', 'Status', and 'Help'. The 'Advanced' tab is selected. On the left is a sidebar menu with options: 'Advanced', '2.4G Advanced Wireless', 'ALG', 'Port Forwarding', 'Porttrigger', 'DMZ', 'SAMBA', 'Parental Control', 'Filtering Options', 'QoS', 'Anti-Attack Settings', and 'Dynamic DNS' (which is highlighted). The main content area is titled 'DYNAMIC DNS'. It contains a paragraph explaining the feature: 'The Dynamic DNS feature allows you to host a server (Web, FTP, Game Server, etc...) using a domain name that you have purchased (www.xxx.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. Using a DDNS service provider, your friends can enter your host name to connect to your game server no matter what your IP address is.' Below this text is a table with the following structure:

Hostname	Username	Service	Interface
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>			

Click **Add** to add dynamic DNS. The page shown in the following figure appears.

## DYNAMIC DNS

The Dynamic DNS feature allows you to host a server (Web, FTP, Game Server, etc...) using a domain name that you have purchased (www.xxx.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. Using a DDNS service provider, your friends can enter your host name to connect to your game server no matter what your IP address is.

## DYNAMIC DNS

Hostname	Username	Service	Interface
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>			

## ADD DYNAMIC DNS

DDNS provider : DynDNS.org ▼

Hostname :

Interface : D\_PPPE\_0\_1 ▼

Username :

Password :

The following table describes the parameters of this page.

Field	Description
DDNS provider	Select one of the DDNS registration organizations from the down-list drop. Available servers include <b>DynDns.org</b> , <b>3322.org</b> and <b>freedns.afraid.org</b> .
Host Name	Enter the host name that you registered with your DDNS service provider.
Username	Enter the user name for your DDNS account.
Password	Enter the password for your DDNS account.

Click **Apply** to save the settings.



## 5.2.10 Network Tools

Choose **Advanced > Network Tools**. The page shown in the following figure appears.

The screenshot displays the 'Network Tools' configuration page. At the top, there is a navigation bar with buttons for Home, Setup, Advanced, Management, Status, and Help. On the left, a sidebar menu lists various configuration options, with 'Network Tools' selected and highlighted. The main content area is titled 'NETWORK TOOLS - PORT MAPPING' and contains the following sections:

- NETWORK TOOLS - PORT MAPPING:** Describes port mapping for multiple ports to PVC and bridging groups. Includes a 'Port Mapping' button.
- NETWORK TOOLS - IGMP PROXY:** Describes transmission of identical content (e.g., multimedia) from a source to multiple recipients. Includes an 'IGMP Proxy' button.
- NETWORK TOOLS - IGMP SNOOPING:** Describes transmission of identical content (e.g., multimedia) from a source to multiple recipients. Includes an 'IGMP Snooping' button.
- NETWORK TOOLS - MLD CONFIGURATION:** Describes transmission of identical content (e.g., multimedia) from a source to multiple recipients. Includes an 'MLD Configuration' button.
- NETWORK TOOLS - UPNP:** Allows enabling or disabling UPnP. Includes an 'Upnp' button.
- NETWORK TOOLS - DSL:** (Section header visible, but content not fully shown).

(Network Tools-1)

### NETWORK TOOLS -- DSL

---

Allows you to configure advanced settings for DSL.

DSL

### NETWORK TOOLS -- TR-069

---

Allows you to configure TR-069 protocol.

TR-069

### NETWORK TOOLS -- CERTIFICATES

---

Allows you to manage certificates used with TR-069.

Certificates

### NETWORK TOOLS -- PRINTER

---

Allows you to manage printer .

printer

(Network Tools-2)

### 5.2.10.1 Port Mapping

Choose **Advanced > Network Tools** and click **Port Mapping**. The page shown in the following figure appears. In this page, you can bind the WAN interface and the LAN interface to the same group.

## PORT MAPPING

Port Mapping – A maximum 5 entries can be configured

Port Mapping supports multiple port to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the "Add" button. The "Delete" button will remove the grouping and add the ungrouped interfaces to the Default group.

## PORT MAPPING SETUP

	Group Name	Interfaces
<input type="checkbox"/>	Lan1	ethernet1,ethernet2,ra0,ra1,ra2,ra3,

Click **Add** to add port mapping. The page shown in the following figure appears.

## ADD PORT MAPPING

To create a new mapping group:

1. Enter the Group name and select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. The group name must be unique.
2. Click "Apply" button to make the changes effective immediately.

## PORT MAPPING CONFIGURATION

Group Name :

Grouped Interfaces	Available Interfaces
<input type="text"/>	ethernet1 ethernet2 ra0 ra1 ra2 ra3

The procedure for creating a mapping group is as follows:

- Step 1** Enter the group name.
- Step 2** Select interfaces from the **Available Interface** list and click the <- arrow button to add them to the grouped interface list, in order to create the required mapping of the ports. The group name must be unique.
- Step 3** Click **Apply** to save the settings.

### 5.2.10.2 IGMP Proxy

Choose **Advanced > Network Tools** and click **IGMP Proxy**. The page shown in the following figure appears.

## 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 hosts.

## IGMP PROXY CONFIGURATION

**WAN Interface :** D\_PPPOE\_0\_1 ▾  
**IGMP Version :** IGMP V3 ▾  
**Enable IGMP Proxy :**   
**LAN Connection :** Lan1 ▾  
**Enable FastLeaving :**   
**General Query Interval :** 150 (seconds)  
**General Query Response Interval :** 20 (1~255)(\*100 milliseconds)  
**Group Query Interval :** 325 (seconds)  
**Group Query Response Interval :** 20 (1~255)(\*100 milliseconds)  
**Group Query Count :** 3  
**Last Member Query Interval :** 1 (seconds)  
**Last Member Query Count :** 1

## IGMP TABLE

Group Address	Interface	State
E0000016	br0	0
E0000002	br0	0

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 after you enable it.

Click **Apply** to save the settings.

