Conceptronic C150APRA2

Extended User Manual

Congratulations on the purchase of your Conceptronic wireless ADSL modem router.

This user manual gives you a step-by-step explanation of how to install and use the Conceptronic wireless ADSL modem router.

When you need more information or support for your product, we advise you to visit our **Service & Support** website at www.conceptronic.net/support and select one of the following options:

- **FAQ** : Frequently Asked Questions database
- **Downloads** : Manuals, Drivers, Firmware and more downloads
- **Contact** : Contact Conceptronic Support

For general information about Conceptronic products visit the Conceptronic website at www.conceptronic.net.

The information in this quick installation guide is based on Windows 7 and Vista, but can differ from your computer when you are using a different operating system.

Table of contents

1. Introduction

The C150APRA2 supports multiple line modes. It provides four 10/100 base-T Ethernet interfaces at the user end. The device provides high speed ADSL broadband connection to the Internet or Intranet for high-end users, such as net cafes and office users. It provides high performance access to the Internet, downstream up to 24 Mbps and upstream up to 1 Mbps.
The device supports WLAN access. It can connect to the Internet through a WLAN AP or WLAN device. It complies with IEEE 802.11, 802.11b/g specifications, WEP, WPA, and WPA2 security specifications.
In the IEEE 802.11n mode, 1T1R can reach the maximum wireless transmission rate of 150 Mbps.

1.1 Safety Precautions

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

- Use volume labels to mark the type of power.
- Use the power adapter packed within the device package.
- Pay attention to the power load of the outlet or prolonged lines. An overburden power outlet or damaged lines and plugs may cause electric shock or fire accident. Check the power cords regularly. If you find any damage, replace the power cords at once.
- Proper space left for heat dissipation is necessary to avoid damage caused by overheating to the device. The long and thin holes on the device are designed for heat dissipation to ensure that the device works normally. Do not cover these heat dissipation holes.
- Do not put this device close to a place where a heat source exits or high temperature occurs. Avoid the device from direct sunshine.
- Do not put this device close to a place where it is over damp or watery. Do not spill any fluid on this device.
- Do not connect this device to any PCs or electronic products, unless our customer engineer or your broadband provider instructs you to do this, because any wrong connection may cause power or fire risk.
- Do not place the device on an unstable surface or support.

1.2 Features

The device supports the following features:

- 802.11b/g/n
- Various line modes
- External PPPoE dial-up access
- Internal PPPoE and PPPoA dial-up access
- 1483 Bridged, 1483 Routed, and MER access
- Multiple PVCs (up to eight) that can be isolated from each other
- A single PVC with multiple sessions
- Multiple PVCs with multiple sessions
- Binding of ports with PVCs
- 802.1Q
- DHCP server
- NAT and NAPT
- Static routing
- Firmware upgrade through Web or TFTP
- Restore to the factory defaults
- DNS
- Virtual server
- DMZ
- Web user interface
- Telnet CLI
- System status displaying
- PPP session PAP, CHAP, and MS-CHAP
- IP filter
- IP QoS
- Remote access control
- Line connection status test
- Remote management through telnet or HTTP
- Backup and restoration of configuration file
- Ethernet interface supports crossover detection, auto-correction and polarity correction
- UPnP

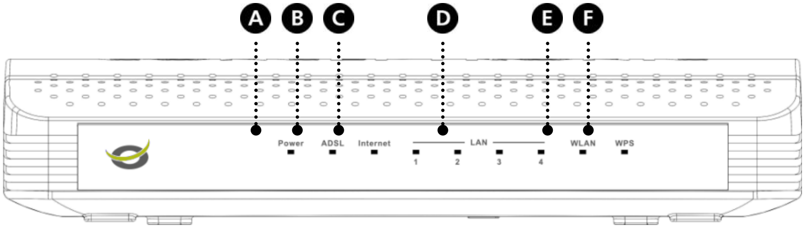
1.3 Package contents

The following items are present in the package of the Conceptronic wireless ADSL modem router:

- Conceptronic wireless ADSL modem router (C150APRA2)
- Antenna for wireless connections
- Power supply 12V DC, 800mA
- Network (LAN) cable
- Phone cable (RJ-11)
- Product CD-ROM
- This multi language user manual
- Warranty card & CE declaration booklet

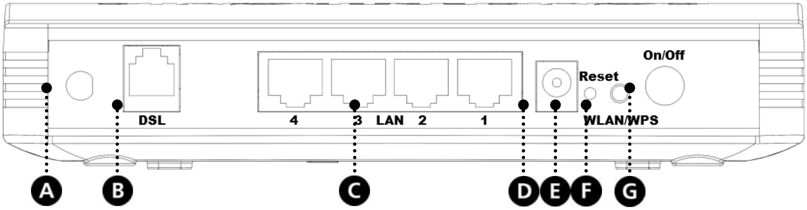
2. The wireless ADSL modem router explained

2.1 Front panel



Nr	Description	Status	Status Explanation
A	Power LED	**OFF** **ON - GREEN** **ON - RED** **ON - FLASHING**	Power is OFF Power is on and the initialization is normal Device is initiating Firmware is upgrading
B	ADSL LED	**OFF** **ON - FLASHING** **ON - STEADY**	Initial self test failed Device is detecting DSL signal DSL signal detected, self test succeeded
C	Internet LED	**ON - Red** **ON - Green**	No DSL connection Internet connection available
D	LAN LEDs (1, 2, 3, 4)	**OFF** **ON - STEADY** **ON - FLASHING**	LAN port is not connected A device is connected to the LAN port Data is being transmitted
E	WLAN LEDs	**OFF** **ON - STEADY** **ON - FLASHING**	Wireless LAN is turned off Wireless LAN is active and normal Wireless LAN activity (sending or receiving data)
F	WPS LED	**OFF** **ON - FLASHING** **ON - STEADY**	WPS (Wi-Fi Protected setup) not active WPS active, new WLAN clients can be added WPS client successfully added

2.2 Back panel



Nr	Description	Explanation
A	**Antenna connection**	Connect the included antenna to the modem router.
B	**DSL port**	Connect your ADSL line to the modem router.
C	**LAN ports (**1 – 4**)**	Connect your computer(s)/network device(s) to the modem router.
D	**Power connector**	Connect the power supply to the modem router.
E	**Reset**	Perform a factory reset (hold).
F	**WLAN / WPS button**	Short press (1 sec) : Turn WiFi on or off. Long press (> 3 sec) : Start WPS Push Button configuration.
G	**Power button**	Turn the modem router on or off.

3. Hardware Installation

- Connect the included antenna to the antenna connection [A] on the back of the modem router.
- Connect the power supply to the power connection [D] on the back of the modem router and to an available wall socket.
- Press the power [G] button on the back of the modem router.

The power LED on the front of the modem router will light up and the modem router will perform a system startup.

3.1 DSL (Telephone) port

Most ADSL providers require a splitter between your phone line and the ADSL modem that prevents the ADSL line from interfering with regular telephone services. Not using such a splitter could lead to connection problems or bad performance.

Note: The C150APRA2 is not delivered with a splitter for the ADSL connection. Please contact your telephone or internet provider for the correct ADSL splitter.

The connection ports of an ADSL splitter are typically labelled as following:

- **Line** : This port connects to the wall jack
- **ADSL** : This port connects to the router
- **Phone** : This port connects to a telephone or other telephone device

Make sure the lines are properly connected. If you are unable to hear a dial tone with the telephone, check the connections to make sure the cables are securely attached and connected to the correct port.

Use a telephone cable to connect the Conceptronic wireless ADSL modem router (B) to your local analog telephone line (or splitter). The ADSL led will light up when an ADSL signal has been detected.

Note: If the ADSL LED on the front does not lit up, make sure that:
- The wireless ADSL modem router is powered on (the power LED should burn).
- There is an ADSL signal on the line.
- The Internet LED will only be green when correct DSL and user account settings are applied into the Web Interface of the ADSL modem router.

3.2 LAN port(s)

Connect the network (LAN) cable to 1 of the 4 LAN ports on the back panel of the wireless ADSL modem routerand to the network card of your computer.
The LAN LED of the used LAN port will lit up, indicating that the computer is connected. (Your computer must be switched on and the LAN connection must be enabled).

4. Configuring the computer

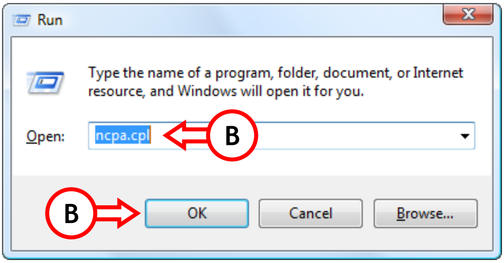
4.1 Configure your IP address

The C150APRA2 is equipped with a built-in DHCP server. The DHCP server will automatically assign an IP address to each connected computer if the connected computer is set to “**Obtain an IP address automatically**”.

By default most computers are configured to automatically obtain an IP address. When this is not the case, you will need to configure your computer to obtain an IP address automatically by following the instructions below. These instructions are based on Windows Vista with Service Pack 1. If your computer has a different version or operaring system, the steps required might be different.

A. Click “**Start**” → “**Run**”.

B. Enter the command “**NCPA.CPL**” and press “**OK**”.



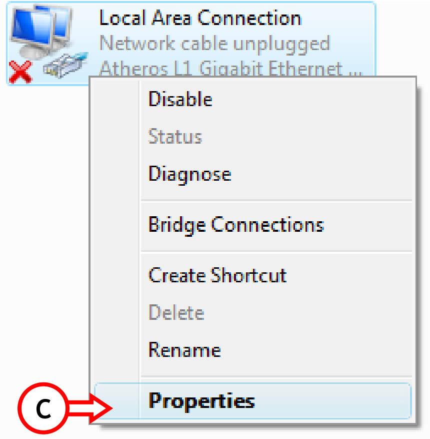
Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: ncpa.cpl

The “**Network Connections**” window will appear.

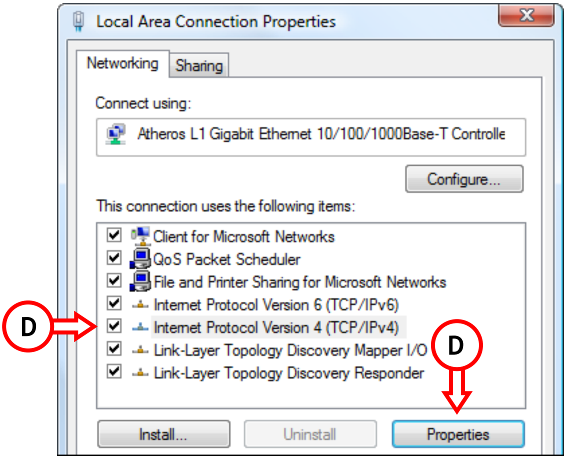
C. Right click your “**Local Area Connection**” (wired or wireless, depending on the connection you use) and select “**Properties**”.



Local Area Connection
Network cable unplugged
Atheros L1 Gigabit Ethernet ...

The Properties window of the Local Area Connection will appear.

D. Select the “**Internet Protocol Version 4 (TCP/IPv4)**” and click “**Properties**”.



Connect using:

Atheros L1 Gigabit Ethernet 10/100/1000Base-T Controlle

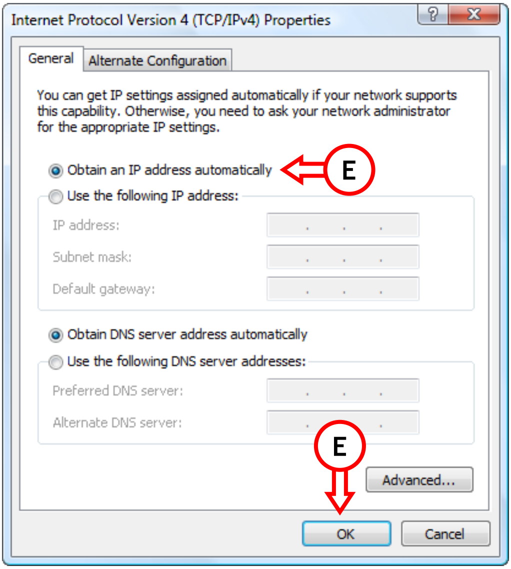
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O
- ☑ Link-Layer Topology Discovery Responder

The Properties window of the Internet Protocol Version 4 (TCP/IPv4) will appear.

E. Set the properties to “**Obtain an IP address automatically**” and press “**OK**” to save the settings.

F. Press “**OK**” in the properties window of the Local Area Connection to save the settings.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

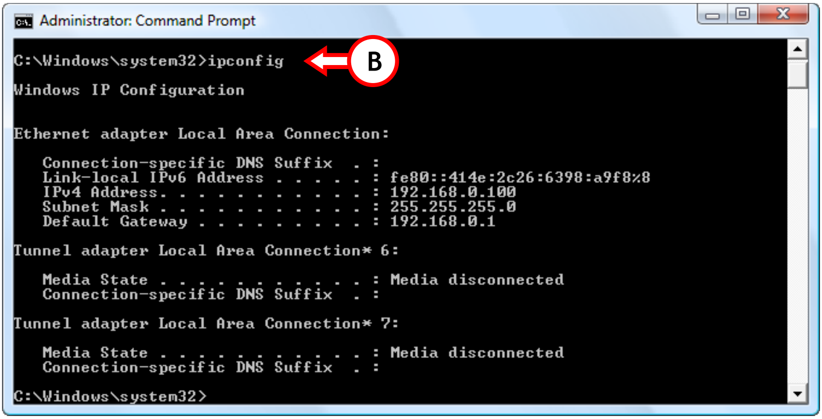
4.2 Checking your connection

With the Command Prompt of Windows you can verify if you have received a correct IP address on your (wired or wireless) Local Area Connection. This example is based on Windows Vista with Service Pack 1. Windows Vista needs administrative rights to perform the steps below. There is an explanation on how to gain administrative rights.

A. Click “**Start**” → “**All programs**” → “**Accessories**”, right click “**Command Prompt**” and select “**Run as administrator**”. You might get a warning message, which you need to accept by clicking “**Continue**”.

The Command Prompt will appear. Make sure the Command Prompt title bar mentions “**Administrator: Command Prompt**”. When “**Administrator**” is not mentioned, you do not have the needed administrative rights for these steps and you will need to perform step **A** again.

B. Enter the command “**IPCONFIG**” and press **ENTER**.



```
C:\Windows\system32>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::414e:2c26:6398:a9f8%8
   IPv4 Address. . . . . . . . . . . : 192.168.0.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Tunnel adapter Local Area Connection* 6:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Local Area Connection* 7:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Windows\system32>
```

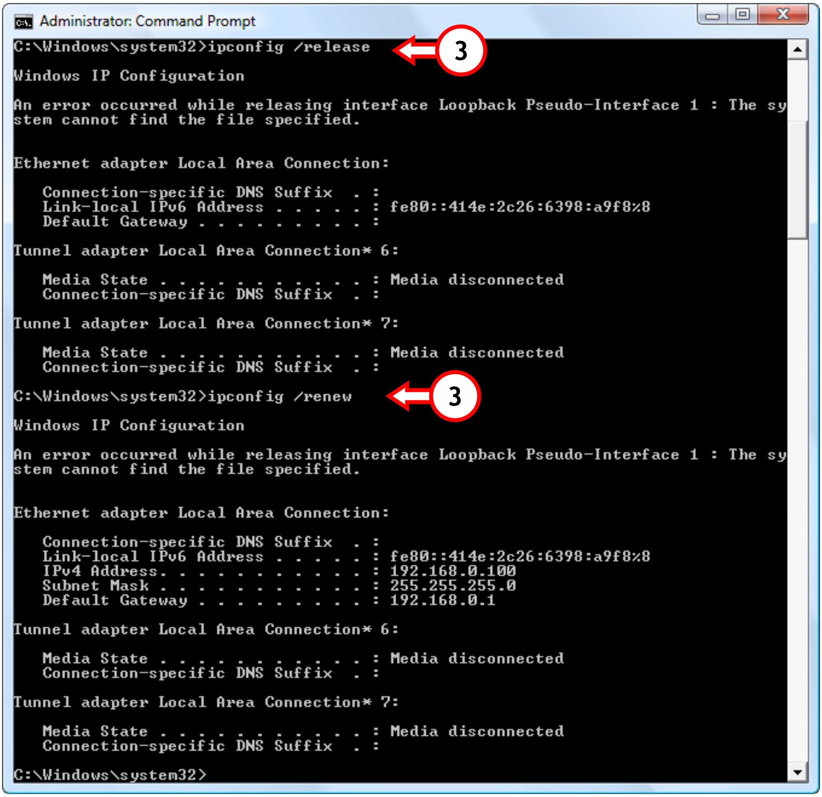
You should see the following information

IPv4 Address	: **192.168.0.xxx** (Where **xxx** can vary between **100** ~ **199**).
Subnet Mask	: **255.255.255.0**
Default Gateway	: **192.168.0.1**

If the information shown above matches your configuration you can continue the configuration of the device in **Chapter 5**.

If the information shown above does not match your configuration (i.e. your IP address is 169.254.xxx.xxx) please check the options below:

1. Power **off** and power **on** the device.
2. Reconnect the LAN cable to the device and to your computer.
3. Renew the IP address of your computer with the following commands:
   - “**IPCONFIG /RELEASE**” to release the incorrect IP address.
   - “**IPCONFIG /RENEW**” to receive a new IP address from the device.



```
C:\Windows\system32>ipconfig /release

Windows IP Configuration

An error occurred while releasing interface Loopback Pseudo-Interface 1 : The sy
stem cannot find the file specified.


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::414e:2c26:6398:a9f8%8
   Default Gateway . . . . . . . . . :

Tunnel adapter Local Area Connection* 6:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Local Area Connection* 7:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Windows\system32>ipconfig /renew

Windows IP Configuration

An error occurred while releasing interface Loopback Pseudo-Interface 1 : The sy
stem cannot find the file specified.


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::414e:2c26:6398:a9f8%8
   IPv4 Address. . . . . . . . . . . : 192.168.0.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Tunnel adapter Local Area Connection* 6:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Local Area Connection* 7:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Windows\system32>
```

If above steps do not solve the IP address problem, you can reset the device to the factory default settings with the Reset button on the back of the device.
Press and hold the Reset button for +/- 15 seconds to load the factory default settings. When the Status LED is active again, repeat step **B** to renew your IP address.

Note: If the problem remains, check if all cables are connected correctly. The ADSL port should be connected to the ADSL line and the LAN port to the computer.

5. Modem router configuration

This chapter describes how to configure the C150APRA2 using the built-in Quick Start Wizard. After completing the steps in this chapter your router has been set up for an ADSL connection and will be able to connect to the internet.

5.1 Factory default settings

The C150APRA2 is preconfigured with several settings. The preconfigured settings can be found below:

IP Address	: **192.168.0.1** (DHCP Server for LAN/WLAN clients Enabled)
Username	: **admin** (select this user)
Password	: **admin** (small characters)
Wireless SSID	: **C150APRA2**
Wireless Channel	**: Channel 6**
Wireless Security	**: WPA2**
UPnP	**: disabled (can be enabled when internet connection is configured)**

When you have changed settings in the configuration of the C150APRA2, they will be saved to the memory of the router. To restore the factory default settings, press and hold the reset button on the back of the device for +/- 15 seconds.

5.2 Web-based configuration

The configuration of the C150APRA2 is web based. You will need a web browser for the configuration of the device.

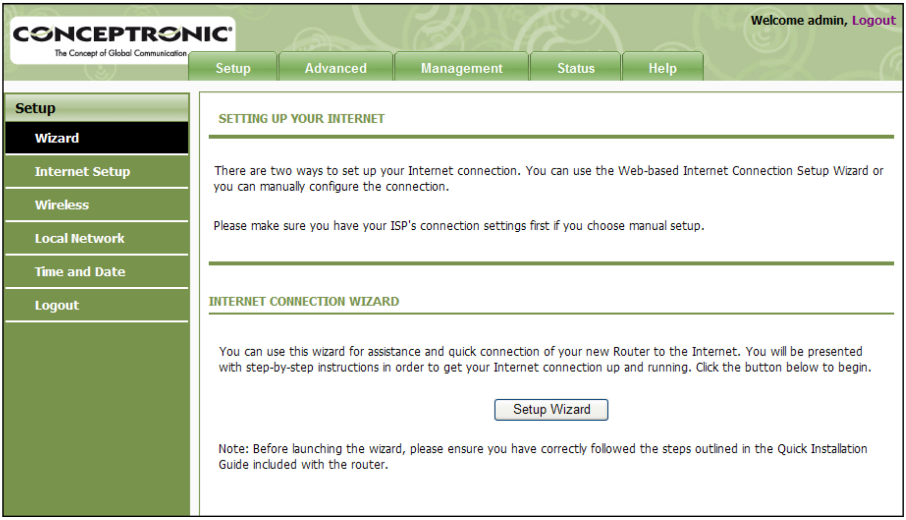
Note: For configuration of the router it is advised to use a LAN cable connection to the device instead of a wireless connection.

A. Start your web browser (like: Internet Explorer, FireFox, Safari or Chrome).

B. Enter the IP address of the device in the address bar of your web browser (by default: **http://192.168.0.1/).**

C. You will first get a login window asking you for a Username and Password. Select the user "**admin**" from the dropdown list, enter the password for the administrator (default = '**admin**') and click "**Login**" to enter the web-based configuration.

When the Username and Password are correct the router will display the “**overview**” page:



SETTING UP YOUR INTERNET

There are two ways to set up your Internet connection. You can use the Web-based Internet Connection Setup Wizard or you can manually configure the connection.

Please make sure you have your ISP's connection settings first if you choose manual setup.

INTERNET CONNECTION WIZARD

You can use this wizard for assistance and quick connection of your new Router to the Internet. You will be presented with step-by-step instructions in order to get your Internet connection up and running. Click the button below to begin.

Note: Before launching the wizard, please ensure you have correctly followed the steps outlined in the Quick Installation Guide included with the router.

The “**overview**” page shows a quick menu for configuring and maintaining the C150APRA2.

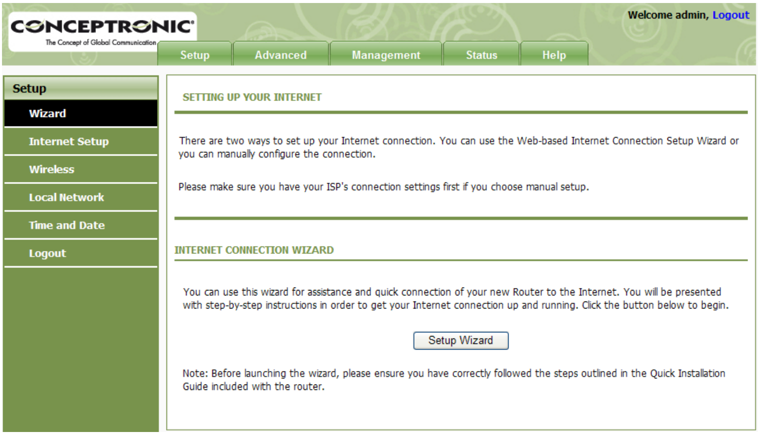
5.3 Setup

In the “**Setup**” menu, you can configure the basic configuration for your modem router.

5.3.1 Setup - Wizard

Wizard helps you to fast and accurately configure Internet connection and other important parameters. The following sections describe these various configuration parameters.
When subscribing to a broadband service, be aware of the Internect connection mode. The physical WAN device can be Ethernet, DSL, or both. Technical information about properties of Internet connection is provided by your Internet service provider (ISP). For example, your ISP should inform you whether you are connected to the Internet using a static or dynamic IP address, and the protocol, such as PPPoA or PPPoE, that you use to communicate on the Internet.

Step 1 Choose **Setup** > **Wizard.** The page as shown in the following figure appears:



SETTING UP YOUR INTERNET

There are two ways to set up your Internet connection. You can use the Web-based Internet Connection Setup Wizard or you can manually configure the connection.

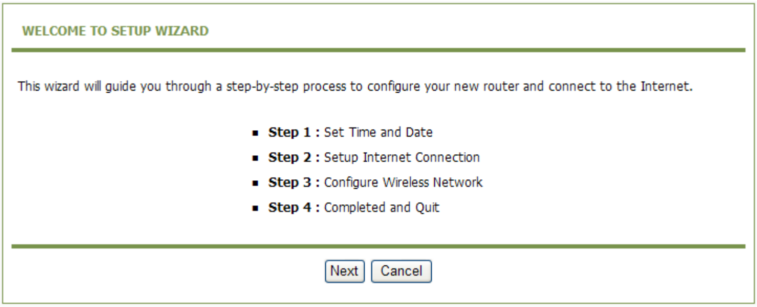
Please make sure you have your ISP's connection settings first if you choose manual setup.

INTERNET CONNECTION WIZARD

You can use this wizard for assistance and quick connection of your new Router to the Internet. You will be presented with step-by-step instructions in order to get your Internet connection up and running. Click the button below to begin.

Note: Before launching the wizard, please ensure you have correctly followed the steps outlined in the Quick Installation Guide included with the router.

Step 2 Click **Setup Wizard**. The page as shown in the following figure appears:



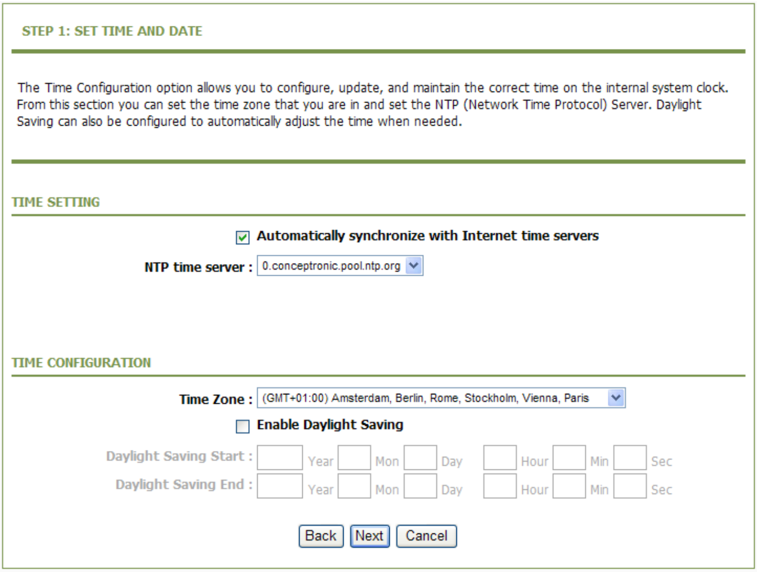
WELCOME TO SETUP WIZARD

This wizard will guide you through a step-by-step process to configure your new router and connect to the Internet.

- **Step 1 :** Set Time and Date
- **Step 2 :** Setup Internet Connection
- **Step 3 :** Configure Wireless Network
- **Step 4 :** Completed and Quit

There are four steps to configure the device. Click **Next** to continue.

Step 3 Set the time and date. Then, click **Next**.



STEP 1: SET TIME AND DATE

The Time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone that you are in and set the NTP (Network Time Protocol) Server. Daylight Saving can also be configured to automatically adjust the time when needed.

TIME SETTING

☑ **Automatically synchronize with Internet time servers**

NTP time server : 0.conceptronic.pool.ntp.org

TIME CONFIGURATION

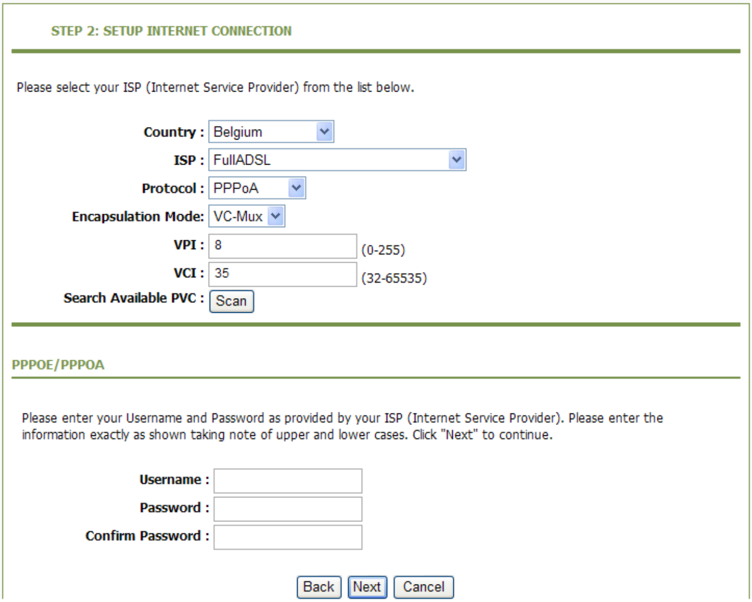
Time Zone : (GMT+01:00) Amsterdam, Berlin, Rome, Stockholm, Vienna, Paris

□ **Enable Daylight Saving**

Daylight Saving Start : Year Mon Day Hour Min Sec

Daylight Saving End : Year Mon Day Hour Min Sec

Step 4 Configure the Internet connection.
Select the country and ISP from the drop-down list. If the **Country** is set to **Belgium**, the **ISP** is set to **FullADSL**, the **Protocol** is set to **PPPoE** or **PPPoA**, the page as shown in the following figure appears:



STEP 2: SETUP INTERNET CONNECTION

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

Country : Belgium

ISP : FullADSL

Protocol : PPPoA

Encapsulation Mode: VC-Mux

VPI : 8 (0-255)

VCI : 35 (32-65535)

Search Available PVC : Scan

PPPOE/PPPOA

Please enter your Username and Password as provided by your ISP (Internet Service Provider). Please enter the information exactly as shown taking note of upper and lower cases. Click "Next" to continue.

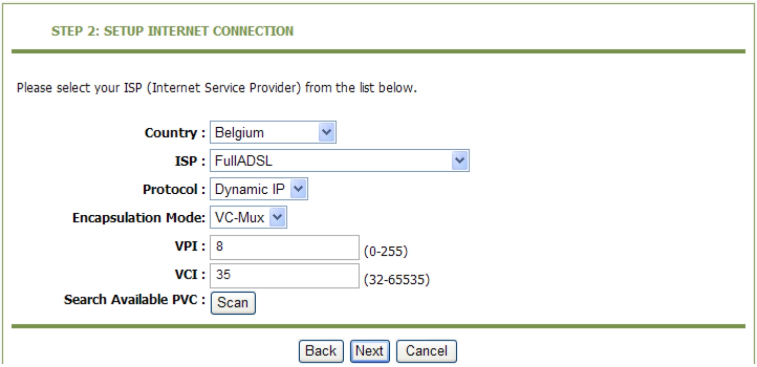
Username :

Password :

Confirm Password :

You need to enter the user name and password for PPPoE or PPPoA dialup.

If the **Protocol** is set to **Dynamic IP**, the page as shown in the following figure appears:

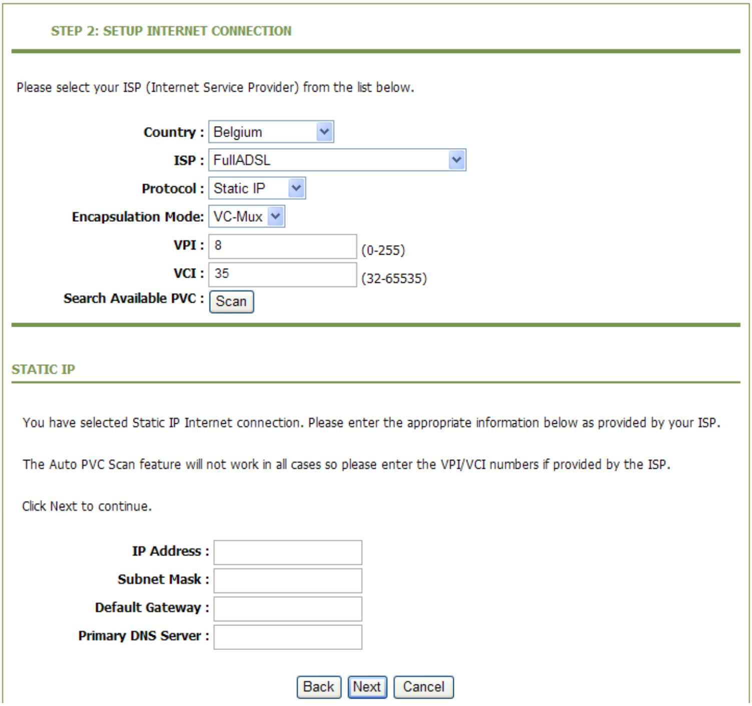


STEP 2: SETUP INTERNET CONNECTION

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

Country :	Belgium
ISP :	FullADSL
Protocol :	Dynamic IP
Encapsulation Mode:	VC-Mux
VPI :	8 (0-255)
VCI :	35 (32-65535)
Search Available PVC :	Scan

If the **Protocol** is set to **Static IP**, the page as shown in the following figure appears:



STEP 2: SETUP INTERNET CONNECTION

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

Country :	Belgium
ISP :	FullADSL
Protocol :	Static IP
Encapsulation Mode:	VC-Mux
VPI :	8 (0-255)
VCI :	35 (32-65535)
Search Available PVC :	Scan

STATIC IP

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

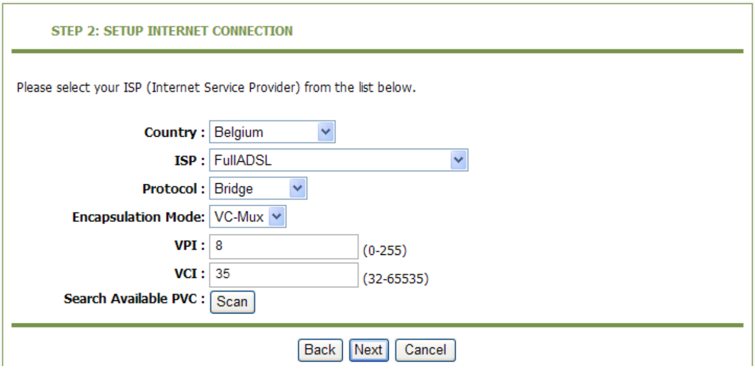
The Auto PVC Scan feature will not work in all cases so please enter the VPI/VCI numbers if provided by the ISP.

Click Next to continue.

IP Address :	
Subnet Mask :	
Default Gateway :	
Primary DNS Server :	

You need to enter the information of the IP address, subnet mask, and gateway.

If the **Protocol** is set to **Bridge**, the page as shown in the following figure appears:



STEP 2: SETUP INTERNET CONNECTION

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

Country : Belgium

ISP : FullADSL

Protocol : Bridge

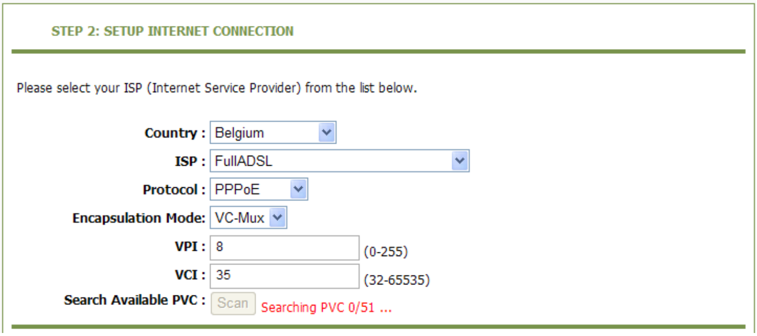
Encapsulation Mode: VC-Mux

VPI : 8 (0-255)

VCI : 35 (32-65535)

Search Available PVC :

If you click **Scan**, the system automatically searches the available PVCs.



STEP 2: SETUP INTERNET CONNECTION

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

Country : Belgium

ISP : FullADSL

Protocol : PPPoE

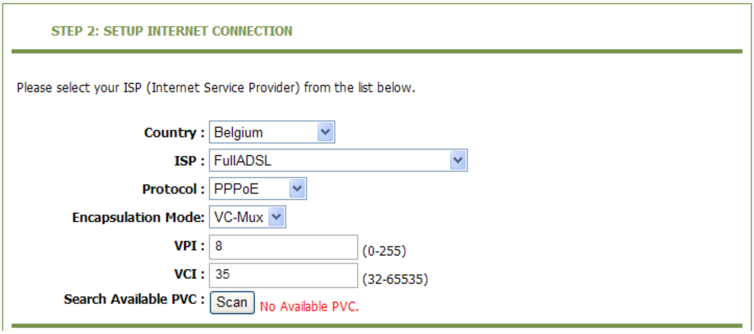
Encapsulation Mode: VC-Mux

VPI : 8 (0-255)

VCI : 35 (32-65535)

Search Available PVC : Searching PVC 0/51 ...

After the searching is complete, the result appears next to the **Scan** button.



STEP 2: SETUP INTERNET CONNECTION

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

Country : Belgium

ISP : FullADSL

Protocol : PPPoE

Encapsulation Mode: VC-Mux

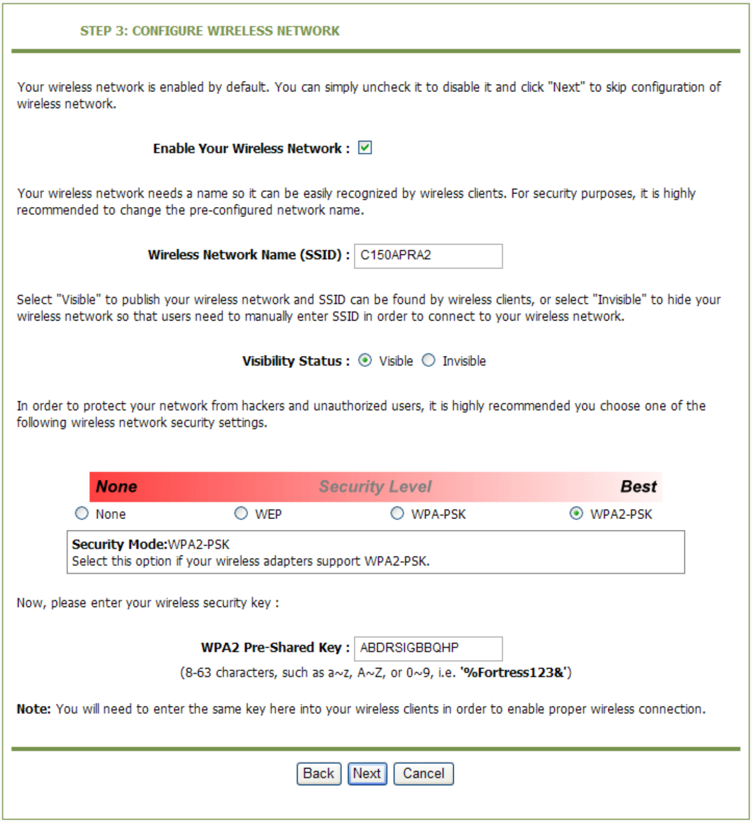
VPI : 8 (0-255)

VCI : 35 (32-65535)

Search Available PVC : No Available PVC.

After setting, click **Next**.

Step 5 Configure the wireless network. Enter the information and click **Next**.



STEP 3: CONFIGURE WIRELESS NETWORK

Your wireless network is enabled by default. You can simply uncheck it to disable it and click "Next" to skip configuration of wireless network.

Enable Your Wireless Network : ☑

Your wireless network needs a name so it can be easily recognized by wireless clients. For security purposes, it is highly recommended to change the pre-configured network name.

Wireless Network Name (SSID) : C150APRA2

Select "Visible" to publish your wireless network and SSID can be found by wireless clients, or select "Invisible" to hide your wireless network so that users need to manually enter SSID in order to connect to your wireless network.

Visibility Status : ● Visible ○ Invisible

In order to protect your network from hackers and unauthorized users, it is highly recommended you choose one of the following wireless network security settings.

○ None ○ WEP ○ WPA-PSK ● WPA2-PSK

Security Mode:WPA2-PSK
Select this option if your wireless adapters support WPA2-PSK.

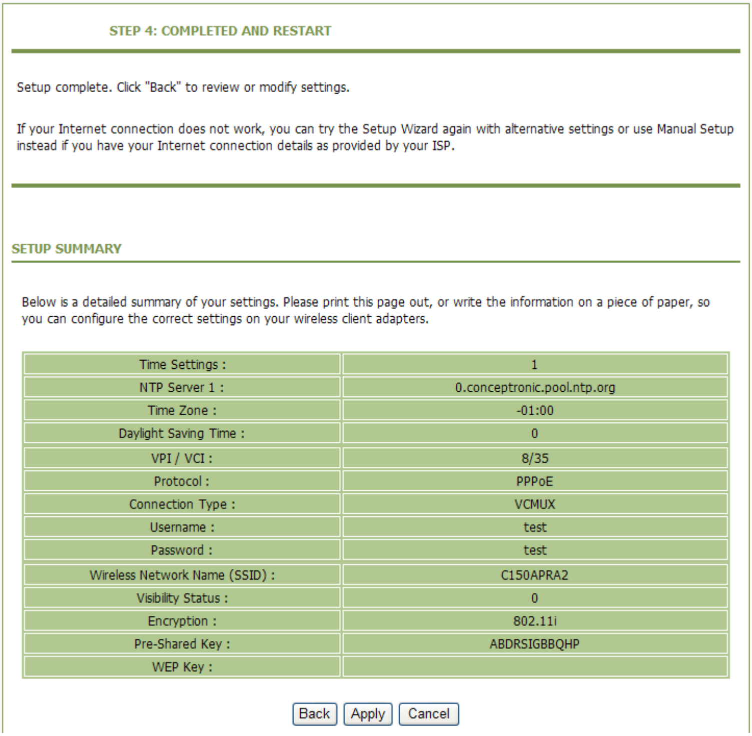
Now, please enter your wireless security key :

WPA2 Pre-Shared Key : ABDRSIGBBQHP

(8-63 characters, such as a~z, A~Z, or 0~9, i.e. **'%Fortress123&'**)

Note: You will need to enter the same key here into your wireless clients in order to enable proper wireless connection.

Step 6 View the configuration information of the device. To modify the information, click **Back**. To effect the configuration, click **Apply**.



STEP 4: COMPLETED AND RESTART

Setup complete. Click "Back" to review or modify settings.

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

SETUP SUMMARY

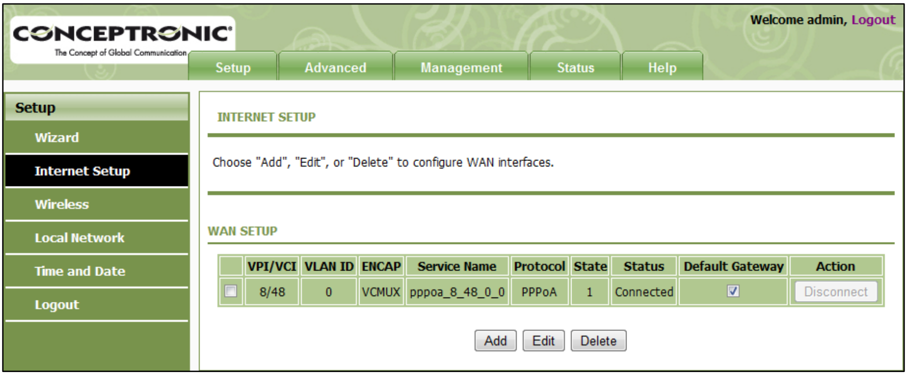
Below is a detailed summary of your settings. Please print this page out, or write the information on a piece of paper, so you can configure the correct settings on your wireless client adapters.

Time Settings :	1
NTP Server 1 :	0.conceptronic.pool.ntp.org
Time Zone :	-01:00
Daylight Saving Time :	0
VPI / VCI :	8/35
Protocol :	PPPoE
Connection Type :	VCMUX
Username :	test
Password :	test
Wireless Network Name (SSID) :	C150APRA2
Visibility Status :	0
Encryption :	802.11i
Pre-Shared Key :	ABDRSIGBBQHP
WEP Key :	

Note: In each step of the Wizard page, you can click Back to review or modify the previous settings or click Cancel to exit the wizard.

5.3.2 Setup - Internet Setup

Choose **Setup** > **Internet Setup**. The page as shown in the following figure appears:



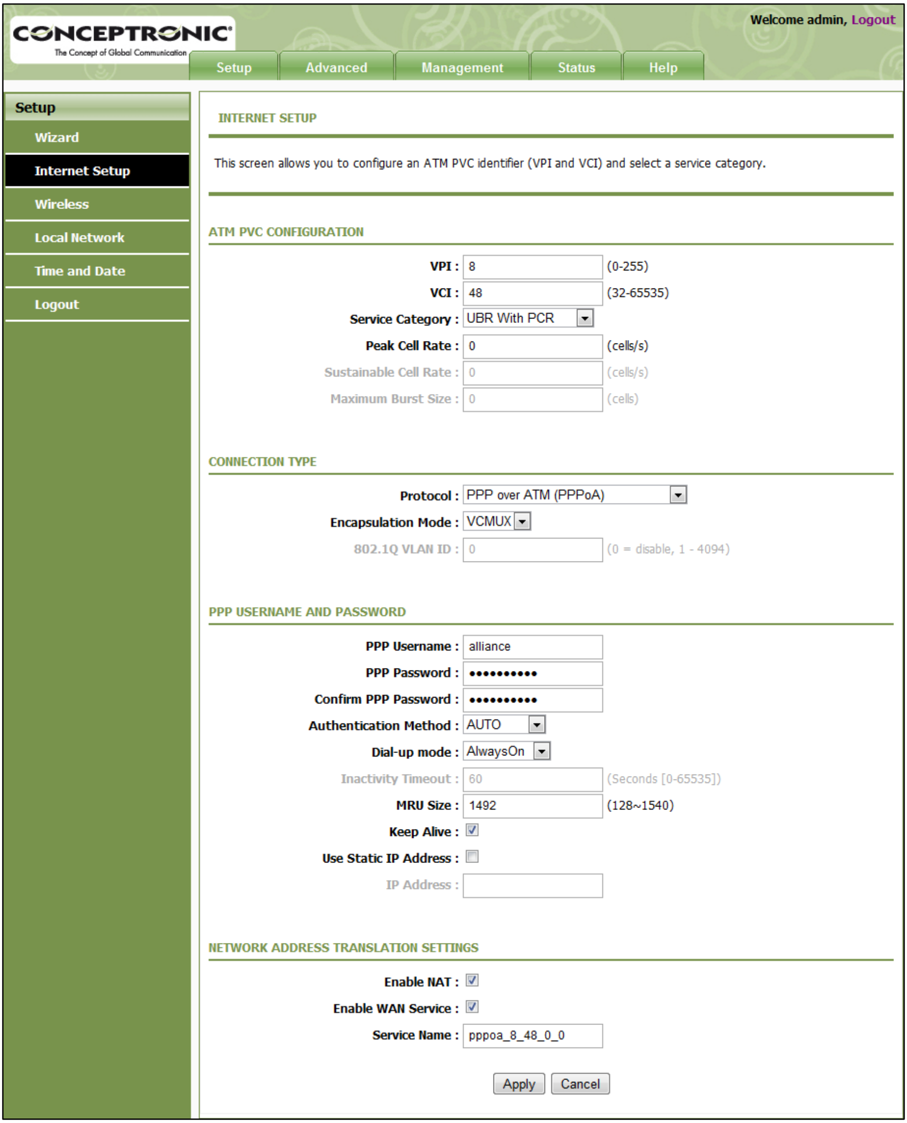
INTERNET SETUP

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

WAN SETUP

	VPI/VCI	VLAN ID	ENCAP	Service Name	Protocol	State	Status	Default Gateway	Action
□	8/48	0	VCMUX	pppoa_8_48_0_0	PPPoA	1	Connected	☑	Disconnect

In this page, you can configure the WAN interface of the device.
Click **Add** and the page as shown in the following figure appears:



INTERNET SETUP

This screen allows you to configure an ATM PVC identifier (VPI and VCI) and select a service category.

ATM PVC CONFIGURATION

VPI :	8	(0-255)
VCI :	48	(32-65535)
Service Category :	UBR With PCR	
Peak Cell Rate :	0	(cells/s)
Sustainable Cell Rate :	0	(cells/s)
Maximum Burst Size :	0	(cells)

CONNECTION TYPE

Protocol :	PPP over ATM (PPPoA)	
Encapsulation Mode :	VCMUX	
802.1Q VLAN ID :	0	(0 = disable, 1 - 4094)

PPP USERNAME AND PASSWORD

PPP Username :	alliance	
PPP Password :	••••••••••	
Confirm PPP Password :	••••••••••	
Authentication Method :	AUTO	
Dial-up mode :	AlwaysOn	
Inactivity Timeout :	60	(Seconds [0-65535])
MRU Size :	1492	(128~1540)
Keep Alive :	☑	
Use Static IP Address :	□	
IP Address :		

NETWORK ADDRESS TRANSLATION SETTINGS

Enable NAT :	☑
Enable WAN Service :	☑
Service Name :	pppoa_8_48_0_0

The following table describes the parameters in this page.

ATM PVC CONFIGURATION

Field	Description
VPI	Virtual Path Identifier (VPI) is the virtual path between two points in an ATM network. Its value range is from 0 to 255.
VCI	Virtual Channel Identifier (VCI) is the virtual channel between two points in an ATM network. Its value range is from 32 to 65535 (0 to 31 is reserved for local management of ATM traffic).
Service Category	Select **UBR with PCR**, **UBR without PCR**, **CBR**, **Non Realtime VBR**, or **Realtime VBR** from the drop-down list.
Peak Cell Rate	Set the maximum transmission rate of the cell in ATM transmission.
Sustainable Cell Rate	Set the minimum transmission rate of the cell in ATM transmission.
Maximum Burst Size	Set the maximum burst size of the cell in ATM transmission.

CONNECTION TYPE

Field	Description
Protocol	Select **PPP over ATM (PPPoA)**, **PPP over Ethernet (PPPoE)**, **MAC Encryption Routing (MER)**, **IP over ATM (IPoA)**, or **Bridging** from the drop-down list.
Encapsulation Mode	Select **LLC** or **VCMUX** from the drop-down list. Usually, you can select **LLC**.
802.1Q VLAN ID	If you enter a value, packets from the interface is tagged with the set 802.1q VLAN ID. Its value range is 0-4094, while **0** indicates to disable this function.

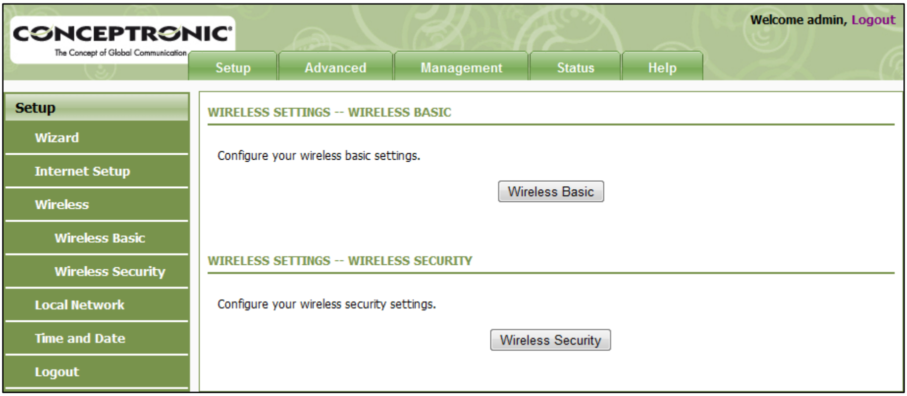
NETWORK ADDRESS TRANSLATION SETTINGS

Field	Description
Enable Bridge Service	Select or deselect the check box to enable or disable the WAN connection.
Service Name	The name to identify the WAN connection. You need not modify it.

5.3.3 Setup - Wireless

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

Choose **Setup** > **Wireless**. The **WIRELESS SETTINGS** page as shown in the following figure appears:



WIRELESS SETTINGS -- WIRELESS BASIC

Configure your wireless basic settings.

Wireless Basic

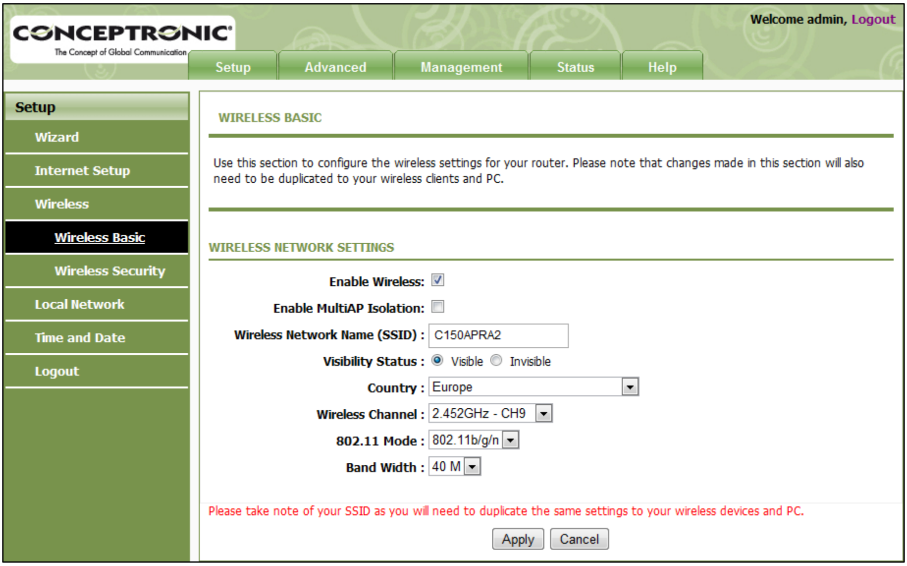
WIRELESS SETTINGS -- WIRELESS SECURITY

Configure your wireless security settings.

Wireless Security

5.3.3.1 Setup – Wireless - Wireless Basic

In the **WIRELESS SETTINGS** page, click **Wireless Basic**. The page as shown in the following figure appears:



WIRELESS BASIC

Use this section to configure the wireless settings for your router. Please note that changes made in this section will also need to be duplicated to your wireless clients and PC.

WIRELESS NETWORK SETTINGS

Enable Wireless: ☑

Enable MultiAP Isolation: ☐

Wireless Network Name (SSID) : C150APRA2

Visibility Status : ● Visible ○ Invisible

Country : Europe

Wireless Channel : 2.452GHz - CH9

802.11 Mode : 802.11b/g/n

Band Width : 40 M

Please take note of your SSID as you will need to duplicate the same settings to your wireless devices and PC.

In this page, you can configure the parameters of wireless LAN clients that may connect to the device.

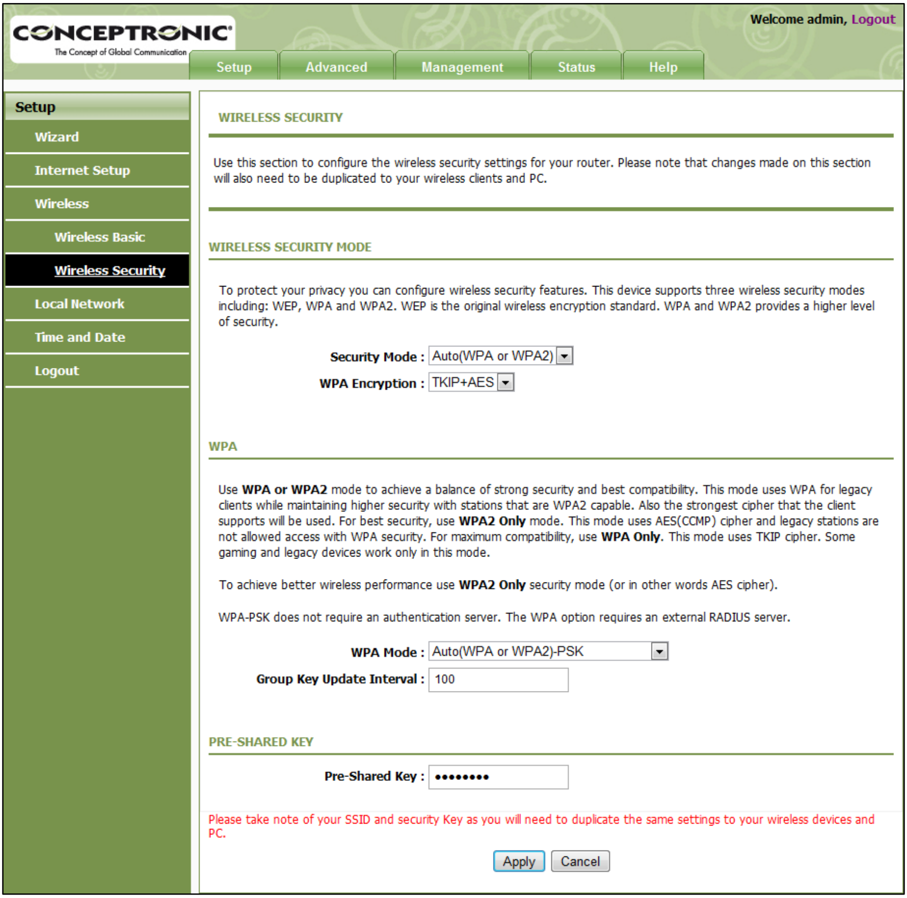
The following table describes the parameters in this page.

Field	Description
Enable Wireless	Select or deselect the check box to enable or disable the wireless function.
Enable MultiAP Isolation	Select or deselect the check box to enable or disable multiAP isolation. If this function is enabled, clients of different SSIDs cannot access each other.
Wireless Network Name (SSID)	Network name. It can contain up to 32 characters. It can consist of letters, numerals, and/or underlines.
Visibility Status	● **Visible** indicates that the device broadcasts the SSID. ● **Invisible** indicates that the device does not broadcast the SSID.
Country	Select the country where you are in from the drop-down list.
Wireless Channel	Select the wireless channel used by the device from the drop-down list. You can select **Auto Scan** or a value from **CH1**—**CH13**. **Auto Scan** is recommended.
802.11 Mode	Select the 802.11 mode of the device from the drop-down list. The device supports 802.11b, 802.11g, 802.11n, 802.11b/g, 802.11n/g, and 802.11b/g/n.
Band Width	You can set the bandwidth only in the 802.11n mode. You can set the bandwidth of the device to **20M** or **40M**.

Click **Apply** to save the settings.

5.3.3.2 Setup – Wireless - Wireless Security

In the **WIRELESS SETTINGS** page, click **Wireless Security**. The page as shown in the following figure appears:



WIRELESS SECURITY

Use this section to configure the wireless security settings for your router. Please note that changes made on this section will also need to be duplicated to your wireless clients and PC.

WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2. WEP is the original wireless encryption standard. WPA and WPA2 provides a higher level of security.

Security Mode : Auto(WPA or WPA2)

WPA Encryption : TKIP+AES

WPA

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

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

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

WPA Mode : Auto(WPA or WPA2)-PSK

Group Key Update Interval : 100

PRE-SHARED KEY

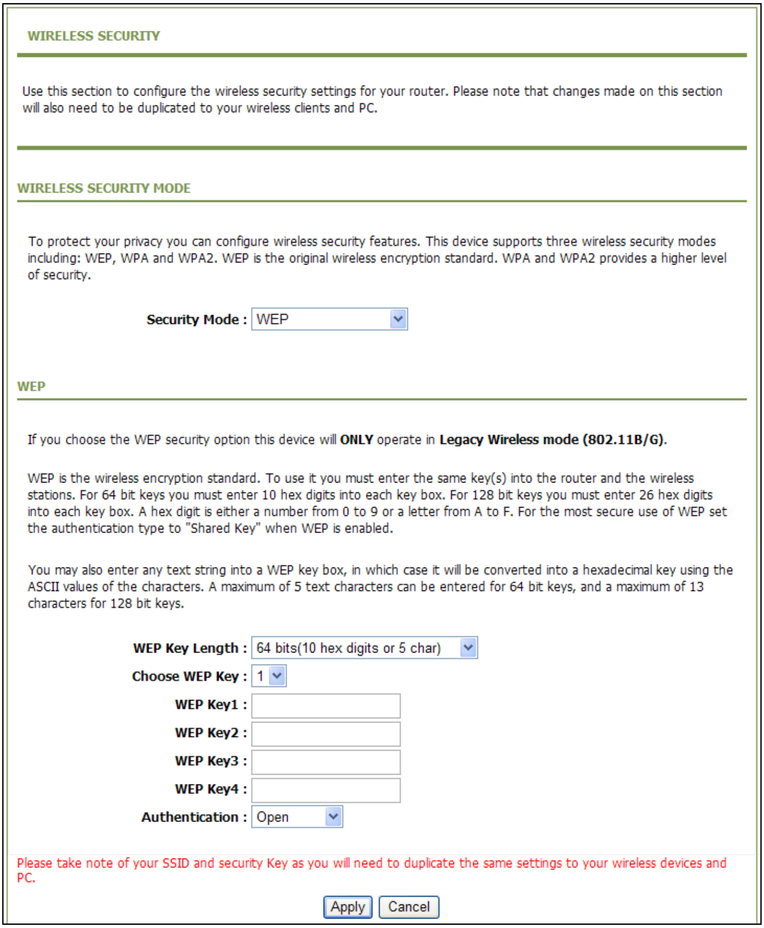
Pre-Shared Key : ••••••••

Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

Wireless security is vital to your network to protect the wireless communication among wireless stations, access points and the wired network. This device provides the following encryption modes: **None**, **WEP**, **Auto (WPA or WPA2)**, **WPA2 Only**, and **WPA Only**.

WEP

If the **Security Mode** is set to **WEP**, the page as shown in the following figure appears:



WIRELESS SECURITY

Use this section to configure the wireless security settings for your router. Please note that changes made on this section will also need to be duplicated to your wireless clients and PC.

WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2. WEP is the original wireless encryption standard. WPA and WPA2 provides a higher level of security.

Security Mode : WEP

WEP

If you choose the WEP security option this device will **ONLY** operate in **Legacy Wireless mode (802.11B/G)**.

WEP is the wireless encryption standard. To use it you must enter the same key(s) into the router and the wireless stations. For 64 bit keys you must enter 10 hex digits into each key box. For 128 bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. For the most secure use of WEP set the authentication type to "Shared Key" when WEP is enabled.

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

WEP Key Length : 64 bits(10 hex digits or 5 char)

Choose WEP Key : 1

WEP Key1 :

WEP Key2 :

WEP Key3 :

WEP Key4 :

Authentication : Open

Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

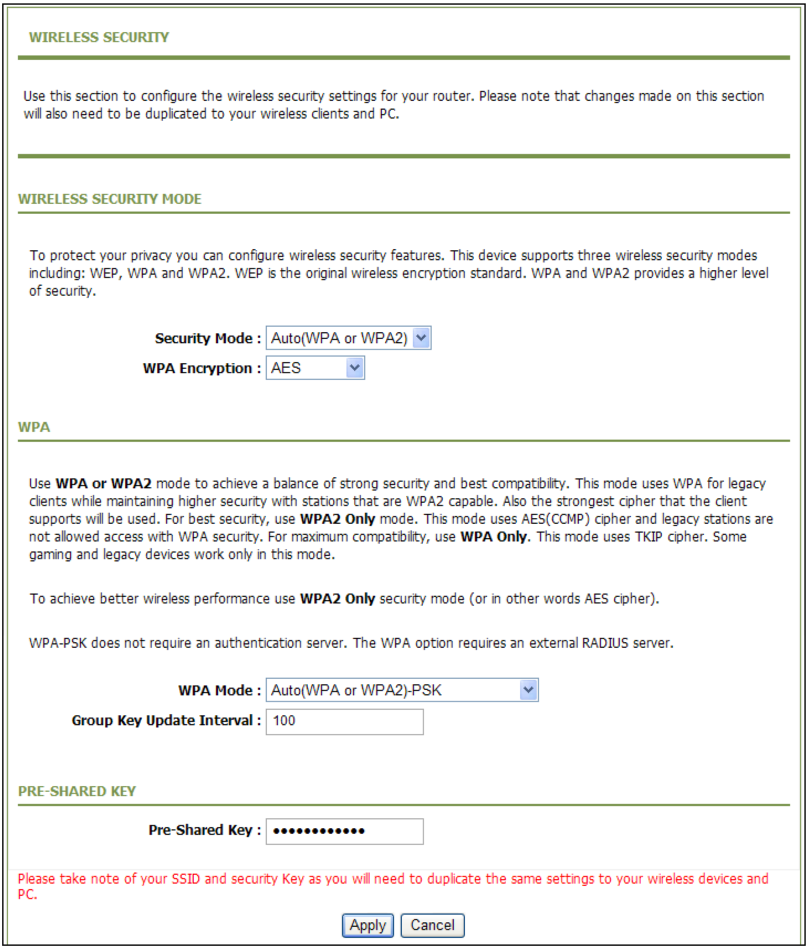
The following table describes the parameters in this page.

Field	Description
WEP Key Length	You can select **64 bits** or **128 bits** from the drop-down list. ● If you select **64 bits**, you need to enter 10 hexadecimal numbers or 5 characters. ● If you select **128 bits**, you need to enter 26 hexadecimal numbers or 13 characters.
Choose WEP Key	Select the WEP key from the drop-down list. Its value range is 1—4.
WEP Keys 1—4	Set the 64 bits or 128 bits key, in the format of Hex or ASCII.
Authentication	Select the authentication mode from the drop-down list. You can select **Open** or **Share Key**.

Click **Apply** to save the settings.

Auto (WPA or WPA2)

If the **Security Mode** is set to **Auto (WPA or WPA2)**, the page as shown in the following figure appears:



WIRELESS SECURITY

Use this section to configure the wireless security settings for your router. Please note that changes made on this section will also need to be duplicated to your wireless clients and PC.

WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2. WEP is the original wireless encryption standard. WPA and WPA2 provides a higher level of security.

Security Mode : Auto(WPA or WPA2)

WPA Encryption : AES

WPA

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

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

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

WPA Mode : Auto(WPA or WPA2)-PSK

Group Key Update Interval : 100

PRE-SHARED KEY

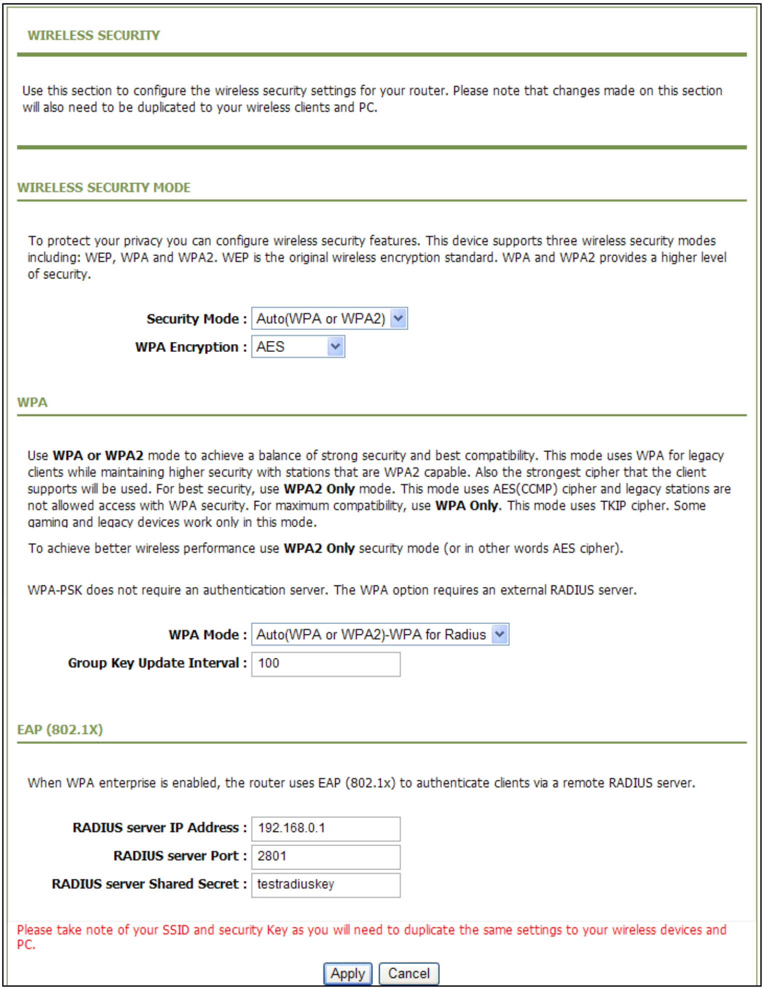
Pre-Shared Key : ••••••••••••

Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

The following table describes the parameters in this page.

Field	Description
WPA Mode	You can select **Auto (WPA or WPA2)-PSK** or **Auto (WPA or WPA2)-WPA for Enterprise** from the drop-down list.
Group Key Update Interval	Set the interval for updating the key.
Pre-Shared Key	Set the preshared key to identify the workstation.

If the **WPA Mode** is set to **Auto (WPA or WPA2)-Enterprise**, the page as shown in the following figure appears:



WIRELESS SECURITY

Use this section to configure the wireless security settings for your router. Please note that changes made on this section will also need to be duplicated to your wireless clients and PC.

WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2. WEP is the original wireless encryption standard. WPA and WPA2 provides a higher level of security.

Security Mode : Auto(WPA or WPA2)

WPA Encryption : AES

WPA

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

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

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

WPA Mode : Auto(WPA or WPA2)-WPA for Radius

Group Key Update Interval : 100

EAP (802.1X)

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

RADIUS server IP Address : 192.168.0.1

RADIUS server Port : 2801

RADIUS server Shared Secret : testradiuskey

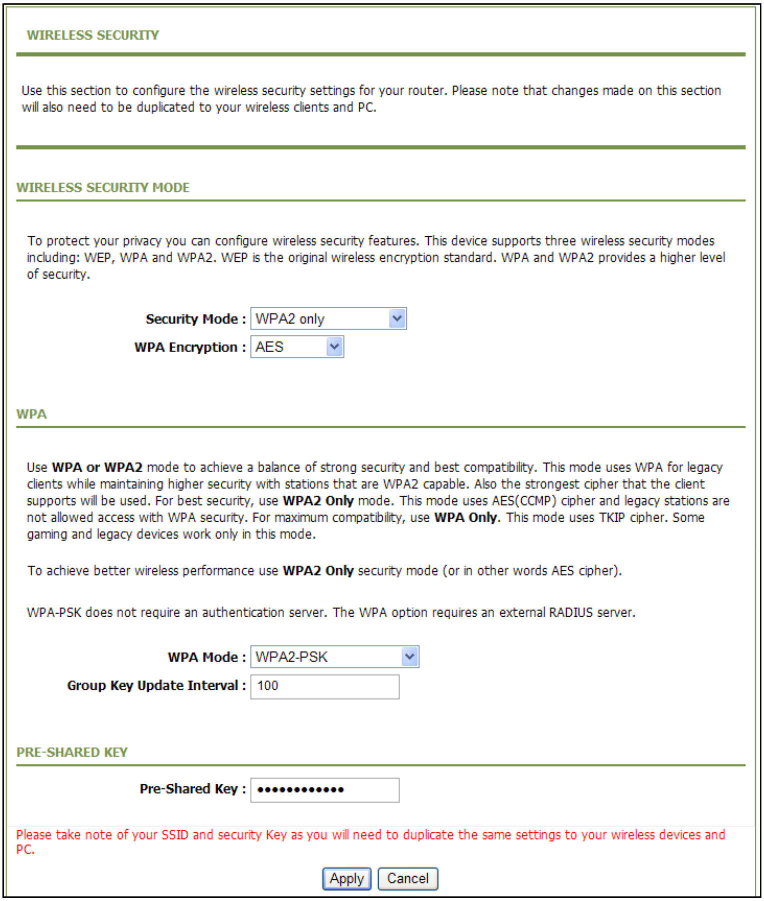
Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

You need to enter the IP address, port, shared key of the RADIUS server.

Click **Apply** to save the settings.

WPA2 Only

If the **Security Mode** is set to **WPA2 only**, the page as shown in the following figure appears:



WIRELESS SECURITY

Use this section to configure the wireless security settings for your router. Please note that changes made on this section will also need to be duplicated to your wireless clients and PC.

WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2. WEP is the original wireless encryption standard. WPA and WPA2 provides a higher level of security.

Security Mode : WPA2 only

WPA Encryption : AES

WPA

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

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

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

WPA Mode : WPA2-PSK

Group Key Update Interval : 100

PRE-SHARED KEY

Pre-Shared Key : ••••••••••••

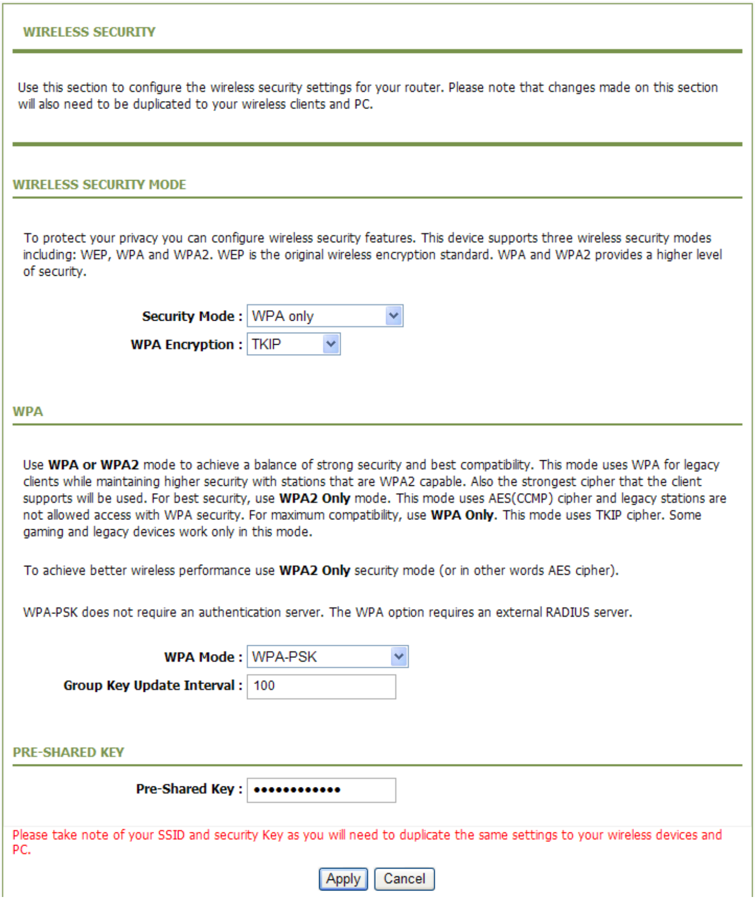
Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

Parameters in this page are similar to those in the page for **Auto (WPA or WPA2)**.

Click **Apply** to save the settings.

WPA Only

If the **Security Mode** is set to **WPA only**, the page as shown in the following figure appears:



WIRELESS SECURITY

Use this section to configure the wireless security settings for your router. Please note that changes made on this section will also need to be duplicated to your wireless clients and PC.

WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2. WEP is the original wireless encryption standard. WPA and WPA2 provides a higher level of security.

Security Mode : WPA only

WPA Encryption : TKIP

WPA

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

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

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

WPA Mode : WPA-PSK

Group Key Update Interval : 100

PRE-SHARED KEY

Pre-Shared Key : ●●●●●●●●●●●●

Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

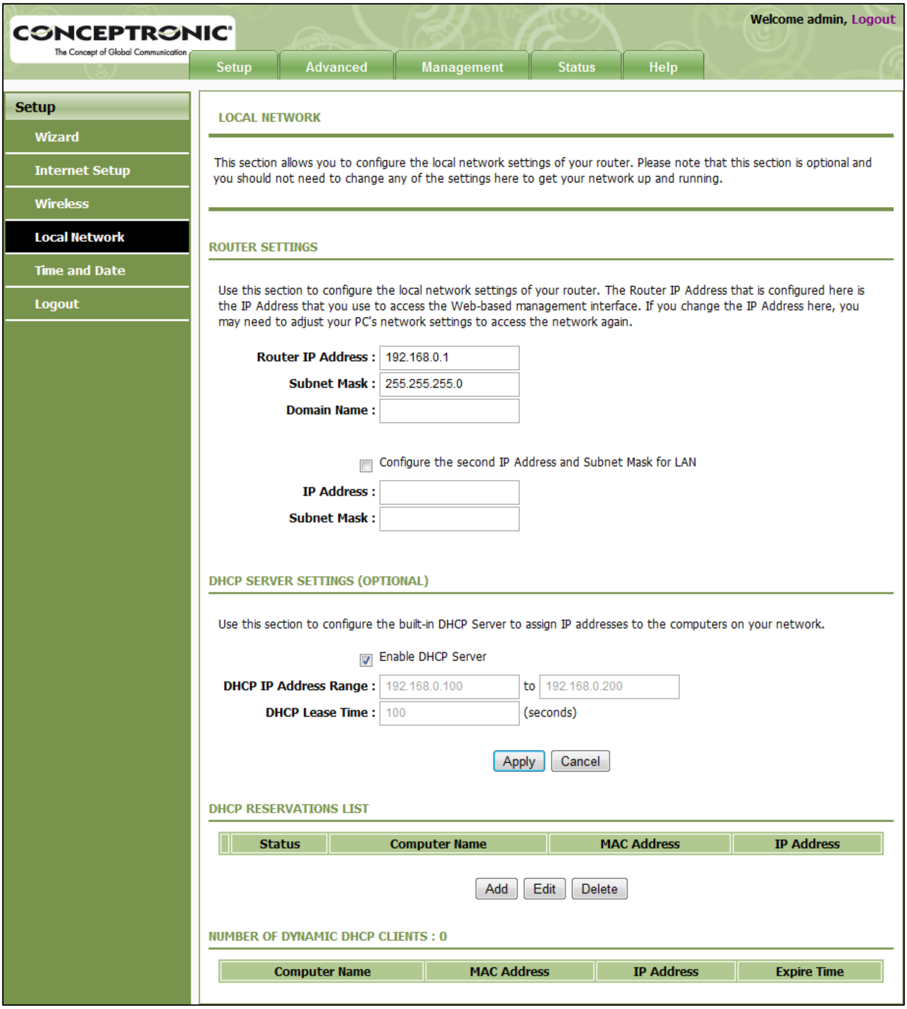
Parameters in this page are similar to those in the page for **Auto (WPA or WPA2)**.

Click **Apply** to save the settings.

5.3.4 Setup - Local Network

You can configure the LAN IP address according to the actual application. The preset IP address is 192.168.0.1. You can use the default settings and DHCP service to manage the IP settings of the private network. The IP address of the device is the base address used for DHCP. To use the device for DHCP in your LAN, the IP address pool used for DHCP must be compatible with the IP address of the device. The IP address available in the DHCP IP address pool changes automatically if the IP address of the device changes.
You can also enable the secondary LAN IP address. The primary and the secondary LAN IP addresses must be in different network segments.

Choose **Setup** > **Local Network**. The **LOCAL NETWORK** page as shown in the following figure appears:



LOCAL NETWORK

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

ROUTER SETTINGS

Use this section to configure the local network settings of your router. The Router IP Address that is configured here is the IP Address that you use to access the Web-based management interface. If you change the IP Address here, you may need to adjust your PC's network settings to access the network again.

Router IP Address : 192.168.0.1
Subnet Mask : 255.255.255.0
Domain Name :

☐ Configure the second IP Address and Subnet Mask for LAN

IP Address :
Subnet Mask :

DHCP SERVER SETTINGS (OPTIONAL)

Use this section to configure the built-in DHCP Server to assign IP addresses to the computers on your network.

☑ Enable DHCP Server

DHCP IP Address Range : 192.168.0.100 to 192.168.0.200
DHCP Lease Time : 100 (seconds)

DHCP RESERVATIONS LIST

	Status	Computer Name	MAC Address	IP Address

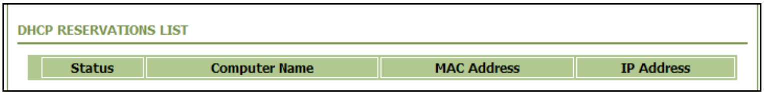
NUMBER OF DYNAMIC DHCP CLIENTS : 0

Computer Name	MAC Address	IP Address	Expire Time

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

Click **Apply** to save the settings.

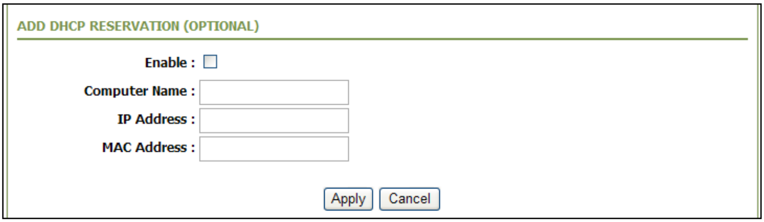
In the **LOCAL NETWORK** page, you can assign LAN IP addresses for specific computers according to their MAC addresses.



DHCP RESERVATIONS LIST

Status	Computer Name	MAC Address	IP Address

Click **Add** to add static DHCP reservation. The page as shown in the following figure appears:



ADD DHCP RESERVATION (OPTIONAL)

Enable : □

Computer Name :

IP Address :

MAC Address :

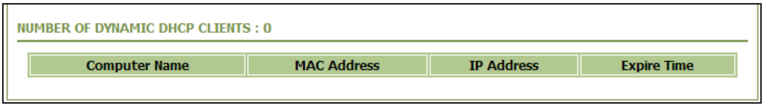
The following table describes the parameters in this page.

Field	Description
Enable	Select the check box to reserve the IP address for the designated PC with the configured MAC address.
Computer Name	Enter the computer name. It helps you to recognize the PC with the MAC address. For example, Father's Laptop.
IP Address	Enter the IP address of the computer.
MAC Address	Enter the MAC address of the computer.

Click **Apply** to save the settings.

After the DHCP reservation information is saved, the DHCP reservations list displays the information. If the DHCP reservations list is not empty, you can select one or more items and click **Edit** or **Delete**.

The **NUMBER OF DYNAMIC DHCP CLIENTS** page displays the DHCP clients (PCs or Laptops) currently connected to the device and the detailed information of the connected computers.

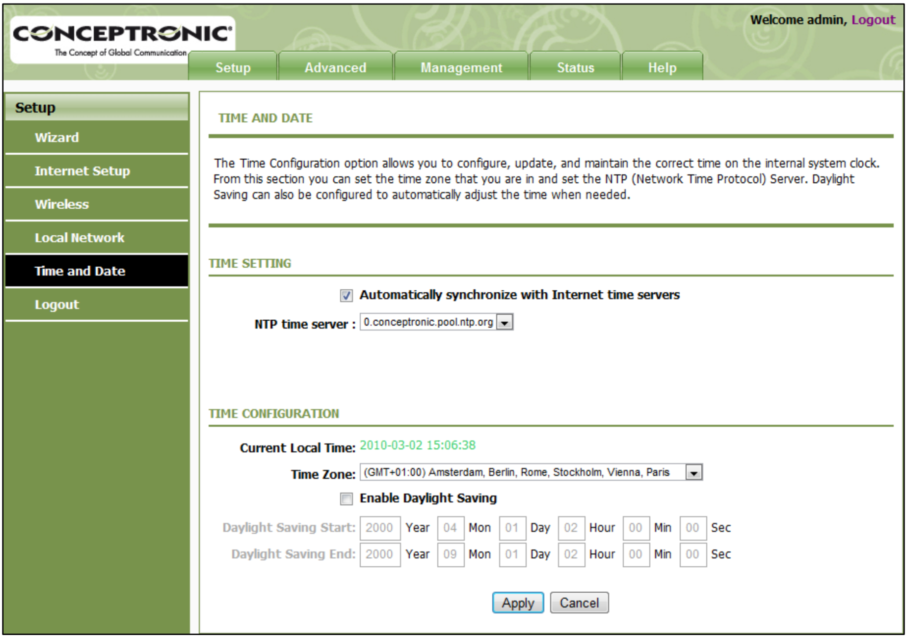


NUMBER OF DYNAMIC DHCP CLIENTS : 0

Computer Name	MAC Address	IP Address	Expire Time

5.3.5 Setup - Time and Date

Choose **Setup** > **Time and Date**. The **TIME AND DATE** page as shown in the following figure appears:



TIME AND DATE

The Time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone that you are in and set the NTP (Network Time Protocol) Server. Daylight Saving can also be configured to automatically adjust the time when needed.

TIME SETTING

☑ Automatically synchronize with Internet time servers

NTP time server : 0.conceptronic.pool.ntp.org

TIME CONFIGURATION

Current Local Time: 2010-03-02 15:06:38

Time Zone: (GMT+01:00) Amsterdam, Berlin, Rome, Stockholm, Vienna, Paris

☐ Enable Daylight Saving

Daylight Saving Start: 2000 Year 04 Mon 01 Day 02 Hour 00 Min 00 Sec

Daylight Saving End: 2000 Year 09 Mon 01 Day 02 Hour 00 Min 00 Sec

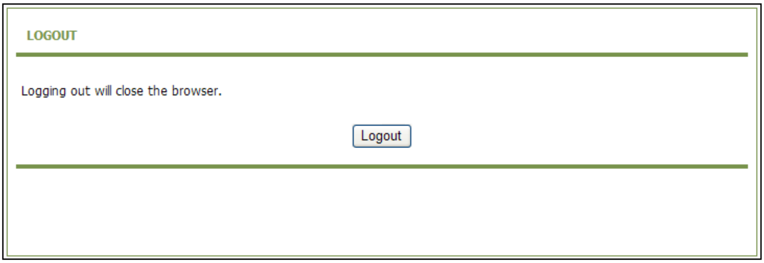
In the **TIME AND DATE** page, you can configure, update, and maintain the time of the internal system clock. You can set the time zone that you are in and the network time protocol (NTP) server. You can also set daylight saving time to automatically adjust the time when needed.

Select **Automatically synchronize with Internet time servers**.
Select the appropriate time server and the time zone from the corresponding drop-down lists.
Select **Enable Daylight Saving** if necessary. Enter the correct the start and end time of the daylight saving.

Click **Apply** to save the settings.

5.3.6 Setup - Logout

Choose **Setup** > **Logout**. The page as shown in the following figure appears:


LOGOUT

Logging out will close the browser.

Click **Logout** to log out of the configuration page.

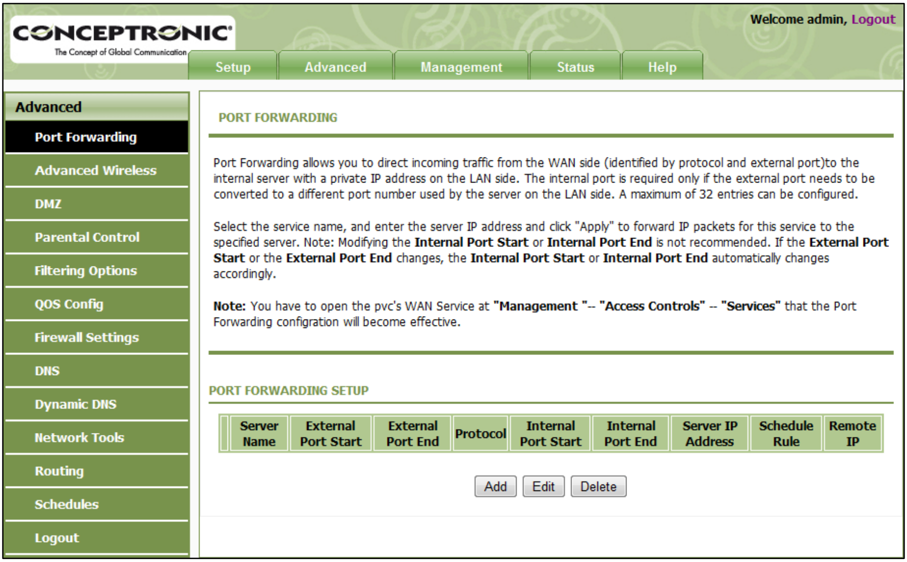
5.4 Advanced

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

5.4.1 Advanced – Port Forwarding

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

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



PORT FORWARDING

Port Forwarding allows you to direct incoming traffic from the WAN side (identified by protocol and external port)to the internal server with a private IP address on the LAN side. The internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum of 32 entries can be configured.

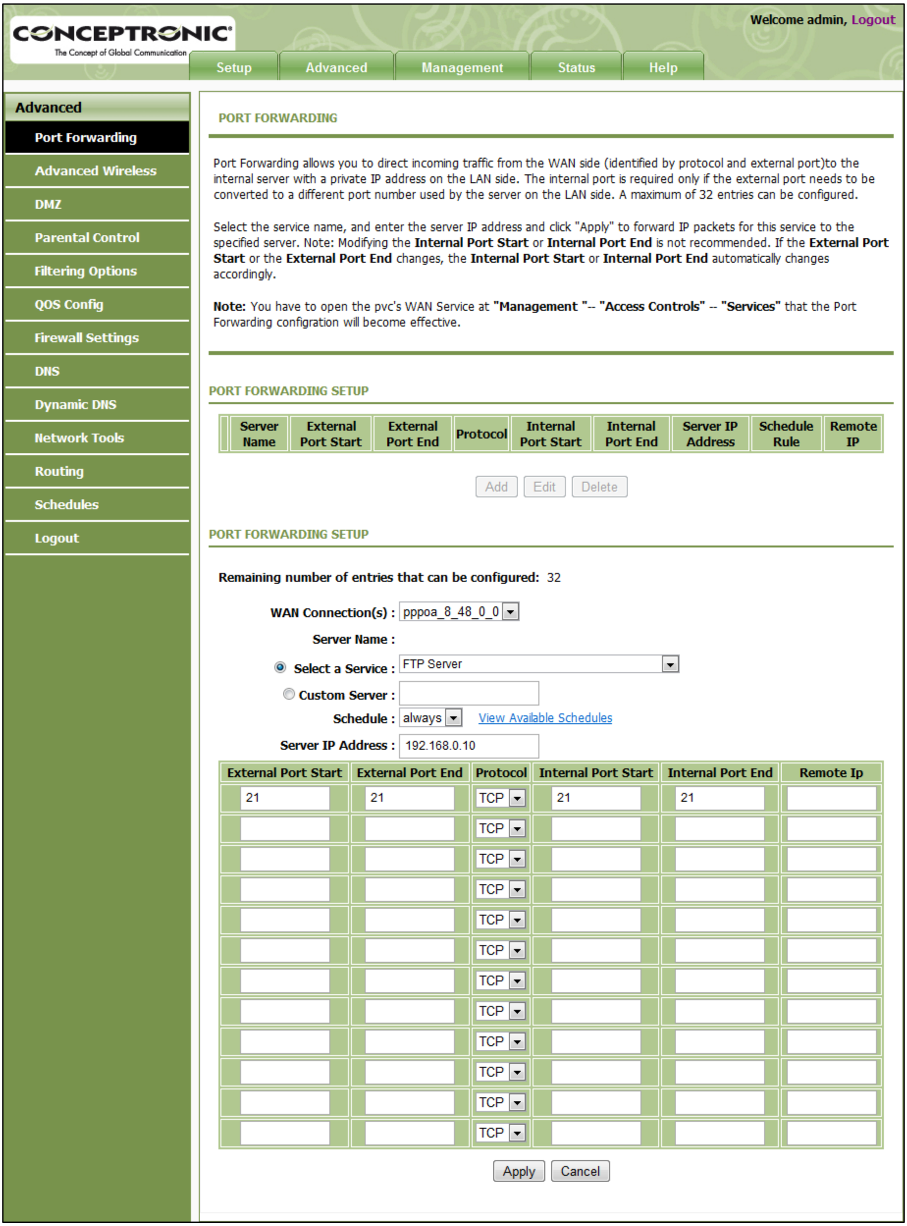
Select the service name, and enter the server IP address and click "Apply" to forward IP packets for this service to the specified server. Note: Modifying the **Internal Port Start** or **Internal Port End** is not recommended. If the **External Port Start** or the **External Port End** changes, the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

Note: You have to open the pvc's WAN Service at **"Management "-- "Access Controls"** -- **"Services"** that the Port Forwarding configration will become effective.

PORT FORWARDING SETUP

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	Schedule Rule	Remote IP

Click **Add** to add a virtual server. See the following figure:



PORT FORWARDING

Port Forwarding allows you to direct incoming traffic from the WAN side (identified by protocol and external port)to the internal server with a private IP address on the LAN side. The internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum of 32 entries can be configured.

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

Note: You have to open the pvc's WAN Service at **"Management "-- "Access Controls" -- "Services"** that the Port Forwarding configration will become effective.

PORT FORWARDING SETUP

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	Schedule Rule	Remote IP

PORT FORWARDING SETUP

Remaining number of entries that can be configured: 32

WAN Connection(s) : pppoa_8_48_0_0

Server Name :

● **Select a Service :** FTP Server

○ **Custom Server :**

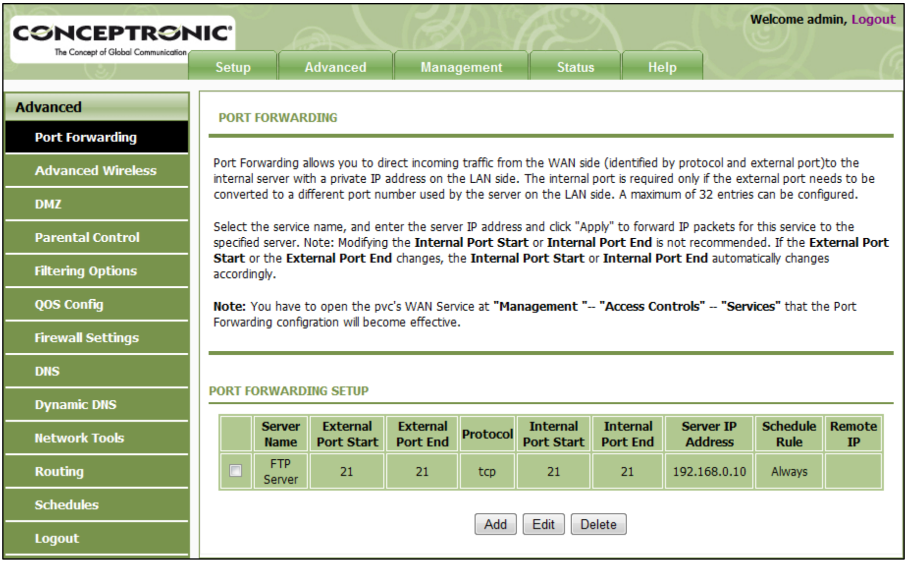
Schedule : always

Server IP Address : 192.168.0.10

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Remote Ip
21	21	TCP	21	21	
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			

Select a service for a preset application or enter the name in the **Custom Server** field.
Enter an IP address in the **Server IP Address** field, to appoint the corresponding PC to receive forwarded packets.
The port table displays the ports that you want to open on the device. The **Protocol** indicates the type of protocol used by each port.

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



PORT FORWARDING

Port Forwarding allows you to direct incoming traffic from the WAN side (identified by protocol and external port)to the internal server with a private IP address on the LAN side. The internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum of 32 entries can be configured.

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

Note: You have to open the pvc's WAN Service at **"Management "**-- **"Access Controls"** -- **"Services"** that the Port Forwarding configration will become effective.

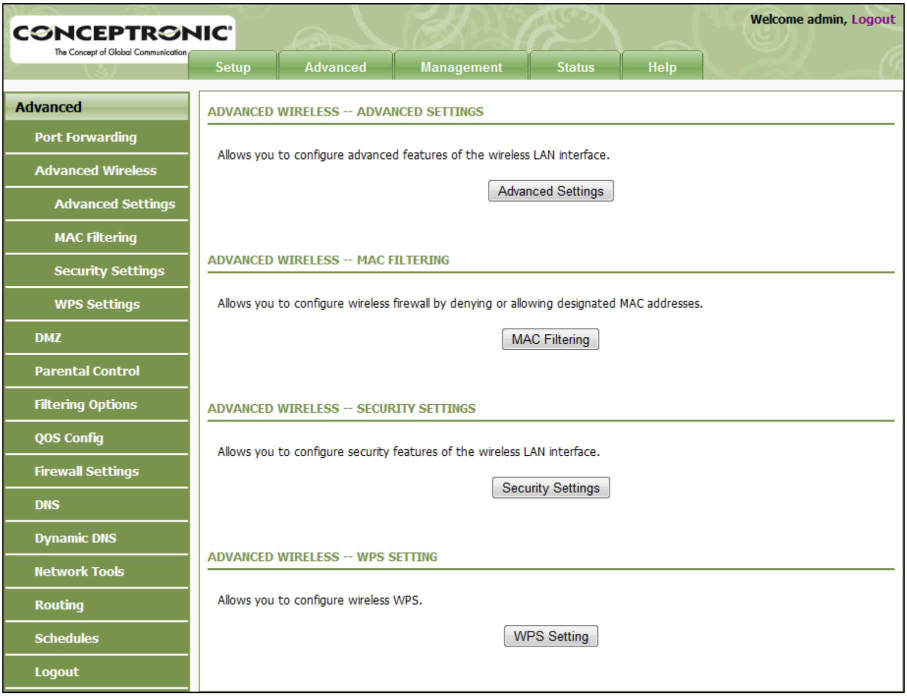
PORT FORWARDING SETUP

	Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	Schedule Rule	Remote IP
□	FTP Server	21	21	tcp	21	21	192.168.0.10	Always	

5.4.2 Advanced – Advanced Wireless

This function is used to modify the standard 802.11g wireless settings. It is recommended not changing the default settings, because incorrect settings may affect the performance of the wireless performance. The default settings provide the best wireless performance in most environments.

Choose **Advanced** > **Advanced Wireless**. The **ADVANCED WIRELESS** page as shown in the following figure appears:



ADVANCED WIRELESS -- ADVANCED SETTINGS

Allows you to configure advanced features of the wireless LAN interface.

Advanced Settings

ADVANCED WIRELESS -- MAC FILTERING

Allows you to configure wireless firewall by denying or allowing designated MAC addresses.

MAC Filtering

ADVANCED WIRELESS -- SECURITY SETTINGS

Allows you to configure security features of the wireless LAN interface.

Security Settings

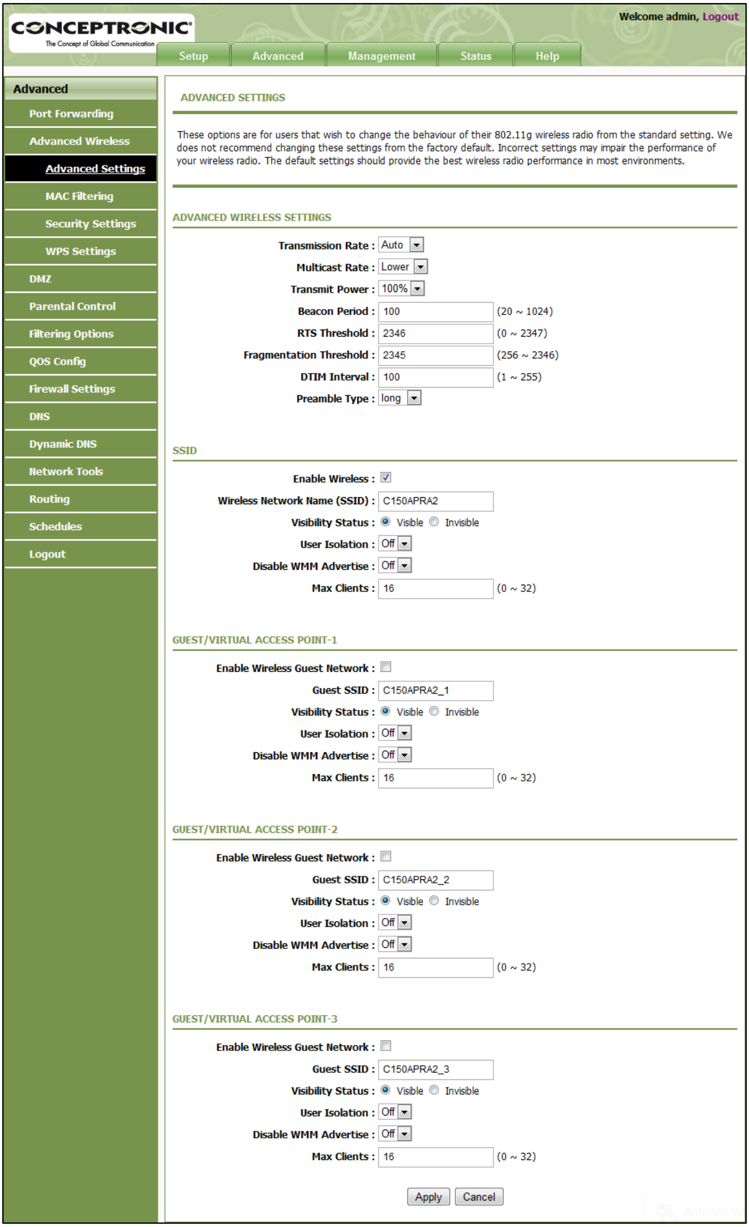
ADVANCED WIRELESS -- WPS SETTING

Allows you to configure wireless WPS.

WPS Setting

5.4.2.1 Advanced – Advanced Wireless – Advanced Settings

In the **ADVANCED WIRELESS** page, click **Advanced Settings.** The page as shown in the following figure appears:



ADVANCED SETTINGS

These options are for users that wish to change the behaviour of their 802.11g wireless radio from the standard setting. We does not recommend changing these settings from the factory default. Incorrect settings may impair the performance of your wireless radio. The default settings should provide the best wireless radio performance in most environments.

ADVANCED WIRELESS SETTINGS

Transmission Rate : Auto
Multicast Rate : Lower
Transmit Power : 100%
Beacon Period : 100 (20 ~ 1024)
RTS Threshold : 2346 (0 ~ 2347)
Fragmentation Threshold : 2345 (256 ~ 2346)
DTIM Interval : 100 (1 ~ 255)
Preamble Type : long

SSID

Enable Wireless : ☑
Wireless Network Name (SSID) : C150APRA2
Visibility Status : ● Visible ○ Invisible
User Isolation : Off
Disable WMM Advertise : Off
Max Clients : 16 (0 ~ 32)

GUEST/VIRTUAL ACCESS POINT-1

Enable Wireless Guest Network : □
Guest SSID : C150APRA2_1
Visibility Status : ● Visible ○ Invisible
User Isolation : Off
Disable WMM Advertise : Off
Max Clients : 16 (0 ~ 32)

GUEST/VIRTUAL ACCESS POINT-2

Enable Wireless Guest Network : □
Guest SSID : C150APRA2_2
Visibility Status : ● Visible ○ Invisible
User Isolation : Off
Disable WMM Advertise : Off
Max Clients : 16 (0 ~ 32)

GUEST/VIRTUAL ACCESS POINT-3

Enable Wireless Guest Network : □
Guest SSID : C150APRA2_3
Visibility Status : ● Visible ○ Invisible
User Isolation : Off
Disable WMM Advertise : Off
Max Clients : 16 (0 ~ 32)

The following table describes the parameters in this page.

ADVANCED WIRELESS SETTINGS

Field	Description
Transmission Rate	Select the transmission rate of the wireless network from the drop-down list.
Multicast Rate	Select the multicast transmission rate of the wireless network from the drop-down list. You can select **Lower** or **Higher**.
Transmit Power	Select the power for data transmission from the drop-down list. You can select **100%**, **80%**, **60%**, **40%**, or **20%**.
Beacon Period	By default, the wireless beacon frame sends the data once every 100ms. Its value range is 20—1024.
RTS Threshold	The threshold of transmission request. Its value range is 0—2347 and the default value is 2346.
Fragmentation Threshold	Its value range is 256—2346 and the default value is 2345.
DTIM Interval	Data beacon proportion (transmission quantity indication). Its value range is 1—255 and the default value is 100.
Preamble Type	Select the preamble code from the drop-down list. You can select **long** or **short**.

SSID

Field	Description
Enable Wireless	Select or deselect the check box to enable or disable the wireless function.
Wireless Network Name (SSID)	Set the wireless network name, that is, SSID. SSID is used to distinguish different wireless networks.
Visibility Status	Select whether to hide the AP. You can select **Visible** or **Invisible**. If you select **Invisible**, the AP is hidden and the terminal cannot obtain the SSID through passive scanning.
User Isolation	Select whether users of the AP can communicate with each other. You can select **Off** or **On** from the drop-down list. **On** indicates that computers connected to the device cannot communicate with each other.
Disable WMM Advertise	Select whether to disable WMM. You can select **Off** or **On**.
Max Clients	Set the maximum number of clients that can be connected to the AP at the same time. Its value range is 0—32.

GUEST/VIRTUAL ACCESS POINTS-1—3

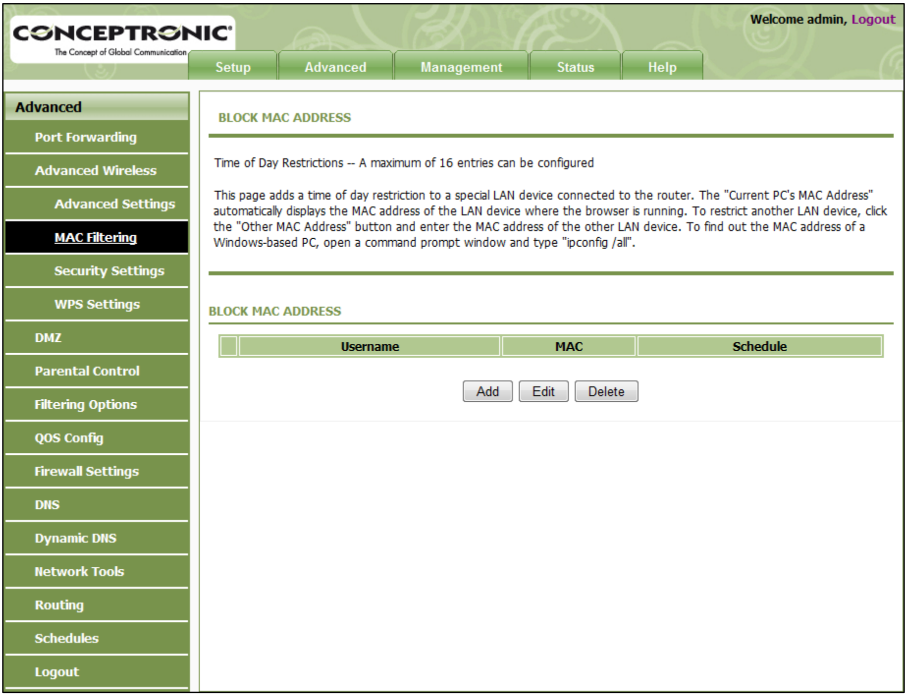
Field	Description
Enable Wireless Guest Network	Select or deselect the check box to enable or disable the wireless interface.
Guest SSID	Similar to the primary SSID, it identifies a wireless AP.

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

Click **Apply** to save the settings.

5.4.2.2 Advanced – Advanced Wireless – MAC Filtering

In the **ADVANCED WIRELESS** page, click **MAC Filtering**. The page as shown in the following figure appears:



BLOCK MAC ADDRESS

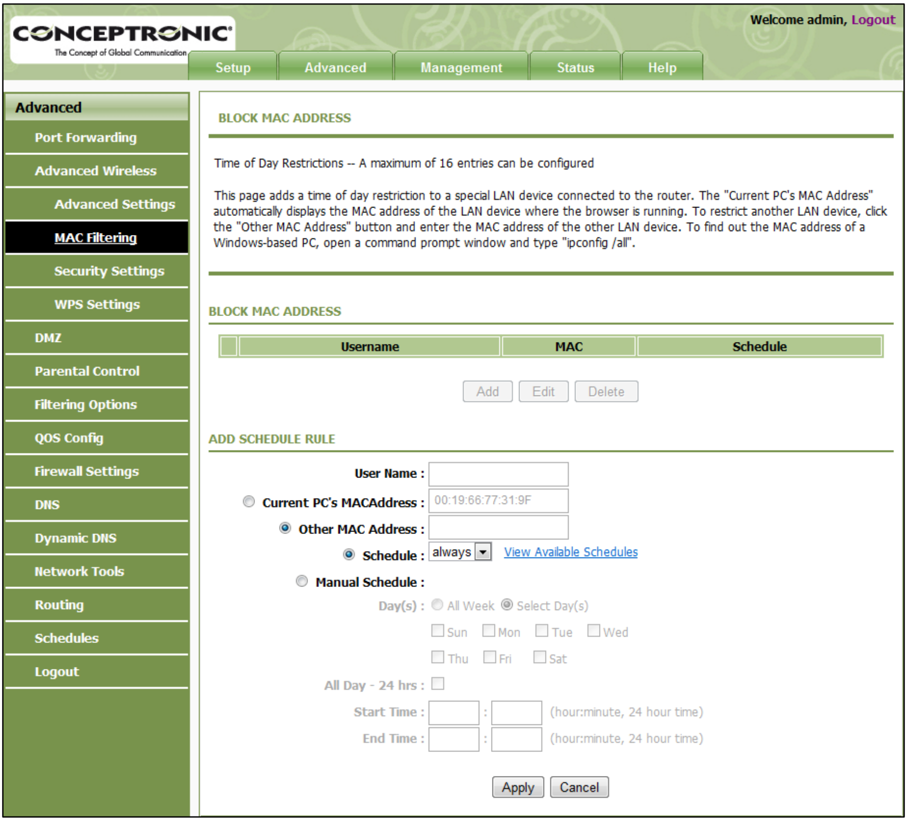
Time of Day Restrictions -- A maximum of 16 entries can be configured

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

BLOCK MAC ADDRESS

	Username	MAC	Schedule

Click **Add** and the page as shown in the following figure appears:



BLOCK MAC ADDRESS

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

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

BLOCK MAC ADDRESS

	Username	MAC	Schedule

Add Edit Delete

ADD SCHEDULE RULE

User Name :

○ Current PC's MACAddress : 00:19:66:77:31:9F

● Other MAC Address :

● Schedule : always View Available Schedules

○ Manual Schedule :

Day(s) : ○ All Week ● Select Day(s)

□ Sun □ Mon □ Tue □ Wed

□ Thu □ Fri □ Sat

All Day - 24 hrs : □

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

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

Apply Cancel

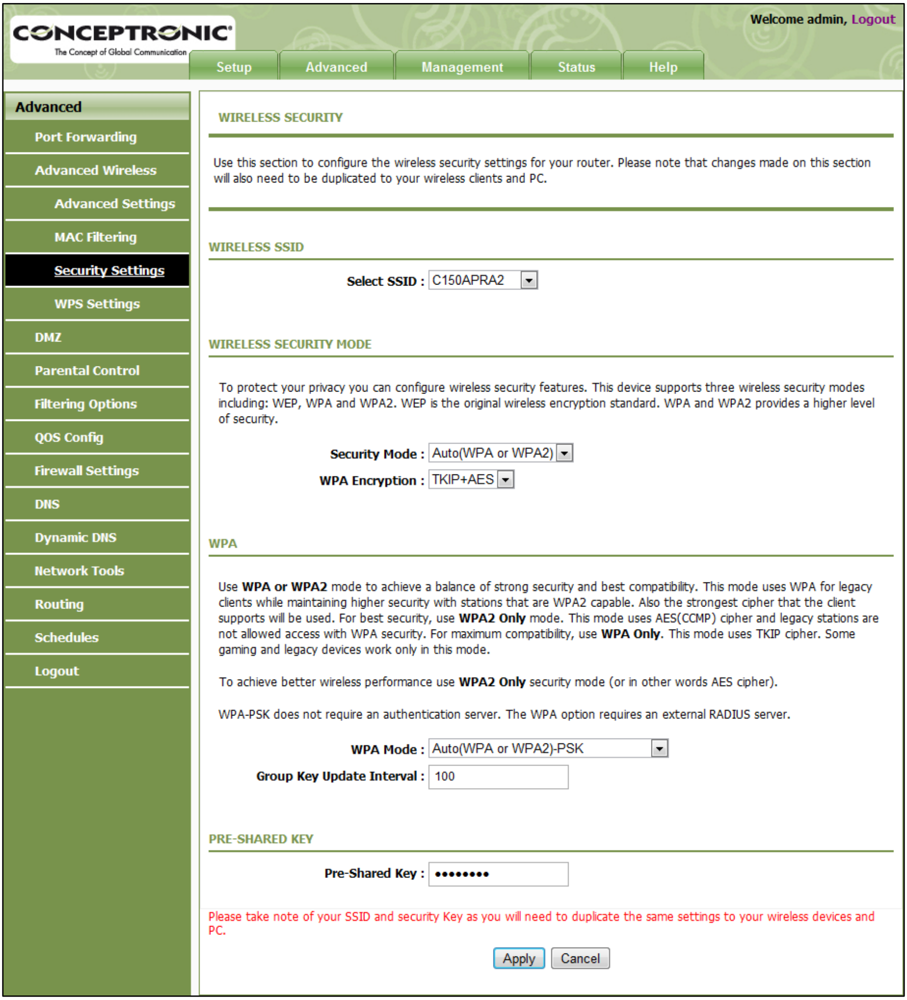
The following table describes the parameters in this page.

Field	Description
User Name	Enter the name that identifies your configuration. For example, *kids*.
Current PC's MAC Address	Enter the MAC address of the computer that connects to the device.
Other MAC Address	Enter the MAC address of another device that is included in MAC filtering.
Schedule	Select the time of MAC filter from the drop-down list. You can select **always** or **never**.
Manual Schedule	If you select this check box, you need to manually set the time of MAC filtering.

Click **Apply** to save the settings.

5.4.2.3 Advanced – Advanced Wireless – Security Settings

In the **ADVANCED WIRELESS** page, click **Security Settings**. The page as shown in the following figure appears:



WIRELESS SECURITY

Use this section to configure the wireless security settings for your router. Please note that changes made on this section will also need to be duplicated to your wireless clients and PC.

WIRELESS SSID

Select SSID : C150APRA2

WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2. WEP is the original wireless encryption standard. WPA and WPA2 provides a higher level of security.

Security Mode : Auto(WPA or WPA2)

WPA Encryption : TKIP+AES

WPA

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

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

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

WPA Mode : Auto(WPA or WPA2)-PSK

Group Key Update Interval : 100

PRE-SHARED KEY

Pre-Shared Key : ••••••••

Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

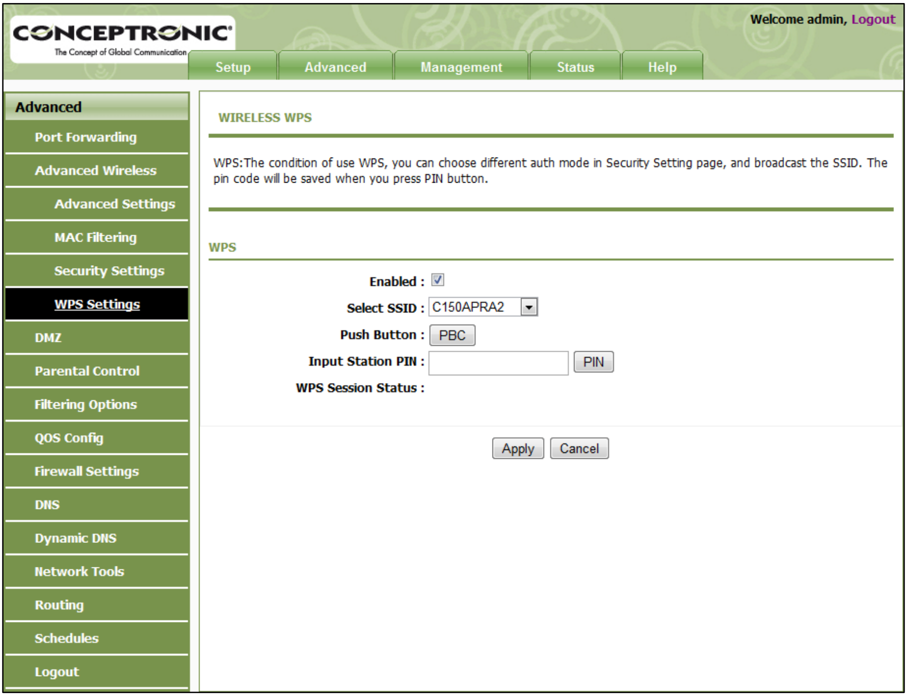
Select the desired SSID from the drop-down list.

Select the encryption type from the **Security Mode** drop-down list. You can select **None**, **WEP**, **AUTO (WPA or WPA2)**, **WPA Only**, or **WPA2 Only.** For parameters of different encryption types, see section **Error! Reference source not found.** "**Error! Reference source not found.**".

Click **Apply** to save the settings.

5.4.2.4 Advanced – Advanced Wireless – WPS Settings

In the **ADVANCED WIRELESS** page, click **WPS Settings**. The **WIRELESS WPS** page as shown in the following figure appears:



WIRELESS WPS

WPS:The condition of use WPS, you can choose different auth mode in Security Setting page, and broadcast the SSID. The pin code will be saved when you press PIN button.

WPS

Enabled : ☑

Select SSID : C150APRA2

Push Button : PBC

Input Station PIN :

WPS Session Status :

Enabled: The WPS service is enabled by default.

Note: Ensure that the network card supports the WPS function.

You can use one of the following there methods to use WPS authentication:

- Press the **WPS** button on the side panel for 3 seconds.
- In the **WIRELESS WPS** page, click **PBC**. It has the same function of the **WPS** button on the side panel. This is an optional method on wireless clients.

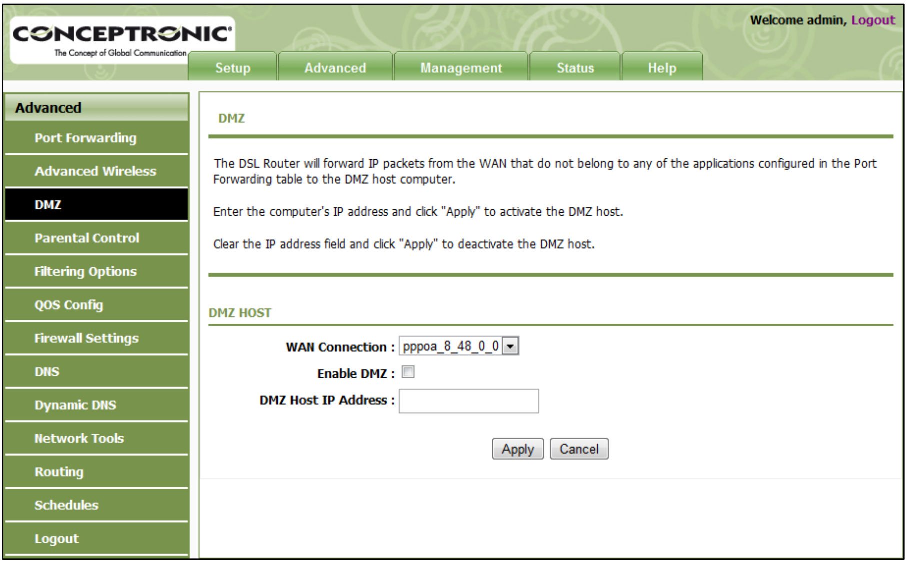
Note: You need a Registrar when using the PBC method in a special case in which the PIN is all zeros.

- In the **WIRELESS WPS** page, enter the **PIN** code provided by the station and click **PIN**. PIN entry is a mandatory method of setup for all WPS certified devices.

Note: If you are using the PIN method, you need a Registrar, either an access point or a wireless router, to initiate the registration between a new device and an active access point or a wireless router.

5.4.3 Advanced – DMZ

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



DMZ

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

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

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

DMZ HOST

WAN Connection : pppoa_8_48_0_0

Enable DMZ : □

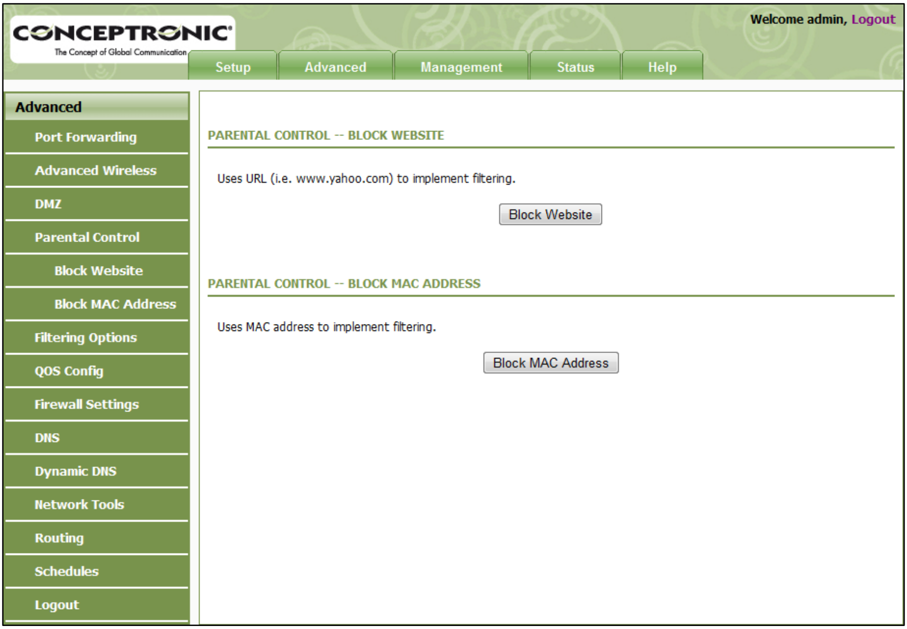
DMZ Host IP Address :

In this page, you can enable a DMZ host. In this way, access from Internet to the WAN IP address of the device is forwarded to the DMZ host and network server of the internal LAN is protected.

Click **Apply** to save the settings.

5.4.4 Advanced – Parental Control

Choose **Advanced** > **Parental Control**. The **PARENTAL CONTROL** page as shown in the following figure appears:



PARENTAL CONTROL -- BLOCK WEBSITE

Uses URL (i.e. www.yahoo.com) to implement filtering.

Block Website

PARENTAL CONTROL -- BLOCK MAC ADDRESS

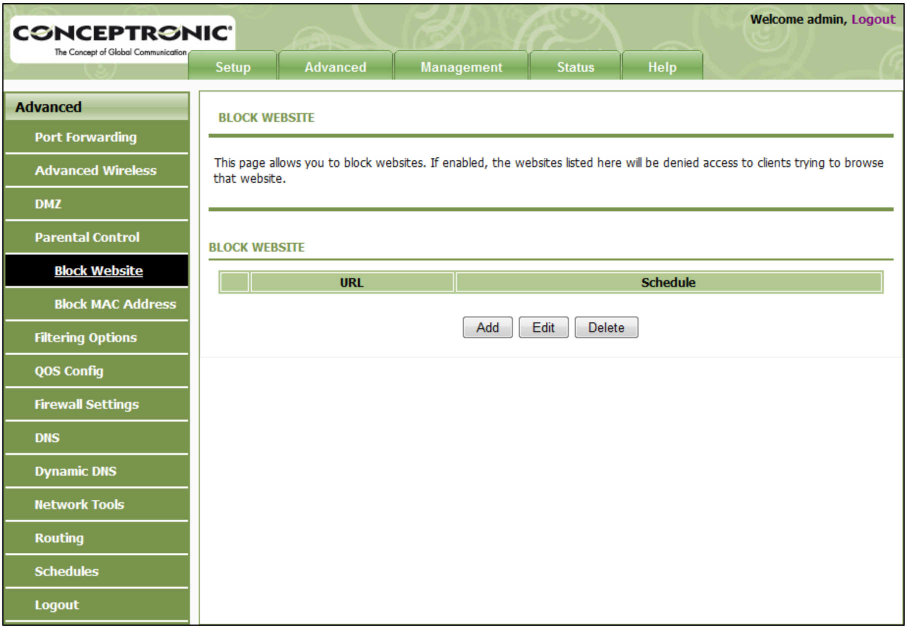
Uses MAC address to implement filtering.

Block MAC Address

This page provides two useful tools for restricting Internet access. **Block Website** allows you to quickly create a list of websites that you wish to prevent users from accessing. **Block MAC Address** allows you to control Internet access by clients or PCs connected to the device.

5.4.4.1 Advanced – Parental Control - Block Website

In the **PARENTAL CONTROL** page, click **Block Website**. The page as shown in the following figure appears:



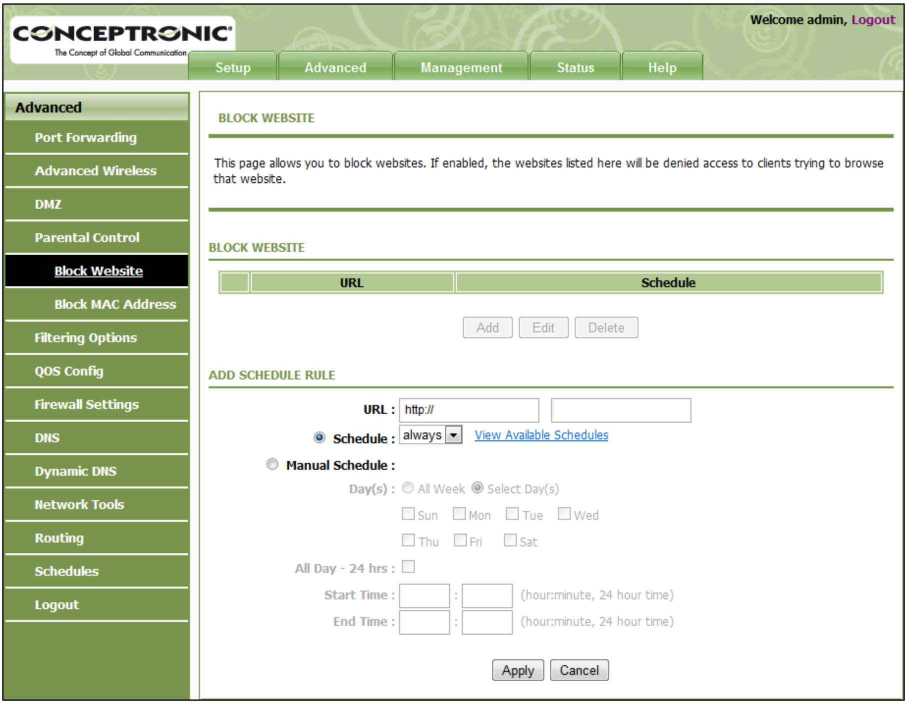
BLOCK WEBSITE

This page allows you to block websites. If enabled, the websites listed here will be denied access to clients trying to browse that website.

BLOCK WEBSITE

	URL	Schedule

Click **Add**. The page as shown in the following page appears:



BLOCK WEBSITE

This page allows you to block websites. If enabled, the websites listed here will be denied access to clients trying to browse that website.

BLOCK WEBSITE

	URL	Schedule

ADD SCHEDULE RULE

URL : http://

● Schedule : always

○ Manual Schedule :

Day(s) : ○ All Week ● Select Day(s)

□ Sun □ Mon □ Tue □ Wed

□ Thu □ Fri □ Sat

All Day - 24 hrs : □

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

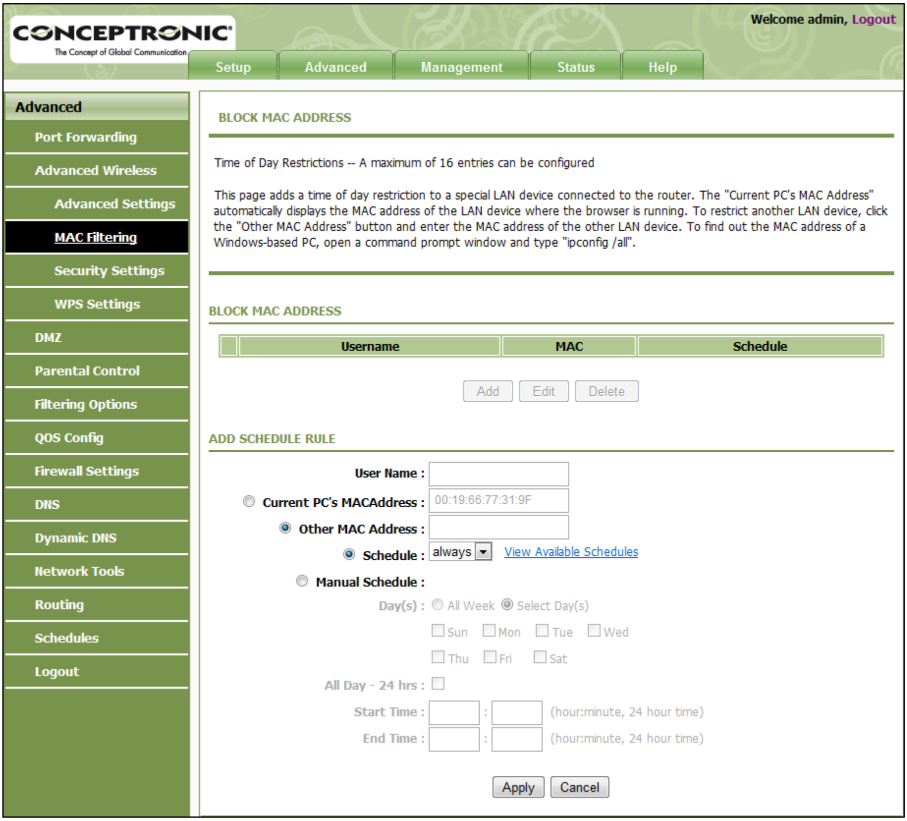
End Time : : (hour:minute, 24 hour time)

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

Click **Submit** to add the website to the **BLOCK WEBSITE** table.

5.4.4.2 Advanced – Parental Control – Block MAC Address

In the **PARENTAL CONTROL** page, click **Block MAC Address**. The page as shown in the following figure appears:



BLOCK MAC ADDRESS

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

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

BLOCK MAC ADDRESS

	Username	MAC	Schedule

ADD SCHEDULE RULE

User Name :

○ Current PC's MACAddress : 00:19:66:77:31:9F

● Other MAC Address :

● Schedule : always

○ Manual Schedule :

Day(s) : ○ All Week ● Select Day(s)

□ Sun □ Mon □ Tue □ Wed

□ Thu □ Fri □ Sat

All Day - 24 hrs : □

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

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

Note: The **Block MAC Address** feature from the **PARENTAL CONTROL** page refers to the **MAC Filtering** from the **ADVANCED SETTINGS** page.

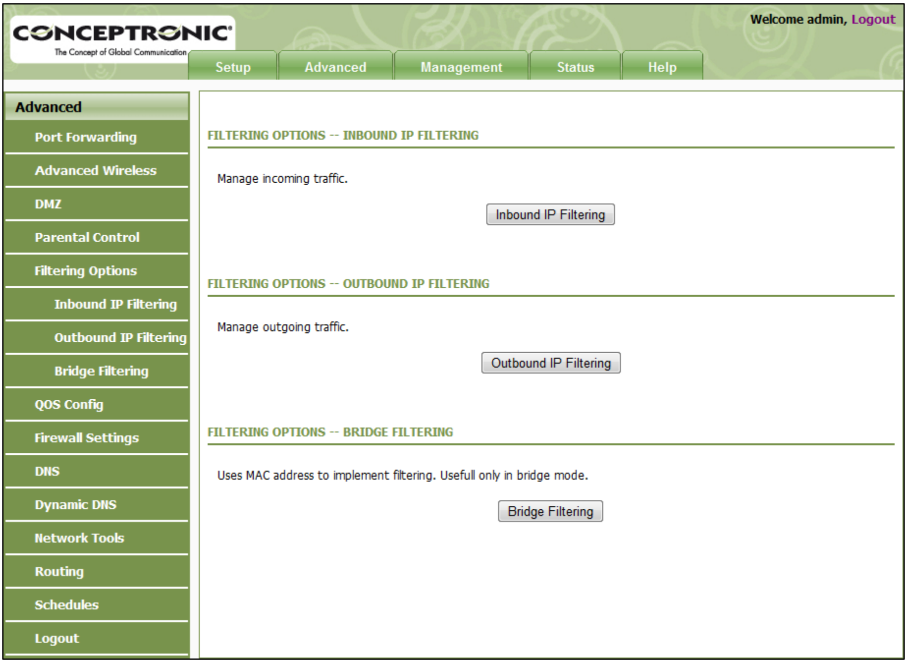
The following table describes the parameters in this page.

Field	Description
User Name	Enter the name that identifies your configuration. For example, *kids*.
Current PC's MAC Address	Enter the MAC address of the computer that connects to the device.
Other MAC Address	Enter the MAC address of another device that is included in MAC filtering.
Schedule	Select the time of MAC filter from the drop-down list. You can select **always** or **never**.
Manual Schedule	If you select this check box, you need to manually set the time of MAC filtering.

Click **Apply** to save the settings.

5.4.5 Advanced – Filtering Options

Choose **Advanced** > **Filtering Options**. The **FILTERING OPTIONS** page as shown in the following figure appears:



FILTERING OPTIONS -- INBOUND IP FILTERING

Manage incoming traffic.

FILTERING OPTIONS -- OUTBOUND IP FILTERING

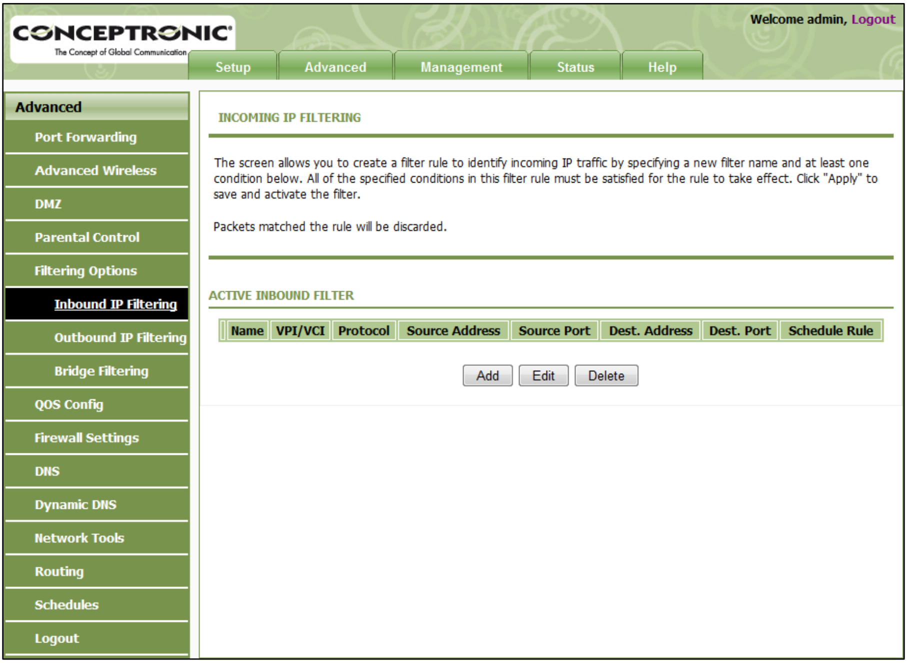
Manage outgoing traffic.

FILTERING OPTIONS -- BRIDGE FILTERING

Uses MAC address to implement filtering. Usefull only in bridge mode.

5.4.5.1 Advanced – Filtering Options – Inbound IP Filtering

In the **FILTERING OPTIONS** page, click **Inbound IP Filtering**. The **INCOMING IP FILTERING** page as shown in the following figure appears:



INCOMING IP FILTERING

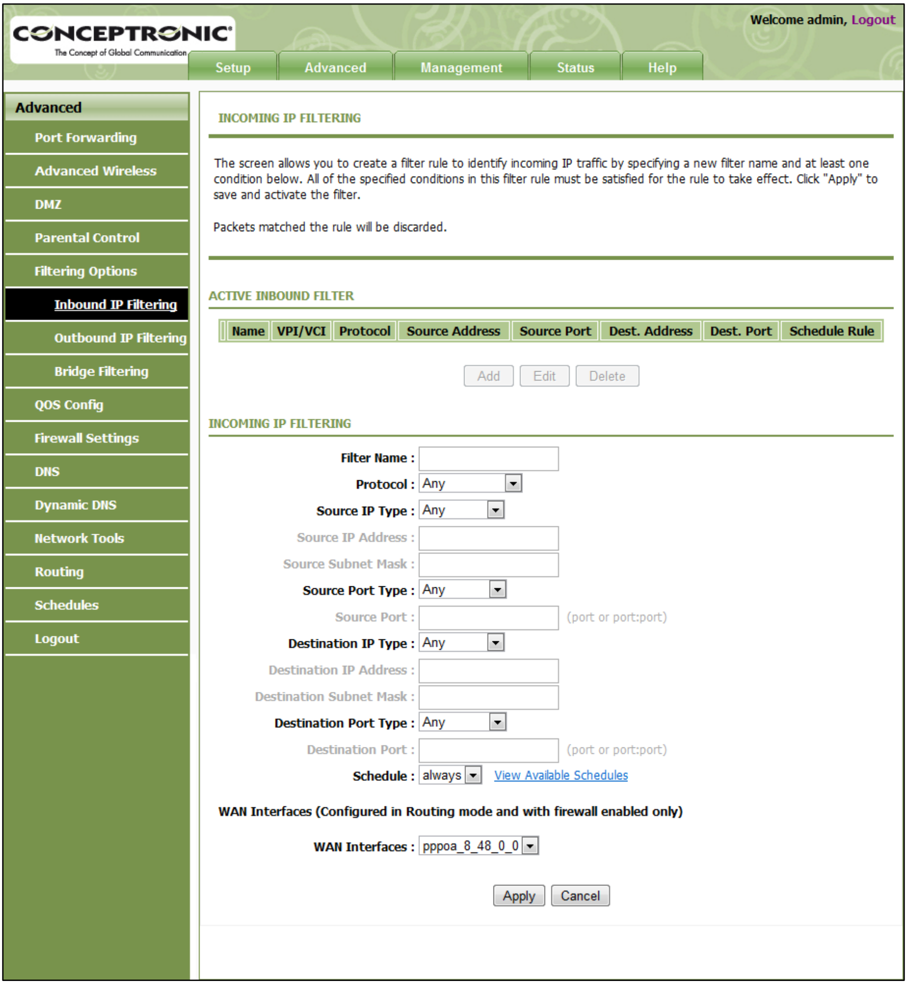
The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click "Apply" to save and activate the filter.

Packets matched the rule will be discarded.

ACTIVE INBOUND FILTER

Name	VPI/VCI	Protocol	Source Address	Source Port	Dest. Address	Dest. Port	Schedule Rule

Click **Add** to add an inbound IP filter. The page as shown in the following figure appears:



INCOMING IP FILTERING

The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click "Apply" to save and activate the filter.

Packets matched the rule will be discarded.

ACTIVE INBOUND FILTER

Name	VPI/VCI	Protocol	Source Address	Source Port	Dest. Address	Dest. Port	Schedule Rule

INCOMING IP FILTERING

Filter Name :	
Protocol :	Any
Source IP Type :	Any
Source IP Address :	
Source Subnet Mask :	
Source Port Type :	Any
Source Port :	(port or port:port)
Destination IP Type :	Any
Destination IP Address :	
Destination Subnet Mask :	
Destination Port Type :	Any
Destination Port :	(port or port:port)
Schedule :	always View Available Schedules

WAN Interfaces (Configured in Routing mode and with firewall enabled only)

WAN Interfaces : pppoa_8_48_0_0

Enter the **Filter Name** and specify at least one of the following criteria: protocol, source/destination IP address, subnet mask, and source/destination port.

Click **Apply** to save the settings.

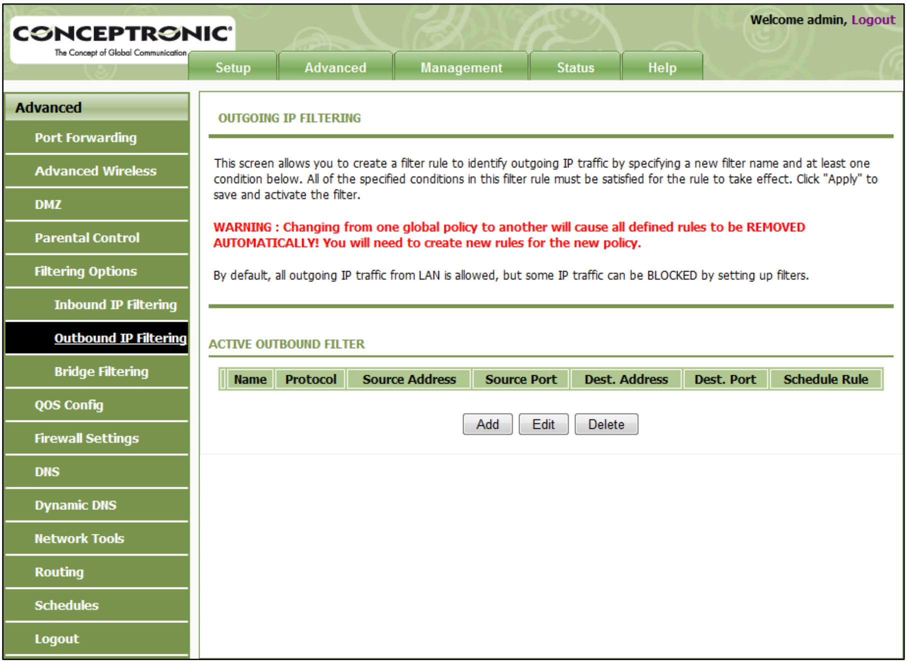
Note: The settings apply only when the firewall is enabled.

The **ACTIVE INBOUND FILTER** in the **INCOMING IP FILTERING** page displays detailed information of each created inbound IP filter. Click **Delete** to delete an IP filter. Note that the **Delete** button appears only when at least one IP filter exists.

5.4.5.2 Advanced – Filtering Options – Outbound IP Filtering

By default, all outgoing IP traffic from the LAN is allowed. The outbound filter allows you to create a filter rule to block outgoing IP traffic by specifying a filter name and at least one criterion.

In the **FILTERING OPTIONS** page, click **Outbound IP Filtering**. The **OUTGOING IP FILTERING** page as shown in the following figure appears:



OUTGOING IP FILTERING

This screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click "Apply" to save and activate the filter.

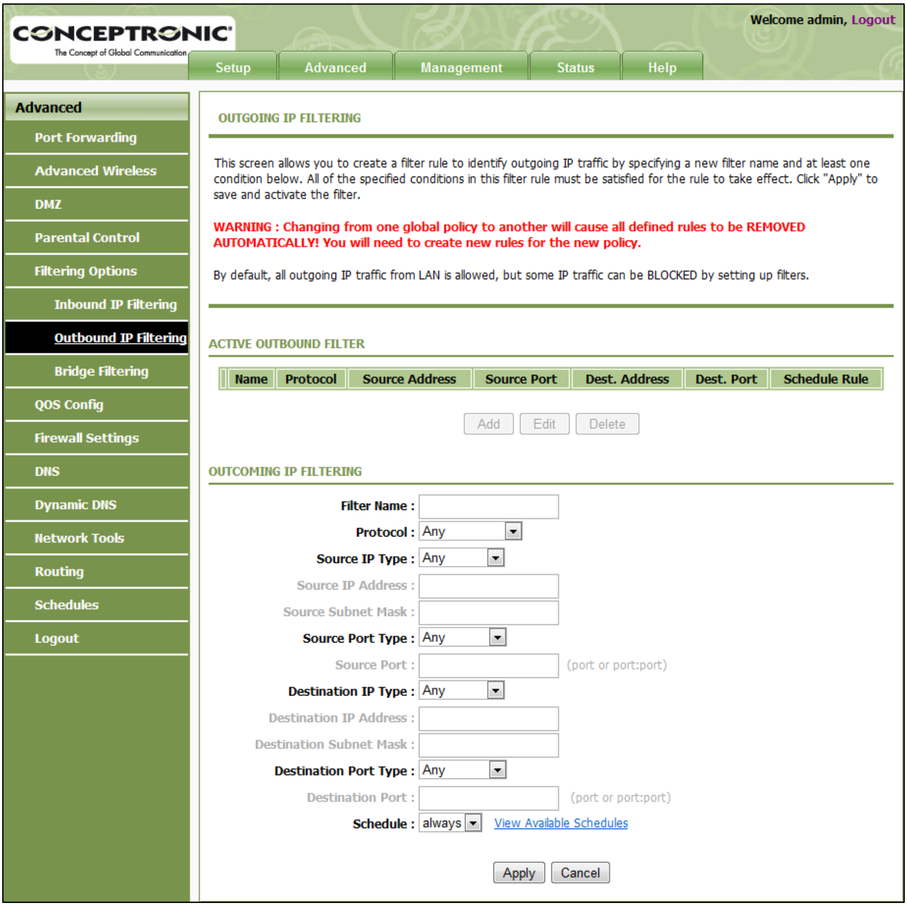
WARNING : Changing from one global policy to another will cause all defined rules to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be BLOCKED by setting up filters.

ACTIVE OUTBOUND FILTER

Name	Protocol	Source Address	Source Port	Dest. Address	Dest. Port	Schedule Rule

Click **Add** to add an outbound IP filter. The page as shown in the following figure appears:



OUTGOING IP FILTERING

This screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click "Apply" to save and activate the filter.

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

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be BLOCKED by setting up filters.

ACTIVE OUTBOUND FILTER

	Name	Protocol	Source Address	Source Port	Dest. Address	Dest. Port	Schedule Rule

Add Edit Delete

OUTCOMING IP FILTERING

Filter Name :	
Protocol :	Any
Source IP Type :	Any
Source IP Address :	
Source Subnet Mask :	
Source Port Type :	Any
Source Port :	(port or port:port)
Destination IP Type :	Any
Destination IP Address :	
Destination Subnet Mask :	
Destination Port Type :	Any
Destination Port :	(port or port:port)
Schedule :	always View Available Schedules

Apply Cancel

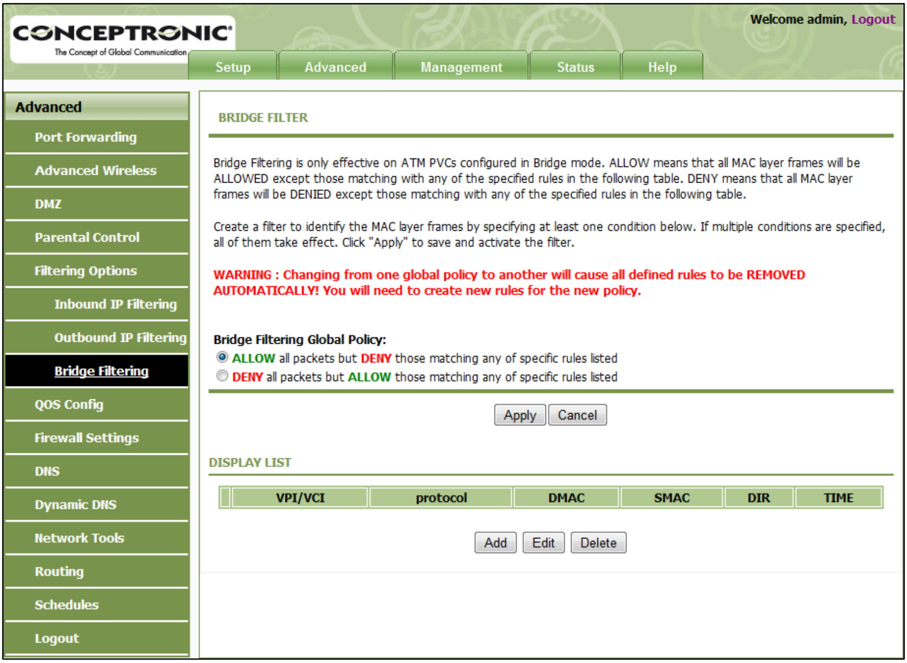
Enter the **Filter Name** and specify at least one of the following criteria: protocol, source/destination IP address, subnet mask, and source/destination port.

Click **Apply** to save the settings.

The **ACTIVE OUTBOUND FILTER** in the **OUTGOING IP FILTERING** page displays detailed information OF each created outbound IP filter. Click **Delete** to delete an IP filter. Note that the **Delete** button appears only when at least one IP filter exists.

5.4.5.3 Advanced – Filtering Options – Bridge Filtering

In the **FILTERING OPTIONS** page, click **Bridge Filtering**. The page as shown in the following figure appears:



BRIDGE FILTER

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

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

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

Bridge Filtering Global Policy:
● ALLOW all packets but DENY those matching any of specific rules listed
○ DENY all packets but ALLOW those matching any of specific rules listed

Apply Cancel

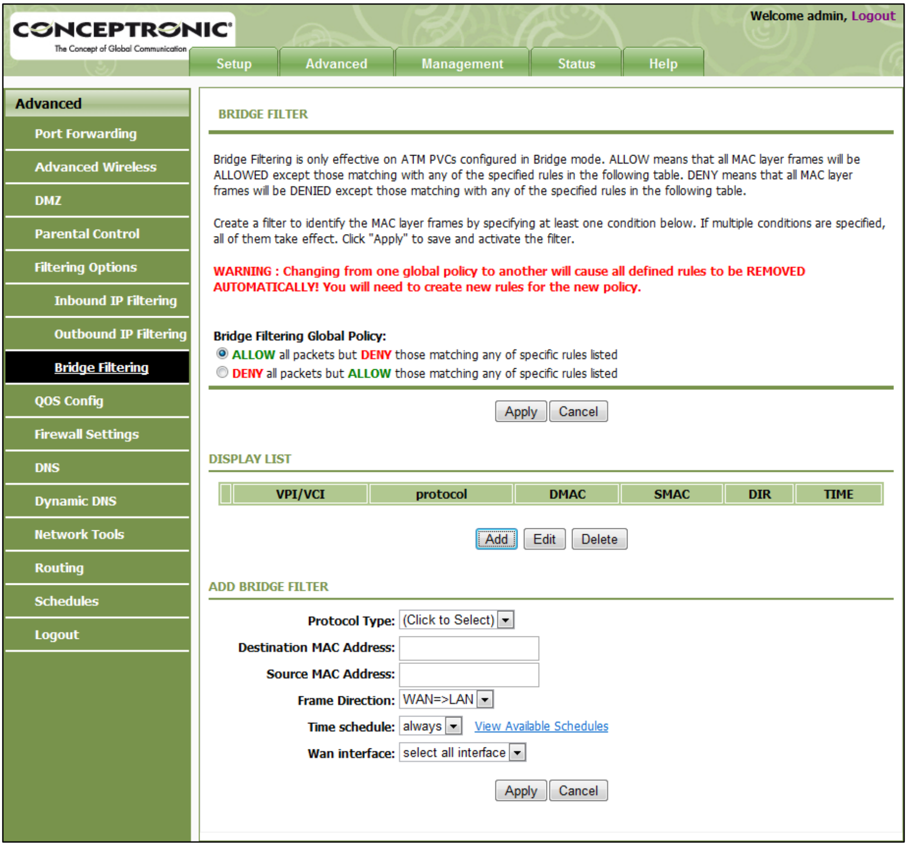
DISPLAY LIST

	VPI/VCI	protocol	DMAC	SMAC	DIR	TIME

Add Edit Delete

This page is used to configure bridge parameters. In this page, you can modify the settings or view the information of the bridge and its attached ports.

Click **Add** to add a bridge filter. The page as shown in the following figure appears:



BRIDGE FILTER

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

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

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

Bridge Filtering Global Policy:
● ALLOW all packets but DENY those matching any of specific rules listed
○ DENY all packets but ALLOW those matching any of specific rules listed

DISPLAY LIST

	VPI/VCI	protocol	DMAC	SMAC	DIR	TIME

ADD BRIDGE FILTER

Protocol Type:	(Click to Select)
Destination MAC Address:	
Source MAC Address:	
Frame Direction:	WAN=>LAN
Time schedule:	always View Available Schedules
Wan interface:	select all interface

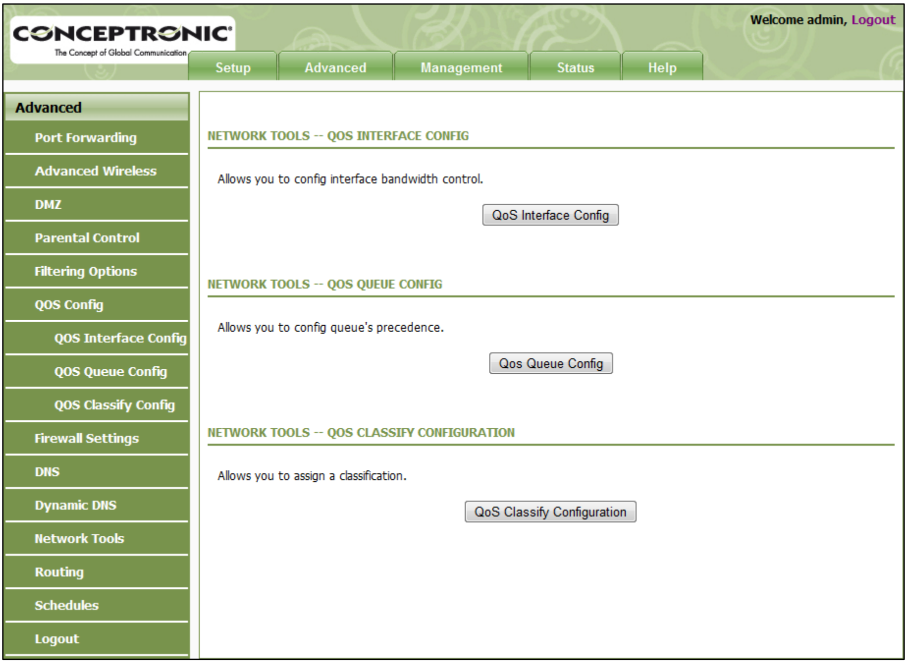
The following table describes the parameters in this page.

Field	Description
Protocol Type	Select the protocol type to be mapped from the drop-down list. You can select **PPPoE**, **IPv4**, **IPv6**, **AppleTalk**, **IPX**, **NetBEUI**, or **IGMP**.
Destination MAC Address	Enter the destination MAC address to be mapped.
Source MAC Address	Enter the source MAC address to be mapped.
Frame Direction	Select the frame direction to be mapped from the drop-down list. The device supports frame direction from LAN to WAN and that from WAN to LAN.
Time schedule	Select the time that you want to apply the rule from the drop-down list. You can select **always** or **never**.
Wan interface	Select the WAN interface to be mapped from the drop-down list.

Click **Apply** to save the settings.

5.4.6 Advanced – QOS Config

Choose **Advanced** > **QoS Config**. The page as shown in the following figure appears:



NETWORK TOOLS -- QOS INTERFACE CONFIG

Allows you to config interface bandwidth control.

QoS Interface Config

NETWORK TOOLS -- QOS QUEUE CONFIG

Allows you to config queue's precedence.

Qos Queue Config

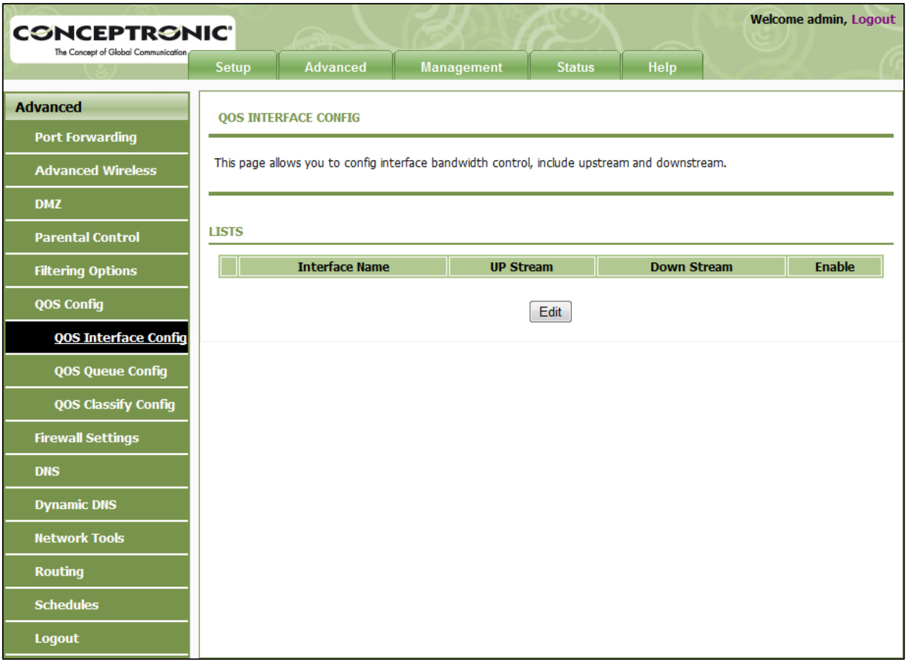
NETWORK TOOLS -- QOS CLASSIFY CONFIGURATION

Allows you to assign a classification.

QoS Classify Configuration

5.4.6.1 Advanced – QOS Config – QOS Interface Config

In the **QoS CONFIG** page, click **QoS Interface Config.** The page as shown in the following figure appears:



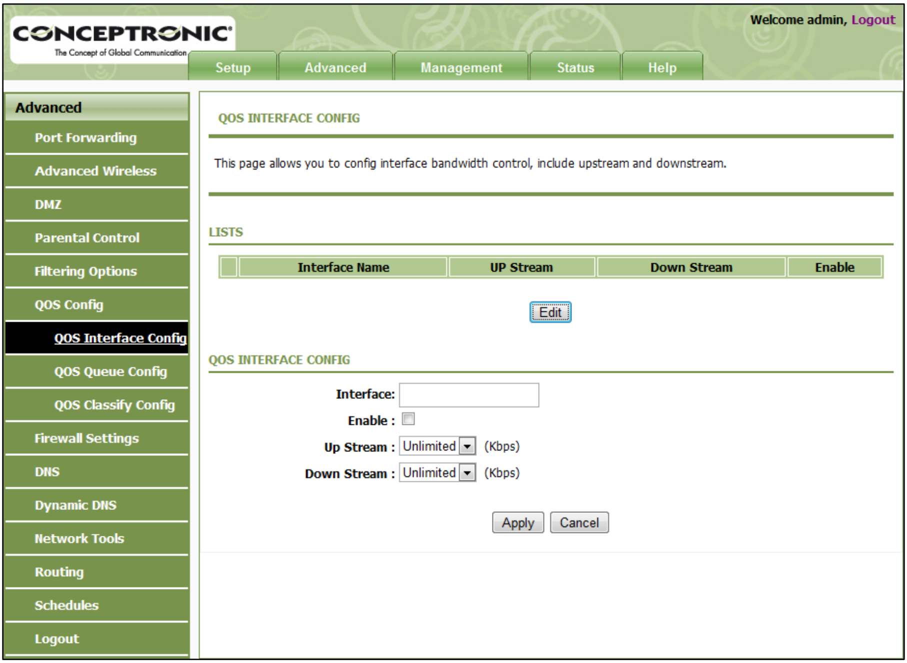
QOS INTERFACE CONFIG

This page allows you to config interface bandwidth control, include upstream and downstream.

LISTS

	Interface Name	UP Stream	Down Stream	Enable

Click **Edit** and the page as shown in the following figure appears:



QOS INTERFACE CONFIG

This page allows you to config interface bandwidth control, include upstream and downstream.

LISTS

	Interface Name	UP Stream	Down Stream	Enable

QOS INTERFACE CONFIG

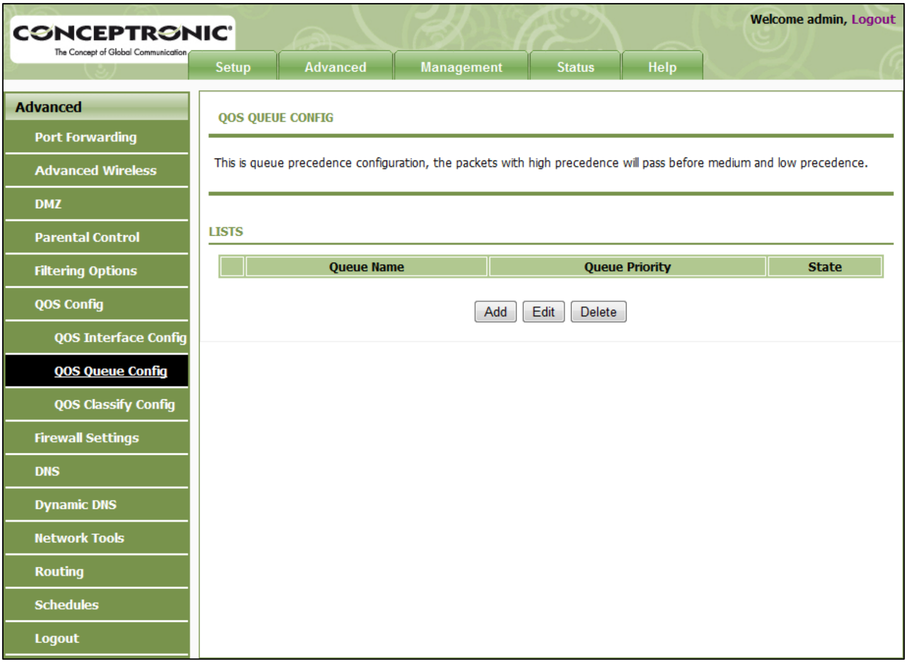
Interface:	
Enable :	□
Up Stream :	Unlimited (Kbps)
Down Stream :	Unlimited (Kbps)

In this page, you can configure the uplink bandwidth and downlink bandwidth of each interface. The uplink rate and the downlink rate are limited according to the configured bandwidth.

Click **Apply** to save the settings.

5.4.6.2 Advanced – QOS Config – QOS Queue Config

In the **QoS CONFIG** page, click **Qos Queue Config**. The page as shown in the following figure appears:



QOS QUEUE CONFIG

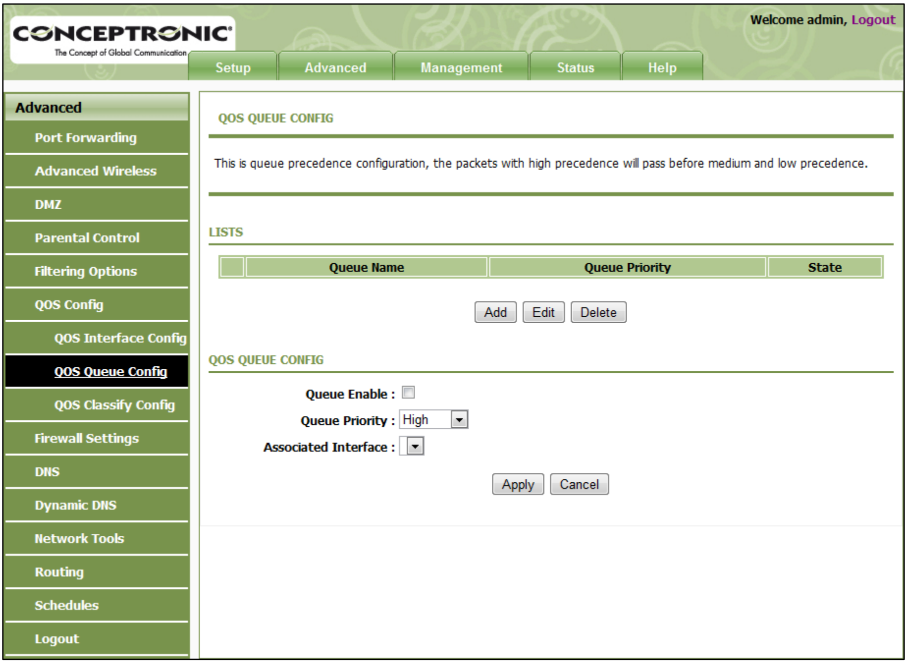
This is queue precedence configuration, the packets with high precedence will pass before medium and low precedence.

LISTS

	Queue Name	Queue Priority	State

In this page, you can configure the priority of the queue. The device supports the following three priority levels: high, medium, low. The device handles packets of the high queue priority first, then packets of medium, and finally packets of low priority.

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



QOS QUEUE CONFIG

This is queue precedence configuration, the packets with high precedence will pass before medium and low precedence.

LISTS

	Queue Name	Queue Priority	State

Add Edit Delete

QOS QUEUE CONFIG

Queue Enable : □

Queue Priority : High

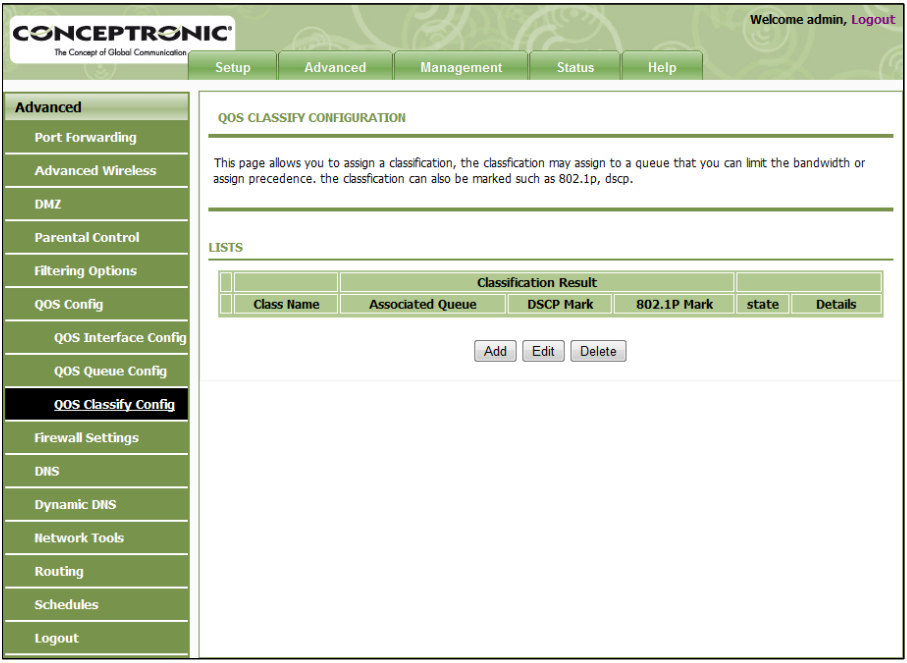
Associated Interface :

Apply Cancel

Click **Apply** to save the settings.

5.4.6.3 Advanced – QOS Config – QOS Classify Config

In the **QoS CONFIG** page, click **QoS Classify Configuration**. The page as shown in the following figure appears:



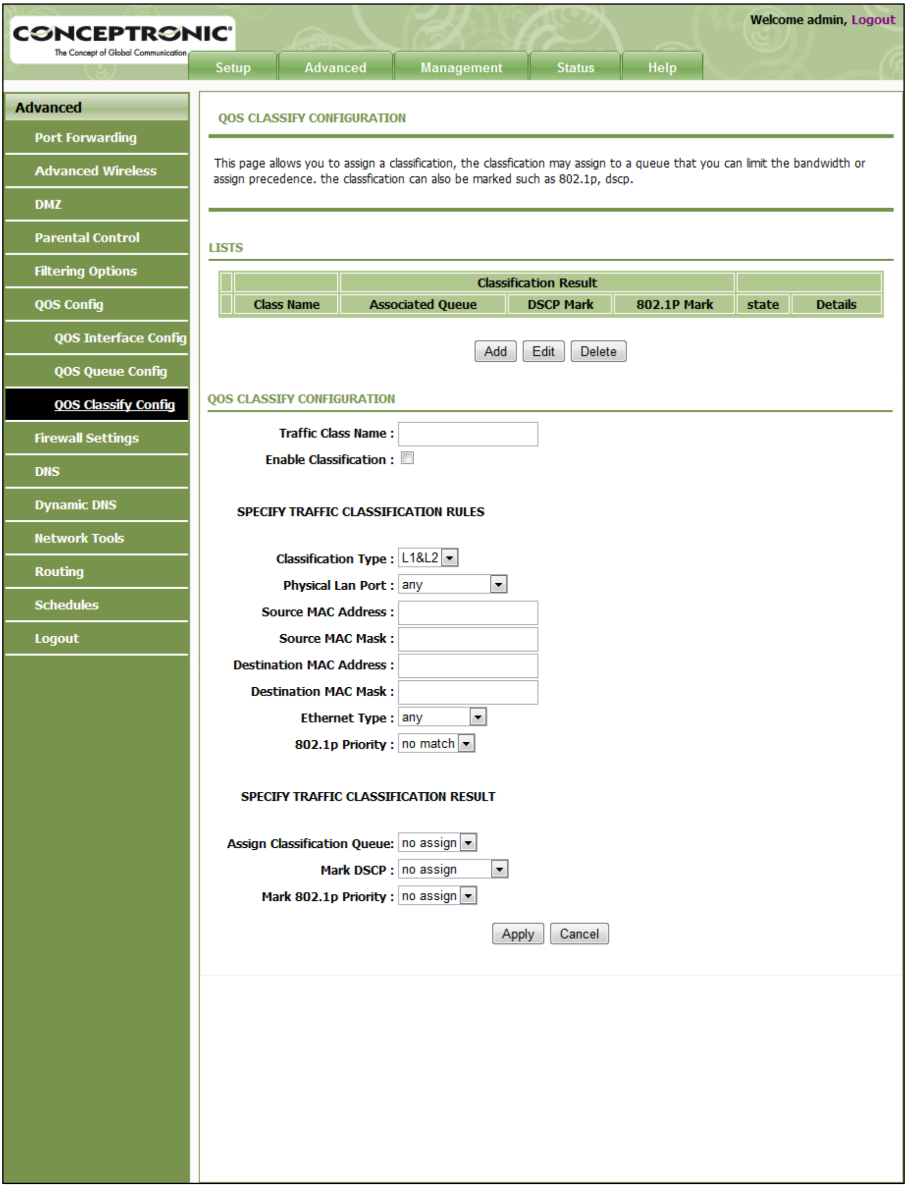
QOS CLASSIFY CONFIGURATION

This page allows you to assign a classification, the classfication may assign to a queue that you can limit the bandwidth or assign precedence. the classfication can also be marked such as 802.1p, dscp.

LISTS

		Classification Result				
	Class Name	Associated Queue	DSCP Mark	802.1P Mark	state	Details

This page displays the classes. Click **Add** and the page as shown in the following figure appears:



QOS CLASSIFY CONFIGURATION

This page allows you to assign a classification, the classfication may assign to a queue that you can limit the bandwidth or assign precedence. the classfication can also be marked such as 802.1p, dscp.

LISTS

		Classification Result				
	Class Name	Associated Queue	DSCP Mark	802.1P Mark	state	Details

QOS CLASSIFY CONFIGURATION

Traffic Class Name :

Enable Classification : □

SPECIFY TRAFFIC CLASSIFICATION RULES

Classification Type : L1&L2

Physical Lan Port : any

Source MAC Address :

Source MAC Mask :

Destination MAC Address :

Destination MAC Mask :

Ethernet Type : any

802.1p Priority : no match

SPECIFY TRAFFIC CLASSIFICATION RESULT

Assign Classification Queue: no assign

Mark DSCP : no assign

Mark 802.1p Priority : no assign

The following table describes the parameters in this page.

Field	Description
Traffic Class Name	Enter the name of the traffic class.
Enable Classification	Select or deselect the check box to enable or disable QoS classification.

SPECIFY TRAFFIC CLASSIFICATION RULES

Field	Description
Classification Type	Select **L1&L2** or **L3&L4** from the drop-down list. ● **L1&L2** maps to the features of layer 1 and layer 2, such as the MAC address. ● **L3&L4** maps to the features of layer 3 and layer 4, such as the IP address and the port.
Physical Lan Port	Select the physical port of the packet from the drop-down list. For example, ethernet1, ethernet2, ethernet3, and ethernet4.
Source MAC Address	Enter the source MAC address of the packet.
Source MAC Mask	Use mask 000000ffffff to mask the MAC address. 00 indicates not mapped and ff indicates mapped.
Destination MAC Address	Enter the destination MAC address of the packet.
Destination MAC Mask	Use mask 000000ffffff to mask the MAC address. 00 indicates not mapped and ff indicates mapped
Ethernet Type	Select the layer 2 protocol type from the drop-down list. For example, IP protocol and IPX protocol.
802.1p Priority	Select the 802.1p priority of the packet from the drop-down list. You can select **no assign** or a value in the range of 0—7. Note that this function is not supported at the moment.

SPECIFIC TRAFFIC CLASSIFICATION RESULT

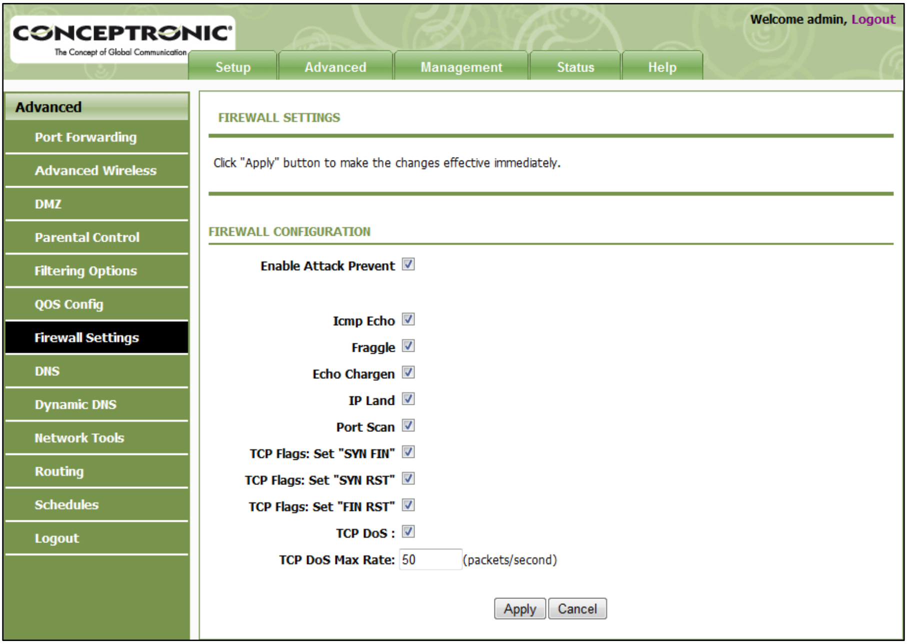
Field	Description
Assign Classification Queue	Specify the queue to which the packet belongs. You can set the queue in the classification configuration.
Mark DSCP	Attach the DSCP mark to the mapped packet.
Mark 802.1p Priority	Attach the 802.1p mark to the mapped packet.

Click **Apply** to save the settings.

5.4.7 Advanced – Firewall Settings

A denial-of-service (DoS) attack is one of the most common network attacks and is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. It usually leads to overload of system server or core dump of the system.

Choose **Advanced** > **Firewall Settings**. The page as shown in the following figure appears:



FIREWALL SETTINGS

Click "Apply" button to make the changes effective immediately.

FIREWALL CONFIGURATION

Enable Attack Prevent ☑

Icmp Echo ☑

Fraggle ☑

Echo Chargen ☑

IP Land ☑

Port Scan ☑

TCP Flags: Set "SYN FIN" ☑

TCP Flags: Set "SYN RST" ☑

TCP Flags: Set "FIN RST" ☑

TCP DoS : ☑

TCP DoS Max Rate: 50 (packets/second)

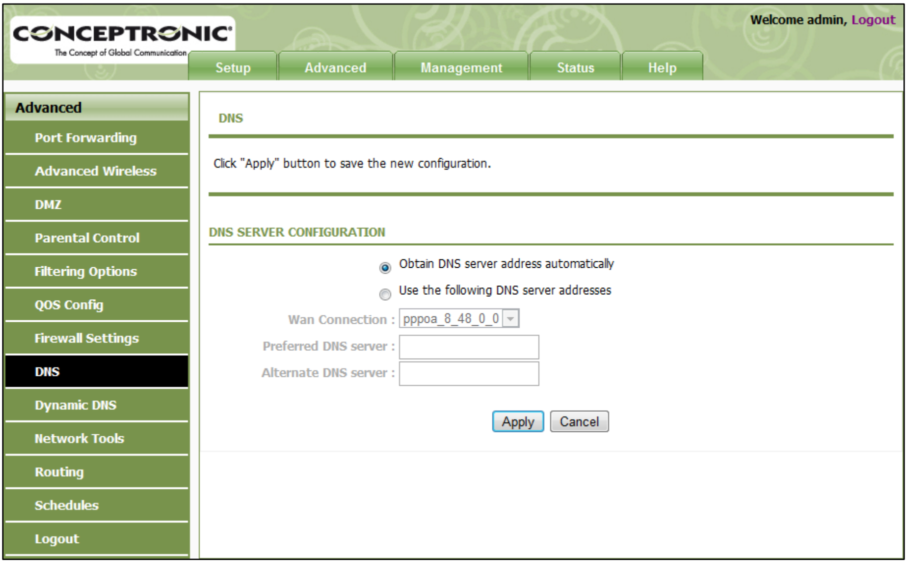
Click **Apply** to save the settings.

5.4.8 Advanced – DNS

Domain name system (DNS) is an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they are easier to remember. The Internet, however, is actually based on IP addresses. Each time you use a domain name, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might be translated to 198.105.232.4.

The DNS system is, in fact, its own network. If one DNS server does not know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

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



DNS

Click "Apply" button to save the new configuration.

DNS SERVER CONFIGURATION

● Obtain DNS server address automatically

○ Use the following DNS server addresses

Wan Connection : pppoa_8_48_0_0

Preferred DNS server :

Alternate DNS server :

The following table describes the parameters in this page.

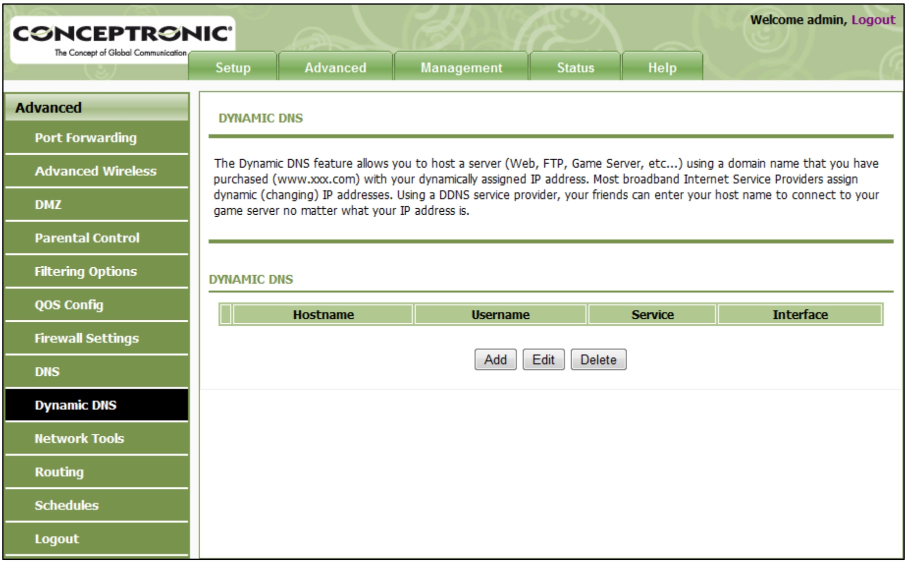
Field	Description
Obtain DNS server address automatically	If you select this radio button, the device automatically obtains IP address of the DNS server from the ISP. You need not manually enter the IP address of the server.
Use the following DNS server addresses	If you select this radio button, you need to manually enter the IP address of the server provided by the ISP.
WAN Connection	Select the WAN interface of the DNS server to be connected from the drop-down list.
Preferred DNS server	Enter the IP address of the primary DNS server.
Alternate DNS server	Enter the IP address of the secondary DNS server. If the primary DNS server fails to work, the device tries to connect the secondary DNS server.

Click **Apply** to save the settings.

5.4.9 Advanced – Dynamic DNS

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

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



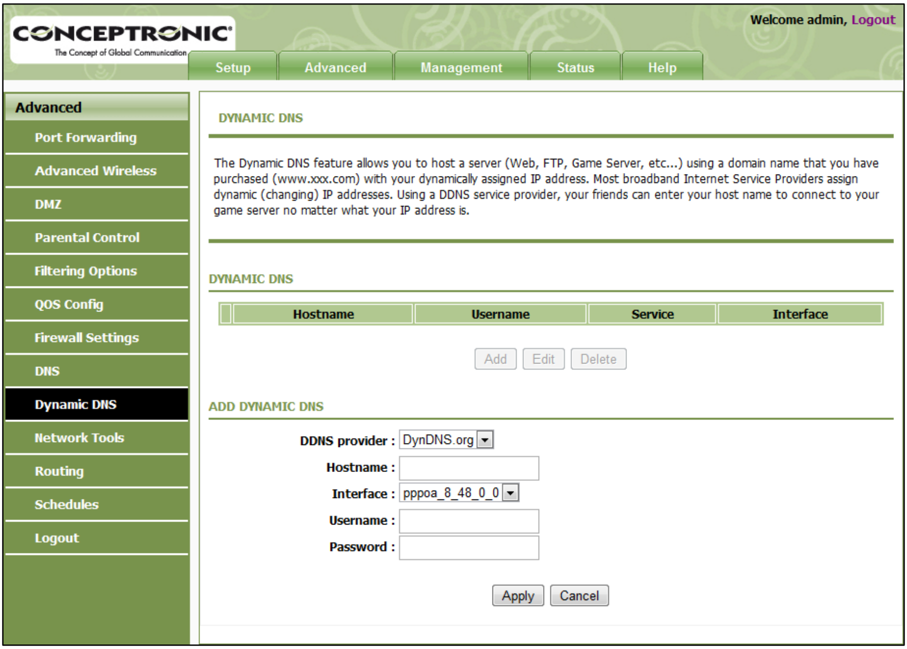
DYNAMIC DNS

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

DYNAMIC DNS

	Hostname	Username	Service	Interface

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



DYNAMIC DNS

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

DYNAMIC DNS

	Hostname	Username	Service	Interface

ADD DYNAMIC DNS

DDNS provider : DynDNS.org
Hostname :
Interface : pppoa_8_48_0_0
Username :
Password :

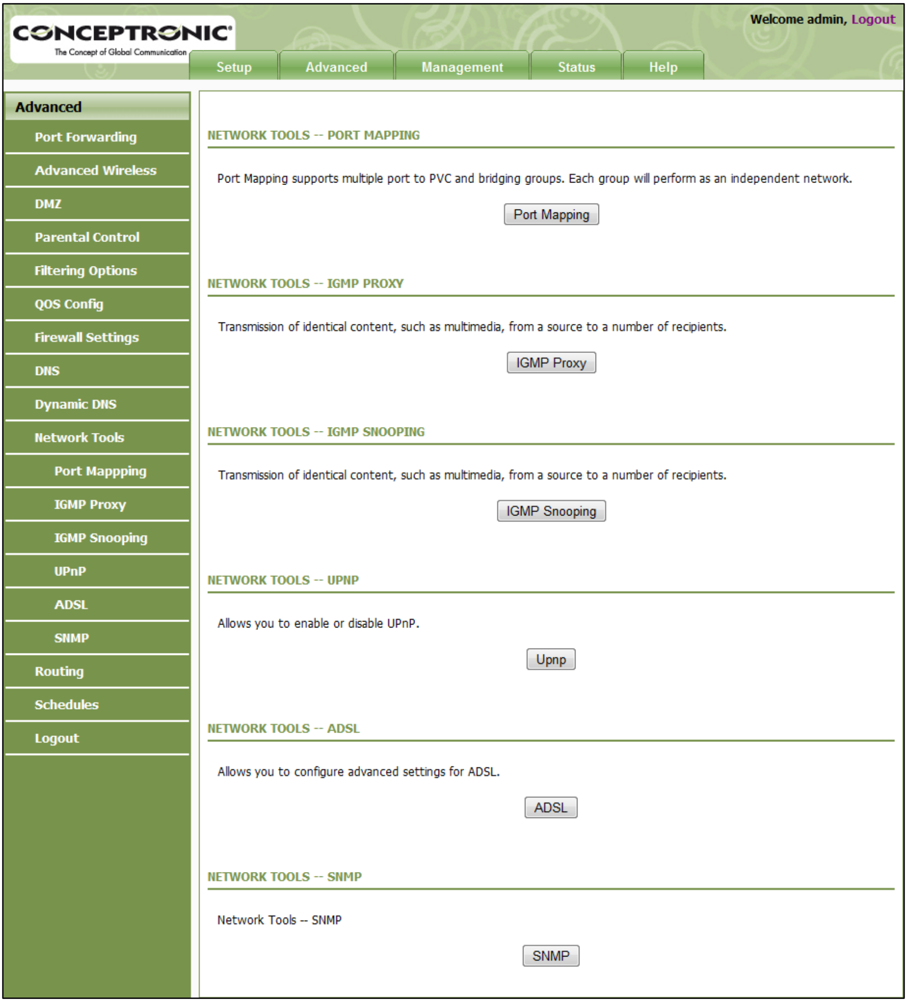
The following table describes the parameters in this page.

Field	Description
DDNS provider	Select the DDNS provider from the drop-down list. You can select **DynDns.org**, **TZO**, or **GnuDIP**.
Hostname	Enter the host name that you register with your DDNS provider.
Interface	Select the interface that is used for DDNS service from the drop-down list. The IP address of the interface corresponds to the host name.
Username	Enter the user name of your DDNS account.
Password	Enter the password of your DDNS account.

Click **Apply** to save the settings.

5.4.10 Advanced – Network Tools

Choose **Advanced** > **Network Tools**. The **NETWORK TOOLS** page as shown in the following figure appears:



NETWORK TOOLS -- PORT MAPPING

Port Mapping supports multiple port to PVC and bridging groups. Each group will perform as an independent network.

NETWORK TOOLS -- IGMP PROXY

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

NETWORK TOOLS -- IGMP SNOOPING

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

NETWORK TOOLS -- UPNP

Allows you to enable or disable UPnP.

NETWORK TOOLS -- ADSL

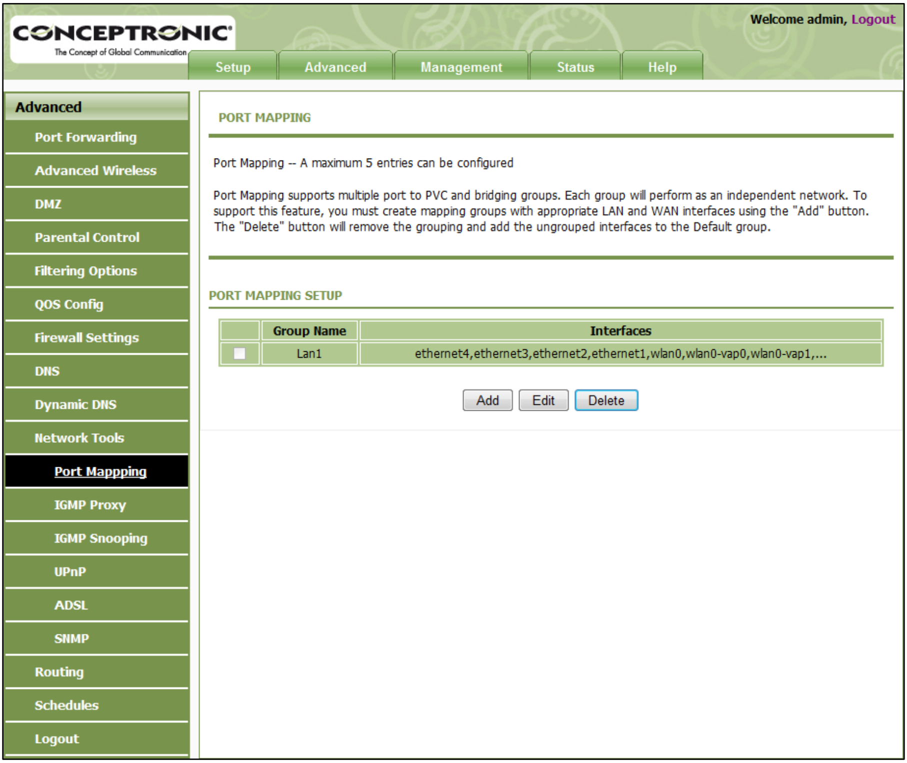
Allows you to configure advanced settings for ADSL.

NETWORK TOOLS -- SNMP

Network Tools -- SNMP

5.4.10.1 Advanced – Network Tools – Port Mapping

In the **NETWORK TOOLS** page, click **Port Mapping**. The page as shown in the following figure appears:



PORT MAPPING

Port Mapping -- A maximum 5 entries can be configured

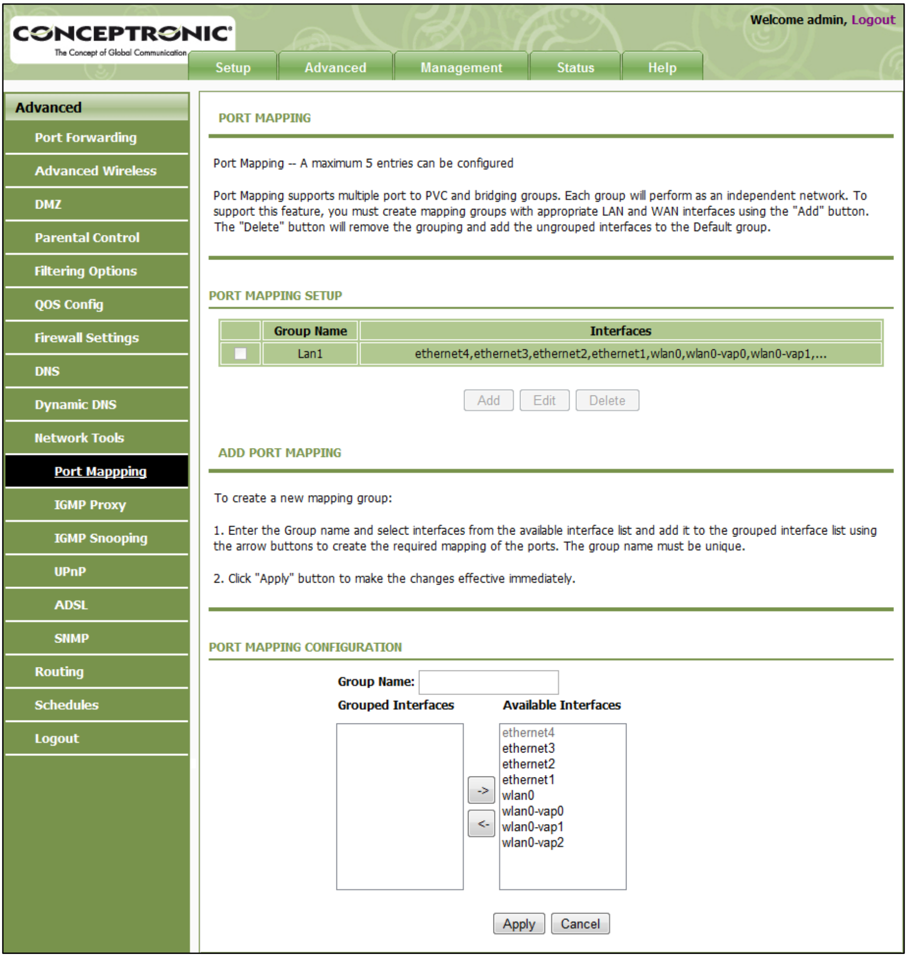
Port Mapping supports multiple port to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the "Add" button. The "Delete" button will remove the grouping and add the ungrouped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

PORT MAPPING SETUP

	Group Name	Interfaces
□	Lan1	ethernet4,ethernet3,ethernet2,ethernet1,wlan0,wlan0-vap0,wlan0-vap1,...

In this page, you can bind the WAN interface and the LAN interface to the same group.

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



PORT MAPPING

Port Mapping -- A maximum 5 entries can be configured

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

PORT MAPPING SETUP

	Group Name	Interfaces
□	Lan1	ethernet4,ethernet3,ethernet2,ethernet1,wlan0,wlan0-vap0,wlan0-vap1,...

ADD PORT MAPPING

To create a new mapping group:

1. Enter the Group name and select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. The group name must be unique.

2. Click "Apply" button to make the changes effective immediately.

PORT MAPPING CONFIGURATION

Group Name:

Grouped Interfaces

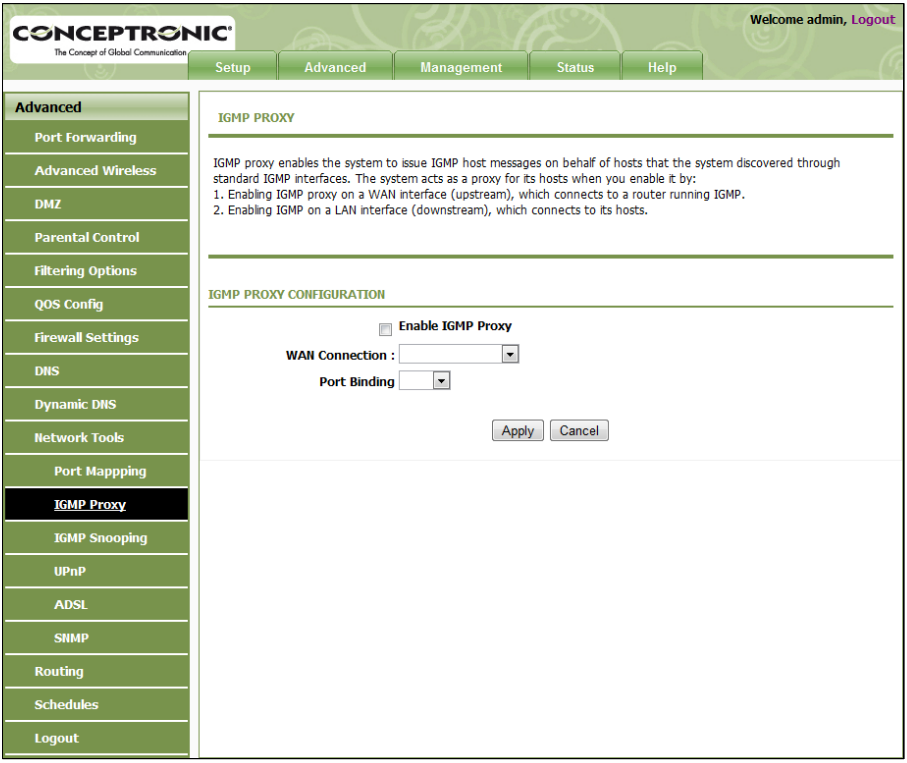
Available Interfaces
ethernet4
ethernet3
ethernet2
ethernet1
wlan0
wlan0-vap0
wlan0-vap1
wlan0-vap2

To create a mapping group, do as follows:

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

5.4.10.2 Advanced – Network Tools – IGMP Proxy

In the **NETWORK TOOLS** page, click **IGMP Proxy**. The page as shown in the following figure appears:



IGMP PROXY

IGMP proxy enables the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. The system acts as a proxy for its hosts when you enable it by:
1. Enabling IGMP proxy on a WAN interface (upstream), which connects to a router running IGMP.
2. Enabling IGMP on a LAN interface (downstream), which connects to its hosts.

IGMP PROXY CONFIGURATION

□ Enable IGMP Proxy

WAN Connection :

Port Binding

IGMP proxy enables the device to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. The device serves as a proxy for its hosts after you enable the function.

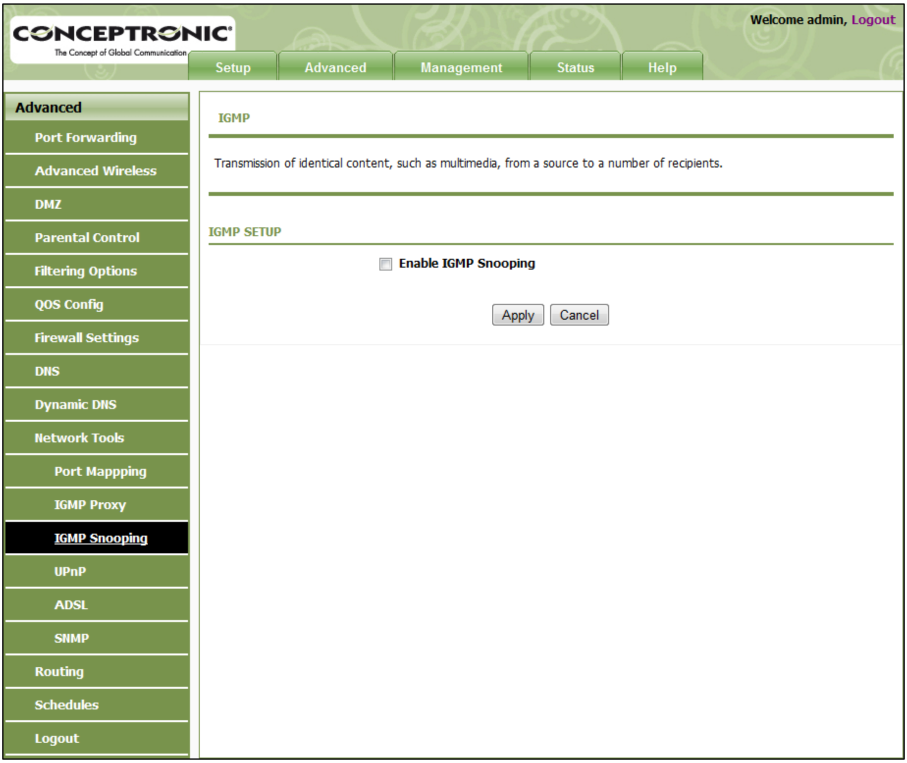
Select Enable IGMP Proxy and select the desired WAN and corresponding LAN interface.

Click **Apply** to save the settings.

5.4.10.3 Advanced – Network Tools – IGMP Snooping

When IGMP snooping is enabled, only hosts that belong to the group receive the multicast packets. If a host is deleted from the group, the host cannot receive the multicast packets any more.

In the **NETWORK TOOLS** page, click **IGMP Snooping**. The page as shown in the following figure appears:



IGMP

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

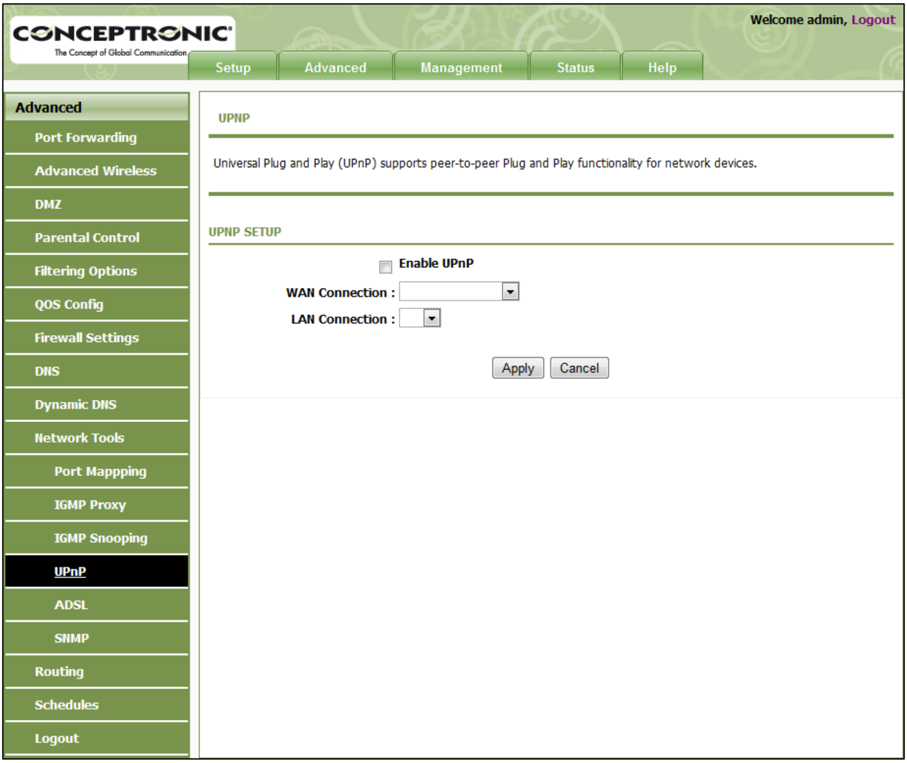
IGMP SETUP

□ Enable IGMP Snooping

Click **Apply** to save the settings.

5.4.10.4 Advanced – Network Tools – UPnP

In the **NETWORK TOOLS** page, click **Upnp**. The page as shown in the following figure appears:



UPNP

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

UPNP SETUP

□ Enable UPnP

WAN Connection :

LAN Connection :

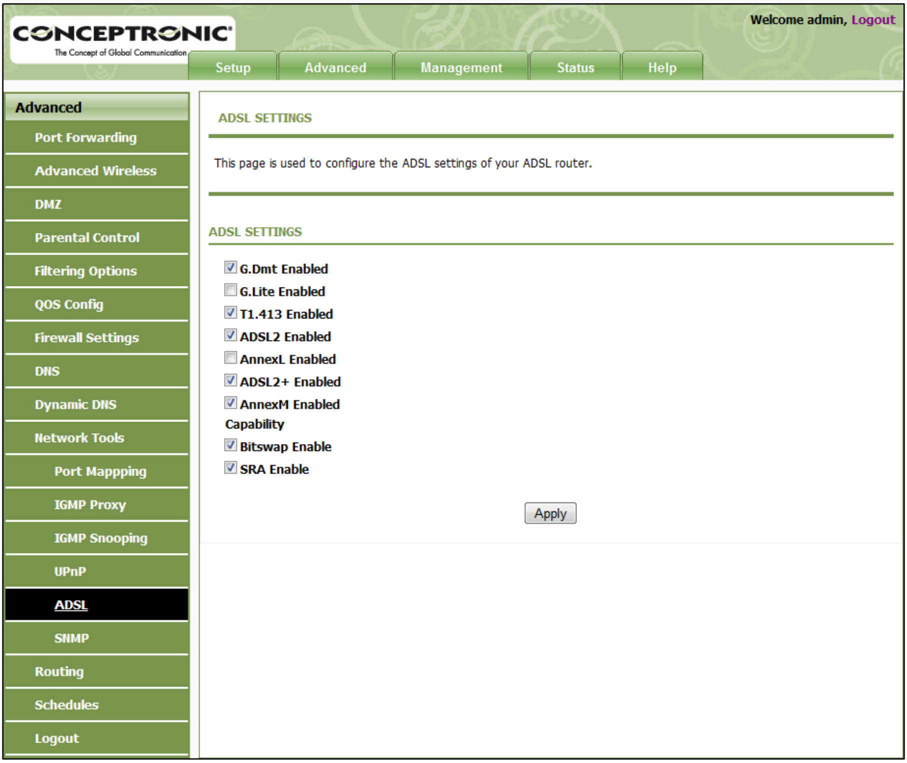
In this page, you can enable universal plug and play (UPnP) and then the system serves as a daemon.

UPnP is widely applied in audio and video software. It automatically searches devices in the network. If you are concerned about UPnP security, you can disable it.

Select the WAN and LAN interfaces at which you want to enable UPnP and click **Apply** to save the settings.

5.4.10.5 Advanced – Network Tools – ADSL

In the **NETWORK TOOLS** page, click **ADSL**. The page as shown in the following figure appears:



ADSL SETTINGS

This page is used to configure the ADSL settings of your ADSL router.

ADSL SETTINGS

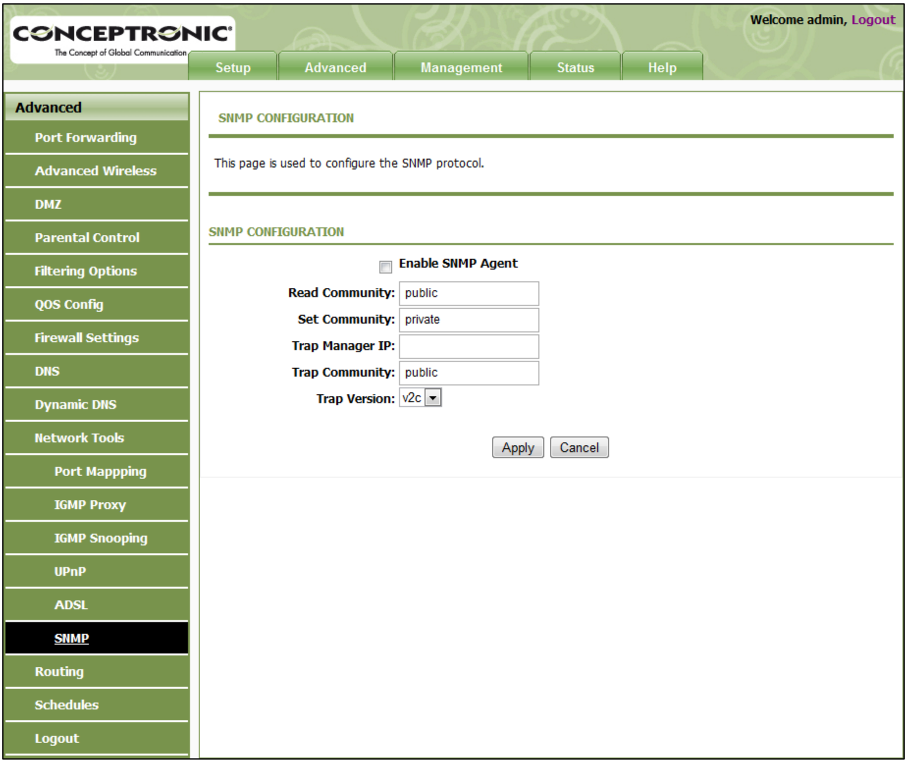
☑ G.Dmt Enabled
☐ G.Lite Enabled
☑ T1.413 Enabled
☑ ADSL2 Enabled
☐ AnnexL Enabled
☑ ADSL2+ Enabled
☑ AnnexM Enabled
Capability
☑ Bitswap Enable
☑ SRA Enable

In this page, you can select the ADSL modulation. Normally, you are recommended to keep the factory defaults. The device supports the following modulation types: G.Dmt, G.lite, T1.413, ADSL2, AnnexL, ADSL2+, and AnnexM. The device negotiates the modulation mode with the DSLAM.

Click **Apply** to save the settings.

5.4.10.6 Advanced – Network Tools – SNMP

In the **NETWORK TOOLS** page, click **SNMP**. The page as shown in the following figure appears:



SNMP CONFIGURATION

This page is used to configure the SNMP protocol.

SNMP CONFIGURATION

□ Enable SNMP Agent

Read Community: public

Set Community: private

Trap Manager IP:

Trap Community: public

Trap Version: v2c

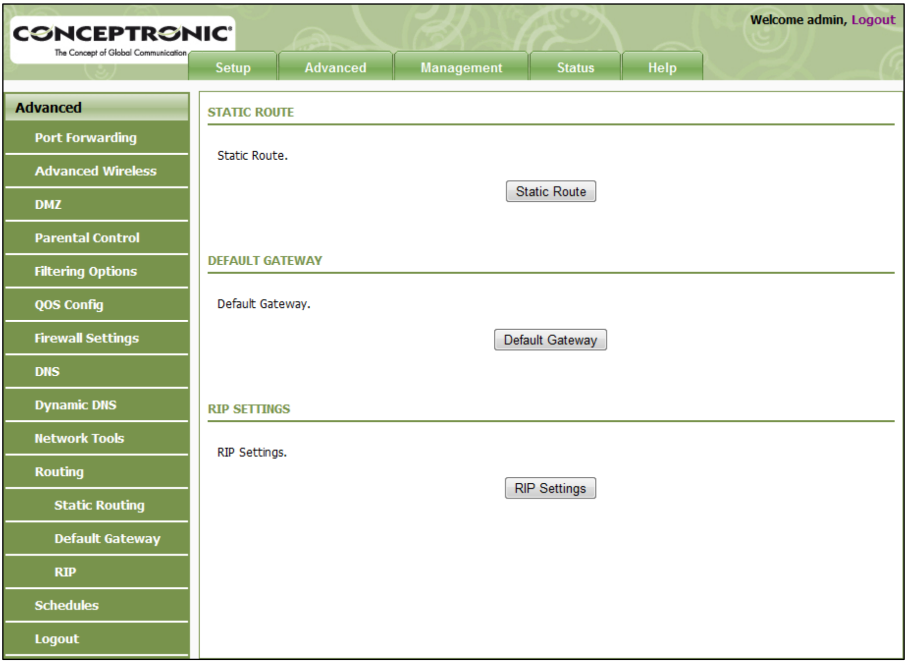
In this page, you can set the SNMP parameters. The following table describes the parameters in this page.

Field	Description
Enable SNMP Agent	Select or deselect the check box to enable or disable SNMP agent.
Read Community	Universal character to obtain the device information. It is similar to the password. The SNMP application entity can use it to directly obtain the device information.
Set Community	Universal character to modify the device configuration. It is similar to the password. The SNMP application entity can use it to directly modify the device configuration.
Trap Manager IP	Enter the address of the server that receives the trap message.
Trap Community	The field that is included in the trap message sent by the device.
Trap Version	Select the trap version from the drop-down list. You can select **v1** or **v2c**.

Click **Apply** to save the settings.

5.4.11 Advanced – Routing

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



STATIC ROUTE

Static Route.

Static Route

DEFAULT GATEWAY

Default Gateway.

Default Gateway

RIP SETTINGS

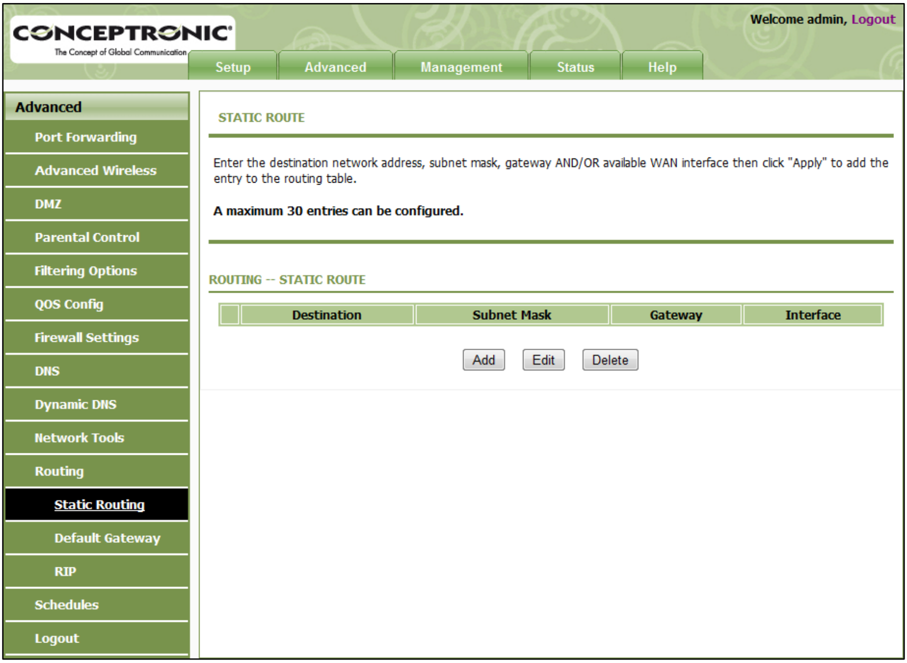
RIP Settings.

RIP Settings

This page contains the following function items: static route, default gateway, and RIP settings.

5.4.11.1 Advanced – Routing – Static Routing

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



STATIC ROUTE

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

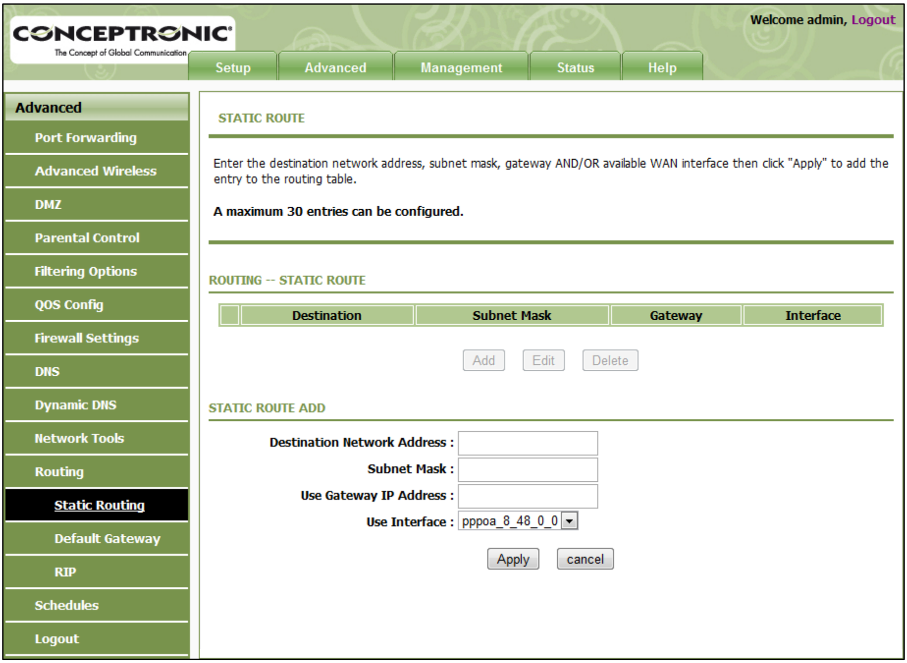
A maximum 30 entries can be configured.

ROUTING -- STATIC ROUTE

	Destination	Subnet Mask	Gateway	Interface

This page displays the information of existing static routes.

Click **Add** and the page as shown in the following figure appears:



STATIC ROUTE

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

A maximum 30 entries can be configured.

ROUTING -- STATIC ROUTE

	Destination	Subnet Mask	Gateway	Interface

STATIC ROUTE ADD

Destination Network Address :

Subnet Mask :

Use Gateway IP Address :

Use Interface : pppoa_8_48_0_0

The following table describes the parameters in this page.

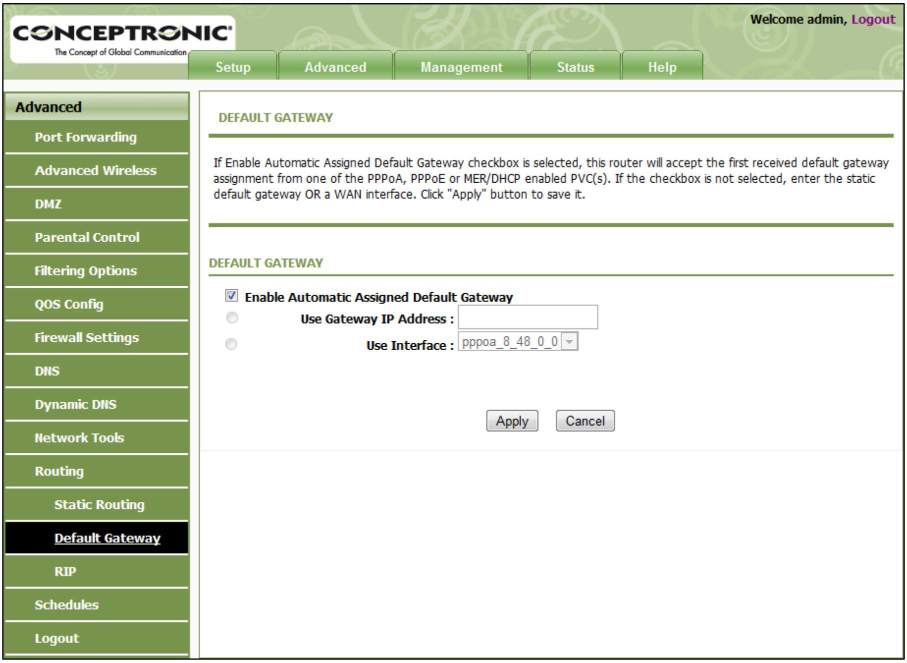
Field	Description
Destination Network Address	The destination IP address of the device.
Subnet Mask	The subnet mask of the destination IP address.
Use Gateway IP Address	The gateway IP address of the device.
Use Interface	Select the interface of the static routing used by the device from the drop-down list.

Note: You can enter the gateway IP address of the device in the Use Gateway IP Address field or set the User Interface, but cannot apply the two settings at the same time.

Click **Apply** to save the settings.

5.4.11.2 Advanced – Routing – Default Gateway

Choose **Advanced** > **Routing** and click **Default Gateway**. The page as shown in the following figure appears:



DEFAULT GATEWAY

If Enable Automatic Assigned Default Gateway checkbox is selected, this router will accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s). If the checkbox is not selected, enter the static default gateway OR a WAN interface. Click "Apply" button to save it.

DEFAULT GATEWAY

☑ Enable Automatic Assigned Default Gateway

○ Use Gateway IP Address :

○ Use Interface : pppoa_8_48_0_0

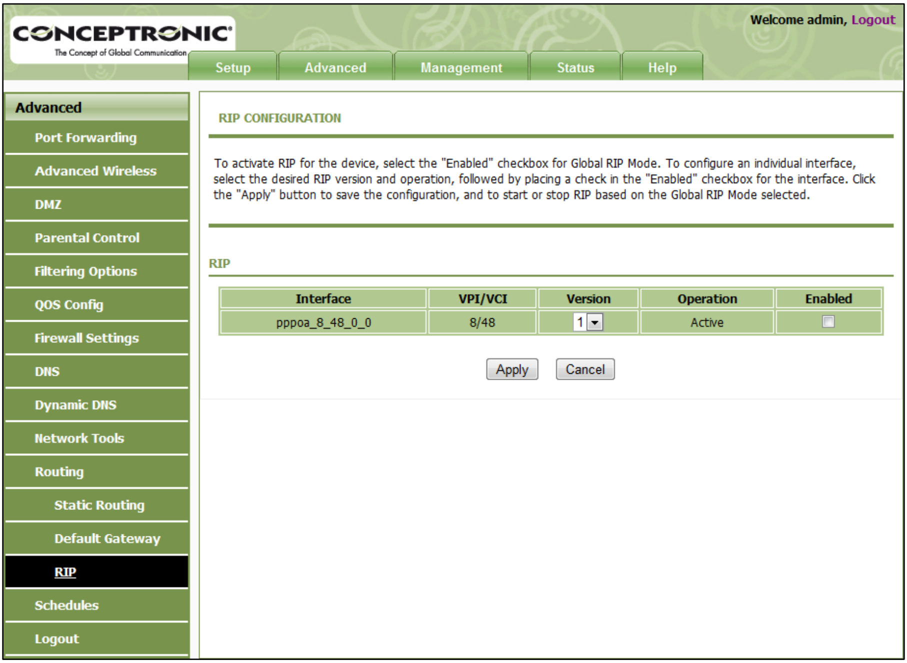
Apply Cancel

In this page, you can select **Enable Automatic Assigned Default Gateway**, or enter the information in the **Use Gateway IP Address** and **Use Interface** fields.

Click **Apply** to save the settings.

5.4.11.3 Advanced – Routing – RIP

Choose **Advanced** > **Routing** and click **RIP**. The page as shown in the following figure appears:



RIP CONFIGURATION

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

RIP

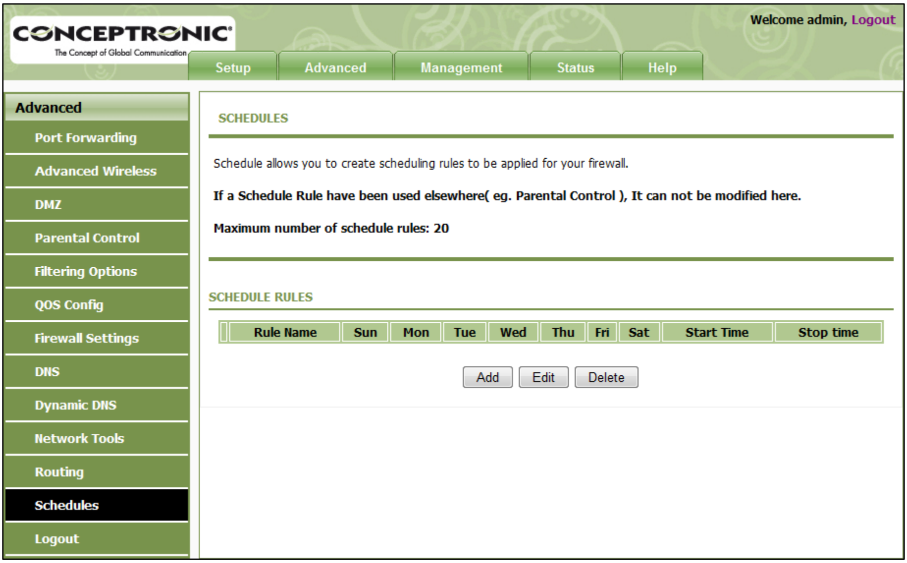
Interface	VPI/VCI	Version	Operation	Enabled
pppoa_8_48_0_0	8/48	1	Active	□

In this page, you can view the interfaces on your device that use RIP and the version of the protocol used. If you enable RIP, the device communicates with other devices using the routing information protocol (RIP).

Click **Apply** to save the settings.

5.4.12 Advanced – Schedules

Choose **Advanced** > **Schedules**. The page as shown in the following figure appears:



SCHEDULES

Schedule allows you to create scheduling rules to be applied for your firewall.

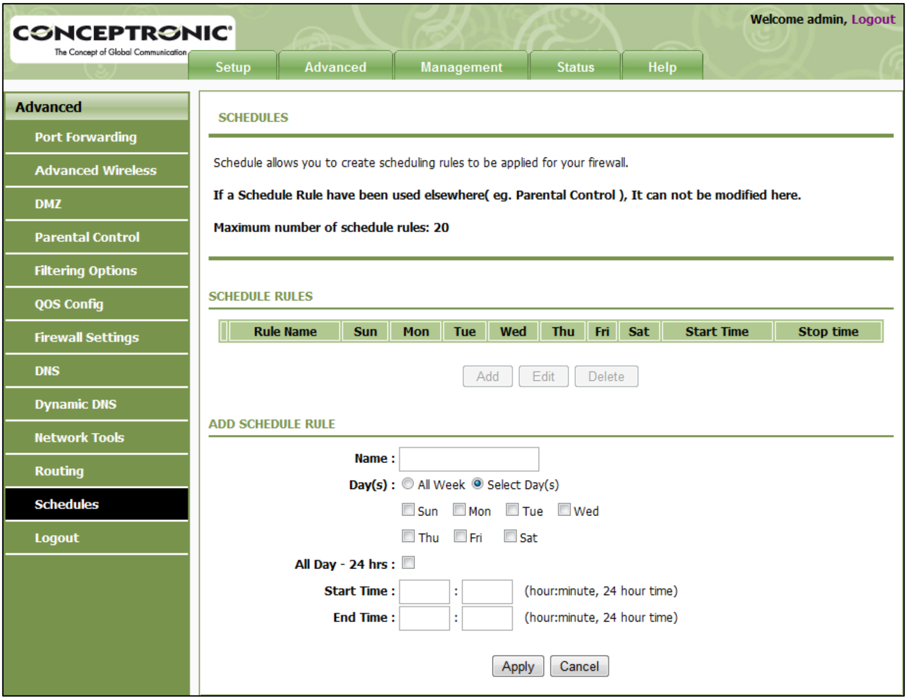
If a Schedule Rule have been used elsewhere(eg. Parental Control), It can not be modified here.

Maximum number of schedule rules: 20

SCHEDULE RULES

	Rule Name	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Start Time	Stop time

Click **Add** to add a schedule rule. The page as shown in the following figure appears:



SCHEDULES

Schedule allows you to create scheduling rules to be applied for your firewall.

If a Schedule Rule have been used elsewhere(eg. Parental Control), It can not be modified here.

Maximum number of schedule rules: 20

SCHEDULE RULES

	Rule Name	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Start Time	Stop time

ADD SCHEDULE RULE

Name :

Day(s) : ○ All Week ● Select Day(s)

□ Sun □ Mon □ Tue □ Wed

□ Thu □ Fri □ Sat

All Day - 24 hrs : □

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

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

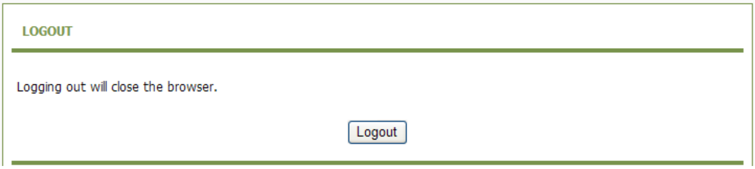
The following table describes the parameters in this page.

Field	Description
Name	Set the name of the schedule.
Day(s)	You can select one, more, or all of the seven days in a week.
All Day – 24 hrs	If you select the check box, the rule applies throughout the 24 hours of the day.
Start Time	Set the start time of the firewall.
End Time	Set the end time of the firewall.

Click **Apply** to save the settings.

5.4.13 Advanced – Logout

Choose **Advanced** > **Logout**. The page as shown in the following figure appears:



LOGOUT

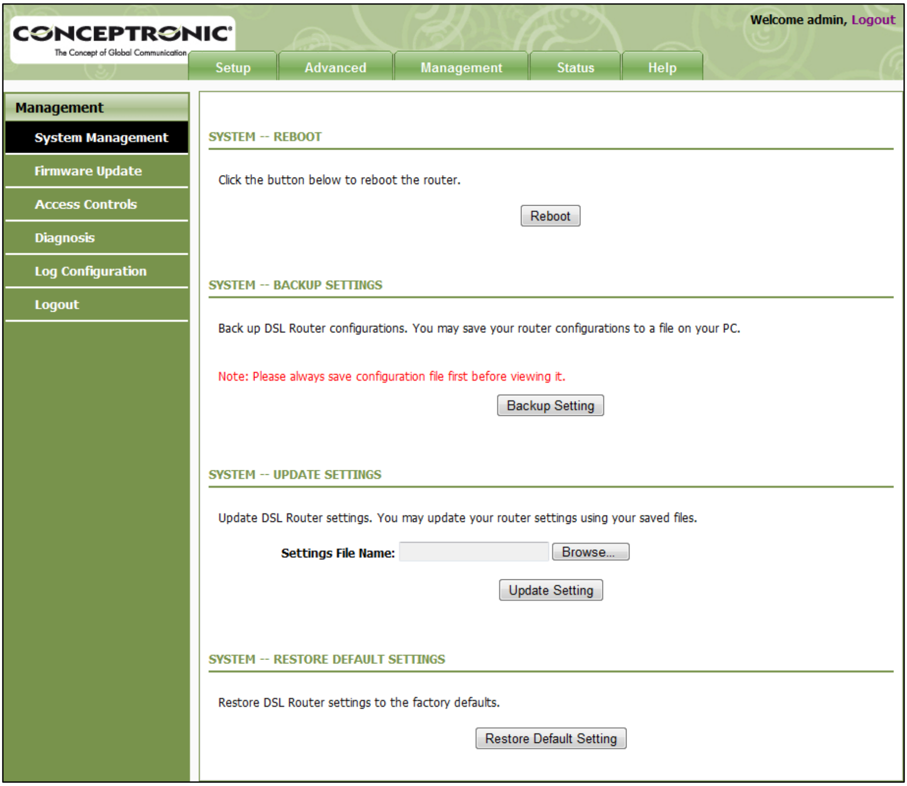
Logging out will close the browser.

Click **Logout** to log out of the configuration page.

5.5 Management

5.5.1 Management – System Management

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



SYSTEM -- REBOOT

Click the button below to reboot the router.

SYSTEM -- BACKUP SETTINGS

Back up DSL Router configurations. You may save your router configurations to a file on your PC.

Note: Please always save configuration file first before viewing it.

SYSTEM -- UPDATE SETTINGS

Update DSL Router settings. You may update your router settings using your saved files.

Settings File Name:

SYSTEM -- RESTORE DEFAULT SETTINGS

Restore DSL Router settings to the factory defaults.

In this page, you can restart the device, back up the current settings to a file, update the backup file, and restore the factory default settings.

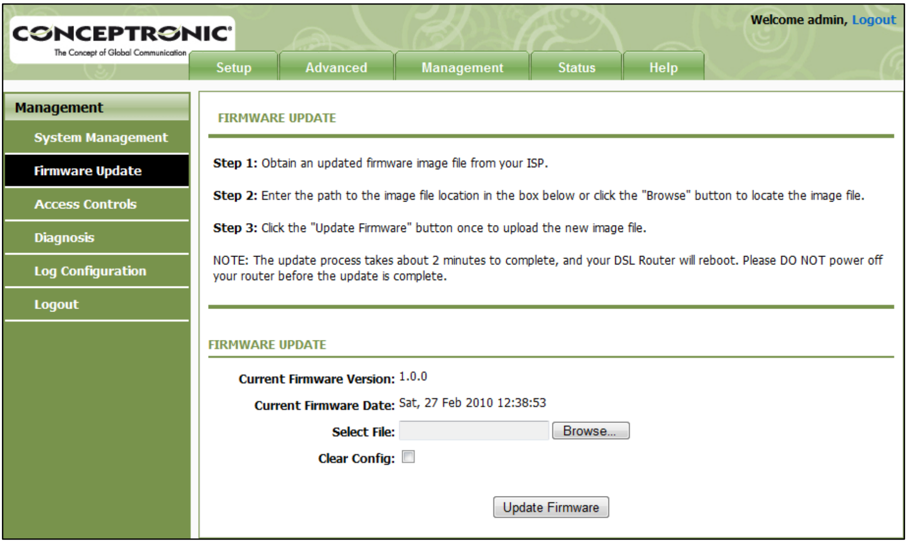
The following table describes the buttons in this page.

Button	Description
Reboot	Restart the device.
Backup Setting	Specify the path to back up the current configuration in a configuration file on your computer. You can rename the configuration file.
Update Setting	Click **Browse…** to select the configuration file of device and click **Update Setting** to update the configuration of the device.
Restore Default Setting	Reset the device to default settings.

Caution: **Do not turn off your device or press the Reset button when the procedure is in progress.**

5.5.2 Management – Firmware Update

Choose **Management** > **Firmware Update**. The page as shown in the following figure appears:



FIRMWARE UPDATE

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

Step 2: Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.

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

NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot. Please DO NOT power off your router before the update is complete.

FIRMWARE UPDATE

Current Firmware Version: 1.0.0

Current Firmware Date: Sat, 27 Feb 2010 12:38:53

Select File:

Clear Config: □

In this page, you can upgrade the firmware of the device. To update the firmware, do as follows:

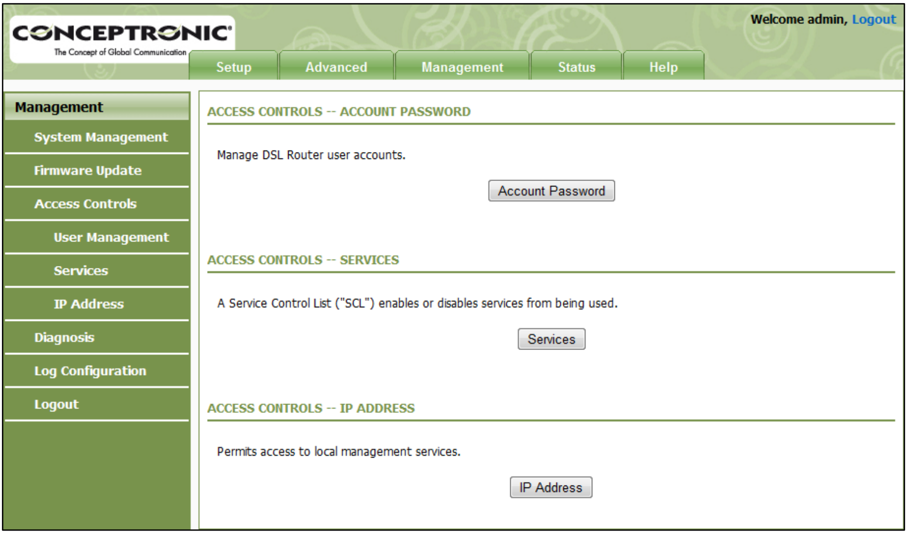
Step 1 Click **Browse…**to select the file.
Step 2 Click **Update Firmware** to update the configuration file.

The device loads the file and reboots automatically.

Caution: **Do not turn off your device or press the Reset button when the procedure is in progress**

5.5.3 Management – Access Controls

Choose **Management** > **Access Controls**. The **ACCESS CONTROLS** page as shown in the following figure appears:



ACCESS CONTROLS -- ACCOUNT PASSWORD

Manage DSL Router user accounts.

ACCESS CONTROLS -- SERVICES

A Service Control List ("SCL") enables or disables services from being used.

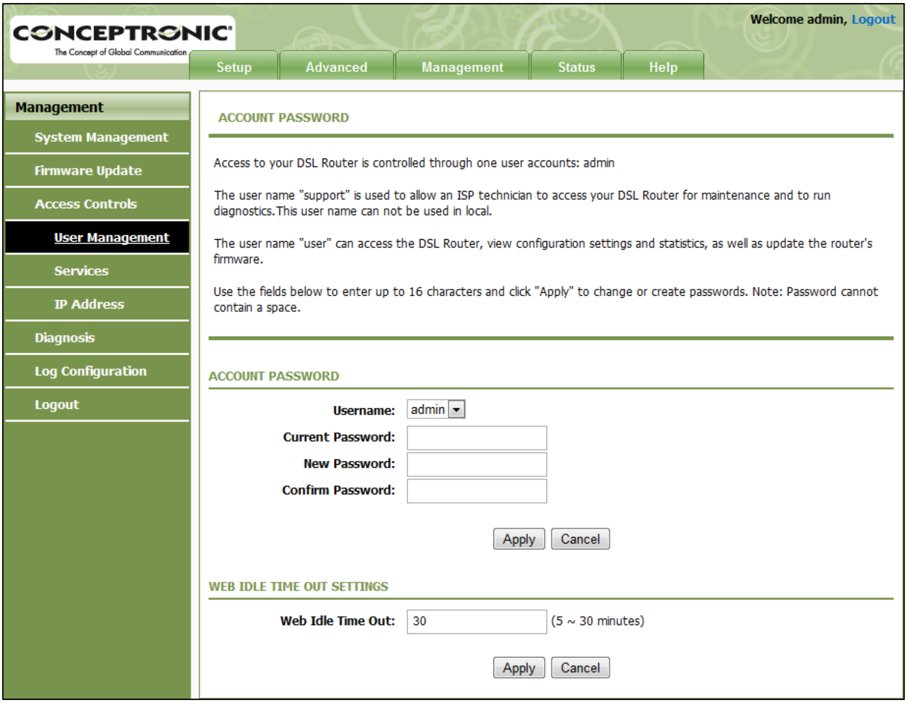
ACCESS CONTROLS -- IP ADDRESS

Permits access to local management services.

This page contains **Account Password**, **Services**, and **IP Address**.

5.5.3.1 Management – Access Controls – User Management

In the **ACCESS CONTROLS** page, click **Account Password**. The page as shown in the following figure appears:



ACCOUNT PASSWORD

Access to your DSL Router is controlled through one user accounts: admin

The user name "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics.This user name can not be used in local.

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

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

ACCOUNT PASSWORD

Username: admin
Current Password:
New Password:
Confirm Password:

Apply Cancel

WEB IDLE TIME OUT SETTINGS

Web Idle Time Out: 30 (5 ~ 30 minutes)

Apply Cancel

In this page, you can change the password and set the time for automatic logout.
You are recommended to change the default password to ensure the security of your network. Ensure that you remember the new password or write it down and keep it in a safe location for future reference. If you forget the password, you need to reset the device to the factory default settings. In that case, all configuration settings of the device are lost.

The following table describes the parameters in this page.

ACCOUNT PASSWORD

Field	Description
Username	Select a user name from the drop-down list to access the device. You can select **admin**.
Current Password	Enter the password of the user.
New Password	Enter the new password.
Confirm Password	Enter the new password again for confirmation.

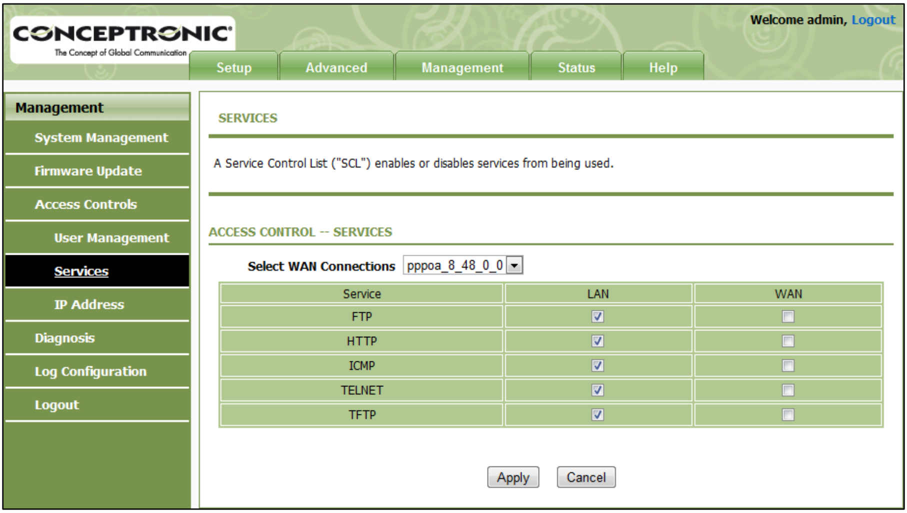
WEB IDLE TIME OUT SETTINGS

Field	Description
Web Idle Time Out	Set the time after which the system automatically exits the configuration page. Its value range is 5—30 minutes.

Click **Apply** to apply the settings.

5.5.3.2 Management – Access Controls – Services

In the **ACCESS CONTROLS** page, click **Services**. The page as shown in the following figure appears:



SERVICES

A Service Control List ("SCL") enables or disables services from being used.

ACCESS CONTROL -- SERVICES

Select WAN Connections pppoa_8_48_0_0

Service	LAN	WAN
FTP	☑	□
HTTP	☑	□
ICMP	☑	□
TELNET	☑	□
TFTP	☑	□

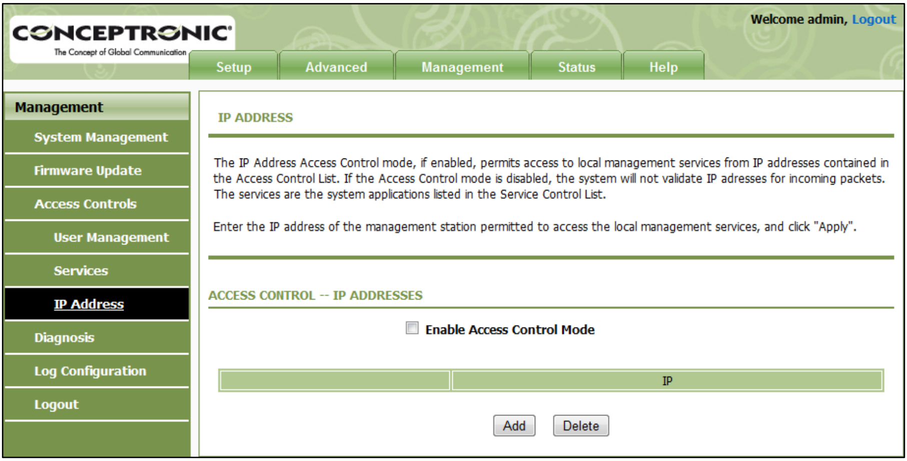
In this page, you can enable or disable the services that are used by the remote host. For example, if telnet service is enabled at port 23, the remote host can access the device by telnet through port 23.

Select the management services that you want to enable or disable at the LAN or WAN interface and click **Apply** to apply the settings.

<u>Caution:</u> **If you disable the HTTP service, you cannot access the configuration page of the device any more.**

5.5.3.3 Management – Access Controls – IP Address

In the **ACCESS CONTROLS** page, click **IP Address**. The page as shown in the following figure appears:



IP ADDRESS

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

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

ACCESS CONTROL -- IP ADDRESSES

□ Enable Access Control Mode

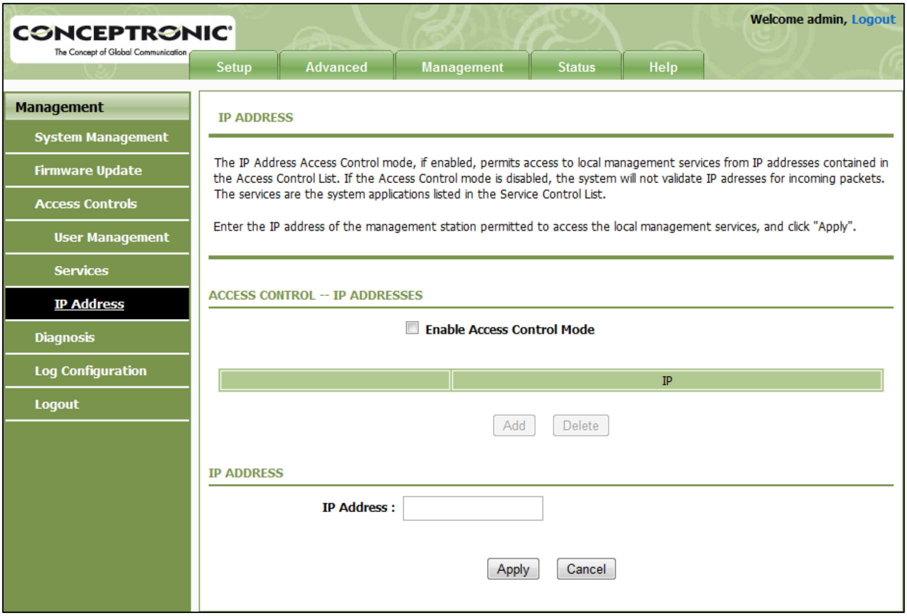
	IP

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

Select **Enable Access Control Mode** to enable ACL.

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

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



IP ADDRESS

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

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

ACCESS CONTROL -- IP ADDRESSES

□ Enable Access Control Mode

	IP

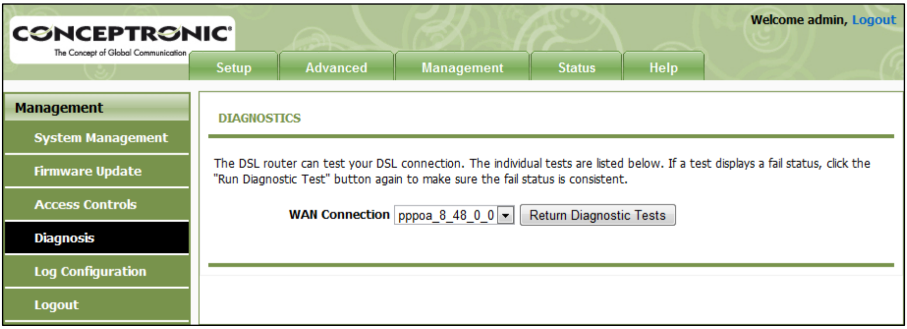
IP ADDRESS

IP Address :

Enter the IP address of the desired device in the **IP Address** field and click **Apply** to apply the settings.

5.5.4 Management – Diagnosis

Choose **Management** > **Diagnosis**. The page as shown in the following figure appears:

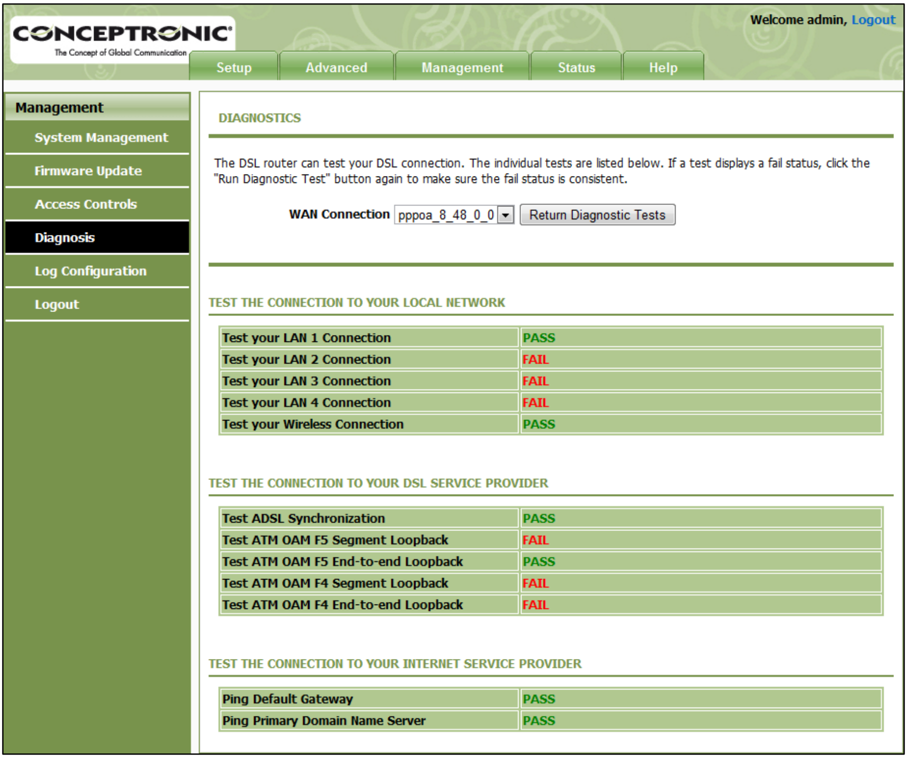


The DSL router can test your DSL connection. The individual tests are listed below. If a test displays a fail status, click the "Run Diagnostic Test" button again to make sure the fail status is consistent.

WAN Connection: pppoa_8_48_0_0

In this page, you can test the connection status of the device.

Click **Return Diagnostics Test** to run diagnostics. The page as shown in the following figure appears:



The DSL router can test your DSL connection. The individual tests are listed below. If a test displays a fail status, click the "Run Diagnostic Test" button again to make sure the fail status is consistent.

WAN Connection: pppoa_8_48_0_0

TEST THE CONNECTION TO YOUR LOCAL NETWORK

Test your LAN 1 Connection	PASS
Test your LAN 2 Connection	FAIL
Test your LAN 3 Connection	FAIL
Test your LAN 4 Connection	FAIL
Test your Wireless Connection	PASS

TEST THE CONNECTION TO YOUR DSL SERVICE PROVIDER

Test ADSL Synchronization	PASS
Test ATM OAM F5 Segment Loopback	FAIL
Test ATM OAM F5 End-to-end Loopback	PASS
Test ATM OAM F4 Segment Loopback	FAIL
Test ATM OAM F4 End-to-end Loopback	FAIL

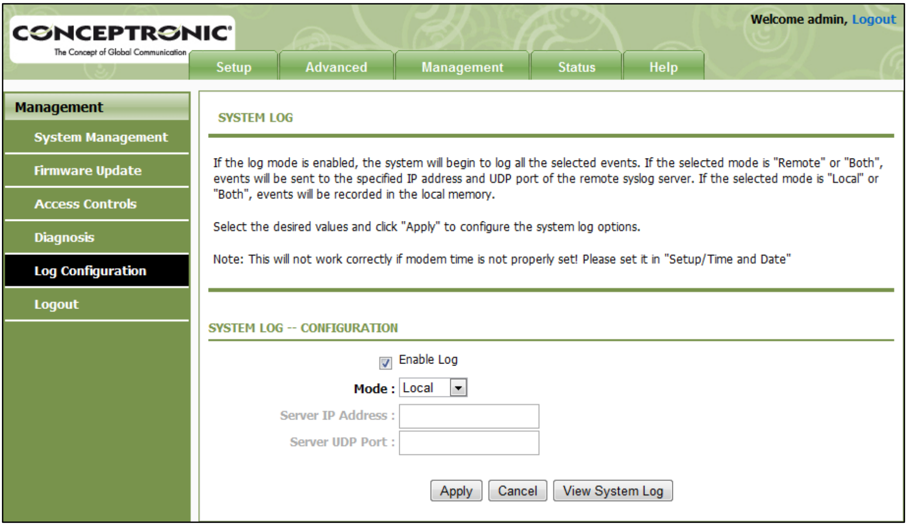
TEST THE CONNECTION TO YOUR INTERNET SERVICE PROVIDER

Ping Default Gateway	PASS
Ping Primary Domain Name Server	PASS

Note: The above diagnostics information is an example. In your situation, the results can be different.

5.5.5 Management – Log Configuration

Choose **Management** > **Log Configuration**. The **SYSTEM LOG** page as shown in the following figure appears:



SYSTEM LOG

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

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

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

SYSTEM LOG -- CONFIGURATION

☑ Enable Log

Mode : Local

Server IP Address :

Server UDP Port :

In this page, you can enable the log function. You can set **Mode** to **Local**, **Remote**, or **Both**. **Local** indicates to save the log in the local computer. **Remote** indicates to send the log to the remote log server. **Both** indicates to save the log in the local computer and the remote log server.

To log the events, do as follows:

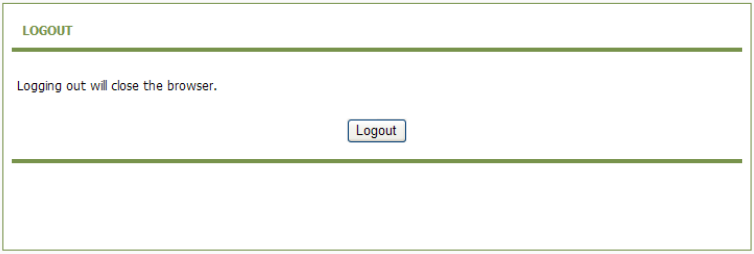
Step 1 Select **Enable Log**.
Step 2 Select a mode from the drop-down list.

If you select **Remote** or **Both**, enter the IP address and port number of the server.

Step 3 Click **Apply** to apply the settings.
Step 4 Click **View System Log** to view the detail information of the system log.

5.5.6 Management – Logout

Choose **Management** > **Logout**. The page as shown in the following figure appears:



LOGOUT

Logging out will close the browser.

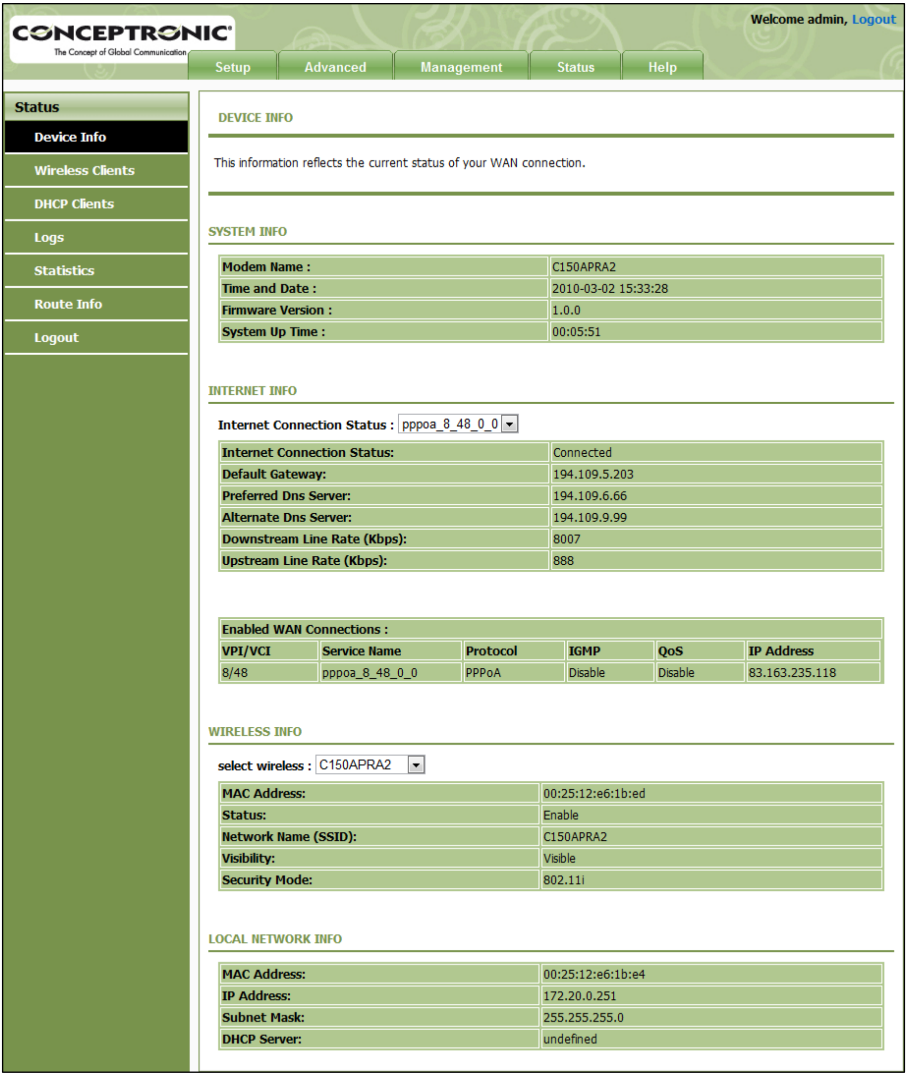
Click **Logout** to log out of the configuration page.

5.6 Status

In the **Status** page, you can view the system information and monitor the performance of the device.

5.6.1 Status – Device Info

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



DEVICE INFO

This information reflects the current status of your WAN connection.

SYSTEM INFO

Modem Name :	C150APRA2
Time and Date :	2010-03-02 15:33:28
Firmware Version :	1.0.0
System Up Time :	00:05:51

INTERNET INFO

Internet Connection Status : pppoa_8_48_0_0

Internet Connection Status:	Connected
Default Gateway:	194.109.5.203
Preferred Dns Server:	194.109.6.66
Alternate Dns Server:	194.109.9.99
Downstream Line Rate (Kbps):	8007
Upstream Line Rate (Kbps):	888

Enabled WAN Connections :

VPI/VCI	Service Name	Protocol	IGMP	QoS	IP Address
8/48	pppoa_8_48_0_0	PPPoA	Disable	Disable	83.163.235.118

WIRELESS INFO

select wireless : C150APRA2

MAC Address:	00:25:12:e6:1b:ed
Status:	Enable
Network Name (SSID):	C150APRA2
Visibility:	Visible
Security Mode:	802.11i

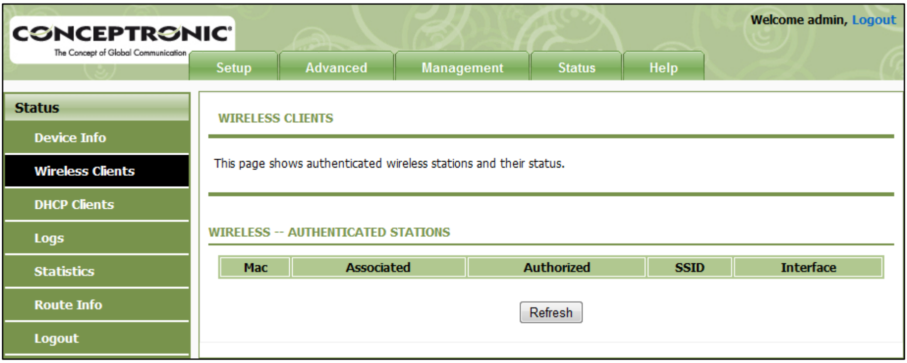
LOCAL NETWORK INFO

MAC Address:	00:25:12:e6:1b:e4
IP Address:	172.20.0.251
Subnet Mask:	255.255.255.0
DHCP Server:	undefined

The page displays the summary of the device status, including the system information, WAN connection information, wireless information, and local network information.

5.6.2 Status – Wireless Clients

Choose **Status** > **Wireless Clients**. The page as shown in the following page appears:



WIRELESS CLIENTS

This page shows authenticated wireless stations and their status.

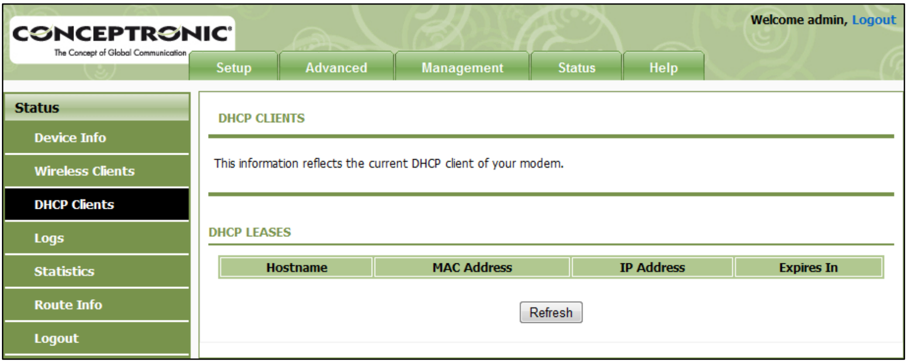
WIRELESS -- AUTHENTICATED STATIONS

Mac	Associated	Authorized	SSID	Interface

The page displays authenticated wireless stations and their statuses.

5.6.3 Status – DHCP Clients

Choose **Status** > **DHCP Clients**. The page as shown in the following page appears:



DHCP CLIENTS

This information reflects the current DHCP client of your modem.

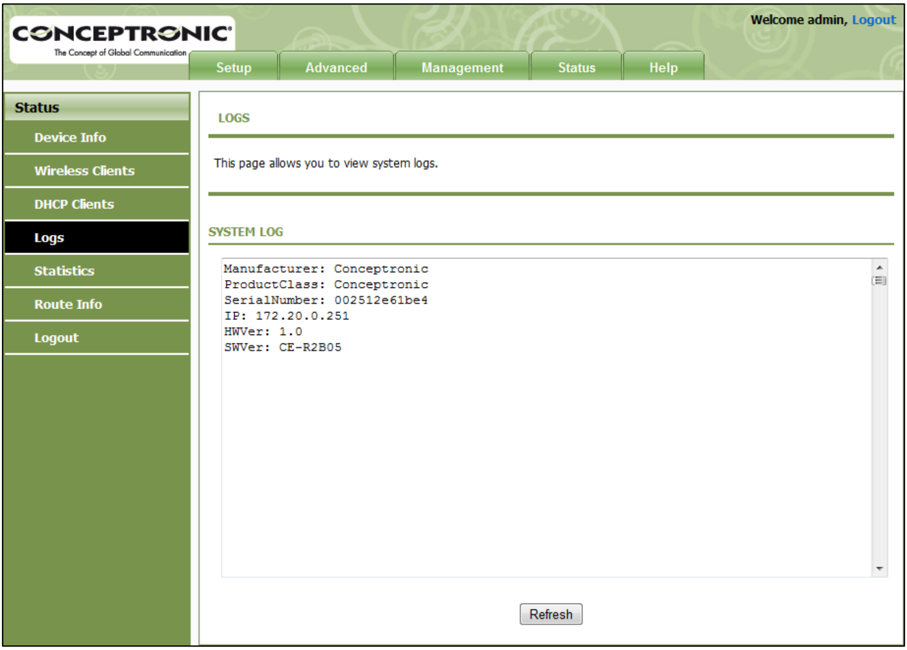
DHCP LEASES

Hostname	MAC Address	IP Address	Expires In

This page displays all client devices that obtain IP addresses from the device. You can view the host name, IP address, MAC address, and expiration time of the IP address.

5.6.4 Status – Logs

Choose **Status** > **Logs**. The page as shown in the following figure appears:



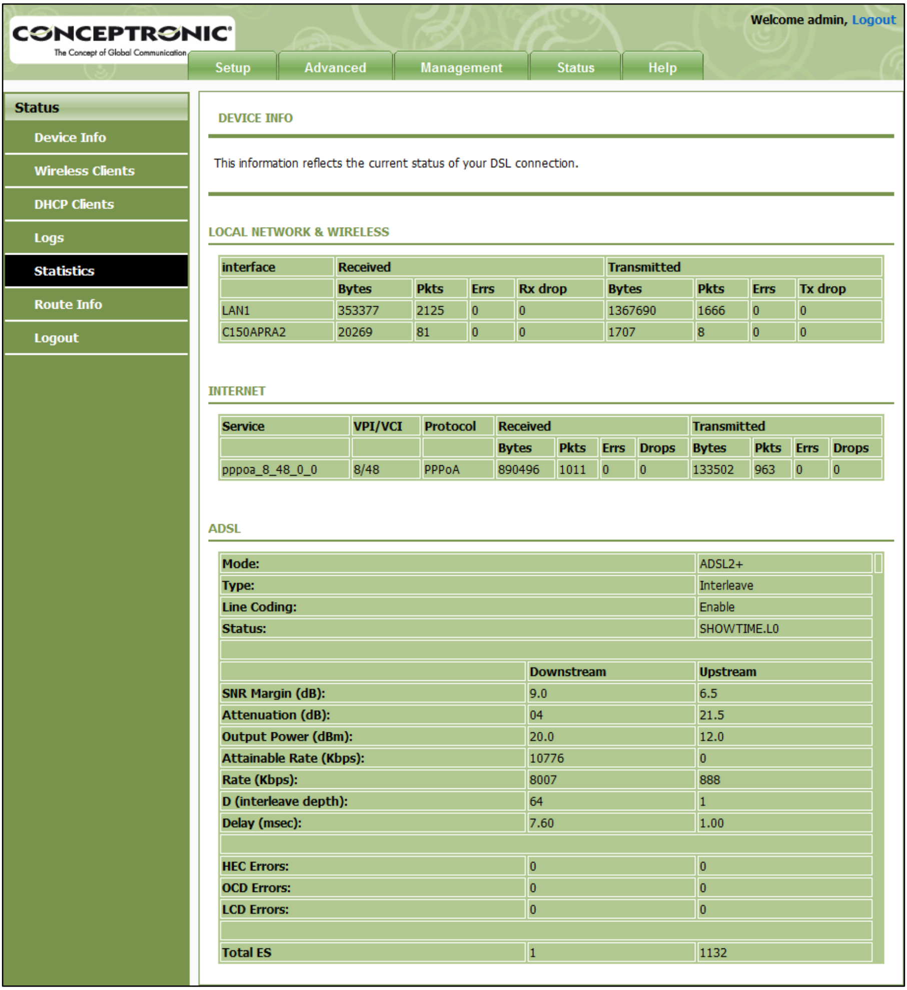
This page allows you to view system logs.

```
Manufacturer: Conceptronic
ProductClass: Conceptronic
SerialNumber: 002512e61be4
IP: 172.20.0.251
HWVer: 1.0
SWVer: CE-R2B05
```

This page displays the system log. Click **Refresh** to refresh the system log shown in the box.

5.6.5 Status – Statistics

Choose **Status** > **Statistics**. The page as shown in the following figure appears:



DEVICE INFO

This information reflects the current status of your DSL connection.

LOCAL NETWORK & WIRELESS

interface	Received				Transmitted			
	Bytes	Pkts	Errs	Rx drop	Bytes	Pkts	Errs	Tx drop
LAN1	353377	2125	0	0	1367690	1666	0	0
C150APRA2	20269	81	0	0	1707	8	0	0

INTERNET

Service	VPI/VCI	Protocol	Received				Transmitted			
			Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
pppoa_8_48_0_0	8/48	PPPoA	890496	1011	0	0	133502	963	0	0

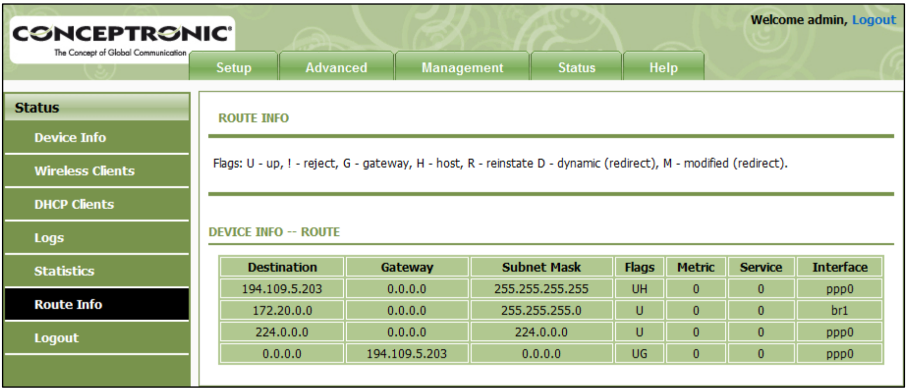
ADSL

Mode:		ADSL2+
Type:		Interleave
Line Coding:		Enable
Status:		SHOWTIME.L0
	Downstream	Upstream
SNR Margin (dB):	9.0	6.5
Attenuation (dB):	04	21.5
Output Power (dBm):	20.0	12.0
Attainable Rate (Kbps):	10776	0
Rate (Kbps):	8007	888
D (interleave depth):	64	1
Delay (msec):	7.60	1.00
HEC Errors:	0	0
OCD Errors:	0	0
LCD Errors:	0	0
Total ES	1	1132

This page displays the statistics information of the network and data transmission. The information helps technicians to identify whether the device is functioning properly. The information does not affect the functions of the device.

5.6.6 Status – Route Info

Choose **Status** > **Route Info**. The page as shown in the following figure appears:



ROUTE INFO

Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate D - dynamic (redirect), M - modified (redirect).

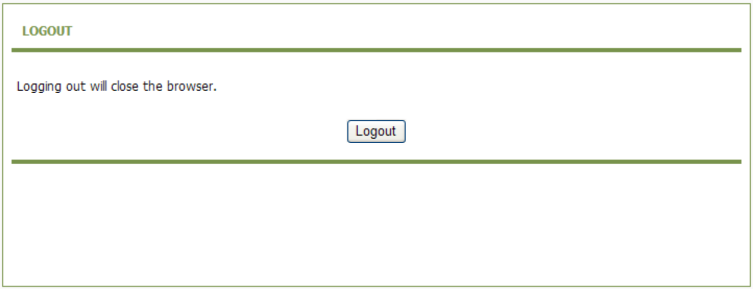
DEVICE INFO -- ROUTE

Destination	Gateway	Subnet Mask	Flags	Metric	Service	Interface
194.109.5.203	0.0.0.0	255.255.255.255	UH	0	0	ppp0
172.20.0.0	0.0.0.0	255.255.255.0	U	0	0	br1
224.0.0.0	0.0.0.0	224.0.0.0	U	0	0	ppp0
0.0.0.0	194.109.5.203	0.0.0.0	UG	0	0	ppp0

The table displays destination routes commonly accessed by the network.

5.6.7 Status – Logout

Choose **Staus** > **Logout**. The page as shown in the following figure appears:



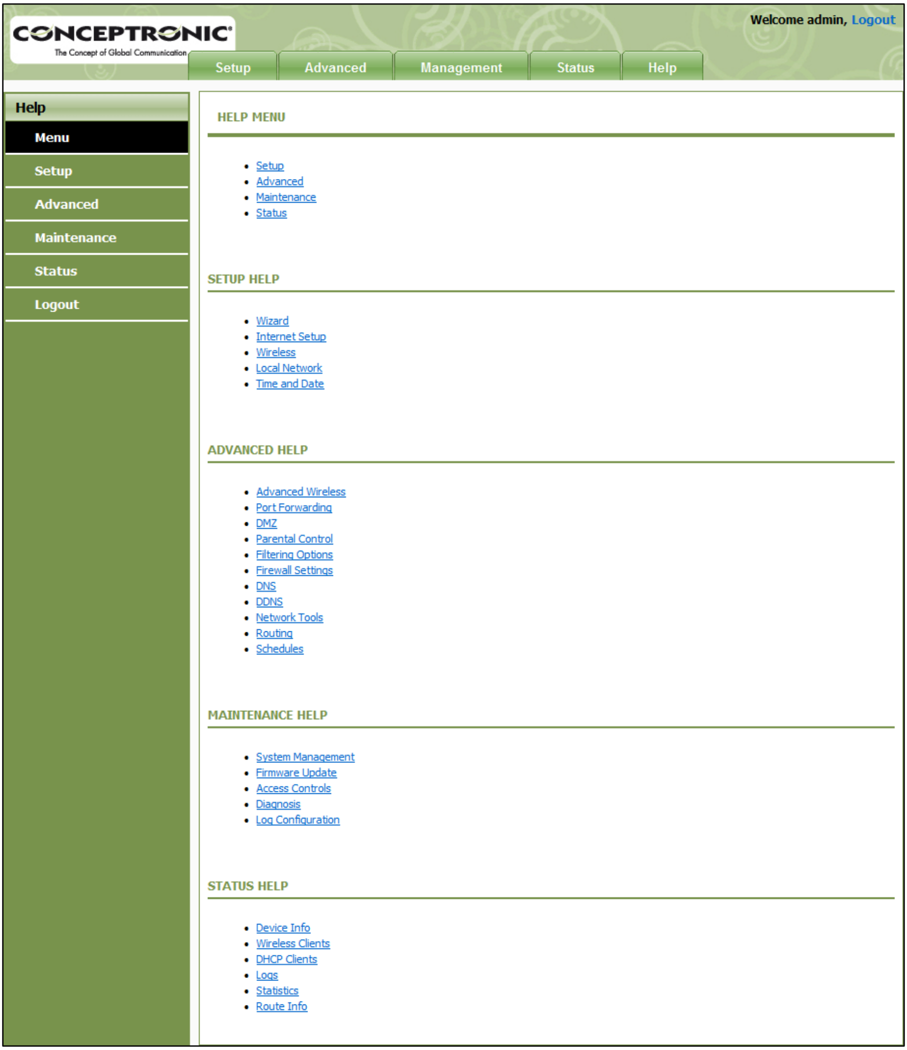
LOGOUT

Logging out will close the browser.

Click **Logout** to log out of the configuration page.

5.7 Help

The Help menu will help you with information about all the items in the configuration of the device.



HELP MENU

- Setup
- Advanced
- Maintenance
- Status

SETUP HELP

- Wizard
- Internet Setup
- Wireless
- Local Network
- Time and Date

ADVANCED HELP

- Advanced Wireless
- Port Forwarding
- DMZ
- Parental Control
- Filtering Options
- Firewall Settings
- DNS
- DDNS
- Network Tools
- Routing
- Schedules

MAINTENANCE HELP

- System Management
- Firmware Update
- Access Controls
- Diagnosis
- Log Configuration

STATUS HELP

- Device Info
- Wireless Clients
- DHCP Clients
- Logs
- Statistics
- Route Info

6. Frequently Asked Questions

Below you will find some frequently asked questions for the device.

Question	Answer
Why are all the indicators off?	● Check the connection between the power adapter and the power socket. ● Check whether the power switch is turned on.
Why is the LAN indicator not on?	Check the following: ● The connection between the device and the PC, the hub, or the switch. ● The running status of the computer, hub, or switch. ● The cables that connects the device and other devices: – If the device connects to a computer, use the cross over cable. – If the device connects to a hub or a switch, use the straight-through cable.
Why is the DSL indicator not on?	Check the connection between the **DSL** interface of the device and the socket.
Why does the Internet access fail when the DSL indicator is on?	Ensure that the following information is entered correctly: ● VPI and VCI ● User name and password
Why does the web configuration page of the device fail to be accessed?	Choose **Start** > **Run** from the desktop. Enter **Ping 192.168.0.1** (the default IP address of the device) in the DOS window. If the web configuration page still cannot be accessed, check the following configuration: ● The type of the network cable ● The connection between the device and the computer ● The TCP/IP properties of the network card of the computer
How to restore the default configuration after incorrect configuration?	Keep the device powered on and press the **Reset** button for 5 seconds. Then, the device automatically reboots and is restored to the factory default configuration. The default configuration of the device is as follows: ● IP address: 192.168.0.1 ● Subnet mask: 255.255.255.0. ● Password of user **admin**: **admin**

Enjoy the use of your
Conceptronic C150APRA2!

7. License Information

This Conceptronic product C150APRA2 includes copyrighted third-party software licensed under the terms of the GNU General Public License. Please see The GNU General Public License for the exact terms and conditions of this license.

Availability of source code

Conceptronic. has eposed the full source code of the GPL licensed software, including any scripts to control compilation and installation of the object code. All future firmware updates will also be accompanied with their respective source code. For more information on how you can obtain our open source code, please visit our web site.

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of
it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License.Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS