



# CellPipe 7130 VDSL Residential Gateway 500V series

7130 RG 5Ve.A2000 and 7130 RG 5Ve.B2000

USER MANUAL

401-389-004

MAY 2008  
ISSUE 1

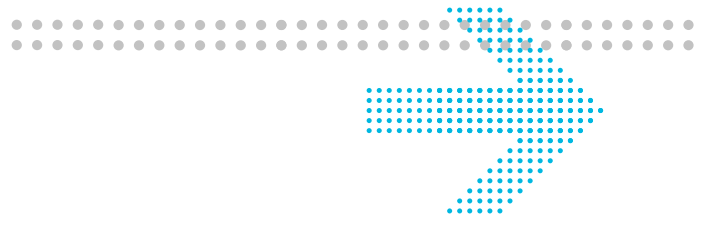
Alcatel, Lucent, Alcatel-Lucent and the Alcatel-Lucent logo are trademarks of Alcatel-Lucent. All other trademarks are the property of their respective owners..

The information presented is subject to change without notice. Alcatel-Lucent assumes no responsibility for inaccuracies contained herein.

Copyright © 2008 Alcatel-Lucent. All Rights Reserved.

**Conformance statements**

The device complies with Part 68 of the Federal Communications Commission (FCC) statements, Japan VCCI Class B, and the requirements of the Council Directive 89/336/EEC on the Approximation of the laws of the member states relating to Electromagnetic Compatibility and 72/23/EEC for electrical equipment used within certain voltage limits and the Amendment Directive 93/68/EEC as stated in the CE Mark Declaration of Conformance for EMI and Safety.



# Contents

## About this document

Purpose .....	v
Reason for revision .....	v
Intended audience .....	v
Supported systems .....	v
How to use this document .....	v
Safety information .....	vi
Conventions used .....	vi
Eco-environmental statements .....	vii
Technical support .....	vii
How to order .....	vii
How to comment .....	viii

## 1 Quick Installation Guide (QIG)

Hardware description .....	1-2
Install the CPE .....	1-5

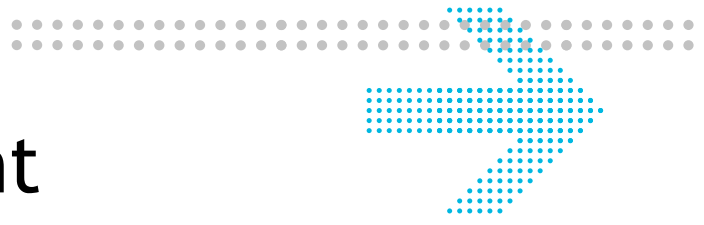
## 2 Web Management Interface

The Web Management Interface .....	2-3
Access to Web Management Interface via Internet browser .....	2-5
Retrieve Status .....	2-7
LAN Settings .....	2-9
WiFi Settings .....	2-12
Security Mode configuration .....	2-15
Wi-Fi MAC .....	2-17
WiFi QoS .....	2-19
Advanced Setup .....	2-23
DHCP .....	2-24
PPPoE Settings .....	2-26
VLAN + 2PPPoE Settings .....	2-28
Bridge Settings .....	2-30
Route Setting .....	2-32
Bridge MAC Filter .....	2-34

---

DDNS Setting .....	2-36
Port Range Forwarding .....	2-38
Virtual Server Basic .....	2-40
Virtual Server Advance .....	2-42
DMZ and UPnP .....	2-44
Filter .....	2-47
NAT Passthrough .....	2-49
QoS Setup .....	2-51
Default QoS .....	2-54
QoS Policy .....	2-56
QoS Interface Policy .....	2-58
QoS ALG .....	2-60
Reboot Gateway .....	2-62
Restore Factory Defaults .....	2-64
Web Firmware Upload .....	2-66
System Settings .....	2-68
MCL Settings .....	2-70

- A Troubleshooting**
- B Configuring the TCP/IP protocols on the PC**
- C Product conformance**



# About this document

## Purpose

The purpose of the *User Manual* is to provide installation information, procedures for installation, service activation and system reconfiguration for the 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000 VDSL2 gateway. Additionally the *User Manual* contains status indicators and troubleshooting information and a comprehensive description of safety guidelines.

## Reason for revision

This version 1.0 of the *User Manual* is the first issue.

## Intended audience

The intended audience of the *User Manual* primarily is for individuals who install, configure and maintain this customer premises equipment (CPE) and in addition responsible for the supervision of transmission operation.

## Supported systems

For the 7130 RG 5Ve.A2000 or 7130 RG 5Ve.B2000 VDSL2 gateway operation as described in this manual, a specific hardware consists of the following components is required:

- One 7130 RG 5Ve.A2000 or 7130 RG 5Ve.B2000 VDSL2 gateway
- One standard telephone cable (1.8 m)
- One category 5 UTP network cable (1.5 m)
- One power adapter
- One cradle for stand-up mounting
- Quick Installation Guide
- User Manual on CD-ROM.

## How to use this document

Each chapter of this *User Manual* treats a specific aspect of the 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000 VDSL2 gateway. This ensures that the reader can inform himself according to his special needs. This also means that the *User Manual* provides more

---

information than needed by many of the readers. Before you start reading the manual, it is therefore necessary to assess which aspects or chapters will cover the individual area of interest.

The following information is provided in this information product:

- Quick Installation Guide (QIG)
- Install the CPE
- The Web Management Interface
- Access to Web Management Interface via Internet browser
- Configure the CPE by using the Web Management Interface
- Guidance for troubleshooting
- Configuring the TCP/IP protocols on the PC.

## Safety information

**Important!** The following information lists the safety reminders for installation and maintenance personnel.

Read all instructions before attempting to unpack, install, operate, or connect power to this CPE. Please remember the following when you unpack and install this equipment:

- Always follow basic safety precautions to reduce the risk of fire, electrical shock and injury.
- To prevent fire or shock hazard, do not expose the CPE to rain, moisture or install this equipment near water. Never spill any form of liquid on or into this product.
- Do not insert any sharp object into the products module openings or empty slots. Doing so may accidentally damage its parts.
- Do not attach the power supply cable on building surfaces or floorings. Rest the power cable freely without any obstacle or heavy items piled on top of it. Refrain from abusing, stepping or walking on the cable.
- To protect the equipment from overheating, do not block the slots and openings in the module housing that provide ventilation.
- Exercise caution when installing or modifying telephone lines. Never install telephone wiring during inclement weather conditions (i.e., storm).
- Electrostatic discharge (ESD) can permanently damage semiconductor devices. Always follow ESD-prevention guidelines for equipment handling and storage.

## Conventions used

**Important!** Introduces important additional information.

**CAUTION:** Warns that a failure to follow the recommended procedure could result in loss of data or damage to equipment.

**WARNING:** Warns that a failure to take appropriate safety precautions could result in physical injury. In addition it warns of danger of electrical shock.

---

## Eco-environmental statements

The statements that follow are the eco-environmental statements that apply to 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000 products.

Countries, states, localities, or other jurisdictions may require that systems be established for the return and/or collection of packaging waste from the consumer, or other end user, or from the waste stream. Additionally, reuse, recovery, and/or recycling targets for the return and/or collection of the packaging waste may be established.

For more information regarding collection and recovery of packaging waste within specific jurisdictions, please contact the Alcatel-Lucent Technologies Field Services/Installation or Environmental Health and Safety organization.

## Technical support

To obtain technical support, contact your local sales representative or use the Online Customer Support (OLCS) (<https://support.lucent.com>).

## How to order

To order Alcatel-Lucent documents, contact your local sales representative or Alcatel-Lucent Customer Information Center (CIC) as follows:

- For mail order

**Alcatel-Lucent Customer Information Center**  
**7525 E. 39th Street**  
**Ste. 1100**  
**Indianapolis, IN 46226-5157**

- For telephone order

**888-582-3688** (toll free in the United States)  
**1-317-377-8617** (direct dial and outside the United States)

- For Fax order

**800-566-9568** (toll free in the United States)  
**1-317-377-8616** (direct dial and outside the United States)

- For credit card orders

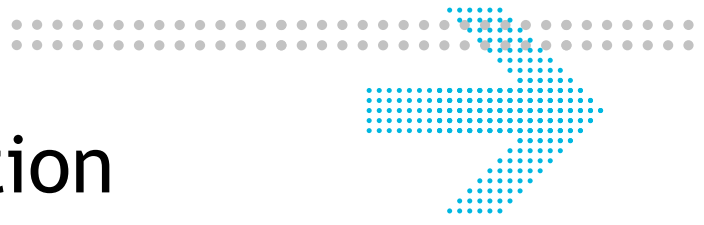
**800-744-7755** (toll free in the United States)  
**1-317-377-8619** (direct dial and outside the United States)

## How to comment

To comment on this information product, go to the [Online Comment Form](http://www.lucent-info.com/comments/) (<http://www.lucent-info.com/comments/>) or e-mail your comments to the Comments Hotline ([comments@alcatel-lucent.com](mailto:comments@alcatel-lucent.com)).







# 1 Quick Installation Guide (QIG)

## Overview

### Purpose

This Quick Installation Guide provides information about how to install the 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000 at the customers premises, which may be apartment blocks, hotels or office complexes.

This customer premises equipment (CPE) supports Ethernet-over-VDSL2 via four Ethernet data link rated up to 100 Mbps symmetrically. With its bridge functionality, it connects any device equipped with a 10BASE-T or 100BASE-TX network interface card via a standard telephone cable to a VDSL switch. Additionally the CPE provides a WLAN connection for client computers. For this purpose, it provides:

- One VDSL port
- Four Ethernet LAN ports (10/100BASE-TX)
- WLAN link for wireless network.

### Reason for revision

The version 1.0 of the Quick Installation Guide is the first issue.

### Contents

This chapter covers these topics.

<a href="#">Hardware description</a>	1-2
<a href="#">Install the CPE</a>	1-5

---

# Hardware description

## Package content

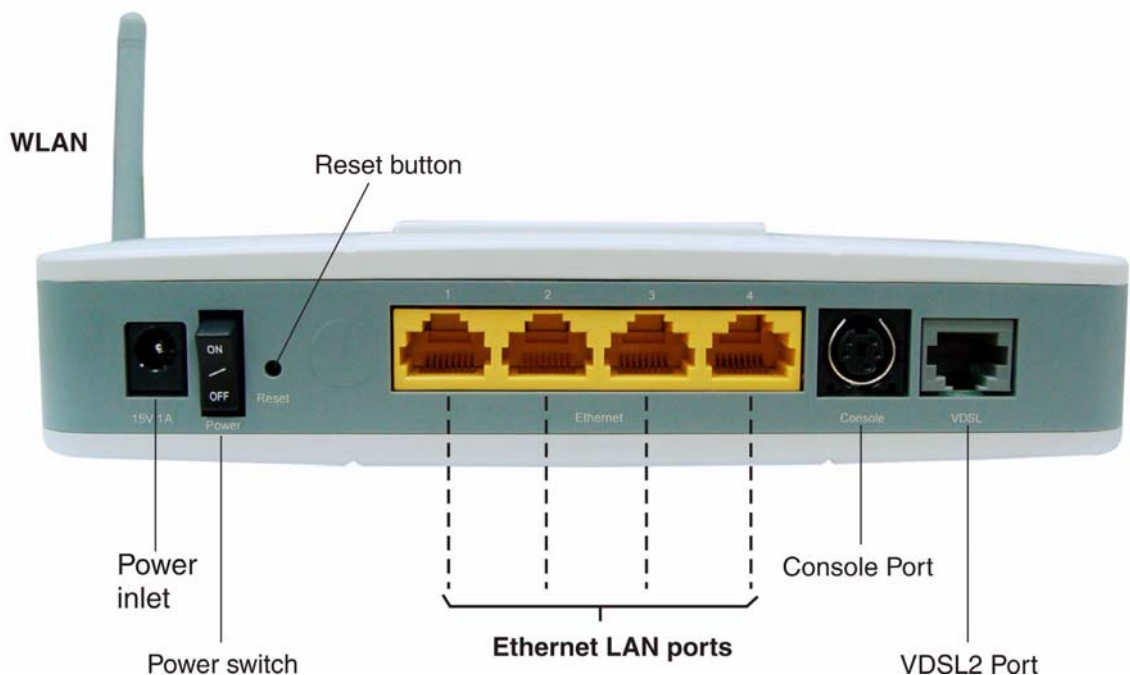
The package consists of the following components:

- One 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000 VDSL2 gateway
- One standard telephone cable (1.8 m)
- One category 5 UTP network cable (1.5 m)
- One power adapter
- One cradle for stand-up mounting
- Quick Installation Guide
- User Manual on CD-ROM.

## Side view LED and connector panel

The LED panel of the CPE provides several LEDs as system and port status indicators. The connector panel includes four Ethernet LAN ports for 10/100 Mb/s Ethernet connections and one port for VDSL line. The connector panel also includes the power inlet (15V/1A).

The following figure shows the connector panel with the different ports.



**Figure 1-1 Connector panel**

The left-most socket is for connecting the power adapter.

---

## **WARNING:**

*Please use for this inlet only the power adapter, which is shipped with your 7130 RG 5Ve.AL2000/7130 RG 5Ve.B2000 VDSL2 gateway. Failure to comply with may cause damage to the CPE.*

### **Power switch**

The power switch is used for turning “ON” and “OFF” the device.

### **Reset switch**

The reset switch serves two functions as explained here:

- Reset the device
- Turn “OFF” the **Power switch** and turn it “ON” again to reset the device.
- Reset and restore the default settings
- Using a pointed object, push down the **Reset button** and hold for 5 seconds (PWR LED turns “Off”), then release. This operation will reset the device to **factory defaults**.

### **Interfaces**

- Ethernet  
The Ethernet LAN ports are RJ-45 connectors with switching functionality. They also feature the Auto MDI/MDIX function, which allows using either a crossover or a straight cable to connect a Hub or PC.  
The left LED indicates connectivity with a device. The second LED indicates whether the connection speed is 10 Mbps or 100 Mbps; that is, it will be “ON” if the connection speed is 100 Mbps.
- The left LED indicates connectivity with a device. The second LED indicates whether the connection speed is 10 Mbps or 100 Mbps, that is it will be “ON” if the connection speed is 100 Mbps.
- VDSL  
The VDSL port is used for the WAN connection.

---

## LED indications for system and port status

Six LEDs on the front panel indicate the following system and port status:

LED	Status	Description
<i>System Status Indicators</i>		
PWR (Power)	On	Power supply is okay.
	Off	Power failure or disconnected.
DIAG (Diagnostics)	Slow Flashing <sup>*</sup>	Flashes during firmware upgrade.
	Off	No Firmware upgrading
INTERNET (Internet)	On	Data/Video session is connected, but no traffic.
	H/W Flashing <sup>†</sup>	Data/Video traffic is present.
	Off	Not connected to the Internet.
<i>Port Status Indicators</i>		
DSL (WAN link)	On	VDSL is operating.
	Slow flashing	VDSL is training.
	Off	VDSL is disconnected or not enabled.
LAN (link/activity)	On	Any of the four Ethernet LAN ports is connected and active.
	H/W flashing	Any of the four Ethernet LAN ports has data traffic.
	Off	None of the four Ethernet LAN ports are connected.
WLAN (link/activity)	H/W flashing	Traffic on wireless
	On	Wireless enabled
	Off	Wireless disabled

\* H/W flashing: LED flashes at the rate depending on the data transmission rate.

† Slow flashing: LED flashes at the rate of 2 seconds "On" and 2 seconds "Off"

Fast flashing: LED flashes at a rate of 0.2 second ON and 0.2 second OFF.

---

# Install the CPE

## When to use

Use this procedure to install the 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000, that means to make the connections to the network (wireless traffic via WLAN included), to the devices which may be for example a notebook, laptop or computer and to the power supply. In addition use the procedure to establish a TCP/IP connection from the device to the CPE. The following figure shows the CPE with all external connections established. This will be described step by step in the procedure below.

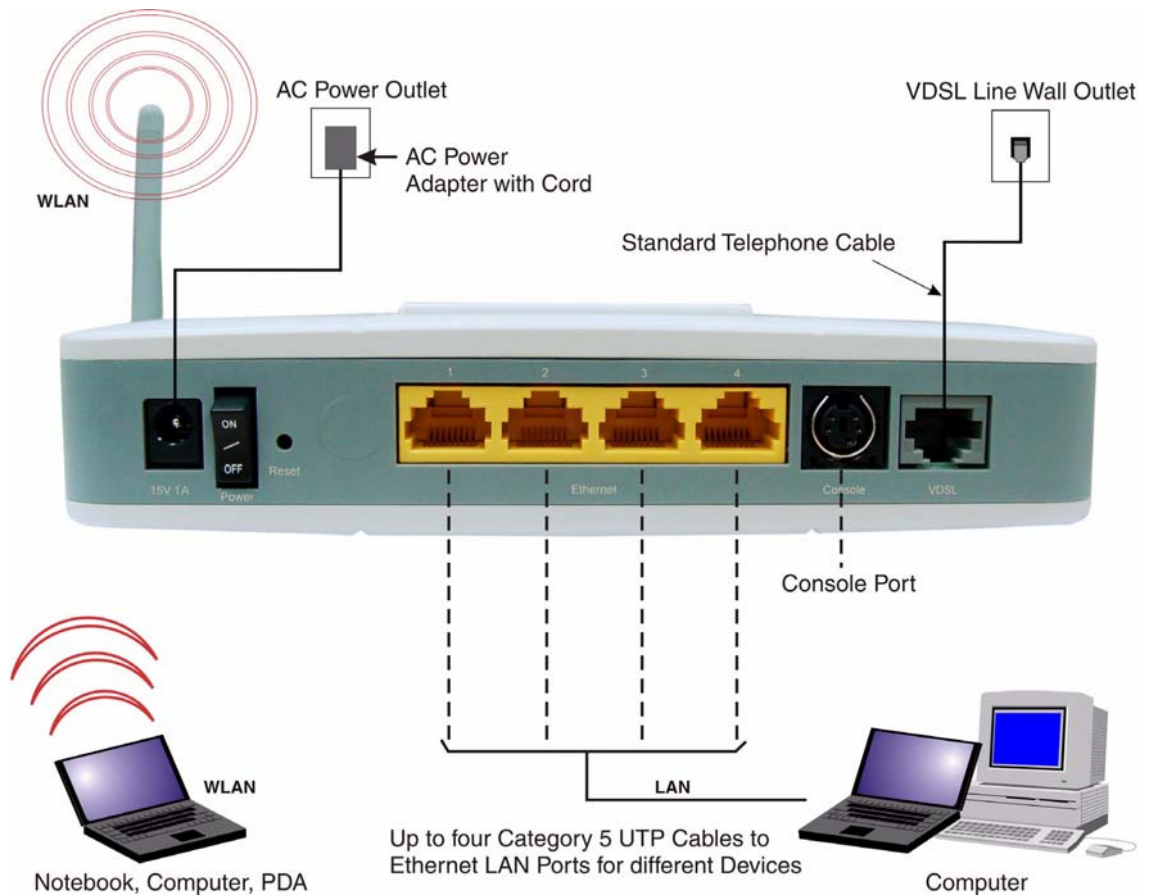


Figure 1-2 Overview about all external connections

## System requirements and safety guidelines

1. The CPE should be located in a cool dry place, with at least 5 cm (2 in.) of space on all sides for ventilation. Place the CPE out of direct sunlight, and away from heat sources or areas with a high amount of electromagnetic interference.
2. For power supply, the CPE requires 15 V DC via the included AC power adapter. The power adapter is designed for a 230 V AC connection.
3. Do not spill liquid of any kind on this CPE.
4. The CPE is a plug-and-play unit and does not need any configuration or maintenance.

- 
5. Do not place the CPE on an unstable stand or table; the CPE may drop and become damaged.
  6. For an Internet access, a PC with a 10/100 Mb/s Ethernet adapter card installed is required. The PC must be configured for TCP/IP.

### Before you begin

Make sure that the package content is complete. Preserve original carton and packaging material.

### Mounting procedure

There are three ways for mounting the CPE:

- Wall mounting

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.

3. Align the holes on the back of the CPE with the screws on the wall.
4. Hang up the CPE on the screw.

- Desktop mounting

Place the CPE on top of the desk with the name “*Alcatel.Lucent*” side up.

- Stand-up mounting

Place the cradle at the bottom of the CPE and sit the CPE on top of the desk.

### HW installation procedure

#### **CAUTION:**

*Please follow the directions from your service provider regarding the connection of your VDSL2 modem. The following procedure are meant as a guideline.*

---

- 1 Connect the cord of the AC power adapter to the power socket on the CPE which is labeled 15 V 1 A. Then plug the power adapter directly into the AC power outlet.

**Result:** The LED marked PWR (power) on the LED panel is on.

---

- 2 Restore this CPE to factory defaults if necessary. See section [Reset and restore the default settings](#) to restore the CPE to the factory defaults.

- 
- 
- 3 Connect one end of the attached standard telephone cable to the port on the CPE which is labeled VDSL and connect the other end to the telephone wall outlet providing the VDSL service.

---

  - 4 Connect one end of the Category 5 UTP network cable to the Ethernet LAN port on the CPE and the other end to the port of the network interface on the appropriate device, for example a PC, Notebook and so on.

---

  - 5 Make sure that the Ethernet adapter of your device is correctly configured for DHCP. For more details refer to Appendix B **Configuring the TCP/IP protocols on the PC**.