### 5.2.10.3 IGMP Snooping

Choose **Advanced > Network Tools** and click **IGMP Snooping**. The page shown in the following figure appears. When IGMP Snooping is enabled, the multicast data transmits through the specific LAN port which has received the request report.

#### IGMP

Transmission of identical content, such as multimedia, from a source to a number of recipients.

#### IGMP SETUP

Enabled :	<input checked="" type="checkbox"/>
Last Member Query Interval :	<input type="text" value="200000"/>
Host Timeout :	<input type="text" value="3000000"/>
Mrouter Timeout :	<input type="text" value="1"/>
Leave Timeout :	<input type="text" value="0"/>
Max Groups :	<input type="text" value="100"/>

### 5.2.10.4 MLD Configuration

Choose **Advanced > Network Tools** and click **MLD Configuration**. The page shown in the following figure appears. This section allows you to configure the MLD setup settings of your router.

## MLD SETTINGS

This section allows you to configure the MLD Setup settings of your Router . Please note that this section is optional and you should not need to change any of the settings here to get your network up and running.

## MLD PROXY

**Enable Mld Proxy**

WAN Connection : D\_PPPE\_0\_1 ▾

Query Interval : 125 (s)

Query Response Interval : 100 (1/10s)

Last Member Query Interval : 1 (1/10s)

## MLD SNOOPING

**Enable Mld Snooping**

Apply Cancel

The following table describes the parameters of this page.

Field	Description
Enable Mld Proxy	You can choose to enable MLD proxy.
WAN Connection	Choose an IPv6 WAN connection.
Enable MLD Snooping	Multicast Listener Discovery Snooping (MLD Snooping) is an IPv6 multicast constraining mechanism that runs on Layer 2 devices to manage and control IPv6 multicast groups. By analyzing received MLD messages, a Layer 2 device running MLD Snooping establishes mappings between ports and multicast MAC addresses and forwards IPv6 multicast data based on these mappings.

## 5.2.10.5 UPnP

Choose **Advanced > Network Tools** and click **UPnP**. The page shown in the following figure appears.

## UPnP

---

Universal Plug and Play (UPnP) supports peer-to-peer Plug and Play functionality for network devices.

---

### UPnP SETUP

---

**Enable UPnP**

Apply

Cancel

In this page, you can configure universal plug and play (UPnP). The system acts as a daemon after you enable UPnP.

UPnP is used for popular audio visual software. It allows automatic discovery of your device in the network. If you are concerned about UPnP security, you can disable it. Block ICMP ping should be enabled so that the device does not respond to malicious Internet requests.

Click **Apply** to save the settings.

## 5.2.10.6 DSL

Choose **Advanced > Network Tools** and click **DSL**. The page shown in the following figure appears.

### DSL SETTINGS

---

This page is used to configure the DSL settings of your DSL router. You need to disable DSL before you change the DSL mode.

---

### DSL SETTINGS

---

xDSL Mode : Auto Sync-Up ▼

xDSL Type : ANNEX A/L/M ▼

Apply

In this page, you can select a DSL mode. Normally, you can keep this factory default setting. The device negotiates the modulation mode with DSLAM.



Click **Apply** to save the settings.

### 5.2.10.7 TR-069

Choose **Advanced > Network Tools** and click **TR069**. The page shown in the following figure appears. In this page, you can configure the TR069 CPE.

#### TR-069

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

Select the desired values and click "Apply" to configure the TR-069 client options.

#### TR-069 CLIENT -- CONFIGURATION

**Cwmp** :  Disabled  Enabled  
**Inform** :  Disabled  Enabled  
**Inform Interval** :   
**ACS URL** :   
**ACS Username** :   
**ACS Password** :   
 Connection Request Authentication

Click **Apply** to save settings.

### 5.2.10.8 Certificates

Choose **Advanced > Network Tools** and click **Certificates**. The **Certificates** page shown in the following figure appears.

#### CERTIFICATES -- TRUSTED CA

Trusted CA certificates are used by you to verify peers' certificates.

Click **Trusted CA** button to import a certificate.

## CERTIFICATES -- TRUSTED CA

---

Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates. Only one certificates can be stored. Notice you have to synchronize your time when use certificate

---

### TRUSTED CA (CERTIFICATE AUTHORITY) CERTIFICATES

---

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

#### Note:

You can input a certificate after deleting the existing certificate.

### IMPORT CA CERTIFICATE

---

Certificate Name :

Certificate : 

```
-----BEGIN CERTIFICATE-----
<insert Certificate here>
-----END CERTIFICATE-----
```

### 5.2.10.9 Printer

Choose **Advanced** > **Network Tools** and click **Printer**. The **Printer** page shown in the following figure appears. In this page, you can enable/disable printer support.

#### PRINT SERVER SETTINGS

This page allows you to enable/disable printer support

Enable :   
Printer Name :   
URL : <http://192.168.1.1:631/printers/Printer>

#### DISPLAY LIST

Manufacturer	Model	CMD	Firmware Version
UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN

## 5.2.11 Routing

Choose **Advanced** > **Routing**. The page shown in the following figure appears.



The screenshot displays the LX220N web interface. At the top left is the Claro logo. A navigation bar contains links for Home, Setup, Advanced, Management, Status, and Help. A left sidebar lists various configuration categories, with 'Routing' selected and highlighted. The main content area is titled 'ROUTING' and contains four sections: 'STATIC ROUTE', 'IPv6 STATIC ROUTE', 'POLICY ROUTE', and 'RIP SETTINGS'. Each section has a corresponding button: 'Static Route', 'IPv6 Static Route', 'Policy Route', and 'RIP Settings'.

### 5.2.11.1 Static Routing

Choose **Advanced > Routing** and click **Static Routing**. The page shown in the following figure appears. This page is used to configure the routing information. In this page, you can add or delete IP routes.

## STATIC ROUTE

Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Apply" to add the entry to the routing table.

A maximum 30 entries can be configured.

