Alcatel·Lucent

CellPipe® 7130

Residential Gateway

6Ve.A4111 & 6Vz.A4111 | Release 01

USER GUIDE

3EQ-10422-AAAA-TCZZA
EDITION 01
FEBRUARY 2011

Conformance statements

The equipment has been tested in the regulation lab and complied with the limits for VDSL device, pursuant to Europe CE/CB, FCC and Canadian. These limits of different regulations are designed provide reasonable protection against harmful interference or damage in a residential installation.

Security statement

In rare instances, unauthorized individuals make connections to the telecommunications network through the use of remote access features. In such an event, applicable tariffs require the customer to pay all network charges for traffic. Alcatel-Lucent cannot be responsible for such charges and will not make any allowance or give any credit for charges that result from unauthorized access.

www.alcatel-lucent.com

About this document

Purpose

This document provides information on the hardware setup, software configuration, and administration necessary to operate the CellPipe 7130 Residential Gateway 6Ve.A4111 and 6Vz.A4111. The 6Vz.A4111 supports HPNA; 6Ve.A4111 does not.

Reason for revision

The following table shows the revision history of this document.

Revision	Date	Reason for reissue
Edition 01	February 2011	First release of this document

Intended audience

This document is intended for users and administrators of the CellPipe 7130 RG 6Ve.A4111 and 6Vz.A4111.

How to use this document

This document introduces the CellPipe 7130 RG 6Ve.A4111 and 6Vz.A4111 hardware, connections, and setup. It also covers the Web configuration interface and provides parameter definitions for the fields on those screens.

Structure of hazard statements

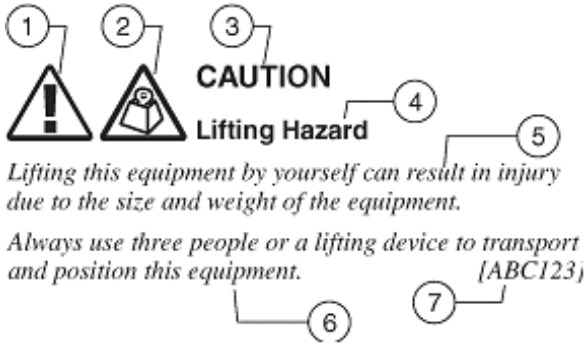
Overview

For the safety of you and your equipment, this document contains hazard statements. Hazard statements are given at points where there may be a risk of damage to personnel, equipment, or operation. Failure to follow the directions in a hazard statement may result in personal harm, equipment damage, or network loss.

General structure

Hazard statements include the structural elements shown in the figure below.

Structure of hazard statements



Item	Structure element	Purpose
1	Personal injury symbol	Indicates the potential for personal injury (optional).
2	Hazard type symbol	Indicates hazard type (optional).
3	Signal word	Indicates the severity of the hazard.
4	Hazard type	Describes the source of the risk of damage or injury.
5	Damage statement	Consequences if protective measures fail.
6	Avoidance message	Protective measures to take to avoid the hazard.
7	Identifier	The reference ID of the hazard statement (optional).

Signal words

The following table defines signal words that identify the hazard severity levels.

Signal words for hazard severity

Signal word	Meaning
DANGER	Indicates an imminently hazardous situation (high risk) which, if not avoided, will result in death or serious injury.
WARNING	Indicates a potentially hazardous situation (medium risk) which, if not avoided, could result in death or serious injury.
CAUTION	*When used with the personal injury symbol:* Indicates a potentially hazardous situation (low risk) which, if not avoided, may result in personal injury. *When used without the personal injury symbol:* Indicates a potentially hazardous situation (low risk) which, if not avoided, may result in property damage, such as service interruption or damage to equipment or other materials.

Related information

The documentation set accompanying this family of routers includes this User Manual and a Quick Installation Guide.

Technical support

For technical support, contact your local Alcatel-Lucent customer support team. See the Alcatel-Lucent Support website for contact information: https://service.esd.alcatel-lucent.com/portal/page/portal/EService/customer_support

Customer Service

If you experience trouble with this telephone equipment, please contact the following address and phone number for information on obtaining service or repairs:

Alcatel-Lucent

600-700 Mountain Avenue

Murray Hill, NJ 07974

1-908-508-8080

Contents

1 Product overview

Overview

Purpose

This chapter provides an introduction to the physical aspects of the CellPipe 7130 RG 6Ve.A4111 and 6Vz.A4111 including safety precautions, prerequisites, and descriptions.

The CellPipe 7130 RG 6Ve.A4111 and 6Vz.A4111 will be referred to as CellPipe 7130 RG throughout the rest of this document.

Contents

This chapter covers the following topics:

Hardware introduction

This CellPipe 7130 RG supports Ethernet-over-VDSL2 using one Ethernet data link that is rated up to 100 Mb/s symmetrically. With its bridge functionality, it can connect to any device equipped with a 10BASE-T or 100BASE-TX network interface card. It supports WAN connection via telephone cable to VDSL switch. It also supports HomePNA, USB storage, VoIP, and wireless local area network. For this purpose, it provides:

- One VDSL port
- Four Ethernet LAN ports (10/100BASE-TX)
- One HPNA interface (Only for 6Vz.A4111)
- Two USB ports
- Wireless (802.11n)
- Two FXS ports

The CellPipe 7130 RG also includes router and firewall functionality.

Safety precautions

Follow these recommendations to protect yourself and the CellPipe 7130 RG from harm:

- Use volume labels to mark the type of power.
- Use the power adapter provided with the CellPipe 7130 RG.
- Pay attention to the power load of the electrical outlet or extension cord. An overburdened power outlet or damaged cords and plugs may cause electric shock or fire. Check the power cords regularly. If you find any damage, replace the cord immediately.
- Leave adequate space for heat dissipation to avoid any damage caused by overheating the CellPipe 7130 RG. Do not cover the ventilation holes.
- Do not put the CellPipe 7130 RG near a heat source. Avoid placing the CellPipe 7130 RG in direct sunlight.
- Do not put the CellPipe 7130 RG in damp or wet locations. Do not spill any liquid on the CellPipe 7130 RG.
- Do not connect the CellPipe 7130 RG to any PC or electronic product unless our customer engineers or your ISP instructs you to do so; incorrect connections may cause fires.
- Do not place the CellPipe 7130 RG on an unstable surface or support.
- Do not place heavy objects on top of the CellPipe 7130 RG.
- Do not use liquid or aerosol cleaners; use a soft, dry cloth for cleaning.

"CAUTION: To reduce the risk of fire, use only No. 26 AWG or larger (e.g., 24 AWG) UL Listed or CSA Certified Telecommunication Line Cord"

"IMPORTANT SAFETY INSTRUCTIONS - When using your telephone equipment, basic safety precautions should always be followed to reduce the risk of fire, electric shock and injury to persons, including the following:

- Do not use this product near water for example, near a bathtub, washbowl, kitchen sink or laundry tub, in a wet basement or near a swimming pool.
- Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
- Do not use the telephone to report a gas leak in the vicinity of the leak.
- Use only the power cord and batteries indicated in this manual. Do not dispose of batteries in a fire. They may explode. Check with local codes for possible special disposal instructions.

SAVE THESE INSTRUCTIONS"

Prerequisites

Ensure that you have the following items before attempting to use the CellPipe 7130 RG:

- Internet services subscription (connection type, account information, and addresses)
- 10/100Base-T Ethernet NIC installed in your PC
- Operating system: Windows 98SE, Windows 2000, Windows NT, Windows ME, Windows XP, Microsoft Vista, Windows 7, or Mac OS
- Internet Explorer v4.0 or higher, Netscape v4.0 or higher, or Mozilla Firefox v1.5 or higher

Note: For optimal display quality, use Internet Explorer v5.0 or Netscape v6.1.

Description of LEDs and interfaces

Figure 1-1 Front panel

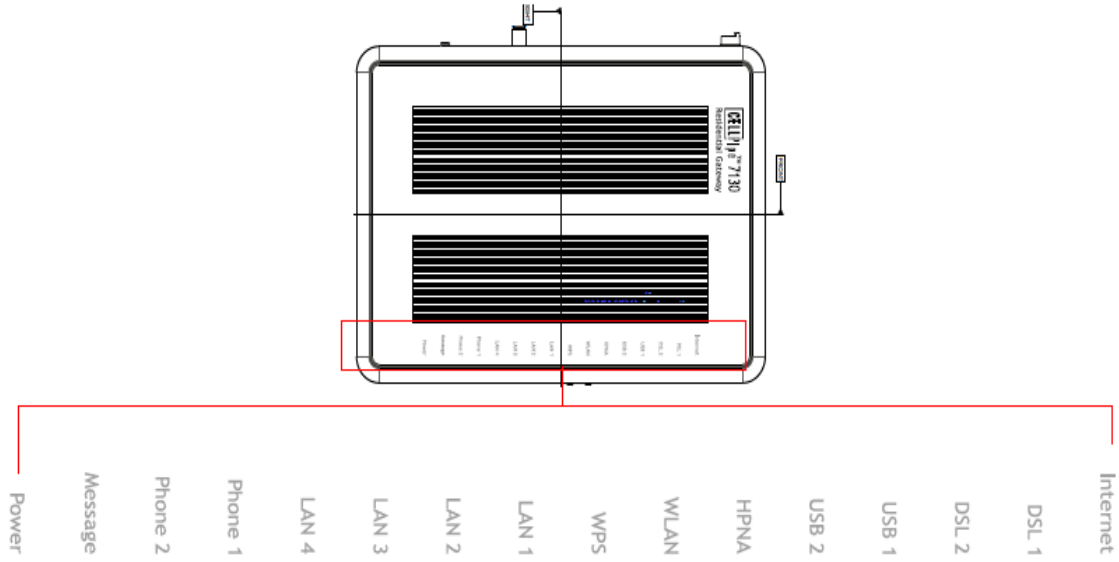


Table 1-1 Front panel LEDs

LED	Status	Description
Internet	On	The CellPipe 7130 RG is connected to the Internet.
	Flashing	Data is being transmitted over the Internet connection.
	Off	The CellPipe 7130 RG is not connected to the Internet.

LED	Status	Description
DSL 1 to 2	On	DSL is operating.
	Flashing	DSL is training.
	Off	DSL is disconnected.
USB 1 to 2	On	A device is connected to the USB port.
	Flashing	USB port has data traffic.
	Off	No device is connected to USB port.
HPNA (Only for 6Vz.A4111)	On	HPNA interface is enabled and connected to a HPNA device.
	Flashing	HPNA traffic is present.
	Off	HPNA interface is disabled or disconnected to any HPNA device.
WLAN	On	Wireless function is enabled.
	Flashing	Data is being transmitted on the wireless link.
	Off	Wireless function is disabled.
WPS	On	WPS is enabled.
	Off	WPS is disabled.
LAN 1 to 4	On	Ethernet LAN port 1 to 4 is connected and active.
	Flashing	Network activity over the corresponding ports.
	Off	Ethernet LAN port 1 to 4 is not active.
Phone 1 to 2	On	Phone 1 to 2 is connected.
	Off	No phones are connected.
Message	Slow flashing*	Firmware upgrade in progress.
	Off	No firmware upgrade in progress.
Power	On	CellPipe 7130 RG is powered on.
	Off	Power is disconnected.

Notes:

* Slow flashing: LED flashes at the rate of 2 seconds on and 2 seconds off.

Figure 1-2 Rear panel of 6Vz.A4111

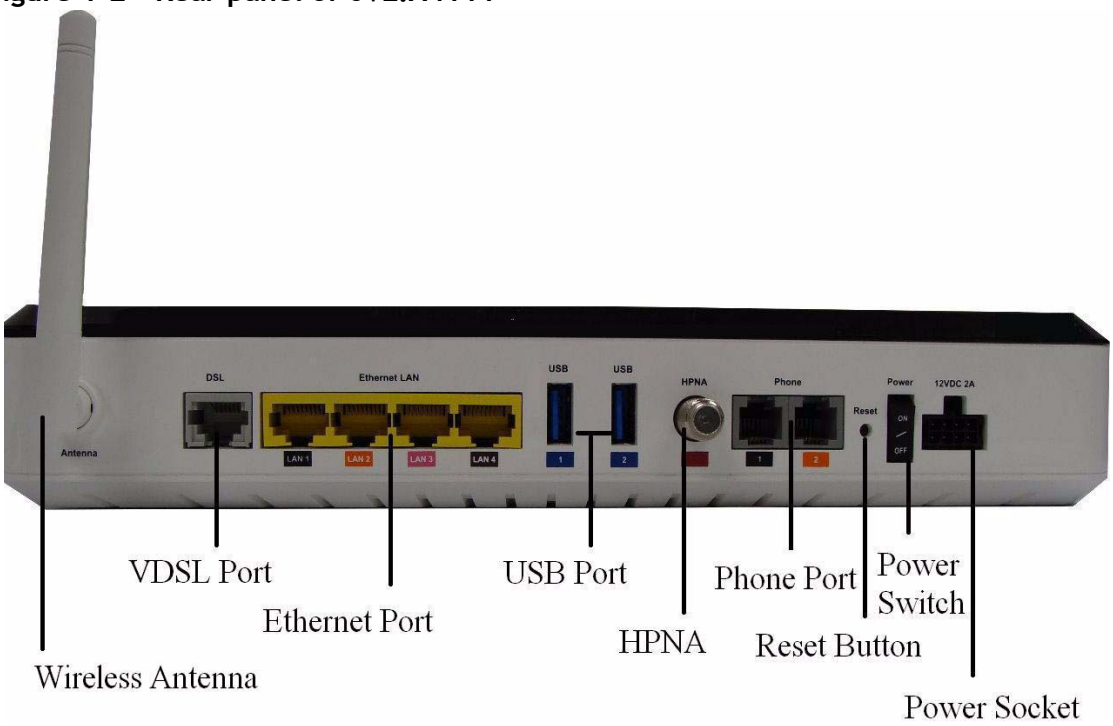


Figure 1-3 Rear panel of 6Ve.A4111

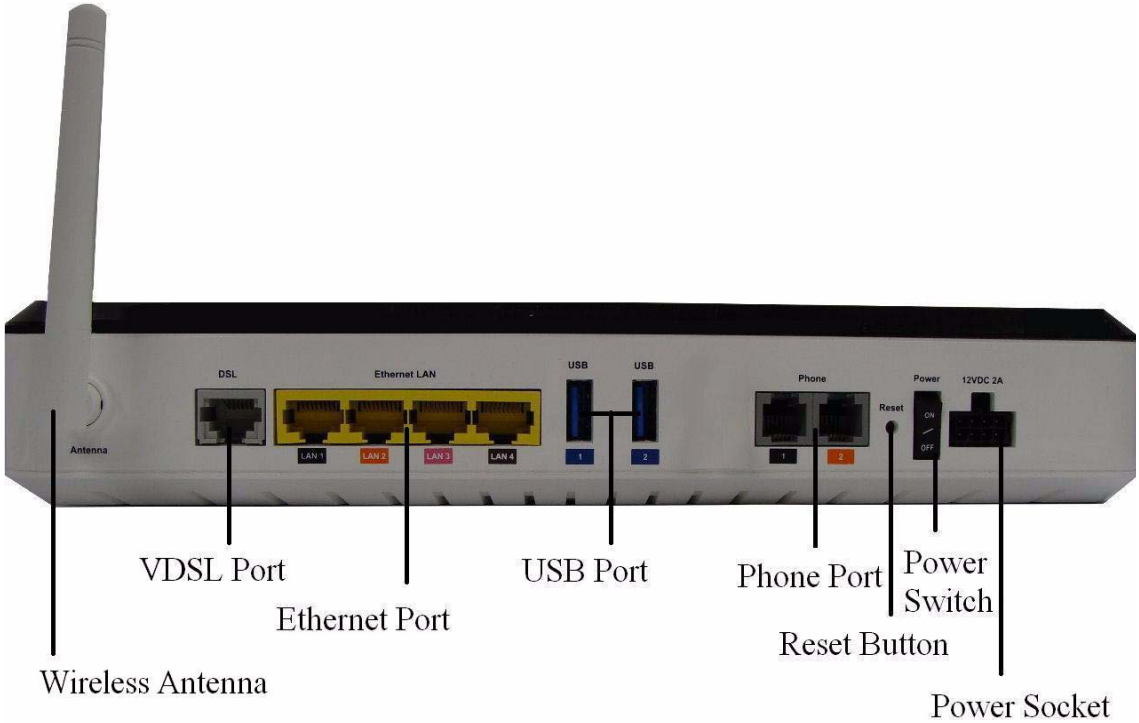


Table 1-2 Rear panel items

Item	Description
Wireless Antenna	Antenna for transmission of wireless signal.

Item	Description
VDSL port	Input port of the VDSL network connection from your ISP. The VDSL port connects to a RJ-11 cable.
Ethernet ports 1 to 4	Four RJ-45 ports to connect up to four PCs or Hub.
USB Port 1 to 2	Support USB 2.0 file sharing and printer server.
HPNA interface (Only for 6Vz.A4111)	One HPNA interface to connect to a HPNA device.
Phone 1/2 ports	Two RJ-11 ports for connecting telephones for VoIP.
Reset button	Press and hold for 10 seconds to restore to factory default settings.
Power switch	Power On/Off switch.
Power socket	DC power adapter port.

2 Hardware installation

Overview

Purpose

This chapter provides the instructions to install the CellPipe 7130 RG hardware.

Contents

This chapter covers the following topic:

Mounting Procedure

There are multiple ways for mounting the CPE:

Wall Mounting

Pre-Requirements

- Anchors
- Screws
- Drill & Drill bit

1. Locate a high position on the wall that is free of obstructions.
2. Connect two screws in the wall 5 cm(2 in.) apart. Do not screw the screws all the way into the wall.

   Important! Make sure that the screws are securely fixed to the wall and strong enough to hold the weight of the CPE. (recommended screw type and size: Nylon wall plug (T8x25mm) and screws (T3.5x16mm)).

3. Align the holes on the back of the CPE with the screws on the wall.

4. Hang up the CPE on the screws.

Desktop Mounting

Place the CPE on top of the desk with the rubber feet standing at the bottom.

Stand-up Mounting

Snap the cradle into the holes located on the side of the CellPipe 7130 RG and then place it on a desk so that LEDs are visible.

To install the CellPipe 7130 RG

Supplies

- CellPipe 7130 RG
- RJ-11 telephone cable
- Two RJ-45 category 5 Ethernet cable
- Power adapter

Before you begin

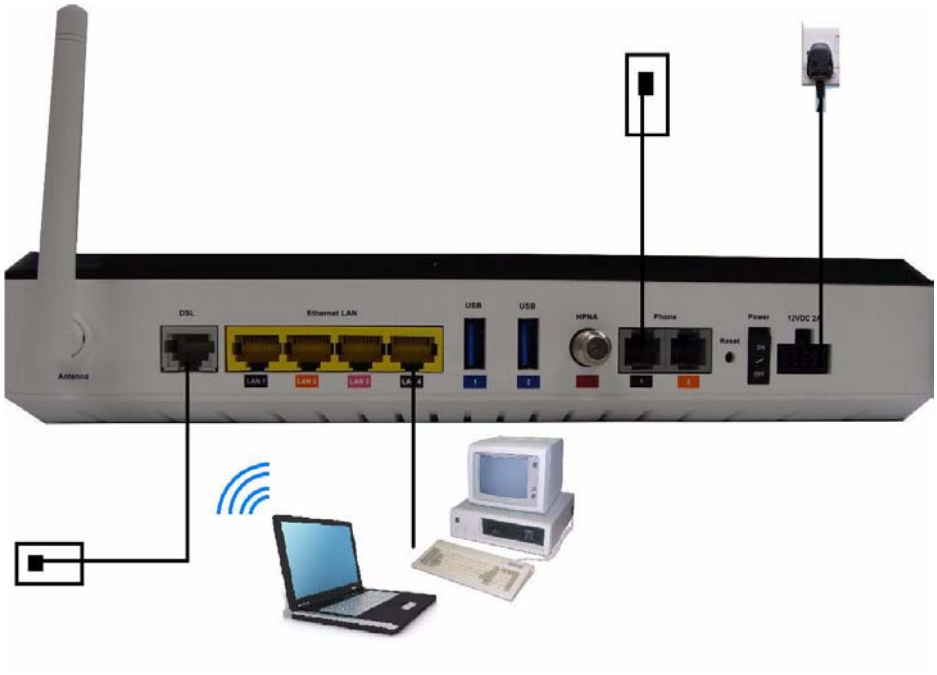
CAUTION

Potential for equipment damage and personal harm

Before installing the CellPipe 7130 RG, ensure you have thoroughly read the Safety precautions and Prerequisites in chapter 1.

Turn off all devices (computer, hub, CellPipe 7130 RG) before beginning this procedure.

Figure 2-1 Cable connections of 6Ve.A4111 & 6Vz.A4111



Procedure

1. Connect the power adapter's cord into the power socket on the back of CellPipe 7130 RG and plug the power adapter into a power source.
2. Connect one end of the RJ-11 cable into the VDSL port on the CellPipe 7130 RG and the other end to your telephone/DSL service connection.
3. Connect one end of the RJ-45 Ethernet cable to one of the Ethernet LAN port (1 to 4) on the CellPipe 7130 RG and the other end to the ethernet port on your device (such as PC, or a hub if your are setting up Intranet).
4. Turn the power switch on.

END OF STEPS

You must also configure the Internet properties on your computer; Please refer to the TCP/IP Appendix or *Quick Installation Guide* for detailed instructions.

After setting up and configuring the CellPipe 7130 RG and your PC(s), you can access the web configuration tool.

3 TCP/IP configuration

Overview

The following procedures provide TCP/IP configuration instructions for all supported operating systems.

Windows 7

1. Open **Network and Internet** from the Control Panel.
2. Open **Network and Sharing Center** from the **Network and Internet**.
3. Right-click **Local Area Connection** from **Network and Sharing Center**.
4. Under the **General** tab, select **Internet Protocol (TCP/IPv4)**, and click Properties.
5. Select the **Obtain an IP address automatically** radio button.
6. Select the **Obtain DNS server address automatically** radio button.
7. Click **OK** to save the settings.

END OF STEPS

Windows Vista

1. Open **Network and sharing Center** from the Control Panel.
2. Open **Manage network connections** from the **Network and sharing Center**.
3. Right-click **Ethernet connection** and select **Properties**.
4. Under the **General** tab, select **Internet Protocol (TCP/IPv4)**, and click **Properties**.
5. Select the **Obtain an IP address automatically** radio button.
6. Select the **Obtain DNS server address automatically** radio button.
7. Click **OK** to save the settings.

END OF STEPS

Windows XP

1. Open **Network Connections** from the Control Panel.
2. Right-click **Ethernet connection** and select **Properties**.

3. Under the **General** tab, select **Internet Protocol (TCP/IP)**, and click **Properties**. The Internet Protocol (TCP/IP) properties window appears.
4. Select the **Obtain an IP address automatically** radio button.
5. Select the **Obtain DNS server address automatically** radio button.
6. Click **OK** to save the settings.

END OF STEPS

Windows Me/2000/98/95

1. Open **Network and Dialing Connections** from the Control Panel.
2. Right click the **Ethernet connection** icon and select **Properties**.
3. Select **Internet Protocol (TCP/IP)** component, and click **Properties**. The Internet Protocol (TCP/IP) properties window appears.
4. Select the **Obtain an IP address automatically** radio button.
5. Select the **Obtain DNS server address automatically** radio button.
6. Click **OK** to save the settings.

END OF STEPS

Windows NT

1. Open **Network** from the Control Panel.
2. From the **Protocol** tab, select the **Internet Protocol (TCP/IP)** component, and click the **Properties** button.
3. From the **IP Address** tab, select the **Obtain an IP address automatically** radio button.
4. From the **DNS** tab, verify that no DNS server is defined in the **DNS Service Search Order** box and no suffix is defined in the **Domain Suffix Search Order** box.

END OF STEPS

Mac OS

1. Open **System Preferences** from the Panel.
2. Choose **Network** from **Internet & Network**.
3. Make sure the window is unlocked. If it is locked, click the lock to make changes and enter the password for authentication.
4. From the **TCP/IP** tab, choose the **Using DHCP** on **Configure IPv4** field.
5. Click on the **Apply Now** button to obtain an IP address from the DHCP server.

END OF STEPS

4 Accessing the CellPipe 7130 RG web configuration tool

Overview

Purpose

This chapter explains how to access the CellPipe 7130 RG web configuration tool by entering the IP address and the default passwords.

The management interface software is HTML-based and can be accessed using a web browser.

Contents

This chapter covers the following topic:

To access the CellPipe 7130 RG web configuration tool

When to use

Use this procedure to access the web configuration interface of the CellPipe 7130 RG. The configuration interface enables you to secure the CellPipe 7130 RG, limit access, set traffic routes, modify passwords, and change advanced settings.

Before you begin

Before you can configure the CellPipe 7130 RG, it must be installed, connected to a web-enabled PC, and turned on.

Management IP settings

To establish the initial connection, either use a computer configured to be a DHCP client, or use a computer with IP settings in the 192.168.2.0 subnet. The IP address of the web configuration is 192.168.2.1 with a subnet mask of 255.255.255.0.

Note: If you are not sure how to configure your computer to be a DHCP client or to set your IP address and subnet mask, please refer to the TCP/IP Appendix or the *Quick Installation Guide* for more information.

Procedure

1. Open a web browser and type in the IP address of the CellPipe 7130 RG in the address bar:

   `http://192.168.2.1` ↵

   The login window appears; see Figure 4-1.

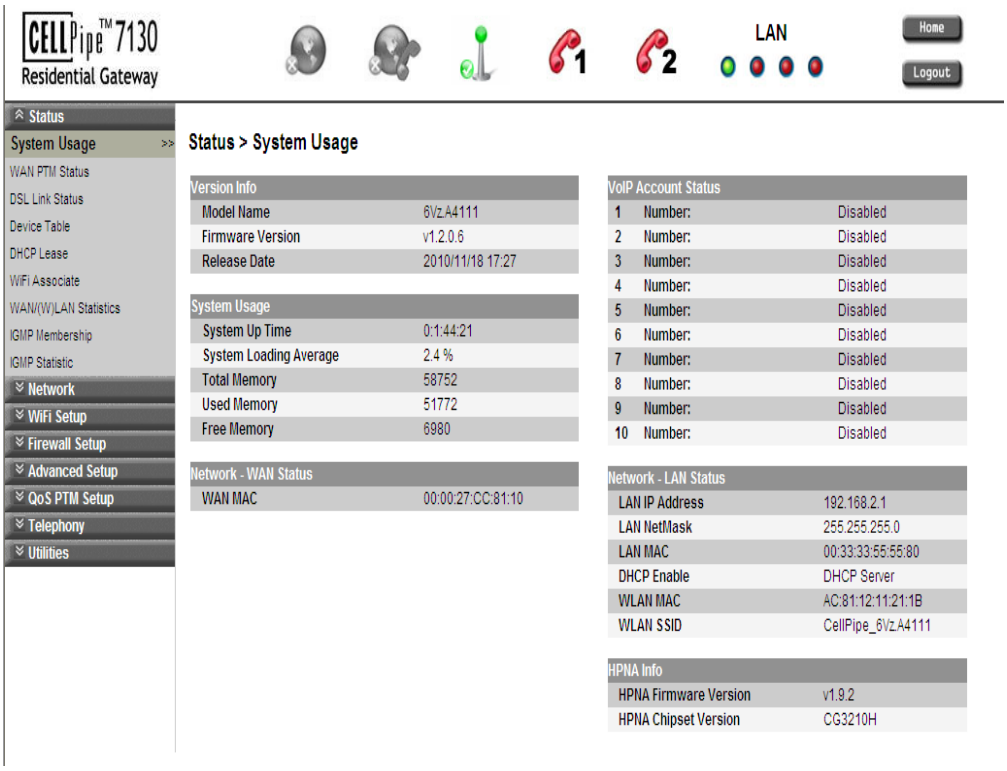
Figure 4-1 Login window

2. Enter your username and password and click **OK**.

   The default admin username is **`admin`** and the default admin password is **`admin`**.

   The Status window appears; see Figure 4-2.

Figure 4-2 Status window



The status window is described in Chapter 5, “Status”.

Note: Once you have logged in for the first time, you should change your login password. See the System Setting section in the Utilities chapter for instructions.

END OF STEPS

Configuration menus

All configuration and management of the CellPipe 7130 RG is done using the web configuration tool. Click on the **Status**, **Network**, **WiFi Setup**, **Firewall Setup**, **Advanced Setup**, **QoS Setup**, **Telephony** and **Utilities** tabs to view the configuration menus or information located in each directory.

5 Status

Overview

Purpose

This chapter describes the contents of the Status menu, which contains the status information for the CellPipe 7130 RG, its connections, and the connected hardware.

Click the **Status** drop-down menu to open the **Status** menu.

Contents

This chapter covers the following topics:

System Usage

The System Usage window displays the current status of the software, system time, memory, WAN connection and LAN connection.

Select **System Usage** in the **Status** menu to access the System Usage window; see Figure 5-1.

Figure 5-1 System Usage window

Status > System Usage

Version Info	
Model Name	6Vz.A4111
Firmware Version	v1.2.0.6
Release Date	2010/11/18 17:27

System Usage	
System Up Time	0:1:45:23
System Loading Average	2.8 %
Total Memory	58752
Used Memory	51768
Free Memory	6984

Network - WAN Status	
WAN MAC	00:00:27:CC:81:10

VoIP Account Status		
1	Number:	Disabled
2	Number:	Disabled
3	Number:	Disabled
4	Number:	Disabled
5	Number:	Disabled
6	Number:	Disabled
7	Number:	Disabled
8	Number:	Disabled
9	Number:	Disabled
10	Number:	Disabled

Network - LAN Status	
LAN IP Address	192.168.2.1
LAN NetMask	255.255.255.0
LAN MAC	00:33:33:55:55:80
DHCP Enable	DHCP Server
WLAN MAC	AC:81:12:11:21:1B
WLAN SSID	CellPipe_6Vz.A4111

HPNA Info	
HPNA Firmware Version	v1.9.2
HPNA Chipset Version	CG3210H

Table 5-1 describes the fields of the System Usage window.

Table 5-1 Field descriptions

Field	Description
Version Info	
Model Name	The model name of the modem.
Firmware Version	The current version of the firmware.
Release Date	The release date of the firmware.
System Usage	
System Up Time	The amount of time the system has been operational.
System Loading Average	The average loading of the system's CPU.
Total Memory	The memory capacity of the system in Kb.
Used Memory	The memory used in the system.
Free Memory	The free memory in the system.
Network - WAN Status	
WAN MAC	The MAC address of the WAN connection.
VoIP Account Status	

Field	Description
1 to 10 Number:	The status (Enabled or Disabled) of accounts 1 to 10.
Network - LAN Status	
LAN IP Address	The IP address of the LAN interface.
LAN NetMask	The subnet mask of the LAN interface.
LAN MAC	The MAC address of the LAN interface.
DHCP Enable	The status of the LAN DHCP.
WLAN MAC	The WLAN MAC address of the WLAN interface.
WLAN SSID	The service set identifier used to identify this gateway.
HPNA Info (Only for 6Vz.A4111)	
HPNA Firmware Version	The current version of the HPNA firmware.
HPNA Chipset Version	The current version of the HPNA chipset.

WAN PTM Status

The WAN Status window displays each WAN connection's name, mode, and connection state. Select **WAN PTM Status** in the **Status** menu to access the WAN Status window; see Figure 5-2.