---

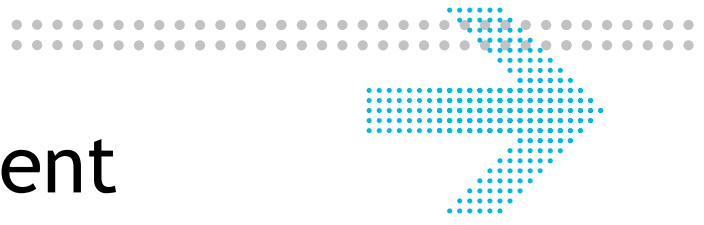
  - 6 Establish the first connection to the ISP provider. For information about how to configure an internet connection refer to the: *User Manual*.

**END OF STEPS**

---







# 2 Web Management Interface

## Overview

The Web Management Interface is provided to let the configuration of 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000 as easily as possible. It provides a user-friendly graphical interface through a Web platform. You can configure bridge or router functions to accommodate your needs. In the section below, each configuration item is described in detail.

## Contents

This chapter covers these topics.

<a href="#">The Web Management Interface</a>	2-3
<a href="#">Access to Web Management Interface via Internet browser</a>	2-5
<a href="#">Retrieve Status</a>	2-7
<a href="#">LAN Settings</a>	2-9
<a href="#">WiFi Settings</a>	2-12
<a href="#">Security Mode configuration</a>	2-15
<a href="#">Wi-Fi MAC</a>	2-17
<a href="#">WiFi QoS</a>	2-19
<a href="#">Advanced Setup</a>	2-23
<a href="#">DHCP</a>	2-24
<a href="#">PPPoE Settings</a>	2-26
<a href="#">VLAN + 2PPPoE Settings</a>	2-28
<a href="#">Bridge Settings</a>	2-30
<a href="#">Route Setting</a>	2-32
<a href="#">Bridge MAC Filter</a>	2-34
<a href="#">DDNS Setting</a>	2-36
<a href="#">Port Range Forwarding</a>	2-38
<a href="#">Virtual Server Basic</a>	2-40
<a href="#">Virtual Server Advance</a>	2-42

---

DMZ and UPnP	2-44
Filter	2-47
NAT Passthrough	2-49
QoS Setup	2-51
Default QoS	2-54
QoS Policy	2-56
QoS Interface Policy	2-58
QoS ALG	2-60
Reboot Gateway	2-62
Restore Factory Defaults	2-64
Web Firmware Upload	2-66
System Settings	2-68
MCL Settings	2-70

---

# The Web Management Interface

## Overview

The following summarizes how to configure the 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000 by using the **Web Management Interface**. The **Web Management Interface** is a graphical interface and allow user to access the system for statistics, configuration, administration and maintenance activities. The Web Management Interface has several pages, each page can be accessed directly by clicking the menu item from the navigation bar on the left side.

The main navigation bar is divided in five groups:

## Status

The pages that accessed from these menu items group present information about the current configuration status of your 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000.

Following information items are available:

- Status
- Device Table
- IGMP Statistics
- IGMP Membership
- System Log
- VDSL
- DHCP Lease Table
- WiFi Associate Table
- Network Statistics

## LAN Setup

On this page you can setup the network configurations for your gateway's LAN port.

- LAN Settings

## WiFi Setup

On this pages you can configure the wireless settings.

- WiFi Settings
- WiFi Security
- WiFi MAC
- WiFi QoS

---

## Advanced Setup

On this pages you can configure the WAN ports connection method.

- WAN Settings
  - DHCP
  - PPPoE
  - VLAN + 2PPPoE
  - Bridge
- Route Setting
- Bridge MAC Filter
- DDNS Setting
- Port Range Forwarding
- Virtual Server Basic
- Virtual Server Advance
- DMZ & UPnP
- Filter
- URL Filter
- NAT Passthrough

## QoS

On this pages you can configure the QoS method.

- Scheduler
- Default QoS
- Policy
- Interface Policy
- ALG

## Utilities

On this pages you can restore the factory settings to the 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000 or update the firmware.

- Restore Factory Defaults
- Web Firmware Upload
- System Setting
- MCL Settings.

---

# Access to Web Management Interface via Internet browser

## Purpose

Use this procedure to access to the 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000 **Web Management Interface** via Internet browser.

## Related information

The 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000 is with following default settings configured:

- User Name: admin
- Password: admin
- Operation Mode: Bridge Mode
- Local port address: 192.168.2.1
- Subnet mask: 255.255.255.0

## Before you begin

Make sure that the 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000 hardware is properly connected and switched on (refer to QIG).

Your PC is configured to the same IP subnet mask as the 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000.

Configuration example:

7130 RG 5Ve.A2000/7130 RG 5Ve.B2000: 192.168.2.1 Your PC:192.168.2.x  
Subnet mask: 255.255.255.0

## Procedure

Connect to the **Home Area** from the 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000

---

- 1 Open your internet browser on the computer (e.g. IE or Netscape), and enter the default IP address 192.168.2.1 (for your 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000) into the address bar as the URL to access the Web management page on the 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000.

**Result:** The **Login** dialog box will appear first.

- 
- 2 Enter the **User name** and the **Password** (“admin” for both per default), and then click **OK**.



**Note:** The username and password are case-sensitive.

**Result:** The **Home Area** screen with the basic setting of your 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000 configuration and connection statistics opens.

**END OF STEPS**

---

---

# Retrieve Status

## Purpose

Use this procedure to retrieve the basic settings of your current configuration as well as a network and connection statistics.

## Before you begin

Make sure that you are connected to the **Home Area** from the 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000 via your internet browser.

- 1 From the main navigation bar, follow this path to retrieve basic settings of your current configuration.

**Status > Status**

**Result:** The **Status** window opens.

- 2 Example of a **Status** window:

The screenshot shows the web interface of a CELL Pipe 7130 Residential Gateway. The browser window is titled "CELL Pipe 7130 - Microsoft Internet Explorer" and the address bar shows "http://192.168.2.1/index.html". The page content includes a navigation menu on the left and a main content area displaying the "Status > Status" page. The main content area is divided into three sections: Version Info, System Info, and Network Settings.

Version Info	
Firmware Version	v1.0.6.0AE
Release Date	2008/04/25

System Info	
System Up Time	0:0:3:16
System Loading Average	1.15
Total Memory	28996
Used Memory	24828
Free Memory	4168

Network Settings	
WAN Connection 1	PPPoE (VLAN ID : 35)
WAN IP Address	
WAN NetMask	
WAN Gateway	
WAN DNS1	
WAN DNS2	
WAN Connection 2	PPPoE (VLAN ID : 36)
WAN MAC	00:1A:73:C1:00:51
LAN IP Address	192.168.2.1
LAN NetMask	255.255.255.0
LAN MAC	00:1A:73:C1:00:50
DHCP Enable	Enabled
WLAN MAC	00:1A:73:C1:00:54
WLAN SSID	"mobileAP_for 1"

---

Following parameters are displayed in the **Status** window:

<b>Parameter</b>	<b>Description</b>
Version Info:	The version of currently used firmware
Release Date:	The release date of your firmware
System Up Time:	Shows how long the system has been up and operated
Total Memory:	Shows the memory (Random Access Memory) capacity of the system.
Used Memory:	Shows the memory used in the system.
Free Memory:	Shows free memory in the system.
WAN IP Address:	The IP Address of the WAN interface.
WAN NetMask:	The network mask of the WAN interface.
WAN Gateway:	The gateway IP address for the WAN interface.
WAN DNS1 or 2:	Shows the Domain Name Server IP address.
WAN MAC:	Shows the MAC address of the WAN interface.
LAN IP Address:	Shows the IP Address of the LAN interface.
LAN NetMask:	The IP subnet mask of the LAN interface.
LAN MAC:	The MAC address of the LAN interface.

**END OF STEPS**

---



# LAN Settings

## Purpose

Use this procedure to configure the network settings for your gateway and LAN port.

## Before you begin

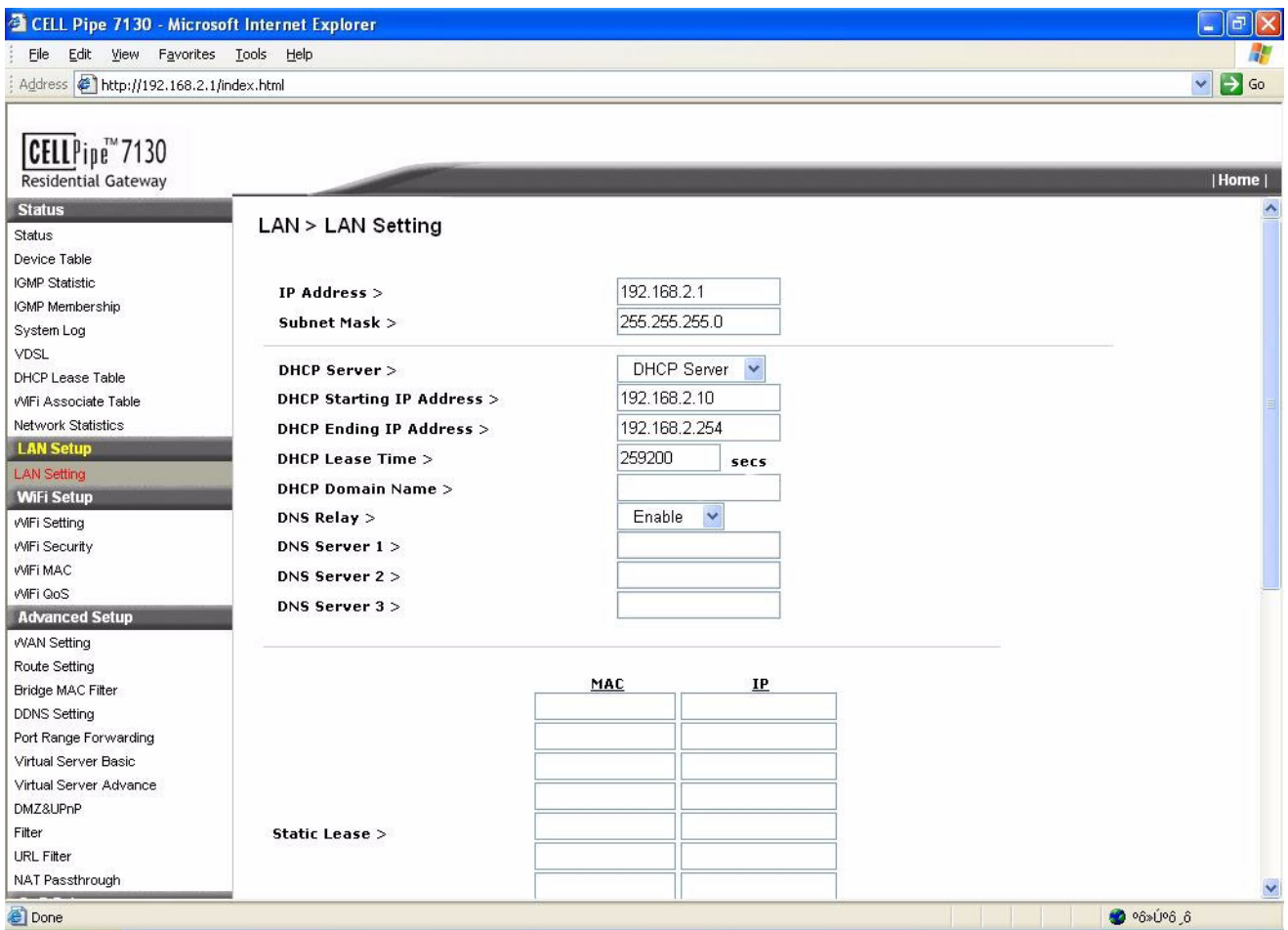
Make sure that you are connected to the **Home Area** from the 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000 via your internet browser.

- 1 From the main navigation bar, follow this path to configure the network settings for your gateways and LAN port.

**Status > LAN Settings**

**Result:** The LAN Settings window opens.

- 2 Example of a LAN Settings window:



- 
- 
- 3** To configure the gateway and the LAN port enter the **IP Address** and the **Subnet Mask**.  
For example: IP Address 10.x.x.x or 192.x.x.x and Subnet Mask 255.255.255.0

**Additional Information:** This defines the IP address of local port and has to be a private one. The subnet mask determines the number of computers that are allowed in this local network. A class C network with the subnet mask 255.255.255.0 allows up to 253 users in your local area network. Usually a class C network is satisfactory for a LAN environment.

---

- 4** To enable the **DHCP Service**, click the pull-down menu and enable the DHCP server on this unit.
- 

- 5** Enter the **DHCP Start IP Address**.

This specifies the starting IP address for DHCP users, which has 192.168.2.10 as default value.

---

- 6** Enter the **DHCP End IP Address**.

This specifies the ending IP address for DHCP users, which has 192.168.2.254 as default value.

**Note:** Please make sure that there is no existing LAN client with fixed IP address within the range you assigned here. Otherwise, the DHCP client may not get the IP address correctly.

---

- 7** Enter the **DHCP Lease Time**.

**Additional information:** A DHCP user's PC gets the IP address with a lease time. When the lease time is expired, the user's PC must connect to the DHCP server to request the dynamic IP address again. When there are many nomadic users using DHCP service in your network, select an appropriate time to make sure IP addresses will be released after they logout. The gateway may not know at when an user turns his computer off and leaves, thus that IP address will be occupied there until the lease time expires. The default value of the lease time is 72 hours.

---

- 8** Enter the **DHCP Domain Name**.

The name for your group or zone. This will be published with your DHCP service.

---

**9 Enable/Disable DNS Relay.**

This is optional. You may have already setup a DHCP server in your domain and let the unit to forward the DHCP request to this server.

**10 Enter the DNS Server 1...3 IP Address.**

Enter the DNS server IP address if this is not automatically relaying (obtained by your Internet service provider ISP).

**11 Configure a Static IP Lease.**

Enter the clients' **MAC** addresses and **IP** addresses to configure the **Static DHCP Lease**.

You can assign a fixed IP address to a DHCP client identified by its MAC address. Enter the new entry into the list.

**12 Enter the client's MAC addresses in the fields provided, to filter a client from getting a DHCP release. (Configure Not Assign IP).**

**13 Click **Apply Changes** at the bottom of the page to apply your changes.**

**END OF STEPS**

---

# WiFi Settings

## Purpose

Use this procedure to configure the basic wireless network settings. The Router can connect up to 253 wireless clients.

## Before you begin

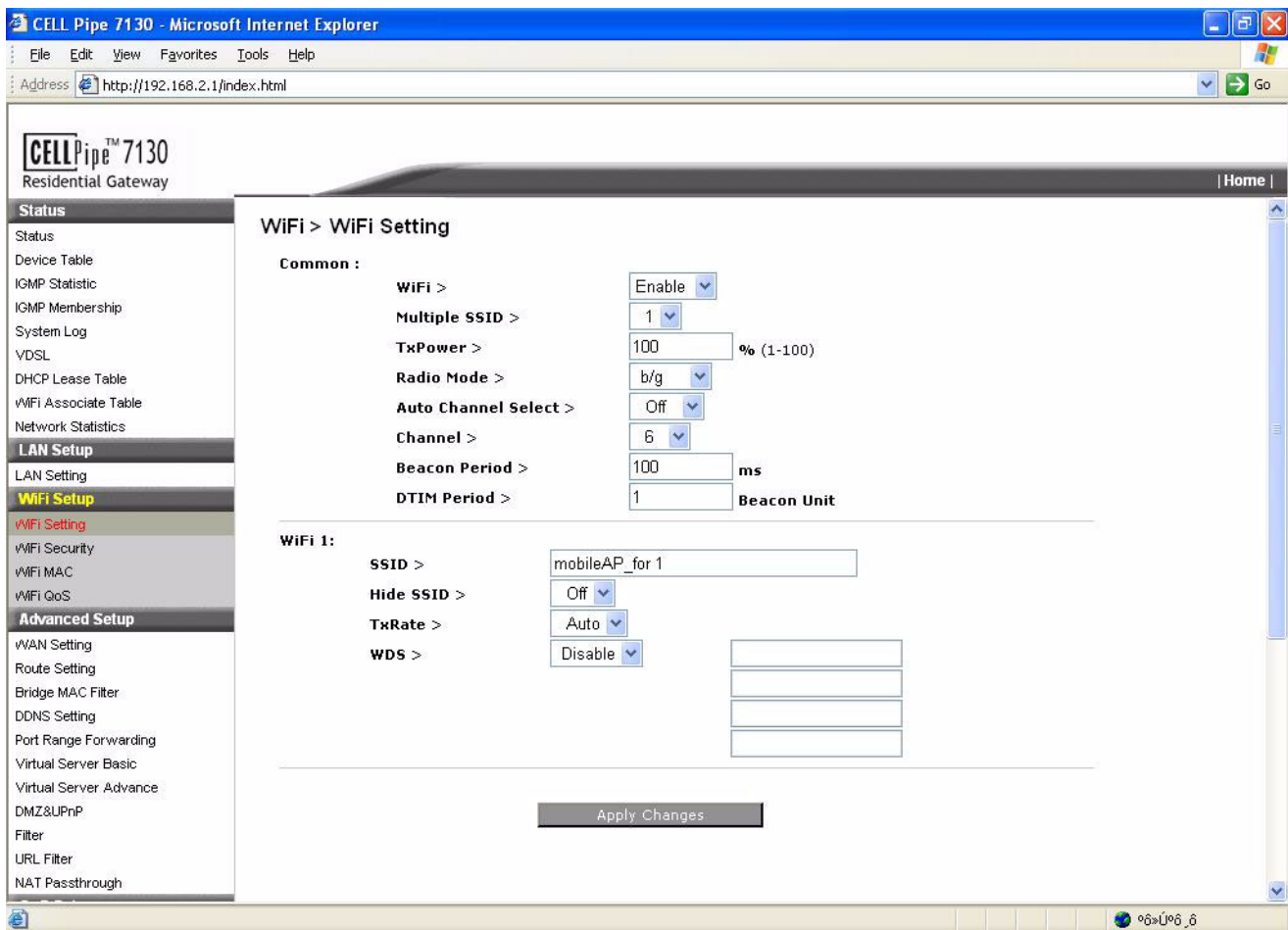
Make sure that you are connected to the **Home Area** from the 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000 via your internet browser.

- 1 From the main navigation bar, follow this path to configure the **WiFi Settings** for your wireless network.

**Status > WiFi Settings**

**Result:** The **WiFi Settings** window opens.

- 2 Example of a **WiFi Settings** window:



- 
- 
- 3 To configure the wireless LAN settings enable the WiFi function first. Select from the pull-down menu **Enable** (Enable/Disable).

---
  - 4 Set a appropriate value for the **TxPower** capability (ranges 1-100%).  
This parameter allow you to manage your transmission power consumption.

---
  - 5 Specify the **Radio Mode**.  
Select from the pull-down menu the wireless mode one of following options: b/g mix, b or g only.

---
  - 6 Specify the **Channel**.  
Select the appropriate channel to be used among your Access Points and your client devices. Default is channel 6. When you select **Auto** your Access Point will select the channel with the lowest amount of wireless interference while the system is powering up.  
The **Auto channel select** start when you click **Apply Changes** button, it take several seconds to scan through all the channels to find the best channel.

---
  - 7 Specify the **Beacon Period**. This is optional.  
This value indicates the frequency interval of the beacon. This is a packet broadcast by the Access Point to keep the network synchronized.

---
  - 8 Specify the **DTIM Period**. This is optional.  
This value indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages.

---
  - 9 Enter the **DHCP Start IP Address**.  
This specifies the starting IP address for DHCP users, which has 192.168.2.10 as default value.

---
  - 10 Enter the **SSID**.  
The SSID is the unique name shared among all devices in a wireless network. It is case sensitive, must not exceed 32 alphanumeric characters, and may be any keyboard character. Make sure that this setting is the same for all devices in your wireless network.

---

**11** Configure **Hide SSID**.

Select **On** to hide the SSID or select **Off** to make the SSID visible.

**Additional Info:** This option allows the SSID to be broadcast on your network. You may want to enable this function while configuring your network, but make sure that you disable it when you are finished.

With this enabled, someone could easily obtain the SSID information with site survey software or Windows XP and gain unauthorized access to your network. Select off to allow broadcasting the SSID to all wireless devices in range. Select on to increase network security and prevent the SSID from being seen on networked PCs.

---

**12** Configure **TxRate**. This is optional.

You may restrict the transmission rate by entering the transmission rate. Specify the rate of transmission up to its maximum which is 54Mbps for 802.11g

---

**13** Click **Apply Changes** at the bottom of the page to apply your changes

**END OF STEPS**

---

# Security Mode configuration

## Purpose

Use this procedure to configure security mode on your wired or wireless network, the 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000 supports the security mechanisms WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) and WPA2.

## Before you begin

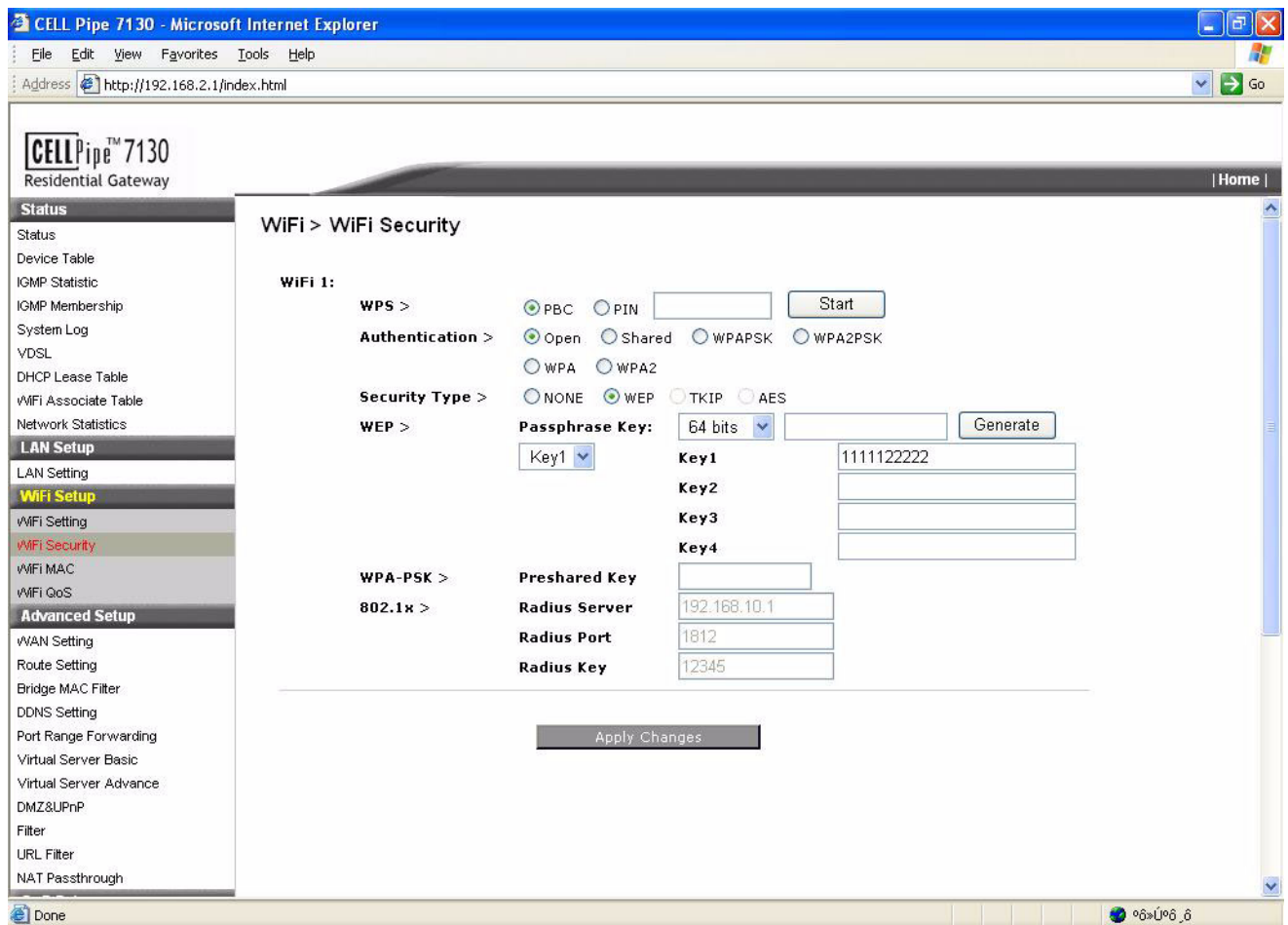
Make sure that you are connected to the **Home Area** from the 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000 via your internet browser.

- 1 From the main navigation bar, follow this path to configure the **WiFi Security** for your wireless network.

**Status > WiFi Security**

**Result:** The WiFi Security window opens.

- 2 Example of a WiFi Security window:



---

3 Following options are available:

- **Open** - For this type of security mode, your wireless connection is unprotected. This is strongly not recommended.
- **WEP** - This security mode is defined in the original IEEE 802.11. This mode is not recommended now due to its weak security protection. Users are urged to migrate to WPA or WPA2.  
**Default Transmit Key** - Select the key to be used for data encryption. WEP Encryption.  
Select a level of WEP encryption, 64 bits (10 hex digits) or 128 bits (26 hex digits). Key 1-4. If you want to manually enter WEP keys, then complete the fields provided. Each WEP key can consist of the letters "A" through "F" and the numbers "0" through "9". It should be 10 characters in length for 64-bit encryption or 26 characters in length for 128-bit encryption.
- **WPA-PSK** - This is the WPA Algorithm. WPA offers you two encryption methods, TKIP and AES for data encryption.  
Select the type of algorithm you want to use, TKIP or AES. The default is TKIP. WPA PreShared Key. Enter a PassPhrase Key of 8-63 characters.
- **WPA2-PSK** - This is the WPA2 Algorithm. WPA2 offers you two encryption methods, TKIP and AES for data encryption.  
Select the type of algorithm you want to use, TKIP or AES. The default is TKIP. WPA PreShared Key. Enter a PassPhrase Key of 8-63 characters.
- **802.1x** - This is for authenticating with a Radius server. Please enter your Radius server's IP address, port number and key in the boxes.

**Note:** To configure your wireless network for the best security setting of your wireless network, it is recommended that you use WPA/WPA2- PSK and setup your pre-shared key in the router. Or you may choose to use WPA/WPA2 if you have a radius server in your local network.

---

4 Click **Apply Changes** at the bottom of the page to apply your changes.

**END OF STEPS**

---



---

# Wi-Fi MAC

## Purpose

Use this procedure to restrict some of the wireless clients association with the Access Point.

## Related information

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters. You need to know the MAC address of the devices to configure the Wi-Fi MAC filter. You can allow access up to 32 devices or exclude access up to 32 devices.

## Before you begin

Make sure that you are connected to the **Home Area** from the 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000 via your internet browser.

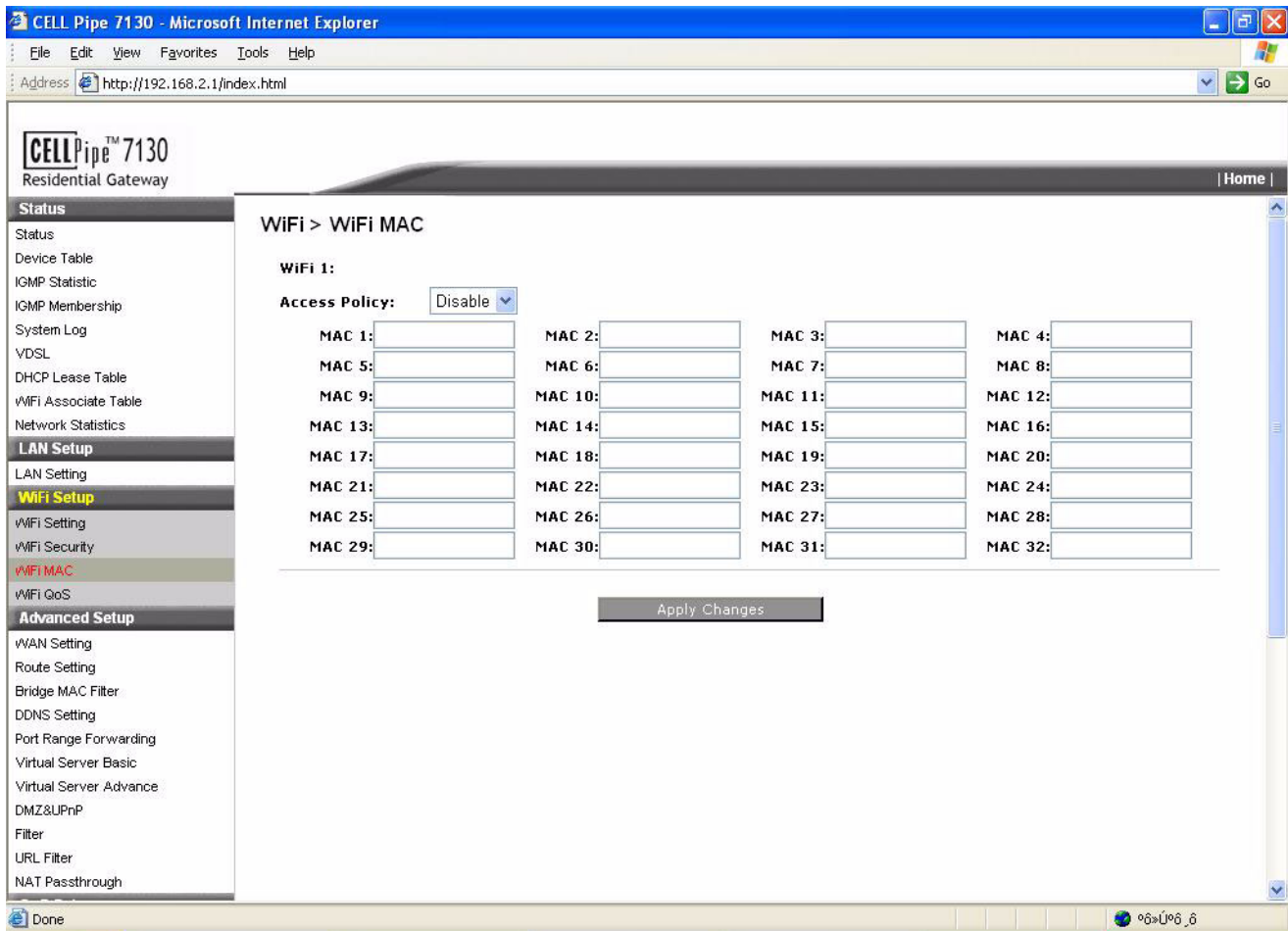
---

- 1 From the main navigation bar, follow this path to enable and change the Wi-Fi MAC filter settings.

**Status > WiFi MAC**

**Result:** The **WiFi MAC** window opens.

## 2 Example of a WiFi MAC window:



- 3 Enter the MAC addresses of the wireless devices that are allowed or denied access to your wireless network.
- 4 Select **Disable** to turn off the Wi-Fi MAC filtering function. Select **Allow** to allow the following MAC addresses to connect the router. Select **Deny** to deny the following MAC addresses to connect the router.
- 5 Click **Apply Changes** at the bottom of the page to apply your changes.

END OF STEPS

---

# WiFi QoS

## Purpose

Use this procedure to enable the media access prioritization Wi-Fi Multimedia (WMM). Three access categories are support by the Wi-Fi QoS, for audio, video, and voice applications over the wireless network. This give you a higher priority for different types of multimedia traffic.

### Before you begin

Make sure that you are connected to the **Home Area** from the 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000 via your internet browser.

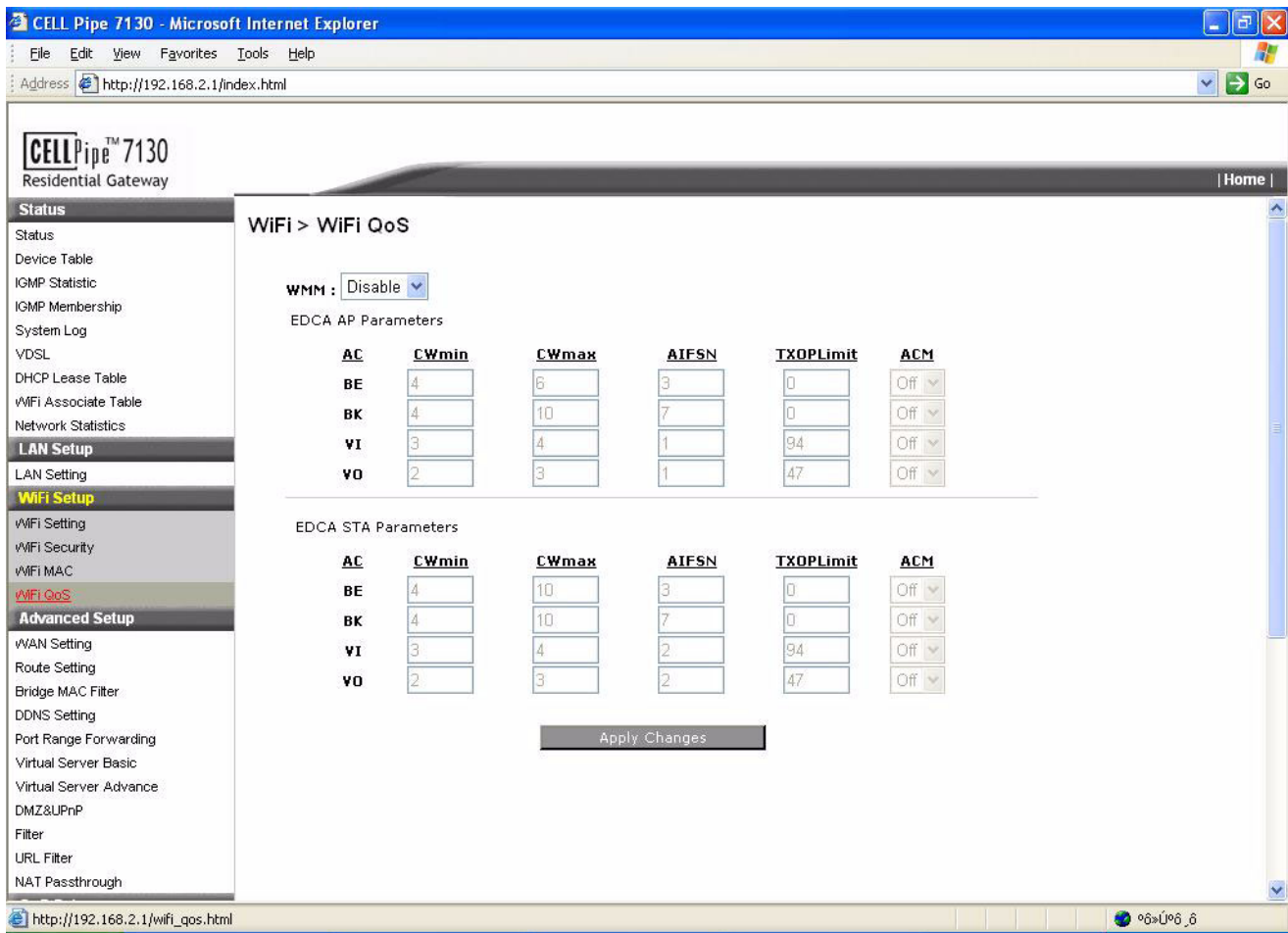
---

- 1 From the main navigation bar, follow this path to configure the **WiFi QoS** for your wireless network.

**Status > WiFi QoS**

**Result:** The **WiFi QoS** window opens.

## 2 Example of a WiFi QoS window:



## 3 EDCA Parameter

The IEEE 802.11e standard improves the Medium Access Control (MAC) of the legacy 802.11 with regard to Quality of Service (QoS) by introducing the Enhanced Distributed Channel Access (EDCA). The 802.11e MAC is based on both centrally-controlled and contention-based channel accesses. The EDCA provides differentiated channel access to frames with different priorities.

Typically, voice and video traffic types are delay-sensitive, but are tolerant of some frame losses. On the other hand, data traffic type is delay-tolerable, but requires loss-free transmission. So you may adjust these parameters with regard to the characteristics of these types of data to better manage your network flow.

### AC (Access Category):

using 4 different ACs: From high to low: VO: Voice, VI: Video, BE: Best Effort, BK: Background

---

**AIFS (Arbitrary Interframe Space):**

The back-off timing for each access category consists of a fixed period called the Arbitrary Inter-Frame Space Number followed by a random period called the Contention Window (CW), both specified in multiples of the slot time.

**TXOP (Transmission Opportunity):**

WMM (Wireless Multimedia) Transmission Opportunity: defined by IEEE 802.11e, the TXOP is the interval of time when a particular STA (station) has the right to initiate transmissions.

**ACM (Admission Control Mandatory):**

Advertised in the EDCA parameter set element to indicate that the admission control is taken over by the client when it is turned on. It only has the effect on AC VI and VO.

**Access Point**

These values of AIFS, CWmin, and CWmax are announced by the AP via beacon frames. The AP can adapt these parameters dynamically depending on the network conditions. Basically, the smaller AIFS and CWmin, the shorter the channel access delay for the corresponding priority, and hence the more capacity share for a given traffic condition. However, the probability of collisions increases when operating with smaller CWmin. These parameters can be used in order to differentiate the channel access among different priority traffic.

**Note:** You may slightly adjust these values when you experience latency in your network traffic according to the following explained properties for each of the data types. For instance, if you experience delay in your video applications, you may give a bigger value for TXOPLimit while reduce the difference between CWmin and CWmax, and the number for AIFSN.

---

**4 STA**

Each station maintains a Contention Window (CW), which is used to select the random back off counter. The BC is determined as a random integer drawn from a uniform distribution over the interval (0, CW). The CW size is initially assigned CWmin, and increases when a transmission fails, i.e., the transmitted data frame has not been acknowledged. After any unsuccessful transmission attempt, another back off timer is performed, with an upper bound of CWmax. This reduces the collision probability in case there are multiple stations attempting to access the channel.

**CW min:**

should be smaller for delay-sensitive data

**CW max:**

should be smaller for delay-sensitive data

**AIFSN:**

should be smaller for delay-sensitive data

---

**TXOPLimit:**

These will allow multiple MAC frames consecutively as long as the whole transmission time does not exceed the TXOP limit. So keep it larger for delay-sensitive data.

**ACM:**

Admission Control Mandatory: The admission control is taken over by the client when you turn on this. Otherwise, the connecting AP is in charge.

**Important!** Do not change any of these values unless you are an experienced network administrator.

**END OF STEPS**

---

---

# Advanced Setup

## Purpose

Use this procedure to setup your WAN ports connection method.

## Related information

These settings determine how the router will make a connection with the modem/internet. A Dynamic Connection, meaning that the IP address, Subnet Mask, Gateway, and DNS addresses are supplied automatically by the ISP.

## Before you begin

Make sure that you are connected to the **Home Area** from the 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000 via your internet browser.

---

- 1 Click on the **Wan Setting** link on the navigation bar to configure the gateway's WAN connection method. Your service provider will specify which WAN setting option is required.

Following options are displayed:

- DHCP
- PPPoE
- VLAN + 2 PPPoE
- Bridge.

Select your connection method from **DHCP**, **PPPoE**, **VLAN + 2 PPPoE** or **Bridge** and click **Next**.

**Result:** The window with the selected settings opens.

**END OF STEPS**

---

# DHCP

## Purpose

Use this procedure to configure the **DHCP** settings.

## Before you begin

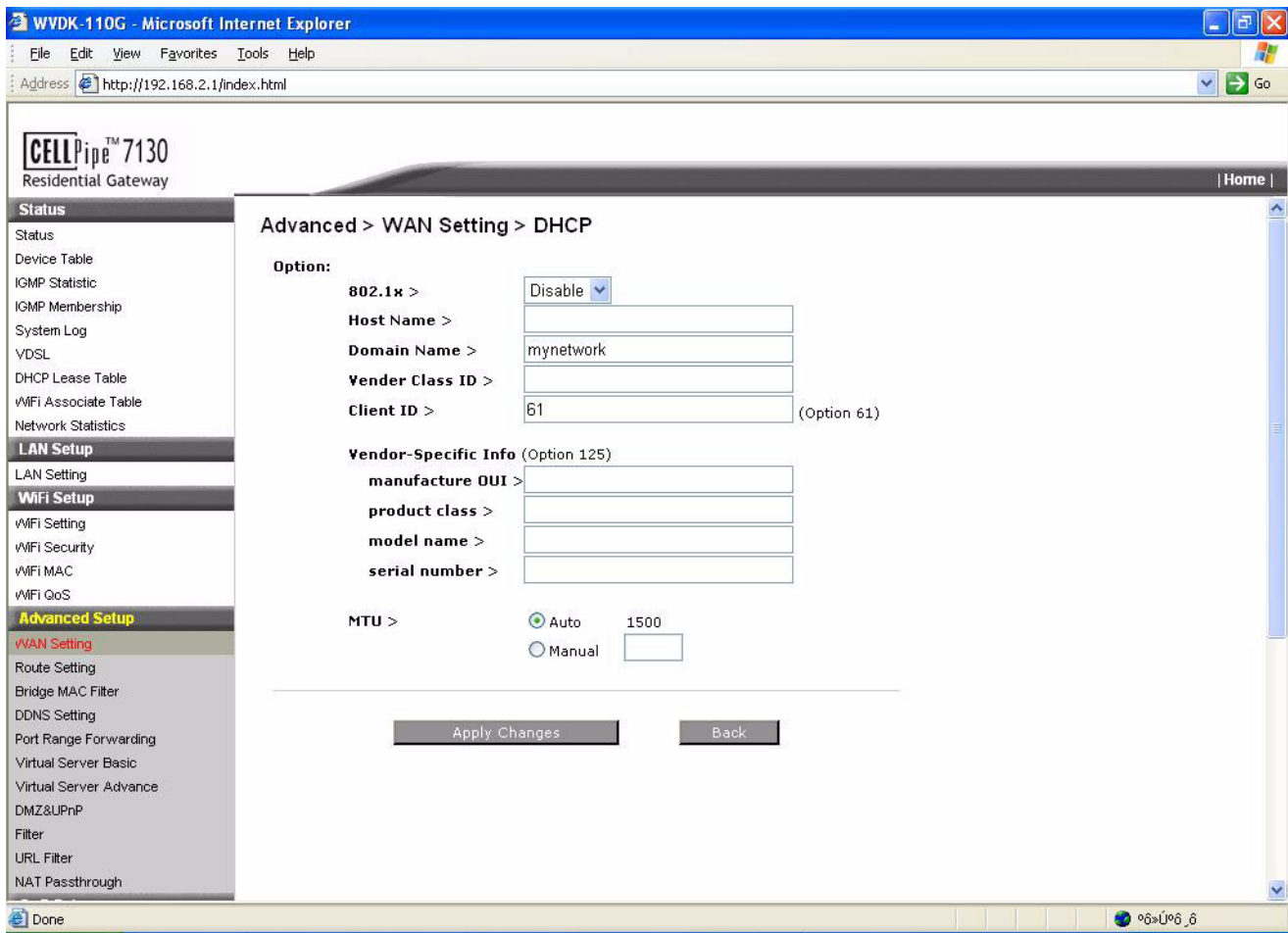
Make sure that you are connected to the **Home Area** from the 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000 via your internet browser.

- 1 From the main navigation bar, follow this path to configure the gateway connected via **DHCP** for your wireless network.

**Status > WAN Settings > DHCP**

**Result:** The **DHCP** window opens.

- 2 Example of a **DHCP** window:





- 
- .....
- .....
- 3 Enter the appropriate **Host Name** and **Domain Name** for your connection: For this type of connection method, just identify your router with the **Host Name** and **Domain Name**. Select **Auto** or **Manual** configuration and enter the appropriate value for the **MTU** (Maximum Transfer Unit).
  - 4 Configure the **Client ID/Vendor Class ID**: You may also need to set the **Client ID** or **Vendor Class ID** to set the DHCP class ID the client uses when obtaining its lease from the DHCP server. Please consult your ISP for this option.
  - 5 Click **Apply Changes** at the bottom of the page to apply your changes.

.....

**END OF STEPS**

.....

# PPPoE Settings

## Purpose

Use this procedure to configure the **PPPoE** settings.

## Before you begin

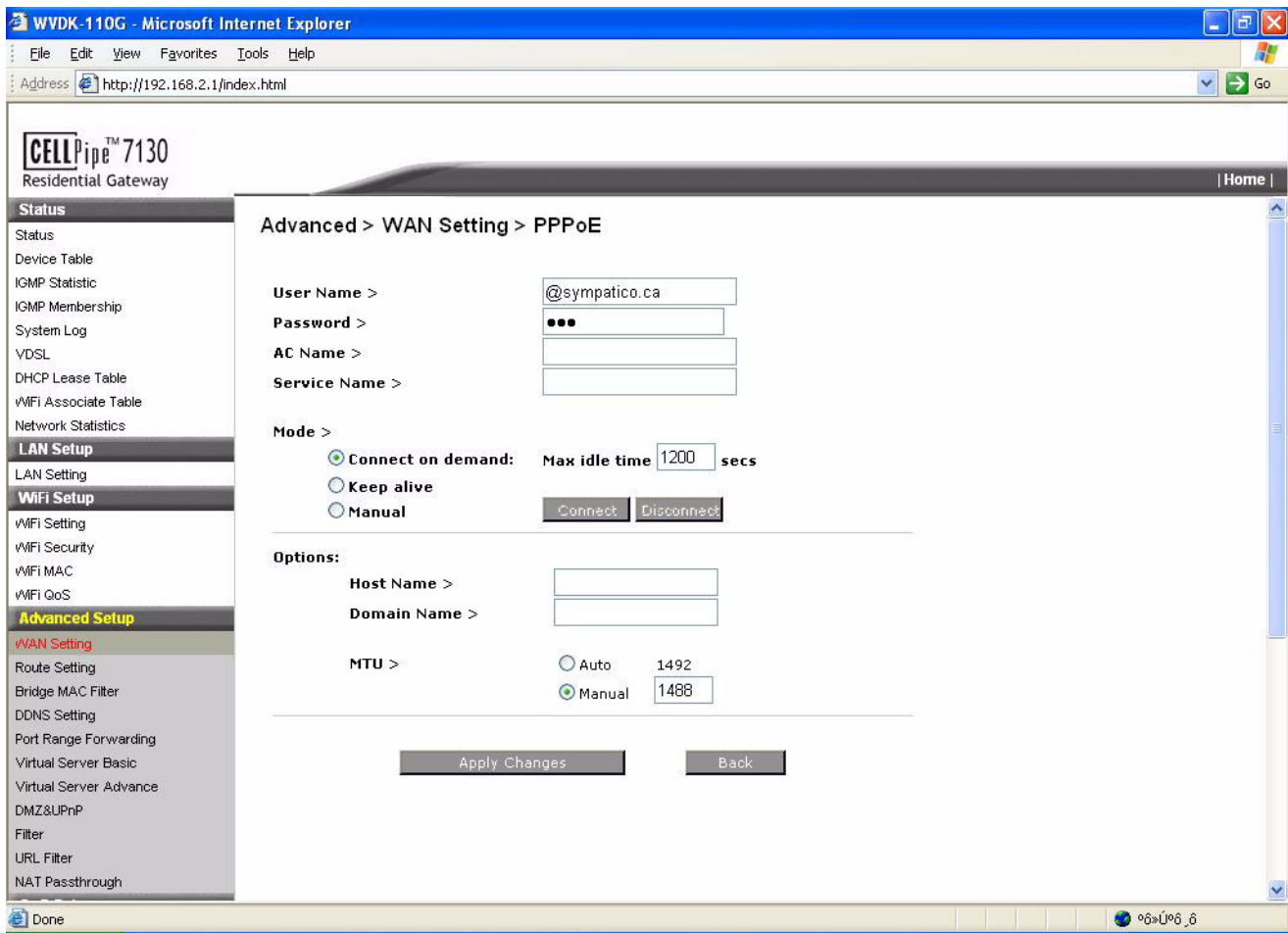
Make sure that you are connected to the **Home Area** from the 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000 via your internet browser.

- 1 From the main navigation bar, follow this path to configure the **PPPoE** settings for your wireless network.

**Status > WAN Settings > PPPoE**

**Result:** The PPPoE window opens.

- 2 Example of a PPPoE window:



---

3 Enter the **Username** and the **Password** for your PPPoE connection. **AC Name** and **Service Name** are optional, please consult your ISP.

---

4 Select from the radio button for either **Connection on Demand** or **Keep alive**.

For connection on demand, the router will only connect to the internet service when it is instructed to do so.

Enter the **Max Idle Time** in the box to specify the maximum number of seconds of being idle before it can drop a connection.

---

5 In the **Options** section enter the **Host Name** and **Domain Name** to setup your router as hostname@domainname. Select your **MTU** (Maximum Transfer Unit) size from either **Auto** (Default:1488) or **Manual**.

---

6 Click **Apply Changes** at the bottom of the page to apply your changes.

**END OF STEPS**

---

# VLAN + 2PPPoE Settings

## Purpose

Use this procedure to configure the **PPPoE** settings over VLAN for multiple PPPoE connections.

## Before you begin

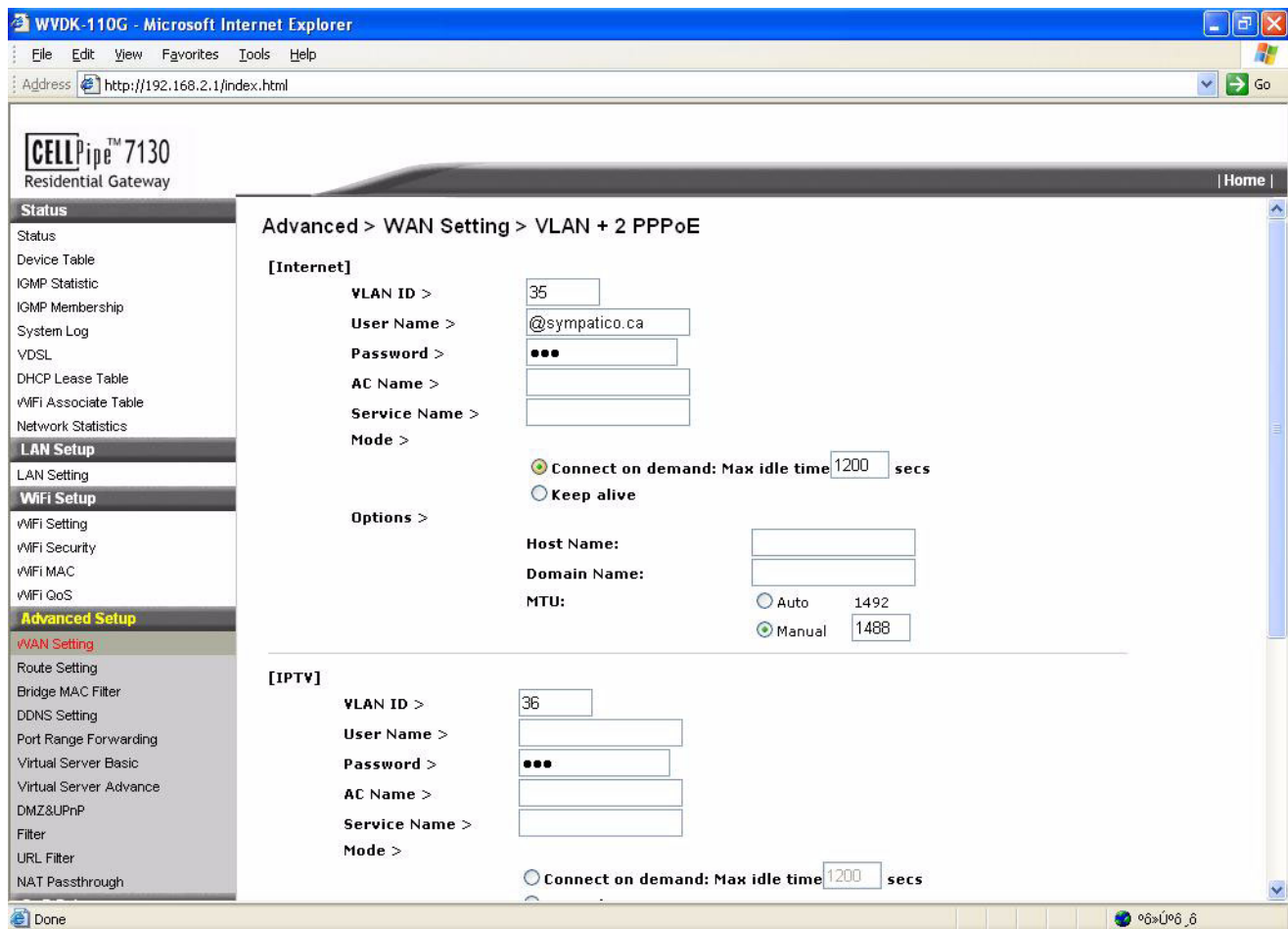
Make sure that you are connected to the **Home Area** from the 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000 via your internet browser.

- 1 From the main navigation bar, follow this path to configure the **VLAN + 2PPPoE** settings over VLAN for your wireless network.

**Status > WAN Settings > VLAN + 2PPPoE**

**Result:** The PPPoE window opens.

- 2 Example of a **VLAN + 2PPPoE** window:



- 
- 
- 3 Enter the **VLAN ID**: Please give the Vlan-ID if you have two different PPPoE accounts for these two services.

**Important!** This configuration should be given by your ISP or configured by them.

---

- 4 Enter the **User Name** and **Password** for your connection.
- 

- 5 Enter the **AC Name** (Access Concentrator) for your PPPoE account
- 

- 6 Select from the radio button for either **Connection on Demand** or **Keep alive**.

For connection on demand, the router will only connect to the internet service when it is instructed to do so.

Enter the **Max Idle Time** in the box to specify the maximum number of seconds of being idle before it can drop a connection.

---

- 7 In the **Options** section enter the **Host Name** and **Domain Name** to setup your router as hostname@domainname. Select your **MTU** (Maximum Transfer Unit) size from either **Auto** (Default:1488) or **Manual**.
- 

- 8 Click **Apply Changes** at the bottom of the page to apply your changes.

**END OF STEPS**

---

# Bridge Settings

## Purpose

Use this procedure to set the connection type for your wireless network.

## Before you begin

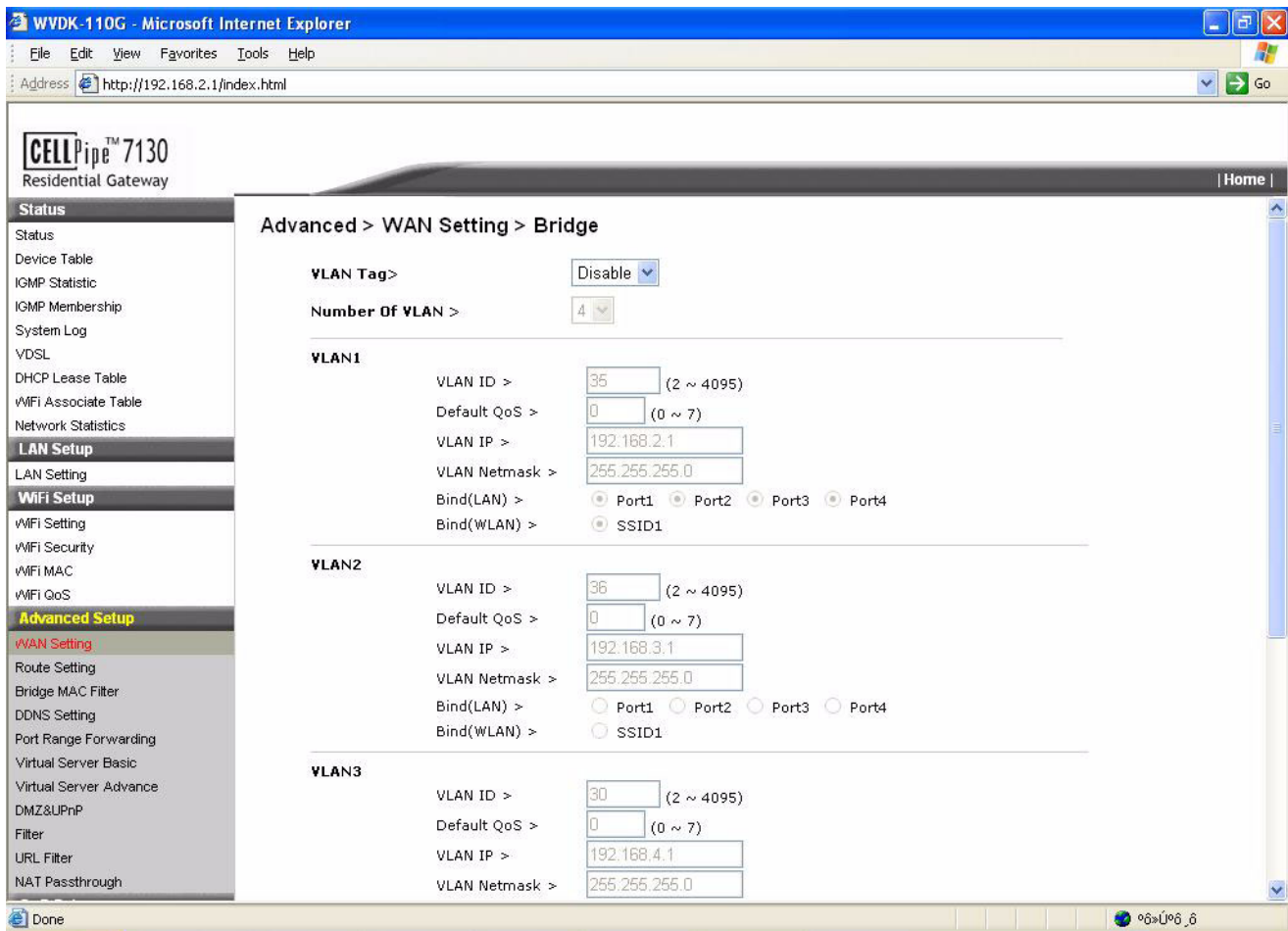
Make sure that you are connected to the **Home Area** from the 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000 via your internet browser.

- 1 From the main navigation bar, follow this path to configure the **Connection Type** for your wireless network.

**Status > WAN Setting**

**Result:** The **WAN Setting** window opens.

- 2 Example of a **WAN Setting** window:



---

3 Click **Apply Changes** at the bottom of the page to apply your changes.

4 In this case your router is configured as a simply bridge and act like a bridge.

**END OF STEPS**

---

# Route Setting

## Purpose

Use this procedure to setup static routes when the routing packets come from a specific network to another.

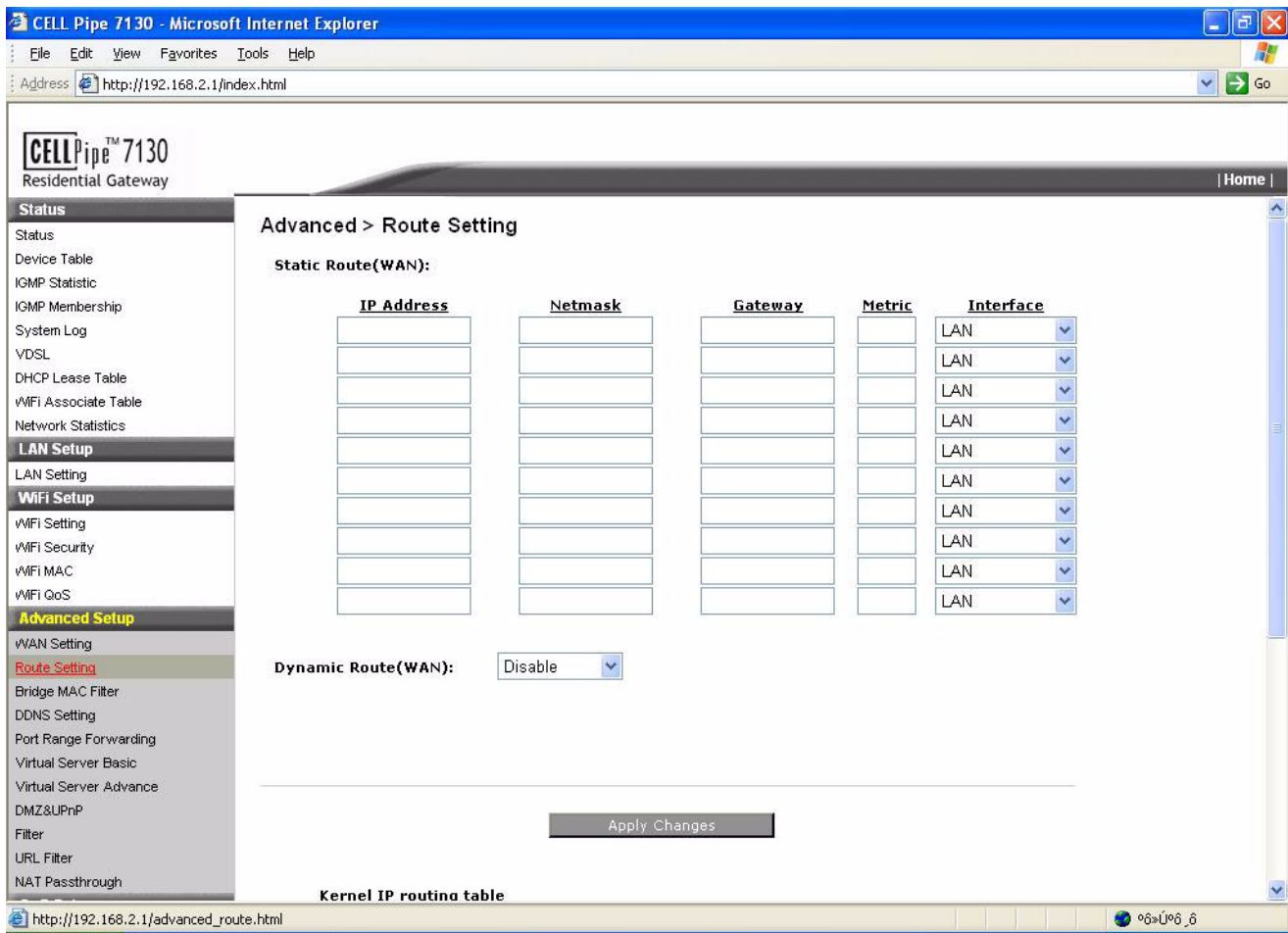
## Before you begin

Make sure that you are connected to the **Home Area** from the 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000 via your internet browser.

- 1 From the main navigation bar, follow this path to setup the **Static Routes**.  
**Status > Route Setting**

**Result:** The **Route Setting** window opens.

- 2 Example of a **Route Setting** window:





- 
- 
- 3 Enter the **IP Address** for the destination network (destination network ID).

---

  - 4 Enter the **Netmask**, the network mask for the destined network.

---

  - 5 Enter the **Gateway**, the address to which the packet is forwarded.

---

  - 6 Enter the **Metric** value, the number that is used to specify the cost of the route, so that the best route (potentially among multiple routes to the same destination) can be selected.

---

  - 7 Enter the **Interface**, the network interface that is used to forward the packet. All the addresses defined by the destination IP Address are reachable over the interface.

---

  - 8 Click **Apply Changes** at the bottom of the page to apply your changes.

**END OF STEPS**

---

# Bridge MAC Filter

## Purpose

Use this procedure to provides filtering for traffic from certain MAC addresses, i.e., MAC access control list.

## Before you begin

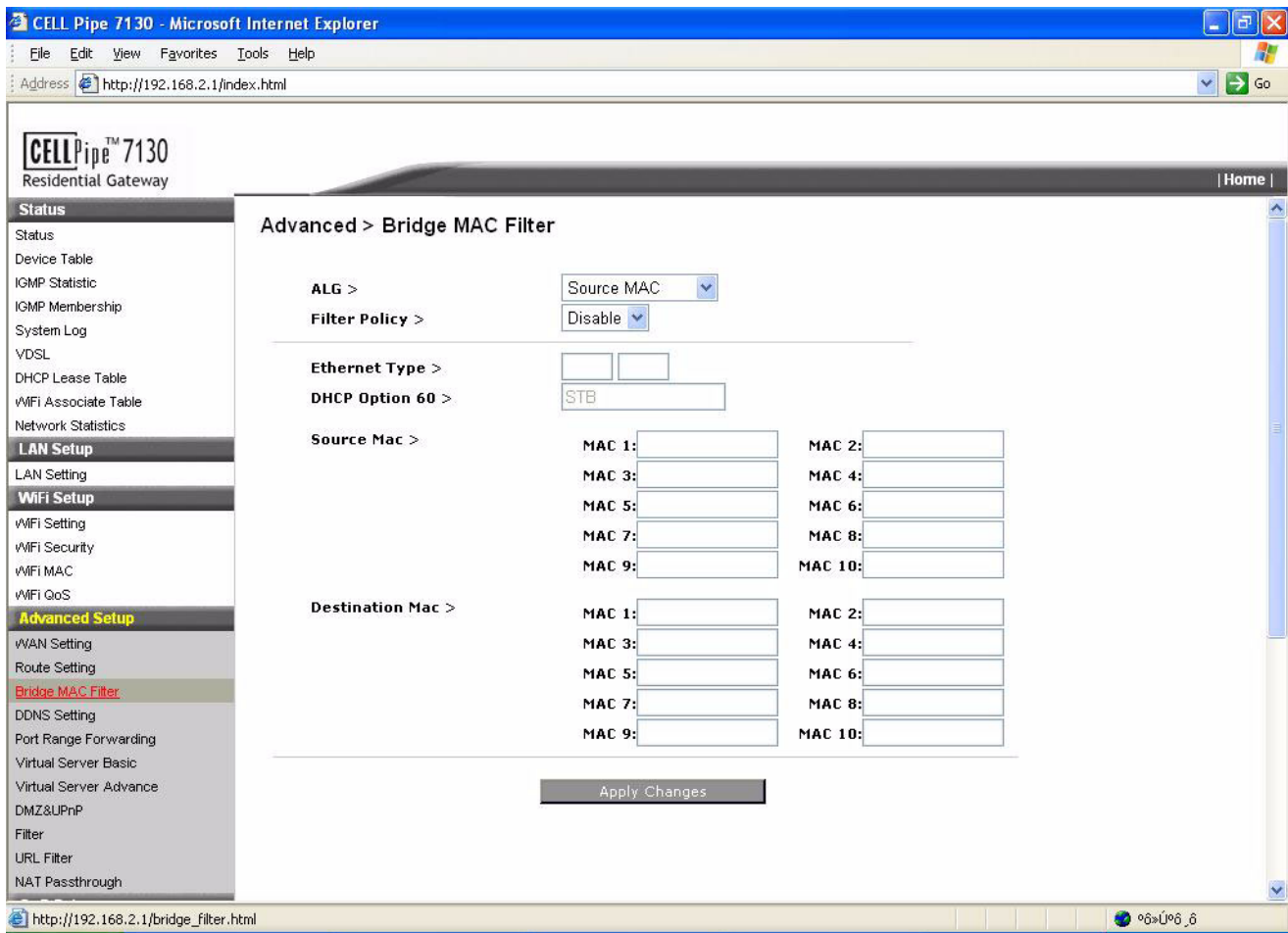
Make sure that you are connected to the **Home Area** from the 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000 via your internet browser.

- 1 From the main navigation bar, follow this path to setup the **Bridge MAC Filter**.

**Status > Bridge MAC Filter**

**Result:** The **Bridge MAC Filter** window opens.

- 2 Example of a **Bridge MAC Filter** window:



- 
- 
- 3 Enter the **IP Address** for the destination network (destination network ID).

---

  - 4 Select your filtering Algorithm, **Alg**, choose from the drop-down menu to specify your filtering rules, i.e., **Source MAC** or **Destination Mac**, then the **Ethernet Type** (the Ethernet type code contains 4 digits of Hex numbers).

---

  - 5 Enable or disable the **Filter Policy**.

---

  - 6 Enter the **Ethernet Type** of traffic (please refer to Ethernet type code for this value) if you select Ethernet type from the above Alg.

---

  - 7 Enter your **Source MAC** and you **Destination Mac** addresses for the designated rule.

---

  - 8 Click **Apply Changes** at the bottom of the page to apply your changes.

**END OF STEPS**

---

---

# DDNS Setting

## Purpose

Use this procedure to register a dynamic IP address with a Domain name over DDNS (Domain Name Service).

## Before you begin

Make sure that you are connected to the **Home Area** from the 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000 via your internet browser.

---

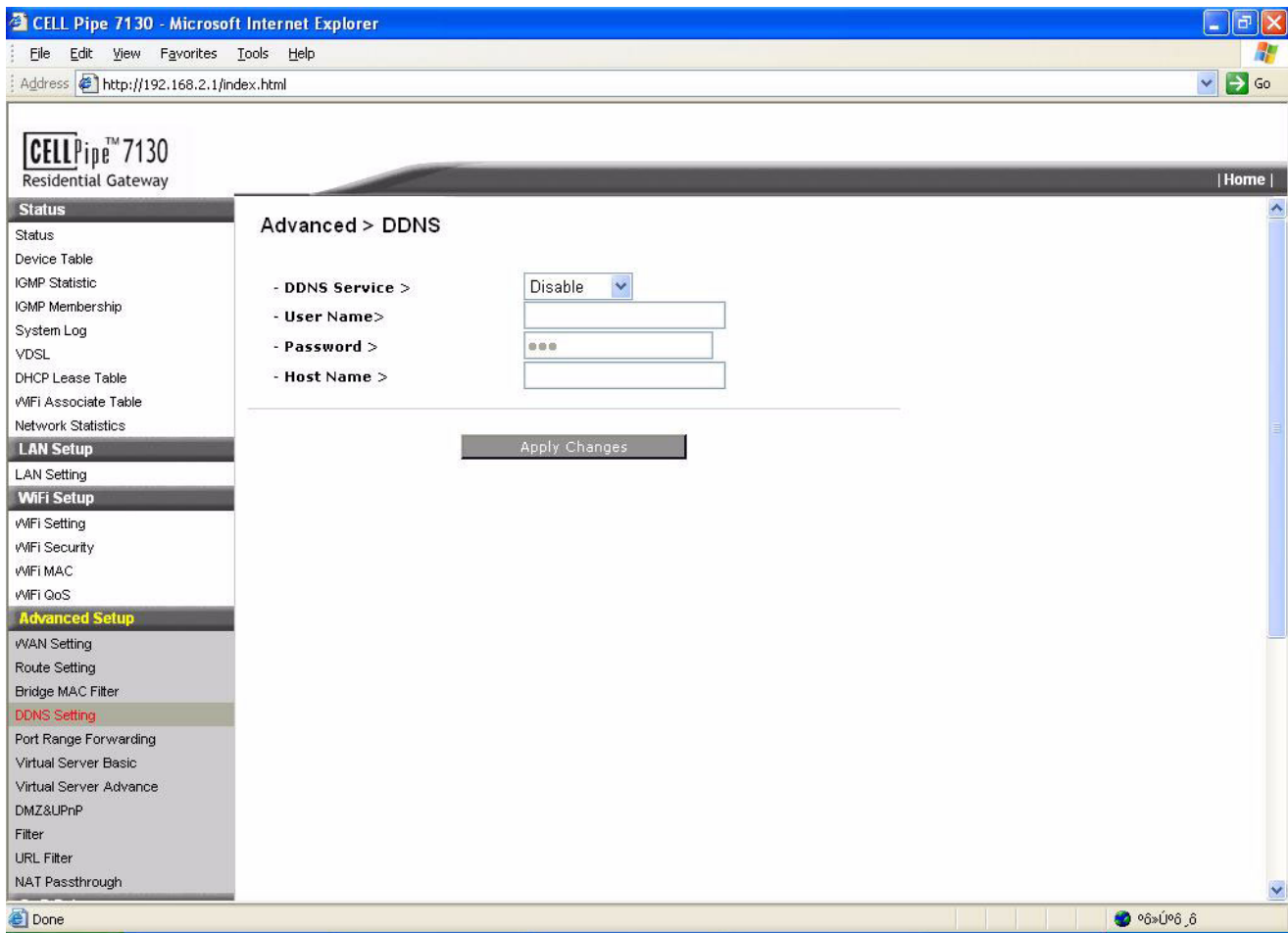
- 1 From the main navigation bar, follow this path to setup the **DDNS**.

**Status > DDNS**

**Result:** The **DDNS** window opens.

---

- 2 Example of a **DDNS** window:



- 
- 
- 3 Enable your DDNS Service first then select from pull-down menu to specify your DDNS service name. You may need to register an account with the above providers first and enter your service name here.  

---
  - 4 Enter the **User Name**, this is your user name for your DDNS account.  

---
  - 5 Enter the **Password**.  

---
  - 6 Enter the **Hostname**.  

---
  - 7 Click **Apply Changes** at the bottom of the page to apply your changes.

**END OF STEPS**

---



- 
- 
- 4 In the **Start Port** column enter the number of the first port of the range you want to seen by users on the Internet and forwarded to your PC.  

---
  - 5 In the **End Port** column enter the number of the last port of the range you want to seen by users on the Internet and forwarded to your PC.  

---
  - 6 From the **Protocol** pull-down menu select the right protocol TCP, UDP or Both. Set this to what the application requires.  

---
  - 7 In the **IP Address** column enter the IP Address of the PC running the application.  

**Note:** Any PC whose port is being forwarded must have a static IP address assigned to it because its IP address may change when using the DHCP function.

---
  - 8 From the **Enable** pull-down menu select the **Enable** to enable port forwarding for the application.  

---
  - 9 Click **Apply Changes** at the bottom of the page to apply your changes.

**END OF STEPS**

---

# Virtual Server Basic

## Purpose

Use this procedure to activate and configure a virtual server in your router.

## Before you begin

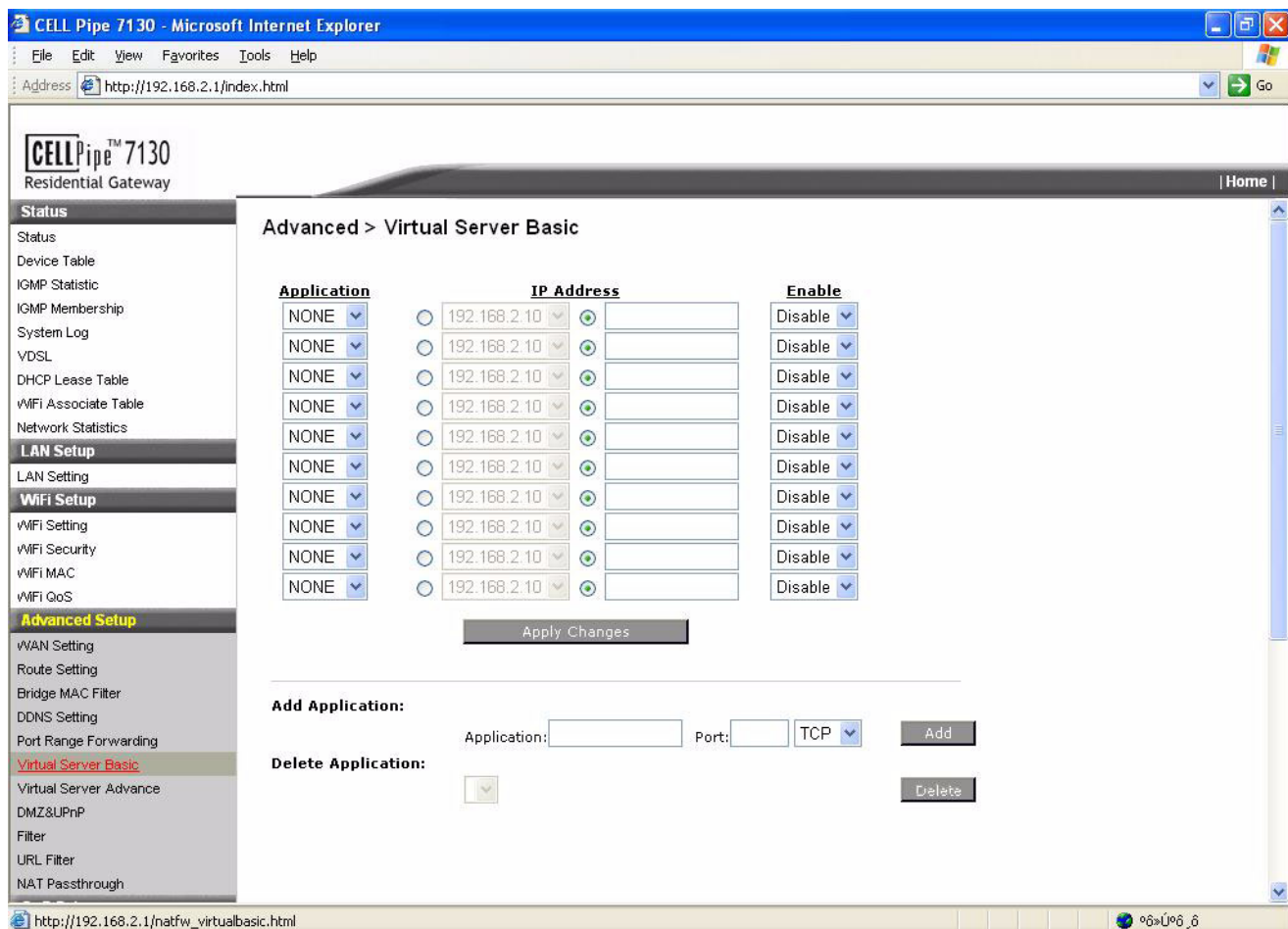
Make sure that you are connected to the **Home Area** from the 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000 via your internet browser.

- 1 From the main navigation bar, follow this path to activate a **Virtual Server**.

**Status > Virtual Server Basic**

**Result:** The **Virtual Server Basic** window opens.

- 2 Example of a **Virtual Server Basic** window:





- 
- 
- 3 From the **Application** pull-down menu select the name for the application to be served by this virtual server.  

---
  - 4 Check the radio button for automatically-configured LAN hosts or choose to enter the **IP Address** manually.  

---
  - 5 Enable or Disable on the pull-down menu the basic virtual server setting.  

---
  - 6 Click **Apply Changes** at the bottom of the page to save your changes.  

---
  - 7 To add or delete an application to or from bypass the firewall restrictions, enter the application name.  

---
  - 8 Enter the application port number and select from TCP, UDP or both.  

---
  - 9 Click **Add** or **Delete**.  

---
  - 10 Click **Apply Changes** at the bottom of the page to save your changes.

**END OF STEPS**

---

# Virtual Server Advance

## Purpose

Use this procedure to activate and configure an advance virtual server in your router.

## Before you begin

Make sure that you are connected to the **Home Area** from the 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000 via your internet browser.

- 1 From the main navigation bar, follow this path to activate an **Advance Virtual Server**.

**Status > Virtual Server Advance**

**Result:** The **Virtual Server Advance** window opens.

- 2 Example of a **Virtual Server Advance** window:

The screenshot shows the web interface of a CELL Pipe 7130 Residential Gateway. The browser window title is "CELL Pipe 7130 - Microsoft Internet Explorer" and the address bar shows "http://192.168.2.1/index.html". The page content is titled "Advanced > Virtual Server Advance". On the left, there is a navigation menu with categories: Status, LAN Setup, WiFi Setup, Advanced Setup, and NAT Passthrough. The "Virtual Server Advance" option is highlighted in red. The main content area contains a table with the following columns: Application, Ext.Port, Protocol, Int.Port, IP Address, and Enable. The table has 15 rows, each with a radio button in the IP Address column and a "Disable" dropdown in the Enable column.

Application	Ext.Port	Protocol	Int.Port	IP Address	Enable
		Both		<input type="radio"/> 192.168.2.10	Disable
		Both		<input type="radio"/> 192.168.2.10	Disable
		Both		<input type="radio"/> 192.168.2.10	Disable
		Both		<input type="radio"/> 192.168.2.10	Disable
		Both		<input type="radio"/> 192.168.2.10	Disable
		Both		<input type="radio"/> 192.168.2.10	Disable
		Both		<input type="radio"/> 192.168.2.10	Disable
		Both		<input type="radio"/> 192.168.2.10	Disable
		Both		<input type="radio"/> 192.168.2.10	Disable
		Both		<input type="radio"/> 192.168.2.10	Disable
		Both		<input type="radio"/> 192.168.2.10	Disable
		Both		<input type="radio"/> 192.168.2.10	Disable
		Both		<input type="radio"/> 192.168.2.10	Disable
		Both		<input type="radio"/> 192.168.2.10	Disable
		Both		<input type="radio"/> 192.168.2.10	Disable

- 
- 
- 3 Specify the **Application** name first, enter the name for the application to be served by this virtual server.  

---
  - 4 Enter the **Ext. Port** number (Ext. Port, means the ports for traffic coming in from the WAN) to be used for this type of application/service. The external port is associated with this application.  

---
  - 5 Specify the **Protocol** to be used with this service (TCP, UDP or both).  
Enter the **Int. Port** number  

---
  - 6 Enter the **Int. Port** number (the ports that the router uses for traffic forwarding). The internal port is associated with the application.  

---
  - 7 Enter the **IP Address** for your server. The IP Address for you server where the service request will be forwarded to.  

---
  - 8 Select **Enable** or **Disable** for this rule.  

---
  - 9 Click **Apply Changes** at the bottom of the page to save your changes.

**END OF STEPS**

---

---

# DMZ and UPnP

## Purpose

Use this procedure to enable or disable DMZ and UPnP.

## Related information

**UPnP** (Universal Plug and Play) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network.

**DMZ** (De-Militarized Zone) Host is a computer without the protection of the firewall. This feature allows a single computer to be exposed to an unrestricted 2-way communication from outside of your network. This feature should be used only if the Virtual Server or Special Applications options do not provide the level of access needed for certain applications.

## Before you begin

Make sure that you are connected to the **Home Area** from the 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000 via your internet browser.

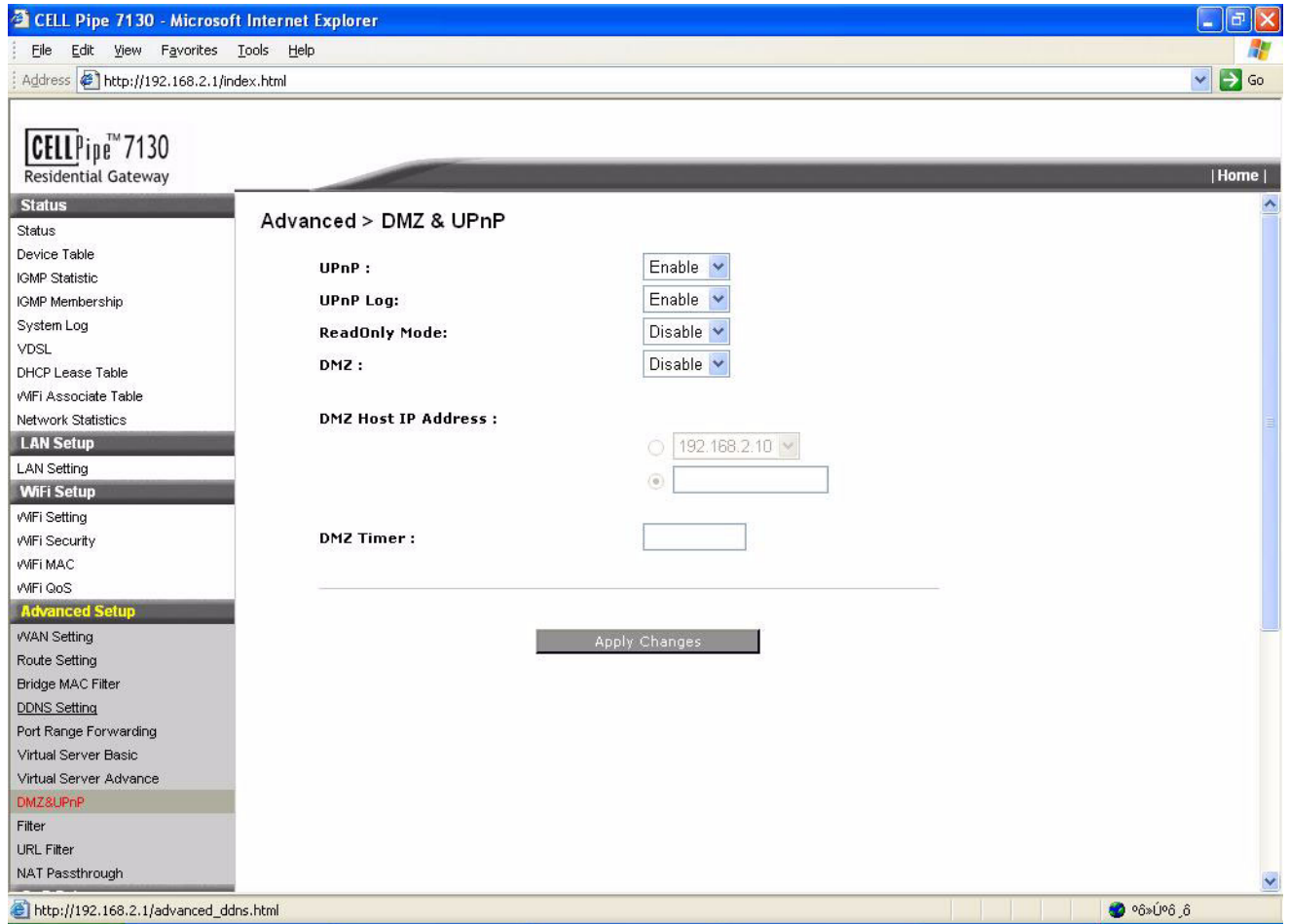
---

- 1 From the main navigation bar, follow this path to activate an **DMZ and UPnP**.

**Status > DMZ and UPnP**

**Result:** The **DMZ and UPnP** window opens.

## 2 Example of a DMZ and UPnP window:



3 **UPnP:** Select **Enable** or **Disable** for the UPnP function.

4 **UPnP Log:** Select **Enable** or **Disable** the UPnP logging activities.

5 **Read Only Mode:** Enable or disable the read only mode.

6 **DMZ Host IP Address:** Enter the IP Address for your DMZ host.

7 **DMZ Timer:** Enter the number of seconds for DMZ Timer.  
For high security, enter a specific time in seconds to allow the length of time in which the DMZ will be functional.

- 
- 
- 8 Click **Apply Changes** at the bottom of the page to save your changes.

**END OF STEPS**

---

# Filter

## Purpose

Use this procedure to disable some internet applications with associated service port numbers for the specific clients.

## Before you begin

Make sure that you are connected to the **Home Area** from the 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000 via your internet browser.

- 1 From the main navigation bar, follow this path to setup the **Filter** functions.

**Status > Filter**

**Result:** The **Filter** window opens.

- 2 Example of a **Filter** window:

The screenshot shows the web interface for the CELL Pipe 7130 Residential Gateway. The browser window title is "CELL Pipe 7130 - Microsoft Internet Explorer" and the address bar shows "http://192.168.2.1/index.html". The page title is "CELL Pipe™ 7130 Residential Gateway" with a "Home" link. A left-hand navigation menu includes sections for "Status", "LAN Setup", "WiFi Setup", "Advanced Setup", and "Filter". The "Filter" section is highlighted in red. The main content area is titled "Advanced > Filter" and contains a table with the following columns: Application, IP Type, IP, Netmask, Protocol, Port Type, Starting Port, Ending Port, and Enable. The table lists 10 entries, all with "Source" IP Type, "255.255.255.255" Netmask, and "Both" Protocol. Below the table, there are two policy settings: "MAC Filter Access Policy" set to "Disable" and "DSCP Policy" set to "Disable" with a "DSCP Value" of "0" (range 0~63). An "Apply Changes" button is located at the bottom of the configuration area.

Application	IP Type	IP	Netmask	Protocol	Port Type	Starting Port	Ending Port	Enable
	Source		255.255.255.255	Both	Source			Enable
	Source		255.255.255.255	Both	Source			Enable
	Source		255.255.255.255	Both	Source			Enable
	Source		255.255.255.255	Both	Source			Enable
	Source		255.255.255.255	Both	Source			Enable
	Source		255.255.255.255	Both	Source			Enable
	Source		255.255.255.255	Both	Source			Enable
	Source		255.255.255.255	Both	Source			Enable
	Source		255.255.255.255	Both	Source			Enable
	Source		255.255.255.255	Both	Source			Enable

MAC Filter Access Policy :

DSCP Policy :  DSCP Value :  (0~63)

- 
- 
- 3 Enter the **Application** name first.  

---
  - 4 Specify the **IP Address** and **Netmask** of the hosts for which you would like to block this type of application.  

---
  - 5 Specify the **Protocol** to be used with this application (TCP, UDP or both).  

---
  - 6 Specify the **Starting Port** and **Ending Port**: This is the starting and ending port number to be blocked for the associated application.  

---
  - 7 **Enable** or **Disable** the filter rules.  

---
  - 8 In addition to the IP address and service port filtering, you can also filter the internet access with the MAC addresses.  

Select **Enable** or **Disable** the **MAC Filter Access Policy** first to allow or not allow the MAC addresses below to access the internet.

---
  - 9 **MAC1-32**: Please enter the MAC addresses to be applied for the filtering policy.  

---
  - 10 Click **Apply Changes** at the bottom of the page to apply your changes.  

---
  - 11 **Enable** or **Disable** the **DSCP Policy**.  

Select **Disable** to disable the **DSCP policy**. Select **Deny** to deny packets with the specified IP header 's DSCP value to access the internet or select **Allow** to allow packets with the specified IP header's DSCP value to access the internet.

DSCP value: means please enter your DSCP value.

---
  - 12 Click **Apply Changes** at the bottom of the page to apply your changes.

END OF STEPS

---



---

# NAT Passthrough

## Purpose

Use this procedure to enable or disable security protocols NAT Passthrough.

## Related information

Internet Protocol Security (IPSec) is a standards-based VPN that offers flexible solutions for secure data communications across a public network like the Internet.

L2TP refers to Layer 2 Tunneling Protocol and PPTP refers to Point to Point Tunneling Protocol. These protocols are used for communications between two networking sites without the expense of leased site-to-site lines.

## Before you begin

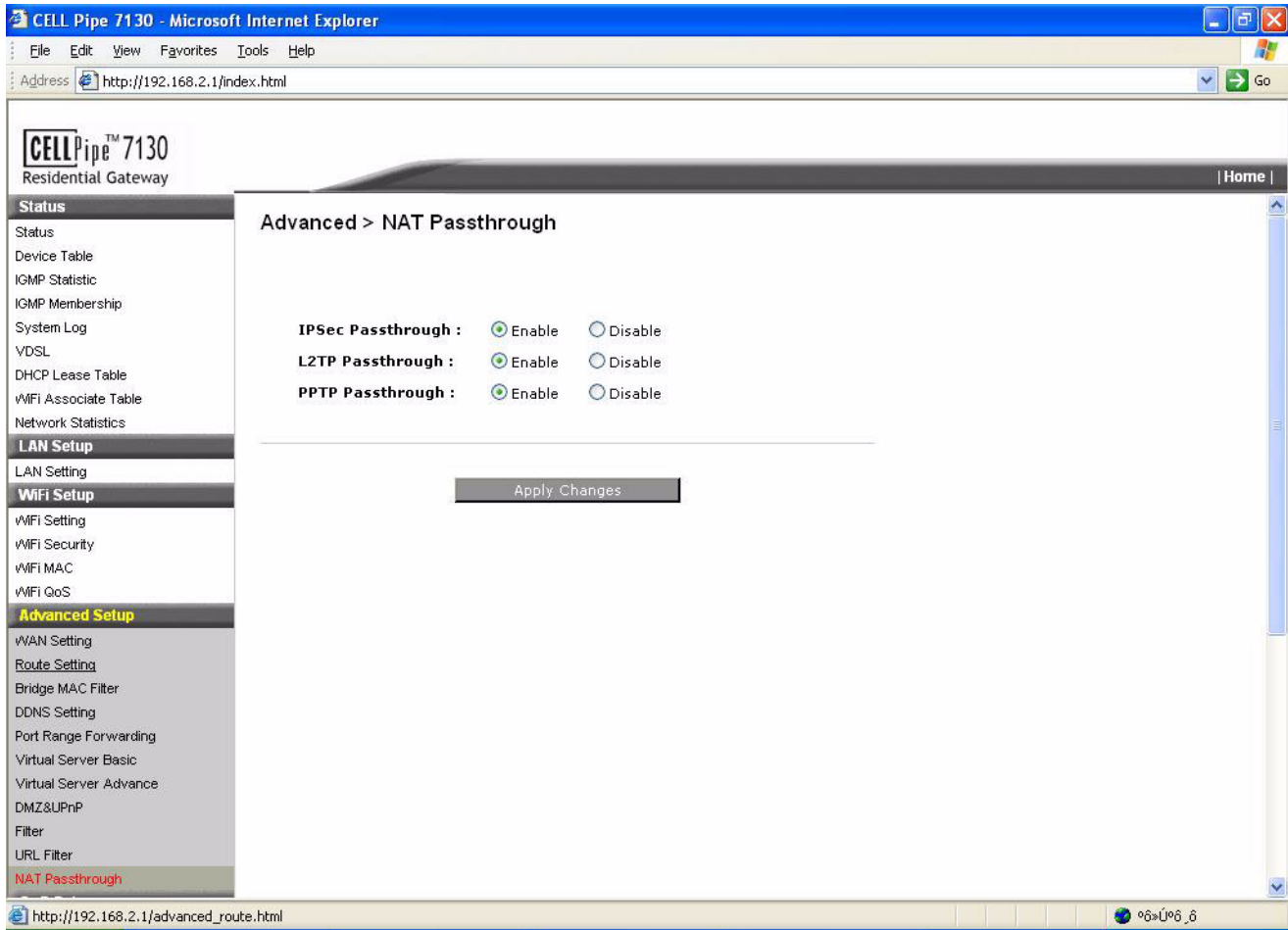
Make sure that you are connected to the **Home Area** from the 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000 via your internet browser.

- 
- 1 From the main navigation bar, follow this path to enable or disable **NAT Passthrough** protocols.

### Status > NAT Passthrough

**Result:** The **NAT Passthrough** window opens.

## 2 Example of a NAT Passthrough window:



### 3 Enable or Disable following security protocols:

- IPSec Passthrough
- L2TP Passthrough
- PPTP Passthrough

### 4 Click **Apply Changes** at the bottom of the page to save your changes.

**END OF STEPS**

---

# QoS Setup

## Purpose

Use this procedure to configure QoS Setup.

## Related information

The IEEE 802.1p specifies the user priority field and defines up to eight separate traffic types. You can give weights to each queue. Thus, you may give priorities to some queues over other queues by assigning weights.

**Contribute:** If you enable this, you may let your queues to give away some up their resource to other queues so that they may also be transmitted when the queue does not use up all of the available bandwidth.

**Borrow:** If you enable this, you may let these queues to use other queues' resources.

## Before you begin

Make sure that you are connected to the **Home Area** from the 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000 via your internet browser.

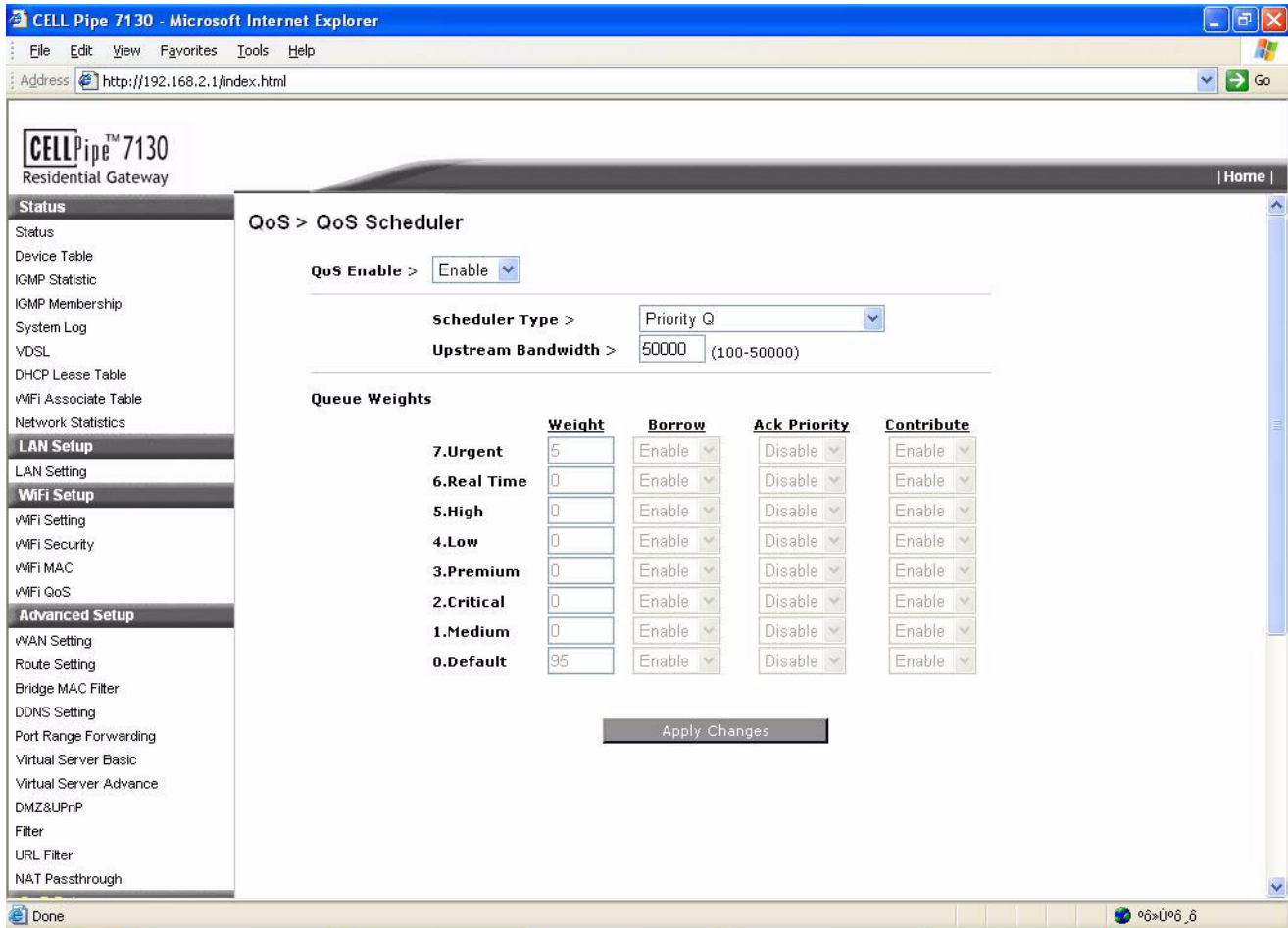
---

- 1 From the main navigation bar, follow this path to enable or disable **QoS Scheduler** protocols.

### Status > QoS Scheduler

**Result:** The **QoS Scheduler** window opens.

## 2 Example of a QoS Scheduler window:



3 Select **Enable** to enable your **QoS Scheduler**.

4 Click the **Scheduler Type** pull down menu, to select the appropriate **Priority Q**.

Following options are displayed:

- **Priority Q**: This type of scheduler will first deliver traffic that has higher weights and only delivers traffic with lower priority when it is empty.
- **Deficit Weighted Priority Fair Q**: For this type of scheduler, each service class will be guaranteed bandwidth but limited to the assigned weights. The eight queues is ranged from low to high according to its sensitivity to jitter.

Enter the appropriate **Upstream Bandwidth** (100... 50000).

5 In the **Queue Weights** field, assign weights to each queue (make sure that they add up to a total of 100).

- 
- **Contribute:** If you enable this, you may let your queues to give away some of their resource to other queues so that they may also be transmitted when the queue does not use up all of the available bandwidth.
  - **Borrow:** If you enable this, you may let these queues to use other queues' resources.
  - **ACK Priority:** If it is enabled, the **TCP ACK Frame** will be put in the front of the queue.
- 

6 Click **Apply Changes** at the bottom of the page to save your changes.

**END OF STEPS**

---

# Default QoS

## Purpose

Use this procedure to setup the QoS default policy for the Internet and IPTV traffic.

## Before you begin

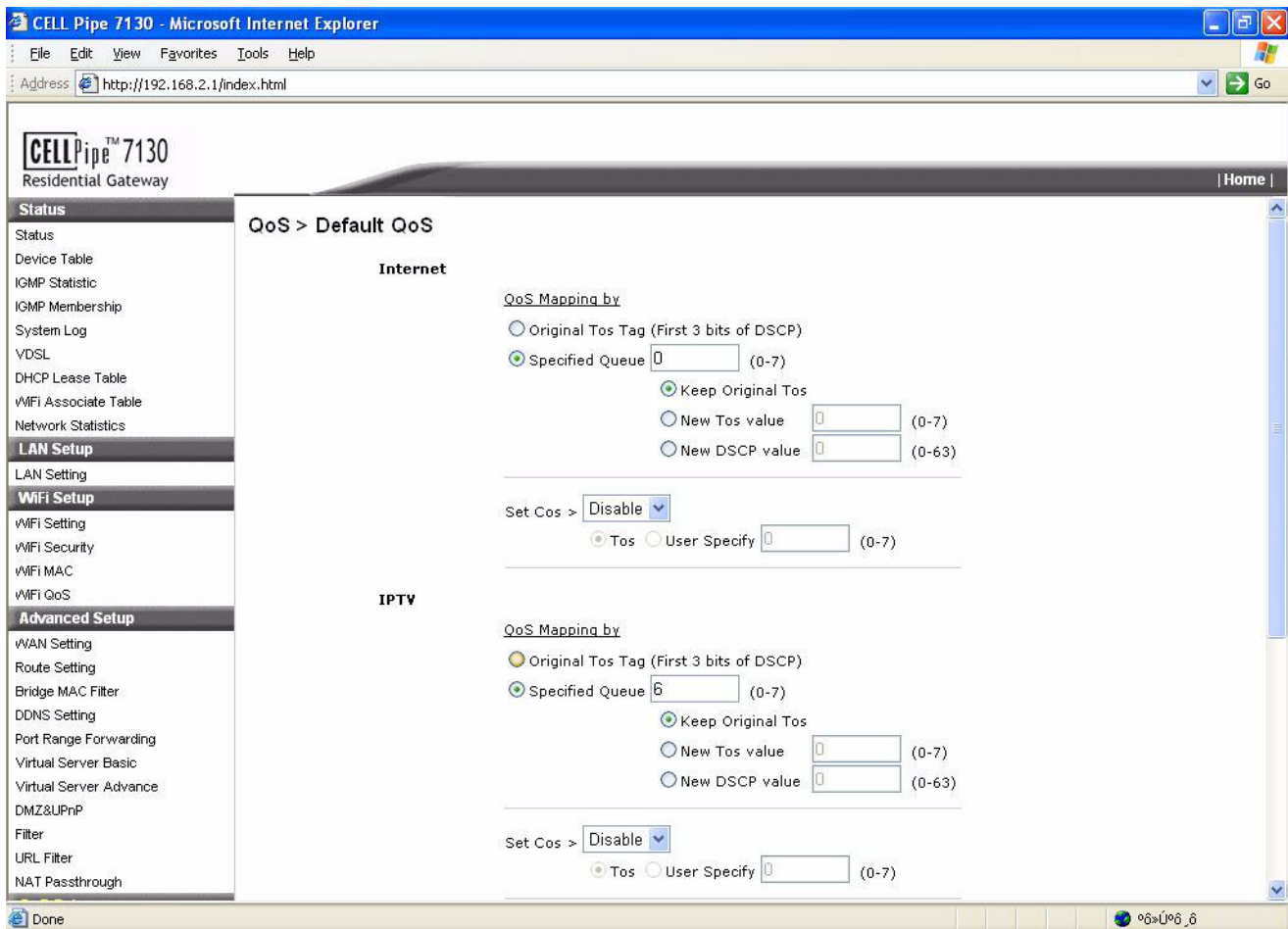
Make sure that you are connected to the **Home Area** from the 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000 via your internet browser.

- 1 From the main navigation bar, follow this path to configure the **Default QoS** method.

### Status > Default QoS

**Result:** The **Default QoS** window opens.

- 2 Example of a **Default QoS** window:



- 3 Configure the QoS default policy for the Internet or IPTV traffic.

- 
- 
- 4 In the **QoS Mapping by** field choose the **Original Tos Tag** if you want to assign queue according to the incoming ToS (Type of Service) value. Then choose the **Specified Queue** and assign a queue number for the incoming traffic (0...7).

---

  - 5 For **ToS** and **DSCP** (DiffServ Code Point) value, you can select **Keep Original Tos** to keep the original value or you can assign a new **ToS** (0...7) value and a new **DSCP** (0...63) value for this type of traffic.

---

  - 6 In the **Set CoS** field configure **CoS** (Class of Service).  
If you enable **Set CoS**, select the **ToS** radio button or enter the appropriate value in the **User Specify** field (0...7).

---

  - 7 To configure **IPTV Default QoS** follow [Step 4](#) to [Step 6](#), then go to [Step 8](#).

---

  - 8 Click **Apply Changes** at the bottom of the page to save your changes.

**END OF STEPS**

---

# QoS Policy

## Purpose

Use this procedure to configure the QoS Policy as provided on the screen.

This screen lists the QoS classifiers or policy. A classifier groups upstream traffic into data flows according to specific criteria such as the source address, destination address, source port or destination port.

## Before you begin

Make sure that you are connected to the **Home Area** from the 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000 via your internet browser.

- 1 From the main navigation bar, follow this path to configure the **QoS Policy** method.

**Status > QoS Policy**

**Result:** The **QoS Policy** window opens.

- 2 Example of a **QoS Policy** window:

The screenshot shows the web interface of the CELL Pipe 7130 Residential Gateway. The browser window title is "CELL Pipe 7130 - Microsoft Internet Explorer" and the address bar shows "http://192.168.2.1/index.html". The page has a navigation menu on the left with categories: Status, LAN Setup, WiFi Setup, and Advanced Setup. The main content area is titled "QoS > QoS Policy".

At the top of the main area, there is a form for defining a QoS classifier with the following fields: Source IP, Subnet Mask, Start Port, End Port, Destination IP, Subnet Mask, Start Port, End Port, and Protocol. A "Select Protocol" button is located to the right of the Protocol field.

Below the classifier form is the "QoS Mapping by" section, which includes the following options:

- Original Tos Tag (First 3 bits of DSCP)
- Specified Queue  (0-7)
  - Keep Original Tos
  - New Tos value  (0-7)
  - New DSCP value  (0-63)
- Set Cos >
- Tos  User Specify  (0-7)

An "Add" button is located below the mapping options.

At the bottom of the main area, there is a table header for the QoS Policy rules:

No.	Source IP	Subnet Mask	StartPort	Destination IP	Subnet Mask	Destination Port	Protocol	Priority	Cos	Tos/DSCP
-----	-----------	-------------	-----------	----------------	-------------	------------------	----------	----------	-----	----------

(Maximum 10 Rules)



- 
- 3 Please enter your settings into the fields provided.

Enter the IP Address and the Subnet Mask of the host that sends the traffic in the **Source IP** field and **Subnet Mask** field.

Enter the port number of the sending host in the **Start Port** and **End Port** field.

Enter the IP Address and the Subnet Mask of the host that receives the traffic in the **Destination IP** field **Subnet Mask** field.

Enter the port number of the destined host in the **Start Port** and **End Port** field.

Select the appropriate protocol e.g. TCP.

---

- 4 In the **QoS Mapping by** field choose the **Original Tos Tag** if you want to assign queue according to the incoming **ToS** (Type of Service) value. Then choose the **Specified Queue** and assign a queue number for the incoming traffic (0...7). For **ToS** and **DSCP** (DiffServ Code Point) value, you can select **Keep Original Tos** to keep the original value or you can assign a new **ToS** (0...7) value and a new **DSCP** (0...63) value for this type of traffic.
- 

- 5 In the **Set CoS** field configure **CoS** (Class of Service).

If you enable **Set CoS**, select the **ToS** radio button or enter the appropriate value in the **User Specify** field (0...7).

---

- 6 Click **Add** at the bottom of the page to save your changes.

**END OF STEPS**

---

# QoS Interface Policy

## Purpose

Use this procedure to configure the Quality of Service for the network interface. Enable or disable the **QoS Interface Policy** for WLAN and LAN.

## Before you begin

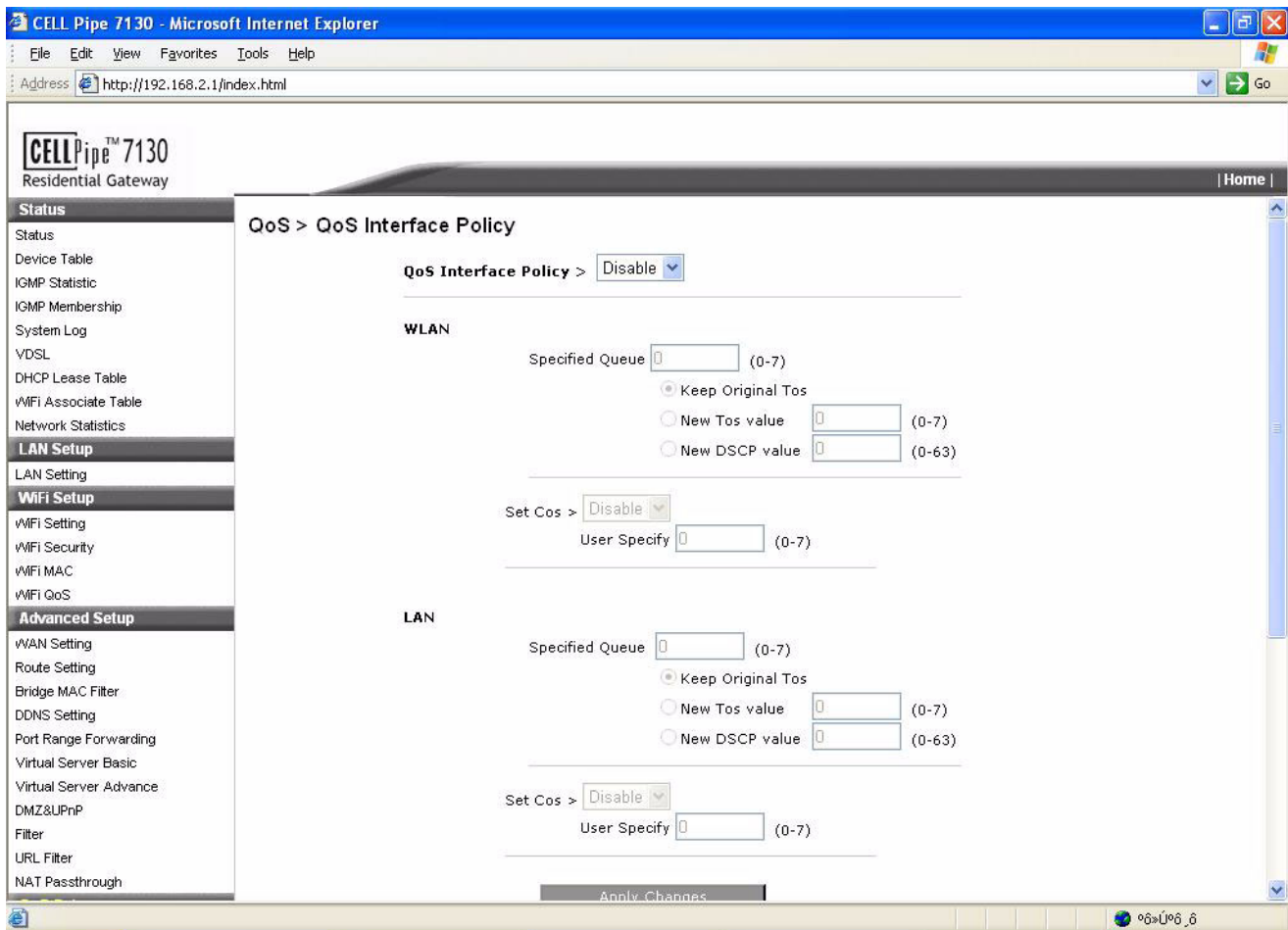
Make sure that you are connected to the **Home Area** from the 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000 via your internet browser.

- 1 From the main navigation bar, follow this path to configure the **QoS Interface Policy** for WLAN and LAN.

**Status > QoS Interface Policy**

**Result:** The **QoS Interface Policy** window opens.

- 2 Example of a **QoS Interface Policy** window:



- 
- 
- 3 The **QoS Interface Policy** screen will let you to setup different QoS policy rules for wireless LAN and wired LAN network traffic.  

---
  - 4 Enable the **QoS Interface Policy** (default value is Disable).  

---
  - 5 Configure the **QoS Interface Policy** for WLAN and LAN network traffic.  
Choose the **Specified Queue** and assign a queue number for the incoming traffic (0...7).  
For **ToS** and **DSCP** (Differentiated Services Code Point) value, you can select **Keep Original Tos** to keep the original value or you can assign a new **ToS** (0...7) value and a new **DSCP** (0...63) value for this type of traffic.  

---
  - 6 In the **Set CoS** field configure **CoS** (Class of Service).  
Therefor enable **Set CoS**, and enter the appropriate value in the **User Specify** field (0...7).  

---
  - 7 To configure wired LAN **QoS Interface Policy** follow [Step 4](#) to [Step 6](#), then go to [Step 8](#).  

---
  - 8 Click **Apply Changes** at the bottom of the page to save your changes.

**END OF STEPS**

---

# QoS ALG

## Purpose

Use this procedure to enable or disable **QoS** for the SIP (Session Initiated Protocol) and RTP (Real-time Transport Protocol). SIP is for the implementation of VOIP. RTP is the protocol which provides end-to-end delivery services for data with real-time characteristics, such as interactive audio and video.

## Before you begin

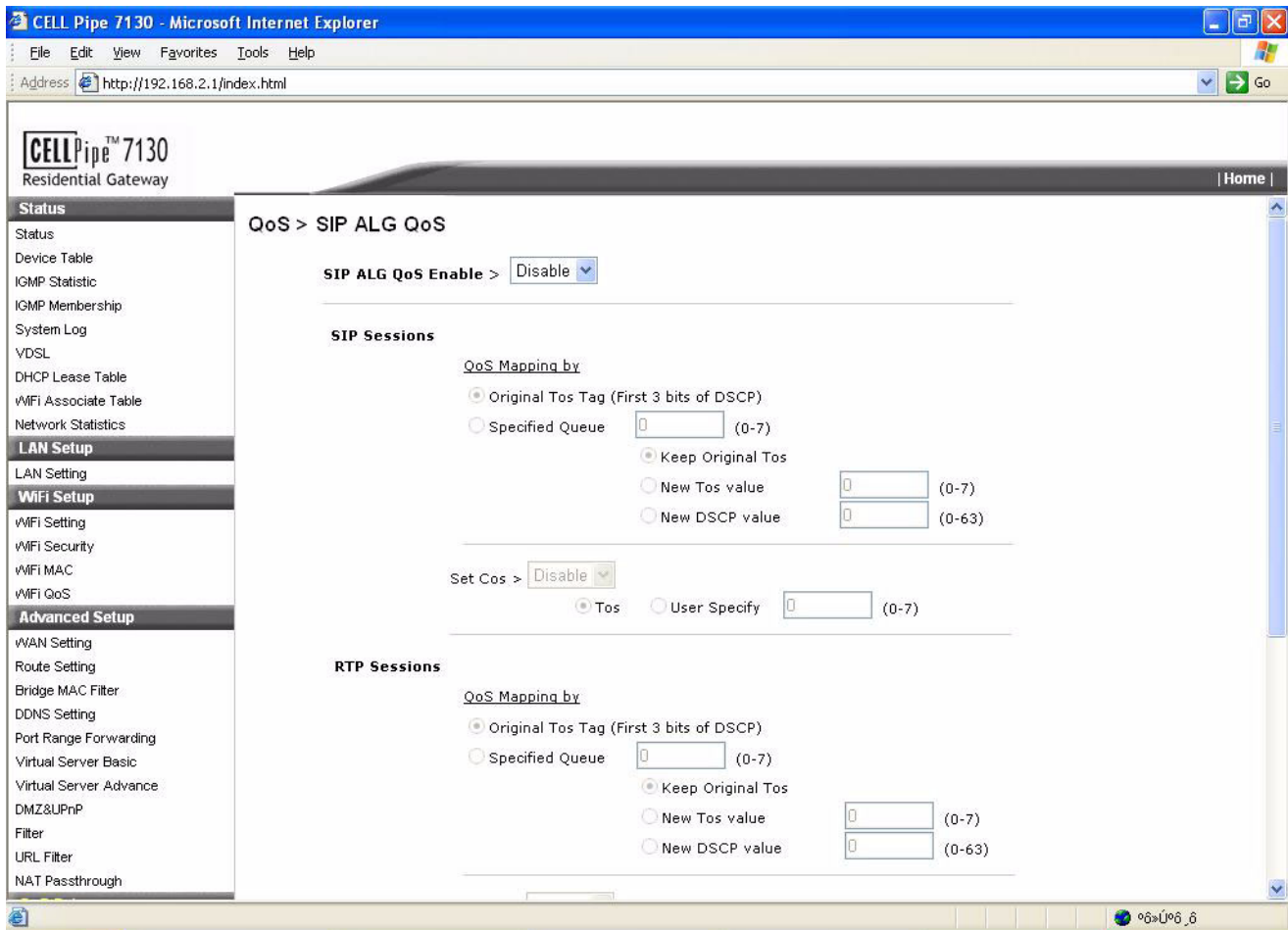
Make sure that you are connected to the **Home Area** from the 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000 via your internet browser.

- 1 From the main navigation bar, follow this path to configure the **SIP ALG QoS** method.

**Status > SIP ALG QoS**

**Result:** The SIP ALG QoS window opens.

- 2 Example of a SIP ALG QoS window:



---

3 The **SIP ALG QoS** screen will let you to enable or disable QoS for the Session Initiated Protocol and Real-time Transport Protocol (RTP). The users can also setup different QoS policy for SIP and RTP sessions.

4 Configure the **SIP ALG QoS** for SIP sessions and RTP sessions.

In the **QoS Mapping by** field choose the **Original Tos Tag** if you want to assign queue according to the incoming ToS (Type of Service) value. Then choose the **Specified Queue** and assign a queue number for the incoming traffic (0...7).

For **ToS** and **DSCP** (DiffServ Code Point) value, you can select **Keep Original Tos** to keep the original value or you can assign a new **ToS** (0...7) value and a new **DSCP** (0...63) value for this type of traffic.

5 In the **Set CoS** field configure **CoS** (Class of Service).

If you enable **Set CoS**, select the **ToS** radio button or enter the appropriate value in the **User Specify** field (0...7).

6 Click **Apply Changes** at the bottom of the page to save your changes.

**END OF STEPS**

---

---

# Reboot Gateway

## Purpose

Use this procedure to reboot the gateway.

## Before you begin

Make sure that you are connected to the **Home Area** from the 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000 via your internet browser.

---

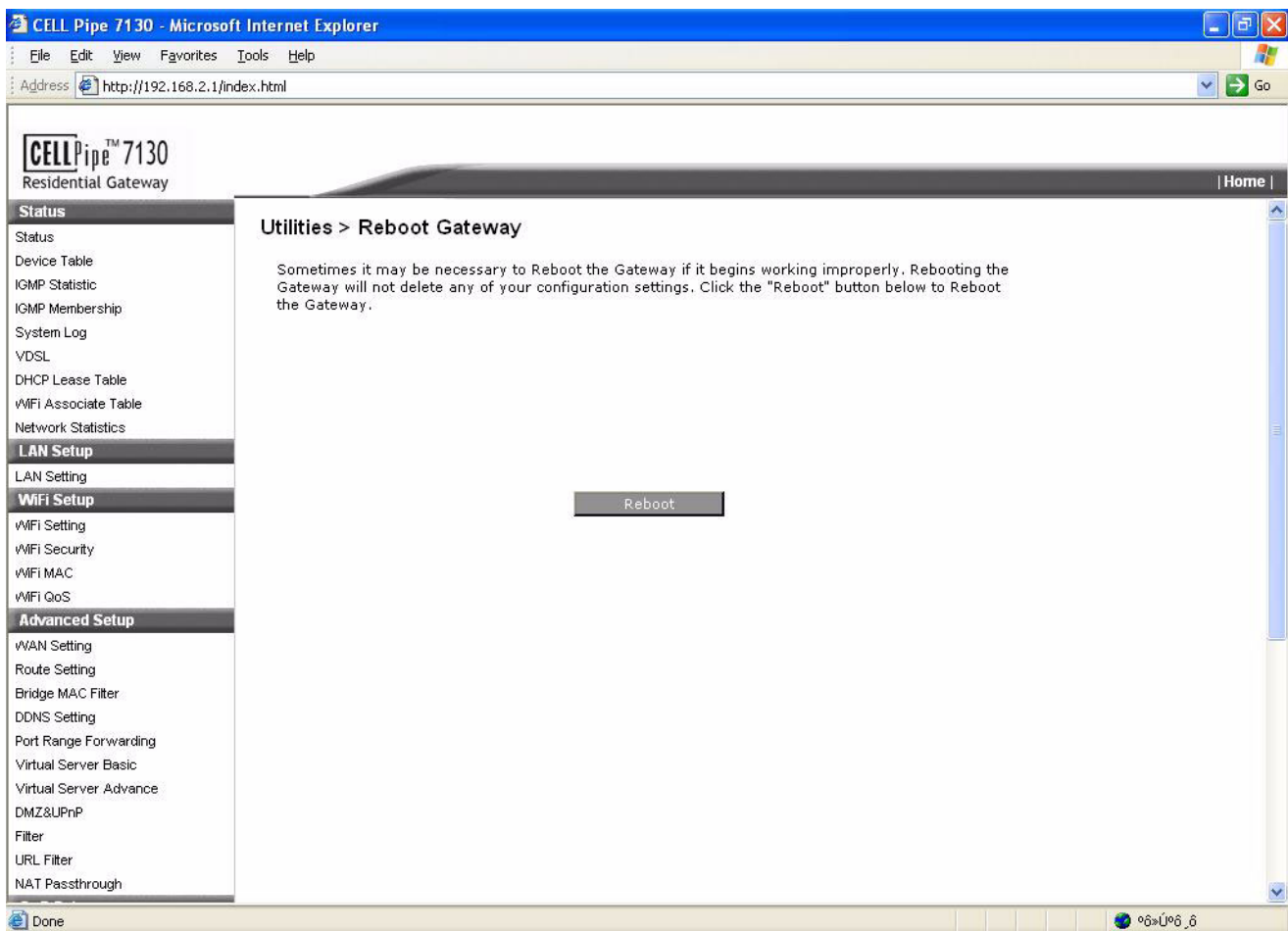
- 1 From the main navigation bar, follow this path to configure the **Reboot Gateway** method.

### Status > Reboot Gateway

**Result:** The **Reboot Gateway** window opens.

---

- 2 Example of a **Reboot Gateway** window:



- 
- 
- 3 Click **Reboot** to reboot your router.

**Result:** The PWR LED will go off and stay on if the restart is successful. Then you may log into the device again.

**Note:** Rebooting your router will not delete your configuration settings.

**END OF STEPS**

---

---

# Restore Factory Defaults

## Purpose

Use this procedure to the restore factory defaults.

## Before you begin

Make sure that you are connected to the **Home Area** from the 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000 via your internet browser.

---

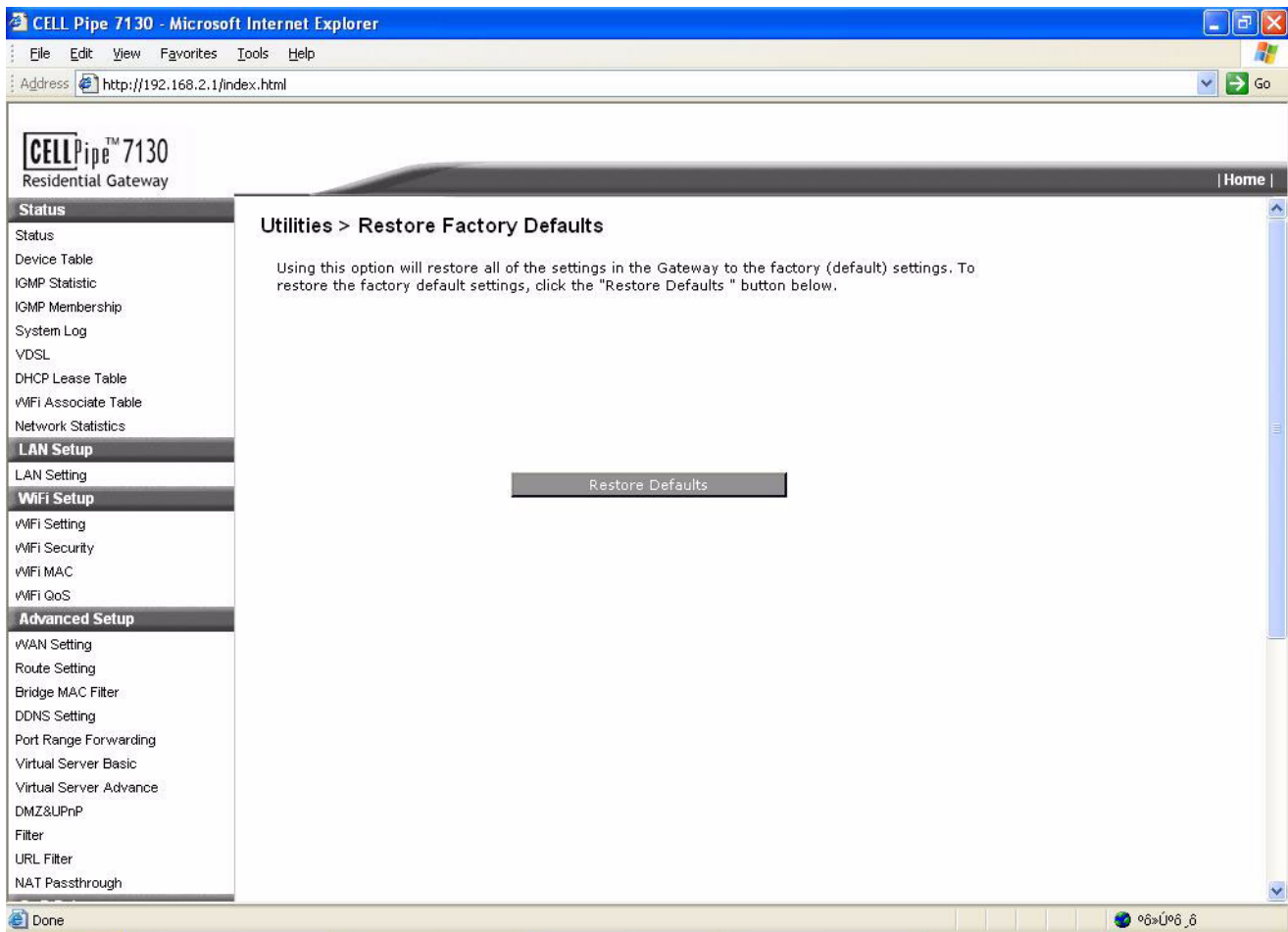
- 1 From the main navigation bar, follow this path to the **Restore Factory Defaults**.

**Status > Restore Factory Defaults**

**Result:** The **Restore Factory Defaults** window opens.

---

- 2 **Restore Factory Defaults** window:





- 
- 
- 3 Click **Restore Defaults** to reset all configuration settings to their default values.

**Result:** After restoring the router is accessible under the default IP address 192.168.2.1 and the default user name and password *admin*.

**Note:** A restore to the factory defaults will delete all your configuration settings. Any settings you have saved will be lost when the default settings are restored.

**END OF STEPS**

---

---

# Web Firmware Upload

## Purpose

Use this procedure to update your router's firmware in this screen

## Before you begin

Make sure that you are connected to the **Home Area** from the 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000 via your internet browser.

---

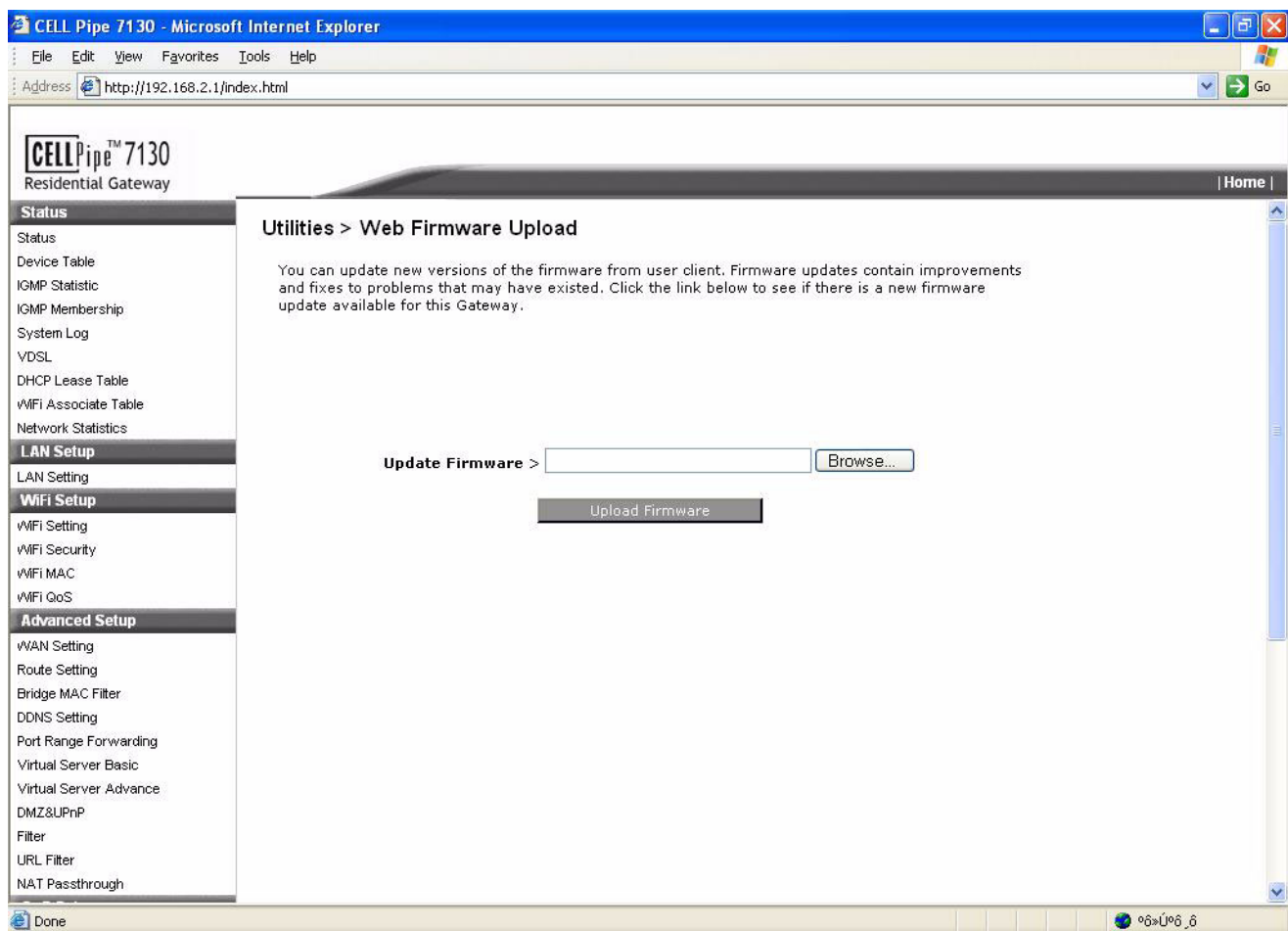
- 1 From the main navigation bar, follow this path to the **Web Firmware Upload**.

**Status > Web Firmware Upload**

**Result:** The **Web Firmware Upload** window opens.

---

- 2 **Web Firmware Upload** window:



**Important!** When you upgrade your router with new firmware, you lose all your configuration settings, so make sure you write down the router settings before you upgrade the firmware.

- 
- 
- 3 Download the firmware upgrade file from the website.

The new firmware versions are posted at [www...](#) and can be downloaded for free.

---

- 4 Click **Browse...** to locate your firmware upgrade and press **Upload Firmware** to upload the new firmware, wait until the upgrade is finished.

**Important!** Do not power off the router or press the reset button while the firmware is being upgraded.

**END OF STEPS**

---

# System Settings

## Purpose

Use this procedure to change your web administrator's login name and password.

## Before you begin

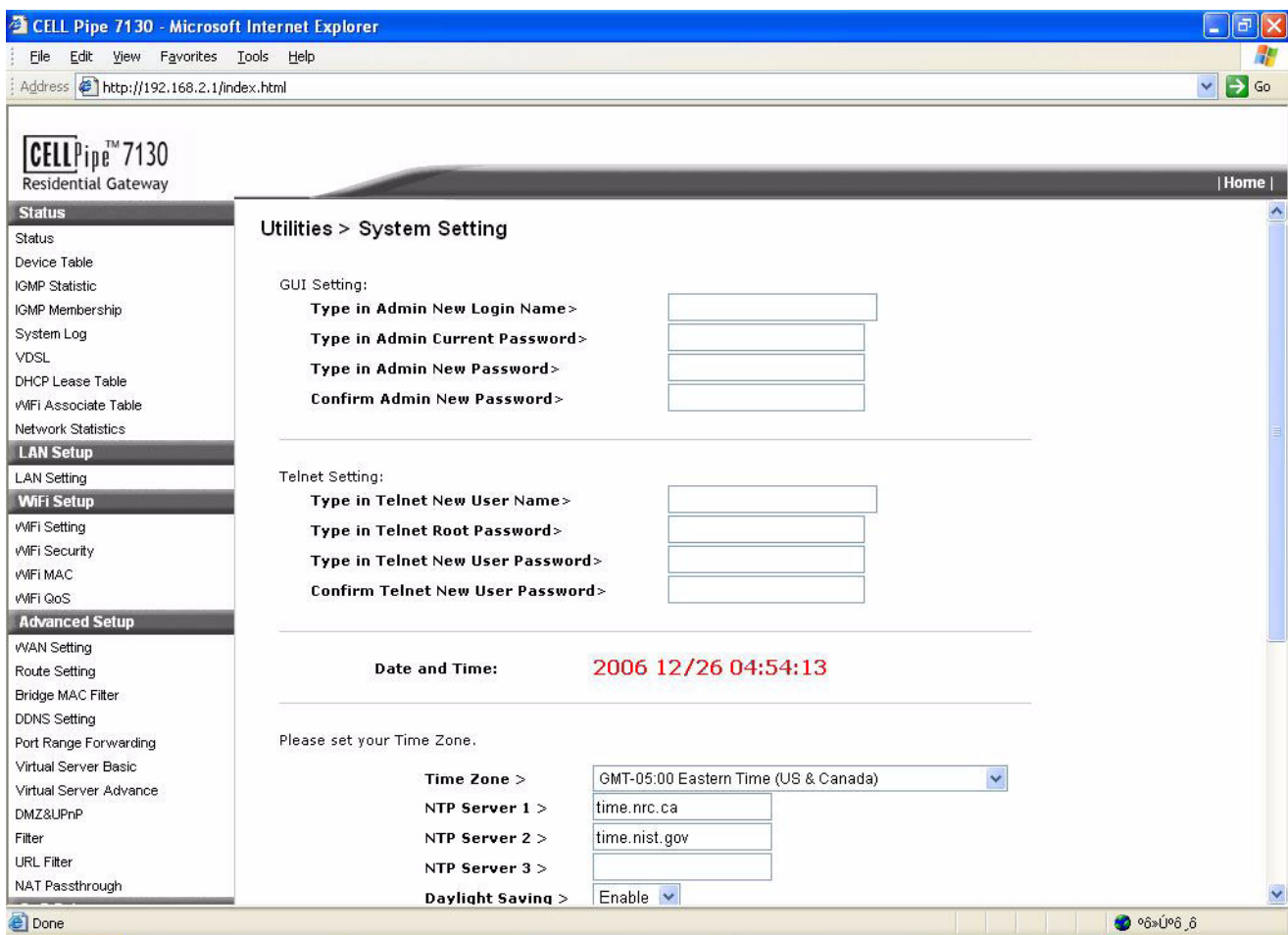
Make sure that you are connected to the **Home Area** from the 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000 via your internet browser.

- 1 From the main navigation bar, follow this path to the **System Settings**.

**Status > System Settings**

**Result:** The **System Settings** window opens.

- 2 **System Settings** window:



- 
- 
- 3 In the **GUI Settings** section, you can change the **Admin Password**.

**Important!** It is strongly recommended that you change the factory default password of the router, which is `admin`.

---

- 4 In the **Telnet Settings** section, you can change the **Telnet Root Password**.

**Important!** It is strongly recommended that you change the factory default telnet login name and password, which is `admin` and `admin`.

---

- 5 Specify the **Time Zone** for your location by selecting the appropriate time zone from the pull-down menu.
- 

- 6 Enter the IP address or the URL of your time Server, **NTP Server 1..3**.
- 

- 7 Enable the option **Daylight Saving** if you use daylight savings time.

Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.

---

- 8 Click **Apply Changes** at the bottom of the page to save your changes.

**END OF STEPS**

---

---

# MCL Settings

## Purpose

Use this procedure to turn on or off certain type of service from the router. Thus, it gives you more control over the router's security.

## Before you begin

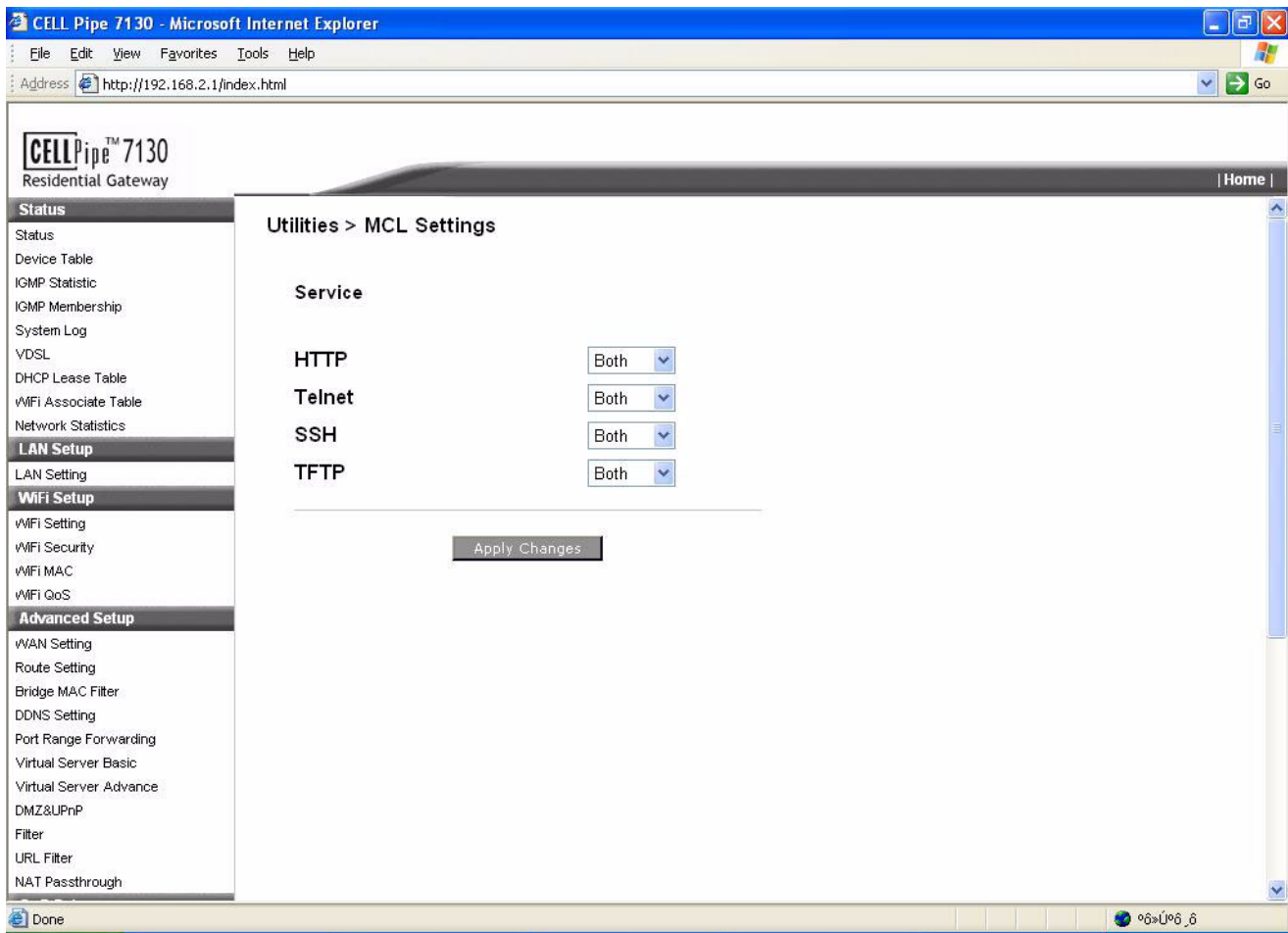
Make sure that you are connected to the **Home Area** from the 7130 RG 5Ve.A2000/7130 RG 5Ve.B2000 via your internet browser.

- 
- 1 From the main navigation bar, follow this path to configure the **MCL Settings** method.  
**Status > MCL Settings**

**Result:** The **MCL Settings** window opens.

---

- 2 **MCL Settings** window:



---

3 From the pull-down menu for each service type, select the appropriate setting.

---

4 Following options are displayed:

- **Disable:** Turn off this type of service on the CPE.
  - **LAN:** Only allow hosts from the LAN to access this type of service.
  - **WAN:** Only allow hosts from the WAN to access this type of service.
  - **Both:** Allow both LAN and WAN hosts to access this type of service
- 

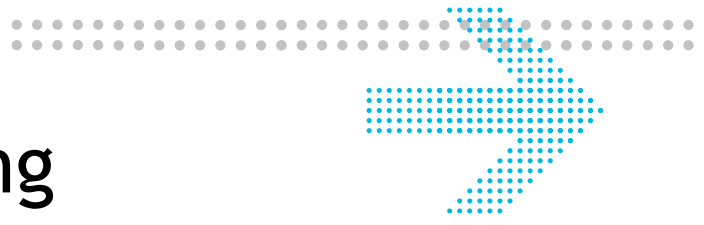
5 Click **Apply Changes** at the bottom of the page to save your changes.

**END OF STEPS**

---







# A Troubleshooting

## Overview

### Purpose

This Appendix provides guidance for troubleshooting. The CPE operation can easily be monitored via the LED indicators to identify problems. The table below describes common problems you may encounter and possible solutions.

### Diagnosing

Symptom	Possible cause	Solution
<i>PWR</i> LED does not light up after power on.	Power outlet, power cord, or power adapter may be defective.	<ul style="list-style-type: none"><li>• Check the power outlet by plugging in another device that is functioning properly.</li><li>• Call the Customer Support Hotline or return the device to the vendor.</li></ul>
<i>DSL</i> LED is flashing slowly after making a connection.	The cabling, or the VDSL port on the CPE may be defect.	<ul style="list-style-type: none"><li>• Verify that the CPE is powered on.</li><li>• Make sure the cable is correctly plugged into the VDSL line wall outlet and the CPE connector labeled "VDSL".</li></ul>
<i>LAN</i> LED does not light up after making a connection.	Network interface (e.g., a network adapter card in the attached computer), network cable, or the LAN port on the CPE may be defect or not connected.	<ul style="list-style-type: none"><li>• Verify that the CPE and the computer device are powered on.</li><li>• Make sure that the cable is plugged into both, the CPE and the device.</li><li>• Verify that the proper cable type is used and its length does not exceed specified limits.</li><li>• Check the network adapter in the device and the cable connections for possible defects. Replace the defective adapter or cable if necessary.</li></ul>
<i>WLAN</i> LED is flashing after wireless traffic.	WLAN link off-grade or the WLAN module may be defect.	<ul style="list-style-type: none"><li>• Check if the WLAN module is in operation and works properly.</li><li>• Make sure that the antenna is correctly plugged into the WLAN socket on the CPE.</li></ul>

Symptom	Possible cause	Solution
<i>DIAG</i> LED is flashing	At the moment a CPE firmware upgrade is executed.	<ul style="list-style-type: none"> <li>• Wait until the firmware upgrade is passed and the <i>DIAG</i> LED is “On” (wireless enabled).</li> </ul>
<i>INTERNET</i> LED is “Off”	You cannot connect to the Internet. The PC may not be configured as required or the network adapter driver may not fit.	<ul style="list-style-type: none"> <li>• Check that your PC is properly configured for TCP/IP. (See <a href="#">Configuring the TCP/IP protocols on the PC</a>).</li> <li>• Make sure the correct network adapter driver is installed for your operating system. If necessary, try reinstalling the driver.</li> <li>• Check that the speed of the network adapter or duplex mode has not been configured manually. We recommend to set the adapter to auto-negotiation when installing the network driver.</li> <li>• Did you establish your network connection before starting your browser?</li> <li>• Verify your username and password entry in the network connection tab.</li> </ul>



# B Configuring the TCP/IP protocols on the PC

## Overview

### Purpose

To connect the CPE to a PC through its Ethernet port, the PC must have an Ethernet network adapter card installed, and be configured for the TCP/IP protocol. Many service providers configure TCP/IP for client PC automatically using a networking technology known as Dynamic Host Configuration Protocol (DHCP). Other service providers may specify an IP configuration (known as a static IP address), which must be entered manually.

Carry out the following steps to check that the computer's Ethernet port is correctly configured for DHCP.

### Windows 95/98/NT

1. Click "Start/Settings/Control Panel."
2. Click the "Network" icon.
3. For Windows NT, click the "Protocols" tab.
4. Select "TCP/IP" from the list of network protocols; this may include details of adapters installed in your computer.
5. Click "Properties."
6. Check the option "Obtain an IP Address."
7. Click "OK" to close the TCP/IP Properties window.
8. Restart your computer.

### Windows 2000

1. Click "Start/Settings/Network and Dial-up Connections."
2. Right-click "Local Area Connections."
3. Select "TCP/IP" from the list of network protocols.
4. Click on "Properties."
5. Select the option "Obtain an IP Address."
6. Click "OK" to close the TCP/IP Properties window.
7. Restart your computer.

---

**Windows XP**

1. Click “Start/Control Panel/Network and Internet Connections.”  
(You may need to choose Settings before Control Panel, depending on your Start Menu configuration.)
2. Right-click the “Local Area Connection” icon for the adapter you want to configure, and choose “Properties.”
3. Highlight “Internet Protocol (TCP/IP).”
4. Click “Properties.”
5. Select the option “Obtain an IP address automatically” and “Obtain DNS server address automatically.”
6. Click “OK” to close the TCP/IP Properties window.
7. Restart your computer.

**Windows Vista**

1. Click “Start/Control Panel/Network and Internet.”  
(You may need to choose Settings before Control Panel, depending on your Start Menu configuration.)
2. Click “Network and Sharing Center” then click “Manage network connections.”
3. Right-click the “Local Area Connection” and choose Properties.
4. Select “Internet Protocol Version 4(TCP/IPv4).”
5. Click “Properties.”
6. Select “Obtain an IP address automatically” and “Obtain DNS server address automatically.”
7. Click “OK” to close the TCP/IP Properties window.
8. Restart your computer.

**Mac OS**

1. Pull down the Apple Menu. Click “Control Panels” and select “TCP/IP.”
2. In the TCP/IP dialog box, verify that “Ethernet” is selected in the “Connect Via:” field.
3. If “Using DHCP Server” is already selected in the “Configure” field, your computer is already configured for DHCP. Otherwise, select “Using DHCP Server” in the “Configure” field and close the window.
4. Another box will appear asking whether you want to save your TCP/IP settings. Click “Save.”
5. Your service provider will now be able to automatically assign an IP address to your computer.



# C Product conformance

## Overview

### Purpose

This section provides the EU Declaration of Conformity (CE) statements, additional international conformity statements.

Note that in regions such as the European Union, the statements that are required are determined primarily by national or multi-national regulations. However, in some regions, contact terms determine which statements are required.

The presence of the statement indicates that the product does comply with that statement wherever it is required to do so.

## Europe - 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:


- EN60950-1:2001 A11:2004  
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 V1.6.1: (2005-09)  
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 V1.2.1 (2002-08)
  - Electromagnetic compatibility and Radio spectrum Matters (ERM);  
ElectroMagnetic Compatibility (EMC) standard for radio equipment and services;  
Part 17: Specific conditions for 2,4 GHz wideband transmission systems and  
5 GHz high performance RLAN equipment

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.

**CE 0560** 

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

---

## 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!**

### **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.