## ROUTING – STATIC ROUTE

Destination	Subnet Mask	Gateway	Interface
-------------	-------------	---------	-----------

Click **Add** to add a static route. The page shown in the following figure appears.

## STATIC ROUTE ADD

Destination Network Address :

Subnet Mask :

Use Gateway IP Address :

Use Interface : D\_PPpOE\_0\_1 ▾

The following table describes the parameters of this page.

Field	Description
Destination Network Address	The destination IP address of the router.
Subnet Mask	The subnet mask of the destination IP
Use Interface	The interface name of the router output port.
Use Gateway IP Address	The gateway IP address of the router.

Click **Apply** to save the settings.

### 5.2.11.2 IPv6 Static Route

Choose **Advanced > Routing** and click **IPv6 Static Route**. The page shown in the following figure appears.

### IPv6 STATIC ROUTE

Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Apply" to add the entry to the routing table, the Gateway IP Address should be the Default Gateway of connected V6 connection so as to take effect.

A maximum 30 entries can be configured.

### ROUTING – IPv6 STATIC ROUTE

Status	Destination	Gateway	Interface
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>			

Click Add to add an IPv6 static route. The page shown in the following figure appears.

### IPv6 STATIC ROUTE ADD

Enable :

Destination Network Address :

Use Gateway IP Address :

Use Interface : D\_PPpoe\_0\_1 ▾

The following table describes the parameters of this page.

Field	Description
Destination Network Address	The destination IP address of the static route.
Use Gateway IP Address	The gateway IP address of the static route.
Use Interface	The interface name of the static route.

### 5.2.11.3 Policy Route

Choose **Advanced > Routing** and click **Policy Route**. The page shown in the following figure appears. The policy route binds one WAN connection and one LAN interface.

#### POLICY ROUTE

Policy Route :chose one Wanconnection and one Lanconnection then bind them.

#### POLICY ROUTE SETUP

WAN	LAN
-----	-----

Click **Add**, and the page shown in the following figure appears. Choose one WAN connection and at least one LAN connection to bind together, and then click **Apply**.

#### WAN INSTANCE AND LAN INSTANCE

WAN Connection :

LAN Connection :  Lan2  
 Lan1  
 Wlan1  
 Wlan2  
 Wlan3  
 Wlan4

### 5.2.11.4 RIP

Choose **Advanced > Routing** and click **RIP**. The page shown in the following figure appears. This page is used to select the interfaces on your device that use RIP and the version of the protocol used.

## RIP CONFIGURATION

To activate RIP for the device, select the "Enabled" checkbox for Global RIP Mode. To configure an individual interface, select the desired RIP version and operation, followed by placing a check in the "Enabled" checkbox for the interface. Click the "Apply" button to save the configuration, and to start or stop RIP based on the Global RIP Mode selected.

## RIP

Interface	Dynamic Route	Direction
D_PPPoE_0_1	OFF ▾	Active ▾
D_PPPoE_0_2	OFF ▾	Active ▾
Lan1	OFF ▾	Active ▾

Apply Cancel

If you are using this device as a RIP-enabled device to communicate with others using the routing information protocol, enable RIP and click **Apply** to save the settings.

## 5.2.11.5RIPng

Choose **Advanced > Routing** and click **RIPng**. The page shown in the following figure appears. You can enable or disable dynamic routing of an IPv6 interface after establishing an IPv6 PVC connection.

## RIPNG CONFIGURATION

To activate RIPng for the interface, place a check in the "Enabled" checkbox for the interface. Click the "Apply" button to save the configuration, and to start or stop RIPng based on the configuration.

## RIPNG

Interface	VPI/VCI	Enabled
D_PPPoE_0_1	PVC:0/32	<input type="checkbox"/>

Apply Cancel



## 5.2.12 NAT

Choose **Advanced** > **NAT**. The page shown in the following figure appears. 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 unidirectional, 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

### NAT

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.

### NAT TABLES

Name	Internal IP Address	External IP Address
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>		

Click **Add** to set a NAT set in the following page. For IP type, you can choose single IP or IP range. Click **Apply** to save and enable the setting.

### NAT SETTINGS

Entry Name :

Internal IP Type : Single IP ▾

Internal IP Address :

External IP Type : Single IP ▾

External IP Address :

## 5.2.13 DLNA

Choose **Advanced > DLNA**. The page shown in the following figure appears. In this page, you can choose to enable DLNA, and then click **Apply**.

### DLNA

---

You can Enable or Disable DLNA here.

---

### DLNA SETTING

---

Enable DLNA :

## 5.2.14 IP Tunnel

Choose **Advanced > IP Tunnel**. The page shown in the following figure appears.

The screenshot displays the web management interface for the LX220N device. At the top, there is a navigation bar with buttons for Home, Setup, Advanced, Management, Status, and Help. The left sidebar contains a menu of configuration options, with 'IP Tunnel' selected and expanded to show '4in6 Tunnel' and '6in4 Tunnel'. The main content area is titled '4IN6 TUNNEL CONFIGURATION' and contains the text 'Configure 4in6 Tunnel.' followed by a 'Configure 4in6 Tunnel' button. Below this, there is a section titled '6IN4 TUNNEL CONFIGURATION' with the text 'Configure 6in4 Tunnel.' and a 'Configure 6in4 Tunnel' button.

### 5.2.14.14in6 Tunnel

Choose **Advanced** > **IP Tunnel** and then click **4in6 Tunnel**. The page shown in the following figure appears. In this page, you can configure IPv4 penetration through IPv6 network. When only IPv6 access is provided by your ISP, you can access the Internet via IPv4 and IPv6.

## IP TUNNEL CONFIGURATION

Network topology in IPv4/v6 Internet, some only run IPv6 protocol stack routers form the pure IPv6 backbone. However, due to the large IPv4 applications will be a period of time is still widely used, so the need for pure IPv6 backbone network to IPv4 stack border access.

## IPTUNNEL

Tunnel Name	Mode	Wan interface	Lan interface	Activated	Counter
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>					

## DS-LITE IPV4 OVER IPV6 TUNNEL LIST

Mechanism	Dynamic	RemoteIPv6Address	ConnStatus	Select
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>				

Click **Add** below the table **IPTUNNEL** to add tunnel items. The page shown in the following figure appears.