Figure 5-2 WAN Status window

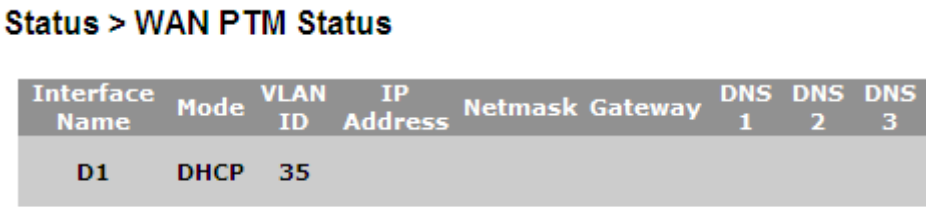


Table 5-2 describes the fields of the WAN Status window.

Table 5-2 Field descriptions

Field	Description
Interface Name	The name you gave to this connection.
Mode	Either DHCP, PPPoE, Static IP or Bridge mode.
VLAN ID	The VLAN ID number (between 2 to 4094).
IP Address	The IP address of this connection.

Field	Description
Netmask	The subnet mask of the IP address.
Gateway	The IP address of gateway.
DNS 1 to 3	The IP address of Domain Name Server.

DSL Link Status

The DSL Link Status window displays the DSL connection status and data.

Select **DSL Link Status** in the **Status** menu to access the DSL Link window; see Figure 5-3.

Figure 5-3 DSL Link Status window

Status > DSL Link Status

Bonding Line Selection Line 0

DSL Firmware Version:	Av4bC032a.d23c			
Mode:				
Traffic Type:				
Status:	Disabled			
Link Power State:	L3			
	Downstream		Upstream	
Line Coding(Trellis):	-		-	
SNR Margin (0.1 dB):	-		-	
Attenuation (0.1 dB):	-		-	
Output Power (0.1 dBm):	-		-	
Attainable Rate (Kbps):	-		-	
	Path 0		Path 1	
	Downstream	Upstream	Downstream	Upstream
Rate (Kbps):	-	-		
MSGc (# of bytes in overhead channel message):				
B (# of bytes in Mux Data Frame):				
M (# of Mux Data Frames in an RS codeword):				
T (# of Mux Data Frames in an OH sub-frame):				
K (number of bytes in DMT frame):				
R :				
S :				
L :				
D (interleaver depth):				
I (interleaver block size in bytes):				
N (RS codeword size):				
Delay (msec):				
INP (DMT symbol):				
OH Frames:				
OH Frame Errors:				
Super Frames:	-	-		
Super Frame Errors:	-	-		
RS Words:	-	-		
RS Correctable Errors:	-	-		
RS Uncorrectable Errors:	-	-		
HEC Errors:	-	-		
OCD Errors:	-	-		
LCD Errors:	-	-		
Total Cells:	-	-		
Data Cells:	-	-		
Bit Errors:	-	-		
Total ES:	-		-	
Total SES:	-		-	
Total UAS:	-		-	

Table 5-3 describes the fields of the DSL Link Status window.

Table 5-3 Field descriptions

Field	Description
DSL Firmware Version	The version of firmware in use.
Mode	The modulation protocol
Traffic Type	The channel type
Status	This is the status of the DSL link.
Link Power State	Displays the power management state of the DSL connection.
Line Coding (Trellis)	The Trellis Coding status of downstream and upstream.
SNR Margin(0.1dB)	This is a signal-to-noise ratio (SNR) margin for traffic going in both directions.
Atternuation(0.1dB)	An estimate of the average loop attenuation downstream and upstream.
Output Power(0.1dBm)	The total output power in both directions.
Attainable Rate (Kbps):	This is the maximum achievable downstream rate.
Rate (Kbps)	The actual rate at which data is flowing in both directions.
MSGc (# of bytes in overhead channel message)	Number of bytes in overhead channel message
B (# of bytes in Mux Data Frame)	Number of bytes in Mux Data Frame
M (# of Mux Data Frames in an RS codeword)	Number of Mux Data Frames in FEC Data Frame
T (# of Mux Data Frames in a OH sub-frame)	Mux Data Frames over sync bytes
K (number of bytes in DMT frame)	This is the number of data bytes in an DSL data frame.
R	The number of redundant check bytes per Reed-Solomon code word.
S	The length of the Reed-Solomon code word, in data frames.
L	Number of bits in PMD Data Frame
D (interleabver depth)	The interleaver depth.
I (interleaver block size in bytes)	Number of bytes in interleaver block size
N (RS codeword size)	The size of RS codeword.
Delay (msec)	The delay, in microseconds, of the DSL connection.

Field	Description
INP (DMT symbol)	INP:Impulse Noise Protection DMT:Discrete Multi-tone
OH Frames	The number of overhead frames.
OH Frame Errors	The number of overhead frame errors.
Super Frames	This is the total number of super frames.
Super Frame Errors	The number of super frames received that had errors.
RS Words	This is the total number of Reed-Solomon code words.
RS Correctable Errors	The number of Reed-Solomon code words with correctable errors.
RS Uncorrectable Errors	The number of R-S code words that had uncorrectable errors.
HEC Errors	The total number of header error checksum errors.
OCD Errors	The number of out-of-cell delineation errors.
LCD Errors	The total of lost-cell-delineation errors.
Total Cells	Total number of cells.
Data Cells	The number of data cells.
Bit Errors	The number of Bit Error.
Total ES	Total number of Errored Seconds.
Total SES	Total number of Severely Errored Seconds.
Total UAS	Total number of Unavailable Seconds.

Device Table

The Device Table displays information about the device that has connected to the CellPipe 7130 RG.

Select **Device Table** in the **Status** menu to access the Device Table; see Figure 5-4.

Figure 5-4 Device Table window

Status > Device Table

Number of Device in your Home Network: 2

Host Name	IP Address	Attached By	MAC Address
user-2098217613	192.168.2.101	Ethernet	20:cf:30:e1:18:f6
UNKNOWN	10.7.206.156	Ethernet	00:24:8c:c4:ac:8b

Table 5-4 describes the fields of the Device Table window.

Table 5-4 Field descriptions

Field	Description
Host Name	The name of the device that has connected to the gateway.
IP Address	The IP address of the device.
Attached By	How the device connected to the gateway.
MAC Address	The MAC address of the device.

DHCP Lease

The DHCP Lease Table lists the IP addresses that are leased to the DHCP clients.

Select **DHCP Lease Table** in the **Status** menu to access the DHCP Lease Table; see Figure 5-5.

Figure 5-5 DHCP Lease window

Status > DHCP Lease

No.	IP Address	MAC Address	Host Name	Vendor	Expiry
1	192.168.2.101	20:cf:30:e1:18:f6	user-2098217613		0Days, 0Hours, 55Min 53Secs

Table 5-5 describes the fields of the DHCP Lease Table window.

Table 5-5 Field descriptions

Field	Description
No.	The number of client.
IP Address	The IP address that is leased to the DHCP client computer.
MAC Address	The MAC address of the DHCP client computer.

Field	Description
Host Name	The host name of the DHCP client computer.
Vendor Class Identifier	The DHCP client platform.
Expiry	The time left before this lease expires.

WiFi Associate

The WiFi Associate Table lists the current wireless clients that have connected to the CellPipe 7130 RG

Select **WiFi Associate** in the **Status** menu to access the WiFi Associate Table; see Figure 5-6.

Figure 5-6 WiFi Associate window

Table 5-6 describes the fields of the WiFi Associate window.

Table 5-6 Field descriptions

Field	Description
No.	The index number of entry in the table.
MAC	The MAC address of the wireless device.
Rate	The transmission rate of the wireless device.

WAN/(W)LAN Statistics

The WAN/(W)LAN Statistics window displays the number of bytes that have been received or transmitted by the WAN, LAN, and WLAN interfaces.

Select **WAN/(W)LAN Statistics** in the **Status** menu to access the Statistics window; see Figure 5-7.

Figure 5-7 WAN/(W)LAN Statistics window

Status > WAN/(W)LAN Statistics

WAN Info	
Rx Bytes	0
Rx Packets	0
Rx Packets - Errored	0
Rx Packets - Dropped	0
Tx Bytes	0
Tx Packets	0
Tx Packets - Errored	0
Tx Packets - Dropped	0
Tx Packets - Collided	0
LAN Info	
Rx Bytes	214890
Rx Packets	1221
Rx Packets - Errored	0
Rx Packets - Dropped	0
Tx Bytes	1079791
Tx Packets	1210
Tx Packets - Errored	0
Tx Packets - Dropped	0
Tx Packets - Collided	0
WLAN Info	
Rx Bytes	0
Rx Packets	0
Rx Packets - Errored	0
Rx Packets - Dropped	0
Tx Bytes	13796
Tx Packets	251
Tx Packets - Errored	0
Tx Packets - Dropped	0
Tx Packets - Collided	0

Table 5-7 describes the WAN, LAN, and WLAN fields of the Statistics window.

Table 5-7 Field descriptions

Field	Description
RX bytes	The number of bytes that have been received.
RX Packets	The number of packets that have been received.
RX Errors	The number of packets that have been received with errors.
RX Dropped	The number of packets that have been dropped after receiving.
TX bytes	The number of bytes that have been transmitted.
TX Packets	The number of packets that have been transmitted.

Field	Description
TX Errors	The number of packets that have been transmitted with errors.
TX Dropped	The number of packets that have been dropped after transmitting.
Collided instead of Collisioned	The number of packets collided when transmitted.

IGMP Membership

The IGMP Membership window displays the IGMP (Internet Group Membership Protocol) members.

Select **IGMP Membership** in the **Status** menu to access the IGMP Membership windows; see Figure 5-8.

Figure 5-8 IGMP Membership window

Table 5-8 describes the IGMP membership window.

Table 5-8 Field descriptions

Field	Description
Multicast IP Group	The respective Multicast Group.
Client	Lists the clients belong to the specific multicast group.

IGMP Statistic

The IGMP Statistic shows the IGMP(Internet Group Membership Protocol) Statistic.

Select **IGMP Statistic** in the **Status** menu to access the IGMP Membership windows; see Figure 5-9.

Figure 5-9 IGMP Statistic window

Table 5-9 describes the IGMP Statistic window.

Table 5-9 Field descriptions

Field	Description
Period	Select a time period form the list to collect and display the IGMP statistics during that period.
Apply	Click to show IGMP Group information.

6 Network

Overview

Purpose

This chapter explains how to configure the network settings for the CellPipe 7130 RG from the Network menu.

Click the **Network** drop-down menu to open the **Network** menu.

Contents

This chapter covers the following topics:

USB

The USB window enables you to configure the USB storage name, USB printer name and DMS.

Select **USB** in the **Network** menu to access the USB&DMS window; see Figure 6-1.

Figure 6-1 USB window

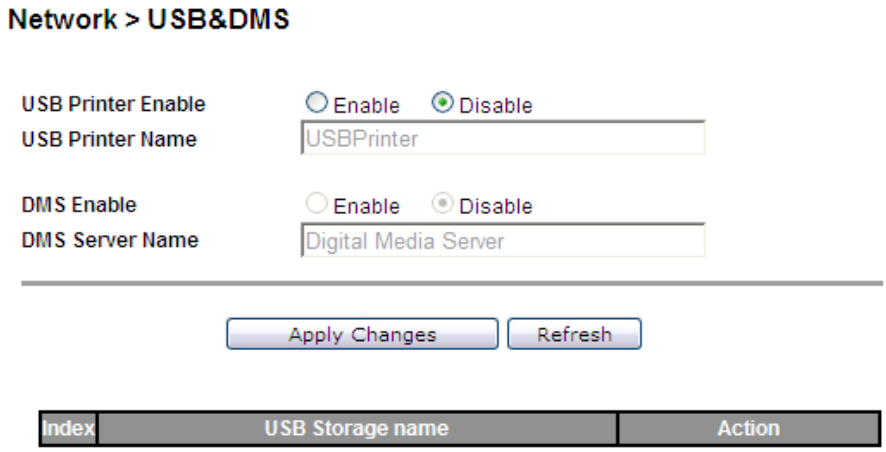


Table 6-1 describes the fields of the USB window.

Table 6-1 Field descriptions

Field	Description
USB Printer Enable	Click the radio button to enable or disable USB Printer.
USB Printer Name	Enter a USB printer name.
DMS Enable	Click the radio button to enable or disable DMS.
DMS Server Name	Enter a DMS Server name.
Apply Changes	Click to save your changes.
Refresh	Click to refresh the state of USB device.

LAN Setting

The LAN Settings include the IP address, subnet mask, DHCP settings, DHCP relay, and static IP lease.

Select **LAN Setting** in the **Network** menu to access the LAN Setting window; see Figure 6-2.

Figure 6-2 LAN Setting window

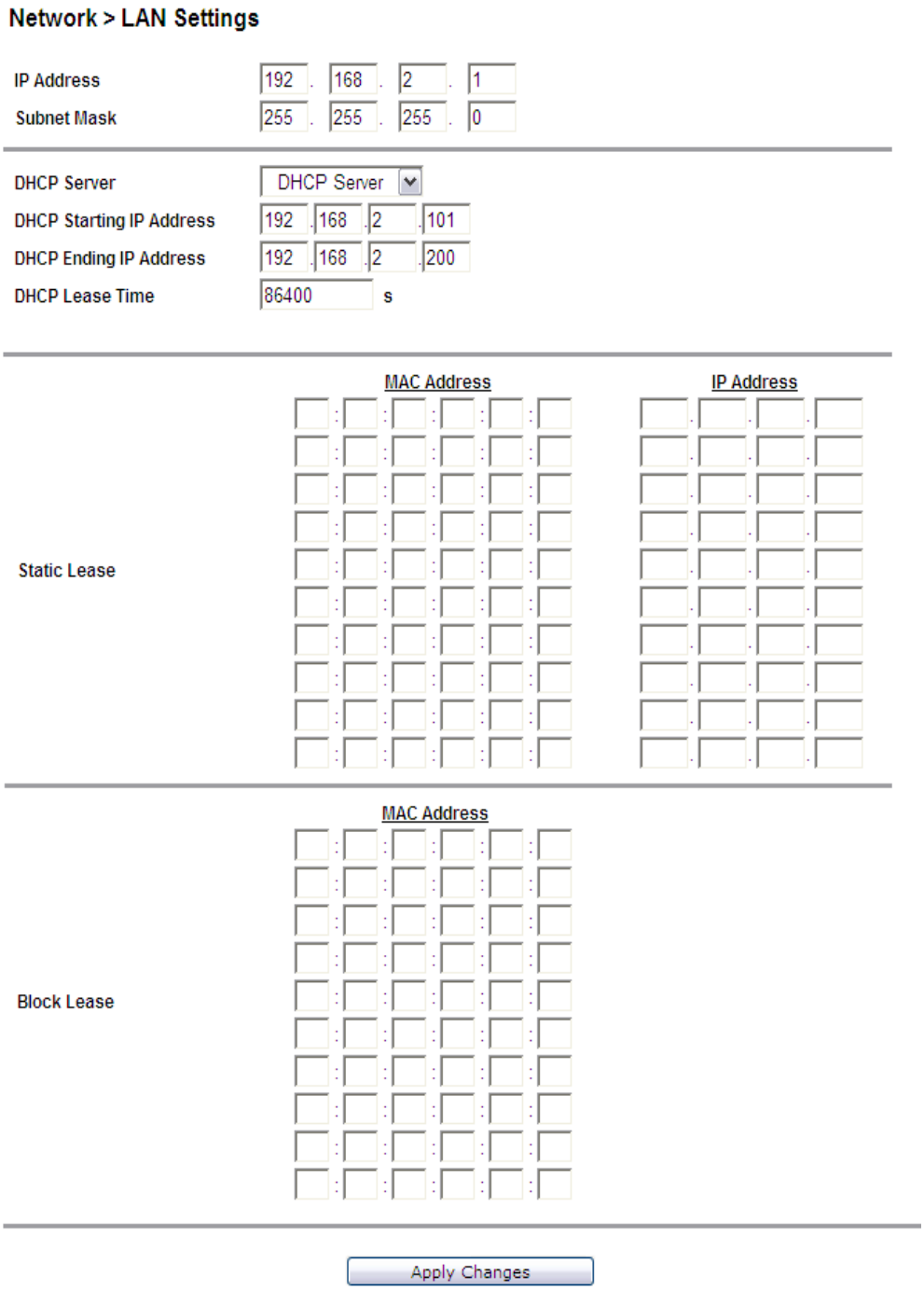


Table 6-2 describes the fields of the LAN Setting window.

Table 6-2 Field descriptions

Field	Description
IP Address	The IP address of the LAN interface in dotted decimal notation. The default is 192.168.2.1. You can change this address as needed to an address that is reserved for private use.

Field	Description
Subnet Mask	The subnet mask of the IP addresses in your LAN; for example, 255.255.255.0.
DHCP Server	If enabled, the CellPipe 7130 RG automatically assigns IP addresses, default gateway, and DNS servers to computers that support the DHCP client; for example, Windows 95, Windows NT.
DHCP Starting IP Address DHCP Ending IP Address	The range of IP addresses that will be assigned to the DHCP client.
DHCP Lease Time	The time period during which the computers retain the IP addresses assigned to them.
Static Lease	Assign a static IP to DHCP clients based on their MAC address.
Block Lease	The client's MAC address to be blocked from acquiring an IP address.
Apply Changes	Click to save your changes.

WAN PTM Connections

WAN PTM Connections are the connections used when the device operates in DSL-PTM mode (if you are uncertain wether your DSL service is PTM, contact your ISP). The WAN PTM Connections window enables you to configure multiple connections.

CAUTION

It is recommended that the WAN PTM connections be changed by trained service personnel. Improper configuration can lead to loss of connectivity to the residential gateway from the LAN side as well as the WAN side.

There are three different binding methods for the connections:

- Port based binding
- MAC based binding
- No LAN/WLAN binding

The four following types of connections can be used:

- Static IP
- DHCP Mode
- PPPoE Mode
- Bridge Mode

Select **WAN PTM Connections** in the **Network** menu to access the WAN PTM Connections window; see Figure 6-3.

Figure 6-3 WAN PTM Connections window

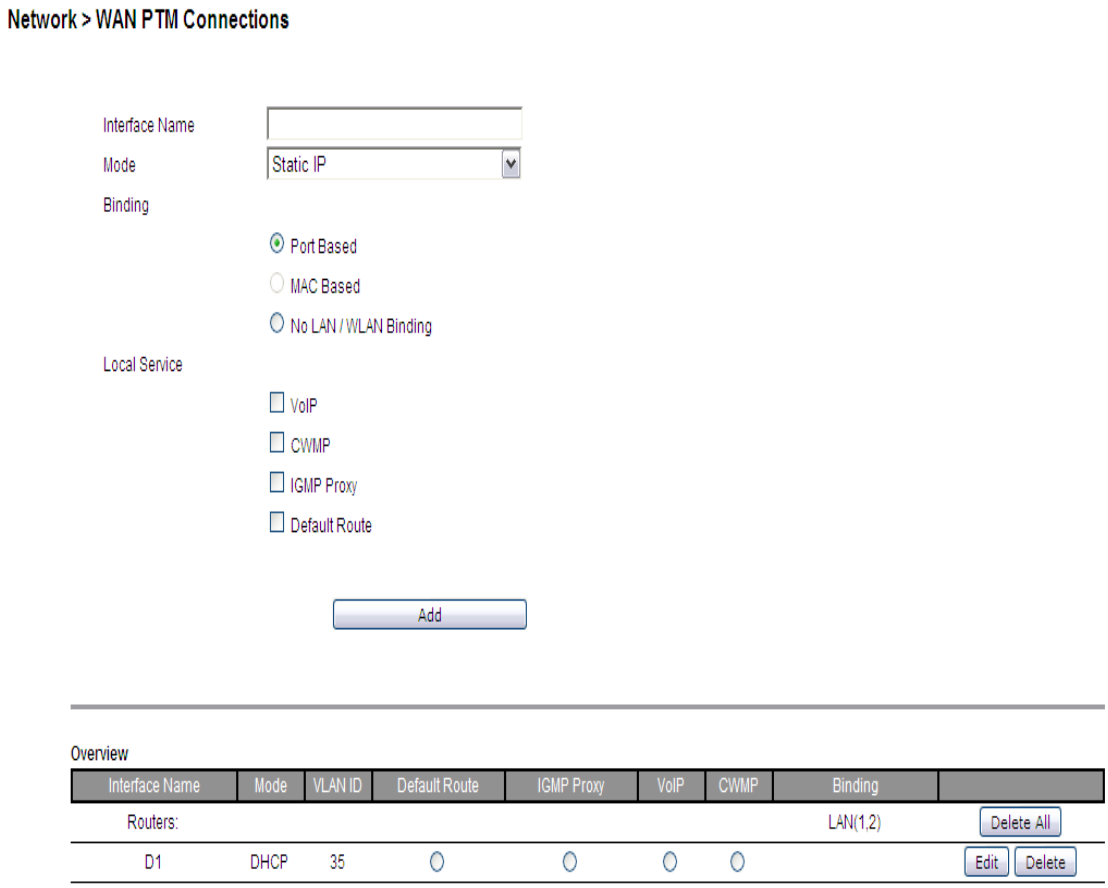


Table 6-3 describes the fields of the WAN PTM Connection window.

Table 6-3 Field descriptions

Field	Description
Interface Name	Enter an appropriate name for your new connection.
Mode	Click the drop-down menu and select either **Static IP**, **DHCP**, **PPPoE**, or **Bridge** as the connection type.
Binding	
Port Based	Bind the interface by LAN or WLAN port
MAC Based	Bind the interface by physical MAC address
No LAN/WLAN Binding	The interface does not bind to any Port or MAC
Local Service	
VoIP	Provide VoIP service to be used.

Field	Description
CMWP (CPE WAN Management Protocol)	Provide remote control service. It will allow remote ACS server to manage this gateway.
IGMP (Internet Group Management Protocol) Proxy	Provide service to be used for video streaming and gaming.
Default Route	Set the connection as the gateway of last resort, every unknown packet will be forwarded via default route.
Add	Click to add the new connection and brings you to next step.
Delete All	Delete all connections below in the table.
Edit	Modify the connection setting.
Delete	Delete the connection.

Port based binding

Port based mode enables you to bind ports to your WAN connection. You can bind LAN ports 1 to 4 and WLAN SSID 1 to 4 in the WAN mode you selected. The default WLAN SSID number is 1 and you can configure 2 to 4 in the **WiFi Setting**.

You can select the **Port Based** radio button for each WAN mode and then click **Add** to proceed to the next configuration window.

In Port based mode, you can add up to four connections in routed mode.

Note: If you do not set a VLAN ID in the connections, you can only have one connection in Static IP or DHCP mode and three connections maximum in PPPoE.

Note: If you already have a connection with Port based binding, you can not select MAC based binding for any other connections.

The following WAN modes support port-based binding:

- Static IP
- DHCP
- PPPoE
- Bridge

Static IP

If you select **Static IP** as the mode in the **WAN PTM Connections**, the Static IP settings window with Port based binding opens; see Figure 6-4.

Figure 6-4 Static IP settings window with Port Based Binding

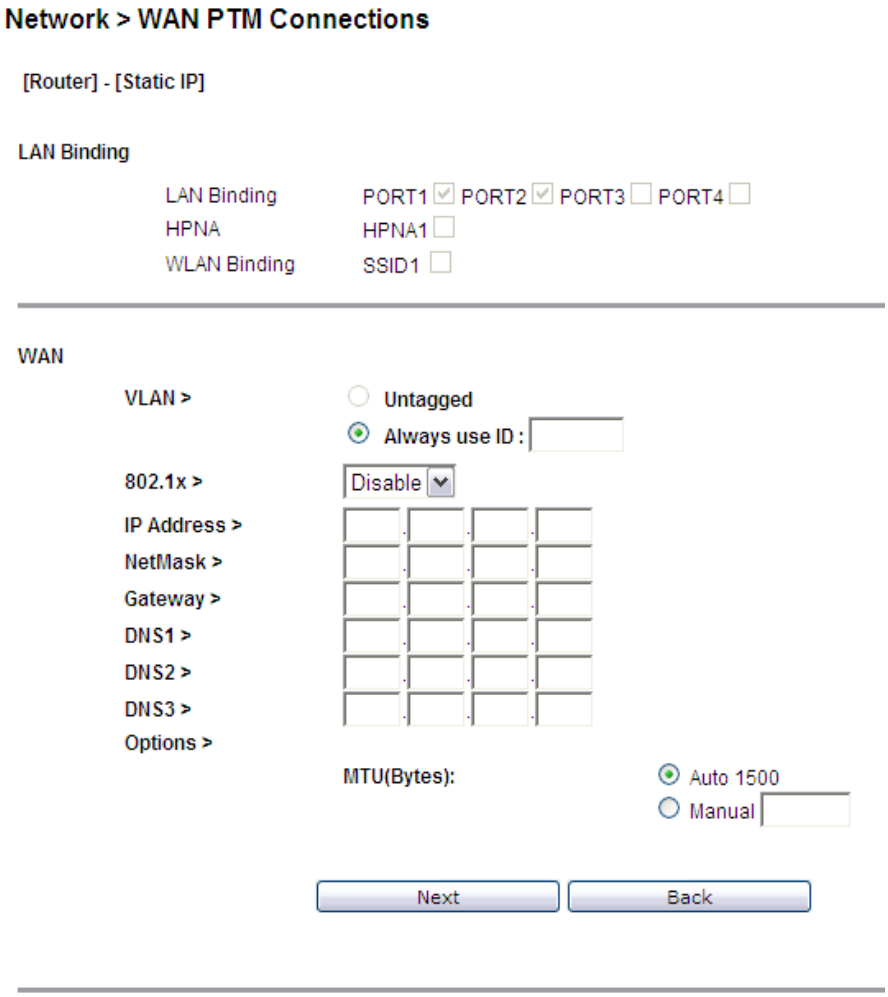


Table 6-4 describes the fields of the Static IP setting window with Port Based Binding.

Table 6-4 Field descriptions

Field	Description
LAN Binding	Select **Lan** port, **HPNA (Only for 6Vz.A4111)** port and **WLAN** port to bind the connection.
Wan	
Untagged	Select this option if VLAN ID is not being used.
Always Use ID	Select this option if VLAN ID is used and enter the VLAN ID number (between 2 and 4094)
IP Address	Enter the IP address provided by your ISP.
NetMask	Enter the subnet mask provided by your ISP.
Gateway	Enter the gateway's IP address provided by your ISP.
DNS1/2/3	Enter the DNS IP address. They are optional.

Field	Description
Options	
MTU	Select **Auto** to set the maximum transfer unit to the default (1500), or select **Manual** to manually enter a value.
Next	Click to go to next step.
Back	Click to go back to previous page.
Activate WAN Settings	Click to activate the connection.
Delete All	Click to remove all WAN connections.
Edit	Click to modify a specific connection.
Delete	Click to remove a specific connection.

DHCP

If you select **DHCP** as the mode in the **WAN PTM Connections** window, the DHCP settings window with Port based binding opens; see Figure 6-5.

Figure 6-5 DHCP settings window with Port Based Binding

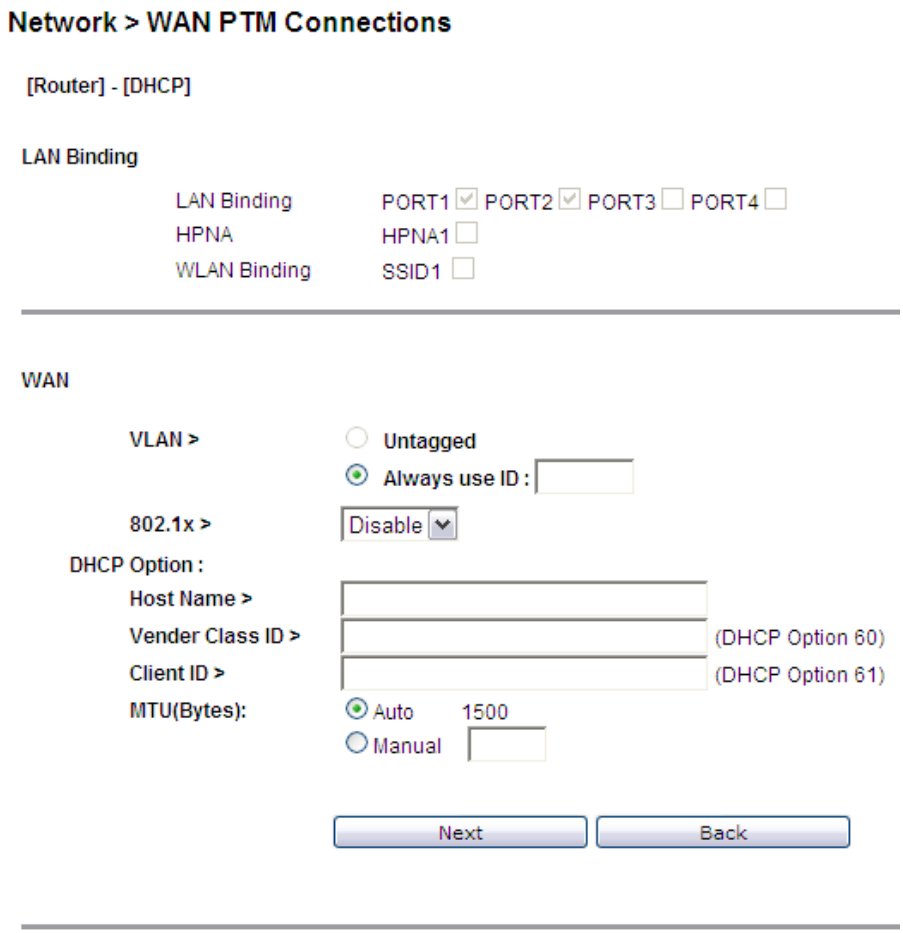


Table 6-5 describes the fields of the DHCP Mode setting window with Port Based Binding.

Table 6-5 Field descriptions

Field	Description
LAN Binding	Select **LAN** port, **HPNA(Only for 6Vz.A4111)** port and **WLAN** port to bind the connection.
WAN	
Untagged	Select this option if VLAN ID is not being used.
Always Use ID	Select this option if VLAN ID is used and enter the VLAN ID number (between 2 and 4094)
802.1x	Select **Enable** to enable 802.1x, or select **Disable** to disable 802.1x. Please consult with your ISP for more information.
DHCP Options	

Field	Description
Host Name Domain Name	Enter the appropriate Host Name and Domain Name provided by your ISP. If you are not sure, please consult with your ISP for more information.
Vender Class ID Client ID	You may also need to set the Client ID or Vender Class ID to obtain its lease from the DHCP server. Please consult with your ISP for more information.
MTU (Bytes)	Enable **Auto** to set the maximum transfer unit to the default (1500), or enable **Manual** to manually enter a value.
Next	Click to go to next step.
Back	Click to go back to preview page.
Activate WAN Settings	Click to activate the connection.
Delete All	Click to remove all WAN connections.
Edit	Click to modify a specific connection.
Delete	Click to remove a specific connection.

PPPoE

If you select **PPPoE** as the mode in the **WAN PTM Connections** window, the PPPoE settings window with Port based binding opens; see Figure 6-6.

Figure 6-6 PPPoE Mode settings window with Port Based Binding

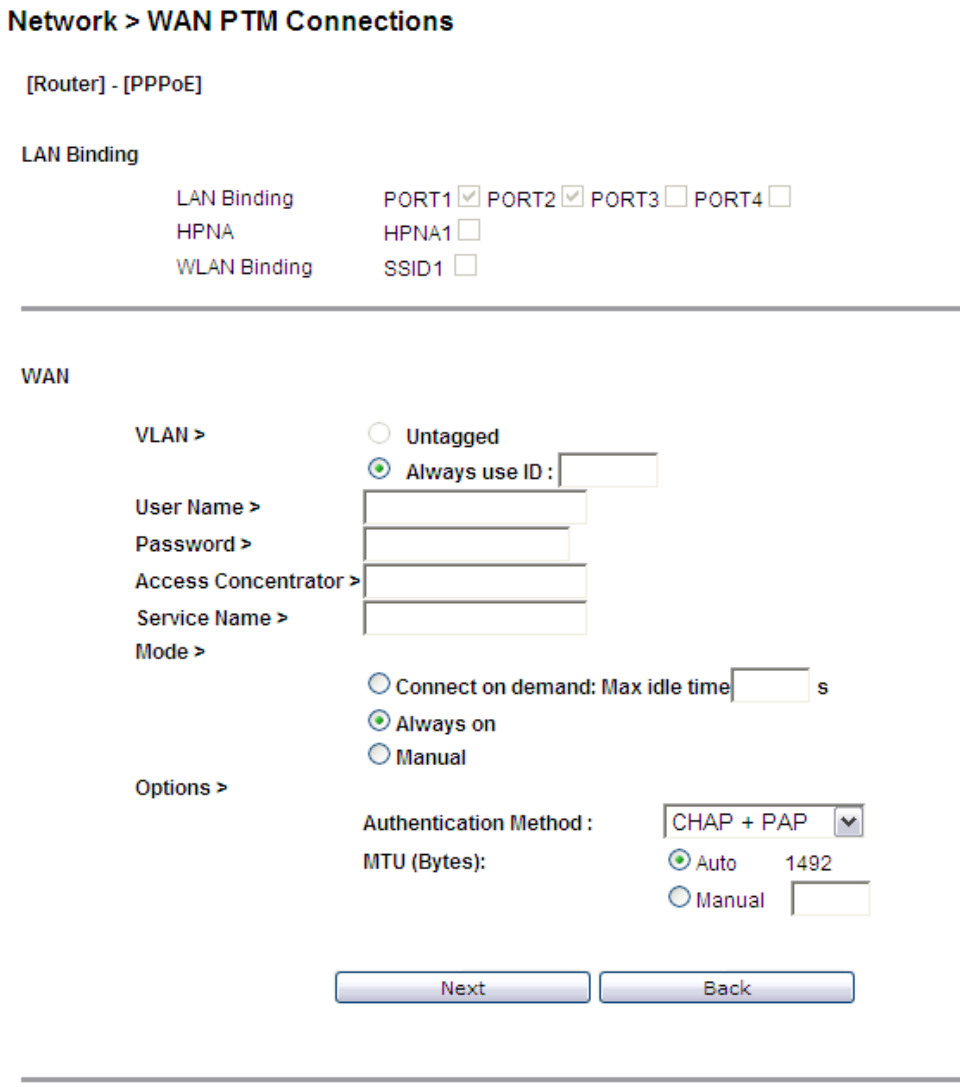


Table 6-6 describes the fields of PPPoE Mode setting window with Port Based Binding.

Table 6-6 Field descriptions

Fields	Description
LAN Binding	Select **LAN** port, **HPNA(Only for 6Vz.A4111)** port and **WLAN** port to bind the connection.
WAN	
Untagged	Select this option if VLAN ID is not being used.
Always use ID	Select this option if VLAN ID is used and enter the VLAN ID number (between 2 and 4094)
User Name	Enter the user name for the PPPoE connection.If you are not sure, please consult with your ISP for more information.

Fields	Description
Password	Enter the password for the PPPoE connection.If you are not sure, please consult with your ISP for more information.
Access Concentrator	The access concentrator is optional. Please consult with your ISP for information.
Service Name	The service name is optional. Please consult with your ISP for information.
Mode	
Connect on demand: Max idle time	Select this option to let the gateway connect to Internet only when your trying to access it. If there are no activities in the specified period (Max idle time), the gateway will disconnect the connection.
Always on	Select this option to let the gateway always connected to the Internet.
Manual	Select and then click **Connect** to manually connect the router to the Internet. Click **Disconnect** to disconnect the connection.
Options	
Authentication Mode	Select the authentication mode from the drop-down menu. Options include: • **CHAP + PAP** • **Only MS-CHAP** • **Only CHAP** • **Only PAP** This is optional. Your ISP will provide this information if it is necessary.
MTU (bytes)	Select **Auto** to set the maximum transfer unit to the default (1492), or enable **Manual** to manually enter a value.
Next	Click to go to next step.
Back	Click to go back to previous page.
Activate WAN Settings	Click to activate the connection.
Delete All	Click to remove all WAN connections.
Edit	Click to modify a specific connection.
Delete	Click to remove a specific connection.

Bridge

If you select **Bridge** as the mode in the **WAN PTM Connections** window, the Bridge settings window with Port based binding opens; see Figure 6-7.

Figure 6-7 Bridge Mode settings window with Port Based binding

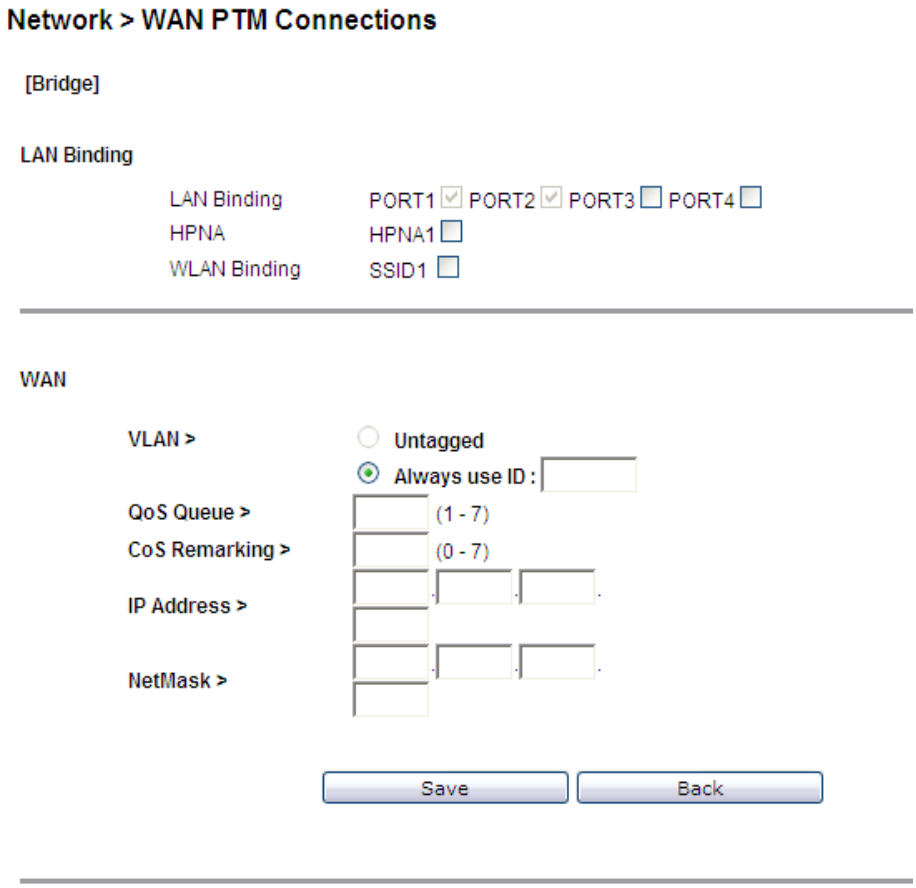


Table 6-7 describes the fields of the Bridge Mode setting window with Port Based binding.

Table 6-7 Field descriptions

Fields	Description
LAN Binding	Select **LAN** port, **HPNA(Only for 6Vz.A4111)** port and **WLAN** port to bind the connection.
WAN	
Untagged	Select this option if VLAN ID is not being used.
Always Use ID	Select this option if VLAN ID is used and enter the VLAN ID number (between 2 and 4094)
QoS Queue	Enter a queue number (0 to 7) to assign to the incoming traffic.
CoS Remarking	Enable **New Cos Value** to assign CoS (class of service) for incoming traffic.
IP Address	Enter the given IP address for your connection.
NetMask	Enter the subnet mask for your connection.
Save	Click to save your setting.

Fields	Description
Back	Click to back preview page.
Activate WAN Settings	Click to activate the connection.
Delete All	Click to remove all WAN connections.
Edit	Click to modify a specific connection.
Delete	Click to remove a specific connection.

MAC based binding

MAC based mode enables you to bind your connection by DHCP Option 60, Ethernet type, source MAC, or destination MAC.

Before you begin, you must configure a default connection. It should be routed or bridge mode. Afterwards you can configure MAC based binding (the other binding options are Port based and No LAN/WLAN) by DHCP Option 60, Ethernet type, source MAC, or destination MAC.

You can select the **MAC Based** radio button for each WAN mode and then click **Add** to enter the next configuration window.

You can set a maximum of 20 connections in MAC based binding.

Note: If you already have a connection with MAC based binding, you cannot select Port based binding for any other connections.

The following section shows the creation of a default DHCP connection with MAC based binding.

DHCP Mode

If you select DHCP as the mode, the DHCP settings window with MAC based binding opens; see Figure 6-8.

Figure 6-8 DHCP settings window

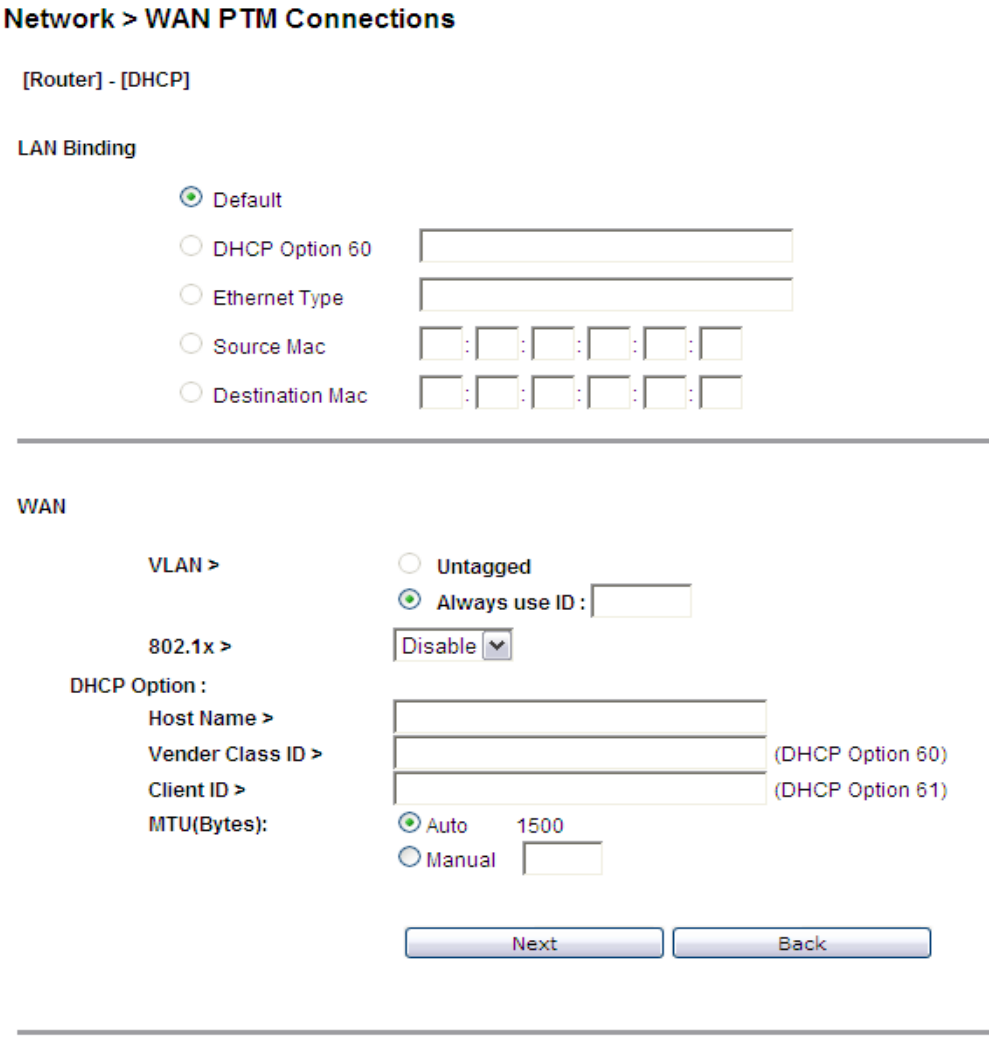


Table 6-8 describes the fields of the DHCP Mode setting window.

Table 6-8 Field descriptions

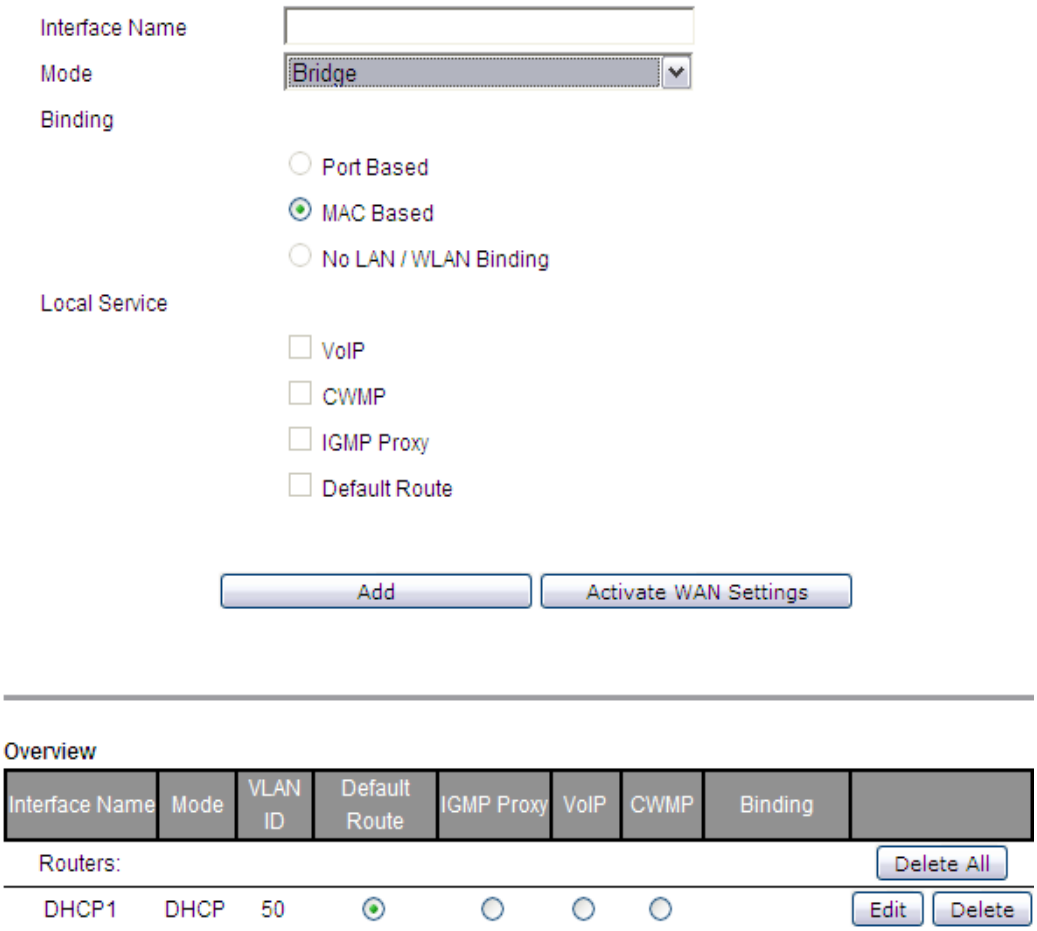
Fields	Description
LAN Binding	
Default	The first rule must be the default. After you have a default rule you can choose the other options. For example, you can select DHCP Option 60, Ethernet Type, Source MAC, or Destination MAC.
DHCP Option 60	Select the radio button and enter the applicable alphanumeric identification (wildcard * is also applicable).
Ethernet Type	Select the radio button and enter the applicable Ethernet Type code (4 hex digits).
Source MAC	Select the radio button and enter the applicable Source MAC address in hexadecimal format.

Fields	Description
Destination MAC	Select the radio button and enter the applicable Destination MAC address in hexadecimal format.
WAN	
VLAN	Select **Untagged** if VLAN tagging is not to be used for this WAN connection. Select **Always use ID** if VLAN tagging is to be used and enter the VLAN ID number (between 0 and 4094).
802.1x	Select **Enable** to use 802.1x or select **Disable** to turn off 802.1x. Please consult your ISP for more information.
Host Name	Enter the host name provided by your ISP. Please consult with your ISP for more information.
Domain Name	Enter the domain name provided by your ISP. Please consult with your ISP for more information.
Vender Class ID	If you are required, set the vender class ID to obtain its lease from the DHCP server. Please consult with your ISP for more information.
Client ID	If you are required, set the client ID to obtain its lease from the DHCP server. Please consult with your ISP for more information.
MTU(Bytes)	Select **Auto** to set the MTU to the default (1500) or select **Manual** and enter a value in bytes.
Next	Click to go to the QoS Defaults window.
Back	Click to return to the previous page.

Now that you have a default connection, the WAN PTM Connections window with MAC based binding opens; see Figure 6-9.

Figure 6-9 WAN PTM Connections window with MAC based binding

Network > WAN PTM Connections



After you have a default connection, you can choose the WAN Mode you want and click **Add** to add a new connection. You can only choose Bridge mode with MAC based binding. Click **Add** to set the configurations.

Bridge Mode

When you select Bridge mode with MAC based binding and click **Add**, the Bridge settings window with MAC based binding opens; see Figure 6-10.

Figure 6-10 Bridge Mode settings window with MAC based binding

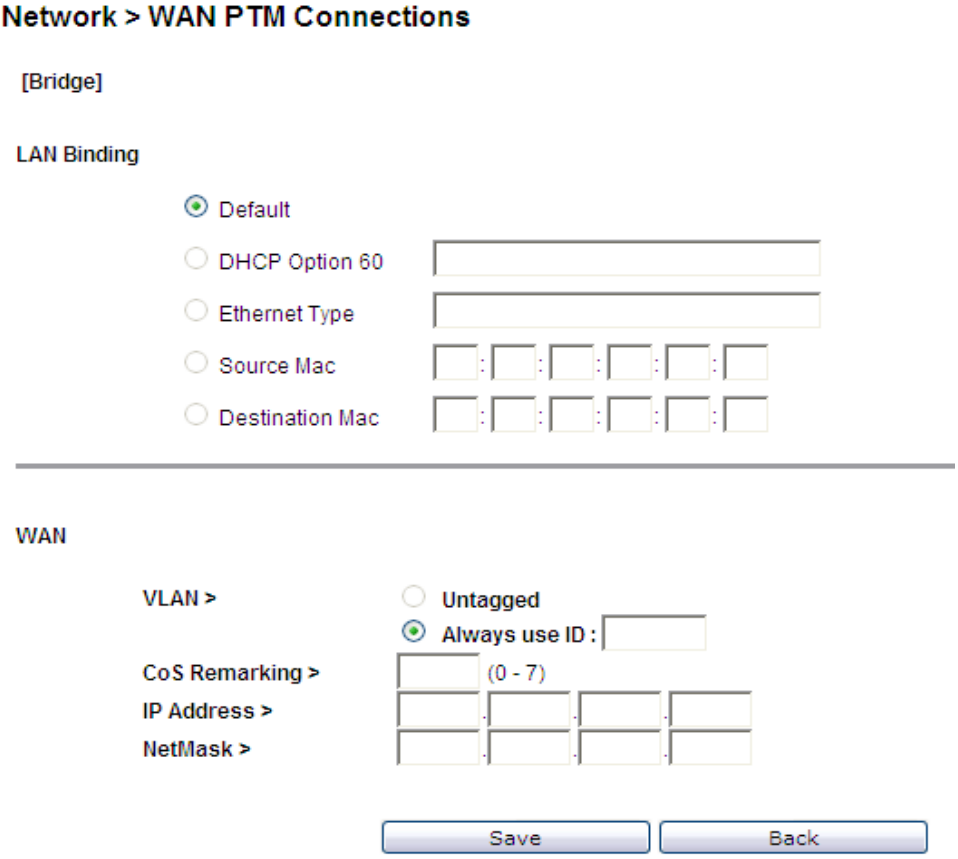


Table 6-9 describes the fields of Bridge Mode setting window with MAC based binding.

Table 6-9 Field descriptions

Fields	Description
LAN Binding	
Default	The first rule must be the default. After you have a default rule you can choose the other options. For example, you can select DHCP Option 60, Ethernet Type, Source MAC, or Destination MAC.
DHCP Option 60	Select the radio button and enter the applicable alphanumeric identification (wildcard * is also applicable).
Ethernet Type	Select the radio button and enter the applicable Ethernet Type code (4 hex digits).
Source MAC	Select the radio button and enter the applicable Source MAC address in hexadecimal format.
Destination MAC	Select the radio button and enter the applicable Destination MAC address in hexadecimal format.
WAN	

Fields	Description
VLAN	Select **Untagged** if VLAN tagging is not to be used for this WAN connection. Select **Always use ID** if VLAN tagging is to be used and enter the VLAN ID number (between 0 and 4094).
CoS Remarking	Enter the CoS remarking number.
IP Address	Enter the IP address provided by your ISP.
NetMask	Enter the subnet mask provided by your ISP.
Next	Click to proceed to the next step.
Back	Click to return to the previous page.

After the second connection is set, you are returned to the WAN PTM Connections window; see Figure 6-11. The two new connections, default and bridged, appear in the Overview table.

Figure 6-11 WAN PTM Connections window with MAC based binding

Network > WAN PTM Connections

Interface Name

Mode: Static IP

Binding

- Port Based
- MAC Based
- No LAN / WLAN Binding

Local Service

- VoIP
- CWMP
- IGMP Proxy
- Default Route

Add | Activate WAN Settings

Overview

Interface Name	Mode	VLAN ID	Default Route	IGMP Proxy	VoIP	CWMP	Binding	
Routers:								Delete All
DHCP1	DHCP	50	◉	○	○	○		Edit Delete
Bridge1	Bridges	36					Destination Mac 00:26:18:37:bb:fd	Edit Delete

You can only choose Bridge mode with MAC based binding and you can select Static IP, DHCP, or PPPoE with No LAN/WLAN Binding for CWMP and VoIP.

No LAN/WLAN binding

No LAN/WLAN binding enables you to configure your connection with local service CWMP and VoIP. In order to avoid other connections using CWMP and VoIP, No LAN/WLAN Binding is specifically for CWMP and VoIP to build an independent connection.

Select the **No LAN/WLAN Binding** radio button for the binding method and then click **Add** to enter the next configuration page.

Static IP

If you select **Static IP** as the mode and click **Add**, the Static IP window with No LAN/WLAN Binding opens; see Figure 6-12.

Figure 6-12 Static IP settings window with No LAN/WLAN Binding

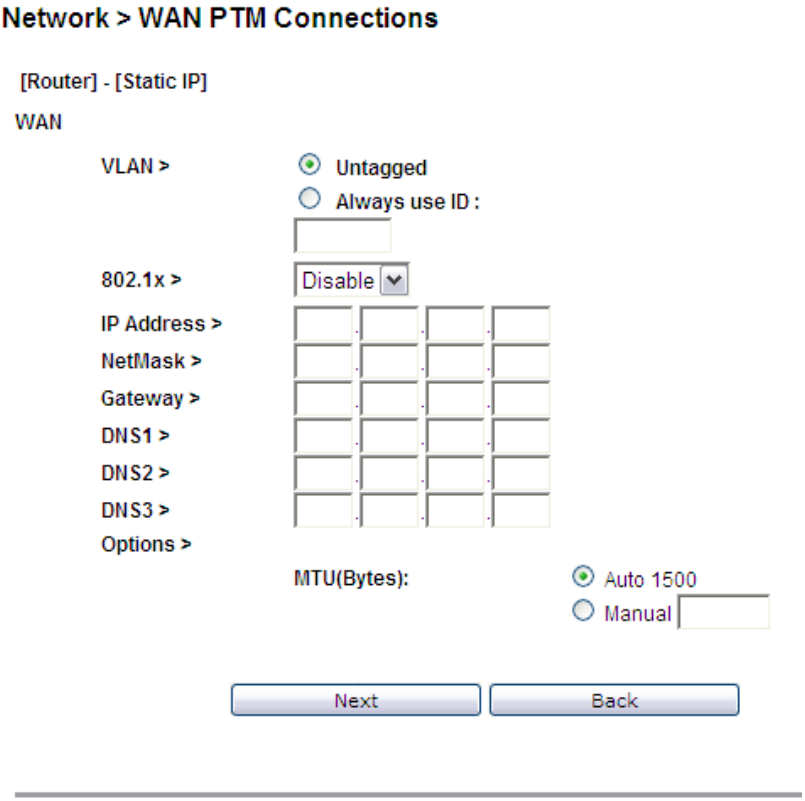


Table 6-10 describes the fields of Static IP setting window with No LAN/WLAN Binding.

Table 6-10 Field descriptions

Field	Description
WAN	
Untagged	Select this option if VLAN ID is not being used.
Always Use ID	Select this option if VLAN ID is used and enter the VLAN ID number (between 2 and 4094)
IP Address	Enter the IP address provided by your ISP.
NetMask	Enter the subnet mask provided by your ISP.
Gateway	Enter the gateway's IP address provided by your ISP.
DNS1/2/3	Enter the DNS IP address. They are optional
Options	
MTU	Select **Auto** to set the maximum transfer unit to the default (1500), or select **Manual** to manually enter a value.
Next	Click to go to next step.
Back	Click to go back to previous page.

DHCP Mode

If you select **DHCP** as the mode and click Add, the DHCP window with No LAN/WLAN Binding opens; see Figure 6-13.

Figure 6-13 DHCP settings window with No LAN/WLAN Binding

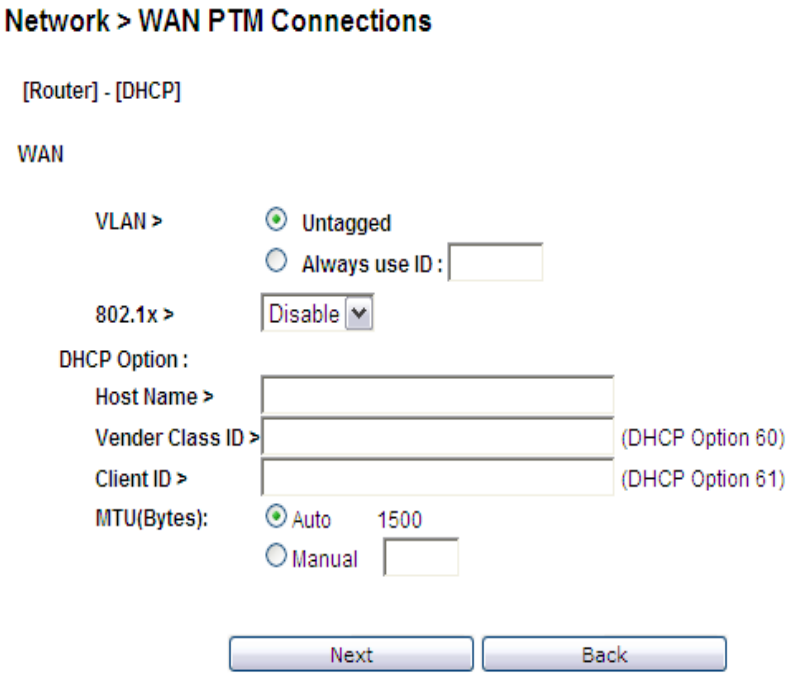


Table 6-11 describes the fields of DHCP Mode setting window with No LAN/WLAN binding.

Table 6-11 Field descriptions

Field	Description
WAN	
Untagged	Select this option if VLAN ID is not being used.
Always Use ID	Select this option if VLAN ID is used and enter the VLAN ID number (between 2 and 4094)
802.1x	Select **Enable** to enable 802.1x, or select **Disable** to disable 802.1x. Please consult with your ISP for more information.
DHCP Options	
Host Name Domain Name	Enter the appropriate Host Name and Domain Name provided by your ISP. If you are not sure, please consult with your ISP for more information.
Vender Class ID Client ID	You may also need to set the Client ID or Vender Class ID to obtain its lease from the DHCP server. Please consult with your ISP for more information.

Field	Description
MTU (Bytes)	Enable **Auto** to set the maximum transfer unit to the default (1500), or enable **Manual** to manually enter a value.
Next	Click to go to next step.
Back	Click to go back to preview page.

PPPoE Mode

If you select **DHCP** as the mode and click Add, the DHCP window with No LAN/WLAN Binding opens; see Figure 6-14.

Figure 6-14 PPPoE Mode settings window with No LAN/WLAN Binding

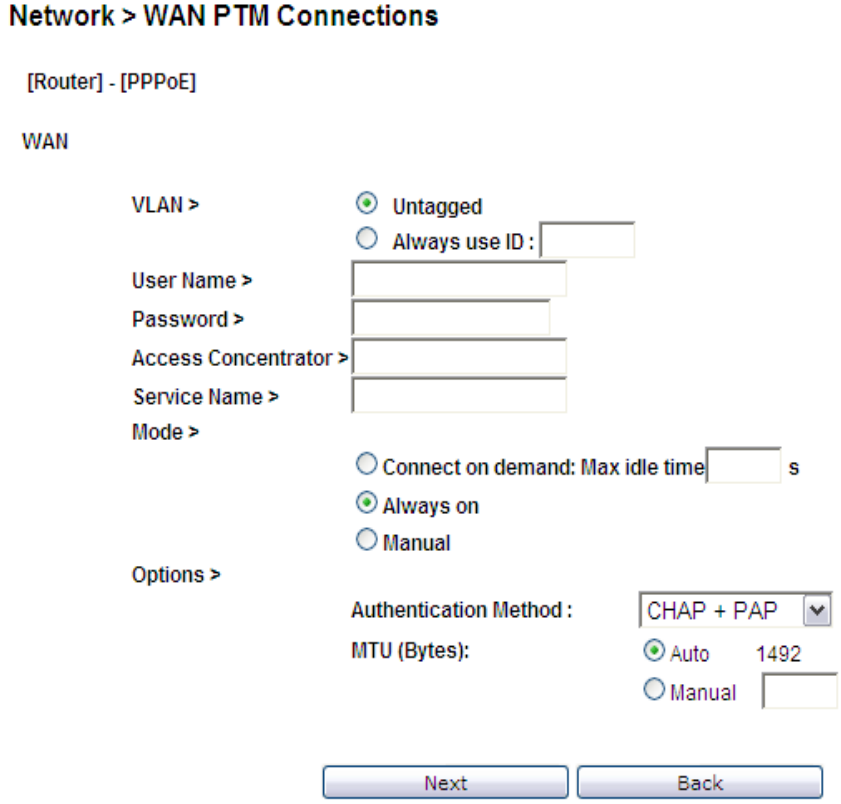


Table 6-12 describes the fields of PPPoE Mode setting window with No LAN/WLAN Binding.

Table 6-12 Field descriptions

Fields	Description
Wan	

Fields	Description
Untagged	Select this option if VLAN ID is not being used.
Always use ID	Select this option if VLAN ID is used and enter the VLAN ID number (between 2 and 4094)
User Name	Enter the user name for the PPPoE connection.If you are not sure, please consult with your ISP for more information.
Password	Enter the password for the PPPoE connection.If you are not sure, please consult with your ISP for more information.
Access Concentrator	The access concentrator is optional. Please consult with your ISP for information.
Service Name	The service name is optional. Please consult with your ISP for information.
Mode	
Connect on demand: Max idle time	Select this option to let the gateway connect to Internet only when your trying to access it. If there are no activities in the specified period (Max idle time), gateway will disconnect the connection.
Always on	Select this option to let the gateway always connected to the Internet.
Manual	Select and then click **Connect** to manually connect the router to the Internet. Click **Disconnect** to disconnect the connection.
Options	
Authentication Mode	Select the authentication mode from the drop-down menu. Options include: • **CHAP + PAP** • **Only MS-CHAP** • **Only CHAP** • **Only PAP** This is optional. Your ISP will provide this information if it is necessary.
MTU (bytes)	Select **Auto** to set the maximum transfer unit to the default (1492), or enable **Manual** to manually enter a value.
Next	Click to go to next step.
Back	Click to go back to previous page.

QoS Defaults

The QoS Defaults window enables you to configure the default QoS policy for each WAN connection, see Figure 6-15.

Figure 6-15 QoS Defaults window

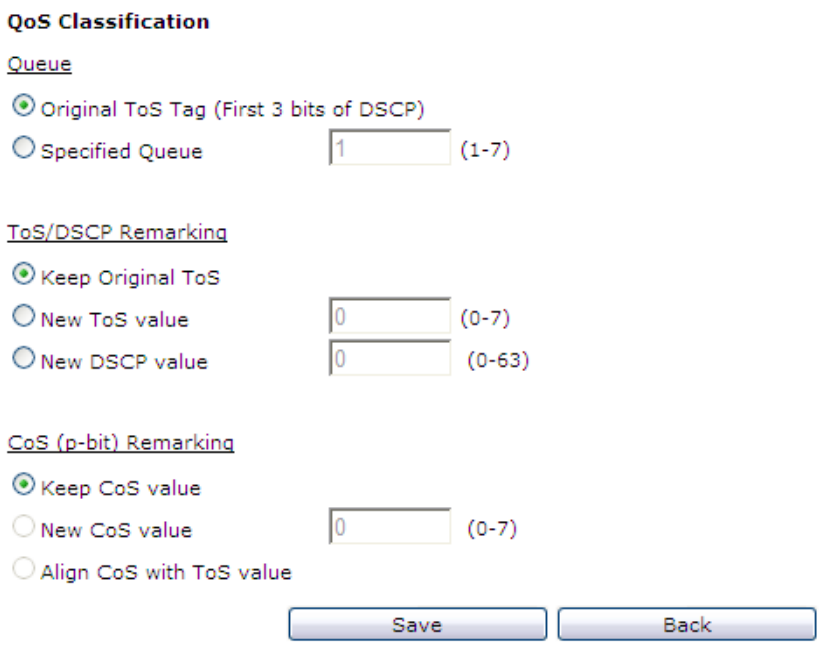


Table 6-13 describes the fields of the QoS Defaults window.

Table 6-13 Field descriptions

Field	Description
QoS Classification	
Queue	
Original ToS Tag (First 3 bits of DSCP)	Select **Original ToS Tag** to assign the queue according to the ToS value of the packet.
Specified Queue	Select **Specified Queue** and enter a queue number (0 to 7) to which the network traffic will be assigned. **Note:** When **Specified Queue** is chosen, you cannot choose **Align CoS with ToS Value**.
ToS/DSCP Remarking	
Keep Original ToS	Select **Keep Original ToS** to retain the original ToS value.

Field	Description
New ToS Value	Select **New Tos Value** and enter a queue number (0 to 7) to assign to the network traffic.
New DSCP Value	Select **New DSCP Value** and enter a DSCP value (0 to 63).
CoS (p-bit) Remarking	
Keep CoS Value	Select **Keep CoS Value** to retain the original CoS value.
New CoS Value	Select **New CoS Value** to assign CoS for network traffic.
Align CoS with ToS Value	Select to align CoS with ToS value. **Note:** This field can only be set if you keep **Original ToS Tag** in queue setting.
Save	Click to save your changes.
Back	Click to return to the previous window.

7 WiFi Setup

Overview

Purpose

This chapter explains how to configure the WiFi settings for the CellPipe 7130 RG from the WiFi setup menu.

Click the **WiFi Setup** drop-down menu to open the **WiFi Setup** menu.

Contents

This chapter covers the following topics:

WiFi Setting

The WiFi Setting window enables you to configure the common wireless and SSID settings.

Click on **WiFi Setting** in the **WiFi Setup** menu to access the WiFi Setting window; see Figure 7-1.

Figure 7-1 WiFi Setting window

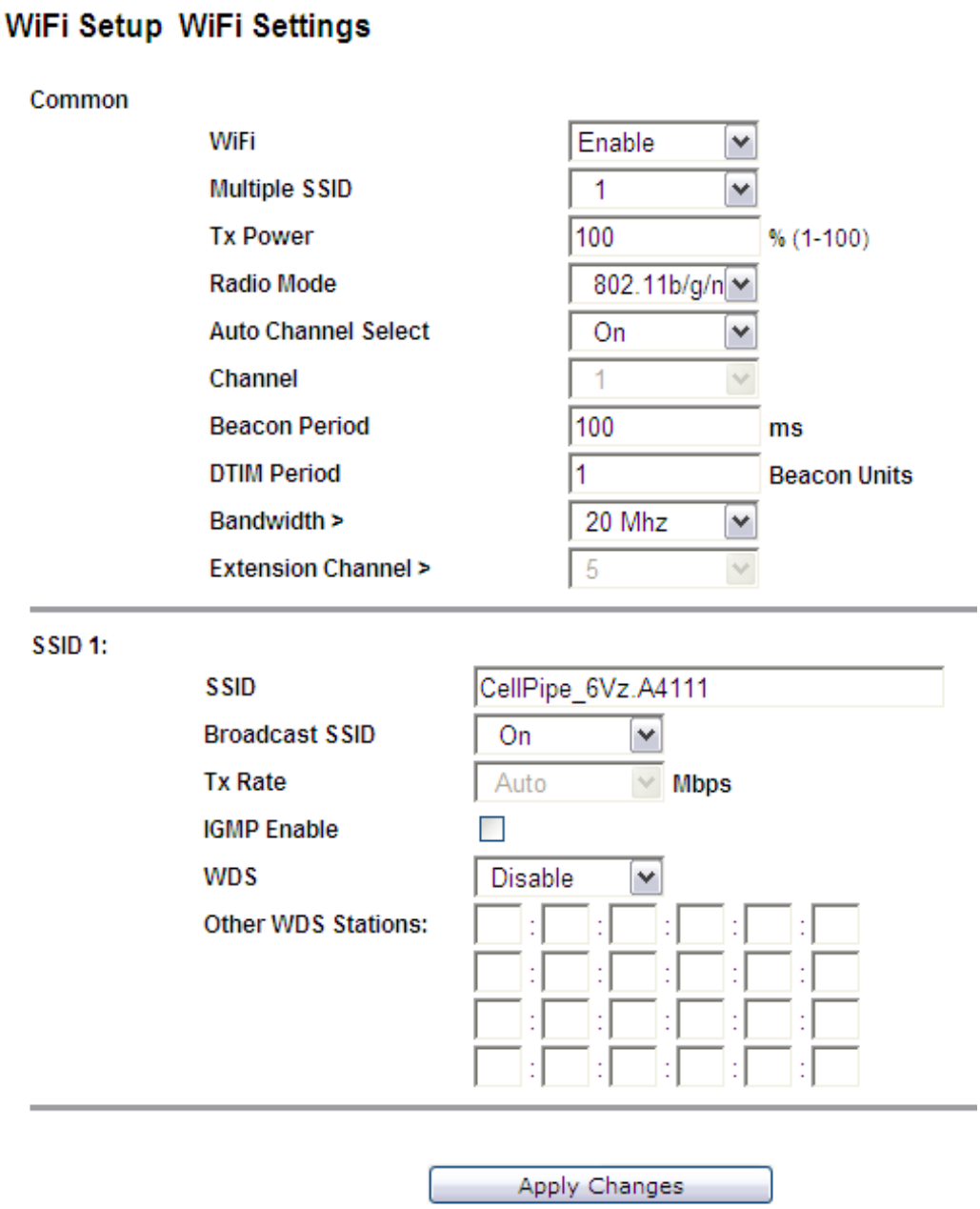


Table 7-1 describes the fields of the WiFi Setting window.

Table 7-1 Field descriptions

Field	Description
Common	
WiFi	Select **Enable** to turn wireless on and configure the wireless settings. Or select **Disable** to turn wireless off.
Multiple SSID	Click the drop-down menu and select either **1**, **2**, or **4** for multiple SSIDs.

Field	Description
Tx Power	Enter a value between 1~100 to control the level of transmitting signal strength.
Radio Mode	Click the drop-down menu and select either **b/g/n, b/g, g/n**, **b**, **g** or **n** for the wireless mode.
Auto Channel Select	Click the drop-down menu and select **On** to let the wireless access point automatically select a channel with the least interference. Select **Off** to configure manually. Select **Now** to set the channel automatically once.
Channel	If auto channel select is off, you can manually select a channel for the wireless access point. The default is 1.
Beacon Period	Enter a beacon period in ms to determine the frequency of the beacon to keep the network synchronized. This is optional.
DTIM Period	Enter a value to set the delivery traffic indication message. The DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages.
Bandwidth	Click the drop-down menu and select either **20/40Mhz** or **20Mhz** as the transmitting frequency for 802.11n. Select **20/40Mhz** can provide double the data transmitting rate of **20Mhz**.
Extension Channel	802.11n will create an extension channel to transmit data. Select a channel from the drop-down menu to use as the extension channel.
SSID 1 to 4	
SSID	Enter a SSID name (Maximum of 32 characters). The SSID is an alphanumeric name shared by all the devices on the wireless network. It must be unique.
Broadcast SSID	Click the drop-down menu and select **On** to broadcast the SSID or **Off** to hide your SSID.
Tx Rate	Click the drop-down menu and select **Auto** to automatically determine the transmission rate or select a transmission rate (Max. 54Mbps).
IGMP Enable	Enable to use IGMP or disable to turn off IGMP.
WDS[1]	Click the drop-down menu and select **Enable** if you would like to enter the wireless MAC of other wireless access points or routers that are in the same WDS.
Other WDS Stations	Enter the wireless MAC addresses of other wireless APs or routers that are in the same WDS.
Apply Changes	Click to save your changes.

Notes:

1 If you enable WDS, check that all other WDS APs are enabled, configured with the same channel, SSID, and encryption keys, and that each AP has a different LAN port IP address.

WiFi Security

WiFi security enables you to configure the WEP, WPA, or WPA2 security settings.

Select **WiFi Security** in the **WiFi Setup** menu to access the WiFi security window; see Figure 7-2.

Figure 7-2 WiFi Security window

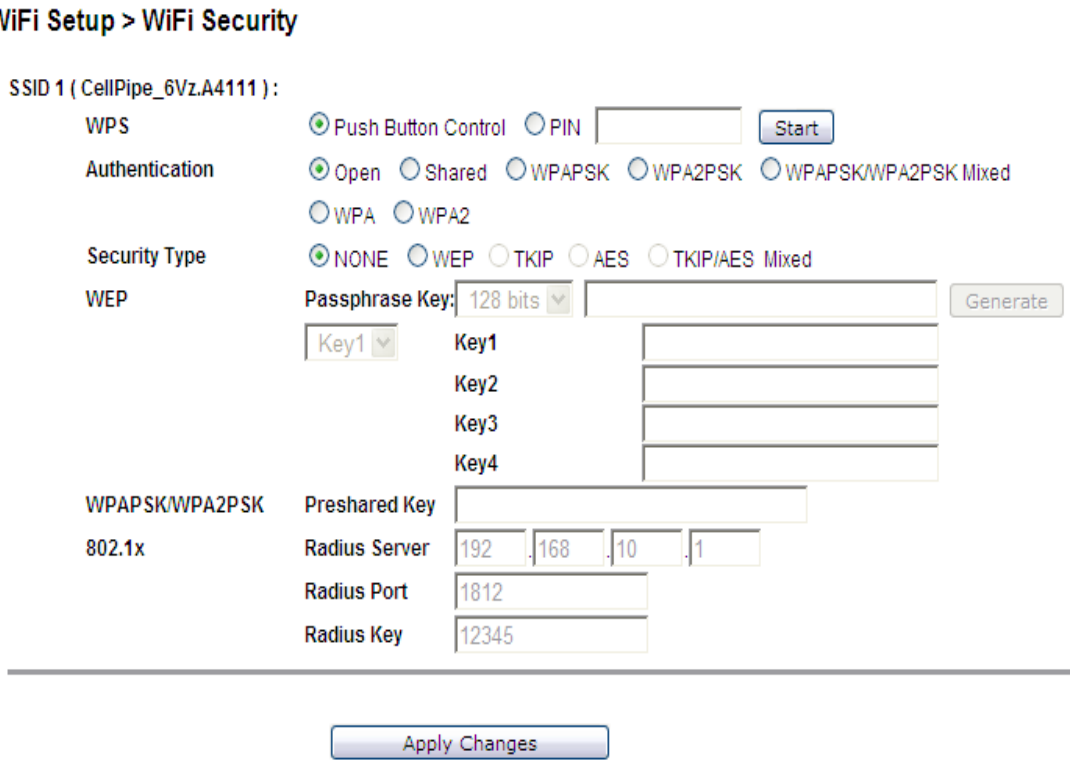


Table 7-2 describes the fields of the WiFi Security settings window.

Table 7-2 Field descriptions

Field	Description
WPS	Enable **Push Button Control** or enable **PIN** and enter your PIN number and click **Start**.

Field	Description
Authentication	Select one of the following encryption methods for the wireless network: • **Open** • **Shared** • **WPAPSK** • **WPA2PSK** • **WPAPSK/WPA2PSK Mixed** • **WPA** • **WPA2**
Security Type	Select one of the following for the security type: • **NONE** • **WEP** • **TKIP** • **AES** • **TKIP/AES Mixed**
WEP	
Passphrase Key	Select a level of encryption (**64 bits** or **128 bits**). Enter a passphrase key consisting of 8 to 63 alphanumeric characters and click **Generate**.
Key 1 to 4	Select either **Key1**, **Key2**, **Key3**, **Key4**. Enter a WEP key in the respective field. The WEP key must: • contain letters from A to F and numbers from 0 to 9 • contain 10 characters for 64 bit and 26 characters for 128 bit encryption
WPA-PSK/WPA2PSK	
Preshared Key	Enter a preshared key consisting of 8 to 63 alphanumeric characters.
802.1x	
Radius Server	Enter the IP address of the RADIUS server.
Radius Port	Enter the port number of the RADIUS server.
Radius Key	Enter the key of the RADIUS server.
Apply Changes	Click to save your changes.

WiFi Access Filter

The WiFi Access Filter window enables you to either block or permit access for wireless clients by MAC address.

Select **WiFi Access** in the **WiFi Setup** menu to access the WiFi Access Filter window; see Figure 7-3.

Figure 7-3 WiFi Access Filter window

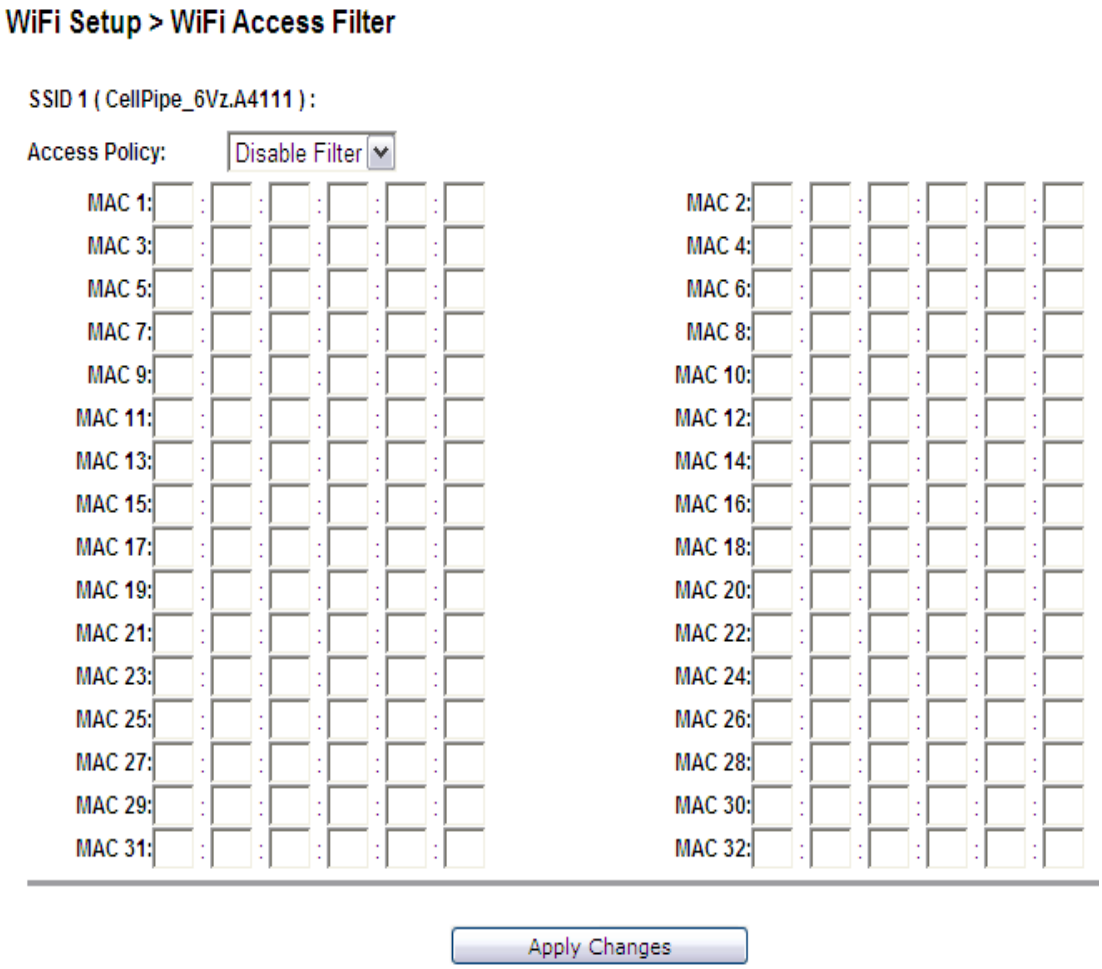


Table 7-3 describes the fields of the WiFi Access Filter window.

Table 7-3 Field descriptions

Field	Description
Access Policy	Select one of the following: • **Disable** to turn off WiFi filtering • **Allow** to permit access from the specified MAC address. • **Deny** to deny access from the specified MAC address.

Field	Description
MAC 1 to 32	Enter up to 32 MAC addresses to control their access.
Apply Changes	Click to save your changes.

8 Firewall Setup

Overview

Purpose

This chapter explains how to configure the firewall for the CellPipe 7130 RG.

Click the **Firewall** drop-down menu to open the **Firewall Setup** menu.

Contents

This chapter covers the following topics:

Port Forwarding

The Port Forwarding window enables you to control the incoming requests from the Internet to pass through the port to your local computer, and acts as a gateway to pass your service request using a different port or port range other than the standard port from the Internet client to your local servers.

Note: It is recommended that port forwarding be configured with the assistance of your ISP.

Select **Port Forwarding** in the **Firewall Setup** menu to access the Port Forwarding window; see Figure 8-1.

Figure 8-1 Port Forwarding window

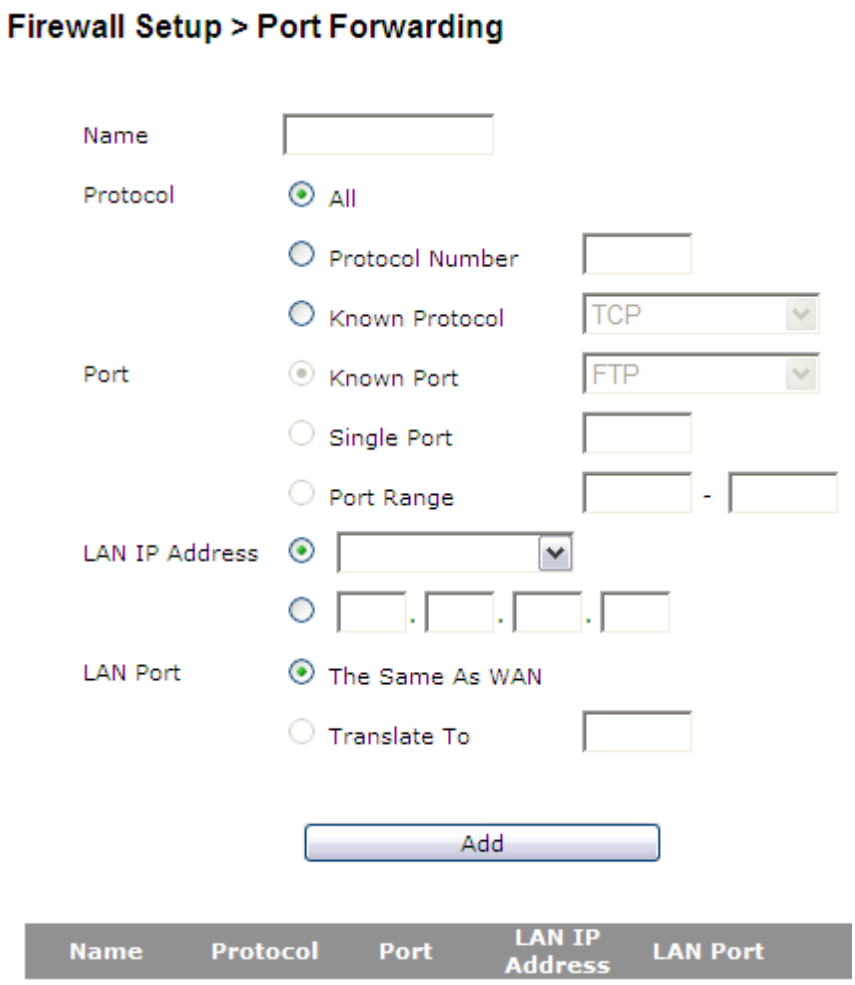


Table 8-1 describes the fields of the Port Forwarding window.

Table 8-1 Field descriptions

Field	Description
Name	Enter a name for the application you are hosting on your LAN computer; for example, Real Audio.
Protocol	Select the type of protocol(s) used by this application: • **ALL** • **Protocol Number** • **Known Protocol**

Field	Description
Port	Select or enter the port used by this application: • **Known Port** • **Single Port** • **Port Range**
LAN IP Address	Select the first radio button to choose a pre-configured LAN host or select the second radio button to enter an IP address manually.
LAN Port	Select the first radio button to use the port or port range same as the WAN or select the second radio button enter the LAN port manually.
Apply Changes	Click to save your changes.

Demilitarized Zone (DMZ)

The Demilitarized Zone window enables you to configure a single computer on your local side exposed to the Internet. All incoming packets will be forwarded to this computer; see Table 8-2.

Note: Use the demilitarized zone setting only if the virtual server or port range forwarding options do not provide the level of access required for certain applications. It is recommended that you contact your ISP for assistance.

Select **Demilitarized Zone** in the **Firewall Setup** menu to access the demilitarized zone window; see Figure 8-2.

Figure 8-2 Demilitarized Zone window

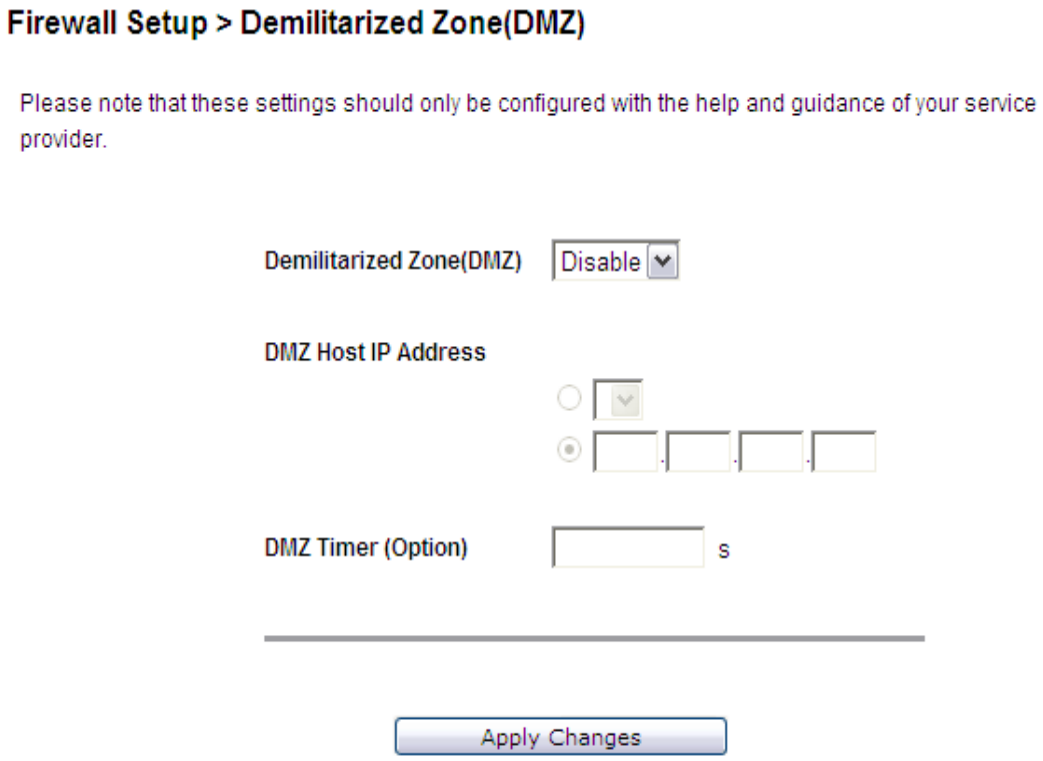


Table 8-2 describes the fields of the Demilitarized Zone window.

Table 8-2 Field descriptions

Field	Description
Demilitarized Zone (DMZ)	Select **Enable** to turn on the demilitarized zone function. Select **Disable** to turn it off.
DMZ Host IP Address	Select the first radio button and choose a pre-existing (or preset) LAN host or select the second radio button to enter an IP address manually.
DMZ Timer (Option)	To improve security, specify the length of time (in seconds) during which the DMZ is active.
Apply Changes	Click to save your changes.

UPnP

UPnP is an open networking standard that allows peer-to-peer network connectivity between devices. It enables software or devices, such as video game consoles, to function properly using NAT. See Table 8-3 below.

Note: It is recommended that you contact your ISP for assistance.

Select **UPnP** in the **Firewall Setup** menu to access the UPnP window; see Figure 8-3.

Figure 8-3 UPnP window

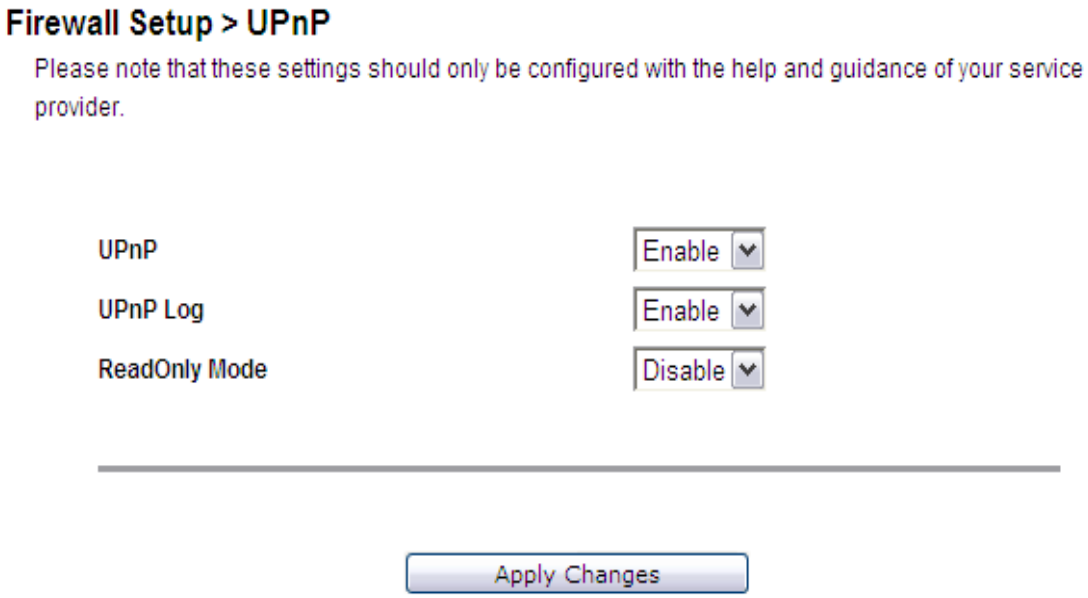


Table 8-3 describes the fields of the UPnP window.

Table 8-3 Field descriptions

Field	Description
UPnP	Select **Enable** to enable the UPnP function. Select **Disable** to disable the UPnP function.
UPnP Log	Select **Enable** to enable the logging activities. Select **Disable** to disable the logging activities.
ReadOnly Mode	Select **Enable** to turn on the read-only mode. Select **Disable** to turn off the read-only mode. **Note:** In read-only mode, users are unable to change port forwarding settings or any other UPnP enabled application settings.
Apply Changes	Click to save your changes.

Layer 2 Filter

Select **Layer 2 Filter** in the **Firewall Setup** menu to access the Layer 2 Filter window; see Figure 8-4.

Figure 8-4 Layer 2 Filter window

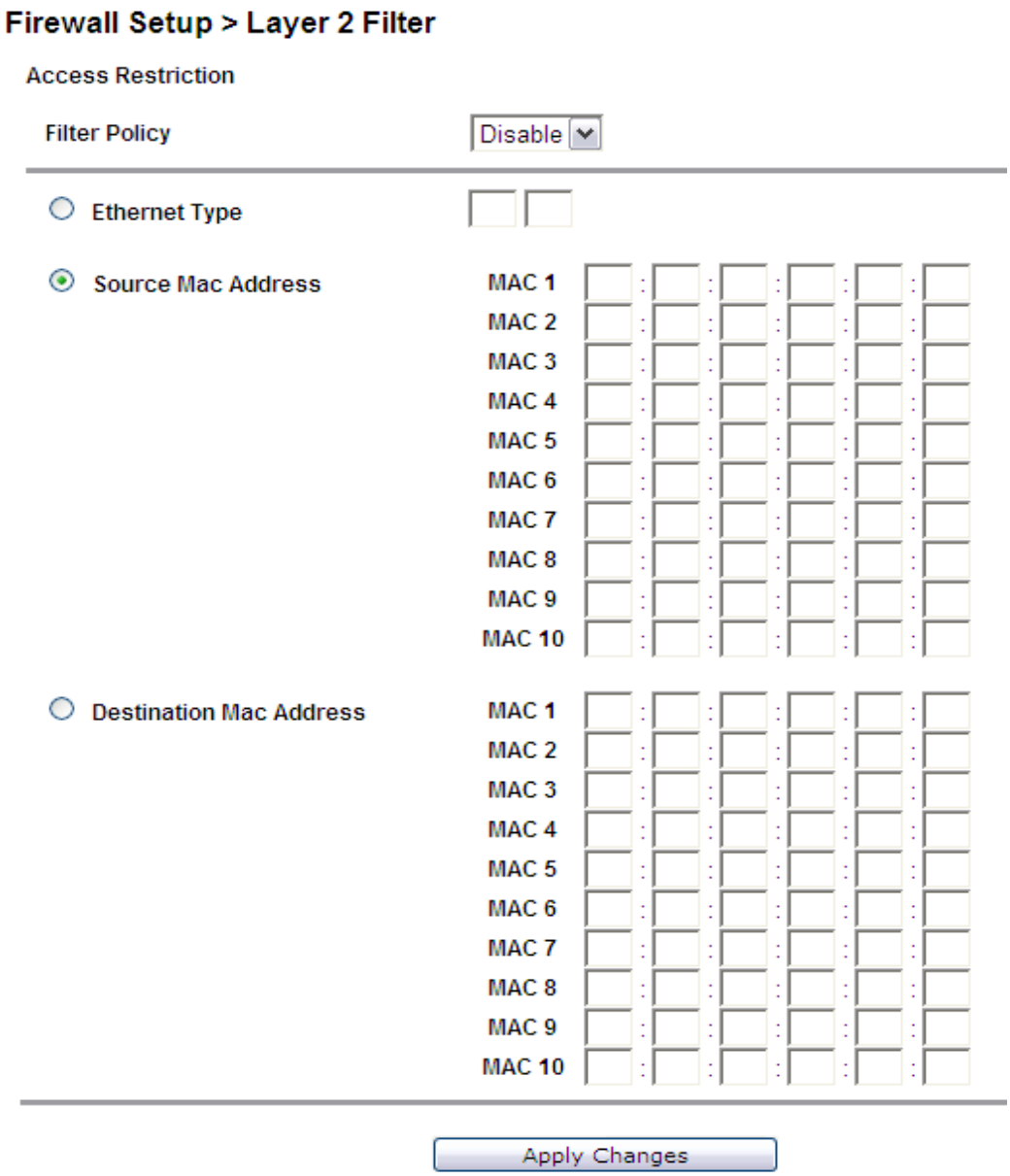


Table 8-4 describes the fields of the Filter window.

Table 8-4 Field descriptions

Field	Description
Filter Policy	Select the policy for filters: • **Allow** • **Deny** • **Disable**
Ethernet Type	Select to use Ethernet Type as the filtering algorithm and enter the applicable Ethernet Type code.

Field	Description
Source Mac Address 1 to 10	Select and then enter the source MAC address of the device.
Destination Mac Address 1 to 10	Select and then enter the destination MAC address of the device.
Apply Changes	Click to save your changes.

Layer 3 Filter

Select **Layer 3 Filter** in the **Firewall Setup** menu to access the Layer 3 Filter window; see Figure 8-5.

Figure 8-5 Layer 3 Filter window

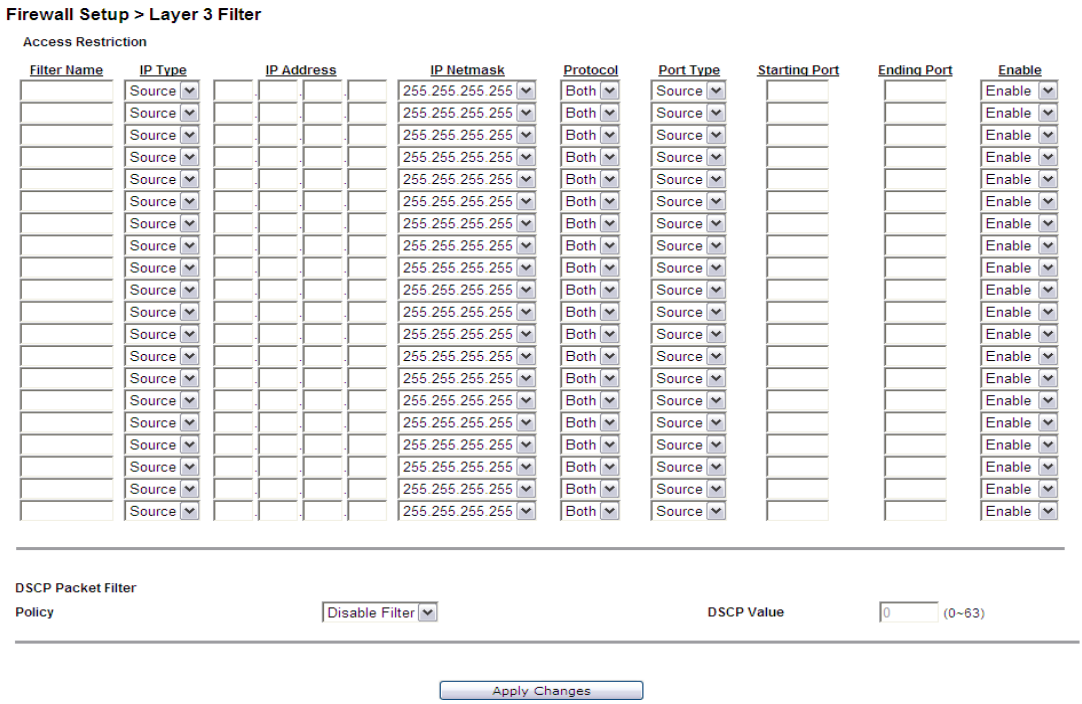


Table 8-5 describes the fields of the Filter window.

Table 8-5 Field descriptions

Field	Description
Filter Name	Enter a name for this filtering rule.
IP Type	Select **Dest** (destination) or **Source** depending on the how the rule is going to be used.

Field	Description
IP Address	Enter the IP address of the host that you are blocking.
IP Netmask	Select the Netmask of the host that you are blocking.
Protocol	Select the type protocol(s) used by this application: • **TCP** • **UDP** • **Both**
Port Type	Select **Dest** (destination) or **Source** depending on the type of application.
Starting Port Ending Port	Enter the range of the ports used by this application.
Enable	Select **Enable** to apply this filter rule or **Disable** to turn off this filter rule.
DSCP Policy	Select **Disable Filter** to disable the DSCP policy. Select **Deny** to deny packets that are accessing the Internet with the specified DSCP value in IP header or select **Allow** to allow packets that are accessing the Internet with the specified DSCP value in IP header.
DSCP Value	Enter a DSCP value between 0 and 63.
Apply Changes	Click to save your changes.

NAT Passthrough

The NAT Passthrough window allows you to enable or disable specific protocols from passing through the gateway.

Select **NAT Passthrough** in the **Firewall Setup** menu to access the NAT Passthrough window; see Figure 8-6.

Figure 8-6 NAT Passthrough window

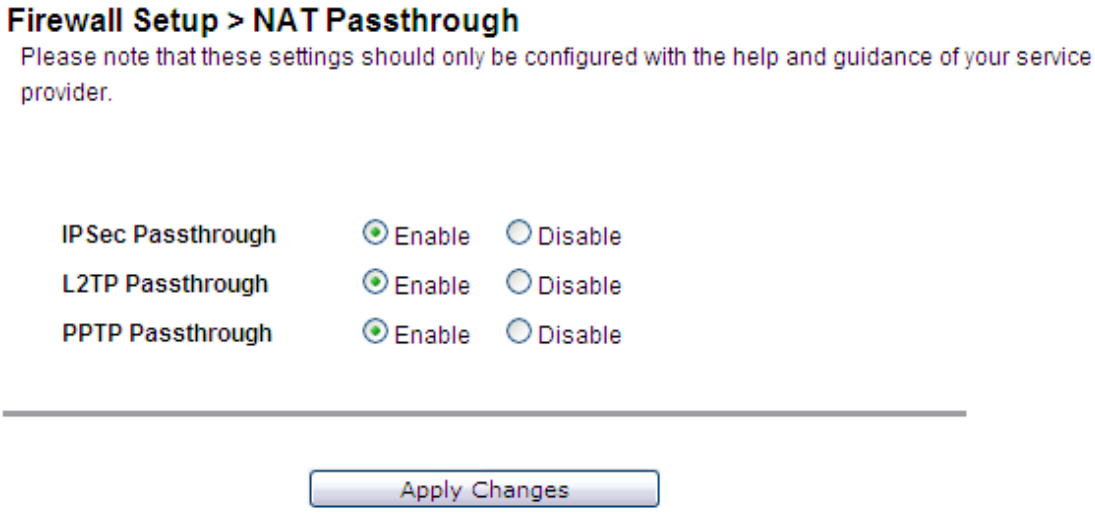


Table 8-6 describes the fields of the NAT Passthrough window.

Table 8-6 Field descriptions

Field	Description
IPSec Passthrough	Select **Enable** to allow IPSec passthrough. Select **Disable** to disallow the IPSec passthrough.
L2TP Passthrough	Select **Enable** to allow L2TP passthrough. Select **Disable** to disallow L2TP passthrough.
PPTP Passthrough	Select **Enable** to allow PPTP passthrough. Select **Disable** to disallow PPTP passthrough.
Apply Changes	Click to save your changes.

URL Blocking

The URL Blocking window enables you to block requests form your local computer to access specific websites.

Select **URL Blocking** in the **Firewall Setup** menu to access the URL Blocking window; see Figure 8-7.

Figure 8-7 URL Blocking window

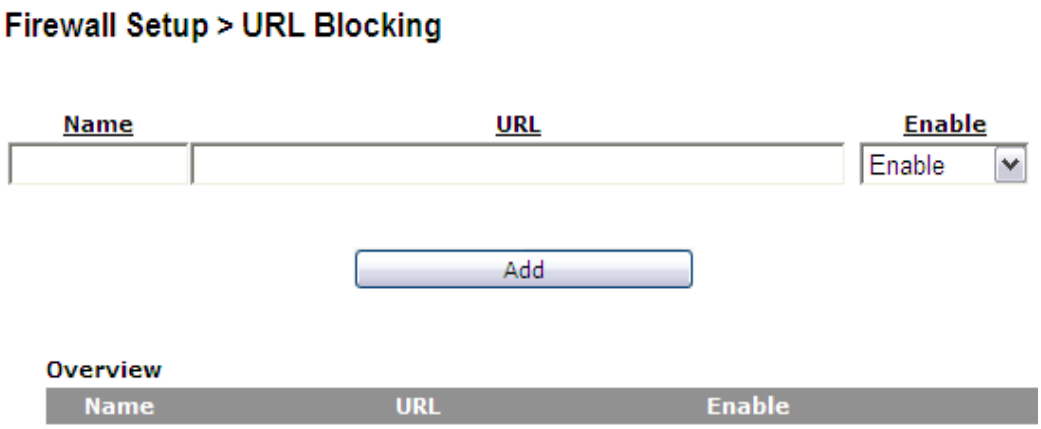


Table 8-7 describes the fields for the URL Blocking window.

Table 8-7 Field descriptions

Field	Description
Name	Enter a name for this URL filter.
URL	Enter a URL or keyword of the URL you are blocking. If the keyword is too general, you might inadvertently block other websites.
Enable	Select **Enable** to apply this URL filter. Select **Disable** to turn off this URL filter.
Add	Click to add the URL in blocking rule.

Content Screening

The Content Screening window lets you configure keywords to screen website content. If the keywords appears in the website content and content screening is enabled, firewall will block user from accessing this website.

Select **Content Screening** in the **Firewall Setup** menu to access the Content Screening window; see Figure 8-8.

Figure 8-8 Content Screening window

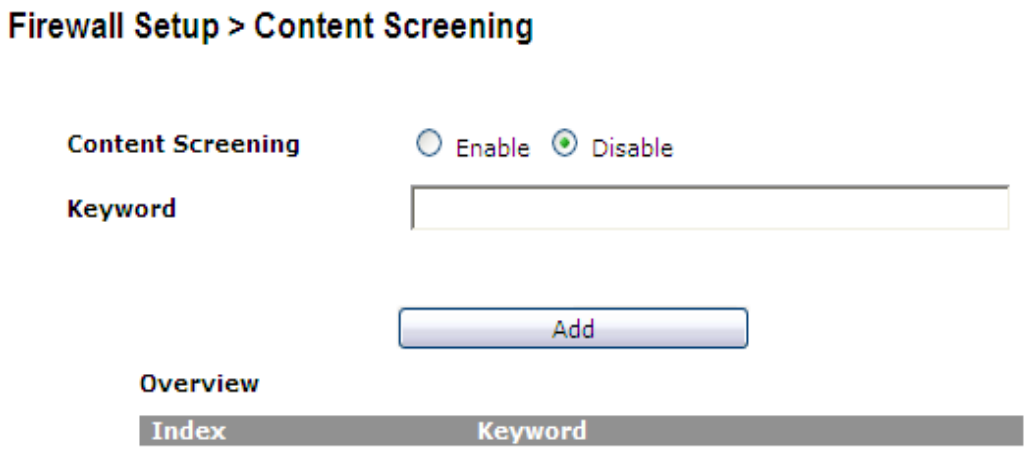


Table 8-8 describes the fields for the Content Screening window.

Table 8-8 Field descriptions

Field	Description
Content Screening	Select **Enable** to apply content screening content and block websites that have configured keywords in their contents. Select **Disable** to disable content screening.
Key Words	Enter a keyword you are blocking. If the keyword is too general, you might inadvertently block other websites. Type in only one keyword, if you want to screen multiple keywords, add them in separate rules. Maximum number of keywords allowed are 254.
Index	The index of rule. The index is created by system.
Add	Click to add the keyword in content screening rule.
Edit	Click to edit the keyword to the content screening rule.
Delete	Click to delete the keyword to the content screening rule.

Parental Control

The Parental Control window enables you to limit your computer's Internet connection based on the time and day of the week.

Select **Parental Control** in the **Firewall Setup** menu to access the Parental Control window; see Figure 8-9.

Figure 8-9 Parental Control window

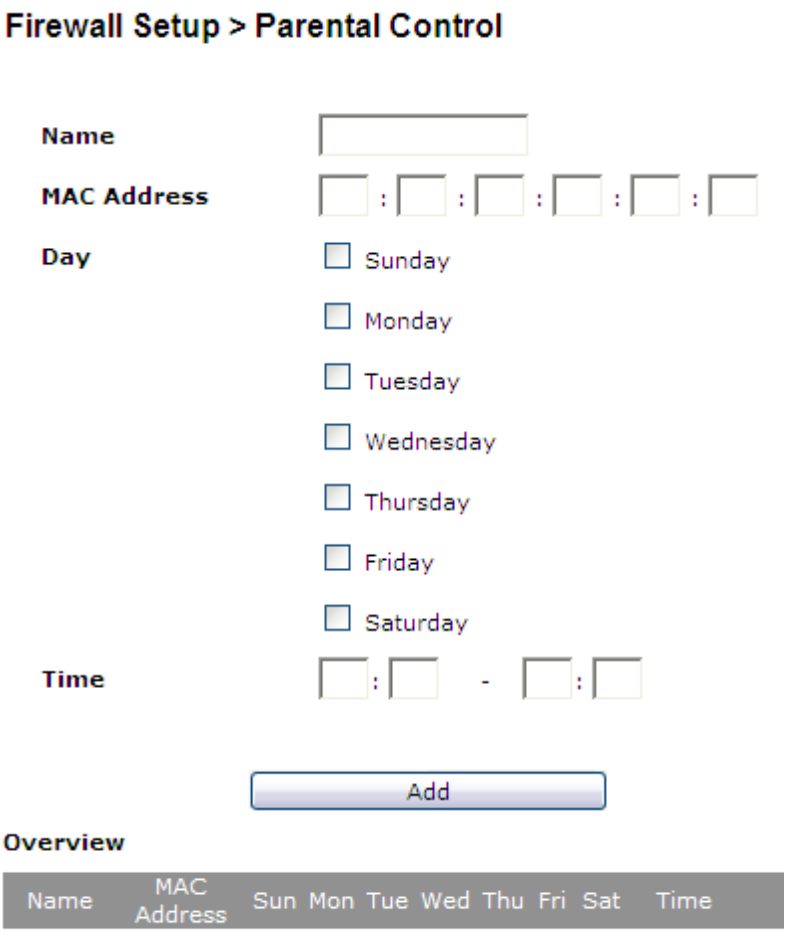


Table 8-9 describes the fields for the Parental Control window.

Table 8-9 Field descriptions

Field	Description
Name	Enter an appropriate name for your rule.
Mac Address	Enter the MAC address of the client computer.
Day	Check the days you want to limit the client's Internet connection.

Field	Description
Time	Enter a time period (in hours and minutes) to limit the Internet connection.
Add	Click to add rule in Parental control.

9 Advanced Setup

Overview

This chapter explains how to configure the advanced settings of the CellPipe 7130 RG such as the route setting, DNS, dynamic DNS, system log, IGMP settings and 802.1x.

Click the **Advanced Setup** drop-down menu to open the **Advanced Setup** menu.

Contents

This chapter covers the following topics:

Route Setting

The Route Setting window enables you to configure static and dynamic routes for routing packets from one network to another network.

Select **Route Setting** in the **Advanced Setup** menu to access the Route Setting window; see Figure 9-1.

Figure 9-1 Route Setting window

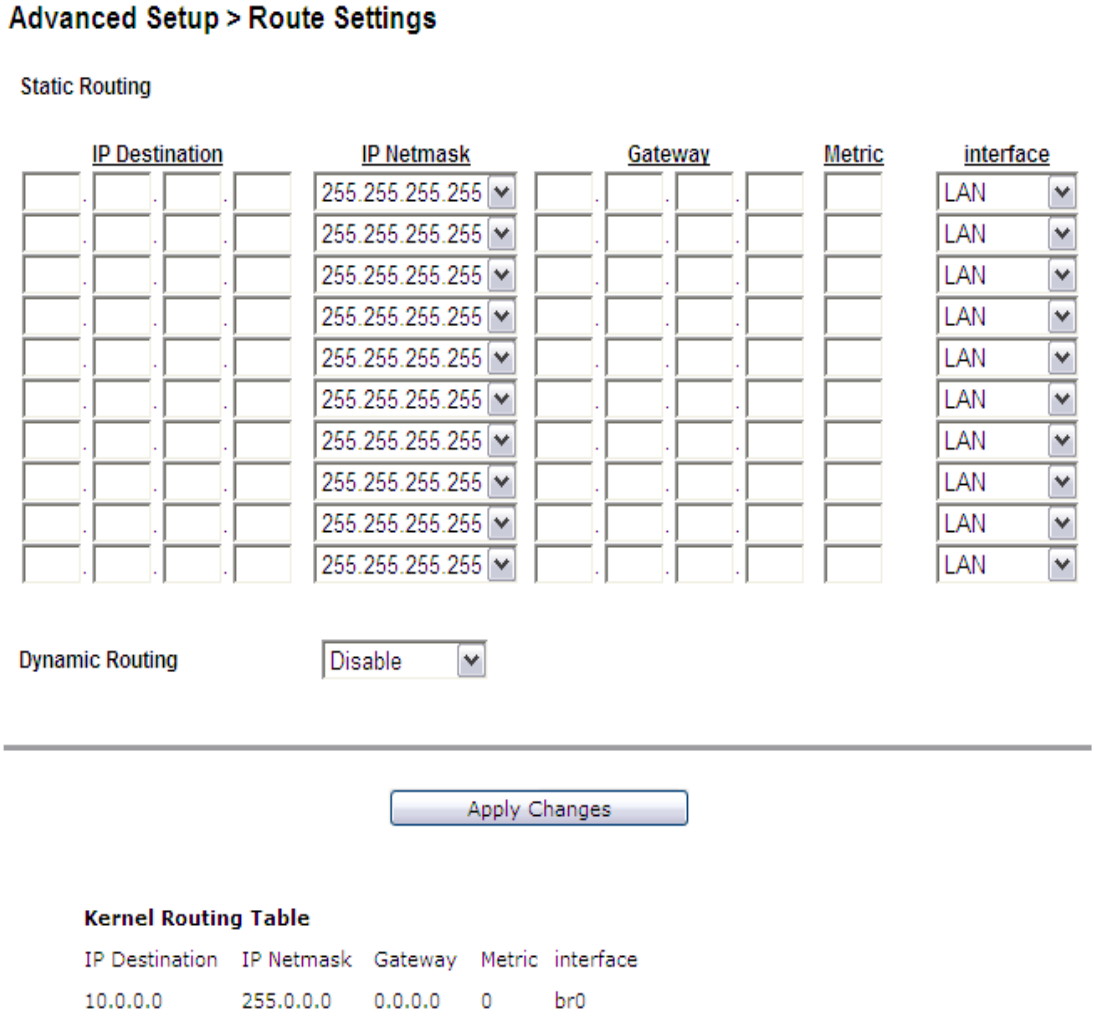


Table 9-1 describes the fields of the Route Setting window.

Table 9-1 Field descriptions

Field	Description
Static Route	Static routing enables you to configure a pre-determined path that network traffics need to travel to reach other network or host.
IP Destination	Enter the IP address of the destination network.
IP Netmask	Select the subnet mask of the destination network.
Gateway	Enter the IP address of the gateway for the destination network.
Metric	In order to determine the best route, a value is used to specify the cost of the route (the metric value). Enter the metric value in the metric field. IP routing uses hop count as measurement of the metric.
Interface	Select **LAN** or **WAN** interface. The packets sent to the addresses of the destination IP address are sent through this interface. However, for the WAN interface it will depends on the WAN configuration.

Field	Description
Dynamic Route (WAN)	Select **Enable** to use dynamic routing instead of static. Dynamic routing enables the router to adapt to changes in the network and exchange rating table with other router(s). Select **Disable** to turn off dynamic routing.
Apply Changes	Click to save your changes.

DNS Settings

The DNS Settings window enables you to configure the domain name and IP address of the domain name.

Note: You can set up to 64 entries.

Select **DNS Settings** in the **Advanced Setup** menu to access the DNS Settings window; see Figure 9-2.

Figure 9-2 DNS Settings window

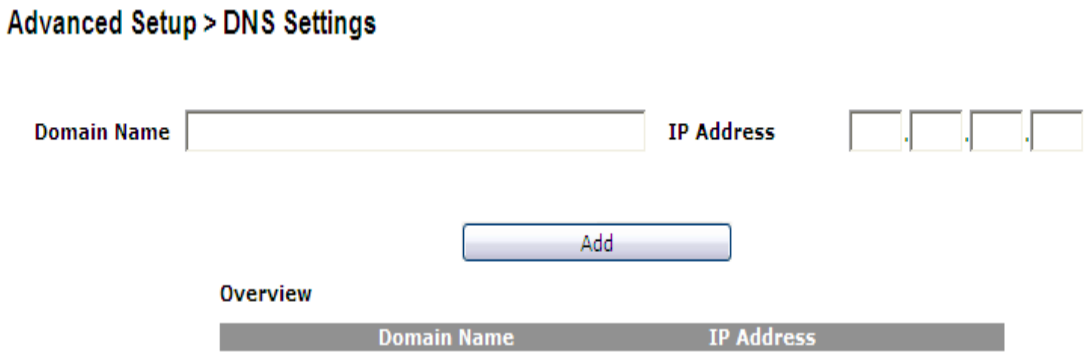


Table 9-2 describes the fields of the Dynamic DNS window.

Table 9-2 Field descriptions

Field	Description
Domain Name	Enter the domain name to which you want to connect.
IP Address	Enter the IP address of the Static DNS.
Add	Click to add the DNS settings and save your changes.

Dynamic DNS

The Dynamic DNS (DDNS) window enables you to configure your registered domain name with a dynamic IP address.

Note: Before you can use this feature, you need to sign up a DDNS service at one of the supported DDNS service providers; see DynDNS.org or ChangeIP.com.

Click on **Dynamic DNS** in the **Advanced Setup** menu to access the dynamic DNS window; see Figure 9-3.

Figure 9-3 Dynamic DNS window

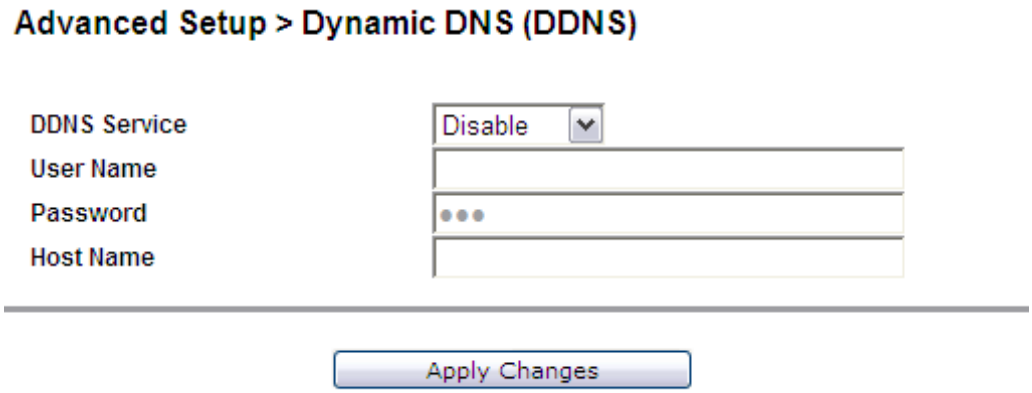


Table 9-3 describes the fields of the Dynamic DNS window.

Table 9-3 Field descriptions

Field	Description
DDNS Service	If you have signed up a DDNS, select the DDNS service.
User Name	Enter the username of your DDNS account.
Password	Enter the password of your DDNS account.
Host Name	Enter the host name.
Apply Changes	Click to save your changes.

System Log

The System Log window enables you to view the system logs and to send them to a remote system log server.

Click on **System Log** in the **Advanced Setup** menu to access the system log window; see Figure 9-4.

Figure 9-4 System Log window

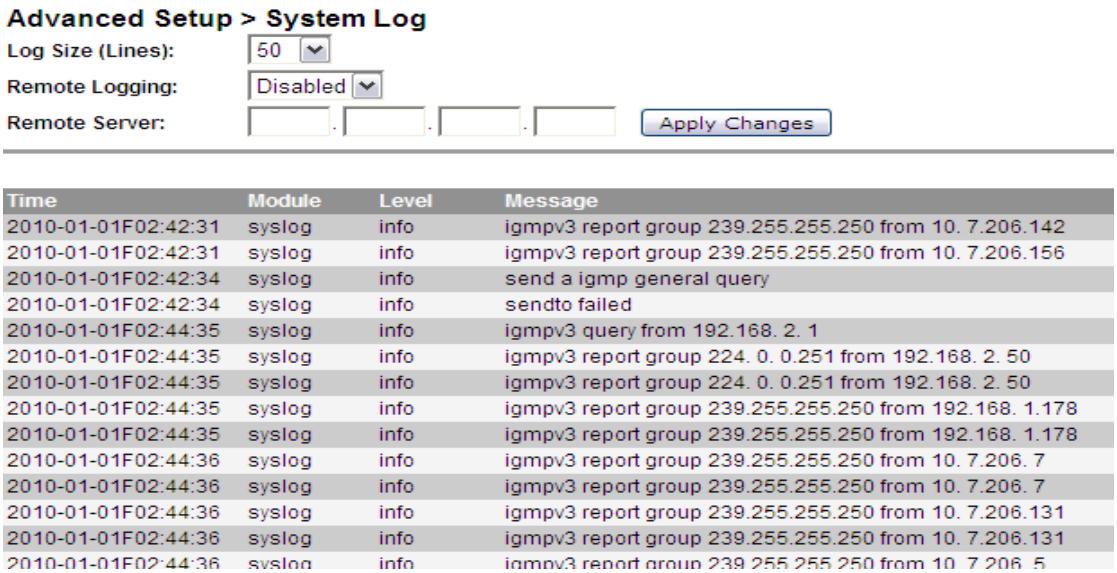


Table 9-4 describes the fields of the System Log window.

Table 9-4 Field descriptions

Field	Description
Log Size (Lines)	Select the number of lines to display in your log.
Remote Logging	Select **LAN** or **WAN** for the remote logging server. Select **Disable** to turn off remote logging.
Remote Server	Enter the IP address of the remote logging server.
Apply Changes	Click to save your changes to view the log. If you are configuring remote logging, click **Apply Changes** after changing the remote logging and remote server fields.
Time	The time that the action was performed.
Module	The type of module the action involved.

Field	Description
Level	The level of logging activity: • **Info** • **Error** • **Debug**
Message	The details of the action that was performed.

IGMP Proxy/Snooping

The IGMP Setting window enables you to setup LAN-side IGMP protocol supporting which enable LAN-side user to receive multicast traffic.

Click on **IGMP Settings** in the **Advanced Setup** menu to access the system log window; see Figure 9-5.

Figure 9-5 IGMP Proxy/Snooping window

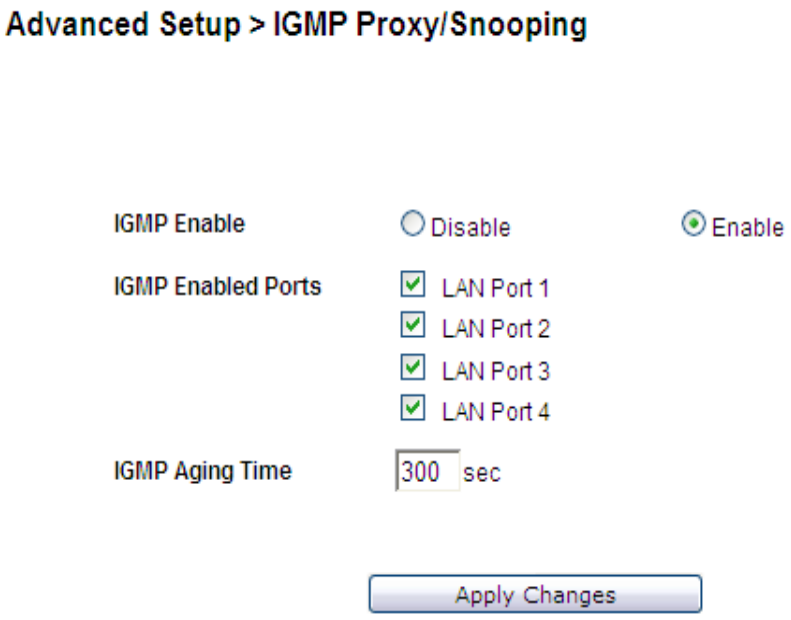


Table 9-5 describes the fields of the System Log window.

Table 9-5 Field descriptions

Field	Description
IGMP Enable	Select **Enable** to allow IGMP support. Select **Disable** to disable IGMP support.
Port Enable	**Enable/Disable** IGMP support for each individual LAN port.
IGMP Aging Time	Enter the IGMP aging time in seconds.
Apply Changes	Click to save your changes.

802.1x Config

The 802.1x Config window enables you to setup the 802.1x configuration. 802.1x is an authentication mechanism for clients connecting to an IEEE 802 network such as Ethernet (access) networks and 802.11 (public) wireless LANs.

Click on **802.1x Config** in the **Advanced Setup** menu to access the 802.1x Config window; see Figure 9-6.

Figure 9-6 802.1x Config window

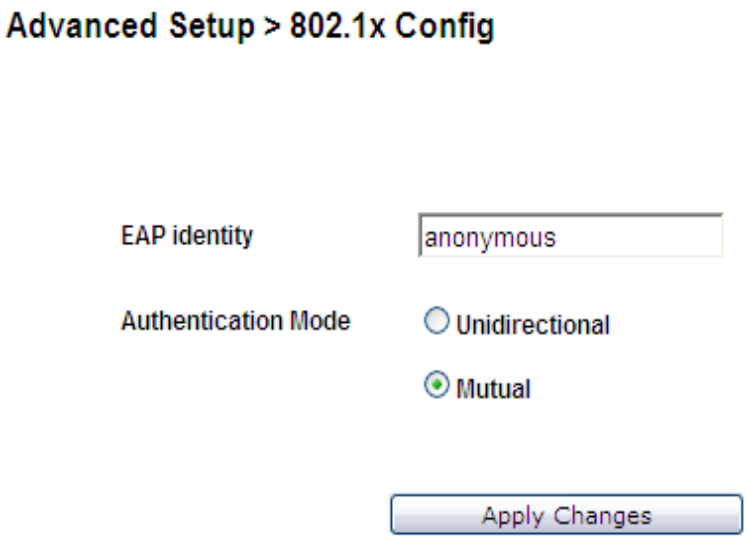


Table 9-6 describes the fields of the 802.1x Config window.

Table 9-6 Field descriptions

Field	Description
EAP identify	Enter the EAP identity.
Authentication Mode	Select **Unidirectional** or **Mutual** support for each.

Field	Description
Apply Changes	Click to save your changes.

10 QoS PTM Setup

Overview

This chapter explains how to configure the QoS settings via PTM. QoS is the ability to provide better service to selected applications and data flows.

Click the **QoS PTM Setup** drop-down menu to open the **QoS PTM Setup** menu.

Contents

This chapter covers the following topics:

QoS Overview

The QoS overview window allows you to see all current QoS settings.

Select **QoS Overview** in the **QoS PTM Setup** menu to access the QoS overview window; see Figure 10-1.

Figure 10-1 QoS Overview window

QoS PTM Setup > QoS Overview

Precedence	Source	Destination	Protocol	Source Port	Destination Port	QoS Classification	ToS/DSCP Settings	CoS Settings
Default	Interface Name: DHCP1					Original ToS Tag	Keep Original ToS	Keep CoS value

Table 10-1 describes the fields of the QoS overview window.

Table 10-1 Field descriptions

Field	Description
Precedence	The Precedence presents the priority of each QoS rule. (Precedence 1 is the highest priority.)
Source	IP address of source host.
Destination	IP address of destination host.
Protocol	The protocol type of this QoS rule.
Source Port	Port number of source host.
Destination Port	Port number of destination host.
QoS Classification	The classification of this QoS rule: • **Original ToS Tag** - assign the queue according to the incoming traffic ToS value. • **Specified Queue** - incoming traffic will assign a specific queue (0 to 7).
ToS/DSCP Setting	TOS/DSCP marking setting for incoming traffic.
CoS Setting	CoS (class of service) setting of this QoS rule.

QoS Scheduler

The QoS Scheduler window allows you to enable and disable the scheduler protocol and determine the upstream bandwidth.

Select **QoS Scheduler** in the **QoS PTM Setup** menu to access the QoS scheduler window; see Figure 10-2.

Figure 10-2 QoS Scheduler window

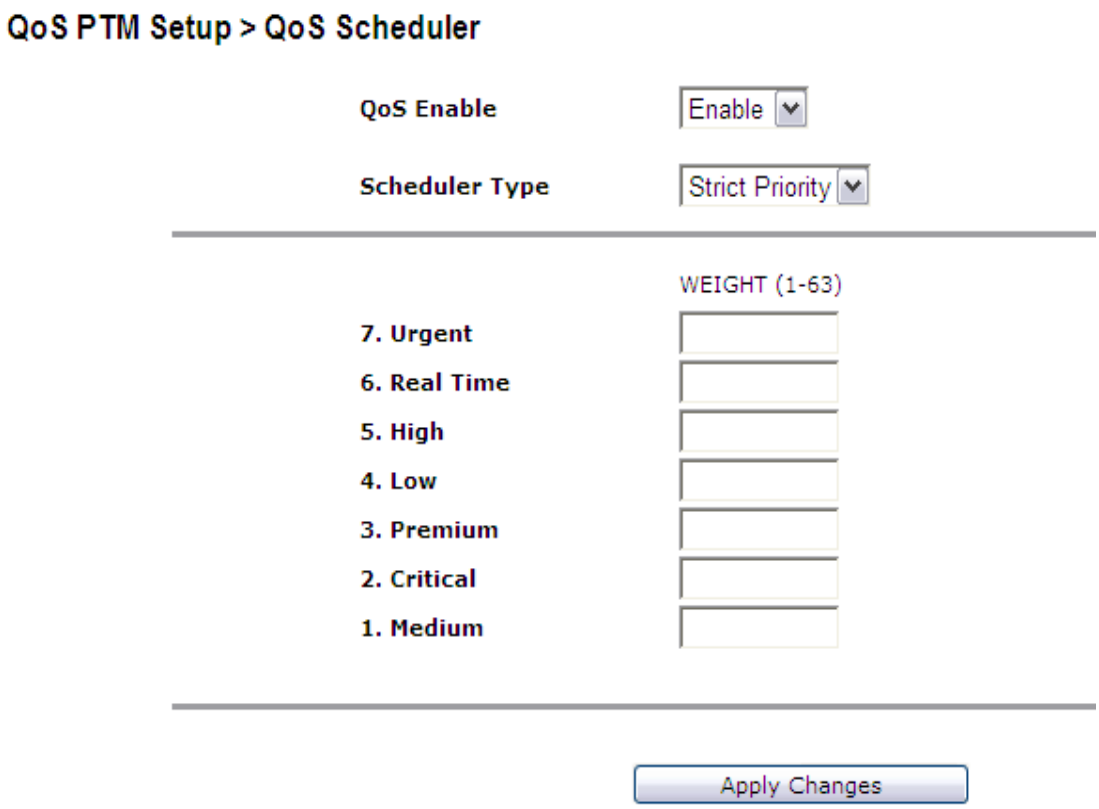


Table 10-2 describes the fields of the QoS Scheduler window.

Table 10-2 Field descriptions

Field	Description
QoS Enable	Select **Enable** to activate the QoS scheduler. Select **Disable** to turn off the QoS scheduler.
Scheduler Type	The QoS scheduler type is either: • **Strict Priority** - Strict Priority scheduling delivers high priority(7.Urgent queue is the highest) traffic first and then lower priority traffic when higher ones are empty. • **Min - Max Bandwidth** - Min - Max Bandwidth scheduling to specify the minimum and maximum bandwidth for each queue.
7. Urgent	Specify the minimum and maximum bandwidth for the **Urgent queue**.
6. Real Time	Specify the minimum and maximum bandwidth for the **Real Time queue**.
5. High	Specify the minimum and maximum bandwidth for the **High queue**.

Field	Description
4. Low	Specify the minimum and maximum bandwidth for the **Low queue**.
3. Premium	Specify the minimum and maximum bandwidth for the **Premium queue**.
2. Critical	Specify the minimum and maximum bandwidth for the **Critical queue**.
1. Medium	Specify the minimum and maximum bandwidth for the **Medium queue**.
Apply Changes	Click to save your changes.

QoS Policy

The QoS Policy window enables you to group upstream traffic into data flows according to the source address, destination address, source port, and destination port.

Select **QoS Policy** in the **QoS PTM Setup** menu to access the QoS Policy window; see Figure 10-3.

Figure 10-3 QoS Policy window

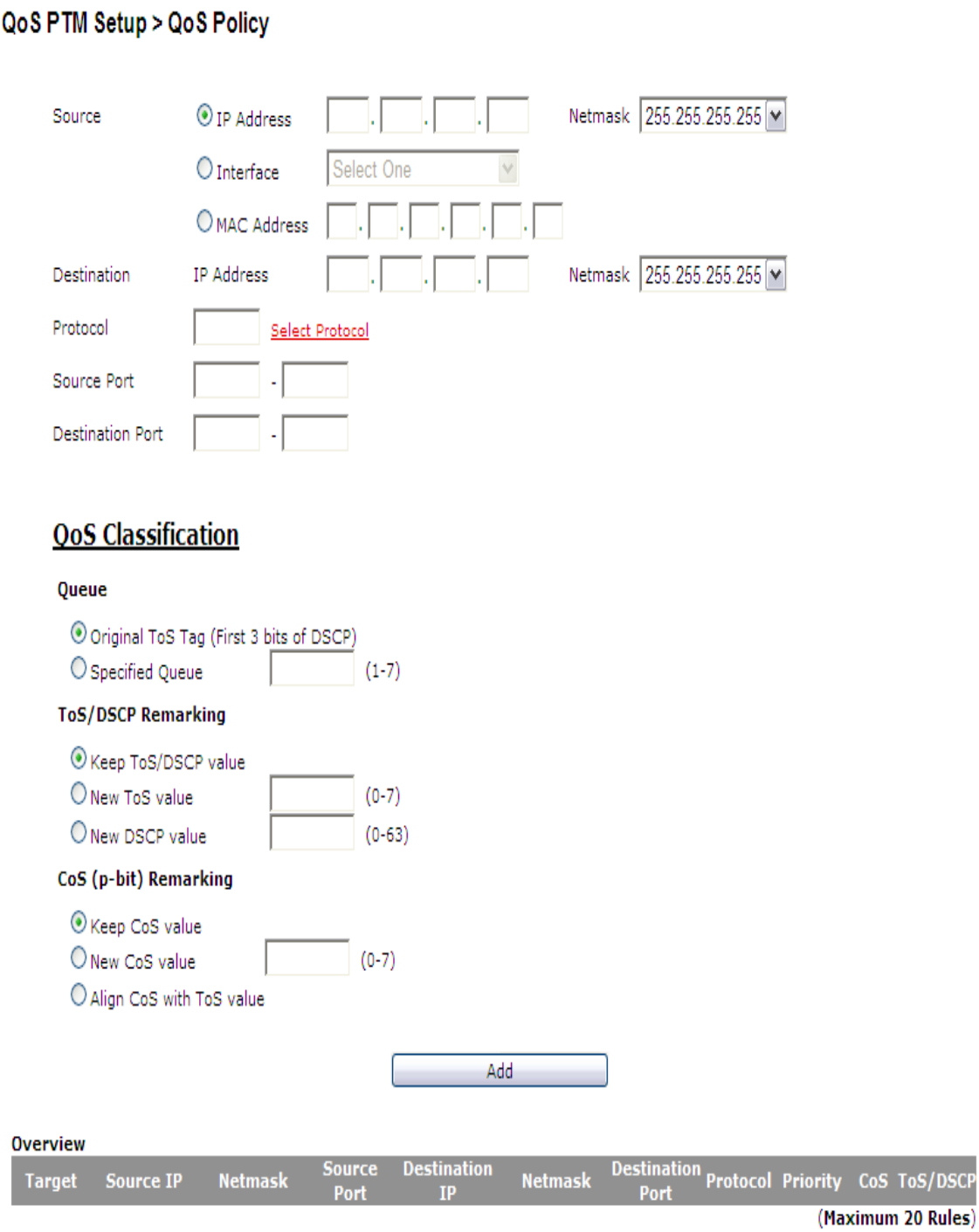


Table 10-3 describes the fields of the QoS Policy window.

Table 10-3 Field descriptions

Field	Description
Source	
IP Address	Select the radio button and enter the IP address of the source host.

Field	Description
Netmask	Select the subnet mask of the source host.
Interface	Select the radio button and select a connection to configure its QoS policy.
MAC Address	Select the radio button and enter the MAC address.
Destination	
IP Address	Enter the IP address of the destination host.
Netmask	Select the subnet mask of the destination host.
Protocol	Click **Select Protocol** to choose a protocol.
Source Port	Enter the range of source ports for this QoS policy.
Destination Port	Enter the range of destination ports for this QoS policy.
QoS Classification	
Queue	Select one of the following: • **Original ToS Tag** to assign the queue according to the incoming ToS value. • **Specified Queue** and enter a queue number (0 to 7) to assign to the incoming traffic.
ToS/DSCP Remarking	Select one of the following: • **Keep Original ToS/DSCP** to retain the original value. • **New ToS Value** and enter a queue number (0 to 7) to assign to the incoming traffic. • **New DSCP Value** and enter a DSCP value (0 to 63).
CoS (p-bit) Remarking	Select one of the following: • **Keep CoS Value** to retain the original value. • **New CoS Value** to set a new CoS value for incoming traffic. • **Align CoS with ToS value** to set CoS same as the ToS value for incoming traffic.
Add	Click to add the policy and save your changes.
Overview	
Target	Upstream or Downstream. Target 1 is the highest priority.
Source IP	IP address of the source host.
Netmask	Subnet mask of the source IP address.
Source Port	Port number of the source host.
Destination IP	IP address of the destination host.
Netmask	Subnet mask of the destination IP address.
Destination Port	Port number of the destination host.

Field	Description
Protocol	The protocol type for this QoS policy.
Priority	The priority queue (0 to 7) used by the traffic.
CoS	CoS value of the QoS policy.
ToS/DSCP	ToS/DSCP marking setting for incoming traffic.
Change Precedence	Select a QoS rule precedence number and then select where to move it: • **Up**: move this QoS rule to higher priority. • **Down**: move this QoS rule to lower priority. • **Delete**: remove this QoS rule. Click **Apply** to change the precedence.

QoS Phone

The QoS Phone lets you configure the QoS for your SIP session.

Select **QoS Phone** in the **QoS PTM Setup** menu to access the QoS Phone window; see Figure 10-4.

Figure 10-4 QoS Phone window

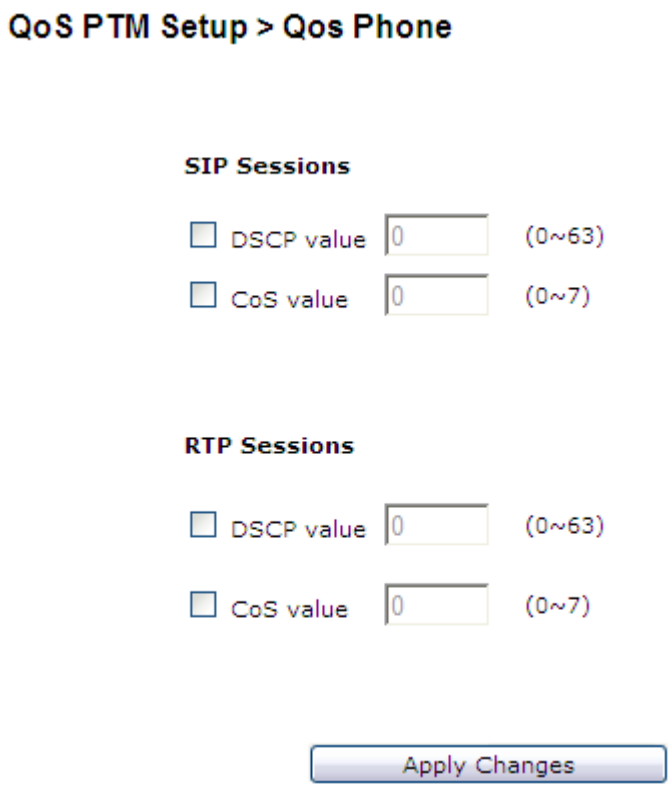


Table 10-4 describes the fields of the QoS Phone window.

Table 10-4 Field descriptions

Field	Description
SIP Sessions	Check **DSCP Value (Diffserv Code Point)** and enter a DSCP value (0 to 63). Check **CoS (class of service)** and set a value.
RIP Sessions	Check **DSCP Value (Diffserv Code Point)** and enter a DSCP value (0 to 63). Check **CoS (class of service)** and set a value.
Apply Changes	Click to save your changes.

QoS ALG

The QoS application level gateway (ALG) window enables you to configure the session initiated protocol (SIP) and the real-time transport protocol (RTP). SIP is used by VoIP, and RTP is the protocol for transferring real-time data (such as interactive audio and video).

Select **QoS ALG** in the **QoS PTM Setup** menu to access the QoS ALG window; see Figure 10-5.

Figure 10-5 QoS ALG window

QoS PTM Setup > QoS ALG

SIP ALG QoS Enable Disable

SIP Sessions

QoS Classification

Queue

Original ToS Tag (First 3 bits of DSCP)

Specified Queue 1 (1-7)

ToS/DSCP Remarking

Keep Original ToS

New ToS value 0 (0-7)

New DSCP value 0 (0-63)

CoS (p-bit) Remarking

Keep CoS value

New CoS value 0 (0-7)

Align CoS with ToS value

RTP Sessions

QoS Classification

Queue

Original ToS Tag (First 3 bits of DSCP)

Specified Queue 1 (1-7)

ToS/DSCP Remarking

Keep Original ToS

New ToS value 0 (0-7)

New DSCP value 0 (0-63)

CoS (p-bit) Remarking

Keep CoS value

New CoS value 0 (0-7)

Align CoS with ToS value

RTP Sessions

QoS Classification

Queue

Original ToS Tag (First 3 bits of DSCP)

Specified Queue 1 (1-7)

ToS/DSCP Remarking

Keep Original ToS

New ToS value 0 (0-7)

New DSCP value 0 (0-63)

CoS (p-bit) Remarking

Keep CoS value

New CoS value 0 (0-7)

Align CoS with ToS value

Apply Changes

Table 10-5 describes the fields of the QoS ALG window.

Table 10-5 Field descriptions

Field	Description
SIP ALG QoS Enable	Select **Enable** to turn on the SIP ALG QoS. Select **Disable** to turn off the SIP ALG QoS.
Original Tos Tag (First 3 bits of DSCP)	Select **Original Tos Tag** (type of service) to assign the queue according to the incoming Tos value.
Specified Queue	Select **Specified Queue** and enter a queue number (0 to 7) to assign to the incoming traffic.
Keep Original ToS	Select **Keep Original Tos** to retain the original value.
New ToS Value	Select **New Tos Value** and enter a queue number (0 to 7) to assign to the incoming traffic.
New DSCP Value	Select **New DSCP Value** and enter a DSCP value (0 to 63).
Keep CoS Value	Select **Keep CoS value** to retain the original value.
New CoS Value	Enable **New Cos Value** to assign CoS (class of service) for incoming traffic.
Align Cos with ToS Value	Enable **Align Cos with Tos value** to assign CoS (class of service) as Tos value for incoming traffic.
Apply Changes	Click to save your changes.

QoS Defaults

The QoS Default window enables you to configure the default QoS policy for each WAN connection.

Select **QoS Defaults** in the **QoS Setup** menu to access the QoS Default window; see Figure 10-6.

Figure 10-6 QoS Defaults window

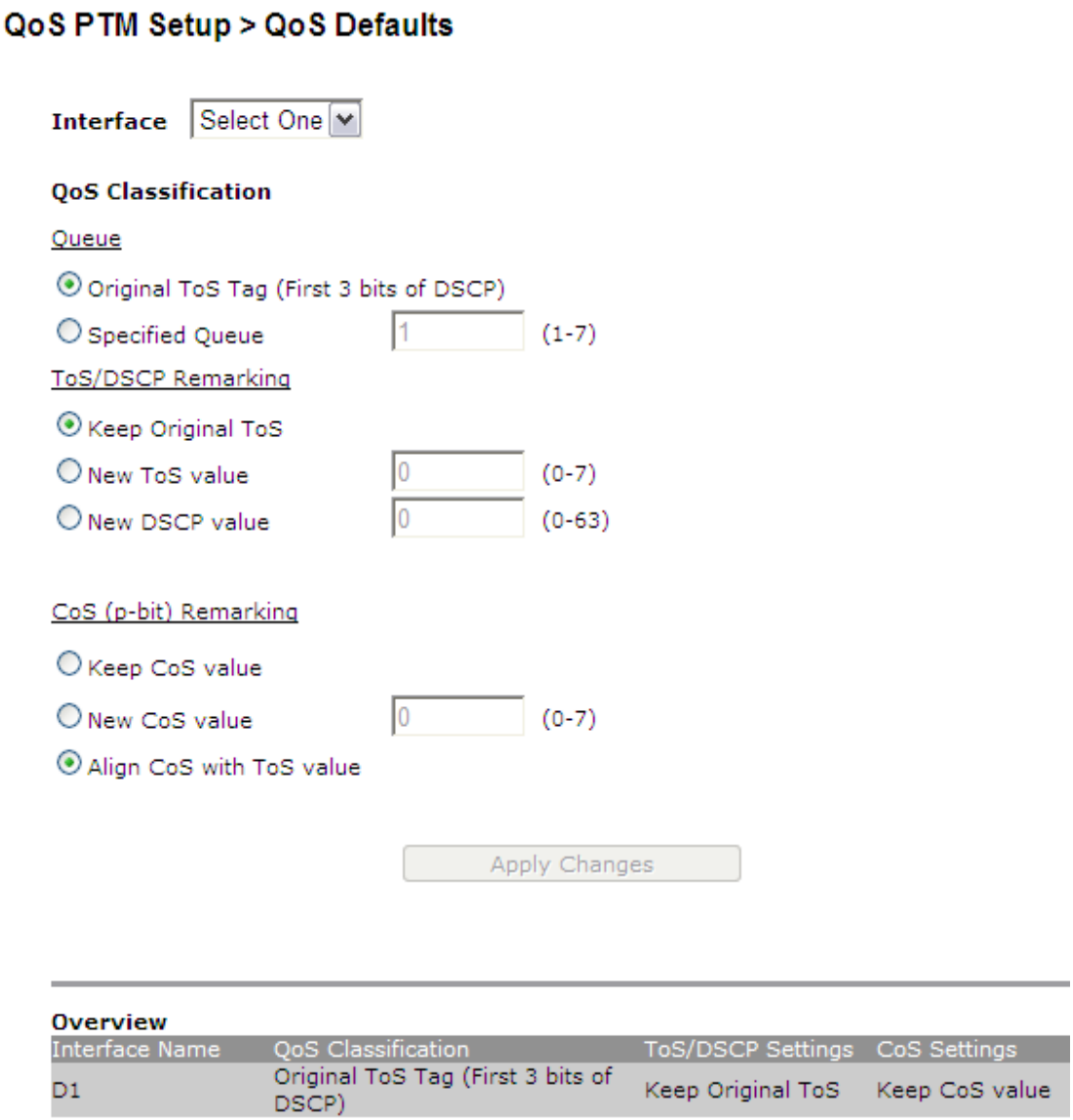


Table 10-6 describes the fields of the QoS Default window.

Table 10-6 Field descriptions

Field	Description
Interface	Select a WAN connection to configure its default QoS policy.
Original Tos Tag (First 3 bits of DSCP)	Select **Original Tos Tag** (type of service) to assign the queue according to the incoming Tos value.
Specified Queue	Select **Specified Queue** and enter a queue number (0 to 7) to assign to the incoming traffic.
Keep Original ToS	Select **Keep Original Tos** to retain the original value.

Field	Description
New Tos Value	Select **New Tos Value** and enter a queue number (0 to 7) to assign to the incoming traffic.
New DSCP Value	Select **New DSCP Value** and enter a DSCP value (0 to 63).
Keep Cos value	Select **Keep CoS value** to retain the original value.
New Cos Value	Select **New Cos Value** to set a new CoS (class of service) value for incoming traffic.
Align Cos with Tos Value	Select **Align Cos with Tos value** to assign CoS (class of service) as Tos value for incoming traffic.
Interface Name	The Interface name of WAN connection to configure its QoS policy.
QoS Classification	The classification of this QoS rule: • **Original Tos Tag** - assign the queue according to the incoming traffic's Tos value. • **Specified Queue** - incoming traffic will be queued in the specific queue (0 to 7).
TOS/DSCP Setting	TOS/DSCP marking setting for incoming traffic.
CoS Setting	Cos (class of service) setting of this QoS rule.
Apply Changes	Click to save your changes.

QoS MAC

The QoS MAC window enables you to configure QoS policy for specific device by MAC address when the gateway is operating in bridge mode.

Select **QoS MAC** in the **QoS Setup** menu to access the QoS MAC window; see Figure 10-7.

Figure 10-7 QoS MAC window

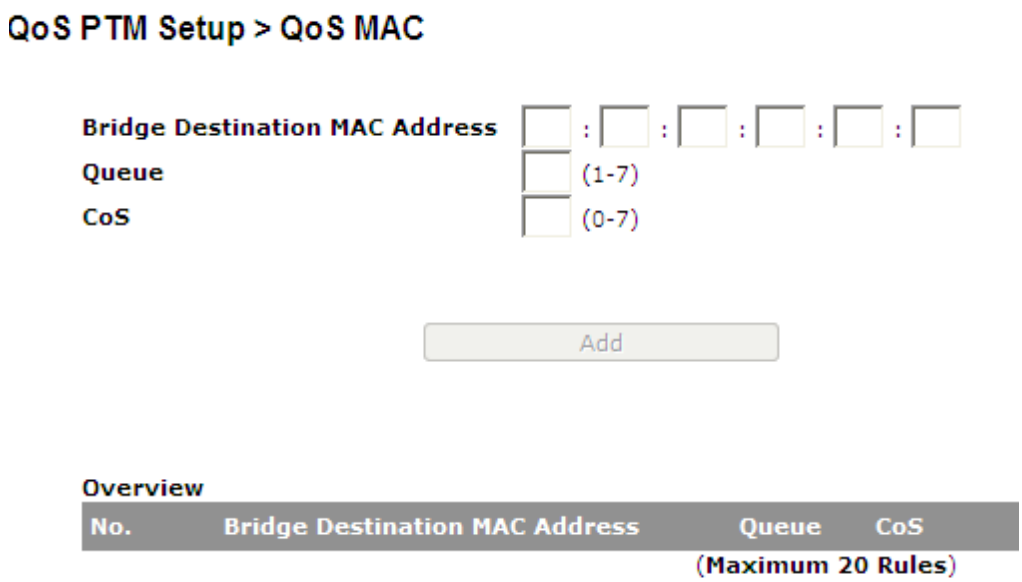


Table 10-7 describes the fields of the QoS ALG window.

Table 10-7 Field descriptions

Field	Description
Bridge Destination MAC Address	Specify the MAC address of QoS service user.
Queue	Specify which queue (0~7) will be assigned for this MAC address.
CoS	Specify the CoS Value(0~7) that will be marked on packets coming form this MAC address.
Add	Click to add this rule.

11 Utilities

Overview

This chapter explains how to configure the utilities of the CellPipe 7130 RG.

Click the **Utilities** drop-down menu to open the **Utilities** menu.

Contents

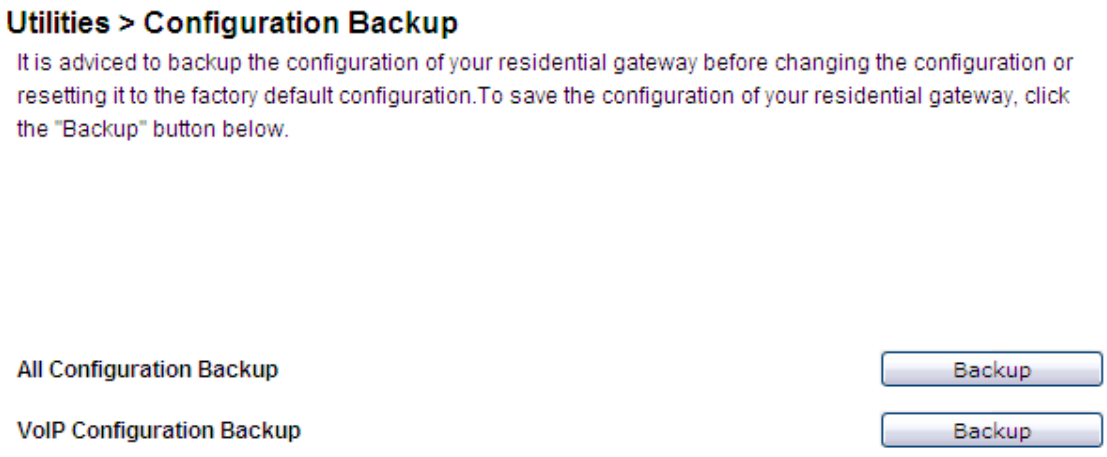
This chapter covers the following topics:

Configuration Backup

The Configuration Backup window enables you to backup your configuration of the CellPipe 7130 RG to a file and stored it on your computer.

Select **Configuration Backup** in the **Utilities** menu to access the Configuration Backup window; see Figure 11-1.

Figure 11-1 Configuration Backup window



Click on **Backup** to save your system configuration.

Configuration Restore

The Configuration Restore window enables you to restore your configuration of the CellPipe 7130 RG from a backup file.

Select **Configuration Restore** in the **Utilities** menu to access the Configuration Restore window; see Figure 11-2.

Figure 11-2 Configuration Restore window

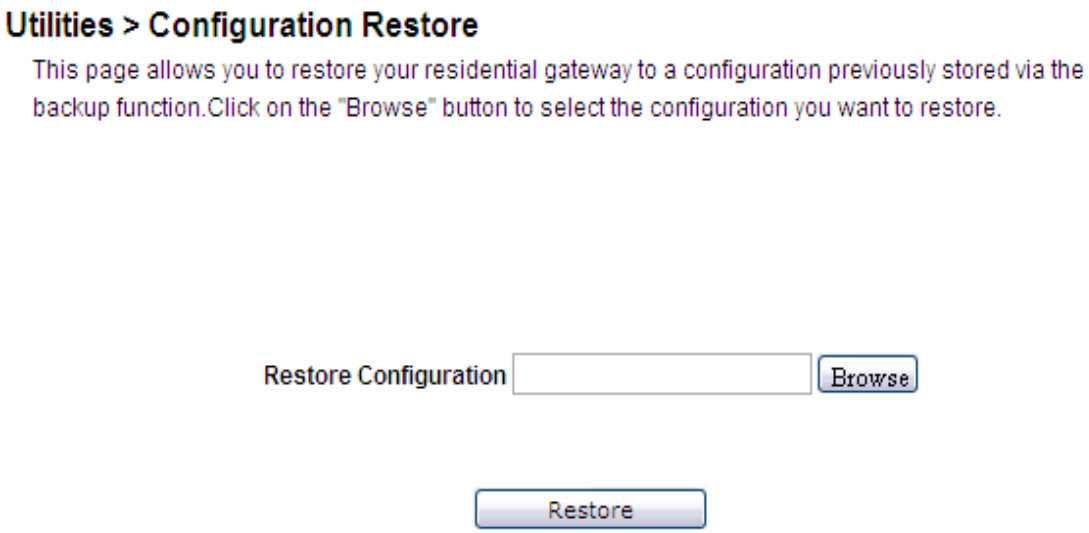


Table 11-1 describes the fields of the Configuration Restore window.

Table 11-1 Field descriptions

Field	Description
Restore Configuration	Click **Browse** and select a configuration backup file to restore.
Restore	Click to restore the configuration.

Firmware Upgrade

The Firmware Upgrade window enables you to update the firmware of the CellPipe 7130 RG.

WARNING

Do not turn off the power or disturb the system during firmware upgrade.

Select **Firmware Upgrade** in the **Utilities** menu to access the Firmware Upgrade window; see Figure 11-3.

Figure 11-3 Firmware Upgrade window

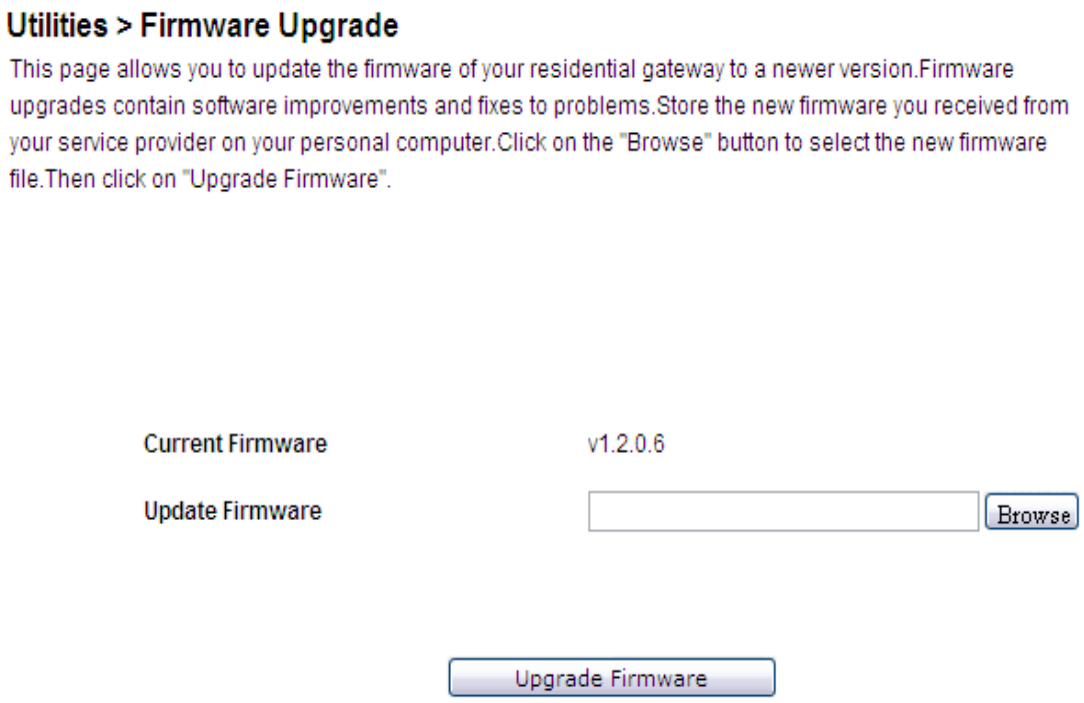


Table 11-2 describes the fields of the Firmware Upgrade window.

Table 11-2 Field descriptions

Field	Description
Update Firmware	Click **Browse** to locate and select the firmware upgrade file to upload. **Note:** Firmware upgrades are available at http://www.alcatel-lucent.com/wps/portal/support. You must obtain the upgrade file before uploading.
Upload Firmware	Click to upload the firmware update.

System Setting

The System Setting window enables you to change the web administrator username and password, and configure settings such as the time zone, NTP, and daylight savings.

Note: It is highly recommended that you change the administrator's default username and password and the Telnet default username and password for telnet.

Select **System Setting** in the **Utilities** menu to access the System Setting window; see Figure 11-4.

Figure 11-4 System Setting window

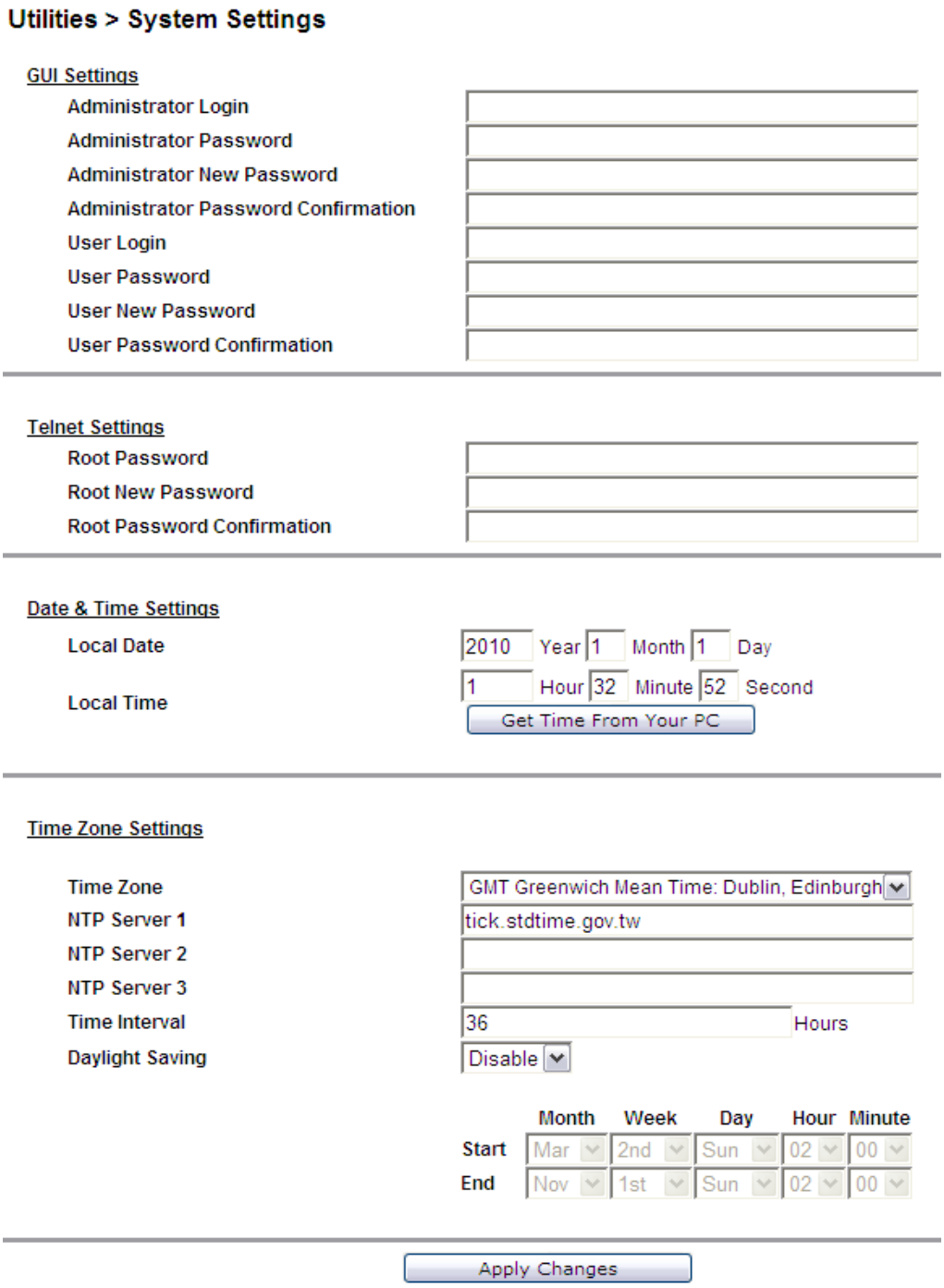


Table 11-3 describes the fields of the System Setting window.

Table 11-3 Field descriptions

Field	Description
GUI Setting	
Administrator Login	Enter a new username for administrator.

Field	Description
Administrator Password	Enter the current admin password. **Note:** If this is the first time the admin password is changed, the default admin password is **`admin`**.
Administrator New Password	Enter a new password.
Administrator Password Confirmation	Retype the new password to confirm.
User Login	Enter a new username for user.
User Password	Enter the current user password.
User New Password	Enter a new password.
User Password Confirmation	Retype the new password to confirm.
Telnet Setting	
Root Password	Enter the current Telnet root password. **Note:** If this is the first time the root password is changed, the default root password is **`admin`**.
Root New Password	Enter a new password.
Root Password Confirmation	Retype the new password to confirm.
Date & Time Setting	
Local Date	Displays the current date according to the time zone configuration.
Local Time	Displays the current time according to the time zone configuration.
Time Zone Settings	
Time Zone	Select your time zone.
NTP Server 1 to 3	Enter the IP address or URL of the network time protocol server.
Time interval	Enter an interval time in hours.
Daylight Saving	Select **Enable** to turn on daylight savings. Select **Disable** to turn off daylight savings.
Start/End	If you have enabled daylight savings, select the **Month**, **Week**, **Day**, **Hour**, and **Minute** for the daylight savings to start and end.
Apply Changes	Click to save your changes.

Management Access Control

The Management Access Control window enables you to control who can access the service provided by the gateway.

Note: It is recommended that you consult your ISP before configuring the access.

Select **Management Access Control** in the **Utilities** menu to access the Management Access window; see Figure 11-5.

Figure 11-5 Management Access Control window

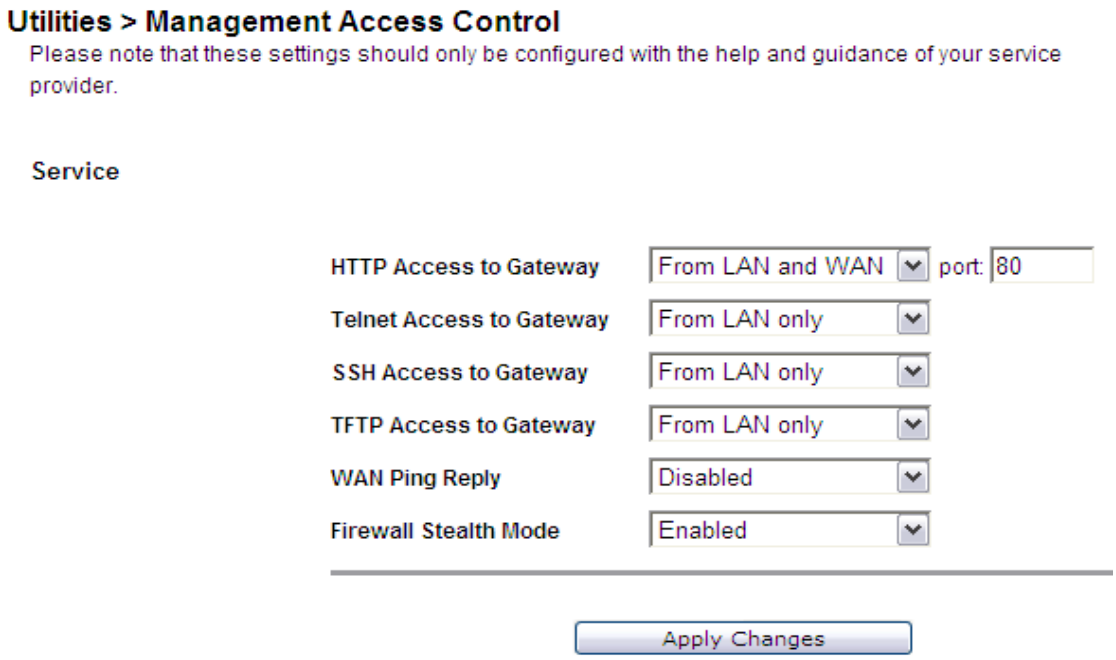


Table 11-4 describes the fields of the Management Access window.

Table 11-4 Field descriptions

Field	Description
HTTP Access to Gateway Telnet Access to Gateway SSH Access to Gateway TFTP Access to Gateway	Select one of the following settings: • **Disable** • **From LAN only** • **From WAN only** • **From LAN and WAN**
WAN Ping Reply	Select **Enable** to allow the WAN interface to respond to the ICMP request from the Internet. Select **Disable** to deny the WAN interface from responding to the ICMP request from the Internet.

Field	Description
Firewall Stealth Mode	Select **Enable** to allow firewall to drop all Stealth or unknown traffic. Select **Disable** to accept all unknown traffic.
Apply Changes	Click to save your changes.

CWMP Management

The CWMP Management window enables you to configure remote access of the CellPipe 7130 RG.

Select **CWMP Management** in the **Utilities** menu to access the CWMP Management window; see Figure 11-6.

Figure 11-6 CWMP Management window

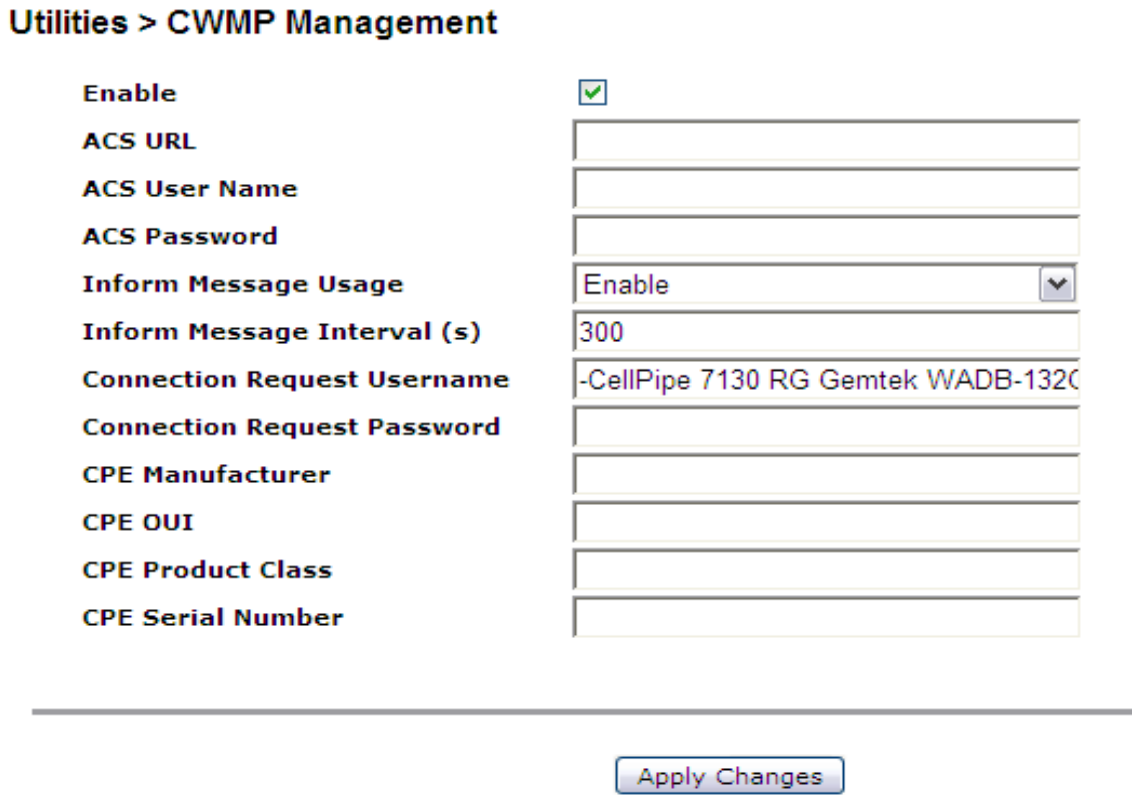


Table 11-5 describes the fields of the CWMP Management window.

Table 11-5 Field descriptions

Field	Description
ACS (Auto-Configuration Server) URL	Enter the URL of the auto-configuration server.

Field	Description
ACS User Name	Enter the username of the auto-configuration server.
ACS Password	Enter the password for the auto-configuration server.
Inform Message Usage	Select **Enable** to have the device information sent to the auto-configuration server. Select **Disable** not to send the information to the auto-configuration server.
Inform Message Interval (s)	Enter an interval of sending inform message in seconds.
Connection Request Username	Enter the username for the connection request of the auto-configuration server to the device.
Connection Request Password	Enter the password for the connection request of the auto-configuration server to the device.
CPE Manufacturer	The manufacturer of the device.
CPE OUI	The organizational unique identifier of the device.
CPE Product Class	The model of the device.
CPE Serial Number	The serial number of the device.
Apply Changes	Click to save your changes.

Connection Test

The Connection Test screen enables you to test the connectivity with other network devices.

Select **Connection Test** in the **Utilities** menu to access the Connection Test window; see Figure 11-7.

Figure 11-7 Connection Test window

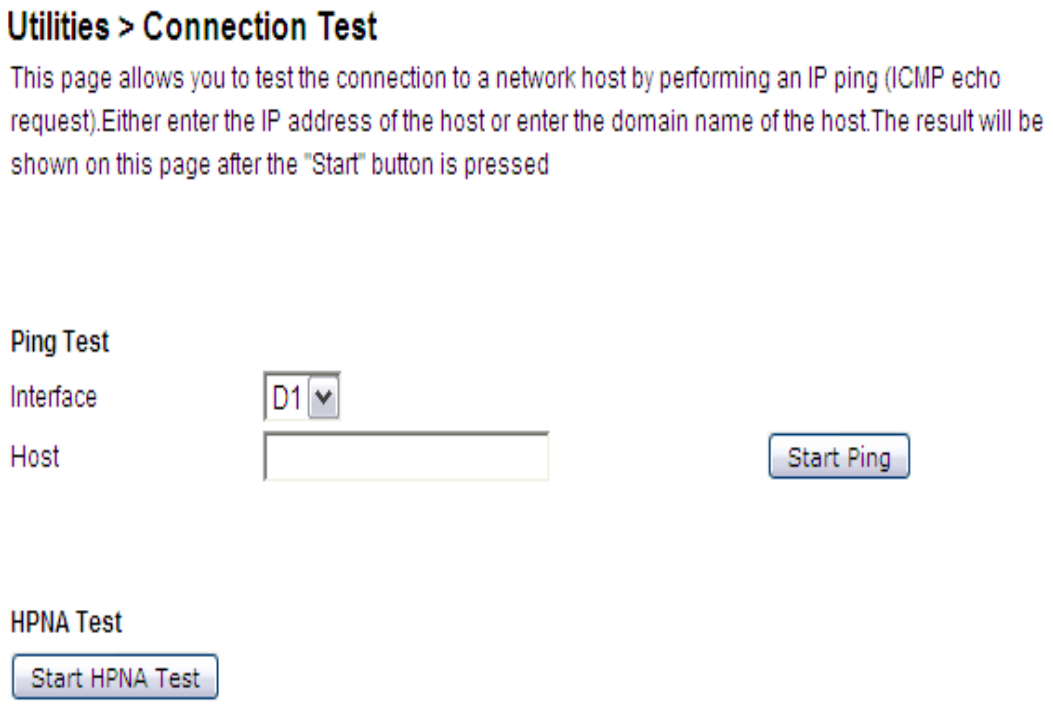


Table 11-6 describes the fields of the Connection Test window.

Table 11-6 Field descriptions

Field	Description
Interface	From the drop-down menu, select a connection to test if the connection is working properly.
Host	Please enter an IP address to test the connection.
Start Ping	Click **Start Ping** to test the connection.
Start HPNA Ping (Only for 6Vz.A4111)	Click **Start HPANA Ping** to test the connection by HPNA.

802.1x CA Upload

The 802.1x CA upload enables you to upload 802.1x CA certificate. If you enabled a DHCP WAN connection with 802.1x enabled.Then you can use this Utility to uploaded a CA that will be used to authenticate with your ISP and get DHCP service.

Select **802.1x CA Upload** in the **Utilities** menu to access the 802.1x CA Upload window; see Figure 11-8.

Figure 11-8 802.1x CA Upload window

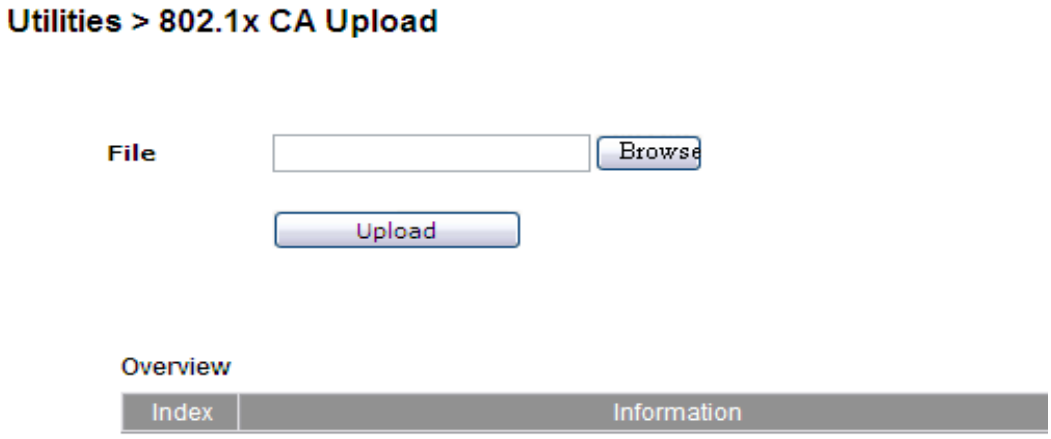


Table 11-7 describes the fields of the 802.1x CA Upload window.

Table 11-7 Field descriptions

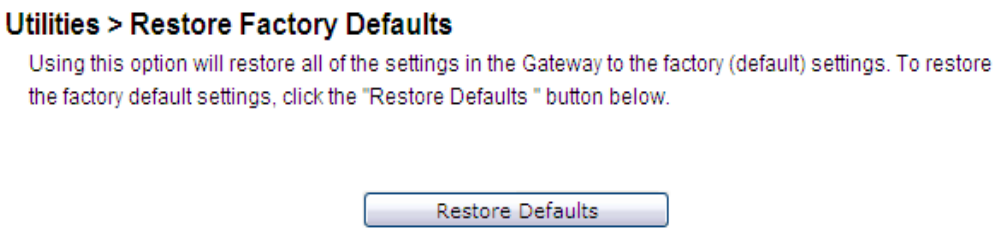
Field	Description
File	Click Browse to select a CA certificate on your computer to upload.
Upload	Upload the selected CA certificate.
Index	Index number of CA certificate. (Maximum of 8 CA certificates are supported.)
Information	Information of the CA certificate.

Restore Factory Defaults

The Restore Factory Defaults window enables you to restore the default settings to the CellPipe 7130 RG.

Select **Restore Factory Defaults** in the **Utilities** menu to access the Restore Factory Defaults window; see Figure 11-9.

Figure 11-9 Restore Factory Defaults window



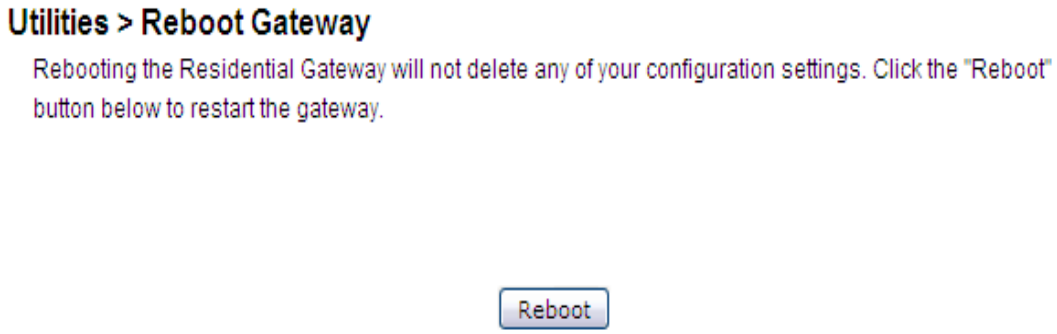
Click on **Restore Defaults** to restore the CellPipe 7130 RG to the factory default settings.

Reboot Gateway

The Reboot Gateway window enables you to reboot the CellPipe 7130 RG. Rebooting the gateway does not reset your settings.

Select **Reboot Gateway** in the **Utilities** menu to access the Reboot Gateway window; see Figure 11-10.

Figure 11-10 Reboot Gateway window



Click on **Reboot** to restart the CellPipe 7130 RG.

12 Telephony

Overview

The CellPipe 7130 RG Telephony menu enables you to configure the settings for your VoIP account and view the calling log.

Click the **Telephony** drop-down menu to open the **Telephony** menu.

Contents

This chapter covers the following topics.

Account Setup

Your VoIP account settings can be configured here.

> **Note:** Some account information, such as the phone number and username, is provided by your VoIP service provider. Please have all the provided information handy when configuring your accounts.

Select **Account Setup** in the **Telephony** menu to access the Account Setting window; see Figure 12-1.

Figure 12-1 Account Setup window

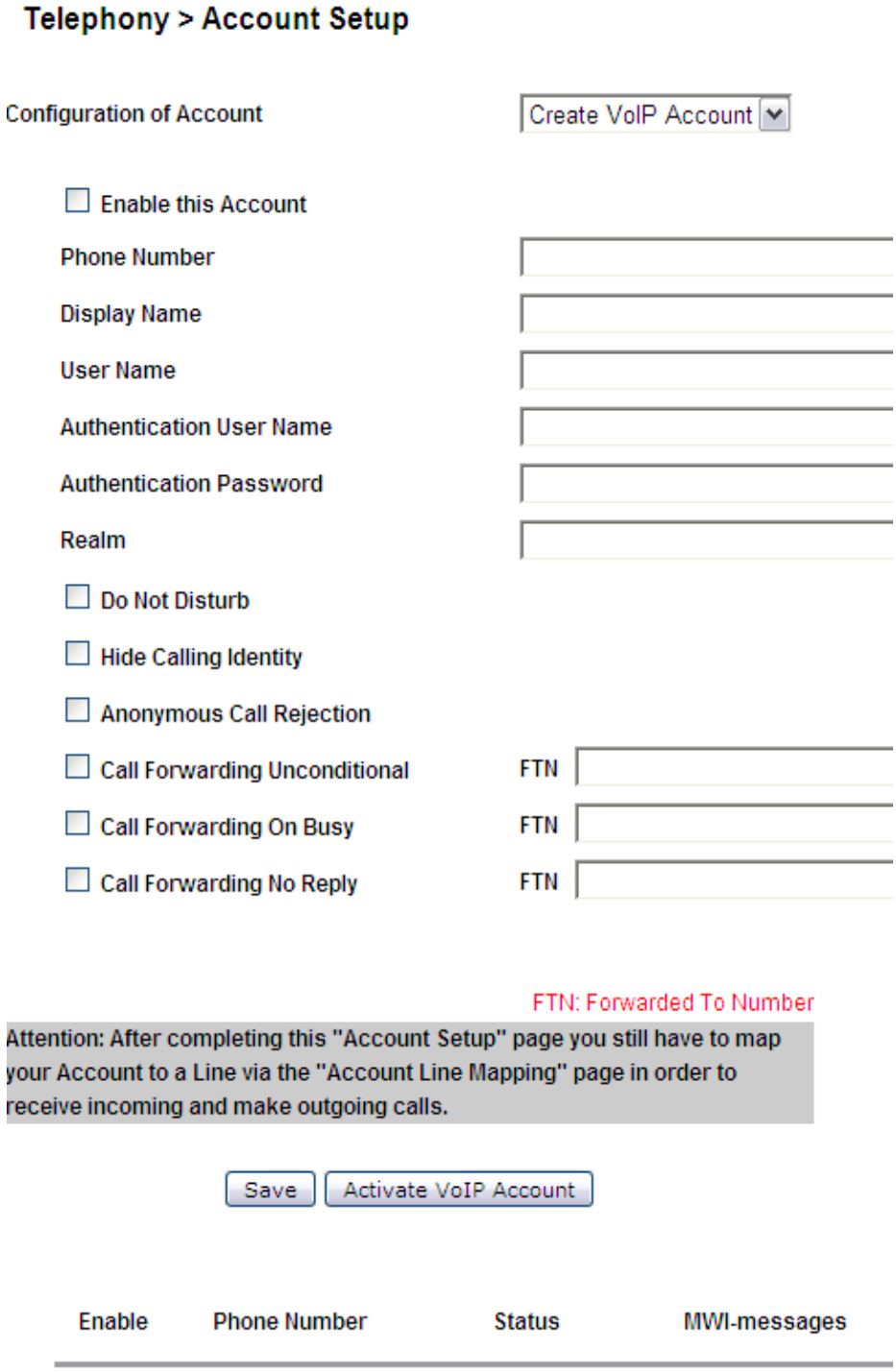


Table 12-1 describes the fields of the Account Setup window.

Table 12-1 Field descriptions

Field	Description
Configuration of Account	Select to configure a VoIP account.

Field	Description
Enable this Account	Enable the check box to enable the account registered to the SIP of the VoIP service provider.
Phone Number	Enter the account's phone number.
Display Name	Enter the display name for the account.
User Name	Enter the user name for the account.
Authentication User Name	Enter the account's username.
Authentication Password	Enter the username's password.
Don't Disturb	Check this checkbox to enable this service. When this service is enabled all incoming phone calls for this number will be blocked i.e. the phone will not ring.
Hide Calling identity	Check this to hide your account's information to the caller.
Anonymous Call Rejection	Check this to reject phone call with anonymous number.
Call Forwarding Unconditional	Check this and enter a phone number to be forwarded to under any circumstances.
Call Forwarding On Busy	Check this and enter a the phone number to be forwarded to when the line is busy.
Call Forwarding No Reply	Check this and enter a phone number to be forwarded to when the phone is not answered.
Save	Click to save your changes.
Activate VoIP Account	Click to register your account with your VoIP service provider.

Service Settings

The Service Settings window enables you to configure advanced settings for the VoIP accounts such as call waiting and third party conference call.

Note: Changes made to the service settings apply to all VoIP accounts.

It is recommended that you contact your VoIP service provider for assistance with configuring the service settings. Depending on your account, some features might not be available.

Select **Service Settings** in the **Telephony** menu to access the Service Setting window; see Figure 12-2.

Figure 12-2 Service Settings window

Telephony > Service Settings

Hide Calling Identity (Per Call)

Service Code
Invoke *67DN#
DN: Directory Number

Call Waiting

☑ Active
CW Alerting Timer 15 Sec
Service Code
Activate *70
DeActivate #70
Interrogate

3 Party Conference

☑ Active

Message Wait Indication

☑ Active
Notify Method ◉ Unsolicited Notify
○ Solicited Subscribe/Notify; Expiration Time 3600 Sec
Reminder Notification ☑ Stutter Dial Tone
☑ Visual "Message" LED

Hot Line/Warm Line

☐ Active
Warm Line Timer 0 Sec
Hot Line destination
Warm Line destination
Service Code
Activate *53DN#
DeActivate #53
Interrogate
DN: Directory Number

Session Timer

☑ Active
Default Session Expire 1800 Sec
Minimal Session Expire 90 Sec
Refresh Method INVITE
Refresh Preference NONE

Do Not Disturb

Service Code
Activate *26
DeActivate #26
Interrogate

Anonymous Call Rejection

Service Code
Activate *77
DeActivate #77
Interrogate

Call Forwarding

☐ Enable Splash Ring
Unconditional Service Code
Activate *72FTN#
DeActivate #72
Interrogate
On Busy Service Code
Activate *90FTN#
DeActivate #90
Interrogate
No Reply Service Code
No Reply Timer 20 Sec
Activate *92FTN#
DeActivate #92
Interrogate
FTN: Forwarded To Number

Save Cancel

Table 12-2 describes the fields of the Service Setting window.

Table 12-2 Field descriptions

Field	Description
Hide Calling Identity (Per call)	The activation code for hiding your account's information when making a call.
Call Waiting	Check **Active** to enable the call waiting feature.
Call Waiting Alerting Timer	Select a time interval for the call waiting alert.Default value is 15 seconds.
Activation Code	The activation code for your call waiting service.
Deactivation Code	The deactivation code for your call waiting service.
Interrogate Code	The interrogate code for your call waiting service.
3 Party Conference	Check **Active** to enable the conference call.
Message Wait Indication	Check **Active** to turn on the message wait indicator which enables your phone to give you a notification alert when you have a voice message. Select one of the following as your MWI method: • **Unsolicited Notify**: The RG is able to receive unsolicited "message wait" NOTIFY messages. No SUBSCRIBE is used. • **Solicited Subscribe/Notify**: The RG will initiate a SUBSCRIBE/NOTIFY dialogue in which "message wait" NOTIFY messages will be received. Enter the number of seconds that your VoIP service should provide. It is the expire time in seconds of your subscription to the voicemail service. The SIP user agent will refresh this subscription automatically before this timer runs out.
	Enable one of the following as the message wait indication: • **Stutter Dial Tone** • **Visual "Message" LED** If Stutter Dial Tone is selected, the alert is set as a dial tone. If Reminder Visual Message LED is selected, the alert is set as a blinking LED (Message LED).
Hot Line/Warm Line	Check **Active** to enable hot line and warm line feature.
Warm Line Timer	Select a time period from the drop down menu. Warm line will be activated after the timer has expired.
Hot Line destination	Enter a phone number for as hot line's destination. When hot line is activated, putting the phone on-hook will automatically makes a call to the hot line's destination.

Field	Description
Warm Line destination	Enter a phone number for as warm line's destination. When warm line is activated, putting the phone on-hook will automatically makes a call to the warm line's destination after the warm line timer has expired.
Active Code	The activation code for your "Hot Line/Warm Line" service.
Deactivate Code	The deactivation code for your "Hot Line/Warm Line" service.
Interrogate Code	The interrogate code for your "Hot Line/Warm Line" service..
Session Timer	Check **Active** to enable session timer. When session timer is enabled, the RG will periodically send a refresh message to refresh the session.
Default Session Expire	Enter the number of seconds to refresh the session.Default value is 1800, and the minimum value is 90.
Minimal Session Expire	Enter the number of seconds as the minimal session expire. This value will be the minimum refresh timer you can accept from the caller.
Refresh Method	Select INVITE or UPDATE from the drop-down menu. This will be the type of message to send for refreshing session.
Refresh Preference	Select a refresher preference from the drop-down menu. Select NONE to let RG decide. Select UAC to let caller refresh the session. Select UAS to let caller refresh the session.
Do Not Disturb	
Active Code	The activation code for your "Don't Disturb" service.
Deactivate Code	The deactivation code for your "Don't Disturb" service.
Interrogate Code	The interrogate code for your "Don't Disturb" service..
Anonymous Call Rejection	
Active Code	The activation code for your "Anonymous Call Rejection" service.
Deactivate Code	The deactivation code for your "Anonymous Call Rejection" service.
Interrogate Code	The interrogate code for your "Anonymous Call Rejection" service..
Call Forwarding	
Enable Splash Ring	Check this item to remind you have a call still holding on line.

Field	Description
Unconditional Service Code	
Activate	The activation code for your “Unconditional Call Forwarding” service.
Deactivate	The deactivation code for your “Unconditional Call Forwarding” service.
Interrogate	The interrogate code for your “Unconditional Call Forwarding” service..
On Busy Service Code	
Activate	The activation code for your “On Busy Call Forwarding” service.
Deactivate	The deactivation code for your “On Busy Call Forwarding” service.
Interrogate	The interrogate code for your “On Busy Call Forwarding” service.
No Reply Service Code	
No Reply Timer	The time in seconds that the incoming call should wait before being forwarding. The default value is 20 seconds.
Activate	The activation code for your “No Reply Call Forwarding” service.
Deactivate	The deactivation code for your “No Reply Call Forwarding” service.
Interrogate	The interrogate code for your “No Reply Call Forwarding” service.
Save	Click to save your changes.
Cancel	Click to cancel your changes.

SIP Server Settings

The SIP Server Setting window enables you to configure the session initiated protocol (SIP) settings for the VoIP accounts.

Note: It is recommended that you contact your VoIP service provider for assistance with configuring the server settings.

Select **SIP Server Setting** in the **Telephony** menu to access the Server Setting window; see Figure 12-3.

Figure 12-3 SIP Server Setting window

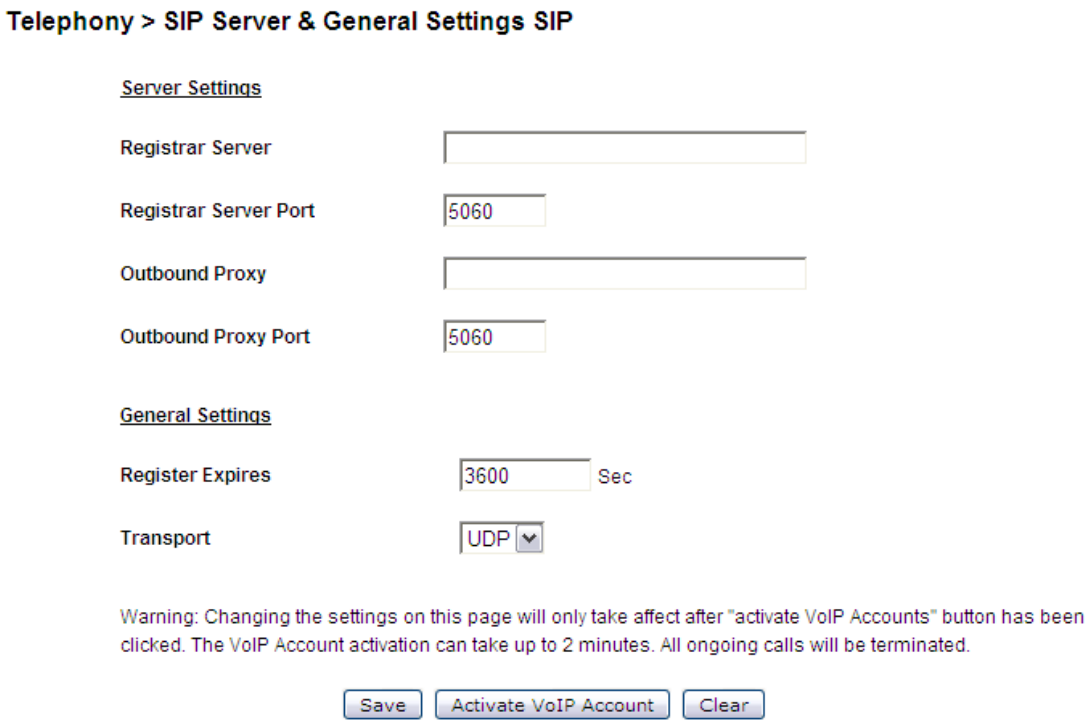


Table 12-3 describes the fields of the Server Setting window.

Table 12-3 Field descriptions

Field	Description
Registrar Server	Enter the location of the SIP registration server.
Registrar Server Port	Enter the port number of the SIP registration server.
Outbound Proxy	Enter the location of the outbound proxy server.
Outbound Proxy Port	Enter the port number of the outbound proxy server.
Register Expires	Enter the number of seconds that your SIP account is registered with the SIP registrar server before it is deleted. The default value is 3600 seconds.
Transport	Please select either UDP or TCP protocol for your transportation.
Save	Click to save your changes.
Activate VOIP Account	Click to register your account with your VOIP service provider.
Clear	Click to clear your settings

RTP/Codec settings

The RTP/Codecs settings window allows you to setup the codecs and ports for your voice traffic.

Select **RTP/Codecs settings** in the **Telephony** menu to access the RTP/Codecs window; see Figure 12-4.

Figure 12-4 RTP/Codecs window

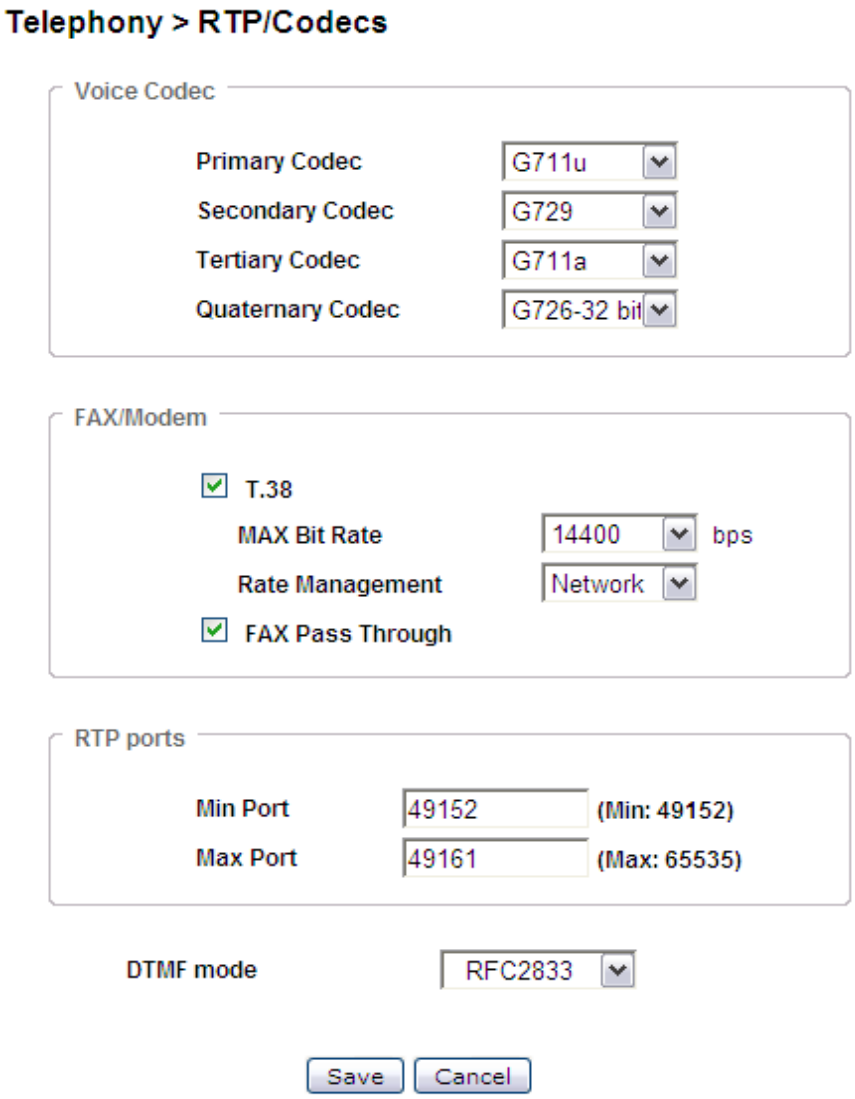


Table 12-4 describes the fields of the RTP/Codecs Settings window.

Table 12-4 Field descriptions

Field	Description
Primary Codec	A codec (coder/decoder) codes analog voice signals into digital signals and decodes the digital signals back into analog voice signals. Please select to give the priorities of your codec.
Secondary Codec	Please select to give the priorities of your codec.
Tertiary Codec	Please select to give the priorities of your codec.
Quaternary Codec	Please select to give the priorities of your codec.
T.38 Fax	Check T.38 to let the device send fax messages through IP networks.
Max Bit Rate	Please select the maximum bit rate in bits per second for your fax message.
Rate Management	Select the data rate management method. Local data rate management requires that the training signal be generated locally. Network data rate management requires that the training signal be transferred over network. Network is the default value.
FAX Pass Through	Select to allow Fax Pass Through method.
RTP Min Port	Enter the minimum port range of the RTP listening port.
RTP Max Port	Enter the maximum port range of the RTP listening port.
DTMF mode	Please indicate how your device should handle the tones that your telephone will make when you push the phone buttons.Please consult your VoIP service provider. RFC 2833: Sending the DTMF tones in RTP packets. PCM: Sending the DTMF tones in the voice data stream. SIP INFO: Sending the DTMF tones in SIP messages.
Save	Click to save the call statistics and call log.
Clear	Click to clear the call statistics and call log.

Account & Line Table

The Account & Line Table enables you to specify which VoIP accounts are associated with your phone ports/lines.

Select **Account & Line Table** in the **Telephony** menu to access the Call List window; see Figure 12-5.

Figure 12-5 Account & Line window

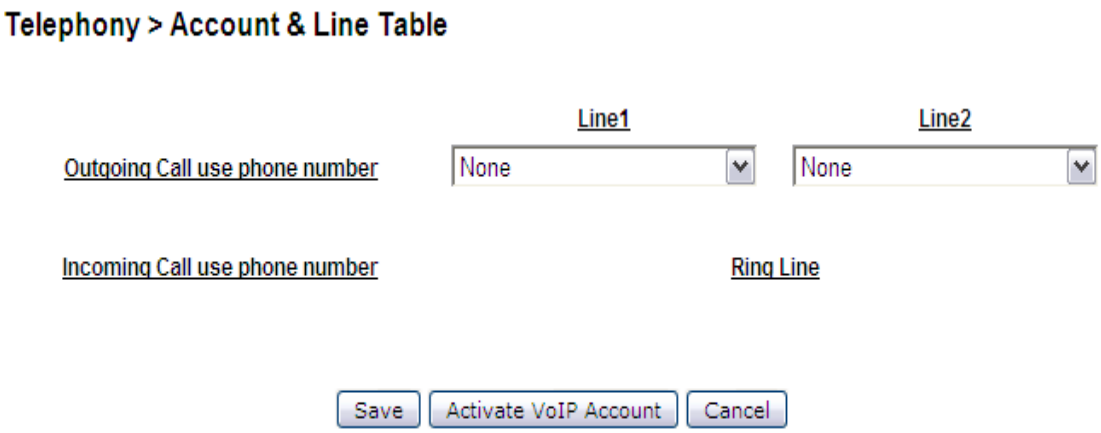


Table 12-5 describes the fields of the Account & Line Table window.

Table 12-5 Field descriptions

Field	Description
Outgoing call use phone number	Please select the VoIP accounts to be associated with phone 1 and phone 2.
Incoming call use phone number	Please select which phone port to be rung when your registered VoIP account(s) has received a call.
Save	Click to save your changes.
Activate VoIP Account	Click to register your account with your VoIP service provider.
Clear	Click to clear the call statistics and call log.

Call History

The Call List window displays the call statistics and call log of your VoIP accounts.

Select **Call History** in the **Telephony** menu to access the Call History window; see Figure 12-6.

Figure 12-6 Call History window

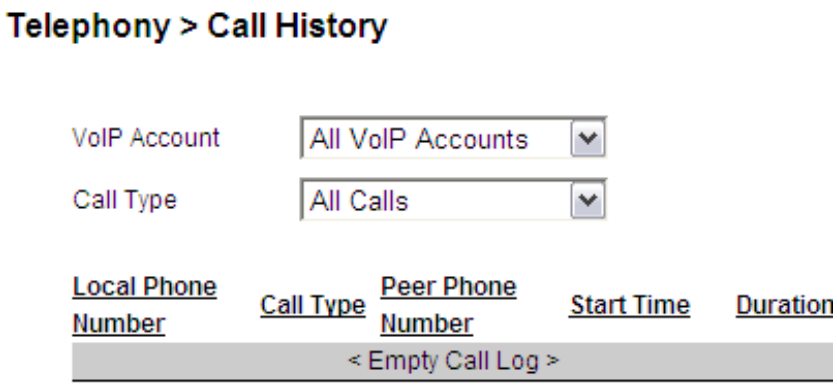


Table 12-6 describes the fields of the Call History window.

Table 12-6 Field descriptions

Field	Description
VoIP Account	Please select to display the call logs for the specified VoIP accounts.
Call Type	Please select to display the call logs for the specified Call Type. • **All Calls** • **Outgoing Calls** • **Answered Calls** • **Missed Calls**

Other Settings

The Other Settings window allows you to change the profile for various countries in order for that country's telephone to operate.

Select **Other Settings** in the **Telephony** menu to access the Other Setting window; see Figure 12-7.

Figure 12-7 Other Settings window

Telephony > CID Settings

Table 12-7 describes the fields of the Other Settings window.

Table 12-7 Field descriptions

Field	Description
Country	Select a country from the list. It will change ring cadence, impedance and DC feed settings to meet the requirements of that country. You must reboot the CellPipe 7130 RG for changes to take effect.
DTMF	Only one protocol is available, ETSI EN 300 659-1
CID	Choose between two different types of CID to specify how the CID are transmitted to the phone.Each CID type has its own protocols.
FSK	Choose between ETSI or Telecordia.
Save	Click to save your changes.

13 USB Service

Overview

This chapter explains how to setup USB devices on CellPipe 7130 RG.

Note: USB hub is also supported

Contents

This chapter covers the following topics:

File sharing

The CellPipe 7130 RG allows you to share files on USB storage devices. Use one of the procedures to configure USB file sharing:

- Access the USB device directly from a browser
- Access the USB device by setting a Network device

Access the USB device directly from browser

The following procedures explain how to access the USB device directly from a browser using Windows or Mac OS.

Windows

1. Plug the USB storage device into the CellPipe 7130 RG USB port.
2. Open a browser.
3. Enter **`\\192.168.2.1`** and press ↵

Note: The address 192.168.2.1 is your LAN management IP. It can be changed by user configuration.

END OF STEPS

Mac OS

1. Plug the USB storage device into the CellPipe 7130 RG USB port.
2. Open a browser.
3. Enter **`smb://192.168.2.1/`** and press ↵

   Note: The address 192.168.2.1 is your LAN management IP. It can be changed by user configuration.

END OF STEPS

Access the USB device by setting a Network device

The following procedures explain how to access the USB device by setting a Network device using Windows or Mac OS.

Windows

1. Plug the USB storage device into the CellPipe 7130 RG USB port.
2. Open **Window Network Neighborhood**.
3. Create a new network device by adding **`\\192.168.2.1`**.

   Note: The default address of your LAN management IP is 192.168.2.1. If you have changed the IP address, enter it instead.
4. Access the USB device by clicking on the newly created network device; see Figure 13-1.

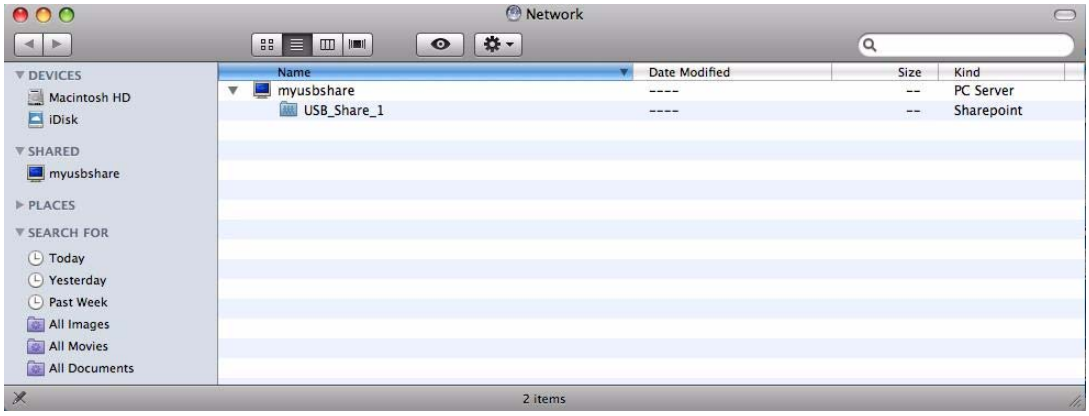
Figure 13-1 File sharing

END OF STEPS

Mac OS

1. Plug the USB storage device into the CellPipe 7130 RG USB port.
2. Open **Network** from the Control Panel named **Go**.
3. Access the USB device by clicking on the device below **myusbshare**; see Figure 13-2.

Figure 13-2 File sharing on Mac



END OF STEPS

Printer Server

CellPipe 7130 RG can also be a printer server. The configuration steps is described below:

Windows

1. Plug the USB printer into the CellPipe 7130 RG USB port.
2. Open **Windows setting**.
3. Under **Printer Tasks**, click **Add a printer** to open the Add Printer Wizard and then click **Next**.
4. Click **A network printer or a printer attached to another computer** and then click **Next**.
5. Click **Connect to a printer on the Internet or on your intranet**.
6. Enter the URL of the printer using the following format:
   `http://Gateway_IP_address:Printserver_port/printers/share_name`

   Here are the explanation for each field:

   Gateway_IP_address: see Table 6-2.

   Printserver_port: fixed to 631 by gateway.

   share_name: Please make a reference to Table 6-1 (where value can be configrued)

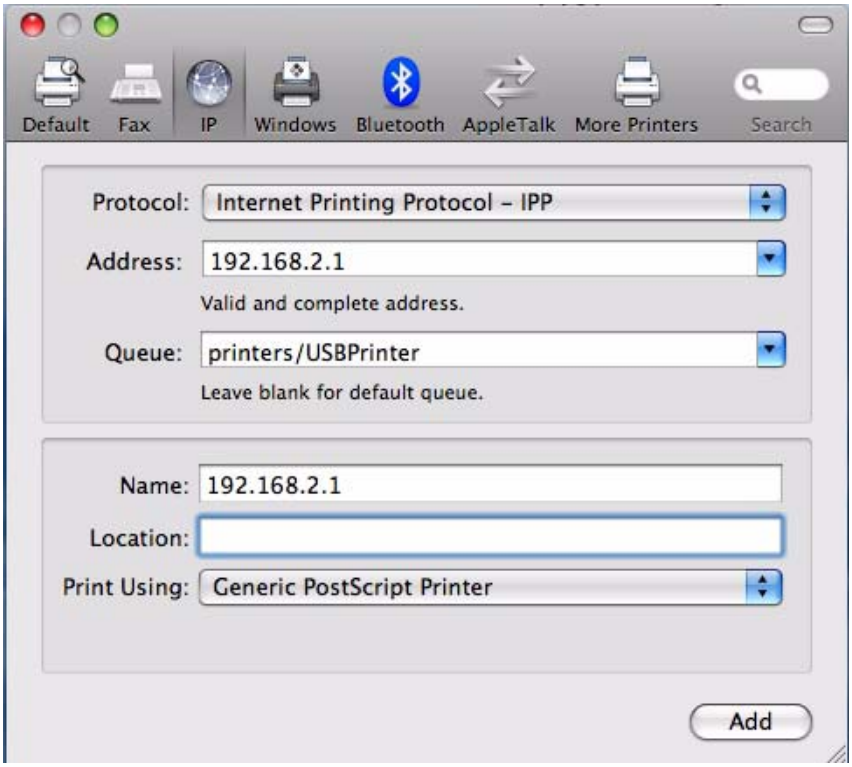
   By default the printer server will be:
   `http://192.168.2.1:631/printers/USBPrinter`
7. Follow the instructions on-screen to complete the setup of the network printer.

END OF STEPS

Mac OS

1. Plug the USB printer into the CellPipe 7130 RG USB port.
2. Open **System Preference** from the Panel.
3. Choose **Print & Fax** from **System Preference**.
4. Configure the settings as shown in Figure 13-3 and click **Add**.

Figure 13-3 Printer setting on Mac



END OF STEPS

14 FCC and IC Statement

Overview

This section lists the product conformance requirements.

Federal Communication Commission Interference Statement

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

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

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

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.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

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

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

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

FCC Part 68 Statement

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On the bass unit of this equipment is a label that contains, among other information, a product identifier in the format US: GEMDL01BWADB132GN. If requested, this number must be provided to the telephone company.

The REN is used to determine the number of devices that may be connected to a telephone line. Excessive RENs on a telephone line may result in the devices not ringing in response to an incoming call. In most but not all areas, the sum of RENs should not exceed five (5.0). To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. For products approved after July 23, 2001, the REN for this product is part of the product identifier that has the format US: GEMDL01BWADB132GN. The digits represented by 01 are the REN without a decimal point (e.g., 03 is a REN of 0.3). For earlier products, the REN is separately shown on the label.

If your equipment causes harm to the telephone network, the telephone company may discontinue your service temporarily. If possible, they will notify you in advance. But if advance notice is not practical, you will be notified as soon as possible. You will be informed of your right to file a complaint with the FCC. Your telephone company may make changes in its facilities, equipment, operations or procedures that could affect the proper functioning of your equipment. If they do, you will be notified in advance to give you an opportunity to maintain uninterrupted telephone service.

If you experience trouble with this telephone equipment, please contact the following address and phone number for information on obtaining service or repairs.

The telephone company may ask that you disconnect this equipment from the network until the problem has been corrected or until you are sure that the equipment is not malfunctioning.

This equipment may not be used on coin service provided by the telephone company. Connection to party lines is subject to state tariffs.

Company: Alcatel-Lucent

Address: 600-700 Mountain Avenue Murry Hill, NJ 07974

Tel no.: 1-908-508-8080

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. See installation instructions for details.

Industry Canada statement

This device complies with RSS-210 of the Industry Canada 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.

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionrement indésirable.

IMPORTANT NOTE:

Radiation Exposure Statement:

This equipment complies with Canada radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

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

NOTE IMPORTANTE: (Pour l'utilisation de dispositifs mobiles)
Déclaration d'exposition aux radiations:
Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

Le module émetteur peut ne pas être coïmplanté avec un autre émetteur ou antenne,

IC TELECOM

"NOTICE: This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment."

"NOTICE: The Ringer Equivalence Number (REN) for this terminal equipment is 01. The REN assigned to each terminal equipment 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 five."

« AVIS : Le présent matériel est conforme aux spécifications techniques d'Industrie Canadaapplicables au matériel terminal Cette conformité est confirmée par le numérod'enregistrement. Le sigle IC, placé devant le numéro d'enregistrement, signifie quel'enregistrement s'est effectué conformément à une déclaration de conformité et indique queles spécifications techniques d'Industrie Canada ont été respectées. Il n'implique pasqu'Industrie Canada a approuvé le matériel. »

« AVIS : L'indice d'équivalence de la sonnerie (IES) du présent matériel est de 01. L'IESassigné à chaque dispositif terminal indique le nombre maximal de terminaux qui peuvent êtreraccordés à une interface téléphonique. La terminaison d'une interface peut consister en unecombinaison quelconque de dispositifs, à la seule condition que la somme d'indicesd'équivalence de la sonnerie de tous les dispositifs n'excède pas 5. »

A Troubleshooting

Overview

This section identifies common problems that can arise during the use of the CellPipe 7130 RG and offers solutions. Most issues are identified by the LEDs on the front panel of the CellPipe 7130 RG.

Troubleshooting Table

Symptom	Possible cause	Solution
Power LED does not come on after power is switched on.	Outlet, power cord, or power adapter might be defective.	• Check the outlet by plugging in another electronic device. • Call the customer service number or return the device to the vendor.
VDSL Link LED flashes slowly after connection is established then it quickly stats to flash slowly again.	The DSL port on the gateway or the cable might be defective.	• Switch the power off and then switch the power on. • Verify that the cable is connected properly to the VDSL wall line and the DSL connector on the CellPipe 7130 RG.
LAN LED does not come on after connection is established.	The LAN port on the CellPipe 7130 RG , the network interface on the computer, or a network cable may be defective or not connected.	• Verify that the power of CellPipe 7130 RG and computer are switched on. • Ensure that the cable is plugged into the CellPipe 7130 RG and the device. • Check the network adapter or the cable connections for defects.

Symptom	Possible cause	Solution
Message LED is flashing.	A firmware upgrade is in progress.	• Verify that a firmware upgrade is in progress. • Wait until the firmware upgrade is finished.
Intenet LED is off.	Your CellPipe 7130 RG is unable to connect to the Internet or CellPipe 7130 RG is not power on.	• Verify that your CellPipe 7130 RG has configured WAN connections properly. • Verify that the power is switched on.

B Product conformance

Overview

This section lists the product conformance requirements for the EU.

EU declaration of conformity

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC:

- EN60950-1:2006+A11:2009

  Safety of Information Technology Equipment
- EN50385 : (2002-08)

  Product standard to demonstrate the compliance of radio base stations and fixed terminal stations for wireless telecommunication systems with the basic restrictions or the reference levels related to human exposure to radio frequency electromagnetic fields (110MHz - 40 GHz) - General public
- EN 300 328 V1.7.1: (2006-10)

  Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive
- EN 301 489-1 V1.8.1: (2008-04)

  Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements
- EN 301 489-17 V2.1.1 (2009)

  Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment; Part 17: Specific conditions for Broadband Data Transmission Systems

This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 – 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

cs Česky [Czech]	*[Jméno výrobce]* tímto prohlašuje, že tento *[typ zařízení]* je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
da Dansk [Danish]	Undertegnede *[fabrikantens navn]* erklærer herved, at følgende udstyr *[udstyrets typebetegnelse]* overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
de Deutsch [German]	Hiermit erklärt *[Name des Herstellers]*, dass sich das Gerät *[Gerätetyp]* in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
et Eesti [Estonian]	Käesolevaga kinnitab *[tootja nimi = name of manufacturer]* seadme *[seadme tüüp = type of equipment]* vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
en English	Hereby, *[name of manufacturer]*, declares that this *[type of equipment]* is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
es Español [Spanish]	Por medio de la presente *[nombre del fabricante]* declara que el *[clase de equipo]* cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
el Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ *[name of manufacturer]* ΔΗΛΩΝΕΙ ΟΤΙ *[type of equipment]* ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
fr Français [French]	Par la présente *[nom du fabricant]* déclare que l'appareil *[type d'appareil]* est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
it Italiano [Italian]	Con la presente *[nome del costruttore]* dichiara che questo *[tipo di apparecchio]* è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo *[name of manufacturer / izgatavotāja nosaukums]* deklarē, ka *[type of equipment / iekārtas tips]* atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo *[manufacturer name]* deklaruoja, kad šis *[equipment type]* atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
nl Nederlands [Dutch]	Hierbij verklaart *[naam van de fabrikant]* dat het toestel *[type van toestel]* in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
mt Malti [Maltese]	Hawnhekk, *[isem tal-manifattur]*, jiddikjara li dan *[il-mudel tal-prodott]* jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
hu Magyar [Hungarian]	Alulírott, *[gyártó neve]* nyilatkozom, hogy a *[... típus]* megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
pl Polski [Polish]	Niniejszym *[nazwa producenta]* oświadcza, że *[nazwa wyrobu]* jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
pt Português [Portuguese]	*[Nome do fabricante]* declara que este *[tipo de equipamento]* está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
sl Slovensko [Slovenian]	*[Ime proizvajalca]* izjavlja, da je ta *[tip opreme]* v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	*[Meno výrobcu]* týmto vyhlasuje, že *[typ zariadenia]* spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
fi Suomi [Finnish]	*[Valmistaja = manufacturer]* vakuuttaa täten että *[type of equipment = laitteen tyyppimerkintä]* tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
sv Svenska [Swedish]	Härmed intygar *[företag]* att denna *[utrustningstyp]* står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

Glossary

Numerics

10/100Base-T
The most widely used standard for Ethernet over twisted pair or copper-based computer networking. Runs at 10 Mb/s, 100 Mb/s, and 1000 Mb/s (1 Gb/s) respectively.

802.1 Q/P
The standard that allows multiple bridged networks to transparently share the same physical network link without leakage of information between networks.

A

ACS
Auto-Configuration Server

ALG
Application-Level Gateway

AP
Access Point

API
Application Programming Interface

C

CHAP
Challenge-Handshake Authentication Protocol

Codec
A device or computer program capable of encoding and/or decoding a digital data stream or signal.

CoS
Class of Service

CPE
Customer Premises Equipment

D

DDNS
Dynamic Domain Name System

DHCP
Dynamic Host Configuration Protocol

DMZ
Demilitarized Zone

DNS
Domain Name System

DSCP
Differentiated Services Code Point

DSL
Digital Subscriber Line

DTIM
Delivery Traffic Indication Message

Dynamic Routing
The capability of a system, through which routes are characterised by their destination, to alter the path that the route takes through the system in response to a change in conditions.

E

Ethernet
A family of frame-based computer networking technologies for local area networks (LANs).

F

Firewall
An integrated collection of security measures designed to prevent unauthorized electronic access to a networked computer system.

G

Gateway
A network node equipped for interfacing with another network that uses different protocols.

H

HTML
Hyper Text Markup Language

I

IP
Internet Protocol

IPSec
Internet Protocol Security

ISP
Internet Service Provider

K

kb/s
Kilobit per second; a data rate unit.

L

L2TP
Layer 2 tunneling protocol; a tunneling protocol used to support virtual private networks (VPNs).

LAN
Local Area Network

M

MAC
Media Access Control

Mb
Megabit; a unit of information commonly used to express the rate data is transferred.

MTU
Maximum Transmission Unit

N

NAT
Network Address Translation

Netmask
The designated IP address routing prefix for a network of computers and devices.

NIC
Network Interface Controller

NTP
Network Time Protocol

O

OUI
Organizationally Unique Identifier

Outbound Proxy Server
The server responsible for handling calls made behind the NAT device by examining and translating the IP addresses.

P

PAP
Password Authentication Protocol

Ping
A computer network tool used to test whether a particular host is reachable across an IP network.

PPPoE
Point-to-Point Protocol over Ethernet

PPTP
Point-to-Point Tunneling Protocol

PSK
Pre-Shared Key

Q

QoS
Quality of Service

R

RJ-11
A physical interface often used for terminating telephone wires.

RJ-45
Most regularly used as an Ethernet connector. RJ-45 connectors are typically used to terminate twisted pair cable.

RTP
Real-time Transport Protocol; handles voice data transfer making VOIP call using SIP.

S

SSH
Secure Shell

SIP
Session Initiation Protocol; an application layer control protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet.

SSID
Service Set Identifier

Subnet
See *Netmask*.

T

TCP
Transmission Control Protocol

Telnet
Telecommunications network; a network protocol used on the internet or local area network (LAN) connections.

TFTP
Trivial File Transfer Protocol

ToS
Type of Service

U

UDP
User Datagram Protocol

UPnP
Universal Plug and Play

URL
Uniform Resource Locator

V

VDSL
Very High Bitrate Digital Subscriber Line

VLAN
Virtual Local Area Network

VoIP
Voice over Internet Protocol

W

WAN
Wide Area Network

WDS
Wireless Distribution System

WEP
Wired Equivalent Privacy

WiFi
Wireless networking compatibility

WLAN
Wireless Local Area Network

WPA
WiFi Protected Access

WPS
WiFi Protected Setup