## ADD TUNNEL ITEMS

**Tunnel Name:**   
**Tunnel Mode:** 4in6 ▾  
**Wan Interface:** D\_PPPoE\_0\_1 ▾  
**Lan Interface:** LAN:br0 ▾

The following table describes the parameters of this page.

Field	Description
Tunnel Name	Set a tunnel name.
Tunnel Mode	Select the tunnel mode as 4 in6 or 6in4.
Wan Interface	Choose a WAN interface used for the tunnel.
Lan Interface	Choose a LAN interface used for the tunnel.

Click **Apply** to enable the settings.

Click **Add** below the table **DS-Lite IPv4 over IPv6 Tunnel List** to add a DS-Lite item, which is a 4in6 tunnel. The page shown in the following figure appears.

**DS-LITE IPV4 OVER IPV6 TUNNEL LIST**

Mechanism: DualStackLite ▾  
Dynamic: 0 ▾  
RemoteIPv6Address:

The following table describes the parameters of this page.

Field	Description
Mechanism	The tunnel type is DS-Lite, which is 4in6 tunnel.
Dynamic	Set the obtaining mode of remote IPv6 addresses. You can select <b>0</b> or <b>1</b> .
RemoteIPv6Address	Set the remote end IPv6 address of the tunnel.

Click **Apply** to enable the settings.

### 5.2.14.2 6in4 Tunnel

Choose **Advanced > IP Tunnel** and then click **6in4 Tunnel**. The page shown in the following figure appears. In this page, you can configure IPv6 penetration through IPv4 network. When only IPv4 access is provided by your ISP, you can access the Internet via IPv4 and IPv6.

## IP TUNNEL CONFIGURATION

6rd is a mechanism to facilitate IPv6 rapid deployment across IPv4 infrastructures of Internet service providers.

It is derived from 6to4, a preexisting mechanism to transfer IPv6 packets over the IPv4 network, with the significant change that it operates entirely within the end-user's ISP's network, thus avoiding the major architectural problems inherent in the original design of 6to4.

## IP TUNNEL

Tunnel Name	Mode	Wan interface	Lan interface	Activated	Counter
-------------	------	---------------	---------------	-----------	---------

## IPV6 RAPID DEPLOYMENT

Mechanism	Dynamic	IPv4MaskLen	Prefix	BorderRelayAddress	ConnStatus	Select
-----------	---------	-------------	--------	--------------------	------------	--------

Click **Add** below the table **IP TUNNEL** to add tunnel items. The page shown in the following figure appears.

## ADD TUNNEL ITEMS

**Tunnel Name:**   
**Tunnel Mode:** 6in4 ▾  
**Wan Interface:** D\_PPPOE\_0\_2 ▾  
**Lan Interface:** LAN:br0 ▾

The following table describes the parameters of this page.

Field	Description
Tunnel Name	Set a tunnel name.
Tunnel Mode	Select the tunnel mode as 4 in6 or 6in4.
Wan Interface	Choose a WAN interface used for the tunnel.
Lan Interface	Choose a LAN interface used for the tunnel.

Click **Apply** to enable the settings.

Click **Add** below the table **IPv6 Rapid Deployment** to add a 6RD item, which is a 6in4 tunnel. The page shown in the following figure appears.

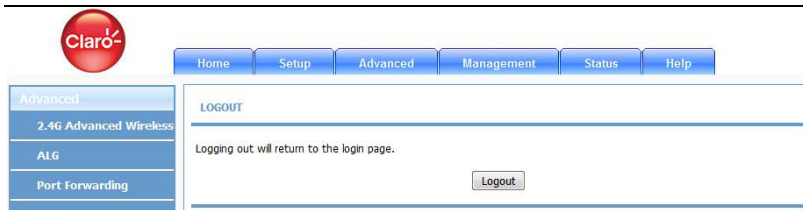
The following table describes the parameters of this page.

Field	Description
Mechanism	The tunnel type is 6RD, which is a 6in4 tunnel.
Dynamic	Set the obtaining mode of Border Relay Address.
IPv4MaskLen	Set the subnet mask digits of the IPv4 address of the local WAN interface.
Prefix	Set the IPv6 prefix of the 6RD tunnel.
BorderRelayAddress	Set the Border Relay IPv4 address at the remote end.

Click **Apply** to enable the settings.

## 5.2.15 Logout

Choose **Advanced > Logout**. The page shown in the following figure appears. In this page, you can log out of the configuration page.



## 5.3 Management

In the main interface, click **Management** tab to enter the **Management** menu as shown in the following figure. The submenus are **Global IPv6**, **System Management**, **Firmware Update**, **Access Controls**, **Diagnosis**, **Log Configuration** and **Logout**.

### 5.3.1 System Management

Choose **Management** > **System Management**. The page shown in the following figure appears.



The screenshot shows the web interface for the LX220N router. At the top, there is a navigation bar with buttons for Home, Setup, Advanced, Management, Status, and Help. On the left, a sidebar menu includes Management, System, Firmware Update, Access Controls, Diagnostics, System Log, and Logout. The main content area is divided into four sections:

- SYSTEM -- REBOOT**: Contains the instruction "Click the button below to reboot the router." and a "Reboot" button.
- SYSTEM -- BACKUP SETTINGS IN DSL ROUTER**: Contains the instruction "The last correct settings information:" and a red note: "Note: Please always save configuration file first before viewing it." Below this is a "Backup Setting" button.
- SYSTEM -- UPDATE SETTINGS**: Contains the instruction "Update DSL Router settings. You may update your router settings using your saved files." Below this is a "Settings File Name:" label, a text input field containing "浏览...", and a "Update Setting" button.
- SYSTEM -- RESTORE DEFAULT SETTINGS**: Contains the instruction "Restore DSL Router settings to the factory defaults." and a "Restore Default Setting" button.

In this page, you can reboot device, back up the current settings to a file, update settings from the file saved previously and restore the factory defaults.

The buttons in this page are described as follows.

Field	Description
Reboot	Click this button to reboot the device.
Backup Setting	Click this button to save the settings to the local hard drive. Select a location on your computer to back up the file. You can name the configuration file.
Update setting	Click <b>Browse</b> to select the configuration file of device and then click <b>Update Settings</b> to begin updating the device configuration.

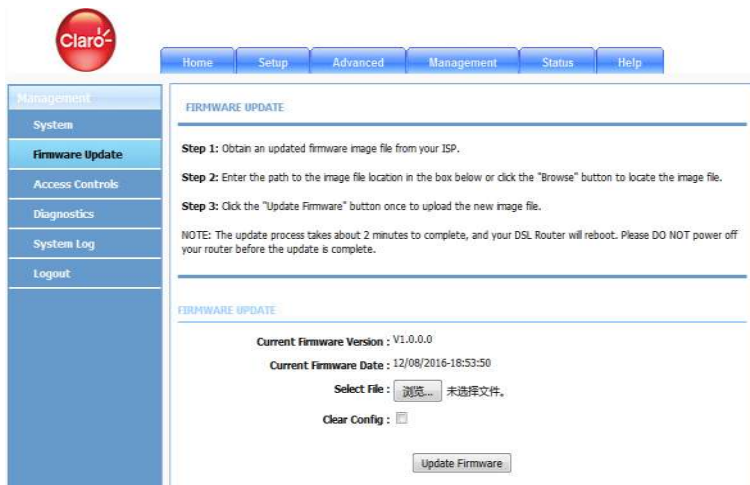
Restore Default Setting	Click this button to reset the device to default settings.
-------------------------	--

**Note:**

Do not turn off your device or press the Reset button while an operation in this page is in progress.

## 5.3.2 Firmware Update

Choose **Management > Firmware Update**. The page shown in the following figure appears. In this page, you can upgrade the firmware of the device.



To update the firmware, take the following steps.

**Step 1** Click **Browse...** to locate the file.

**Step 2** Select **Clear Config** to clear the current configuration and restore the default.

**Step 3** Click **Update Firmware** to copy the file.

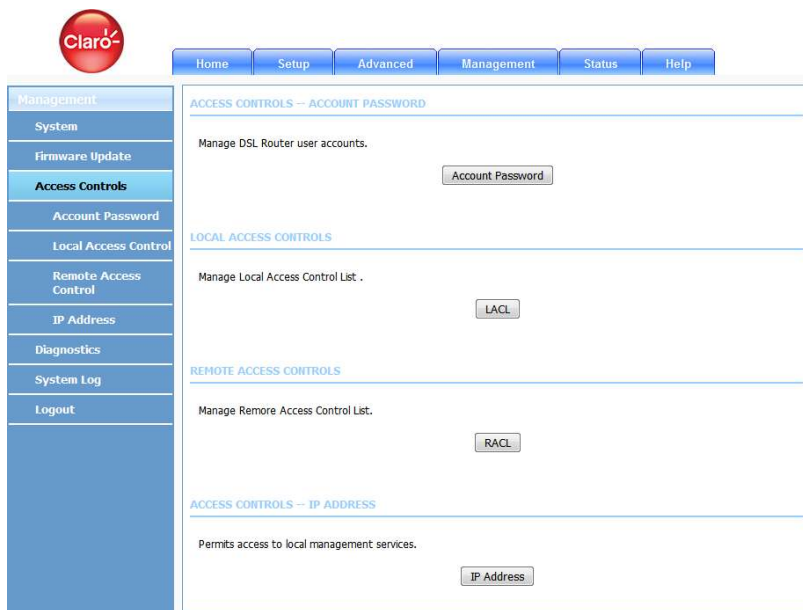
The device loads the file and reboots automatically.

**Note:**

Do not turn off your device or press the Reset button while an operation in this page is in progress.

## 5.3.3 Access Controls

Choose **Management > Access Controls**. The **Access Controls** page shown in the following figure appears. The page contains **User Management**, **Local Access Control**, **Remote Access Control** and **IP Address**.



The screenshot shows the Claro LX220N web interface. At the top left is the Claro logo. A navigation bar contains buttons for Home, Setup, Advanced, Management, Status, and Help. A left-hand navigation menu lists: Management, System, Firmware Update, Access Controls (highlighted), Account Password, Local Access Control, Remote Access Control, IP Address, Diagnostics, System Log, and Logout. The main content area is titled "ACCESS CONTROLS -- ACCOUNT PASSWORD" and contains a button labeled "Account Password". Below this is a section titled "LOCAL ACCESS CONTROLS" with a button labeled "LACL". The next section is "REMOTE ACCESS CONTROLS" with a button labeled "RACL". The final section is "ACCESS CONTROLS -- IP ADDRESS" with a button labeled "IP Address".

### 5.3.3.1 Account Password

In the **Access Controls** page, click **Account Password**. The page shown in the following figure appears. In this page, you can change the password of the user and set time for automatic logout.

## ACCOUNT PASSWORD

---

Access to your DSL Router is controlled through three user accounts: admin, support, and user.

The user name "admin" will have full access to the Web-based management interface.

The user name "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics.

The user name "user" can access the DSL Router, view configuration settings and statistics, as well as update the router's firmware.

Use the fields below to enter up to 16 characters and click "Apply" to change or create passwords. Note: Password cannot contain a space.

---

## ACCOUNT PASSWORD

---

Username :	<input type="text" value="admin"/>
New Username :	<input type="text" value="admin"/>
Current Password :	<input type="password"/>
New Password :	<input type="password"/>
Confirm Password :	<input type="password"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

## WEB IDLE TIME OUT SETTINGS

---

Web Idle Time Out :	<input type="text" value="29"/>	(5 ~ 30 minutes)
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

You should change the default password to secure your network. Ensure that you remember the new password or write it down and keep it in a safe and separate location for future reference. If you forget the password, you need to reset the device to the factory default settings and all configuration settings of the device are lost.

Select the **Username** from the drop-down list. You can select **admin** (subject to different models) or Usuario.

Enter the current and new passwords and confirm the new password to change the password. Click **Apply** to apply the settings.

**Web Idle Time Out** is the idle duration of user interfaces. After this duration, you need to login to the router again for operation.

### 5.3.3.2 Local Access Control

Under the **Access Controls** menu, click **Local Access Control**. The page shown in the following figure appears. This page allows you to enable or disable LAN management services. For example, if the Telnet service is enabled on port 23, the remote host can access the router by Telnet through port 23.

#### LAN ACL

You can set a service control list (SCL) to enable or disable services from being used.

#### LOCAL ACCESS CONTROL -- SERVICES

Enable Local Access :

Choose A Connection : Lan1 ▾

#### IPv4 ACL

Service	Enable	Source IP	Source Mask	Protocol	Port
FTP	<input checked="" type="checkbox"/>	0.0.0.0	0.0.0.0	TCP	21
HTTP	<input checked="" type="checkbox"/>	0.0.0.0	0.0.0.0	TCP	80
ICMP	<input checked="" type="checkbox"/>	0.0.0.0	0.0.0.0	ICMP	-
SSH	<input checked="" type="checkbox"/>	0.0.0.0	0.0.0.0	TCP	22
TELNET	<input checked="" type="checkbox"/>	0.0.0.0	0.0.0.0	TCP	23
TFTP	<input checked="" type="checkbox"/>	0.0.0.0	0.0.0.0	UDP	69
DNS	<input checked="" type="checkbox"/>	0.0.0.0	0.0.0.0	UDP	53
TR069	<input checked="" type="checkbox"/>	0.0.0.0	0.0.0.0	TCP	7547

#### IPv6 ACL

Service	Enable	Source IP	Protocol	Port
HTTP	<input checked="" type="checkbox"/>	::/0	TCP	80
TR069	<input checked="" type="checkbox"/>	::/0	TCP	7547
ICMPv6	<input checked="" type="checkbox"/>	::/0	ICMPv6	-

### 5.3.3.3 Remote Access Control

Under the **Access Controls** menu, click **Remote Access Control**. The page shown in the following figure appears. This page allows you to enable or disable WAN management services. You may refer to 5.3.3.2 Local Access Control.

#### WAN ACL

You can set a service control list (SCL) to enable or disable services from being used.

#### REMOTE ACCESS CONTROL -- SERVICES

Choose A Connection

#### IPv4 ACL

Service	Enable	Source IP	Source Mask	Protocol	Destination Port
ICMP	<input checked="" type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	ICMP	-
FTP	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	TCP	<input type="text" value="21"/>
HTTP	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	TCP	<input type="text" value="80"/>
SSH	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	TCP	<input type="text" value="22"/>
TELNET	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	TCP	<input type="text" value="23"/>
TFTP	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	UDP	<input type="text" value="69"/>
DNS	<input checked="" type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	UDP	<input type="text" value="53"/>
TR069	<input checked="" type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	TCP	<input type="text" value="7547"/>

#### IPv6 ACL

Service	Enable	Source IP	Protocol	Destination Port
HTTP	<input checked="" type="checkbox"/>	<input ":::0"="" type="text" value=""/>	TCP	<input type="text" value="80"/>
ICMPv6	<input checked="" type="checkbox"/>	<input ":::0"="" type="text" value=""/>	ICMPv6	-



### 5.3.3.4 IP Address

In the **Access Controls** page, click **IP Address**. The page shown in the following figure appears.

### IP ADDRESS

---

The IP Address Access Control mode, if enabled, permits access to local management services from IP addresses contained in the Access Control List. If the Access Control mode is disabled, the system will not validate IP addresses for incoming packets. The services are the system applications listed in the Service Control List.

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

---

### ACCESS CONTROL – IP ADDRESSES

---

**Enable Access Control Mode**

	IP

---

In this page, you can configure the IP address for access control list (ACL). If ACL is enabled, only devices with the specified IP addresses can access the device.

**Note:**

If you enable the ACL, ensure that IP address of the host is in the ACL list.

To add an IP address to the IP list, click **Add**. The page shown in the following figure appears.

### IP ADDRESS

---

IP Address :

Click **Apply** to apply the settings, and then choose **Enable Access Control Mode** to enable ACL.

## 5.3.4 Diagnosis

Choose **Management > Diagnosis**. The **Diagnosis** page shown in the following figure appears. The page contains **DSL Test** and **Traceroute**.

The screenshot displays the web interface for the LX220N device. At the top left is the Claro logo. A horizontal navigation bar contains buttons for Home, Setup, Advanced, Management, Status, and Help. A vertical sidebar on the left lists various management options: Management, System, Firmware Update, Access Controls, Diagnostics, DSL test, Traceroute, Ping, System Log, and Logout. The main content area is titled "DIAGNOSTICS -- DSL TEST" and contains the text "DSL Test can diagnostics your DSL connection." followed by a "DSL Test" button. Below this is a section titled "DIAGNOSTICS -- TRACEROUTE" with the text "Traceroute diagnostics sends packets to determine the routers on the Internet." and a "Traceroute" button. The final section is titled "DIAGNOSTICS -- PING" with the text "Ping diagnostics used to test the reachability of a host on a network and to measure the round-trip time for messages sent from the originating host to a destination computer." and a "Ping" button.

### 5.3.4.1 Traceroute

In the **Diagnosis** page, click **Traceroute**. The page shown in the following figure appears. In this page, you can determine the routers on the Internet by sending packets.

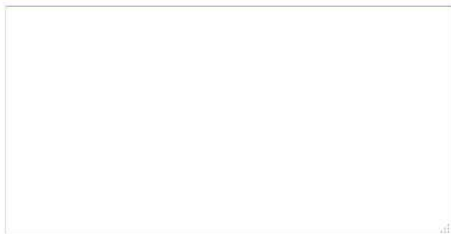


## TRACEROUTE DIAGNOSIS

Traceroute diagnostics sends packets to determine the routers on the Internet.

Protocol :	IPv4	▼
WAN Connction :	D_PPPoE_0_2	▼
Host :	8.8.8.8	
Max TTL :	30	(1-64)
Wait times :	5000	(>1ms)

## RESULT



Click **Traceroute** to begin diagnosis. After finish, the page shown in the following figure appears.

## RESULT

```
Traceroute Status: Traceroute has finished
traceroute to 192.168.1.1 (192.168.1.1), 30
hops max, 38 byte packets
  1 homestation (192.168.1.1)  0.837 ms
0.612 ms  0.622 ms
```

## 5.3.5 System Log

Choose **Management > Log Configuration**. The **System Log** page shown in the following figure appears.

The screenshot shows the 'System Log' configuration page. At the top, there is a navigation bar with tabs: Home, Setup, Advanced, Management, Status, and Help. On the left, a sidebar menu lists: Management, System, Firmware Update, Access Controls, Diagnostics, System Log (selected), and Logout. The main content area is titled 'SYSTEM LOG' and contains the following text:

If the log mode is enabled, the system will begin to log all the selected events. If the selected mode is "Remote" or "Both", events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is "Local" or "Both", events will be recorded in the local memory.

Select the desired values and click "Apply" to configure the system log options.

Note: This will not work correctly if modem time is not properly set! Please set it in "Setup/Time and Date"

Below this is the 'SYSTEM LOG -- CONFIGURATION' section, which includes:

- Enable Log
- Mode : Local (dropdown menu)
- Server IP Address : (input field)
- Server UDP Port : (input field)
- Buttons: Apply, Cancel, View System Log

This page displays event log data in the chronological manner. You can read the event log from the local host or send it to a system log server. In this page, you can enable or disable the system log function.

To log the events, take the following steps.

- Step 1** Select **Enable Log** check box.
- Step 2** Select the display mode from the **Mode** drop-down list.
- Step 3** Enter the **Server IP Address** and **Server UDP Port** if the **Mode** is set to **Both** or **Remote**.
- Step 4** Click **Apply** to apply the settings.
- Step 5** Click **View System Log** to view the detail information of system log.

## 5.4 Status

In the main interface, click **Status** tab to enter the **Status** menu as shown in the following figure. The submenus are **Device Info**, **Wireless Clients**, **DHCP**

**Clients, LAN Clients, Monitor, Stream Rate, Logs, Statistics, Route Info and Logout.** You can view the system information and monitor performance.

## 5.4.1 Device Info

Choose **Status > Device Info**. The page shown in the following figure appears.

### DEVICE INFO

This information reflects the current status of your all connection.

### SYSTEM INFO

Modem Name :	LX220N
Serial Number :	30303030303
Time and Date :	2016-12-09 07:32
HardwareVersion :	VDSLGAW-LT9B-H2H4
SoftwareVersion	LX220N_CLARO_GT_SW01
Firmware Version :	V1.0.0.0
lang_BuiltDate	12/08/2016-18:53:50
System Up Time :	19:29:42

### INTERNET INFO

Internet Connection Status :

IP Protocol:

Internet Connection Status:	Connected
Wan service type:	Internet
IP Address:	10.99.208.107
Sub Mask:	255.255.255.255
Default Gateway:	10.99.208.1
DNS Server:	172.24.11.10,172.24.10.10

#### Enabled WAN Connections :

VPI/VCI	Service Name	Protocol
0/32	D_PPPoE_0_1	PPPoE
0/45	D_PPPoE_0_2	PPPoE

The page displays the summary of the device status. It includes the information of firmware version, upstream rate, downstream rate, uptime and Internet configuration (both wireless and Ethernet statuses).

## 5.4.2 Wireless Clients

Choose **Status > Wireless Clients**. The page shown in the following figure appears. The page displays authenticated wireless stations and their statuses.

The screenshot shows the web interface of the LX220N device. At the top left is the Claro logo. A navigation bar contains buttons for Home, Setup, Advanced, Management, Status, and Help. On the left is a sidebar menu with options: Status, Device Info, Wireless Clients (highlighted), DHCP Clients, LAN Clients, Monitor, Stream Rate, and Logs. The main content area is titled 'WIRELESS CLIENTS' and contains the text: 'This page shows authenticated wireless stations and their status.' Below this is a section titled 'WIRELESS -- AUTHENTICATED STATIONS' which contains a table with the following headers: Mac, Associated, Authorized, SSID, Interface, and Remove to Deny. A 'Refresh' button is located below the table.

## 5.4.3 DHCP Clients

Choose **Status > DHCP Clients**. The page shown in the following figure appears. This page displays all client devices that obtain IP addresses from the device. You can view the host name, IP address, MAC address and time expired(s).

The screenshot displays the LX220N web interface. At the top left is the Claro logo. A navigation bar contains buttons for Home, Setup, Advanced, Management, Status, and Help. A left sidebar menu lists various status pages: Status, Device Info, Wireless Clients, DHCP Clients (highlighted), LAN Clients, Monitor, Stream Rate, Logs, Statistics, Route Info, and Logout. The main content area is titled 'DHCP CLIENTS' and contains the text: 'This information reflects the current DHCP client of your modem.' Below this is a section titled 'DHCP LEASES' with a table header containing 'Hostname', 'MAC Address', 'IP Address', and 'Expires In'. A 'Refresh' button is positioned below the table header.

## 5.4.4 Logs

Choose **Status > Logs**. The page shown in the following figure appears. This page lists the system log. Click **Refresh** to refresh the system log shown in the table.

Claro

Home Setup Advanced Management Status Help

Status

Device Info

Wireless Clients

DHCP Clients

LAN Clients

Monitor

Stream Rate

**Logs**

Statistics

Route Info

Logout

LOGS

This page allows you to view system logs.

SYSTEM LOG

Manufacturer: LANIX  
ProductClass: HG110  
SerialNumber: 30303030303  
IP: 192.168.1.1  
HWVer: VDSLGAW-LT9B-HZH4  
SWVer: LX220N\_CLARO\_GT\_SW01

Refresh

## 5.4.5 Statistics

Choose **Status > Statistics**. The page shown in the following figure appears. This page displays the statistics of the network and data transfer. This information helps technicians to identify if the device is functioning properly. The information does not affect the function of the device.

# LX220N User Manual

## DEVICE INFO

This information reflects the current status of your all connection.

## LOCAL NETWORK & WIRELESS

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Rx drop	Bytes	Pkts	Errs	Tx drop
Lan1	993191	8920	0	0	5173870	16261	0	0
CLARO_be3f2f	0	0	0	0	0	0	0	0

## INTERNET

Service	VPI/VCI	Protocol	Received				Transmitted			
			Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
D_PPPoE_...	0/32	PPPoE	1601	23	0	0	1095	20	0	0
D_PPPoE_...	0/45	PPPoE								

## DSL

<b>Status:</b>	Up	
<b>Mode:</b>	ADSL2+	
<b>Type:</b>	Annex_A	
<b>Traffic Type:</b>	ATM	
<b>Line Coding:</b>	Enable	
<b>Up Time:</b>	466	
	<b>Downstream</b>	<b>Upstream</b>
<b>SNR Margin (0.1dB):</b>	82	90
<b>Attenuation (0.1dB):</b>	93	191
<b>Output Power (dBm):</b>	16.5	29.5
<b>Attainable Rate (Kbps):</b>	19280	19348
<b>Rate (Kbps):</b>	19171	1021
<b>D (interleave depth):</b>	64	8
<b>Delay (msec):</b>	675	1450
<b>Data Counter:</b>	<b>680909731</b>	<b>183</b>
	<input type="button" value="Clear"/>	<input type="button" value="Clear"/>

## 5.4.6 Route Info

Choose **Status > Route Info**. The page shown in the following figure appears. The table shows a list of destination routes commonly accessed by the network.

The screenshot shows the Claro LX220N web interface. At the top, there is a navigation bar with tabs: Home, Setup, Advanced, Management, Status, and Help. On the left, there is a sidebar menu with the following items: Status, Device Info, Wireless Clients, DHCP Clients, LAN Clients, Monitor, Stream Rate, Logs, Statistics, **Route Info** (highlighted), and Logout. The main content area is titled 'ROUTE INFO' and contains a legend: 'Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate D - dynamic (redirect), M - modified (redirect)'. Below the legend is a table titled 'DEVICE INFO -- ROUTE' with the following data:

Destination	Gateway	Subnet Mask	Flags	Metric	Service	Interface
0.0.0.0	10.99.208.1	0.0.0.0	UG	0	0	ppp0
10.99.208.1	0.0.0.0	255.255.255.255	UH	0	0	ppp0
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	br0
216.230.145.96	0.0.0.0	255.255.255.252	U	0	0	br0
239.0.0.0	0.0.0.0	255.0.0.0	U	0	0	eth0

## 5.5 Help

In the main interface, click **Help** tab to enter the **Help** menu as shown in the following figure. This section provides detailed configuration information for the device. Click a wanted link to view corresponding information.



## 6 Trouble Shooting

Question	Answer
Why are all the indicators off?	<ul style="list-style-type: none"> <li>● Check the connection between the power adapter and the power socket.</li> <li>● Check whether the power switch is turned on.</li> </ul>
Why the <b>LAN</b> indicator is off?	<p>Check the following:</p> <ul style="list-style-type: none"> <li>● The connection between the device and your PC, hub or switch</li> <li>● The running status of the computer, hub, or switch</li> </ul>
Why is the <b>DSL</b> indicator not on?	Check the connection between the <b>DSL</b> port of the device and the wall jack.
Why Internet access fails while the ADSL indicator is on?	Check whether the VPI, VCI, user name and password are correctly entered.
Why I fail to access the web configuration page of the DSL router?	Choose <b>Start &gt; Run</b> from the desktop, and ping <b>192.168.1.1</b> (IP address of the DSL router). If the DSL router is not reachable, check the type of the network cable, the connection between the DSL router and the PC, and the TCP/IP configuration of the PC.
How to load the default settings after incorrect configuration?	<p>To restore the factory default settings, turn on the device, and press the reset button for about 3 seconds, and then release it. The default IP address and the subnet mask of the DSL router are <b>192.168.1.1</b> and <b>255.255.255.0</b>, respectively.</p> <ul style="list-style-type: none"> <li>● Administrator username/password: <b>1234/1234</b> <i>(subject to different models)</i></li> <li>● Common username/password: <b>user/user</b>.</li> <li>● ISP technician username/password: <b>support/support</b>.</li> </ul>

## 7. FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

### FCC Radiation Exposure Statement

This device complies with FCC radiation exposure limits set forth for an uncontrolled environment and it also complies with Part 15 of the FCC RF Rules. This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provide with antenna installation instructions and consider removing the no-collocation statement.

This device complies with Part 15 of the FCC Rules. Operation is subject to the

following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

### Caution!

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

### **FCC - PART 68**

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On the bottom of this equipment is a label that contains, among other information, a product identifier in the format US: S90DL01ALX220N. If requested, this number must be provided to the telephone company.

This equipment uses the following USOC jacks: RJ-11, RJ-45, USB Jack, Power Jack

### **REN (RINGER EQUIVALENT NUMBERS) STATEMENT**

Notice: The Ringer Equivalence Number (REN: 0.1A) assigned to each terminal device provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the Ringer Equivalence Numbers of all the devices does not exceed 5.

### **ATTACHMENT LIMITATIONS STATEMENT**

Notice: This equipment meets telecommunications network protective, operational and safety requirements as prescribed in the appropriate Terminal Equipment Technical Requirements document(s). This is confirmed by marking the equipment

with the Industry Canada certification number. The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together.

This precaution may be particularly important in rural areas. Caution: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate