



User's Guide

HGW-2501GN-R2

Edition 1, 8/2014



IMPORTANT!



READ CAREFULLY BEFORE USE.



KEEP THIS GUIDE FOR FUTURE REFERENCE.

Graphics in this book may differ slightly from the product due to differences in operating systems, operating system versions, or if you installed updated firmware/software for your device. Every effort has been made to ensure that the information in this manual is accurate.

Contents

8	Chapter 1: Introducción
8	Overview
9	Hardware Connection
10	LEDs (Lights)
12	Chapter 2: The Installation Wizard
12	Overview
12	Access the Router
14	Changing the Password
15	Tu Router
16	Configuración Básica
16	IPTV Configuration
19	VoIP Configuration
20	Configuración Avanzada
22	The Web Configurator Layout
22	Title Bar
23	Main Window
24	Chapter 3: The Client Wizard
24	Access the Router
25	Configuración Básica
25	Wireless Configuration
27	IPv4 NAT Port Forwarding Configuration
28	IPv6 Firewall Configuration
30	Connection Line Configuration
31	LAN Configuration
33	Profile Configuration
34	Firmware Upgrade
36	Chapter 4: Quick Start
36	Overview
36	Quick Start Setup
38	Chapter 5: Connection Status and System Info
38	The Connection Status Screen
39	The System Info Screen

40	Chapter 6: WAN
40	The WAN Screen
41	Edit Ethernet Connection
44	Chapter 7: Wireless 2.4GHz
44	Wireless General Screen
46	No Security
47	Basic (WEP Encryption)
48	More Secure (WPA(2))
49	More Secure (WPA(2)-PSK)
50	More AP Screen
51	Edit More AP
52	MAC Authentication Screen
53	The WPS Screen
55	The WDS Screen
56	The WMM Screen
57	Scheduling Screen
58	Add or Edit Schedule
59	Advanced Screen
60	Chapter 8: LAN
60	The LAN Setup Screen
62	The Static DHCP Screen
63	The IP Alias Screen
64	The UPnP Screen
65	The IPv6 LAN Setup Screen
69	Chapter 9: Static Route
69	Configuring Static Route
70	Add/Edit Static Route
70	IPv6 Static Route
71	Add/Edit IPv6 Static Route
72	The DNS Route Screen
72	Add/Edit DNS Route
73	The Current Route Screen
74	Chapter 10: DNS Route
74	Overview
74	The DNS Route Screen
75	Add/Edit DNS Route
76	Chapter 11: Quality of Service (QoS)
76	The QoS General Screen

77	The Queue Setup Screen
78	Edit a QoS Queue
78	The Class Setup Screen
80	Add/Edit QoS Class
84	The QoS Monitor Screen
85	Chapter 12: Network Address Translation (NAT)
85	The General Screen
85	The Port Forwarding Screen
86	The Port Forwarding Screen
87	The Port Forwarding Add/Edit Screen
88	The Address Mapping Screen
89	The Address Mapping Rule Edit Screen
90	The DMZ Screen
90	The ALG Screen
92	Chapter 13: Dynamic DNS
92	The Dynamic DNS Screen
94	Chapter 14: Filter
94	The IP/MAC Filter Screen
96	The IPv6/MAC Filter Screen
98	Chapter 15: Firewall
98	TFirewall General Screen
99	Add/Edit Interface Default Policy Screen
99	Rules Screen
101	Rules Edit Screen
102	DoS Screen
103	The DoS Advanced Screen
104	Chapter 16: Parental Control
104	The Parental Control Screen
106	Add/Edit a Parental Control Rule
108	Chapter 17: Certificates
108	Local Certificates
109	Trusted CA
110	Trusted CA Import
111	View Certificate
112	Chapter 18: VoIP
112	The SIP Account Screen

113	Edit SIP Account
116	The SIP Service Provider Screen
117	Edit SIP Service Provider
122	Phone Screen
123	Call Rule Screen
124	Chapter 19: System Monitor
124	The Log Screen
125	The WAN Traffic Status Screen
126	The LAN Traffic Status Screen
127	The NAT Traffic Status Screen
128	The VoIP Status Screen
130	Chapter 20: User Account
130	Overview
130	The User Account Screen
131	Chapter 21: TR-069 Client
131	The TR-069 Screen
133	Chapter 22: System
133	The System Screen
134	Chapter 23: Time Setting
134	The Time Setting Screen
136	Chapter 24: Log Setting
136	The Log Setting Screen
139	Chapter 25: Firmware Upgrade
139	The Firmware Upgrade Screen
141	Chapter 26: Backup/Restore
141	The Backup/Restore Screen
143	The Reboot Screen
144	Chapter 27: Remote Management
144	The General Screen
144	The WWW Screen
146	Telnet Screen
146	FTP Screen
148	SNMP Screen
149	DNS Screen
150	ICMP Screen

151	SSH Screen
153	Chapter 28: Diagnostic
153	The Diagnostic Screen
154	Chapter 29: Troubleshooting
154	Overview
154	Power, Hardware Connections, and LEDs
155	Router Access and Login
156	Internet Access
157	Wireless Internet Access
158	Phone Calls and VoIP
159	UPnP
160	Appendix A: Safety Warnings

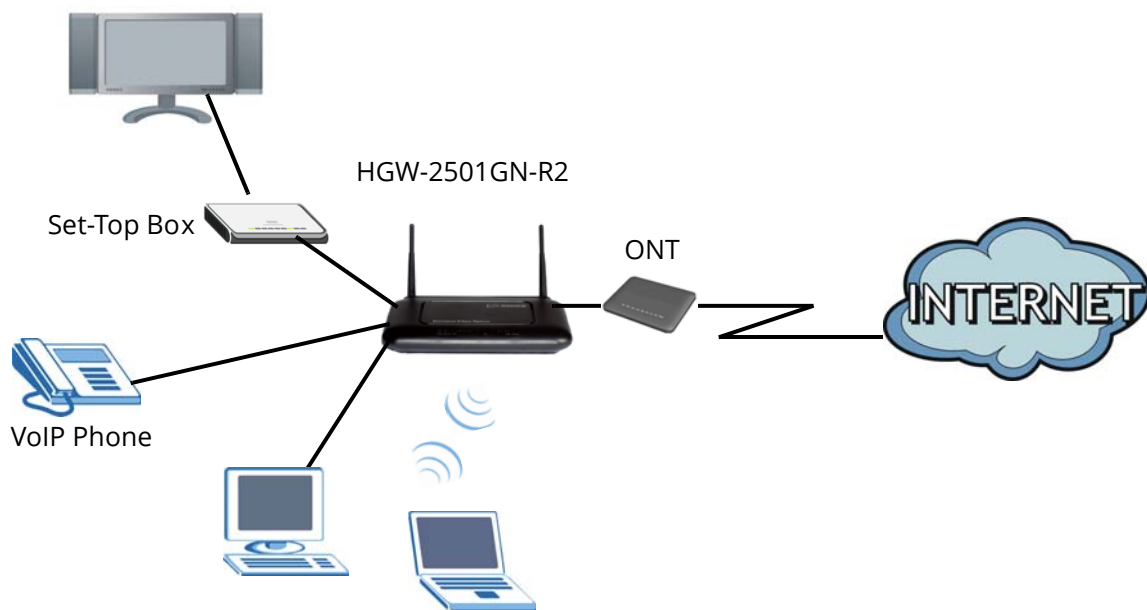
1.1 Overview

The HGW-2501GN-R2 combines a router which combines high-speed Internet access, a built-in switch, a firewall and high-speed wireless networking capability. It has one phone port for making calls over the Internet (Voice over IP or VoIP). In addition, it supports IPTV service if it is available from your service provider.

The following figure shows an application example of the Router:

The Router is connected to a GPON ONT and provides IPTV, VoIP services as well as wired and wireless Internet access to home devices on the LAN.

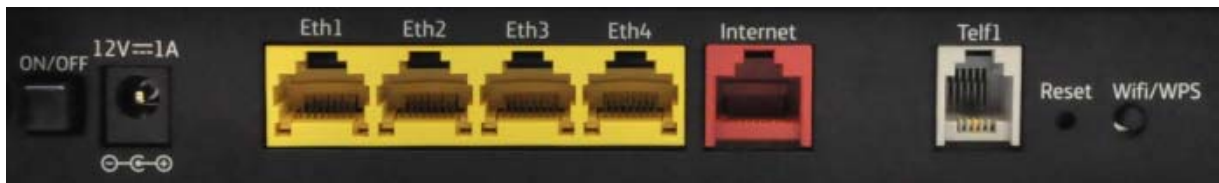
Figure 1 Application Example



1.2 Hardware Connection

Make sure to use the proper cables and power adapter to connect the Router.

Figure 2 The Rear Panel



La descripción de los conectores y botones anteriormente visualizados se muestra en la siguiente tabla:

Table 1 The Rear Panel

CONECTOR	DESCRIPTION
ON/OFF	Use this button to turn the Router on or off.
12V-1A	Connect the provided power adapter to the 12V-1A power connector. Attach the power adapter to a proper power source.
Eth 1-4	Use an Ethernet cable to connect a computer to one of these ports for initial configuration and/or Internet access.
Internet	This is the Router's WAN interface. Use an RJ-45 cable to connect the Router to an ONT.
Telf1	Use a telephone cable to connect the Router to a VoIP phone for VoIP service.
Reset	Use this button to restore the default settings of the Router. Press this button for 10 seconds to restore default values. Press 1 second or longer to restart it. Note: If you reset the Router, you will lose all configurations that you had previously and the password will be reset to the defaults.
Wifi/WPS	Use this button to enable or disable the WiFi and WPS features on the Router. By default, WiFi is enabled on the Router. If you want to turn it off, press this button for 1 second to turn it off. To enable the WPS feature, press the button for more than 3 seconds. The WPS LED on the front panel will flash green while the Router sets up a WPS Connection with the wireless device. Note: To activate WPS, you must enable WPS in the Router and in another wireless device within two minutes of each other.

1.3 LEDs (Lights)

The following graphic displays the labels of the LEDs.

Figure 3 Front Panel LEDs

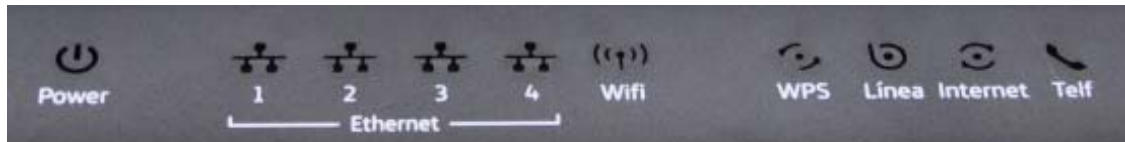


Table 2 LED Descriptions








LED	COLOR	STATUS	DESCRIPTION
Power 	Green	On	The Router is receiving power and ready for use.
	Red	On	The Router has hardware failure.
		Blinking	The Router detected an error while self-testing.
	Off	The Router is not receiving power.	
Ethernet 1-4 	Green	On	The Router has a successful Ethernet connection with a device on the LAN.
		Blinking	The Router is sending or receiving data to/from the LAN.
		Off	The Router does not have an Ethernet connection with the LAN.
Wifi 	Green	On	The wireless network is activated.
		Blinking	The Router is communicating with other wireless clients.
		Off	The wireless network is not activated.
WPS 	Green	On	The WPS is activated but there is no WPS connection.
		Blinking	The Router is setting up a WPS connection.
	Red	On	There is a problem with the WPS connection.
		Off	The WPS is not activated.
Línea 	Green	On	The Router is connected and synchronized with an ONT.
		Off	The Router is off line or not connected to an ONT.

Table 2 LED Descriptions (continued)

LED	COLOR	STATUS	DESCRIPTION
Internet 	Green	On	The Router has an IP connection but no traffic. It has a WAN IP address (either static or assigned by a DHCP server), PPP negotiation was successfully completed (if used).
		Blinking	The Router is negotiating a PPP connection.
		Fast Blinking	The Router is sending or receiving IP traffic.
	Red	On	The Router attempted to make an IP connection but failed. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed.
		Off	There is no Internet connection.
		Off	There is no Internet connection.
Telf 	Green	On	The SIP registration is successful.
		Blinking	The Router is negotiating the SIP registration.
		Fast Blinking	There is incoming/outgoing voice traffic.
	Red	On	The Router has failed to register the VoIP service. There is problem with the SIP account.
		Off	There is no VoIP service.
		Off	There is no VoIP service.

The Installation Wizard **2** Chapter

2.1 Overview

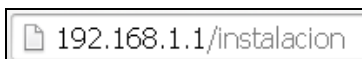
The web configurator HTML-based management interface allows easy device setup and management via Internet browser. Use Internet Explorer 6.0 and later versions, Mozilla Firefox 3 and later versions, or Safari 2.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

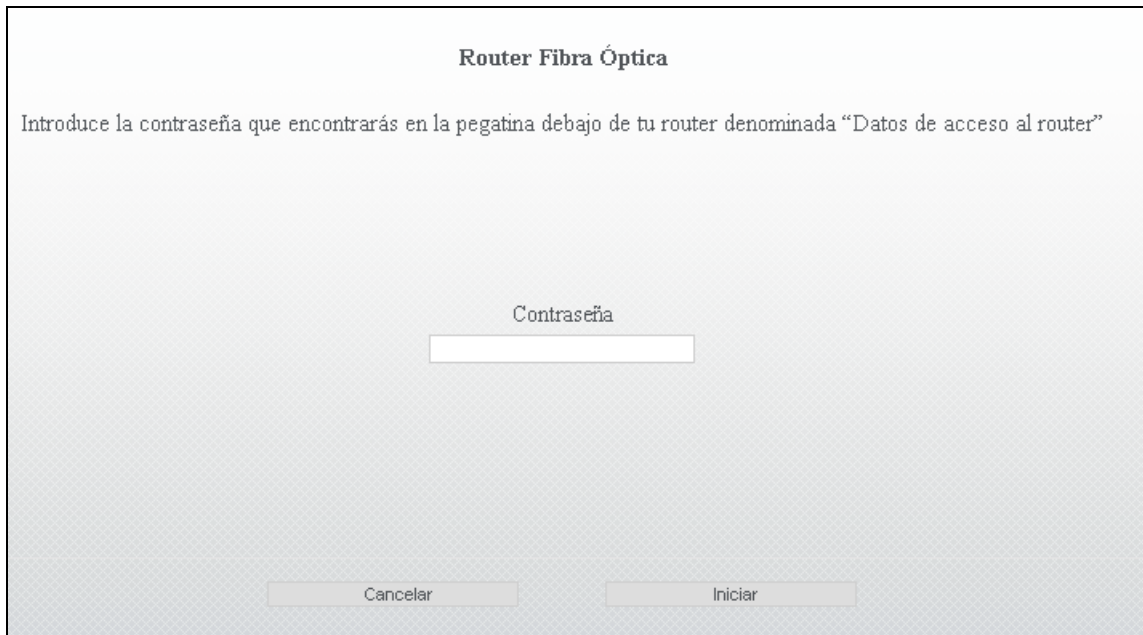
2.2 Access the Router

The **Installation Wizard** helps you to configure the services you want to use on the Router. Connect to the Web Configurator to access the **Installation Wizard** screens. Enter the IP address: <http://192.168.1.1/instalacion>.



192.168.1.1/instalacion

The login screen appears. The default password is **1234**. Enter the password. Click **Iniciar** to enter the **Installation Wizard**.



The image shows a login screen for a fiber optic router. At the top, it says "Router Fibra Óptica". Below that, it asks the user to enter the password found on a sticker on the router. There is a text input field labeled "Contraseña". At the bottom, there are two buttons: "Cancelar" and "Iniciar".

The main screen appears. Click the buttons in this screen for basic or advanced configurations of the Router.



- 1 **Español / English** - change the language.
- 2 **Cambiar contraseña** - change the configuration password (see [Section 2.3 on page 14](#)).

- 3 **Consejos** - display tips and frequently asked questions.
- 4 **Tu Router** - display basic information of the Router (see [Section 2.4 on page 15](#)).
- 5 **Configuración Básica** - select the services you want to use and configure related settings (see [Section 2.5 on page 16](#)).
- 6 **Configuración Avanzada** - access and configure settings for all the features of the Router (see [Section 2.6 on page 20](#)).

2.3 Changing the Password

- 1 Click the main screen's **Cambiar contraseña** link (1 in the figure).
- 2 Enter the Router's current password in the **Contraseña actual** field.
- 3 Enter the new password in the **Nueva contraseña** field. You can check the strength of the new password in the **Fortaleza de la contraseña** indicator.
- 4 Retype the new password in the **Repetir nueva contraseña** field and click **Aplicar** to save the setting and exit this screen.

Cambiar contraseña

Te recomendamos que para aumentar tu seguridad.

1 Contraseña actual

2 Nueva contraseña

3 Repetir nueva contraseña

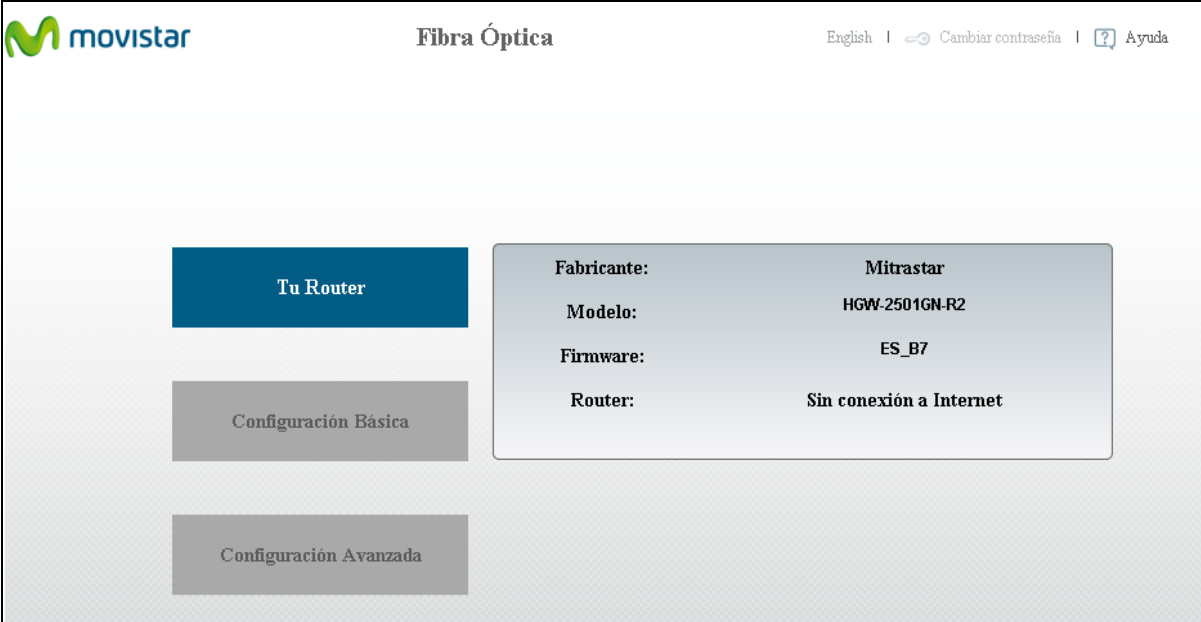
Fortaleza de la contraseña

4

Cancelar Aplicar

2.4 Tu Router

Mouse-over the **Tu Router** button to show basic information of the Router. You can see the manufacturer company name, model name, current firmware version, and whether the Router is connected to the Internet.

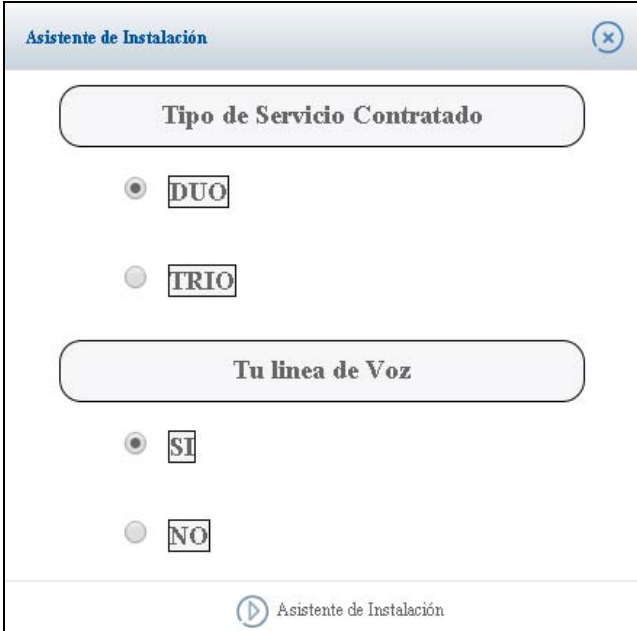


The screenshot displays the Movistar Fibra Óptica router configuration interface. At the top left is the Movistar logo, and at the top center is the text "Fibra Óptica". On the top right, there are links for "English", "Cambiar contraseña", and "Ayuda". The main content area features three buttons: "Tu Router" (highlighted in dark blue), "Configuración Básica", and "Configuración Avanzada". A tooltip is shown over the "Tu Router" button, displaying the following information:

Fabricante:	Mitrastar
Modelo:	HGW-2501GN-R2
Firmware:	ES_B7
Router:	Sin conexión a Internet

2.5 Configuración Básica

In the **Configuración Básica** section of the wizard, you can set the services you want to use on the Router. Make sure the services are provided by your service provider. Click the **Configuración Básica** button to show the following screen.



The screenshot shows a window titled "Asistente de Instalación" with a close button in the top right corner. The window contains two main sections. The first section, "Tipo de Servicio Contratado", has two radio button options: "DUO" (which is selected) and "TRIO". The second section, "Tu línea de Voz", also has two radio button options: "SI" (which is selected) and "NO". At the bottom of the window, there is a play button icon and the text "Asistente de Instalación".

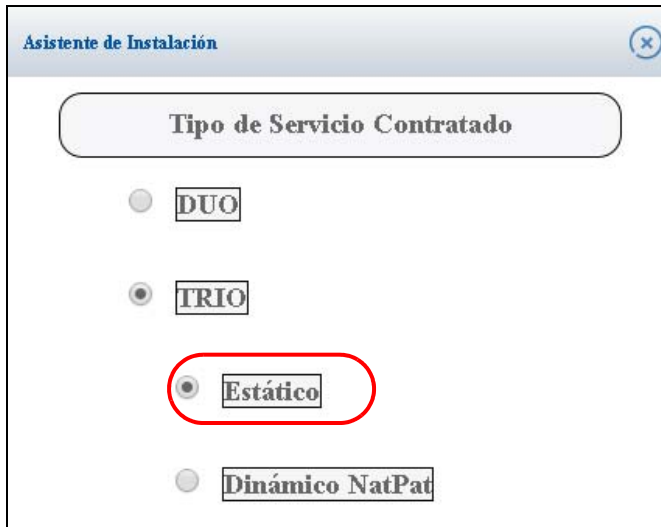
- 1 In the **Tipo de Servicio Contratado** section, if your service provider provides IPTV service, select **TRIO**. If not, select **DUO**:
 - **DUO**: Internet and VoIP service
 - **TRIO**: Internet, VoIP, and IPTV service
- 2 If VoIP service is available, select **SI** from the **Tu línea de Voz** section. Otherwise, select **NO**.
- 3 Click **Asistente de Instalación** to go to the next screen.

2.5.1 IPTV Configuration

The screens in this section are available only when **TRIO** is selected in the previous screen.

The way your set-top box obtains its IP address depends on the service provider.

A. If your service provider provides an IP for the set-top box, select **Estático**.



The screenshot shows a window titled "Asistente de Instalación" with a close button in the top right corner. Below the title bar is a rounded rectangle containing the text "Tipo de Servicio Contratado". Underneath, there are four radio button options: "DUO", "TRIO", "Estático", and "Dinámico NatPat". The "Estático" option is selected, indicated by a filled radio button, and is circled in red.

1 Click **Asistente de Instalación** to show the following screen.

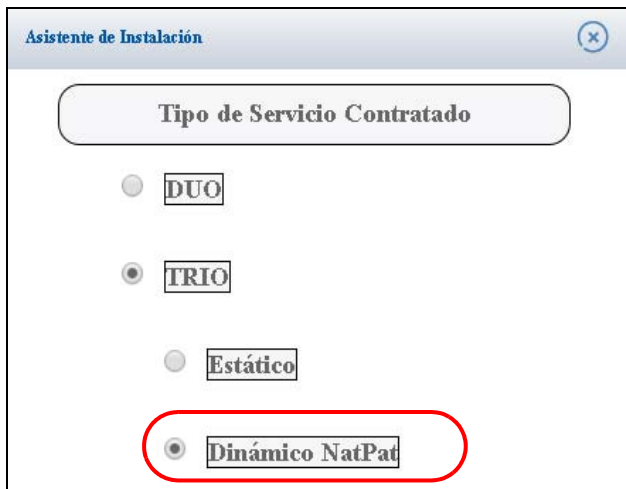


The screenshot shows the same "Asistente de Instalación" window. The "Imagenio Movistar TV Setup" section is visible, containing three input fields: "Dirección IP (LOCAL):" with the value "192.168.249.1", "Dirección IP TV:" with the value "10.69.2.104", and "Máscara de subred:" with the value "255.128.0.0". At the bottom of the window, there are two buttons: "Cancelar" (with a close icon) and "Siguiente" (with a play icon).

2 The NAT feature is disabled and you need to enter the router's LAN IP address in **Dirección IP (LOCAL)**. Enter the IPTV (set-top box)'s IP address (from the service provider) in **Dirección IP TV** and subnet mask in **Máscara de subred**.

3 Click **Siguiente** to go to the next screen.

B. If your service provider did not provide an IP for the set-top box, select **Dinámico NatPat** to enable the NAT feature, so the set-top box obtains its IP address automatically from the service provider.



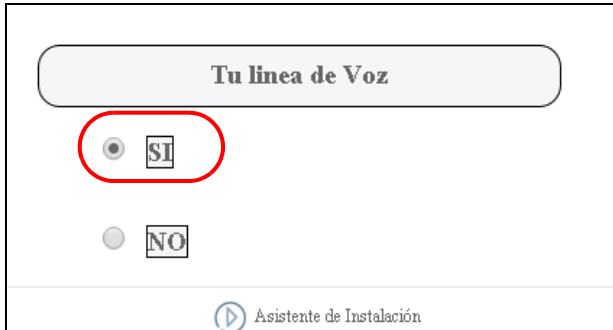
- 1 Click **Asistente de Instalación** to show the following screen.



- 2 The IPTV (set-top box)'s IP address and subnet mask are already configured. If no change is required, click **Siguiete** to go to the next screen.

2.5.2 VoIP Configuration

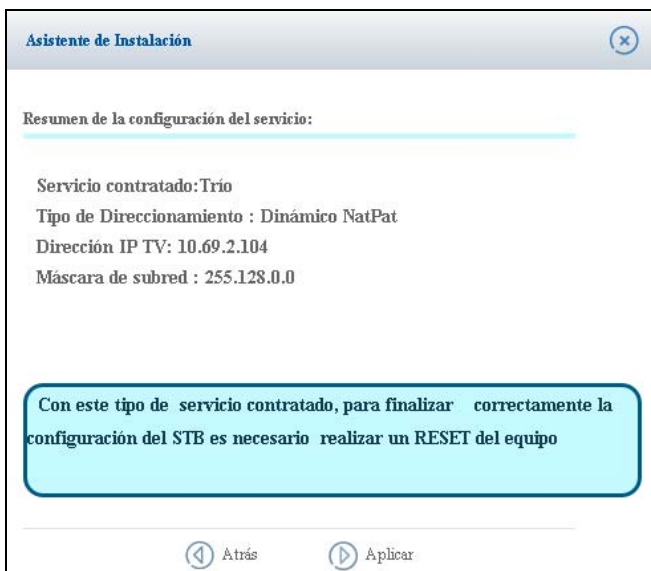
This screen is available only when If you selected **SI** from the **Tu linea de Voz** section in the **Configuración Básica** screen.



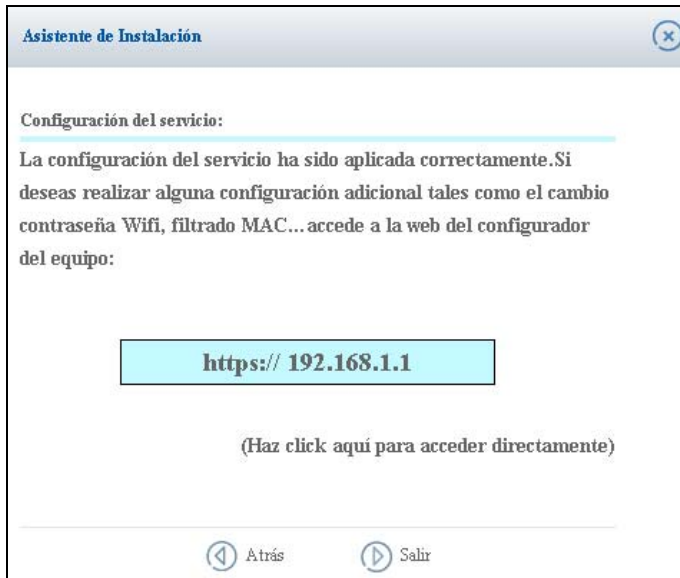
- 1 You need to enter your SIP account number (provided by your service provider) in the following screen.



- 2 Click **Siguiente** to go to the next screen.
- 3 A summary of your settings will appear. Click **Aplicar** to continue.



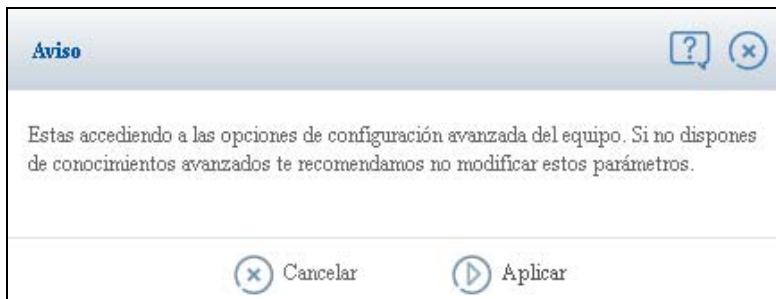
- 4 If you need to configure other settings such as the the Router's LAN and wireless features, click on the IP address shown in the following screen to go to the **Client Wizard** screens. If not, click **Salir** to finish.



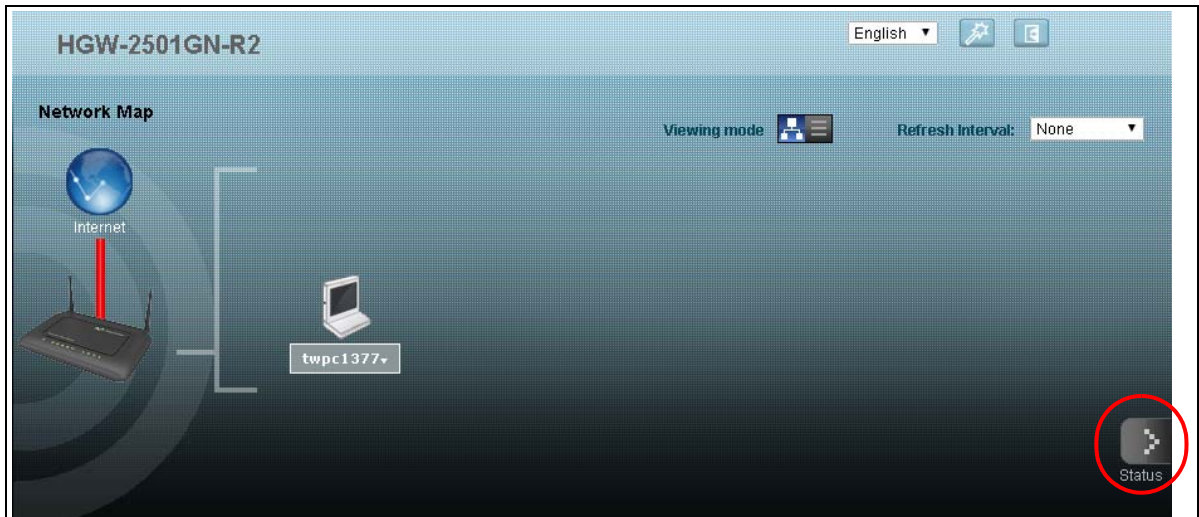
2.6 Configuración Avanzada

In the **Configuración Avanzada** section of the wizard, you can access all of the configuration screens of the Router which can be used for advanced setup. Find detailed information on each configuration screen, starting from [Chapter 5 on page 38](#).

- 1 Click the **Configuración Avanzada** button.
- 2 Click **Aceptar** after reading the following notice.



3 The **Connection Status** screen appears.



4 Click **Status** to display the **System Info** screen, where you can view the Router's interface and system information.

2.7 The Web Configurator Layout

Click **Connection Status > System Info** to show the following screen.

The screenshot shows the web configurator interface for a Movistar HGW-2501GN-R2 device. The interface is divided into three main sections:

- A - Title Bar:** Located at the top, it displays the device name 'HGW-2501GN-R2' and language settings (English).
- B - Main Window:** The central area containing several panels:
 - System Status:** Shows system uptime (3 days: 0 hour: 0 minute), current date/time (Sun Jan 4 00:00:41 UTC 1970), and system resource usage (CPU: 01%, Memory: 19%).
 - Interface Status:** A table showing the status and rate of various interfaces.
 - Registration Status:** A table showing account details and registration actions.
- C - Navigation Panel:** A vertical sidebar on the left containing icons for Connection Status, Network Setting, Security, VoIP, System Monitor, and Maintenance.

Interface	Status	Rate
LAN1	Down	N/A
LAN2	Down	N/A
LAN3	Down	N/A
LAN4	Up	1000M/Full
WLAN	Active	150M
ETHER WAN	Down	N/A

Account	Action	Account St...	URI
1	Register	Disabled	ChangeMe@telefonica.net
2	Register	Disabled	ChangeMe@telefonica.net
3	Register	Disabled	ChangeMe@telefonica.net
4	Register	Disabled	ChangeMe@telefonica.net

As illustrated above, the main screen is divided into these parts:

- **A** - title bar
- **B** - main window
- **C** - navigation panel

2.7.1 Title Bar

The title bar shows icons in the upper right corner. Click the **Quick Start** icon to configure basic initial settings (see [Chapter 4 on page 36](#)). Click the **Logout** icon to log out of the web configurator.

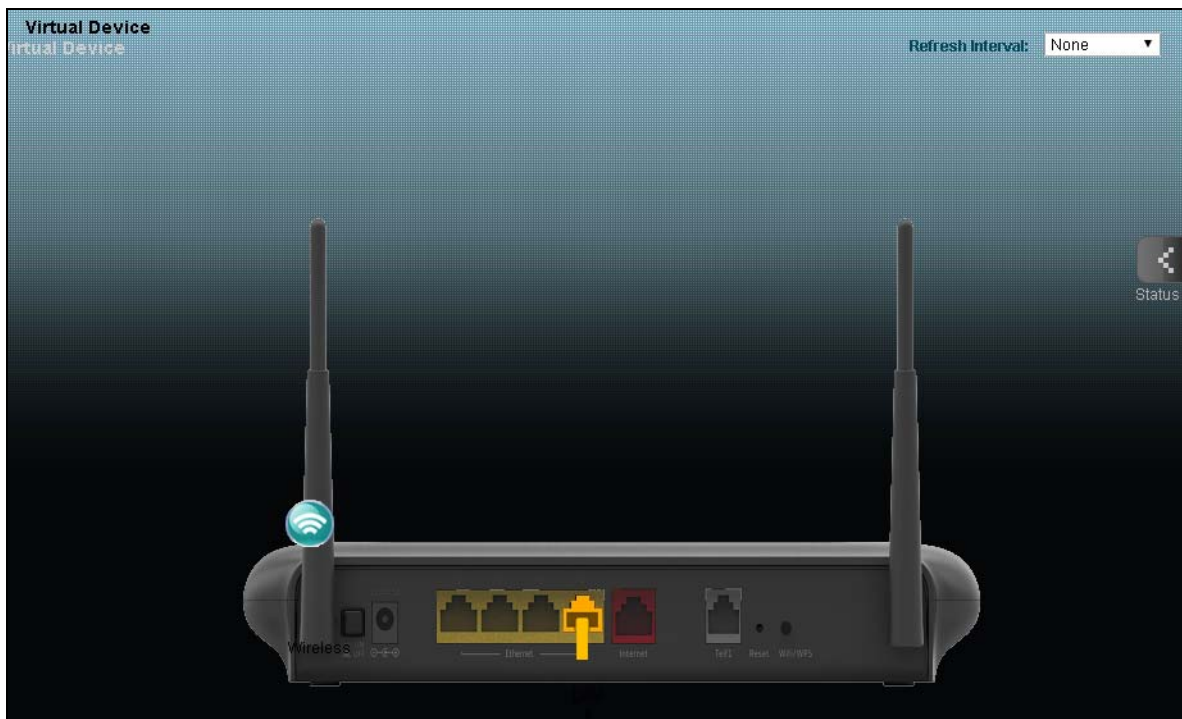


2.7.2 Main Window

The main window displays information and configuration fields. It is discussed in the rest of this document.

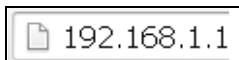
Click **Network Map** on the **System Info** screen (a in [Figure on page 22](#)) to display the **Connection Status** screen. See [Chapter 5 on page 39](#) for more information on the **System Info** and **Connection Status** screens.

Click **Virtual Device** on the **System Info** screen (b in [Figure on page 22](#)) to display a visual graphic showing the connection status of the Router's physical ports.




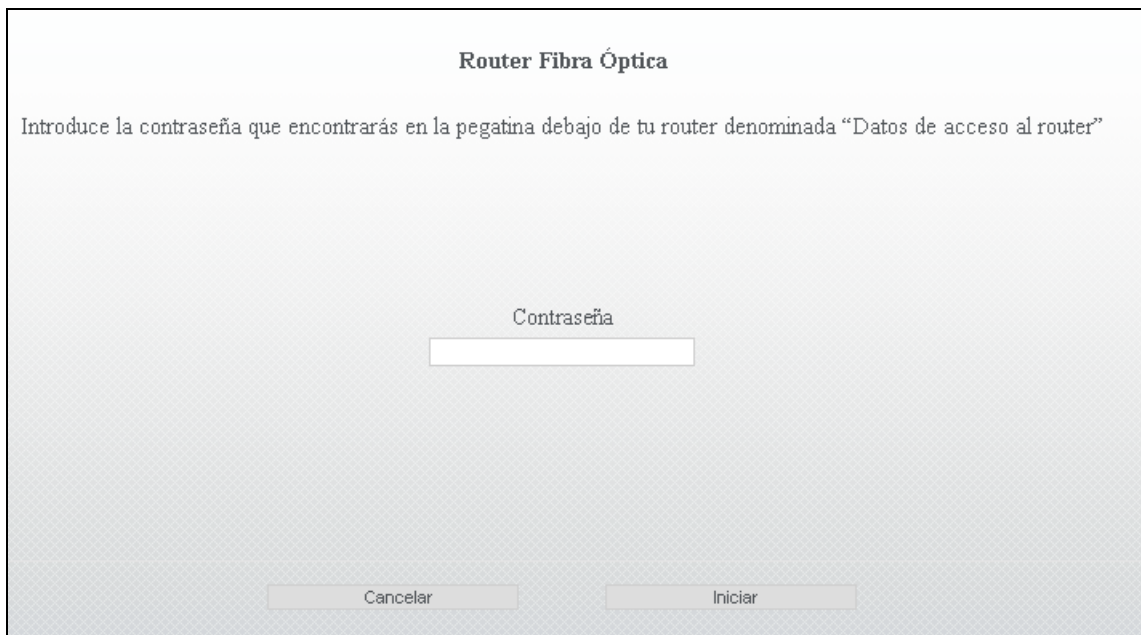
3.1 Access the Router

The **Client Wizard** helps you to configure basic settings such as the LAN and wireless configurations on the Router. Connect to the Web Configurator to access the **Client Wizard** screens. Enter the IP address: <http://192.168.1.1>.

 192.168.1.1

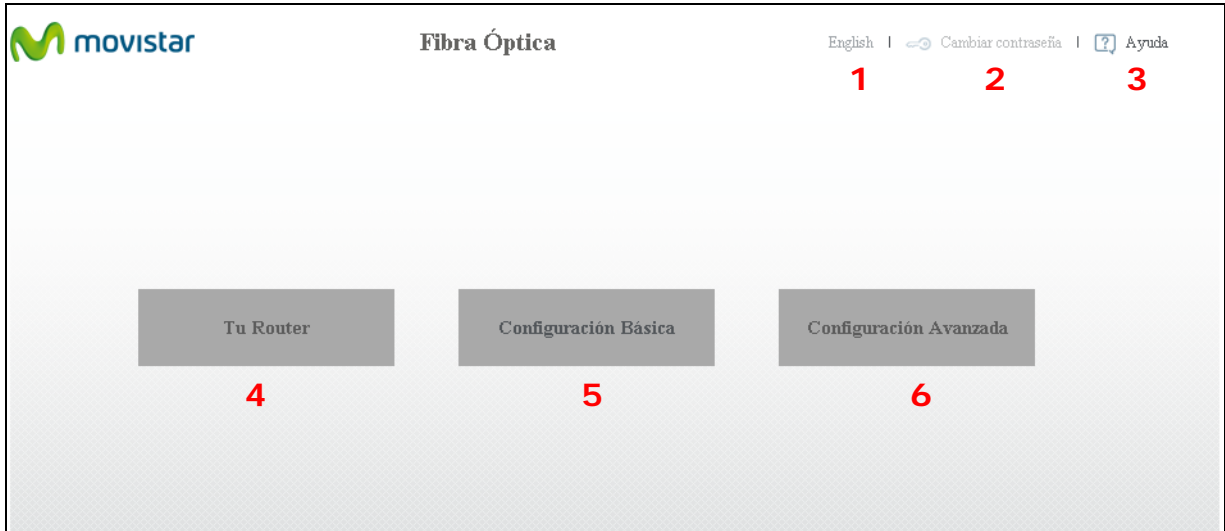
The login screen appears. The default password is **1234**. Enter the password. Click **Iniciar** to enter the **Client Wizard**.

-  If you are connecting to the **Client Wizard** from the **Installation Wizard**, you do not need to log into the Router again.



The screenshot shows a web browser window with the title "Router Fibra Óptica". The main content area contains the text: "Introduce la contraseña que encontrarás en la pegatina debajo de tu router denominada 'Datos de acceso al router'". Below this text is a text input field labeled "Contraseña". At the bottom of the window, there are two buttons: "Cancelar" on the left and "Iniciar" on the right.

The main screen appears. Click the buttons in this screen for basic or advanced configurations of the Router.



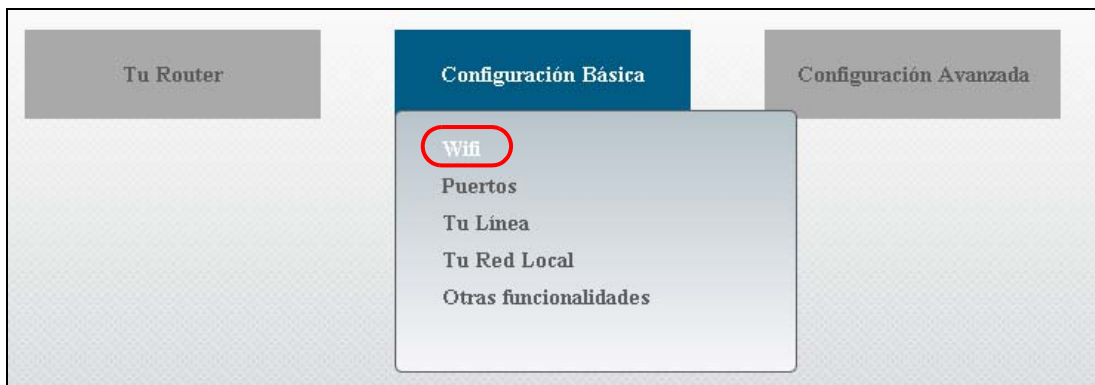
For items 1, 2, 3, 4, and 6, refer to [Chapter 3 on page 25](#) for more information.

3.2 Configuración Básica

In the **Configuración Básica** section of the wizard, you can configure some basic settings, such as LAN and wireless settings on the Router. Mouse-over the **Configuración Básica** button to show the basic setting menu.

3.2.1 Wireless Configuration

- 1 Mouse-over the **Configuración Básica**. Then click **Wifi**.



Click **Wifi** in the menu to show the following screen. Configure the wireless settings in this screen.

Wifi

Red inalámbrica (WiFi)

Estado: **ACTIVADA**

Identificador Red Inalámbrica (SSID): MOVISTAR_1120

Visible:

Seguridad

Tipo de cifrado: WPA2-PSK

Contraseña Wifi (alfanumérica): 4VvX4VUJ9EHER3EHKK9993

Encriptación: AES

Número de Canal: Automáticamente

WPS Configuration

Estado: **ON**

Nota informativa: para habilitar la ventana de WPS debe pulsar el botón físico para esta funcionalidad en su equipo. Para más información consulta tu documentación del equipo.

El método de cifrado de WPA2 no es compatible con WPS 2.0. Para más información consulta el menú de ayuda.

Filtrado MAC + Añadir regla

Listado de direcciones MAC de los equipos que pueden acceder a tu WiFi:

Acción: Ninguna

Dirección MAC:

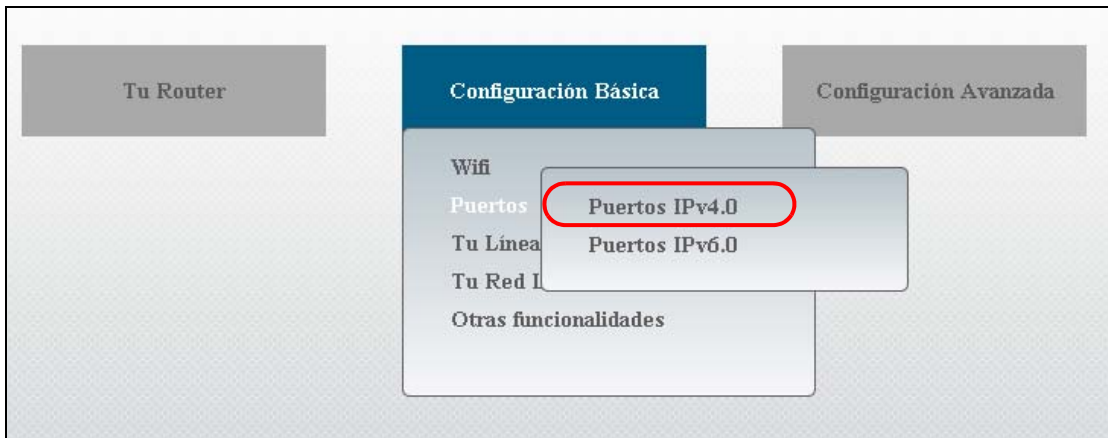
- 1 By default, the wireless feature is enabled. If you want to disable it, switch the **Estado** button to **DESACTIVADA**. You can change the Router's SSID in **Identificador Red Inalámbrica (SSID)** and select **Visible** if you allow it to be seen by a SSID scan. If not, select **Oculto**.
- 2 The basic wireless security mode is **WPA2-PSK**. If you want to change the security mode, password, or encryption mode, you can do so in the **Seguridad** section.

- 3 In the **WPS Configuration** section, you can enable WPS on the Router to quickly set up a secured wireless network with its clients.
- 4 You can also configure wireless MAC filter in the **Filtrado MAC** section to allow or deny clients based on their MAC addresses. Click **Añadir regla** if you want to add more rules.
- 5 Click **Aplicar** to save your settings and exit the screen.

3.2.2 IPv4 NAT Port Forwarding Configuration

You can configure IPv4 virtual service rules to forward incoming service requests to the server(s) on your local network.

- 1 Mouse-over the **Configuración Básica** and **Puertos** to show the **Puertos** menu. Click **Puertos IPv4.0**.



- 2 Click **Añadir IPv4.0 regla** to add a new NAT port forwarding rule.



- 3 If you want to add a single port, select **el puerto** in the **Abrir** field and enter the port number and the internal port number. If you want to add a range of port numbers, select **los puertos** in the **Abrir** field and enter the external start/end ports, the internal start/end ports.

The screenshot shows a configuration window titled "Reglas que se aplican" with a sub-header "Añadir IPv4.0 regla". The interface includes the following fields and controls:

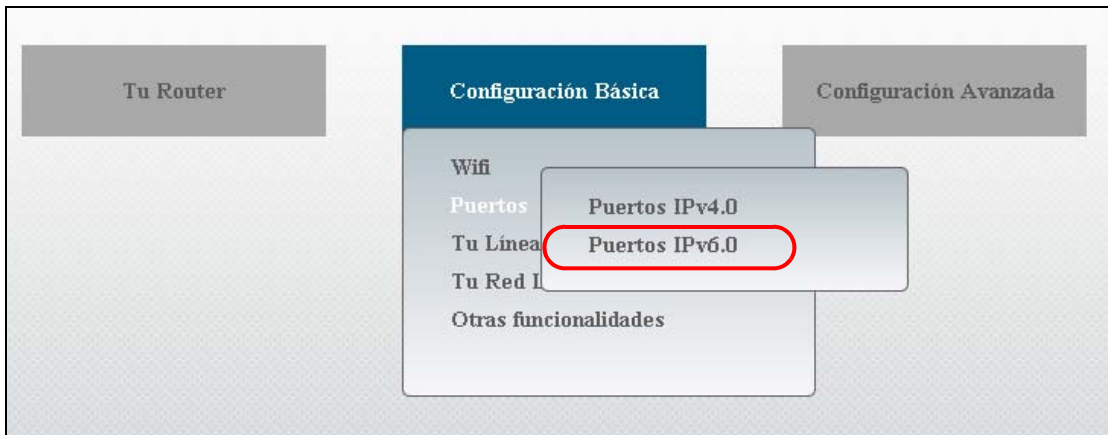
- Abrir:** A dropdown menu currently set to "el puerto".
- número:** A text input field for the port number.
- protocolo:** A dropdown menu currently set to "TCP y UDP".
- Interno:** A text input field for the internal port number.
- IP del dispositivo:** A text input field for the device IP address.
- Buttons:** "Cancelar" (Cancel) and "Guardar cambios" (Save changes) at the bottom.
- Icon:** A minus sign icon (-) next to the "protocolo" dropdown.

- 4 Select the protocol used for this rule in the **protocolo** field.
- 5 Enter the inside IP address of the LAN device to which the virtual server forwards traffic in the **IP del dispositivo** field.
- 6 Click **Añadir IPv4.0 regla** to add another virtual service rule. If you want to remove a rule, click the **-** icon next to the rule.
- 7 Click **Guardar cambios** to save your settings and exit the screen.

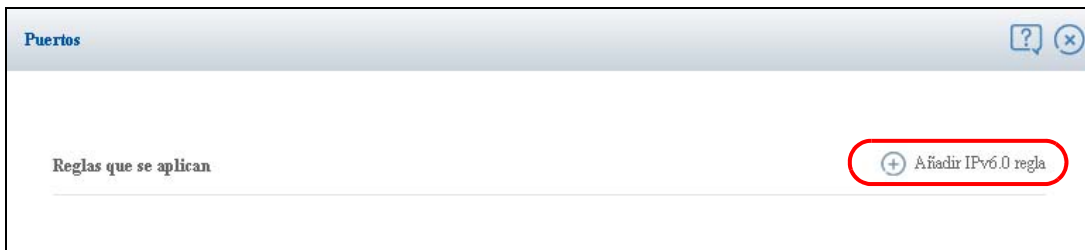
3.2.3 IPv6 Firewall Configuration

You can configure IPv6 firewall rules for the Router.

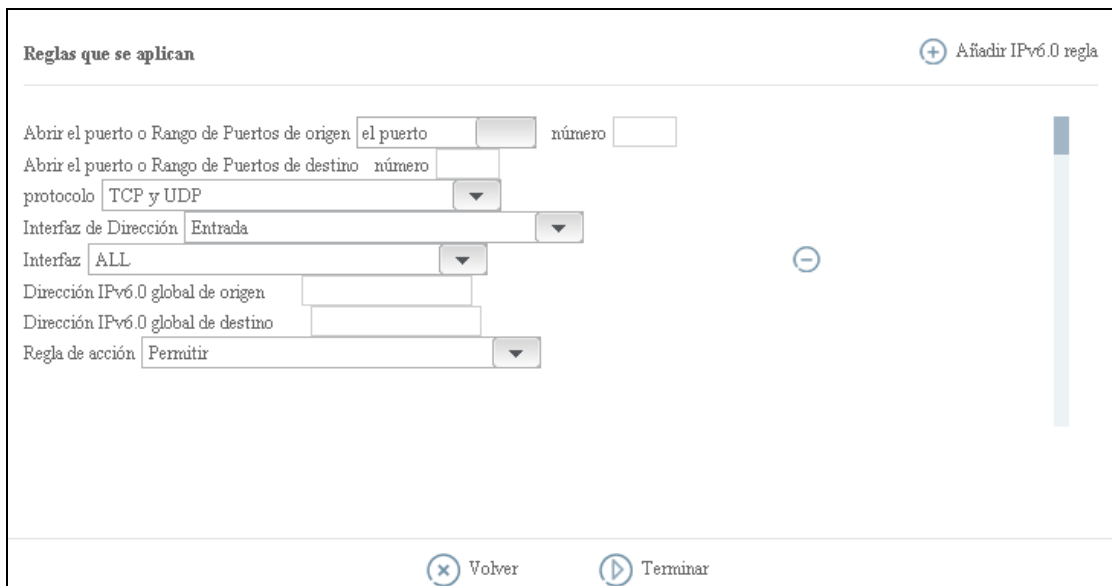
- 1 In the **Puertos** menu. Click **Puertos IPv6.0**.



- 2 Click **Añadir IPv6.0 regla** to add a new firewall rule.



- 3 Select if this rule is for one single port or a range of ports in the **Abrir el puerto o Rango de Puertos de origen** field. Enter the port number or port range.



- 4 In the **Abrir el puerto o Rango de Puertos de destino** field, enter the internal port number if this rule is for one single port. Enter the internal port range if this rule is for a range of ports.

- 5 Select the protocol used for this rule in the **protocolo** field.
- 6 Specify the direction of travel of packets in **Interfaz de Dirección**.
- 7 Select the interface to which this rule is applied in **Interfaz**. **ALL** means this rule applies to all interfaces of the Router.
- 8 Enter the source and destination IPv6 address in the **Dirección IPv6.0 global de origen/destino** fields.
- 9 In **Regla de acción**, set the default action that the firewall takes on packets that do not match the rules.
- 10 Click **Añadir IPv6.0 regla** to add another firewall rule. If you want to remove a rule, click the **■** icon next to the rule.
- 11 Click **Terminar** to save your settings and exit the screen.

3.2.4 Connection Line Configuration

Use this screen to configure the connection of the Router with the ONT.

- 1 Mouse-over the **Configuración Básica** and **Puertos**. Then click **Tu Línea**.



- 2 Select whether your connection has NAT enabled. If yes, select **Multipuesto** and enter the account username and password provided by your ISP to connect to the ONT. If not, select **Monopuesto**.

Tu Línea

Multipuesto (Con NAT) (recomendado)

Usuario: adslppp@telefonicanetpi

Contraseña: adslppp

Monopuesto (Sin NAT)

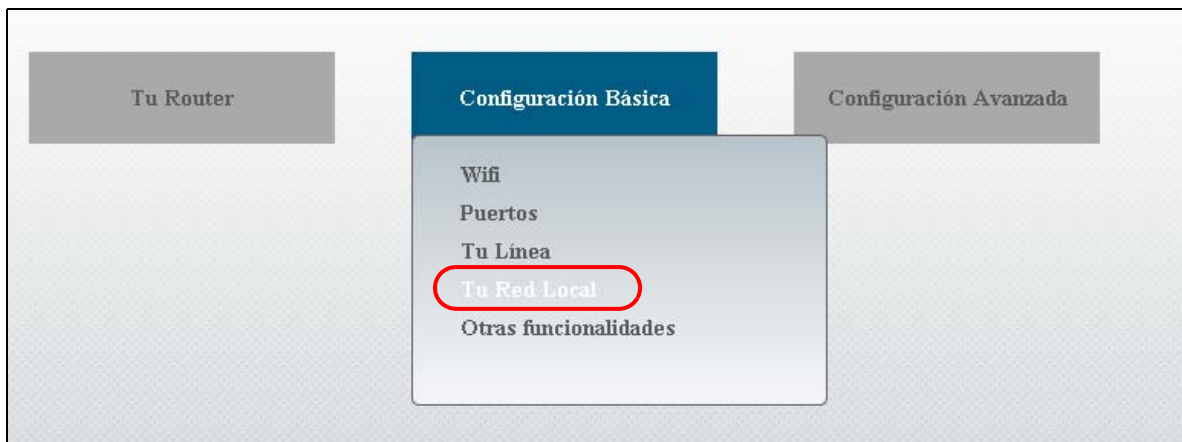
Cancelar Aplicar

- 3 Click **Aplicar** to save your settings and exit the screen.

3.2.5 LAN Configuration

You can configure the Router's LAN IPv4/IPv6 address, subnet mask, DHCP and DNS server information for the LAN interface.

- 1 Mouse-over the **Configuración Básica** and **Puertos**. Then click **Tu Red Local**.



In this screen, configure the Router's LAN IPv4/IPv6 address, subnet mask, DHCP and DNS server information for the LAN interface.

The screenshot shows the 'Asistente de Instalación' (Installation Wizard) interface. It is divided into two main sections: LANv4 IP Setup and LANv6 IP Setup. Each section includes fields for IP address, subnet mask, DHCP server state, and DNS server information.

LANv4 IP Setup

- Dirección IPv4 (LOCAL): 192.168.1.1
- Máscara de subred: 255.255.255.0
- DHCP Server State**: Estado is set to ON.
- IPv4 range start: 192.168.1.33
- El tamaño de la piscina: 167
- Configuring DNSv4 servers**: Servidor DNS 1 is 80.58.61.250 and Servidor DNS 2 is 80.58.61.254.

LANv6 IP Setup

- IPv6 Address (LOCAL): fe80::1
- IPv6 Address (GLOBAL): (empty field)
- Prefijo: 64
- DHCP Server State**: Autoconfiguración is unchecked, and Rango Fijo is checked.
- IPv6 range start: ::33
- IPv6 range end: ::254
- Configuring DNSv6 servers**: DNSv6 Server 1 is fe80::1 and DNSv6 Server 2 is fe80::2.

At the bottom of the wizard, there are two navigation buttons: 'Volver' (Back) and 'Siguiente' (Next).

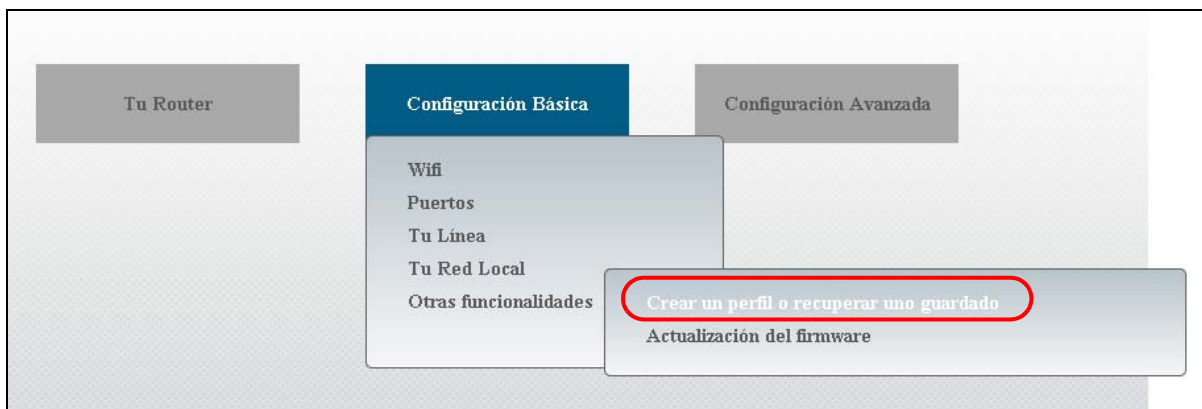
- 1 In the **Configuración DHCP IPv4** section, enter the Router's IPv4 IP address and subnet mask.
- 2 The **DHCP** feature is set to **ACTIVADO** by default to to assign IP addresses and provide subnet mask, gateway, and DNS server information to LAN devices. You can configure the starting IP range and pool size. If you want to disable it, switch the **Estado** button to **DESACTIVADO**.
- 3 If DHCP is enabled, enter the DNS first and second server IP addresses in the **Configuración de servidores DNS** servers section.
- 4 In the **Configuración DHCP IPv6** section, enter the Router's IPv6 IP address and subnet mask.
- 5 In the **DHCP** section, select **Autoconfiguración** to have the Router automatically configure the DHCPv6 server and pass IPv6 addresses, DNS server and domain name information to DHCPv6 clients. If you want to configure it manually, select **Rango Fijo** and enter the IPv6 range.

- 6 Enter the first and second DNS server IPv6 address the Router passes to the DHCPv6 clients in the **Configuración DNS IPv6** section.
- 7 Click **Aplicar** to save your settings and close the screen.

3.2.6 Profile Configuration

In this screen, you can save a profile or restore it on the Router. A profile contains the current settings on the Router which helps you to easily restore the settings in case the Router has been set to factory default.

- 1 Mouse-over the **Configuración Básica** and **Otras funcionalidades** and click **Crear un perfil o recuperar uno guardado**.



- 2 Click **Guardar** to save and download your current settings as a profile (*.cfg). Save it on your computer.



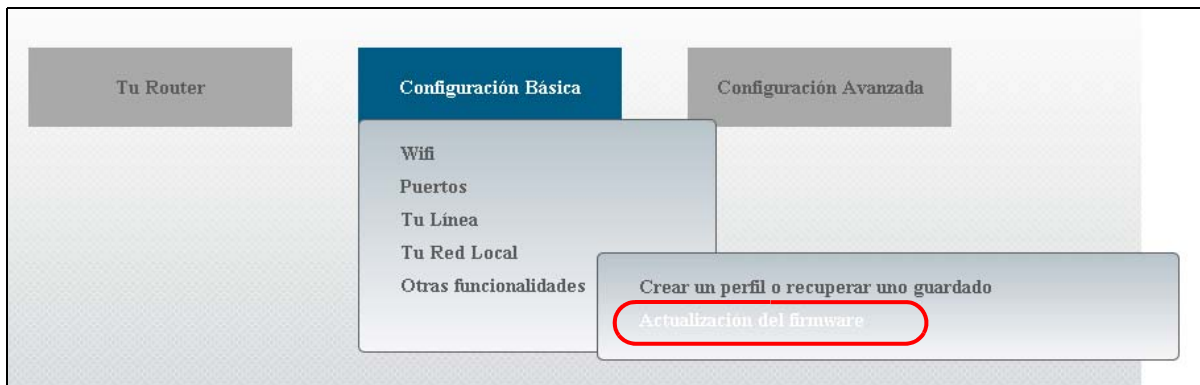
- 3 If you want to restore a profile that you have saved previously, choose the file path in **Ruta del archivo** and click **Cargar**. The Router will restart shortly after the profile has been uploaded. Wait several minutes for the restart to finish.
- 4 If you want to restore the Router to its factory default settings, click the **Restaurar** button. It is suggested to save your settings before doing so.

See [Chapter 26 on page 141](#) for more information about backup and restore device configurations.

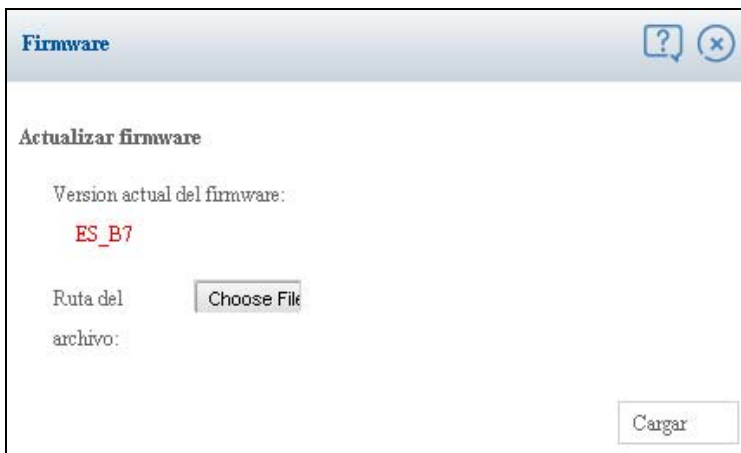
3.2.7 Firmware Upgrade

In this screen, you can upgrade the firmware for the Router. A profile contains the current settings on the Router which helps you to easily restore the settings in case the Router has been set to factory default.

- 1 Mouse-over the **Configuración Básica** and **Otras funcionalidades** and click **Crear un perfil o recuperar uno guardado**.



- 2 The screen show the current firmware version. To upload a newer version of firmware, choose its file path in **Ruta del archivo** and click **Cargar**. The process may take several minutes. After a successful upload, the system will reboot.





Make sure you are using the correct firmware for this device.



Do NOT turn off the Router while firmware upload is in progress!

See [Chapter 25 on page 139](#) for more information about firmware upgrade on the Router.

Quick Start

4 Chapter

4.1 Overview

Use the **Quick Start** screens to configure the Router's time zone, basic Internet access, and wireless settings.

4.2 Quick Start Setup

- 1 Click the **Quick Start** icon in the top right corner of the web configurator to open the quick start wizard screens.



- 2 Select the time zone of the Router's location and click **Next**.

Welcome to Quick Start wizard

The wizard will guide you through the basic settings of this device. This will take about few minutes to complete. Click Next to begin.

Time Zone:

[Back](#) [Next](#) [Close](#)

- 3 Enter the login user name and password provided by your ISP. If your ISP has provided a specific IP address and DNS server(s), you need to configure them manually. If not, the IP address will be assigned automatically. Click **Next**.

Quick Start

Internet Configuration

STEP 1

The current connection type is set to PPPoE and needs a user name and password to get online.

User Name:

Password:

Service Name:

Is there specific IP address information from your Internet Service Provider (ISP)?

Yes No

IP Address:

Primary DNS Server:

Secondary DNS Server:

Back Next Close

- 4 Turn the wireless LAN on or off. If you keep it on, record the security settings so you can configure your wireless clients to connect to the Router. Click **Next**.

Quick Start

Wireless Setup

STEP 2

The following settings are the current wireless settings which your wireless client devices need in order to get connected to this device.

Wireless Service:

Wireless Network Name (SSID): MOVISTAR_1120

Security Level: WPA2PSK

Pre-Shared Key: 4Wx4WU9EHER3EHK9993

Back Next Close

- 5 Your Router saves your settings and attempts to connect to the Internet.

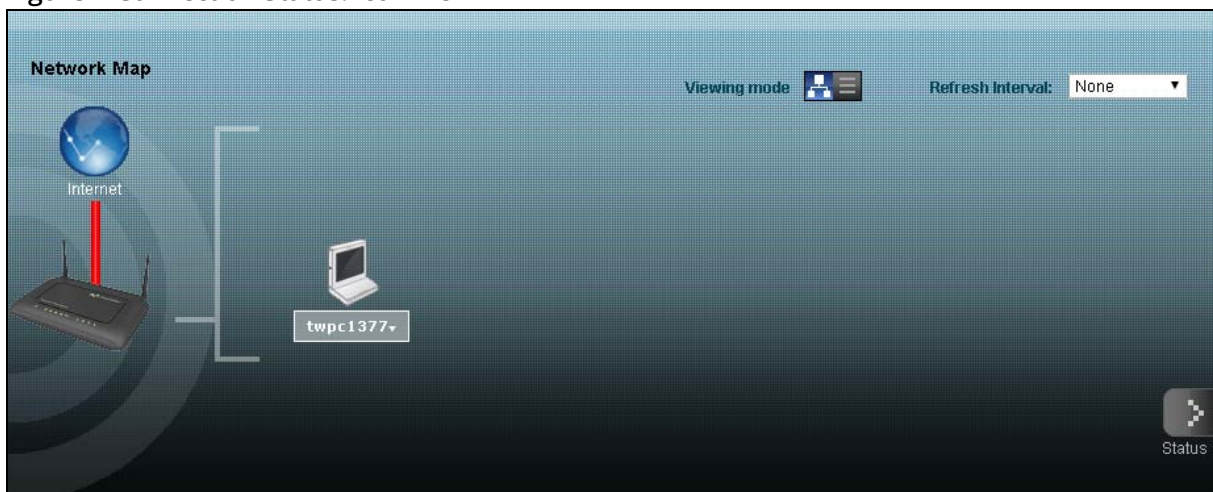
Connection Status and System Info

5 Chapter

5.1 The Connection Status Screen

Use this screen to view the network connection status of the device and its clients. A warning message appears if there is a connection problem. You can configure how often you want the Router to update this screen in **Refresh Interval**.

Figure 1 Connection Status: Icon View



To view the connected LAN devices in a list, click **List View** in the **Viewing mode** selection box.

Figure 2 Connection Status: List View



In **Icon View**, if you want to view information about a client, click the client's name and **Info**.

In **List View**, you can also view the client's information.

5.2 The System Info Screen

Click **Connection Status > System Info** to open this screen. You can look at the current status of the Router, system resources, interfaces (LAN, WAN and WLAN), and SIP accounts. You can also register and unregister SIP accounts.

Figure 3 System Info Screen

The screenshot displays the 'System Info' screen with the following sections:

- Device Information:** Host Name: 1234, Model Name: HGW-25010N-R2, MAC Address: 48 4A 03 AA 11 20, Firmware Version: ES_07, Ethernet WAN: PPPoE, Encapsulation: PPPoE, IPv6 Dual Stack: DualStack, IP Address: 0.0.0.0, IP Subnet Mask: N/A, Default Gateway: 0.0.0.0, Primary DNS: 200.204.0.10, Secondary DNS: 200.204.0.138, IPv6 Global IP: ::, IPv6 Prefix Length: 0, IPv6 Gateway: ::, IPv6 WAN DNS1: ::, IPv6 WAN DNS2: ::, Link-Local Address: ::, Encapsulation: ENET ENCAP, IPv6 Dual Stack: IPv4, IP Address: 0.0.0.0, IP Subnet Mask: 0.0.0.0, Default Gateway: 0.0.0.0, Primary DNS: 0.0.0.0, Secondary DNS: 0.0.0.0, IPv6 Global IP: ::, IPv6 Prefix Length: 0, IPv6 Gateway: ::, IPv6 WAN DNS1: ::, IPv6 WAN DNS2: ::, Link-Local Address: ::, Encapsulation: ENET ENCAP, IPv6 Dual Stack: IPv4, IP Address: 0.0.0.0, IP Subnet Mask: 0.0.0.0, Default Gateway: 0.0.0.0, Primary DNS: 0.0.0.0, Secondary DNS: 0.0.0.0, IPv6 Global IP: ::, IPv6 Prefix Length: 0, IPv6 Gateway: ::, IPv6 WAN DNS1: ::, IPv6 WAN DNS2: ::, Link-Local Address: ::.
- System Status:** System Uptime: 0 day 17 hours: 14 minutes, Current Date/Time: Thu Jan 1 18:14:44 UTC 1970, System Resource: CPU Usage: 02%, Memory Usage: 20%.
- Interface Status:**

Interface	Status	Rate
LAN1	Down	N/A
LAN2	Down	N/A
LAN3	Down	N/A
LAN4	Up	1000M/Full
WLAN	Active	150M
ETHER WAN	Down	N/A
- Registration Status:**

Account	Action	Account Status	URI
1	Registered	Disabled	ChangeMe@telefonica.net
2	Registered	Disabled	ChangeMe@telefonica.net
3	Registered	Disabled	ChangeMe@telefonica.net
4	Registered	Disabled	ChangeMe@telefonica.net
- LAN Information:** IP Address: 192.168.1.1, IP Subnet Mask: 255.255.255.0, DHCP: Server, IPv6 Address: ::, Link-local IPv6 Address: fe80::42a:3ff:feaa:1120, IPv6 Prefix: ::, Preferred Valid Time(sec): 3600/7200, DHCPv6: Server, Radvd State: Enable, IPv6 LAN DNS1: ::, IPv6 LAN DNS2: ::.
- WLAN Information:** Status: On, SSID: MOVISTAR_1120, Channel: 11, undefined: 902.11b+g+n, Security Mode: WPA-PSK/WPA2-PSK, WPS: Configured, Scheduling: Disable, WiFi MAC: 42:4A:03:AA:11:20-42:4A:03:AA:11:23.
- Security:** Firewall: Enable.

6.1 The WAN Screen

The Router must have a WAN interface to allow users to use the Ethernet connection to access the Internet. Use the **WAN** screen to manage WAN interfaces. Click **Network Setting > WAN**.

Figure 4 Network Setting > WAN

Ethernet Connections Table									
#	Active	VLAN	IP	Release	VID/Priority	Encapsulation	NAT	Modify	
1	<input checked="" type="checkbox"/>	Internet	N/A	Release	6/1	ENET ENCAP	Disabled		
2	<input checked="" type="checkbox"/>	Voz	N/A	Renew	3/4	ENET ENCAP	Enable		
3	<input checked="" type="checkbox"/>	Imagenio	N/A	N/A	2/4	ENET ENCAP	Enable		
4	<input type="checkbox"/>	N/A	N/A	N/A	--/--	ENET ENCAP	N/A		
5	<input type="checkbox"/>	N/A	N/A	N/A	--/--	ENET ENCAP	N/A		
6	<input type="checkbox"/>	N/A	N/A	N/A	--/--	ENET ENCAP	N/A		
7	<input type="checkbox"/>	N/A	N/A	N/A	--/--	ENET ENCAP	N/A		
8	<input type="checkbox"/>	N/A	N/A	N/A	--/--	ENET ENCAP	N/A		

Table 3 Network Setting > WAN

LABEL	DESCRIPTION
Active	This shows whether the connection is activated.
VLAN	This is the service name of the connection.
IP	This shows the WAN IP address.
Release	Click the Release button to release this Ethernet connection. Click the Renew button to renew it.
VID/Priority	This is the VLAN ID and IEEE 802.1p priority.
Encapsulation	This shows the method of encapsulation used by this connection.
NAT	This shows whether NAT is activated or not for this connection. NAT is not available when the connection uses the bridging service.
Modify	Click the Edit icon to configure the connection.

6.1.1 Edit Ethernet Connection

In **Network Setting > WAN**, click the **Edit** icon next to an Ethernet connection to display the following screen. Use this screen to configure an Ethernet connection.

Figure 5 Network Setting > WAN: Edit

The screenshot shows the 'Edit' configuration screen for a WAN connection. It is organized into several sections:

- General:** Includes an 'Active' checkbox, a 'VLAN' text field (value: 'Voz'), 'Mode' (dropdown: 'Router'), 'Encapsulation' (dropdown: 'ENET ENCAP'), 'IPv6/IPv4 Dual Stack' (dropdown: 'IPv4/IPv6'), 'Enable VLAN' checkbox, '802.1P Priority [0-7]' (text field: '4'), and '802.1Q VLAN ID [1-4094]' (text field: '3').
- IP Address:** Includes radio buttons for 'Obtain an IP Address Automatically' (selected) and 'Static IP Address'. Under 'Static IP Address', there are text fields for 'IP Address', 'Subnet Mask', 'Gateway IP Address', 'Primary DNS', and 'Secondary DNS', all with '0.0.0.0' as the default value.
- IPv6 address:** Includes radio buttons for 'Obtain an IP Address Automatically' (selected) and 'Static IP Address'. Under 'Static IP Address', there are radio buttons for 'DHCP IPv6' (selected) and 'SLAAC', and radio buttons for 'DHCP PD' (selected) with 'Enable' and 'Disable' options.
- NAT:** Includes radio buttons for 'None', 'SUA Only' (selected), and 'Full Feature'.
- Advanced Setup:** A button to expand additional settings.
- RIP & Multicast Setup:** Includes 'RIP Direction' (dropdown: 'In Only'), 'RIP Version' (dropdown: 'RIP2-B/RIP2-M'), and 'Multicast' (dropdown: 'None').
- MTU:** Includes an 'MTU' text field with the value '1480'.

At the bottom right of the screen, there are 'Apply' and 'Cancel' buttons.

Table 4 Network Setting > WAN: Edit

LABEL	DESCRIPTION
Active	Select this to have the Router use the Ethernet connection.
VLAN	Specify the name for this WAN interface.

Table 4 Network Setting > WAN: Edit (continued)

LABEL	DESCRIPTION
Mode	Select Router (default) if your ISP gives you one IP address only and you want multiple computers to share an Internet account. Select Bridge when your ISP provides you more than one IP address and you want the connected computers to get individual IP address from the ISP's DHCP server directly. If you select Bridge , you cannot use Firewall, DHCP server and NAT on the Router.
Encapsulation	Select the method of encapsulation used by your ISP . Choices vary depending on the mode you select in the Mode field. If you select Router in the Mode field, select ENET ENCAP or PPPoE . If you select Bridge in the Mode field, method of encapsulation is not available.
User Name	(PPPoE encapsulation only) Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	(PPPoE encapsulation only) Enter the password associated with the user name above.
Service Name	(PPPoE only) Type the name of your PPPoE service here.
IPv6/IPv4 Dual Stack	Select IPv4 if you want the Router to run IPv4 only. Select IPv4/IPv6 to allow the Router to run IPv4 and IPv6 at the same time. Select IPv6 if you want the Router to run IPv6 only.
PPP Authentication	Select an authentication protocol for outgoing calls: AUTO - Your Router accepts either CHAP or PAP when requested by this remote node. CHAP - Your Router accepts CHAP only. PAP - Your Router accepts PAP only.
IP Address	This option is available if you select Router in the Mode field and IPv4 or IPv4/IPv6 in the IPv6/IPv4 Dual Stack field. Select Obtain an IP Address Automatically if you have a dynamic IP address; otherwise select Static IP Address .
IP Address	Enter the IP address your ISP has assigned.
Primary DNS	Enter the primary DNS server's address for the Router.
Secondary DNS	Enter the secondary DNS server's address for the Router.
IPv6 address	This option is available if you select Router in the Mode field and IPv6 or IPv4/IPv6 in the IPv6/IPv4 Dual Stack field. If you select ENET ENCAP in the Encapsulation field, select Obtain an IP Address Automatically if you have a dynamic IPv6 address; otherwise select Static IP Address . If your encapsulation mode is PPPoE , the Router's IPv6 address is dynamic and you do not need to configure the IPv6 address settings.
IPv6 Address	Enter the IPv6 address assigned by your ISP.
Prefix length	Enter the address prefix length.

Table 4 Network Setting > WAN: Edit (continued)

LABEL	DESCRIPTION
IPv6 Default Gateway	Enter the default gateway.
IPv6 DNS Server1	Enter the first IPv6 DNS server address.
IPv6 DNS Server2	Enter the second IPv6 DNS server address.
DHCP IPv6	This is available only when you select Obtain an IP Address Automatically . Select DHCP to obtain an IPv6 address from a DHCPv6 server. Select SLAAC to have the Router use the prefix to automatically generate a unique IP address that does not need to be maintained by a DHCP server.
DHCP PD	This is available only when you select Obtain an IP Address Automatically . Select Enable to use DHCP PD (Prefix Delegation) to allow the Router to pass the IPv6 prefix information to its LAN hosts. The hosts can then use the prefix to generate their IPv6 addresses.
NAT	SUA Only is available only when you select Router in the Mode field. Select SUA Only if you have one public IP address and want to use NAT. Select Full Feature if you have multiple public WAN IP addresses for your Router. Select None to disable NAT.
Mapping Set	If you select Full Feature in the NAT field, select the NAT address mapping set of local IP addresses to map to this interface's IP address.
Advanced Setup	Click this to display or hide RIP and multicast and MTU fields.
RIP Direction	Select the RIP Direction from None , Both , In Only and Out Only .
RIP Version	This field is not configurable if you select None in the RIP Direction field. Select the RIP version from RIP-1 and RIP2-B/RIP2-M .
Multicast	The Router supports IGMP-v1 , IGMP-v2 and IGMP-v3 . Select None to disable it.
MTU	Enter the MTU for this WAN interface in this field.

7.1 Wireless General Screen

Use this screen to enable the Wireless LAN, enter the SSID and select the wireless security mode.

- ① If you are configuring the Router from a computer connected to the wireless LAN and you change the Router's SSID or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the Router's new settings.

Click **Network Setting > Wireless 2.4GHz** to open the **General** screen. Select the **Enable Wireless LAN** checkbox to show the Wireless configurations.

Figure 6 Network Setting > Wireless 2.4 > General

The screenshot displays the 'Wireless Network Setup' configuration page. It includes sections for 'Wireless Network Settings' and 'Security Level'. The 'Wireless Network Settings' section contains a text input for the SSID (MOVISTAR_1120), and checkboxes for 'Hide SSID', 'Client Isolation', and 'MBSSID/LAN Isolation'. The 'Channel Selection' section has a dropdown menu set to 'Auto' and buttons for 'Scan' and 'Result'. The 'Security Level' section has a dropdown menu set to 'WPA2-PSK'. Below these settings is a security level slider with three segments: 'No Security' (red), 'Basic' (yellow), and 'More Secure (Recommended)' (green). A blue circle is positioned on the 'More Secure' segment. A tooltip box is open over the slider, containing the text: 'Enter 8-63 characters or 64 hexadecimal digits (a-f, A-F, and 0-9). Pre-Shared Key 4Wx4WU9EHER3EHKJ more...'. At the bottom right of the screen are 'Apply' and 'Undo' buttons.

Table 5 Network Setting > Wireless 2.4GHz > General

LABEL	DESCRIPTION
Wireless	Select the Enable Wireless LAN check box to activate the wireless LAN. Nota: You must also set the Router's physical Wifi/WPS button to ON to use wireless LAN. The Wifi LED should be on.
Wireless Network Name (SSID)	Enter a descriptive name for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Client Isolation	Select this to keep the wireless clients in this SSID from communicating with each other directly through the Router.
MBSSID/LAN Isolation	Select this to keep the wireless clients in this SSID from communicating with clients in other SSIDs or wired LAN devices through the Router. Select both Client Isolation and MBSSID/LAN Isolation to allow this SSID's wireless clients to only connect to the Internet through the Router.
Channel Selection	Set the channel depending on your particular region. Select a channel or use Auto to have the Router automatically determine a channel to use. If you are having problems with wireless interference, changing the channel may help. Try to use a channel that is as many channels away from any channels used by neighboring APs as possible. The channel number which the Router is currently using then displays in the Operating Channel field.
Scan	Click this button to have the Router immediately scan for and select a channel (which is not used by another device) whenever the device reboots or the wireless setting is changed.
Result	Click this to show the scan result of channels and their noise such as the following screen.

#	Noise
1	10.94
2	17.11
3	24.23
4	82.94
5	18.75
6	24.23
7	17.11
8	10.94
9	15.28
10	15.28
11	10.94
12	12.12
13	20.59

Table 5 Network Setting > Wireless 2.4GHz > General (continued)

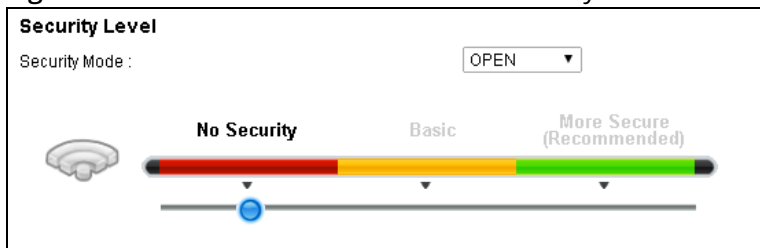
LABEL	DESCRIPTION
Operating Channel	This is the channel currently being used by your AP.
Security Mode	Select WEP (Basic) or WPA(2)/WPA(2)-PSK (More Secure) to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as the Router. When you select to use a security, additional options appears in this screen. If you select Open (No Security) , the Router allows any client to associate with this network without any data encryption or authentication.

7.1.1 No Security

Select the Security Mode to **Open** and **No Security** to allow wireless stations to communicate with the access points without any data encryption or authentication.

- ⓘ If you do not enable any wireless security on your Router, your network is accessible to any wireless networking device that is within range.

Figure 7 Wireless 2.4GHz > General: No Security



7.1.2 Basic (WEP Encryption)

If you want to use WEP encryption for the wireless LAN, select **WEP** in the **Security Mode** field.

Figure 8 Wireless 2.4 > General: Basic (WEP)

Security Level

Security Mode :

No Security **Basic** More Secure (Recommended)

Security Mode : WEP

Generate password automatically

Enter 5 ASCII characters or 10 hexadecimal digits (a-f, A-F, and 0-9). Spaces and underscores are not allowed.

Password

WEP Encryption :

Table 6 Wireless 2.4 > General: Basic (WEP)

LABEL	DESCRIPTION
Security Level	Select WEP to enable WEP data encryption.
Generate password automatically	Select this option to have the Router automatically generate a password.
Password	The password (WEP key) is used to encrypt data. Both the Router and the wireless stations must use the same password (WEP key) for data transmission.
WEP Encryption	Select 64Bits or 128Bits . This is the length of the security key that the network is going to use.

7.1.3 More Secure (WPA(2))

Select **WPA** or **WPA2** from the **Security Mode** field.

Figure 9 Wireless 2.4GHz > General: More Secure: WPA(2)

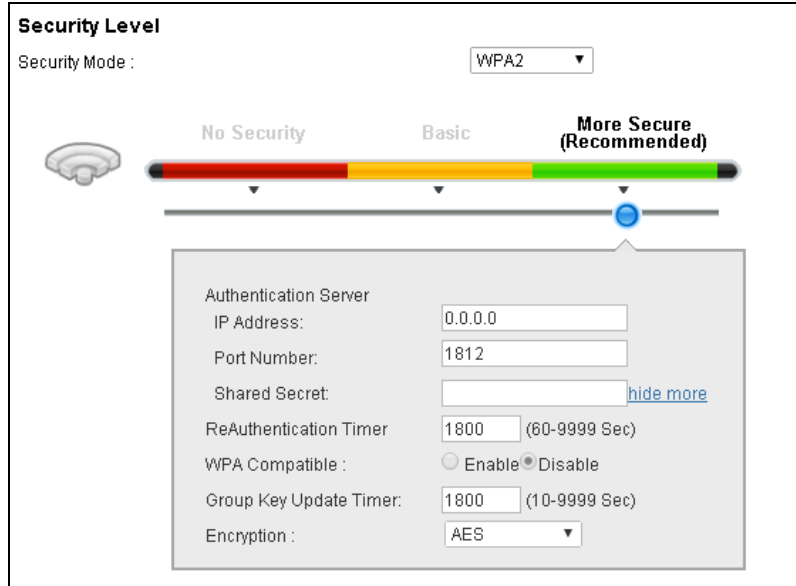


Table 7 Wireless 2.4GHz > General: More Secure: WPA(2)

LABEL	DESCRIPTION
Security Mode	Select WPA or WPA2 as the security mode.
IP Address	Enter the IP address of the external authentication server.
Port Number	Enter the port number of the external authentication server. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password as the key to be shared between the external authentication server and the Router. The key must be the same on the external authentication server and your Router. The key is not sent over the network.
more../hide more	Click more... to show more fields in this section. Click hide more to hide them.
ReAuthentication Timer	Specify how often wireless stations have to resend user names and passwords in order to stay connected. The default value is 0, which means the reauthentication off. Nota: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.

Table 7 Wireless 2.4GHz > General: More Secure: WPA(2) (continued)

LABEL	DESCRIPTION
WPA Compatible	This field is only available for WPA2 . Select this if you want the Router to support WPA and WPA2 simultaneously.
Group Key Update Timer	This is the rate at which the RADIUS server sends a new group key out to all clients. If the value is set to "0", the update timer function is disabled.
Encryption	Select TKIP to enable Temporal Key Integrity Protocol (TKIP) security on your wireless network. Select AES to enable Advanced Encryption System (AES) security on your wireless network. AES provides superior security to TKIP. Select TKIPAESMIX to have both types of security.

7.1.4 More Secure (WPA(2)-PSK)

The WPA2-PSK security mode is a newer, more robust version of the WPA encryption standard. It offers better security.

Select **WPA-PSK** or **WPA2-PSK** from the **Security Mode** field.

Figure 10 Wireless 2.4GHz > General: More Secure: WPA(2)-PSK

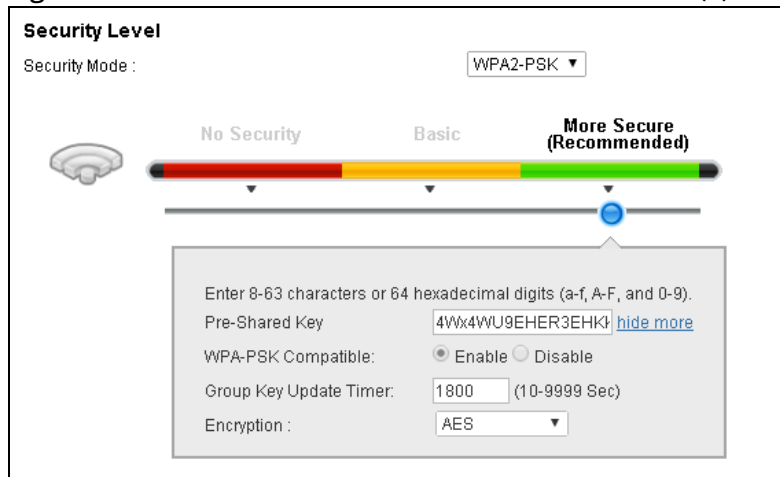


Table 8 Wireless 2.4GHz > General: WPA(2)-PSK

LABEL	DESCRIPTION
Security Mode	Select WPA-PSK or WPA2-PSK as the security mode.
Pre-Shared Key	Enter a pre-shared key.
more.../hide more	Click more... to show more fields in this section. Click hide more to hide them.

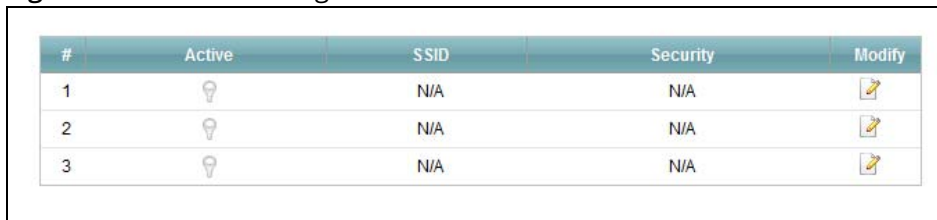
Table 8 Wireless 2.4GHz > General: WPA(2)-PSK (continued)

LABEL	DESCRIPTION
WPA-PSK Compatible	This appears when you choose WPA-PSK2 as the Security Mode . Enable this to allow wireless devices using WPA-PSK security mode to connect to your Router. The Router supports WPA-PSK and WPA2-PSK simultaneously.
Group Key Update Timer	This is the rate at which the RADIUS server sends a new group key out to all clients.
Encryption	Select TKIP to enable Temporal Key Integrity Protocol (TKIP) security on your wireless network. Select AES to enable Advanced Encryption System (AES) security on your wireless network. AES provides superior security to TKIP. Select TKIPAESMIX to have both types of security.

7.2 More AP Screen

This screen allows you to enable and configure multiple Basic Service Sets (BSSs) on the Router. Click **Network Setting > Wireless 2.4GHz > More AP**.

Figure 11 Network Setting > Wireless 2.4GHz> More AP









#	Active	SSID	Security	Modify
1		N/A	N/A	
2		N/A	N/A	
3		N/A	N/A	

Table 9 Network Setting > Wireless 2.4GHz > More AP

LABEL	DESCRIPTION
Active	This field indicates whether this SSID is active. A yellow bulb signifies that this SSID is active. A gray bulb signifies that this SSID is not active.
SSID	This field displays the name of the wireless profile on the network.
Security	This field indicates the security mode of the SSID profile.
Modify	Click the Edit icon to configure the SSID profile.

7.2.1 Edit More AP

Use this screen to edit an SSID profile. Click the **Edit** icon next to an SSID in the **More AP** screen. The following screen displays.

Figure 12 Wireless 2.4GHz > More AP: Edit

Table 10 Wireless 2.4GHz > More AP: Edit

LABEL	DESCRIPTION
2.4GHz Wireless	Select Enable Wireless LAN to activate the wireless LAN.
Wireless Network Name (SSID)	Enter a descriptive name for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Client Isolation	Select this to keep the wireless clients in this SSID from communicating with each other directly through the Router.
MBSSID/LAN Isolation	Select this to keep the wireless clients in this SSID from communicating with clients in other SSIDs or wired LAN devices through the Router. Select both Client Isolation and MBSSID/LAN Isolation to allow this SSID's wireless clients to only connect to the Internet through the Router.
Security Mode	Select the security mode on this wireless network. See Section 7.1.1 on page 46 through Section 7.1.3 on page 48 for more details about wireless security modes.


7.3 MAC Authentication Screen

Use this screen to configure the Router to give exclusive access to specific devices (**Allow**) or exclude specific devices from accessing the Router (**Deny**).

Use this screen to view your Router's MAC filter settings and add new MAC filter rules. Click **Network Setting > Wireless 2.4GHz > MAC Authentication**.

Figure 13 Network Setting > Wireless 2.4GHz > MAC Authentication


Table 11 Network Setting > Wireless 2.4GHz > MAC Authentication

LABEL	DESCRIPTION
SSID	Select the SSID for which you want to configure MAC filter settings.
MAC Restrict Mode	<p>Define the filter action for the list of MAC addresses in the MAC Address table.</p> <p>Select Disable to turn off MAC filtering.</p> <p>Select Allow to permit access to the Router. MAC addresses not listed will be denied access to the Router.</p> <p>Select Deny to block access to the Router. MAC addresses not listed will be allowed to access the Router.</p>
Add new MAC address	<p>Click this and enter a new MAC address entry to add to the MAC filter list.</p> 
MAC Address	This is the MAC addresses of the wireless devices that are allowed or denied access to the Router.
Modify	Click the Delete icon to delete the entry.

7.4 The WPS Screen

Use this screen to configure WiFi Protected Setup (WPS) on your Router.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Set up each WPS connection between two devices. Both devices must support WPS.

-  The Router applies the security settings of the **SSID1** profile (see [Section 7.1 on page 44](#)). If you want to use the WPS feature, make sure you have set the security mode of **SSID1** to WPA2-PSK or WPA-PSK/WPA2-PSK mixed or no security.




Click **Network Setting > Wireless 2.4GHz > WPS**. Select **Enable** and click **Apply** to activate the WPS function. Then you can configure the WPS settings in this screen.

Figure 14 Network Setting > Wireless 2.4GHz > WPS

General

WPS : Enable Disable (settings are invalid when disabled)

Add a new device with WPS Method

<p> Method 1 PBC</p> <p>Step 1. Click WPS button </p> <p>Step 2. Press the WPS button on your new wireless client device within 120 seconds</p>	<p> Method 2 PIN</p> <p>Step 1. Enter the PIN of your new wireless client device and then click <input type="text"/> <input type="button" value="Register"/> <input type="button" value="Register"/></p> <p>Step 2. Press the WPS button on your new wireless client device within 120 seconds</p>
--	---

WPS Configuration Summary

AP PIN : 11455042

Lock Status : Unlocked

802.11 Mode : 802.11b+g+n

SSID : MOVISTAR_1120

Security : WPA-PSK/WPA2-PSK

Pre-Shared Key : 4Wx4WU9EHER3EHKK9993

Note:

- If you enable WPS, it will turn on UPnP service automatically.
- This feature is available only when WPA2-PSK, WPA-PSK/WPA2-PSK or No Security mode is configured.

Table 12 Network Setting > Wireless 2.4GHz > WPS

LABEL	DESCRIPTION
WPS	Select Enable and click Apply to activate WPS on the Router.
Add a new device with WPS Method - These fields display after you enable WPS and click Apply .	

Table 12 Network Setting > Wireless 2.4GHz > WPS (continued)

LABEL	DESCRIPTION
Method 1 PBC	Use this section to set up a WPS wireless network using Push Button Configuration (PBC).
WPS	<p>Click this button to add another WPS-enabled wireless device (within wireless range of the Router) to your wireless network. This button may either be a physical button on the outside of device, or a menu button similar to the WPS button on this screen.</p> <p>Nota: You must press the other wireless device's WPS button within two minutes of pressing this button.</p>
Method 2 PIN	Use this section to set up a WPS wireless network by entering the PIN (Personal Identification Number) of the client into the Router.
Register	<p>Enter the PIN of the device that you are setting up a WPS connection with and click Register to authenticate and add the wireless device to your wireless network.</p> <p>You can find the PIN either on the outside of the device, or by checking the device's settings.</p> <p>Nota: You must also activate WPS on that device within two minutes to have it present its PIN to the Router.</p>
AP PIN	<p>The PIN of the Router is shown here. Enter this PIN in the configuration utility of the device you want to connect to using WPS.</p> <p>The PIN is not necessary when you use WPS push-button method.</p> <p>Click the Generate New PIN button to have the Router create a new PIN.</p>
Lock Status	<p>This displays Configured when the Router has connected to a wireless network using WPS or WPS is enabled and wireless or wireless security settings have been changed. The current wireless and wireless security settings also appear in the screen.</p> <p>This displays Not Configured when there is no wireless or wireless security changes on the Router or you click Release Configuration to remove the configured wireless and wireless security settings.</p>
Release Configuration	<p>This button is available when the WPS status is Configured.</p> <p>Click this button to remove all configured wireless and wireless security settings for WPS connections on the Router.</p>
802.11 Mode	This is the 802.11 mode used. Only compliant WLAN devices can associate with the Router.
SSID	This is the name of the wireless network.
Security	This is the type of wireless security employed by the network.
Pre-Shared Key	This is the wireless LAN password.

7.5 The WDS Screen

The **WDS** screen allows you to configure the Router to connect to other APs wirelessly when WDS is enabled. Configure your WDSlinks between the Router and other wireless APs. You need to know the MAC address of the peer device. Once the security settings of peer sides match one another, the connection between devices is made. Click **Network Setting > Wireless 2.4GHz > WDS**.

- ❶ WDS security is independent of the security settings between the Router and any wireless clients.
- ❷ Not all APs support WDS links. Check your other AP's documentation.

Figure 15 Network Setting > Wireless 2.4GHz > WDS

WDS Security

TKIP (ZyAIR Series Compatible)

AES

#	Active	Remote Bridge MAC Address	PSK
1	<input type="checkbox"/>	00:00:00:00:00:00	
2	<input type="checkbox"/>	00:00:00:00:00:00	
3	<input type="checkbox"/>	00:00:00:00:00:00	
4	<input type="checkbox"/>	00:00:00:00:00:00	

Table 13 Network Setting > Wireless 2.4GHz > WDS

LABEL	DESCRIPTION
WDS Security	Select the type of the key used to encrypt data between APs. All the wireless APs (including the Router) must use the same pre-shared key for data transmission. The option is available only when you set the security mode to WPA(2) or WPA(2)-PSK in the Wireless > General screen.
TKIP	Select this to use TKIP (Temporal Key Integrity Protocol) encryption.
AES	Select this to use AES (Advanced Encryption Standard) encryption.
Active	Select this to activate the link between the Router and the peer device to which this entry refers. When you do not select the check box this link is down.
Remote Bridge MAC Address	Type the MAC address of the peer device in a valid MAC address format (six hexadecimal character pairs, for example 12:34:56:78:9a:bc).
PSK	Enter a Pre-Shared Key (PSK).

7.6 The WMM Screen

Use the **WMM** screen to enable or disable Wi-Fi MultiMedia (WMM) wireless networks for multimedia applications. Click **Network Setting > Wireless 2.4GHz > WMM**.

Figure 16 Network Setting > Wireless 2.4GHz > WMM



The screenshot shows a configuration window with a white background and a thin black border. On the left side, there are four lines of text, each starting with a checked checkbox: "Enable WMM of SSID1", "Enable WMM of SSID2", "Enable WMM of SSID3", and "Enable WMM of SSID4". On the right side, there are two buttons: "Apply" and "Undo", both with a light gray background and black text.

Table 14 Network Setting > Wireless 2.4GHz > WMM

LABEL	DESCRIPTION
Enable WMM of SSID1~4	This enables the Router to automatically give a service a priority level according to the ToS value in the IP header of packets it sends. WMM QoS gives high priority to voice and video, which makes them run more smoothly.

7.7 Scheduling Screen

Use the **Scheduling** screen to manage schedules that turn off wireless service for power saving purposes. Click **Network Setting > Wireless 2.4GHz > Scheduling**.

Figure 17 Network Setting > Wireless 2.4GHz > Scheduling

WLAN Power Off Scheduling : Enable Disable (settings are invalid when disabled)

AddNewRule

#	RuleName	Days	StartTime	EndTime	Modify
1	Night	M T W T F S S	22:00	23:59	

Note:
1.WLAN can be activated manually at any time.

Apply Undo

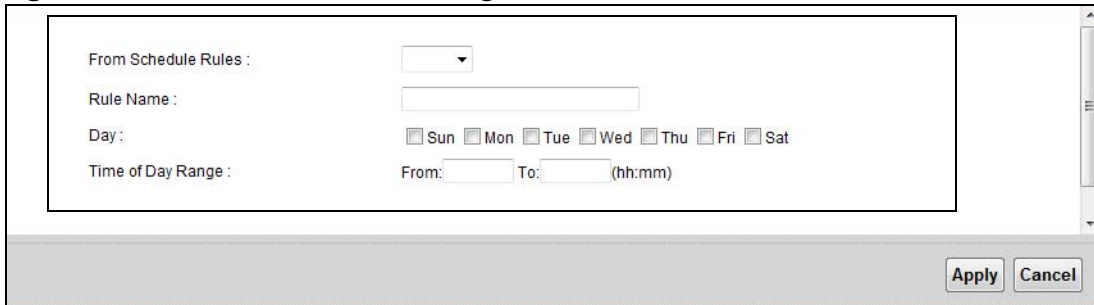
Table 15 Network Setting > Wireless 2.4GHz > Scheduling

LABEL	DESCRIPTION
WLAN Power Off Scheduling	Select Enable to activate wireless LAN scheduling on your Router.
Add New Rule	Click this to create a new wireless LAN scheduling rule.
Rule Name	This field shows the name configured for the scheduling rule.
Days	This field displays to which days of the week the schedule applies.
Start Time	This field displays the time (in 24-hour time format) the rule turns off the wireless LAN.
End Time	This field displays the time (in 24-hour time format) the rule turns the wireless LAN back on.
Modify	Click the Edit icon to configure the scheduling rule. Click the Delete icon to remove the scheduling rule.

7.7.1 Add or Edit Schedule

Use this screen to add or edit a wireless LAN schedule. In the **Scheduling** screen, click **Add New Rule** or the **Edit** icon next to an existing schedule.

Figure 18 Wireless 2.4GHz > Scheduling: Add New Rule



The screenshot shows a dialog box titled "Add New Rule" with the following fields and controls:

- From Schedule Rules :** A dropdown menu.
- Rule Name :** A text input field.
- Day :** A row of checkboxes for Sun, Mon, Tue, Wed, Thu, Fri, and Sat.
- Time of Day Range :** Two text input fields labeled "From:" and "To:" followed by "(hh:mm)".
- Buttons:** "Apply" and "Cancel" buttons at the bottom right.

Table 16 Wireless 2.4GHz > Scheduling: Add New Rule

LABEL	DESCRIPTION
From Schedule Rules	To create a new scheduling rule based off an existing one, select it here.
Rule Name	Specify a descriptive name to identify the scheduling rule.
Day	Select the days of the week to which to apply the schedule.
Time of Day Range	Enter the wireless LAN service start and end times in 24-hour time format.

7.8 Advanced Screen

Use the **Advanced** screen to configure advanced wireless settings. Click **Network Setting > Wireless 2.4GHz > Advanced**.

Figure 19 Network Setting > Wireless 2.4GHz > Advanced

Fragmentation Threshold: ((256 ~ 2346, even numbers only))

Output Power:

Preamble:

802.11 Mode:

Channel Width:

Table 17 Network Setting > Wireless 2.4GHz > Advanced

LABEL	DESCRIPTION
Fragmentation Threshold	Enter the maximum data fragment size that can be sent.
Output Power	Set the output power of the Router. If there is a high density of APs in an area, decrease the output power to reduce interference with other APs.
Preamble	Select a preamble type from the drop-down list menu.
802.11 Mode	<p>Select 802.11b to allow only IEEE 802.11b compliant WLAN devices to associate with the Router.</p> <p>Select 802.11g to allow only IEEE 802.11g compliant WLAN devices to associate with the Router.</p> <p>Select 802.11b+g to allow either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the Router. The transmission rate of your Router might be reduced.</p> <p>Select 802.11n to allow only IEEE 802.11n compliant WLAN devices to associate with the Router.</p> <p>Select 802.11g+n to allow either IEEE 802.11g or IEEE 802.11n compliant WLAN devices to associate with the Router. The transmission rate of the Router might be reduced when an 802.11g wireless client is associated with it.</p> <p>Select 802.11b+g+n to allow IEEE 802.11b, IEEE 802.11g or IEEE 802.11n compliant WLAN devices to associate with the Router. The transmission rate of the Router might be reduced when an 802.11b or 802.11g wireless client is associated with it.</p> <p>Nota: The transmission rate varies depending on the mode the wireless client uses to associate with the Router.</p>
Channel Width	Select the wireless channel width that the Router uses.

8.1 The LAN Setup Screen

Click **Network Setting > LAN** to open the **LAN Setup** screen. Use this screen to set the Local Area Network IP address and subnet mask of your Router and configure the DNS server information that the Router sends to the DHCP client devices on the LAN.

Figure 20 Network Setting > LAN > LAN Setup

LAN IP Setup

IP Address :

Subnet Mask :

RIP Version : Direction :

Multicast :

IGMP Snooping : Disabled Enabled

IGMP Quickleave : Disabled Enabled

DHCP Server State

DHCP : Disable Enable DHCP Relay

IP Addressing Values

IP Pool Starting Address :

Pool Size :

DHCP Conditional Serving Pool

State : Disabled Enabled

Gateway :

Subnet Mask :

Pool Start :

Pool End :

DNS Server 1 :

DNS Server 2 :

VendorID :

VendorID Mode : Exact Prefix Suffix Substring

VendorID Exclude : Disabled Enabled

Option240 State : Disabled Enabled

Option240 Value :

DHCP Server Lease Time

Lease Time : seconds

DNS Values

DNS Server 1 :

DNS Server 2 :

Table 18 Network Setting > LAN > LAN Setup

LABEL	DESCRIPTION
IP Address	Enter the LAN IP address you want to assign to your Router. The factory default is 192.168.1.1.
IP Subnet Mask	Type the subnet mask of your network. The factory default is 255.255.255.0. Your Router automatically computes the subnet mask based on the IP address you enter, so do not change this field unless you are instructed to do so.
RIP Version	Specify the RIP (Routing Information Protocol) version, which allows a router to exchange routing information with other routers.
Direction	Specify how much routing information the Router sends and receives on the subnet.
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group.
IGMP Snooping	Select Enabled to activate IGMP Snooping. This allows the Router to passively learn memberships in multicast groups. Otherwise, select Disabled to deactivate it.
IGMP Quickleave	Select Enabled to immediately removes a port when the Router detects an IGMP version 2 leave message on that port.
DHCP	<p>Select Enable to have the Router assign IP addresses, an IP default gateway and DNS servers to LAN computers and other devices that are DHCP clients.</p> <p>Select DHCP Relay to to have the Router forward DHCP requests to the DHCP server.</p> <p>If you select Disable, you need to manually configure the IP addresses of the computers and other devices on your LAN.</p> <p>You need to configure the following fields if you select Enable or DHCP Relay.</p>
DHCP Relay Server Address	If you set DHCP to DHCP Relay , enter the IP address pf the DHCP relay server.
IP Pool Starting Address	Specify the first of the contiguous addresses in the IP address pool.
Pool Size	Specify the size, or count of the IP address pool.
State	Select Enable to enable the DHCP conditional serving pool for IPTV set-top boxes. DHCP server will offer IP address from the conditional pool if the DHCP request sent from a set-top box contains the specific Vendor ID.
Gateway	Enter the IPTV server's IP address.
Subnet Mask	Enter the IPTV server's subnet mask.
Pool Start/End	Specify the first and last of the contiguous addresses in the IPTV server's IP address pool.
DNS Server 1/2	Enter the IPTV server's first/second DNS server IP address.
VendorID	Specify the IPTV's vendor ID.

Table 18 Network Setting > LAN > LAN Setup (continued)

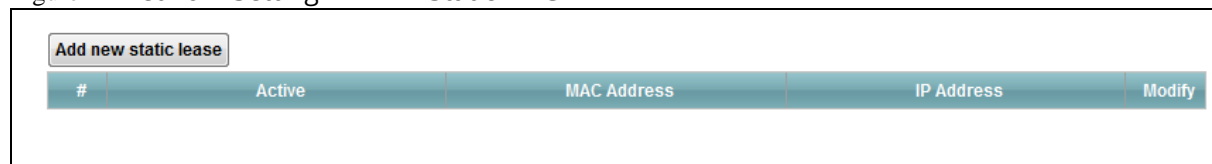
LABEL	DESCRIPTION
VendorID Mode	Specify the IPTV's vendor ID mode type.
VendorID Exclude	Specify if you want to enable vendor ID exclude.
Option240 State	Select Enabled to have the Router multimedia acquire values of option 240 when acquiring parameters of WAN2 interface.
Option240 Value	Enter the option 240 value.
Lease Time	Specify for how long it takes to assign an IP address to a LAN device before making it available for reassignment to other systems.
DNS Server 1/2	<p>Select Obtained From ISP if your ISP dynamically assigns DNS server information (and the Router's WAN IP address).</p> <p>Select User-Defined if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right.</p> <p>Select DNS Proxy to have the DHCP clients use the Router's own LAN IP address. The Router works as a DNS relay.</p> <p>Select None to not configure extra DNS servers.</p>

8.2 The Static DHCP Screen

Use the **Static DHCP** screen to change your Router's static DHCP settings. This table allows you to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses. Find out the MAC addresses of your network devices if you intend to add them to the **Static DHCP** screen.

Click **Network Setting > LAN > Static DHCP**.

Figure 21 Network Setting > LAN > Static DHCP



#	Active	MAC Address	IP Address	Modify
---	--------	-------------	------------	--------

Table 19 Network Setting > LAN > Static DHCP

LABEL	DESCRIPTION
Add new static lease	Click this to add a new static DHCP entry.
Active	This field displays whether the client is connected to the Router.

Table 19 Network Setting > LAN > Static DHCP (continued)

LABEL	DESCRIPTION
MAC Address	This field displays the MAC address of the client on the LAN.
IP Address	This field displays the IP address of the client on the LAN.
Modify	Click the Edit icon to edit the static DHCP settings. Click the Delete icon to remove it.

If you click **Add new static lease** in the **Static DHCP** screen, the following screen displays.

Figure 22 LAN > Static DHCP: Add

The screenshot shows a dialog box with a white background and a grey border. It contains two text input fields. The first is labeled 'MAC Address : ' and the second is labeled 'IP Address : '. Below the input fields, there is a grey bar containing two buttons: 'OK' and 'Cancel'.

Table 20 LAN > Static DHCP: Add

LABEL	DESCRIPTION
MAC Address	Enter the MAC address of a computer on your LAN.
IP Address	Enter the IP address that you want to assign to the computer on your LAN.

8.3 The IP Alias Screen

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The Router supports multiple logical LAN interfaces via its physical Ethernet interface with the Router itself as the gateway for the LAN network.

When you use IP alias, you can also configure firewall rules to control access to the LAN's logical network (subnet).

Use the **IP Alias** screen to change your Router's IP alias settings. Click **Network Setting > LAN > IP Alias**.

Figure 23 Network Setting > LAN > IP Alias

IP Alias

IP Alias : Enable Disable (settings are invalid when disabled)

IP Address :

IP Subnet Mask :

Table 21 Network Setting > LAN > IP Alias

LABEL	DESCRIPTION
IP Alias	Select Enable to configure another LAN network for the Router.
IP Address	Enter the second LAN IP address of your Router.
Subnet Mask	Your Router will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Router.

8.4 The UPnP Screen

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

Use the **UPnP** screen to enable the UPnP feature on your Router. Click **Network Setting > Home Networking > LAN > UPnP**.

Figure 24 Network Setting > LAN > UPnP

UPnP State

UPnP : Enable Disable

The following table describes the labels in this screen.

Table 22 Network Settings > LAN > UPnP

LABEL	DESCRIPTION
UPnP	Select Enable to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the Router's IP address (although you must still enter the password to access the web configurator).

8.5 The IPv6 LAN Setup Screen

Use the **IPv6 LAN Setup** screen to set the Local Area Network interface IPv6 settings. Click **Network Setting > LAN > IPv6 LAN Setup**.

Figure 25 Network Setting > LAN > IPv6 LAN Setup

The screenshot displays the IPv6 LAN Setup configuration screen, organized into several sections:

- IPv6 LAN Setup:**
 - IPv6 Enable
 - Link Local Address Enable
 - Link Local Address Type: Manual EUI64
 - IPv6 Address:
 - Prefix:
 - Lan Global Identifier Type: Manual EUI64
 - Lan Identifier:
 - IPv6 ULA Address Type: Auto Generate Manual
 - IPv6 ULA Address:
- LAN IPv6 Address Setting:**
 - Global Address Enable
 - Delegate prefix from WAN (Dropdown: PVCD)
 - Static
 - Static IPv6 Address Prefix:
 - Prefix length:
 - Preferred Lifetime:
 - Valid Lifetime:
 - LAN IPv6 Address Assign Setup:
 - LAN IPv6 DNS Assign Setup:
- DHCPv6:**
 - DHCPv6 Server: Disable Enable
 - Pool Start:
 - Pool End:
 - DNSv6 Mode: Proxy Relay Manual None
 - Primary DNS:
 - Secondary DNS:
 - Information refresh time:
- RADVD Setup:**
 - Send RA on
 - Advertisement interval option on
 - Hop limit:
 - Router Lifetime:
 - Router Preference:
 - Reachable Time (ms):
 - Retrans Timer (ms):
 - Max RA Interval:
 - Min RA Interval:
 - Delegate MTU from WAN
 - Manual
 - MTU:
 - DAD attempts:

At the bottom right, there are three buttons: **Apply**, **Undo**, and **Advanced Setup**.

Table 23 Network Setting > LAN > IPv6 LAN Setup

LABEL	DESCRIPTION
IPv6 Enable	Select this to enable the IPv6 feature on the Router.
Link Local Address Enable	Select this to enable the Link Local Address feature on the Router.
Link Local Address Type	Select Manual to manually enter a link local address. Select EUI64 to use the EUI-64 format to generate a link local address from the Ethernet MAC address.
IPv6 Address	If you selected Manual in the Link Local Address Type field, enter the LAN IPv6 address you want to assign to your Router.
Prefix	Enter the address prefix to specify how many most significant bits in an IPv6 address compose the network address.
Lan Global Identifier Type	Select Manual to manually enter a LAN Identifier as the interface ID to identify the LAN interface. The LAN Identifier is appended to the IPv6 address prefix to create the routable global IPv6 address. Select EUI64 to use the EUI-64 format to generate an interface ID from the Ethernet MAC address.
Lan Identifier	If you selected Manual , enter the LAN Identifier. The LAN identifier should be unique and 64 bits in hexadecimal form.
IPv6 ULA Address Type	A unique local address (ULA) is a unique IPv6 address for use in private networks but not routable in the global IPv6 Internet. Select Auto Generate to have the Router automatically generate a globally unique address for the LAN IPv6 address. Select Manual to enter a static IPv6 ULA address.
IPv6 ULA Address	If you select Manual in the IPv6 ULA Address Type field, enter a static IPv6 ULA address.
Global Address Enable	Select this to enable IPv6 global address.
Delegate prefix from WAN	Select this option to automatically obtain an IPv6 network prefix from the service provider or an uplink router.
Static	Select this option to configure a fixed IPv6 address for the Router's LAN IPv6 address.
Static IPv6 Address Prefix	If you select static IPv6 address, enter the IPv6 address prefix that the Device uses for the LAN IPv6 address.
Prefix length	If you select static IPv6 address, enter the IPv6 prefix length that the Device uses to generate the LAN IPv6 address.
Preferred Lifetime	Enter the preferred lifetime for the prefix.
Valid Lifetime	Enter the valid lifetime for the prefix.

Table 23 Network Setting > LAN > IPv6 LAN Setup (continued)

LABEL	DESCRIPTION
LAN IPv6 Address Assign Setup	<p>Select how you want to obtain an IPv6 address:</p> <ul style="list-style-type: none"> • Stateless: The Router uses IPv6 stateless autoconfiguration. RADVD (Router Advertisement Daemon) is enabled to have the Router send IPv6 prefix information in router advertisements periodically and in response to router solicitations. DHCPv6 server is disabled. • Stateful: The Router uses IPv6 stateful autoconfiguration. The DHCPv6 server is enabled to have the Router act as a DHCPv6 server and pass IPv6 addresses to DHCPv6 clients. • Stateless and Stateful: The Router uses both IPv6 stateless and stateful autoconfiguration. The LAN IPv6 clients can obtain IPv6 addresses either through router advertisements or through DHCPv6.
LAN IPv6 DNS Assign Setup	<p>Select how the Router provides DNS server and domain name information to the clients:</p> <ul style="list-style-type: none"> • Stateless: The Router uses IPv6 stateless autoconfiguration. RADVD (Router Advertisement Daemon) is enabled to have the Router send IPv6 prefix information in router advertisements periodically and in response to router solicitations. DHCPv6 server is disabled. • Stateful: The Router uses IPv6 stateful autoconfiguration. The DHCPv6 server is enabled to have the Router act as a DHCPv6 server and pass IPv6 addresses to DHCPv6 clients. • Stateless and Stateful: The Router uses both IPv6 stateless and stateful autoconfiguration. The LAN IPv6 clients can obtain IPv6 addresses either through router advertisements or through DHCPv6.
DHCPv6 Server	<p>Select Enable to have the Router act as a DHCPv6 server and pass IPv6 addresses, DNS server and domain name information to DHCPv6 clients.</p>
Pool Start/End	<p>Specify the first/last IPv6 address in the pool of addresses that can be assigned to DHCPv6 clients.</p>
DNSv6 Mode	<p>Select the DNS role (Proxy or Relay) that you want the Router to act in the IPv6 LAN network. Alternatively, select Manual and specify the DNS servers' IPv6 address in the fields below. Select None to disable this feature.</p>
Primary/Secondary DNS	<p>This field is available if you select Manual as the DNSv6 mode. Enter the first/second DNS server IPv6 address the Router passes to the DHCP clients.</p>
DNS Query Mode	<p>Select how the Router handles clients' DNS information requests.</p> <ul style="list-style-type: none"> • IPv4 DNS Server First: The Router forwards the requests to the IPv4 DNS server first and then the IPv6 DNS server. Then it sends clients the first DNS information it receives. • IPv6 DNS Server First: The Router forwards the requests to the IPv6 DNS server first and then the IPv4 DNS server. Then it sends clients the first DNS information it receives. • IPv4 DNS Server Only: The Router forwards the requests to the IPv4 DNS server and sends clients the DNS information it receives. • IPv6 DNS Server Only: The Router forwards the requests to the IPv6 DNS server and sends clients the DNS information it receives.
Information Refresh Time	<p>Enter the number of seconds a DHCPv6 client should wait before refreshing information retrieved from DHCPv6.</p>
Advanced Setup	<p>Click this to show the RADVD Setup section. Click the button again to close it.</p>

Table 23 Network Setting > LAN > IPv6 LAN Setup (continued)

LABEL	DESCRIPTION
Send RA on	<p>Select this to have the Router send RA (Router Advertisement) messages to the LAN hosts.</p> <p>Note: The LAN hosts neither generate global IPv6 addresses nor communicate with other networks if you disable this feature.</p>
Advertisement interval option on	<p>Select this to have the RA messages the Router sends specify the allowed interval between RA messages.</p>
Hop Limit	<p>Enter the maximum number of network segments that a packet can cross before reaching the destination. When forwarding an IPv6 packet, IPv6 routers are required to decrease the Hop Limit by 1 and to discard the IPv6 packet when the Hop Limit is 0.</p>
Router Lifetime	<p>Enter the time in seconds that hosts should consider the Router to be the default router.</p>
Router Preference	<p>Select the router preference for the Router. The Router sends this preference in the router advertisements to tell hosts what preference they should use for the Router. This helps hosts to choose their default router especially when there are multiple IPv6 router in the network.</p> <p>Note: Make sure the hosts also support router preference to make this function work.</p>
Reachable Time (ms)	<p>Enter the time in milliseconds that can elapse before a neighbor is detected.</p>
Retrans Time (ms)	<p>Enter the time in milliseconds between neighbor solicitation packet retransmissions.</p>
Max RA Interval	<p>Enter the maximum time between RA messages.</p>
Min RA Interval	<p>Enter the minimum time between RA messages.</p>
Delegate MTU from WAN	<p>Select this to have the Router obtain the MTU setting from the service provider or uplink router.</p>
Manual	<p>Select this to specify the MTU manually.</p>
MTU	<p>Enter the MTU value.</p>
DAD Attempts	<p>Specify the number of DAD (Duplicate Address Detection) attempts before an IPv6 address is assigned to the Router LAN interface.</p>

9.1 Configuring Static Route

Use the **Static Route** screen to view and configure IP static routes on the Router. Click **Network Setting > Routing** to open the **Static Route** screen.

Figure 26 Network Setting > Routing > Static Route

Add New Static Route						
#	Destination IP	Gateway	Subnet Mask	Metric	Modify	
1	172.28.0.0	10.69.0.1	255.252.0.0	1		
2	201.0.52.0	10.69.0.1	255.255.254.0	1		
3	200.161.71.41	10.69.0.1	255.255.255.255	1		
4	200.161.71.42	10.69.0.1	255.255.255.255	1		
5	200.161.71.46	10.69.0.1	255.255.255.255	1		
6	200.161.71.47	10.69.0.1	255.255.255.255	1		
7	200.161.71.48	10.69.0.1	255.255.255.255	1		
8	200.161.71.49	10.69.0.1	255.255.255.255	1		

Table 24 Network Setting > Routing > Static Route

LABEL	DESCRIPTION
Add New Static Route	Click this to set up a new static route on the Router.
Destination IP	This is the IP network address of the final destination. Routing is always based on network number.
Gateway	This is the IP address of the gateway.
Subnet Mask	This is the IP network subnet mask of the final destination.
Metric	This is the "cost" of transmission for routing purposes.
Modify	Click the Edit icon to go to the screen where you can set up a static route on the Router. Click the Delete icon to remove a static route from the Router.

9.1.1 Add/Edit Static Route

Click **Add New Static Route** in the **Static Route** screen or click the **Edit** icon next to a rule. Use this screen to configure a static route.

Figure 27 Routing > Static Route: Add/Edit

Table 25 Routing > Static Route: Add/Edit

LABEL	DESCRIPTION
Destination IP Address	Enter the IP network address of the final destination.
IP Subnet Mask	Enter the IP subnet mask.
Gateway IP Address	Enter the IP address of the next-hop gateway which helps forward packets to their destinations.
Metric	Enter the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly-connected networks.

9.2 IPv6 Static Route

Use the **IPv6 Static Route** screen to view the IPv6 static route rules. Click **Network Setting > Routing > IPv6 Static Route**.

Figure 28 Network Setting > Routing > IPv6 Static Route

Table 26 Network Setting > Routing > IPv6 Static Route

LABEL	DESCRIPTION
Add New Static Route	Click this to configure a new IPv6 static route.
Destination IP	This is the IP network address of the final destination.
Prefix length	This is the bit number of the IPv6 subnet mask.
Gateway	This is the IPv6 address of the gateway.
Device	This specifies the LAN or WAN PVC.
Modify	Click the Edit icon to go to the screen where you can set up a static route on the Router. Click the Delete icon to remove a static route from the Router.

9.2.1 Add/Edit IPv6 Static Route

Click **Add New Static Route** in the **IPv6 Static Route** screen or click the **Edit** icon next to a rule. Use this screen to configure an IPv6 static route.

Figure 29 Routing > IPv6 Static Route: Add/Edit

The screenshot shows a configuration window with the following fields:

- Destination IPv6 Address :
- IPv6 Prefix Length :
- Gateway IPv6 Address :
- PVC IPv6 Address :

At the bottom right, there are **OK** and **Cancel** buttons.

Table 27 Routing > IPv6 Static Route: Add/Edit

LABEL	DESCRIPTION
Destination IPv6 Address	Enter the IPv6 network address of the final destination.
IPv6 Prefix Length	Enter the address prefix to specify how many most significant bits compose the network address.
Gateway IPv6 Address	Enter the IPv6 address of the next-hop gateway which helps forward packets to their destinations.
PVC IPv6 Address	Select the interface through which the traffic is routed.

9.3 The DNS Route Screen

A DNS route forwards DNS queries for a specific domain name through a specific WAN interface to its DNS server. The **DNS Route** screens let you view and configure DNS routes on the Router. Click **Network Setting > Routing > DNS Route**.

Figure 30 Network Setting > Routing > DNS Route

#	Domain Name	Subnet Mask	Interface	Modify
<p>Note : Maximum of 20 entries could be added.</p>				

Table 28 Network Setting > Routing > DNS Route

LABEL	DESCRIPTION
Add New DNS Route	Click this to create a new DNS route.
Domain Name	This is the domain name to which the DNS route applies.
Subnet Mask	This parameter specifies the IP network subnet mask.
Interface	This is the WAN interface through which the matched DNS request is routed.
Modify	Click the Edit icon to configure a DNS route on the Router. Click the Delete icon to remove a DNS route from the Router.

9.3.1 Add/Edit DNS Route

Click **Add New DNS route** in the **DNS Route** screen or the **Edit** icon next to an existing DNS route. Use this screen to configure the required information for a DNS route.

Figure 31 Routing > DNS Route: Add/Edit

Domain Name :

Subnet Mask :

Interface :

OK Cancel

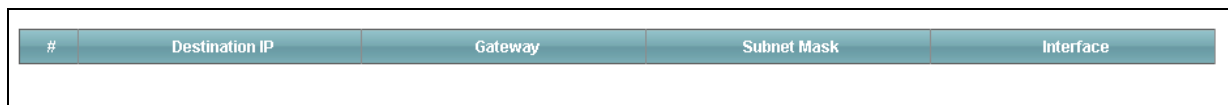
Table 29 Network Setting > Routing > DNS Route: Add/Edit

LABEL	DESCRIPTION
Domain Name	Enter the domain name you want to resolve. You can use the wildcard character, an "*" (asterisk) as the left most part of a domain name, such as *.example.com. The Router forwards DNS queries for any domain name ending in example.com to the WAN interface specified in this route.
IP Subnet Mask	Enter the subnet mask of the network for which to use the DNS route.
Interface	Select a WAN interface through which the matched DNS query is sent. You must have the WAN interface(s) already configured in the WAN screen.

9.4 The Current Route Screen

Use the **Current Route** screen to view a table of the current static and dynamic routes on the Router. Click **Network Setting > Routing > Current Route**.

Figure 32 Network Setting > Routing > Current Route



#	Destination IP	Gateway	Subnet Mask	Interface
---	----------------	---------	-------------	-----------

Table 30 Network Setting > Routing > Current Route

LABEL	DESCRIPTION
Destination IP	This is the IP network address of the final destination.
Gateway	This is the IP address of the gateway.
Subnet Mask	This is the IP network subnet mask of the final destination.
Interface	This is the WAN interface through which the matched traffic is routed.

10.1 Overview

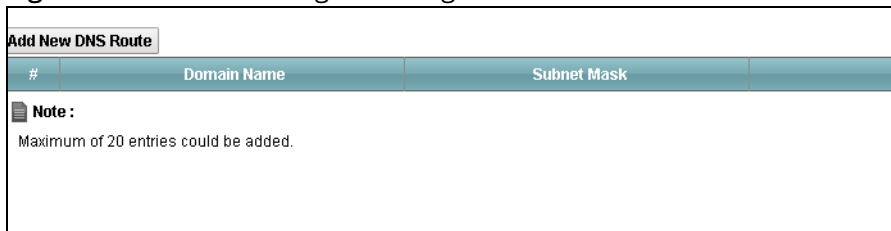
DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it.

In addition to the system DNS servers, each WAN interface (service) is set to have its own static or dynamic DNS server list. You can configure a DNS static route to forward DNS queries for certain domain names through a specific WAN interface to its DNS servers. The Router uses a system DNS server (in the order you specify in the **Broadband** screen) to resolve domain names that do not match any DNS routing entry. After the Router receives a DNS reply from a DNS server, it creates a new entry for the resolved IP address in the routing table.

10.2 The DNS Route Screen

The **DNS Route** screens let you view and configure DNS routes on the Router. Click **Network Setting > Routing > DNS Route** to open the **DNS Route** screen. A DNS route forwards DNS queries for a specific domain name through a specific WAN interface to its DNS server.

Figure 33 Network Setting > Routing > DNS Route



The following table describes the labels in this screen.

Table 31 Network Setting > Routing > DNS Route

LABEL	DESCRIPTION
Add new DNS route	Click this to create a new entry.
#	This is the number of an individual DNS route.

Table 31 Network Setting > Routing > DNS Route (continued)

LABEL	DESCRIPTION
Domain Name	This is the domain name to which the DNS route applies.
Subnet Mask	This parameter specifies the IP network subnet mask.
Interface	This is the WAN interface through which the matched DNS request is routed.
Modify	Click the Edit icon to configure a DNS route on the Router. Click the Delete icon to remove a DNS route from the Router.

10.2.1 Add/Edit DNS Route

Click **Add New DNS route** in the **DNS Route** screen or the **Edit** icon next to an existing DNS route. Use this screen to configure the required information for a DNS route.

Figure 34 Network Setting > Routing > DNS Route: Add/Edit

The screenshot shows a configuration window with the following fields:

- Domain Name :
- Subnet Mask :
- Interface :

At the bottom right, there are two buttons: **OK** and **Cancel**.

The following table describes the labels in this screen.

Table 32 Network Setting > Routing > DNS Route: Add/Edit

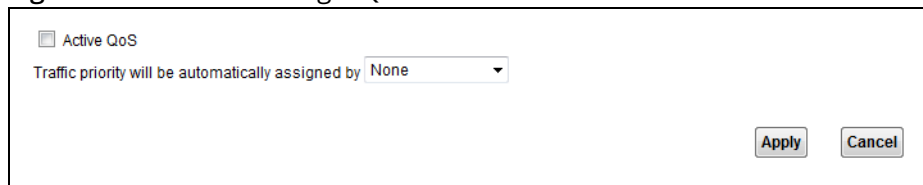
LABEL	DESCRIPTION
Domain Name	Enter the domain name you want to resolve. You can use the wildcard character, an "*" (asterisk) as the left most part of a domain name, such as *.example.com. The Router forwards DNS queries for any domain name ending in example.com to the WAN interface specified in this route.
IP Subnet Mask	Type the subnet mask of the network for which to use the DNS route in dotted decimal notation, for example 255.255.255.255.
WAN Interface	Select a WAN interface through which the matched DNS query is sent. You must have the WAN interface(s) already configured in the Broadband screen.
OK	Click this to save your changes.
Cancel	Click this to exit this screen without saving.

11.1 The QoS General Screen

Use this screen to enable or disable QoS, set the bandwidth, and select to have the Router automatically assign priority to upstream traffic according to the IP precedence or packet length.

Click **Network Setting > QoS** to open the **General** screen.

Figure 35 Network Setting > QoS > General



Active QoS
Traffic priority will be automatically assigned by None

Apply Cancel

Table 33 Network Setting > QoS > General

LABEL	DESCRIPTION
Active QoS	Select the check box to turn on QoS to improve your network performance. You can give priority to traffic that the Router forwards out through the WAN interface. Give high priority to voice and video to make them run more smoothly. Similarly, give low priority to many large file downloads so that they do not reduce the quality of other applications.
Traffic priority will be automatically assigned by	Select how the Router assigns priorities to various upstream traffic flows. <ul style="list-style-type: none">• None: Disables auto priority mapping and has the Router put packets into the queues according to your classification rules. Traffic which does not match any of the classification rules is mapped into the default queue with the lowest priority.• Ethernet Priority: Automatically assign priority based on the IEEE 802.1p priority level.• IP Precedence: Automatically assign priority based on the first three bits of the TOS field in the IP header.• Packet Length: Automatically assign priority based on the packet size. Smaller packets get higher priority since control, signaling, VoIP, internet gaming, or other real-time packets are usually small while larger packets are usually best effort data packets like file transfers.

11.2 The Queue Setup Screen

Use the **Queue Setup** screen to configure QoS queue assignment. Click **Network Setting > QoS > Queue Setup**.

Figure 36 Network Setting > QoS > Queue Setup













Index	Status	Name	Interface	Priority	Weight	Rate Limit	Modify
1		Default_QoS	WAN	1	1	N/A	 
2		N/A	N/A	N/A	N/A	N/A N/A	 
3		N/A	N/A	N/A	N/A	N/A N/A	 
4		N/A	N/A	N/A	N/A	N/A N/A	 

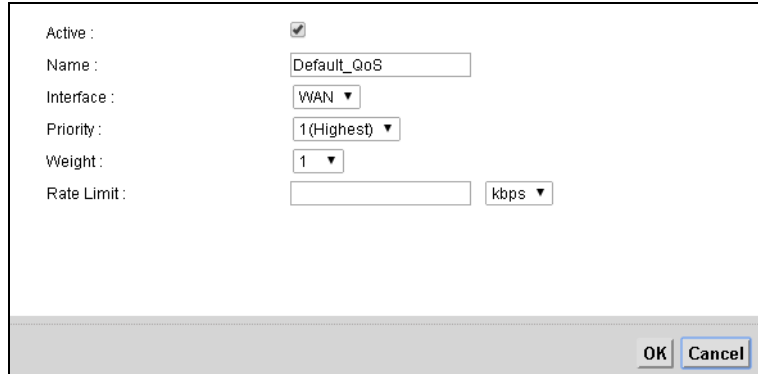
Table 34 Network Setting > QoS > Queue Setup

LABEL	DESCRIPTION
Status	This indicates whether the queue is active or not. A yellow bulb signifies that this queue is active. A gray bulb signifies that this queue is not active.
Name	This shows the descriptive name of this queue.
Interface	This shows the name of the Router's interface through which traffic in this queue passes.
Priority	This shows the priority of this queue.
Weight	This shows the weight of this queue.
Rate Limit	This shows the maximum transmission rate allowed for traffic on this queue.
Modify	Click the Edit icon to edit the queue. Click the Delete icon to delete an existing queue. Note that subsequent rules move up by one when you take this action.

11.2.1 Edit a QoS Queue

Use this screen to configure a queue. Click the **Edit** icon next to a QoS queue.

Figure 37 QoS > Queue Setup: Edit



The screenshot shows a configuration window for a QoS queue. It contains the following fields and controls:

- Active:** A checked checkbox.
- Name:** A text input field containing "Default_QoS".
- Interface:** A dropdown menu showing "WAN".
- Priority:** A dropdown menu showing "1 (Highest)".
- Weight:** A dropdown menu showing "1".
- Rate Limit:** An empty text input field followed by a dropdown menu showing "kbps".
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

Table 35 QoS > Queue Setup: Edit

LABEL	DESCRIPTION
Active	Select to enable or disable this queue.
Name	Enter the descriptive name of this queue.
Interface	Select the interface of this queue.
Priority	Select the priority level of this queue. The lower the number, the higher the priority level. Traffic assigned to higher priority queues gets through faster while traffic in lower priority queues is dropped if the network is congested.
Weight	Select the weight of this queue. If two queues have the same priority level, the Router divides the bandwidth across the queues according to their weights. Queues with larger weights get more bandwidth than queues with smaller weights.
Rate Limit	Specify the maximum transmission rate (in Kbps or %) allowed for traffic on this queue.

11.3 The Class Setup Screen

Use this screen to add, edit or delete QoS classifiers. A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming interface.

You can give different priorities to traffic that the Router forwards out through the WAN interface. Give high priority to voice and video to make them run more smoothly. Similarly, give low priority to many large file downloads so that they do not reduce the quality of other applications.

Click **Network Setting > QoS > Class Setup** to open the following screen.

Figure 38 Network Setting > QoS > Class Setup

Add new Classifier								
Order	Index	Status	From Interface	Classification Criteria	DSCP(Traffic Class) Mark	802.1P/1Q Mark	To Queue	Modify
1	0			Destination IP : 81.47.224.1/255.255.252.0			1	
2	1			Destination IP : 80.58.63.192/255.255.255.192			1	

Table 36 Network Setting > QoS > Class Setup

LABEL	DESCRIPTION
Add new Classifier	Click this to create a new classifier.
Order	This is the order of the classifier.
Index	This is the index number of the classifier.
Status	This indicates whether the classifier is active or not. A yellow bulb signifies that this classifier is active. A gray bulb signifies that this classifier is not active.
From Interface	If the classifier applies to traffic coming in through a specific interface, it displays here.
Classification Criteria	This shows criteria specified in this classifier, for example the interface from which traffic of this class should come and the source MAC address of traffic that matches this classifier.
DSCP (Traffic Class) Mark	This is the DSCP number added to traffic of this classifier.
802.1P/1Q Mark	This is the IEEE 802.1p priority level assigned to traffic of this classifier.
To Queue	This is the name of the queue in which traffic of this classifier is put.
Modify	Click the Edit icon to edit the classifier. Click the Delete icon to delete an existing classifier. Note that subsequent rules move up by one when you take this action.

11.3.1 Add/Edit QoS Class

Click **Add new Classifier** in the **Class Setup** screen or the **Edit** icon next to an existing classifier to configure it.

Figure 39 QoS > Class Setup: Add/Edit

The screenshot shows the 'QoS > Class Setup: Add/Edit' configuration window. It is organized into four main sections:

- Rule Index:** A dropdown menu at the top.
- Class Configuration:**
 - Active
 - Ether Type: IPv4 (0x0800)
 - Interface: From LAN
 - To Queue: (empty dropdown)
- Criteria Configuration:**

Use the configurations below to specify the characteristics of a data flow need to be managed by this QoS rule

 - Basic:** From Interface: LAN1 LAN2 LAN3 LAN4 ra0 ra1 ra2 ra3
 - Source:**
 - IP Address: [] IP Subnet Mask: [] Exclude
 - Port Range: [] ~ [] Exclude
 - MAC Address: [] MAC Mask: [] Exclude
 - Destination:**
 - IP Address: [] IP Subnet Mask: [] Exclude
 - Port Range: [] ~ [] Exclude
 - MAC Address: [] MAC Mask: [] Exclude
 - Others:**
 - Service: []
 - IP Protocol: [] Exclude
 - TCP ACK: Exclude
 - DHCP: [] [] Exclude
 - Packet Length: [] ~ [] Exclude
 - IPP/DS Field: IPP/TOS DSCP
 - IP Precedence Range: [] ~ [] Exclude
 - Type of Service: [] Exclude
 - DSCP Range(0 ~ 63): [] ~ [] Exclude
 - 802.1P: [] ~ [] Exclude
 - VLAN ID: [] ~ [] (Value Range: 1 ~ 4094) Exclude
- Action:**
 - Forward to: Unchange
 - IPP/DS Field: IPP/TOS DSCP
 - IP Precedence Mark: Unchange
 - Type Of Service Mark: Unchange
 - DSCP Mark(0 ~ 63): Unchange
 - 802.1Q Tag: Same
 - Ethernet Priority: []
 - VLAN ID: [] (Value Range: 1 ~ 4094)

Buttons: OK, Cancel

Table 37 QoS > Class Setup: Add/Edit

LABEL	DESCRIPTION
Rule Index	Select the (order) number of this rule.
Active	Select to enable this classifier.
Classification Order	Select an existing number for where you want to put this classifier to move the classifier to the number you selected after clicking Apply . Select Last to put this rule in the back of the classifier list.
Ether Type	Select a predefined application to configure a class for the matched traffic. If you select IPv4 (0x0800) , you also need to configure source or destination MAC address, IP address, DHCP options, DSCP value or the protocol type. If you select ARP (0x0806) (available when you set Interface to From LAN), you can configure source or destination MAC addresses. If you select 802.1Q (0x8100) (available when you set Interface to From LAN) you can configure an 802.1p priority level.
Interface	Select whether to apply this class to traffic from the LAN or from the WAN.
To Queue	Select a queue to apply to this class (available when you set Interface to From WAN). You should have configured a queue in the Queue Setup screen already.
From Interface	Select the interface from which the traffic class comes.
IP Address	Select the check box and enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address.
IP Subnet Mask	Enter the source subnet mask.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Port Range	If you select TCP or UDP in the IP Protocol field, select the check box and enter the port number(s) of the source.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
MAC Address	Select the check box and enter the source MAC address of the packet.
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
IP Address	Select the check box and enter the destination IP address in dotted decimal notation. A blank source IP address means any source IP address.
IP Subnet Mask	Enter the destination subnet mask.

Table 37 QoS > Class Setup: Add/Edit (continued)

LABEL	DESCRIPTION
Port Range	If you select TCP or UDP in the IP Protocol field, select the check box and enter the port number(s) of the source.
MAC Address	Select the check box and enter the destination MAC address of the packet.
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Service	Select the service classification of the traffic (FTP or SIP).
IP Protocol	This field is available only when you select IPv4 (0x0800) in the Ether Type field. Select this option and select the protocol (service type) from TCP or UDP . If you select User defined , enter the protocol (service type) number.
TCP ACK	This field is available only when you select IPv4 (0x0800) in the Ether Type field. If you select this option, the matched TCP packets must contain the ACK (Acknowledge) flag.
DHCP	<p>This field is available only when you select IPv4 (0x0800) in the Ether Type field, and UDP in the IP Protocol field.</p> <p>Select this option and select a DHCP option.</p> <p>If you select Vendor Class ID (DHCP Option 60), enter the Class ID of the matched traffic, such as the type of the hardware or firmware.</p> <p>If you select User Class ID (DHCP Option 77), enter the User Class Data, which is a string that identifies the user's category or application type in the matched DHCP packets.</p> <p>If you select ClientID (DHCP Option 61), enter the Type of the matched traffic and Client ID of the DHCP client.</p> <p>If you select VendorSpecificIntro (DHCP Option 125), enter the Enterprise Number of the software of the matched traffic and Vendor Class Data used by all the DHCP clients.</p>
Packet Length	This field is available only when you select IPv4 (0x0800) in the Ether Type field. Select this option and enter the minimum and maximum packet length (from 46 to 1504) in the fields provided.
IPP/DS Field	<p>Select IPP/TOS to specify an IP precedence range and type of services.</p> <p>Select DSCP to specify a DiffServ Code Point (DSCP) range.</p>
IP Precedence Range	Enter a range from 0 to 7 for IP precedence. 0 is the lowest priority and 7 is the highest.
Type of Service	<p>Select a type of service from the drop-down list box.</p> <p>Available options are: Normal service, Minimize delay, Maximize throughput, Maximize reliability and Minimize monetary cost.</p>

Table 37 QoS > Class Setup: Add/Edit (continued)

LABEL	DESCRIPTION
DSCP Range (0 ~ 63)	Select this option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.
802.1P	Select this option and select a priority level (between 0 and 7) from the drop-down list box. "0" is the lowest priority level and "7" is the highest.
VLAN ID	Select this option and enter the source VLAN ID in this field.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Forward To	Select the interface through which traffic that matches the rule is forwarded out. If you select Unchange , the Router forwards traffic of this class according to the default routing table. If traffic of this class comes from a WAN interface and is in a queue that forwards traffic through the LAN/WLAN interface, the Router ignores the setting here.
IPP/DS Field	Select IPP/TOS to specify an IP precedence range and type of services. Select DSCP to specify a DiffServ Code Point (DSCP) range.
IP Precedence Mark	Enter a range from 0 to 7 to re-assign IP precedence to matched traffic. 0 is the lowest priority and 7 is the highest.
Type Of Service Mark	Select a type of service to re-assign the priority level to matched traffic.
DSCP Mark(0~63)	This field is available only when you select IPv4 (0x0800) in the Ether Type field. If you select Mark , enter a DSCP value with which the Router replaces the DSCP field in the packets. If you select Unchange , the Router keep the DSCP field in the packets.
802.1Q Tag	If you select Remark , select a priority level (in the Ethernet Priority field) and enter a VLAN ID number (in the VLAN ID field) with which the Router replaces the IEEE 802.1p priority field and VLAN ID of the frames. If you select Remove , the Router deletes the VLAN ID of the frames before forwarding them out. If you select Add , the Router treat all matched traffic untagged and add a second priority level and VLAN ID that you specify in the Ethernet Priority and VLAN ID fields. If you select Same , the Router keep the Ethernet Priority and VLAN ID in the packets. To configure the Ethernet Priority, you can either select a priority number in the first drop-down list box (7 is the highest and 0 is the lowest priority) or select an application from the second drop-down list box which automatically maps to the corresponding priority number. (Key Net Traffic: 7; Voice: 6; Video: 5; IGMP: 4; Key Data: 3)
VLAN ID	Select this option and enter the source VLAN ID in this field.

11.4 The QoS Monitor Screen

To view the Router's QoS packet statistics, click **Network Setting > QoS > Monitor**.

Figure 40 Network Setting > QoS > Monitor



Table 38 Network Setting > QoS > Monitor

LABEL	DESCRIPTION
Refresh Interval	Enter how often you want the Router to update this screen and click Set Interval . Click Stop to stop refreshing statistics.
Interface Monitor	
#	This is the index number of the entry.
Name	This shows the name of the interface on the Router.
Pass Rate (bps)	This shows how much traffic (bps) forwarded to this interface are transmitted successfully.
Queue Monitor	
#	This is the index number of the entry.
Name	This shows the name of the queue.
Pass Rate (bps)	This shows how much traffic (bps) assigned to this queue are transmitted successfully.

Network Address Translation (NAT)

12 Chapter

12.1 The General Screen

Click **Network Setting > NAT** to open the **General** screen. You can limit the number of concurrent NAT sessions each client can use.

Figure 41 Network Setting > NAT > General

NAT Full Feature on

Max NAT/Firewall Session Per User (512 - 8192)

Note :
Maximum number of NAT/firewall sessions for the router is 8192. To remove the per user limit, set to 8192.

Table 39 Network Setting > NAT > General

LABEL	DESCRIPTION
NAT Full Feature on	Select this check box if you have multiple public WAN IP addresses for your Router.
Max NAT/ Firewall Session Per User	Use this field to set a common limit to the number of concurrent NAT sessions each client computer can have. If only a few clients use peer to peer applications, you can raise this number to improve their performance. With heavy peer to peer application use, lower this number to ensure no single client uses too many of the available NAT sessions.

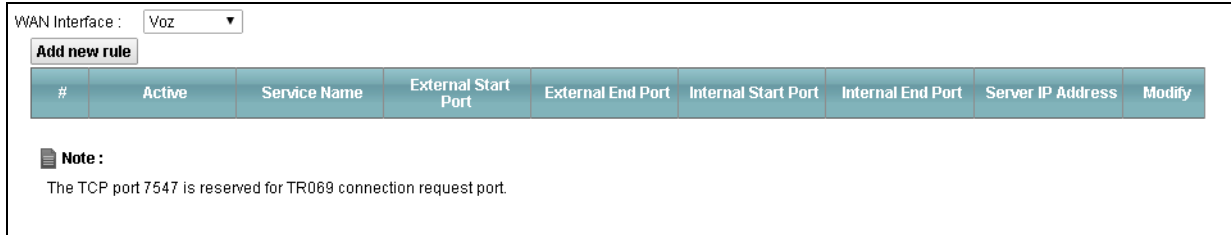
12.2 The Port Forwarding Screen

Use the **Port Forwarding** screen to forward incoming service requests to the servers on your local network.

12.2.1 The Port Forwarding Screen

Click **Network Setting > NAT** to open the **Port Forwarding** screen.

Figure 42 Network Setting > NAT > Port Forwarding



WAN Interface : Voiz

Add new rule

#	Active	Service Name	External Start Port	External End Port	Internal Start Port	Internal End Port	Server IP Address	Modify
---	--------	--------------	---------------------	-------------------	---------------------	-------------------	-------------------	--------

Note :
The TCP port 7547 is reserved for TR069 connection request port.

Table 40 Network Setting > NAT > Port Forwarding

LABEL	DESCRIPTION
WAN Interface	Select the WAN interface for which to configure NAT port forwarding rules.
Add new rule	Click this to add a new port forwarding rule.
Active	This field indicates whether the rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
Service Name	This is the service's name. This shows User Defined if you manually added a service. You can change this by clicking the edit icon.
External Start/End Port	This is the first/last external port number that identifies a service.
Internal Start/End Port	This is the first/last internal port number that identifies a service.
Server IP Address	This is the server's IP address.
Modify	Click the Edit icon to edit the port forwarding rule. Click the Delete icon to delete an existing port forwarding rule. Note that subsequent address mapping rules move up by one when you take this action.

12.2.2 The Port Forwarding Add/Edit Screen

This screen lets you create or edit a port forwarding rule. Click **Add new rule** in the **Port Forwarding** screen or the **Edit** icon next to an existing rule.

Figure 43 NAT > Port Forwarding: Add/Edit

The screenshot shows a configuration form for a port forwarding rule. It features the following elements:

- Active
- Service Name : User Define (dropdown menu)
- External Start Port : (text input field)
- External End Port : (text input field)
- Server IP Address : (text input field)
- Protocol : ALL (dropdown menu)
- Open Start Port : (text input field)
- Open End Port : (text input field)
- Buttons: Apply, Cancel

Table 41 NAT > Port Forwarding: Add/Edit

LABEL	DESCRIPTION
Active	Select or clear this field to turn the port forwarding rule on or off.
Service Name	Select a service to forward or select User Defined and enter a name in the field to the right.
External Start Port	Configure this for a user-defined entry. Enter the original destination port for the packets. To forward only one port, enter the port number again in the External End Port field. To forward a series of ports, enter the start port number here and the end port number in the External End Port field.
External End Port	Configure this for a user-defined entry. Enter the last port of the original destination port range. To forward only one port, enter the port number in the External Start Port field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the External Start Port field above.
Server IP Address	Enter the inside IP address of the virtual server here.
Protocol	Select the protocol supported by this virtual server. Choices are TCP , UDP , or TCP/UDP .

Table 41 NAT > Port Forwarding: Add/Edit (continued)

LABEL	DESCRIPTION
Open Start Port	Configure this for a user-defined entry. This shows the port number to which you want the Router to translate the incoming port. For a range of ports, enter the first number of the range to which you want the incoming ports translated.
Open End Port	Configure this for a user-defined entry. This shows the last port of the translated port range.

12.3 The Address Mapping Screen

Ordering your rules is important because the Router applies the rules in the order that you specify. When a rule matches the current packet, the Router takes the corresponding action and the remaining rules are ignored.

This screen is available only when you select **NAT Full Feature on** in the **General** screen. To change your Router's address mapping settings, click **Network Setting > NAT > Address Mapping**.

Add new rule							
#	Mapping Set	Local Start IP	Local End IP	Global Start IP	Global End IP	Type	Modify

Table 42 Network > NAT > Address Mapping

LABEL	DESCRIPTION
Add new rule	Click this to add a new address mapping rule.
Mapping Set	This is the index number of the address mapping set.
Local Start IP	This is the starting Inside Local IP Address (ILA).
Local End IP	This is the end Inside Local IP Address (ILA).
Global Start IP	This is the starting Inside Global IP Address (IGA).
Global End IP	This is the ending Inside Global IP Address (IGA).
Type	This is the port mapping type.
Modify	Click the edit icon to go to the screen where you can edit the address mapping rule. Click the delete icon to delete an existing address mapping rule. Note that subsequent address mapping rules move up by one when you take this action.

12.3.1 The Address Mapping Rule Edit Screen

Use this screen to edit an address mapping rule. Click the rule's edit icon in the **Address Mapping** screen to display the screen shown next.

Figure 44 NAT > Address Mapping: Edit

The screenshot shows a dialog box for editing NAT address mapping rules. It contains the following fields and values:

- Type: One-to-One (dropdown menu)
- Local Start IP: 0.0.0.0 (text input)
- Local End IP: 0.0.0.0 (text input)
- Global Start IP: 0.0.0.0 (text input)
- Global End IP: 0.0.0.0 (text input)
- Mapping Set: 1 (dropdown menu)

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

Figure 45 NAT > Address Mapping: Edit

LABEL	DESCRIPTION
Type	Choose the port mapping type from one of the following. One-to-One: maps one local IP address to one global IP address. Note that port numbers do not change for One-to-one NAT mapping type. Many-to-One: maps multiple local IP addresses to one global IP address. Many-to-Many: maps multiple local IP addresses to shared global IP addresses. One-to-Many (Server): allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Local Start IP	Enter the starting local IP address (ILA).
Local End IP	Enter the ending local IP address (ILA).
Global Start IP	Enter the starting global IP address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP.
Global End IP	This is the ending global IP address (IGA).
Mapping Set	Select the index number of the address mapping set.

12.4 The DMZ Screen

Click **Network Setting > NAT > DMZ** to open the **DMZ** screen. Use this screen to specify the IP address of a default server to receive packets from ports not specified in the **Port Forwarding** screen.

Figure 46 Network Setting > NAT > DMZ

WAN Interface :

Default Server Address :

Note :
Enter IP address and click 'Apply' to activate the DMZ host.
Input 0.0.0.0 in IP address field and click 'Apply' to deactivate the DMZ host.

Table 43 Network Setting > NAT > DMZ

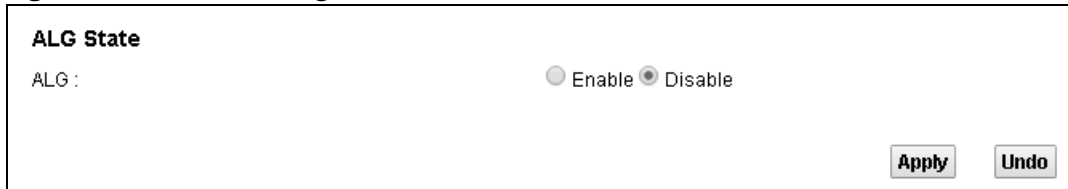
LABEL	DESCRIPTION
WAN Interface	Select the WAN interface for which to configure a default server.
Default Server Address	Enter the IP address of the default server which receives packets from ports that are not specified in the Port Forwarding screen.
	Note: If you do not assign a default server, the Router discards all packets received for ports not specified in the virtual server configuration.

12.5 The ALG Screen

Click **Network Setting > NAT > ALG** to open the **ALG** screen. Use this screen to enable and disable the NAT Application Layer Gateway (ALG) in the Router.

The SIP ALG allows SIP calls to pass through NAT by examining and translating IP addresses embedded in the data stream. When the Router registers with the SIP register server, the SIP ALG translates the Router's private IP address inside the SIP data stream to a public IP address. You do not need to use STUN or an outbound proxy if you enable the SIP ALG.

Figure 47 Network Setting > NAT > ALG



ALG State

ALG : Enable Disable

Apply **Undo**

Table 44 Network Setting > NAT > ALG

LABEL	DESCRIPTION
ALG	Enable this to make sure SIP (VoIP) works correctly with port-forwarding.

13.1 The Dynamic DNS Screen

Use the **Dynamic DNS** screen to enable DDNS and configure the DDNS settings on the Router. Click **Network Setting > Dynamic DNS**.

Figure 48 Network Setting > Dynamic DNS

Dynamic DNS Configuration

Dynamic DNS Enable Disable

Service Provider :

Host Name :

Username :

Password :

Dynamic DNS Status

User Authentication Result :

Last Updated Time :

Current Dynamic IP :

Table 45 Network Setting > Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS	Select Enable to use dynamic DNS.
Service Provider	Select the name of your Dynamic DNS service provider.
Host Name	Type the domain name assigned to your Router by your Dynamic DNS provider.
Username	Type your user name for the Dynamic DNS service provider.
Password	Type your password for the Dynamic DNS service provider.
Apply	Click Apply to save your changes.
Undo	Click Undo to restore your previously saved settings.
Dynamic DNS Status	

Table 45 Network Setting > Dynamic DNS (continued)

LABEL	DESCRIPTION
User Authentication Result	This field displays the results of the Router's attempt to authenticate with the Dynamic DNS service provider.
Last Updated Time	This field displays when the Router last updated its WAN IP address to the Dynamic DNS service provider.
Current Dynamic IP	This field displays the Router's current WAN IP address.

14.1 The IP/MAC Filter Screen

Use the **IP/MAC Filter** screen to create and apply IP/MAC filters. Click **Security > Filter** to show the **IP/MAC Filter** screen.

Figure 49 Security > Filter > IP/MAC Filter

Rule Type
Rule Type selection: White List ▾

IP / MAC Filter Rule Editing

IP / MAC Filter Rule Index: 1 ▾

Active: Yes No

Interface: Internet ▾

Direction: Incoming ▾

Rule Type: IP ▾

Source IP Address: (0.0.0.0 means Don't care)

Subnet Mask:

Port Number: (0 means Don't care)

Destination IP Address: (0.0.0.0 means Don't care)

Subnet Mask:

Port Number:

Protocol: TCP ▾

IP / MAC Filter Listing

#	Active	Interface	Direction	Src IP/Mask	Dest IP/Mask	Mac Address	Src Port	Dest Port	Protocol

Table 46 Security > Filter > IP/MAC Filter

LABEL	DESCRIPTION
Rule Type selection	Select White List to create a filter rule that allows traffic. Select Black List to create a filter rule that blocks traffic.
IP/MAC Filter Rule Index	Select the index number of the filter rule.
Active	Use this field to enable or disable the rule.
Interface	Select the interface to which to apply the filter.
Direction	Apply the filter to Incoming or Outgoing traffic direction.
Rule Type	Select IP to filter traffic by IP addresses. Select MAC to filter traffic by MAC address.
Source IP Address	Enter the source IP address of the packets you wish to filter.
Subnet Mask	Enter the IP subnet mask for the source IP address
Port Number	Enter the source port of the packets that you wish to filter.
Destination IP Address	Enter the destination IP address of the packets you wish to filter.
Subnet Mask	Enter the IP subnet mask for the destination IP address.
Port Number	Enter the destination port of the packets that you wish to filter.
Protocol	Select ICMP , TCP or UDP for the upper layer protocol.
Source MAC Address	This field is only available when you select MAC in the Rule Type field. Enter the MAC address of the packets you wish to filter.
Active	This field shows whether the rule is activated.
Interface	This field shows the interface to which the filter rule applies.
Direction	The filter rule applies to this traffic direction.
Src IP/Mask	This is the source IP address and subnet mask when you select IP as the rule type. This is the MAC address when you select MAC as the rule type.
Dest IP/Mask	This is the destination IP address and subnet mask.
MAC Address	For a MAC filter rule this field shows the MAC address of the packets to filter.
Src Port	This is the source port number.
Dest Port	This is the destination port number.
Protocol	This is the upper layer protocol.

14.2 The IPv6/MAC Filter Screen

Use the **IPv6/MAC Filter** screen to create and apply IPv6 address /MAC filters. Click **Security > Filter > IPv6/MAC Filter**.

Figure 50 Security > Filter > IPv6/MAC Filter

Rule Type
Rule Type selection: White List

IPv6 / MAC Filter Rule Editing
 IPv6 / MAC Filter Rule Index: 1
 Active: Yes No
 Interface: Internet
 Direction: Incoming
 Rule Type: IP
 Source IP Address:
 Source Prefix Length:
 Destination IPv6 Address:
 Destination Prefix Length:
 ICMPv6 Type: 1 / Destination Unreachable (0 - no route to destination)
 Protocol: ICMPv6

IPv6 / MAC Filter Listing
 IPv6 / MAC Filter Rule Index: 1

#	Active	Interface	Direction	ICMPv6Type	Src IP/Prefix length	Dest IP/Prefix length	Mac Address	Protocol
1	No	PVC0	Incoming	N/A	N/A/ N/A	N/A/ N/A	N/A	ICMPv6

Apply Delete Undo

Table 47 Security > Filter > IPv6/MAC Filter

LABEL	DESCRIPTION
Rule Type selection	Select White List to create a filter rule that allows traffic. Select Black List to create a filter rule that blocks traffic.
IPv6/MAC Filter Rule Index	Select the index number of the filter rule.
Active	Use this field to enable or disable the rule.
Interface	Select the interface to which to apply the filter.
Direction	Apply the filter to Incoming or Outgoing traffic direction.
Rule Type	Select IP to filter traffic by IP addresses. Select MAC to filter traffic by MAC address.

Table 47 Security > Filter > IPv6/MAC Filter (continued)

LABEL	DESCRIPTION
Source IP Address	Enter the source IP address of the packets you wish to filter.
Source Prefix Length	Enter the prefix length for the source IPv6 address.
Destination IPv6 Address	Enter the destination IPv6 address of the packets you wish to filter.
Destination Prefix Length	Enter the prefix length for the destination IPv6 address.
ICMPv6 Type	Select one of the ICMPv6 message types to filter.
Protocol	This is the (upper layer) protocol that defines the service to which this rule applies. By default it is ICMPv6 .
Source MAC Address	This field is only available when you select MAC in the Rule Type field. Enter the MAC address of the packets you wish to filter.
IPv6 / MAC Filter Rule Index	Select the index number of the filter set.
Active	This field shows whether the rule is activated.
Interface	This field shows the interface to which the filter rule applies.
Direction	The filter rule applies to this traffic direction.
ICMPv6Type	This is the ICMPv6 message type to filter.
Src IP/Prefix length	This is the source IPv6 address and prefix length.
Dest IP/Prefix length	This displays the destination IPv6 address and prefix length.
MAC Address	This is the MAC address of the packets being filtered.
Protocol	This is the (upper layer) protocol that defines the service to which this rule applies.

15.1 TFirewall General Screen

Use this screen to enable or disable the firewall protection on the Router. You can also edit existing rules or create new ones. Click **Security > Firewall** to open the **General** screen.

Figure 51 Security > Firewall > General

Firewall

On
This setting allows the customer to create and edit individual firewall rules.

Off
This setting is not recommended. It disables firewall protection for your network and could potentially expose your network to significant security risks. This option should only be used for troubleshooting or if you intend using another firewall in conjunction with your MitraStar router.

No.	IP Version	Name	Interface	Direction	Default Action	Num	Modify
1	IPv4	NETBIOS	br0	In	Permit	4	
2	IPv4	DEFAULTWAN	ppp100	In	Drop	10	

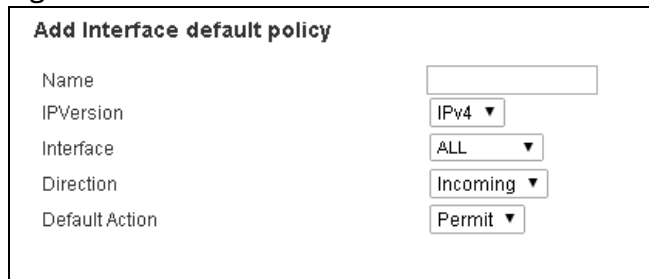
Table 48 Security > Firewall > General

LABEL	DESCRIPTION
On	Select this to enable the firewall protection on the Router.
Off	Select this to disable the firewall protection on the Router. This setting is not recommended. It disables firewall protection for your network and could potentially expose your network to significant security risks. This option should only be used for troubleshooting or if you intend using another firewall in conjunction with your router.
Modify	Click the edit icon to go to the screen where you can edit an existing rule. Click the delete icon to delete an existing existing rule.
Add	Click this to add a new default action that the firewall takes .
Apply	Click this to save your changes.
Cancel	Click this to restore your previously saved settings.

15.1.1 Add/Edit Interface Default Policy Screen

Use this screen to edit existing firewall rules or create new ones. Click the **edit** icon next to an existing firewall rule or click the **Add** button in the **General** screen.

Figure 52 Firewall > General: Add/Edit



Add Interface default policy

Name

IPVersion

Interface

Direction

Default Action

Table 49 Firewall > General: Add/Edit

LABEL	DESCRIPTION
Name	Enter a descriptive name for this firewall rule.
IPVersion	Select the IP version for this firewall rule.
Packet Direction	Select the direction of traffic which applies to this firewall rule.
Default Action	Select the default action that the firewall is to take on packets that are traveling in the selected direction and do not match any of the firewall rules. Select Permit to allow the passage of the packets. Select Drop to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender.

15.2 Rules Screen

The **Rules** screen displays a list of the configured firewall rules. Note the order in which the rules are listed. Click **Security > Firewall > Rules**.


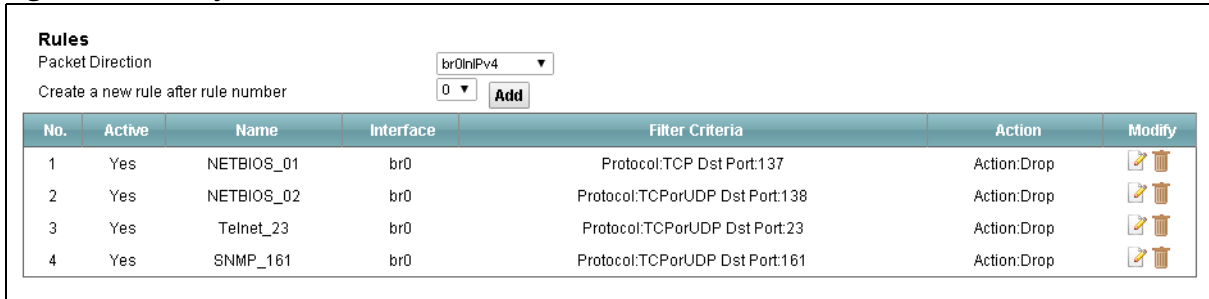
 The ordering of your rules is very important as rules are applied in turn.

Figure 53 Security > Firewall > Rules











No.	Active	Name	Interface	Filter Criteria	Action	Modify
1	Yes	NETBIOS_01	br0	Protocol:TCP Dst Port:137	Action:Drop	 
2	Yes	NETBIOS_02	br0	Protocol:TCPorUDP Dst Port:138	Action:Drop	 
3	Yes	Telnet_23	br0	Protocol:TCPorUDP Dst Port:23	Action:Drop	 
4	Yes	SNMP_161	br0	Protocol:TCPorUDP Dst Port:161	Action:Drop	 

Table 50 Security > Firewall > Rules

LABEL	DESCRIPTION
Packet Direction	Select a direction of travel of packets for which you want to configure firewall rules.
Create a new rule after rule number	Select an index number and click Add to add a new firewall rule after the selected index number. For example, if you select "6", your new rule becomes number 7 and the previous rule 7 (if there is one) becomes rule 8. The following read-only fields summarize the rules you have created that apply to traffic traveling in the selected packet direction. The firewall rules that you configure (summarized below) take priority over the general firewall action settings in the General screen.
No.	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn.
Active	This displays whether a firewall is turned on or not. Select the check box to enable the rule. Clear the check box to disable the rule.
Name	This displays the name of the firewall rule.
Interface	This displays the source interface to which this firewall rule applies. This is the interface through which the traffic entered the Router.
Destination IP Address	This displays the destination addresses or ranges of addresses to which this firewall rule applies.
Filter Criteria	This displays the filter criteria set for this firewall rule.
Action	This field displays whether the firewall silently discards packets (Drop) or allows the passage of packets (Permit).
Modify	Click the Edit icon to go to the screen where you can edit the rule. Click the Remove icon to delete an existing firewall rule. A window displays asking you to confirm that you want to delete the firewall rule. Note that subsequent firewall rules move up by one when you take this action.

15.2.1 Rules Edit Screen

Use this screen to configure firewall rules. In the **Rules** screen, select an index number and click a rule's **Edit** icon.

Figure 54 Firewall > Rules: Edit

Edit Rule

Active

Rule Name:

Select a Service:

Custom Service:

Protocol:

Rules

Source Address

Source IP Address:

Source Subnet Mask:

Source Port(port or port:port): :

Destination Address

Destination IP Address:

Destination Subnet Mask:

Destination Port(port or port:port): :

Action for Matched Packets:

OK Cancel

Table 51 Firewall > Rules: Edit

LABEL	DESCRIPTION
Active	Select this option to enable this firewall rule.
Rule Name	If you want to select an exiting service, choose Select a Service and find the service to which this rule applies to in the drop-down list box. If you want to manually configure a service that is not in the list, choose Custom Service . Enter the name of the service and select its protocol in the Protocol field. If you select ICMP as your protocol, select the ICMP type in the ICMP (Type-code) field below.
Source IP Address	Enter the source IP address.
Source Subnet Mask	Enter the source subnet mask.
Source Port	Enter a single source port or a port range.

Table 51 Firewall > Rules: Edit (continued)

LABEL	DESCRIPTION
Destination IP Address	Enter the destination IP address.
Destination Subnet Mask	Enter the destination subnet mask.
Destination Port	Enter a single destination port or a port range.
Action for Matched Packets	select whether to discard (Drop), deny and send an ICMP destination-unreachable message to the sender of (Reject) or allow the passage of (Permit) packets that match this rule.

15.3 DoS Screen

Use the **DoS** screen to enable DoS protection. Click **Security > Firewall > DoS**.

Figure 55 Security > Firewall > DoS



DoS
Denial of Services Enabled Disabled

Apply **Undo** **Advanced**

Table 52 Security > Firewall > Dos

LABEL	DESCRIPTION
Denial of Services	Enable this to protect against DoS attacks. The Router will drop sessions that surpass maximum thresholds.
Apply	Click this to save your changes.
Undo	Click this to restore your previously saved settings.
Advanced	Click this to go to a screen to specify maximum thresholds at which the Router will start dropping sessions.

15.3.1 The DoS Advanced Screen

Click **Security > Firewall > DoS > Advanced** to display the following screen.

Figure 56 Firewall > DoS > Advanced

The screenshot shows a configuration window titled "Firewall > DoS > Advanced". It contains the following settings:

- TCP SYN Flood Threshold:** TCP SYN-Request Count is set to 500 /sec.
- UDP Packet Threshold:** UDP Packet Count is set to 5000 /sec.
- ICMP Echo-Request Threshold:** ICMP Echo-Request Count is set to 5 /sec.
- Others:**
 - ICMP Redirect: Enable, Disable
 - DoS Log(Log Level:DEBUG): Enable, Disable

At the bottom right, there are "OK" and "Cancel" buttons.

Table 53 Firewall > DoS > Advanced

LABEL	DESCRIPTION
TCP SYN-Request Count	This is the rate of new TCP half-open sessions per second that causes the firewall to start deleting half-open sessions. When the rate of new connection attempts rises above this number, the Router deletes half-open sessions as required to accommodate new connection attempts.
UDP Packet Count	This is the rate of new UDP half-open sessions per second that causes the firewall to start deleting half-open sessions. When the rate of new connection attempts rises above this number, the Router deletes half-open sessions as required to accommodate new connection attempts.
ICMP Echo-Request Count	This is the rate of new ICMP Echo-Request half-open sessions per second that causes the firewall to start deleting half-open sessions. When the rate of new connection attempts rises above this number, the Router deletes half-open sessions as required to accommodate new connection attempts.
ICMP Redirect	Select Enable to monitor for and block ICMP redirect attacks. An ICMP redirect attack is one where forged ICMP redirect messages can force the client device to route packets for certain connections through an attacker's host.
DoS Log(Log Level: DEBUG)	Select Enable to log DoS attacks.

16.1 The Parental Control Screen

Parental control allows you to block web sites with the specific URL. You can also define time periods and days during which the Router performs parental control on a specific user.

Use the **Parental Control** screen to enable parental control, view the parental control rules and schedules. Click **Security > Parental Control**.

Figure 57 Security > Parental Control

General
 Parental Control: Enable Disable (settings are invalid when disabled)

Add new PCP

#	Status	PCP Name	Home Network User	Internet Access Schedule	Network Service	Website Blocked	Modify
---	--------	----------	-------------------	--------------------------	-----------------	-----------------	--------

Apply **Undo**

Table 54 Security > Parental Control

LABEL	DESCRIPTION
Parental Control	Select Enable to activate parental control.
Add new PCP	Click this if you want to configure a new parental control rule.
Status	This indicates whether the rule is active or not. A yellow bulb signifies that this rule is active. A gray bulb signifies that this rule is not active.
PCP Name	This shows the name of the rule.
Home Network User	This shows the MAC address of the LAN user's computer to which this rule applies.
Internet Access Schedule	This shows the days and time on which parental control is enabled.
Network Service	This shows whether the network service is configured. If not, None will be shown.

Table 54 Security > Parental Control (continued)

LABEL	DESCRIPTION
Website Blocked	This shows whether the website block is configured. If not, None will be shown.
Modify	Click the Edit icon to go to the screen where you can edit the rule. Click the Delete icon to delete an existing rule.

16.1.1 Add/Edit a Parental Control Rule

Click **Add new PCP** in the **Parental Control** screen to add a new rule or click the **Edit** icon next to an existing rule to edit it. Use this screen to configure a restricted access schedule and/or URL filtering settings to block the users on your network from accessing certain web sites.

Figure 58 Parental Control: Add/Edit

General

Active

Parental Control Profile Name :

Home Network User :

Internet Access Schedule

Day : Everyday Monday Tuesday Wednesday Thursday Friday Saturday Sunday

Time of Day to Apply:(24-Hour Format)

Start Time(hh:mm) :

End Time(hh:mm) :

Network Service

Network Service Setting : selected service(s)

Active	Service Name	Protocol	Port	Modify
<input type="checkbox"/>	<input type="text" value="UserDefined"/>	<input type="text" value="TCP"/>	<input type="text"/>	

Note :

In "Port" column, the format of "Multi-port" should be like: 3091,4091 (the max port number you can put is 15), the format of "Range-port" should be like: 5091:6892.

Blocked Site/URL

Site/URL :

Site/URL :

Site/URL :

Site/URL :

Site/URL :

Table 55 Parental Control: Add/Edit

LABEL	DESCRIPTION
Active	Select the checkbox to activate this parental control rule.
Parental Control Profile Name	Enter a descriptive name for the rule.
Home Network User	Select the LAN user that you want to apply this rule to from the drop-down list box. If you select Custom , enter the LAN user's MAC address. If you select All , the rule applies to all LAN users.

Table 55 Parental Control: Add/Edit (continued)

LABEL	DESCRIPTION
Internet Access Schedule	
Day	Select check boxes for the days that you want the Router to perform parental control.
Time of Day to Apply: (24-Hour Format)	
Start Time End Time	Enter the time period of each day, in 24-hour format, during which parental control will be enforced.
Network Service Setting	If you select Block , the Router prohibits the users from viewing the Web sites with the URLs listed below. If you select Access , the Router blocks access to all URLs except ones listed below.
Add new service	Click this to show a screen in which you can add a new service rule. You can configure the Service Name , Protocol , and Name of the new rule.
Active	Select the check box next to the service to apply this rule to the service. Clear the check box to not apply this rule to it.
Service Name	Select a service.
Protocol	For services that support multiple protocols, select the protocol.
Port	Specify the port number from 1 to 65535.
Modify	Click the Delete icon to delete an existing rule.
Blocked Site/URL	Specify web sites or URLs to which the Router blocks access.

17.1 Local Certificates

Use the **Local Certificates** screen to view the Router's summary list of certificates and certification requests. You can import the following certificates to your Router:

- Web Server - This certificate secures HTTP connections.
- SSH - This certificate secures remote connections.

Click **Security > Certificates** to open the **Local Certificates** screen.

Figure 59 Security > Certificates > Local Certificates



Table 56 Security > Certificates > Local Certificates

LABEL	DESCRIPTION
WebServer	Click Browse... to find the certificate file you want to upload.
Current File	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country.

Table 56 Security > Certificates > Local Certificates (continued)

LABEL	DESCRIPTION
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Cert	Click this button and then Save in the File Download screen. The Save As screen opens, browse to the location that you want to use and click Save .
SSH	Type in the location of the SSH certificate file you want to upload in this field or click Browse to find it.
Choose file	Click this link to find the certificate file you want to upload.
Current File	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Key Type	This field applies to the SSH/SCP/SFTP certificate. This shows the file format of the current certificate.

17.2 Trusted CA

Use the **Trusted CA** screen to view a summary list of certificates of the certification authorities that you have set the Router to accept as trusted. The Router accepts any valid certificate signed by a certification authority on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certification authorities.

Click **Security > Certificates > Trusted CA** to open the **Trusted CA** screen.

Figure 60 Security > Certificates > Trusted CA

Import Certificate			
Name	Subject	Type	Action
ca1.pem	ST=A78923125/L=PZ. DE LA INDEPENDENCIA 6 28001 MADRID/O=TME/CN=CA Telefonica Moviles Espana SA	ca	 

Table 57 Security > Certificates > Trusted CA

LABEL	DESCRIPTION
Import Certificate	Click this button to open a screen where you can save the certificate of a certification authority that you trust to the Router.
Name	This field displays the name used to identify this certificate.

Table 57 Security > Certificates > Trusted CA (continued)

LABEL	DESCRIPTION
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), OU (Organizational Unit or department), Organization (O), State (ST) and Country (C). It is recommended that each certificate have unique subject information.
Type	This field displays general information about the certificate. ca means that a Certification Authority signed the certificate.
Action	Click the View icon to open a screen with an in-depth list of information about the certificate (or certification request). Click the Delete icon to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use.

17.3 Trusted CA Import

Click **Import Certificate** in the **Trusted CA** screen to open the **Import Certificate** screen. You can save a trusted certification authority's certificate to the Router.


-  You must remove any spaces from the certificate's filename before you can import the certificate.

Figure 61 Certificates > Trusted CA: Import

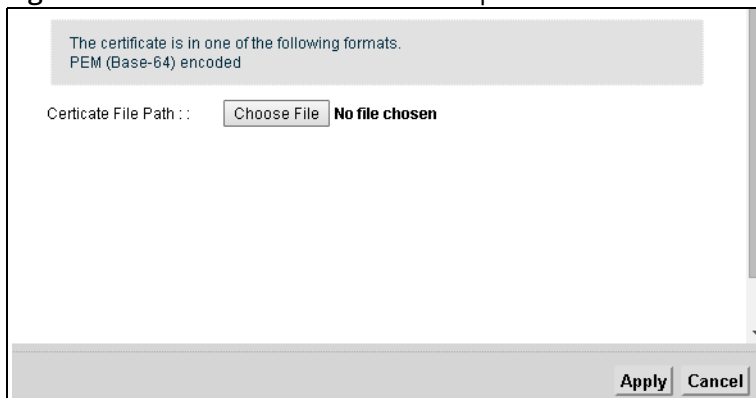


Table 58 Certificates > Trusted CA: Import

LABEL	DESCRIPTION
Certificate File Path	Type in the location of the file you want to upload in this field or click Browse to find it.
Browse	Click Browse to find the certificate file you want to upload.

17.4 View Certificate

Use this screen to view in-depth information about the certification authority's certificate, change the certificate's name and set whether or not you want the Router to check a certification authority's list of revoked certificates before trusting a certificate issued by the certification authority.

Click **Security > Certificates > Trusted CA** to open the **Trusted CA** screen. Click the **View** icon to open the **View Certificate** screen.

Figure 62 Security > Certificates > Trusted CA > View

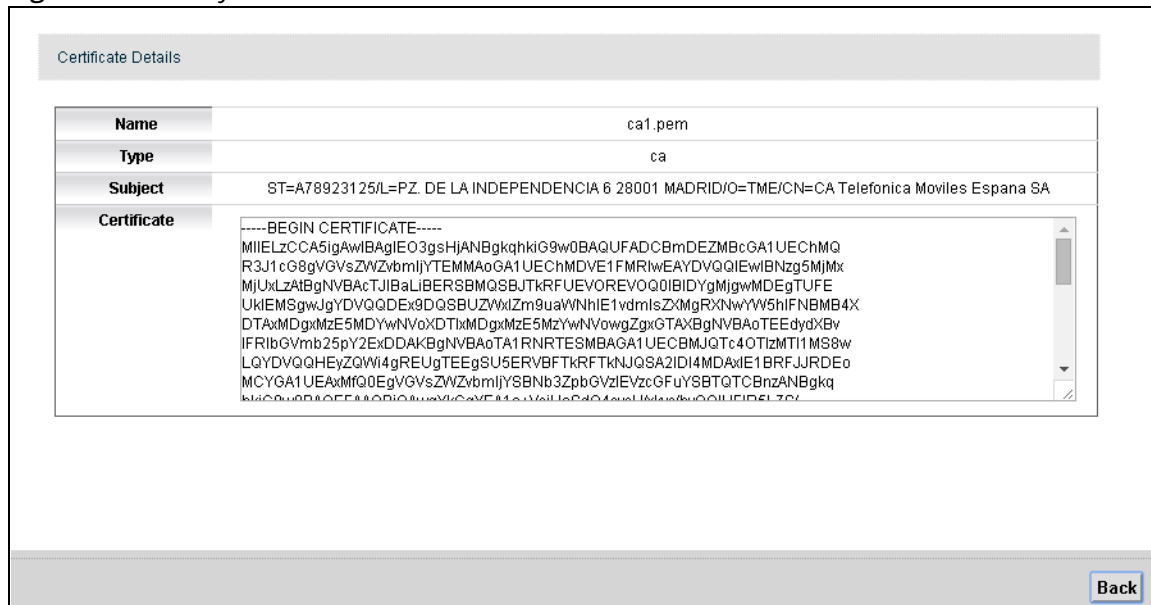


Table 59 Security > Certificates > Trusted CA > View

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate..
Type	This field displays the type of this certificate.
Subject	This field displays the subject of this certificate.
Certificate	<p>This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form.</p> <p>You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).</p>

18.1 The SIP Account Screen

The Router uses a SIP account to make outgoing VoIP calls and check if an incoming call's destination number matches your SIP account's SIP number. In order to make or receive a VoIP call, you need to enable and configure a SIP account, and map it to a phone port. The SIP account contains information that allows your Router to connect to your VoIP service provider.

To access the following screen, click **VoIP > SIP > SIP Account**.

Figure 63 VoIP > SIP > SIP Account





SIP Account Table					
#	Active	SIP Account	Service Provider	Account No.	Modify
1	<input type="checkbox"/>	1	telefonica.net	ChangeMe	
2	<input type="checkbox"/>	2	telefonica.net	ChangeMe	
3	<input type="checkbox"/>	3	telefonica.net	ChangeMe	
4	<input type="checkbox"/>	4	telefonica.net	ChangeMe	

Table 60 VoIP > SIP > SIP Account

LABEL	DESCRIPTION
Active	This shows whether the SIP account is activated or not.
SIP Account	This shows the name of the SIP account.
Service Provider	This shows the name of the SIP service provider.
Account No.	This shows the SIP number.
Modify	Click the Edit icon to configure the SIP account.

18.1.1 Edit SIP Account

You can configure a SIP account. To access this screen, click the **Edit** icon next to an account.

Figure 64 SIP > SIP Account: Add/Edit

General

Enable SIP Account

SIP Account Number:

Authentication

Username:

Password:

URL Type

URL Type:

Voice Features

Primary Compression Type:

Second Compression Type:

Third Compression Type:

Speaking Volume Control:

Listening Volume Control:

Active G.168 (Echo Cancellation)

Active VAD (Voice Active Detector)

Call Features

Send Caller ID

Active Call Transfer

Active Call Waiting

Active Call Waiting Reject Time: (10~60)second

Active Unconditional Forward To Number:

Active Busy Forward To Number:

Active No Answer Forward To Number:

No Answer Ring Time: (10~180)second

Hot Line/Warm Line Enable

Warm Line Hot Line

Hot Line/Warm Line number:

Warm Line number(sec): (5~300)second

Active Anonymous Call Block

Table 61 SIP > SIP Account: Edit

LABEL	DESCRIPTION
Enable SIP Account	Select the check box to use this account. Clear it to not use this account.
SIP Account Number	Enter your SIP number. In the full SIP URI, this is the part before the @ symbol.
Username	Enter the user name for registering this SIP account, exactly as it was given to you.
Password	Enter the password for registering this SIP account, exactly as it was given to you.
URL Type	Select whether or not to include the SIP service domain name when the Router sends the SIP number. SIP - include the SIP service domain name. TEL - do not include the SIP service domain name.
Primary / Secondary / Third Compression Type	Select the type of voice coder/decoder (codec) that you want the Router to use. G.711 provides higher voice quality but requires more bandwidth (64 kbps). When two SIP devices start a SIP session, they must agree on a codec. Select the Router's first, second, and third choice for voice coder/decoder. Select None for the second and third choice if you only want the Router to accept the first choice.
Speaking Volume Control	Select the loudness that the Router uses for speech that it sends to the peer device.
Listening Volume Control	Select the loudness that the Router uses for speech that it receives from the peer device.
Active G.168 (Echo Cancellation)	Select this if you want to eliminate the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.
Active VAD (Voice Active Detector)	Select this if the Router should stop transmitting when you are not speaking. This reduces the bandwidth the Router uses.
Send Caller ID	Select this if you want to send identification when you make VoIP phone calls. Clear this if you do not want to send identification.
Active Call Transfer	Select this to enable call transfer on the Router. This allows you to transfer an incoming call (that you have answered) to another phone.
Active Call Waiting	Select this to enable call waiting on the Router. This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.
Active Call Waiting Reject Time	Specify a time of seconds that the Router waits before rejecting the second call if you do not answer it.
Active Unconditional Forward	Select this if you want the Router to forward all incoming calls to the specified phone number. Specify the phone number in the To Number field on the right.

Table 61 SIP > SIP Account: Edit (continued)

LABEL	DESCRIPTION
Active Busy Forward	Select this if you want the Router to forward incoming calls to the specified phone number if the phone port is busy. Specify the phone number in the To Number field on the right. If you have call waiting, the incoming call is forwarded to the specified phone number if you reject or ignore the second incoming call.
Active No Answer Forward	Select this if you want the Router to forward incoming calls to the specified phone number if the call is unanswered. (See No Answer Time .) Specify the phone number in the To Number field on the right.
No Answer Ring Time	This field is used by the Active No Answer Forward feature. Enter the number of seconds the Router should wait for you to answer an incoming call before it considers the call is unanswered.
Hot Line / Warm Line Enable	Select this to enable the hot line or warm line feature on the Router.
Warm Line	Select this to have the Router dial the specified warm line number after you pick up the telephone and do not press any keys on the keypad for a period of time.
Hot Line	Select this to have the Router dial the specified hot line number immediately when you pick up the telephone.
Hot Line / Warm Line number	Enter the number of the hot line or warm line that you want the Router to dial.
Warm Line number (sec)	Enter a number of seconds that the Router waits before dialing the warm line number if you pick up the telephone and do not press any keys on the keypad.
Active Anonymous Call Block	Select this to have the phone not ring for incoming calls with caller ID deactivated.

18.2 The SIP Service Provider Screen

Use this screen to manage profiles of SIP service provider settings. Click **VoIP > SIP > SIP Service Provider** to open the **SIP Service Provider** screen.

Figure 65 VoIP > SIP > SIP Service Provider



SIP Service Provider Table					
#	SIP Service Provider Name	SIP Server Address	REGISTER Server Address	SIP Service Domain	Modify
1	telefonica.net	telefonica.net	telefonica.net	telefonica.net	
2	telefonica.net	telefonica.net	telefonica.net	telefonica.net	

Table 62 VoIP > SIP > SIP Service Provider

LABEL	DESCRIPTION
SIP Service Provider Name	This shows the name of the SIP service provider.
SIP Server Address	This shows the IP address or domain name of the SIP server.
REGISTER Server Address	This shows the IP address or domain name of the SIP register server.
SIP Service Domain	Enter the SIP service domain name. In the full SIP URI, this is the part after the @ symbol. You can use up to 127 printable ASCII Extended set characters.
Modify	Click the Edit icon to configure the profile of SIP service provider settings.

18.2.1 Edit SIP Service Provider

Use this screen to configure the SIP server information, QoS for VoIP calls, the numbers for certain phone functions and dialing plan for a SIP service provider. Click **VoIP > SIP > SIP Service Provider** and then click the **Edit** icon next to a profile of SIP service provider settings to open the following screen.

Figure 66 VoIP > SIP > SIP Service Provider > Edit

General	
SIP Service Provider	<input checked="" type="checkbox"/>
SIP Service Provider Name	<input type="text" value="telefonica.net"/>
SIP Local Port	<input type="text" value="5060"/> (1025-65535)
Main SIP Server Address	<input type="text" value="telefonica.net"/>
SIP Server Port	<input type="text" value="5060"/> (1025-65535)
REGISTER Server Address	<input type="text" value="telefonica.net"/>
REGISTER Server Port	<input type="text" value="5060"/> (1025-65535)
SIP Service Domain	<input type="text" value="telefonica.net"/>
Bound Interface Name	
Bound Interface Name	<input type="text" value="Multi_WAN"/>
<input type="checkbox"/> Internet	
<input checked="" type="checkbox"/> Voz	
<input type="checkbox"/> Imagenio	
<input type="checkbox"/> test	
<input type="checkbox"/> N/A	
<input type="checkbox"/> N/A	
<input type="checkbox"/> N/A	
<input type="checkbox"/> N/A	
RFC Support	
<input type="checkbox"/> Replace dial digit '#' to '%23' in SIP messages	
<input checked="" type="checkbox"/> Remove '5060' and 'transport=udp' from request-uri in SIP messages	
<input type="checkbox"/> Remove the 'Route' header in SIP	
<input checked="" type="checkbox"/> Don't send re-Invite to the remote party when there are multiple codecs answered in the SDP	
<input checked="" type="checkbox"/> Remove the 'Authentication' header in SIP ACK message	
RTP Port Range	
Start Port:	<input type="text" value="50000"/> (1025-65535)
End Port:	<input type="text" value="51000"/> (1025-65535)
DTMF Mode	
DTMF Mode:	<input type="text" value="InBand"/>
Transport Type	
Transport Type:	<input type="text" value="UDP"/>
FAX Option	
<input type="radio"/> G711 FAX Passthrough	<input checked="" type="radio"/> T38 Fax Relay
Outbound Proxy	
Server Address	<input type="text" value="10.31.255.134"/>
Server Port	<input type="text" value="5070"/> (1025-65535)
QoS Tag	
SIP TOS Priority Setting	<input type="text" value="0"/> (0-255)
RTP TOS Priority Setting	<input type="text" value="0"/> (0-255)
Timr Setting	
Expiration Duration :	<input type="text" value="600"/> (60-65535)second
Register Re-send timer :	<input type="text" value="512"/> (60-3600)second
Session Expires :	<input type="text" value="600"/> (100-65535)second
Min-SE :	<input type="text" value="180"/> (90-65535)second
Dialing interval selection	
Dialing interval selection:	<input type="text" value="5"/> (Second)
Phone Key Config	
Caller Display Call :	<input type="text" value="*30#"/>
Caller Hidden Call :	<input type="text" value="#30#"/>
One Shot Caller Display Call :	<input type="text" value="*31#"/>
One Shot Caller Hidden Call :	<input type="text" value="#31#"/>
Call Waiting Enable :	<input type="text"/>
Call Waiting Disable :	<input type="text"/>
One Shot Call Waiting Enable :	<input type="text" value="*44#"/>
One Shot Call Waiting Disable :	<input type="text" value="#44#"/>

Figure 67 SIP > SIP Service Provider > Edit (continued)

Unconditional Call Forward Enable :	<input type="text"/>
Unconditional Call Forward Disable :	<input type="text"/>
No Answer Call Forward Enable :	<input type="text"/>
No Answer Call Forward Disable :	<input type="text"/>
Call Forward When Busy Enable :	<input type="text"/>
Call Forward When Busy Disable :	<input type="text"/>
Do not Disturb Enable :	*95# <input type="text"/>
Do not Disturb Disable :	#95# <input type="text"/>
Call Return :	*92# <input type="text"/>
Call Completion on Busy :	#37# <input type="text"/>
Subscriber(CCBS) Deactivate :	<input type="text"/>
Outgoing SIP :	*12# <input type="text"/>
Dial Plan	
Dial Plan Enable	<input type="checkbox"/>

Table 63 SIP > SIP Service Provider: Edit

LABEL	DESCRIPTION
SIP Service Provider	Select this if you want the Router to use this SIP provider. Clear it if you do not want the Router to use this SIP provider.
SIP Service Provider Name	Enter the name of your SIP service provider.
SIP Local Port	Enter the Router's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
Main SIP Server Address	Enter the IP address or domain name of the SIP server provided by your VoIP service provider. You can use up to 95 printable ASCII characters. It does not matter whether the SIP server is a proxy, redirect or register server.
SIP Server Port	Enter the SIP server's listening port number, if your VoIP service provider gave you one. Otherwise, keep the default value.
REGISTER Server Address	Enter the IP address or domain name of the SIP register server, if your VoIP service provider gave you one. Otherwise, enter the same address you entered in the SIP Server Address field. You can use up to 95 printable ASCII characters.
REGISTER Server Port	Enter the SIP register server's listening port number, if your VoIP service provider gave you one. Otherwise, enter the same port number you entered in the SIP Server Port field.
SIP Service Domain	Enter the SIP service domain name. In the full SIP URI, this is the part after the @ symbol. You can use up to 127 printable ASCII Extended set characters.
Bound Interface Name	If you select AnyWAN , the Router automatically activates the VoIP service when any WAN connection is up. If you select MultiWAN , you also need to select the pre-configured WAN connections. The VoIP service is activated only when one of the selected WAN connections is up.

Table 63 SIP > SIP Service Provider: Edit (continued)

LABEL	DESCRIPTION
PRACK (RFC 3262)	<p>RFC 3262 defines a mechanism to provide reliable transmission of SIP provisional response messages, which convey information on the processing progress of the request. This uses the option tag 100rel and the Provisional Response ACKnowledgement (PRACK) method.</p> <p>Select Supported or Required to have the Router include a SIP Require/Supported header field with the option tag 100rel in all INVITE requests. When the Router receives a SIP response message indicating that the phone it called is ringing, the Router sends a PRACK message to have both sides confirm the message is received.</p> <p>If you select Supported, the peer device supports the option tag 100rel to send provisional responses reliably.</p> <p>If you select Required, the peer device requires the option tag 100rel to send provisional responses reliably.</p> <p>Select Disabled to turn off this function.</p>
DNS SRV Enabled (RFC 3263)	<p>Select this to have the Router query your ISP's DNS server for a list of any available SIP servers that it maintains. This is useful if your static SIP server experiences difficulties, making it hard for your IP phone users to make SIP calls.</p>
Session Timer (RFC 4028)	<p>Select this to have the Router support RFC 4028.</p> <p>This makes sure that SIP sessions do not hang and the SIP line can always be available for use.</p>
RFC Support	<p>Select VoIP inter-operability settings.</p>
Start Port End Port	<p>Enter the listening port number(s) for RTP traffic, if your VoIP service provider gave you this information. Otherwise, keep the default values.</p> <p>To enter one port number, enter the port number in the Start Port and End Port fields.</p> <p>To enter a range of ports,</p> <ul style="list-style-type: none"> • enter the port number at the beginning of the range in the Start Port field. • enter the port number at the end of the range in the End Port field.
DTMF Mode	<p>Control how the Router handles the tones that your telephone makes when you push its buttons. You should use the same mode your VoIP service provider uses.</p> <p>RFC2833 - send the DTMF tones in RTP packets.</p> <p>Inband - send the DTMF tones in the voice data stream. This method works best when you are using a codec that does not use compression (like G.711). Codecs that use compression (like G.726) can distort the tones.</p> <p>SIPInfo - send the DTMF tones in SIP messages.</p>
Transport Type	<p>Select the transport layer protocol UDP or TCP (usually UDP) used for SIP.</p>
FAX Option	<p>This field controls how the Router handles fax messages.</p>
G711 Fax Passthrough	<p>Select this if the Router should use G.711 to send fax messages. The peer devices must also use G.711.</p>

Table 63 SIP > SIP Service Provider: Edit (continued)

LABEL	DESCRIPTION
T38 Fax Relay	Select this if the Router should send fax messages as UDP or TCP/IP packets through IP networks. This provides better quality, but it may have inter-operability problems. The peer devices must also use T.38.
Server Address	Enter the IP address or domain name of the SIP outbound proxy server.
Server Port	Enter the SIP outbound proxy server's listening port, if your VoIP service provider gave you one. Otherwise, keep the default value.
SIP TOS Priority Setting	Enter the DSCP (DiffServ Code Point) number for SIP message transmissions. The Router creates Class of Service (CoS) priority tags with this number to SIP traffic that it transmits.
RTP TOS Priority Setting	Enter the DSCP (DiffServ Code Point) number for RTP voice transmissions. The Router creates Class of Service (CoS) priority tags with this number to RTP traffic that it transmits.
Expiration Duration	Enter the number of seconds your SIP account is registered with the SIP register server before it is deleted. The Router automatically tries to re-register your SIP account when one-half of this time has passed. (The SIP register server might have a different expiration.)
Register Re-send timer	Enter the number of seconds the Router waits before it tries again to register the SIP account, if the first try failed or if there is no response.
Session Expires	Enter the number of seconds the Router lets a SIP session remain idle (without traffic) before it automatically disconnects the session.
Min-SE	Enter the minimum number of seconds the Router lets a SIP session remain idle (without traffic) before it automatically disconnects the session. When two SIP devices start a SIP session, they must agree on an expiration time for idle sessions. This field is the shortest expiration time that the Router accepts.
Dialing interval selection	Enter the number of seconds the Router should wait after you stop dialing numbers before it makes the phone call. The value depends on how quickly you dial phone numbers.
Phone Key Config	
Use this section to customize the phone keypad combinations you use to access certain features on the Router.	
Caller Display Call	This code is used to display the caller ID for outgoing calls.
Caller Hidden Call	This code is used to hide the caller ID for outgoing calls.
One Shot Caller Display Call	This code is used to display the caller ID only for the phone call your are going to make.
One Shot Caller Hidden Call	This code is used to hide the caller ID only for the phone call your are going to make.

Table 63 SIP > SIP Service Provider: Edit (continued)

LABEL	DESCRIPTION
Call Waiting Enable	This code is used to turn the call waiting feature on. With call waiting, you hear a special beep notifying you of another incoming call while you have a call. It allows you to place the first incoming call on hold and answer the second call so that you won't miss any important calls.
Call Waiting Disable	This code is used to turn the call waiting feature off.
One Shot Call Waiting Enable	This code is used to enable call waiting only for the phone call your are going to make. See the description for the Call Waiting Enable field for more information.
One Shot Call Waiting Disable	This code is used to disable one shot call waiting.
Call Transfer	This code is used to enable call transfer that allows you to transfer an incoming call (that you have answered) to another phone.
Unconditional Call Forward Enable	This code is used to enable unconditional call forwarding. Incoming calls are always forwarded to a specified number without any condition.
Unconditional Call Forward Disable	This code is used to disable unconditional call forwarding.
No Answer Call Forward Enable	This code is used to enable call forwarding when there is no answer at a SIP number (no one picked up the connected phone that uses the SIP number).
No Answer Call Forward Disable	This code is used to disable call forwarding when there is no answer at a SIP number (no one picked up the connected phone that uses the SIP number).
Call Forward When Busy Enable	This code is used to enable call forwarding when the phone is busy.
Call Forward When Busy Disable	This code is used to disable call forwarding when the phone is busy.
Do Not Disturb Enable	This code is used to turn the do not disturb feature on. This has the Router reject all calls destined to the phone line.
Do Not Disturb Disable	This code is used to turn the Do Not Disturb feature off.
Call Return	Specify the key combinations that you can enter to place a call to the last number that called you.
Call Completion on Busy Subscriber (CCBS) Deactivate	Call Completion on Busy Subscriber (CCBS) lets a subscriber have the VoIP server alert him when a called subscriber becomes available if the subscriber's line was busy when the call was attempted. Enter the key combinations that you can enter to disable CCBS.

Table 63 SIP > SIP Service Provider: Edit (continued)

LABEL	DESCRIPTION
Outgoing SIP	Enter the key combinations that you can enter to select the SIP account that you use to make outgoing calls. If you enter #12(by default)<SIP account index number>#<the phone number you want to call>, #1201#12345678 for example, the Router uses the first SIP account to call 12345678.
Dial Plan	
Dial Plan Enable	Select this to activate the dial plan rules you specify in the text box provided.

18.3 Phone Screen

Use this screen to maintain settings that depend on which region of the world the Router is in. To access this screen, click **VoIP > Phone**.

Figure 68 VoIP > Phone



Region Setting : Spain ▼
Call Service Mode : Europe Type ▼
Apply Undo

Table 64 VoIP > Phone

LABEL	DESCRIPTION
Region Setting	Select the place in which the Router is located.
Call Service Mode	Select the mode for supplementary phone services (call hold, call waiting, call transfer and three-way conference calls) that your VoIP service provider supports. <ul style="list-style-type: none">• Europe Type - use supplementary phone services in European mode.• USA Type - use supplementary phone services American mode. You might have to subscribe to these services to use them. Contact your VoIP service provider.

18.4 Call Rule Screen

Use this screen to add, edit, or remove speed-dial numbers for outgoing calls. Speed dial provides shortcuts for dialing frequently-used (VoIP) phone numbers. You also have to create speed-dial entries if you want to call SIP numbers that contain letters. Once you have configured a speed dial rule, you can use a shortcut (the speed dial number, #01 for example) on your phone's keypad to call the phone number.

To access this screen, click **VoIP > Call Rule**.

Figure 69 VoIP > Call Rule

Keys	Number	Description
#01	<input type="text"/>	<input type="text"/>
#02	<input type="text"/>	<input type="text"/>
#03	<input type="text"/>	<input type="text"/>
#04	<input type="text"/>	<input type="text"/>
#05	<input type="text"/>	<input type="text"/>
#06	<input type="text"/>	<input type="text"/>
#07	<input type="text"/>	<input type="text"/>
#08	<input type="text"/>	<input type="text"/>
#09	<input type="text"/>	<input type="text"/>
#10	<input type="text"/>	<input type="text"/>

Table 65 VoIP > Call Rule

LABEL	DESCRIPTION
Clear all speed dials	Click this to erase all the speed-dial entries.
Keys	This field displays the speed-dial number you should dial to use this entry.
Number	Enter the SIP number you want the Router to call when you dial the speed-dial number.
Description	Enter a short description to identify the party you call when you dial the speed-dial number. You can use up to 127 printable ASCII characters.

19.1 The Log Screen

Click **System Monitor > Log** to open the **Log** screen. Use the **Log** screen to see the system logs for the categories that you select in the upper left drop-down list box.

Figure 70 System Monitor > Log

#	Time	Level	Message
1	Jan 1 01:23:48	INFO	received REQUEST
2	Jan 1 01:23:48	INFO	sending NAK
3	Jan 1 01:23:53	INFO	received DISCOVER
4	Jan 1 01:23:55	INFO	DHCP client connect,IP:192.168.1.33
5	Jan 1 01:23:55	INFO	sending OFFER of 192.168.1.33
6	Jan 1 01:23:56	INFO	received REQUEST
7	Jan 1 01:23:56	INFO	server_id = c0a80101
8	Jan 1 01:23:56	INFO	sending ACK to 192.168.1.33
9	Jan 1 01:23:56	INFO	DHCP client connect,IP:192.168.1.33
10	Jan 1 01:58:58	INFO	received REQUEST
11	Jan 1 01:58:58	INFO	sending NAK
12	Jan 1 01:59:04	INFO	received DISCOVER

Table 66 System Monitor > Log

LABEL	DESCRIPTION
Level	Select a severity level from the drop-down list box. This filters search results according to the severity level you have selected. When you select a severity, the Router searches through all logs of that severity or higher.
Refresh	Click this to renew the log screen.
Clear Logs	Click this to delete all the logs.
Export	Click this to save a copy of the logs to your computer.
Email Log Now	Click this to have the Router send the log to the email server you configured in the Log Setting screen.
Time	This field displays the time the log was recorded.
Level	This field displays the severity level of the logs that the device is to send to this syslog server.
Messages	This field states the reason for the log.

19.2 The WAN Traffic Status Screen

Click **System Monitor > Traffic Status** to open the **WAN Traffic Status** screen. You can view the WAN traffic statistics in this screen.

Figure 71 System Monitor > Traffic Status > WAN

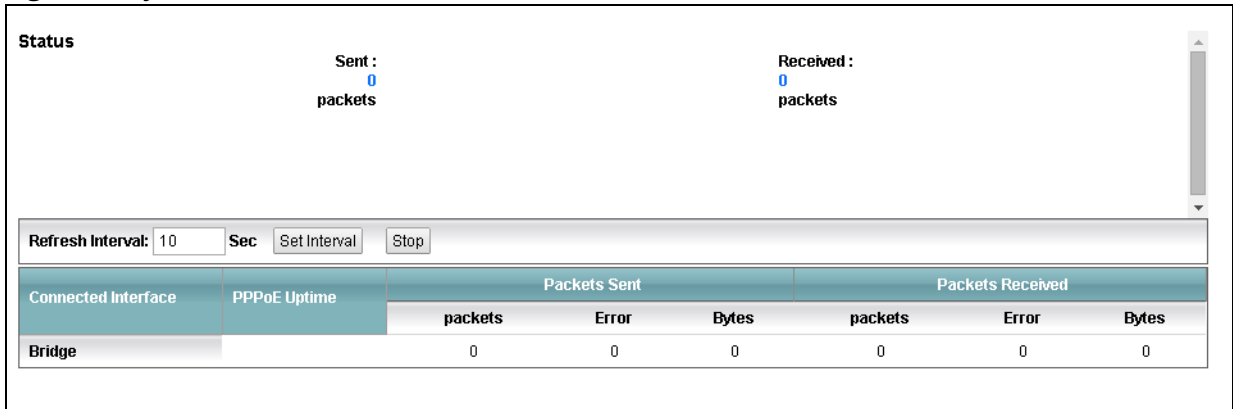


Table 67 System Monitor > Traffic Status > WAN

LABEL	DESCRIPTION
Status	This shows the number of bytes sent and received through the WAN interface of the Router.
Refresh Interval	Specify how often you want the Router to update this screen and click Set Interval to apply the change. Click Stop to halt updating of the screen.
Connected Interface	This shows the name of the WAN interface that is currently connected.
Packets Sent /Received	
Data	This indicates the number of transmitted/received packets on this interface.
Error	This indicates the number of frames with errors transmitted/received on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.

19.3 The LAN Traffic Status Screen

Click **System Monitor > Traffic Status > LAN** to open the following screen. You can view the LAN traffic statistics in this screen.

Figure 72 System Monitor > Traffic Status > LAN

Refresh Interval: <input type="text" value="10"/> Sec <input type="button" value="Set Interval"/> <input type="button" value="Stop"/>					
Interface	LAN1	LAN2	LAN3	LAN4	2.4G Wireless
Bytes Sent	9081892	9081892	9081892	82885325	0
Bytes Received	0	0	0	10457565	0

Interface	LAN1	LAN2	LAN3	LAN4	2.4G Wireless	
Sent (Packet)	Data	39152	39152	39153	173759	0
	Error	0	0	0	0	0
	Drop	0	0	0	0	0
Received (Packet)	Data	0	0	0	128193	0
	Error	0	0	0	0	0
	Drop	0	0	0	0	0

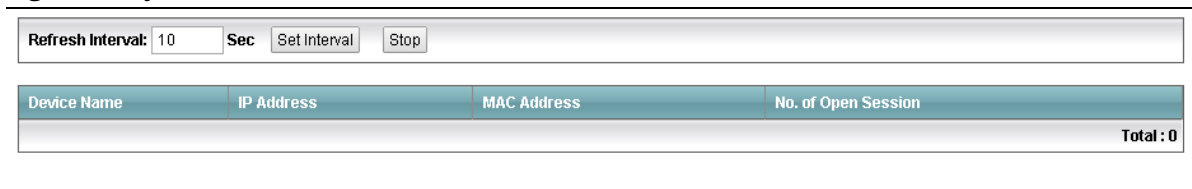
Table 68 System Monitor > Traffic Status > LAN

LABEL	DESCRIPTION
Refresh Interval	Specify how often you want the Router to update this screen and click Set Interval to apply the change. Click Stop to halt updating of the screen.
Interface	This shows the LAN or WLAN interface.
Bytes Sent	This indicates the number of bytes transmitted on this interface.
Bytes Received	This indicates the number of bytes received on this interface.
Interface	This shows the LAN or WLAN interface.
Sent (Packet)	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Received (Packet)	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.

19.4 The NAT Traffic Status Screen

Click **System Monitor > Traffic Status > NAT** to open the following screen. You can view the NAT status of the Router's clients in this screen.

Figure 73 System Monitor > Traffic Status > NAT



The screenshot shows a control panel at the top with a text input for 'Refresh Interval' set to '10', followed by the label 'Sec' and two buttons: 'Set Interval' and 'Stop'. Below this is a table with a teal header row containing the following columns: 'Device Name', 'IP Address', 'MAC Address', and 'No. of Open Session'. The table body is currently empty, and a 'Total : 0' label is positioned at the bottom right of the table area.

Table 69 System Monitor > Traffic Status > NAT

LABEL	DESCRIPTION
Refresh Interval	Specify how often you want the Router to update this screen and click Set Interval to apply the change. Click Stop to halt updating of the screen.
Device Name	This shows the name of the client.
IP Address	This shows the IP address of the client.
MAC Address	This shows the MAC address of the client.
No. of Open Session	This shows the number of NAT sessions used by the client.
Total	This shows the total number of NAT sessions currently open on the Router.

19.5 The VoIP Status Screen

Click **System Monitor > VoIP Status** to open the following screen. You can view the VoIP traffic statistics in this screen.

Figure 74 System Monitor > VoIP Status

The screenshot shows the VoIP Status screen with a 'Refresh Interval' of 10 seconds. It contains three tables: SIP Status, Call Status, and a summary table for Phone1.

SIP Status						
Account	Registration	Last Registration	URL	Message Waiting	Last Incoming Number	Last Outgoing Number
SIP1	Disabled	0:00:00	ChangeMe@telefonica.net	0	N/A	N/A
SIP2	Disabled	0:00:00	ChangeMe@telefonica.net	0	N/A	N/A
SIP3	Disabled	0:00:00	ChangeMe@telefonica.net	0	N/A	N/A
SIP4	Disabled	0:00:00	ChangeMe@telefonica.net	0	N/A	N/A

Call Status				
Account	Duration	Status	Codec	Peer Number
SIP1	0	Idle		None
SIP2	0	Idle		None
SIP3	0	Idle		None
SIP4	0	Idle		None

Account	Outgoing Number	Incoming Number	Phone State
Phone1	N/A	N/A	ONHOOK

Table 70 System Monitor > VoIP Status

LABEL	DESCRIPTION
Refresh Interval	Specify how often you want the Router to update this screen and click Set Interval to apply the change.
SIP Status	
Account	This column displays each SIP account in the Router.
Registration	This field displays the current registration status of the SIP account. You can change this in the Status screen. Registered - The SIP account is registered with a SIP server. Not Registered - The last time the Router tried to register the SIP account with the SIP server, the attempt failed. The Router automatically tries to register the SIP account when you turn on the Router or when you activate it. Inactive - The SIP account is not active. You can activate it in VoIP > SIP > SIP Account .
Last Registration	This field displays the last time you successfully registered the SIP account. The field is blank if you never successfully registered this account.
URL	This field displays the account number and service domain of the SIP account. You can change these in the VoIP > SIP screens.
Message Waiting	This field indicates whether or not there are any messages waiting for the SIP account.

Table 70 System Monitor > VoIP Status (continued)

LABEL	DESCRIPTION
Last Incoming Number	This field displays the last number that called the SIP account. The field is blank if no number has ever dialed the SIP account.
Last Outgoing Number	This field displays the last number the SIP account called. The field is blank if the SIP account has never dialed a number.
Call Status	
Account	This column displays each SIP account in the Router.
Duration	This field displays how long the current call has lasted.
Status	This field displays the current state of the phone call. Idle - There are no current VoIP calls, incoming calls or outgoing calls being made. Dial - The callee's phone is ringing. Ring - The phone is ringing for an incoming VoIP call. Process - There is a VoIP call in progress. DISC - The callee's line is busy, the callee hung up or your phone was left off the hook.
Codec	This field displays what voice codec is being used for a current VoIP call through a phone port.
Peer Number	This field displays the SIP number of the party that is currently engaged in a VoIP call through a phone port.
Phone Status	
Account	This field displays the phone accounts of the Router.
Outgoing Number	This field displays the SIP number that you use to make calls on this phone port.
Incoming Number	This field displays the SIP number that you use to receive calls on this phone port.
Phone State	This field shows whether or the phone connected to the subscriber port is on-hook (ONHOOK) or off-hook (OFFHOOK).

20.1 Overview

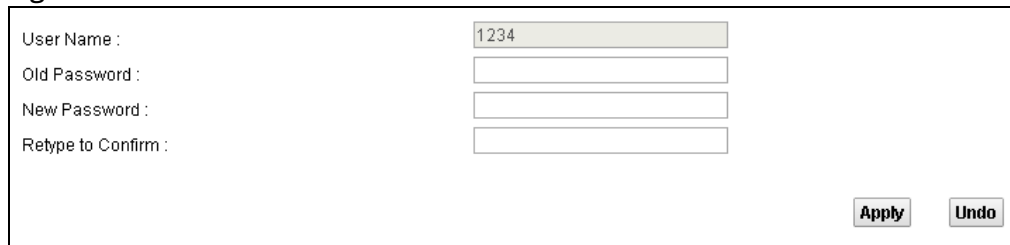
You can configure the system password in the **User Account** screen.

20.2 The User Account Screen

Use the **User Account** screen to configure system password.

Click **Maintenance > User Account** to open the following screen.

Figure 75 Maintenance > User Account



The screenshot shows a web interface for configuring a user account. It features four text input fields stacked vertically. The first field, labeled 'User Name', contains the text '1234'. The other three fields are empty. Below the fields are two buttons: 'Apply' and 'Undo'.

Table 71 Maintenance > User Account

LABEL	DESCRIPTION
User Name	This is the name of the user account.
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type your new system password (up to 30 characters). Note that as you type a password, the screen displays a (*) for each character you type. After you change the password, use the new password to access the Router.
Retype to Confirm	Type the new password again for confirmation.

21.1 The TR-069 Screen

Click **Maintenance > TR-069 Client** to open the following screen. Use this screen to configure your Router to be managed by an ACS.

Figure 76 Maintenance > TR-069 Client

Table 72 Maintenance > TR-069 Client

LABEL	DESCRIPTION
CWMP	Select Enable to allow the Router to be managed by a management server. Otherwise, select Disable to not allow the Router to be managed by a management server.
ACS URL	Enter the URL or IP address of the auto-configuration server.
ACS User Name	Enter the TR-069 user name for authentication with the auto-configuration server.
ACS Password	Enter the TR-069 password for authentication with the auto-configuration server.
Connection Request Path	Type the IP address or domain name of the Router. The management server uses this path to verify the Router.

Table 72 Maintenance > TR-069 Client (continued)

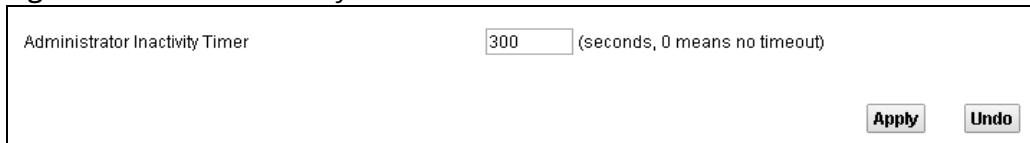
LABEL	DESCRIPTION
Connection Request Port	The default port for access to the Router from the management server is the HTTP port, port 80. If you change it, make sure it does not conflict with another port on your network and it is recommended to use a port number above 1024 (not a commonly used port). The management server should use this port to connect to the Router. You may need to alter your NAT port forwarding rules if they were already configured.
Connection Request User Name	Enter the connection request user name. When the ACS makes a connection request to the Router, this user name is used to authenticate the ACS.
Connection Request Password	Enter the connection request password. When the ACS makes a connection request to the Router, this password is used to authenticate the ACS.
Inform	Select Enable for the Router to send periodic inform via TR-069 on the WAN. Otherwise, select Disable .
Inform Interval	Enter the time interval (in seconds) at which the Router sends information to the auto-configuration server.

22.1 The System Screen

Use the **System** screen to configure the system's inactivity time-out interval.

Click **Maintenance > System** to open the following screen.

Figure 77 Maintenance > System



The screenshot shows a configuration screen for the Administrator Inactivity Timer. It features a text input field containing the value '300', followed by the text '(seconds, 0 means no timeout)'. Below the input field are two buttons: 'Apply' and 'Undo'.

Table 73 Maintenance > System

LABEL	DESCRIPTION
Administrator Inactivity Timer	Type how manyseconds a management session (either via the web configurator) can be left idle before the session times out. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).

23.1 The Time Setting Screen

To change your Router's time and date, click **Maintenance > Time**. The screen appears as shown. Use this screen to configure the Router's time based on your local time zone.

Figure 78 Maintenance > Time Setting

Table 74 Maintenance > System > Time Setting

LABEL	DESCRIPTION
Current Time	This field displays the date and time of your Router.
Manual	Select this to enter the time and date manually in hh:mm:ss and yyyy/mm/dd format.
Get from Time Server	Select this to have the Router get the time automatically from a time server.
Time Server Address 1, 2	Enter the IP address or URL (up to 31 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).

Table 74 Maintenance > System > Time Setting (continued)

LABEL	DESCRIPTION
Daylight Savings	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.
Start/End Date	Configure the day and time when Daylight Saving Time starts/ends if you selected Daylight Savings . The o'clock field uses the 24 hour format.

24.1 The Log Setting Screen

To change your Router's log settings, click **Maintenance > Log Setting**. The screen appears as shown.

Figure 79 Maintenance > Log Setting

The screenshot displays the 'Log Setting' configuration page, organized into several sections:

- Syslog Settings:** Includes a checked 'Active' checkbox, a 'Mode' dropdown set to 'Local File', a text input for 'Syslog Server IP Address', and a text input for 'Syslog Server UDP Port' with the value '514'.
- Email Log Settings:** Includes a checked 'SMTP Authentication' checkbox, and text inputs for 'Mail Server' (with a note '(Outgoing SMTP Server Name or IP Address)'), 'Mail Subject', 'From', 'To' (with a note '(E-Mail Address)'), 'User Name', and 'Password'. It also features a 'Log Schedule' dropdown set to 'None', a 'Day For Sending Log' dropdown set to 'Sunday', and 'Time for Sending Log' inputs for 'hour' (0) and 'minute' (0). A 'Clear log after sending mail' checkbox is present and unchecked.
- Email Alarm Log Settings:** Includes a text input for 'Send Alarm to' (with a note '(E-Mail Address)') and a text input for 'Alarm Interval' (with a note '(Second 0~3600)').
- Active Log and Select Level:** A table with 'Log Category' and 'Log Level' columns. All categories are checked, and all levels are set to 'ALL':

Log Category	Log Level
<input checked="" type="checkbox"/> WAN-DHCP	ALL
<input checked="" type="checkbox"/> ETHER	ALL
<input checked="" type="checkbox"/> PPP	ALL
<input checked="" type="checkbox"/> System Maintenance	ALL
<input checked="" type="checkbox"/> Remote Management	ALL
<input checked="" type="checkbox"/> TR069	ALL
<input checked="" type="checkbox"/> NTP	ALL
<input checked="" type="checkbox"/> DDNS	ALL
<input checked="" type="checkbox"/> NAT	ALL
<input checked="" type="checkbox"/> Firewall	ALL
<input checked="" type="checkbox"/> DHCP-Server	ALL
<input checked="" type="checkbox"/> WLAN	ALL
<input checked="" type="checkbox"/> Internet	ALL
<input checked="" type="checkbox"/> UPnP	ALL
<input checked="" type="checkbox"/> DoS	ALL

At the bottom right, there are 'Apply' and 'Undo' buttons.

Table 75 Maintenance > Log Setting

LABEL	DESCRIPTION
Syslog Logging	Select the Active check box to enable syslog logging.
Mode	Select Local File to have the Router save the log file locally. Select Local File and Remote to have the Router save the log file locally and send it to an external syslog server.
Syslog Server IP Address	If you select Local File and Remote in the Mode field, enter the server name or IP address of the syslog server that will log the selected categories of logs.
Syslog Server UDP Port	If you select Local File and Remote in the Mode field, enter the port number used by the syslog server.
SMTP Authentication	SMTP (Simple Mail Transfer Protocol) is the message-exchange standard for the Internet. SMTP enables you to move messages from one E-mail server to another. Select the check box to activate SMTP authentication. If mail server authentication is needed but this feature is disabled, you will not receive the E-mail logs.
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via E-mail.
Mail Subject	Type a title that you want to be in the subject line of the system log e-mail message that the Router sends.
From	Specify where the logs are sent from.
To	The Router sends logs to the e-mail address specified in this field. If this field is left blank, the Router does not send logs via E-mail.
User Name	Enter the user name (up to 32 characters) (usually the user name of a mail account).
Password	Enter the password associated with the user name above.
Log Schedule	Specify the schedule for sending log. Specify days and times for sending logs in the following fields.
Day For Sending Log	Specify the day for sending log.
Time for Sending Log	Specify the time for sending log.
Clear log after sending mail	Select this to delete all the logs after the Router sends an E-mail of the logs.
Send Alarm to	Alerts are real-time notifications that are sent as soon as an event, such as a DoS attack, system error, or forbidden web access attempt occurs. Enter the E-mail address where the alert messages will be sent. Alerts include system errors, attacks and attempted access to blocked web sites. If this field is left blank, alert messages will not be sent via E-mail.

Table 75 Maintenance > Log Setting (continued)

LABEL	DESCRIPTION
Alarm Interval	Specify the number of seconds between the sending of alarm log e-mails.
Log Category	Select the categories of logs that you want to record.
Log Level	Select the severity level of logs that you want to record. If you want to record all logs, select ALL .

25.1 The Firmware Upgrade Screen

Click **Maintenance > Firmware Upgrade** to open the **following** screen. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to three minutes. After a successful upload, the system will reboot.



-  Only use firmware for your device's specific model. Refer to the label on the bottom of your Router.
-  Do NOT turn off the Router while firmware upload is in progress!

Figure 80 Maintenance > Firmware Upgrade



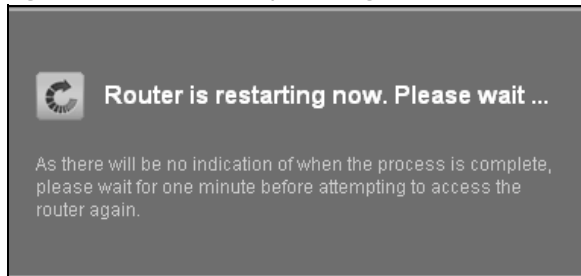
Upgrade Firmware
Current Firmware Version: ES_B7
FilePath : No file chosen

Table 76 Maintenance > Firmware Upgrade

LABEL	DESCRIPTION
Upgrade Firmware	Use these fields to upload firmware to the Router.
Current Firmware Version	This is the present firmware version.
File Path	Click Choose File and find the file you want to upload.
Upload	Click this to begin the upload process. This process may take up to three minutes.

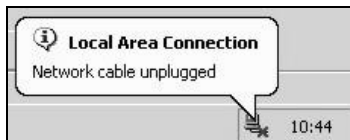
After you see the firmware updating screen, wait a few minutes before logging into the Router again.

Figure 81 Firmware Uploading



The Router automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

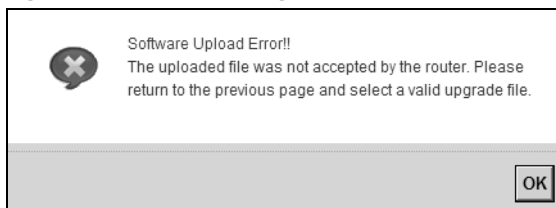
Figure 82 Network Temporarily Disconnected



After two minutes, log in again and check your new firmware version in the **Status** screen.

If the upload was not successful, an error screen will appear. Click **OK** to go back to the **Firmware Upgrade** screen.

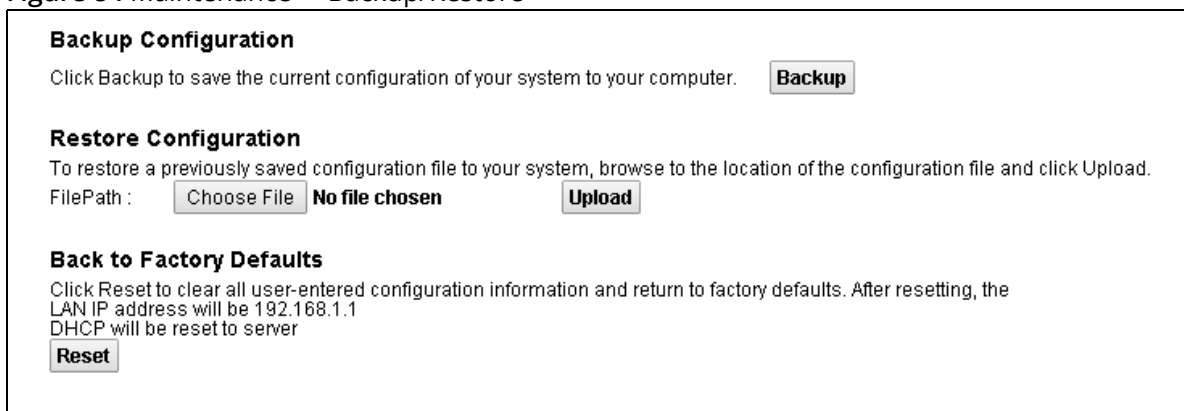
Figure 83 Error Message



26.1 The Backup/Restore Screen

Click **Maintenance > Backup/Restore**. Information related to factory defaults, backup configuration, and restoring configuration appears in this screen, as shown next.

Figure 84 Maintenance > Backup/Restore



Backup Configuration

Backup Configuration allows you to back up (save) the Router's current configuration to a file on your computer. Once your Router is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the Router's current configuration to your computer.

Restore Configuration

Restore Configuration allows you to upload a new or previously saved configuration file from your computer to your Router.

Table 77 Restore Configuration

LABEL	DESCRIPTION
File Path	Click Choose File and find the file you want to restore.
Upload	Click this to begin the upload process.
Reset	Click this to reset your device settings back to the factory default.

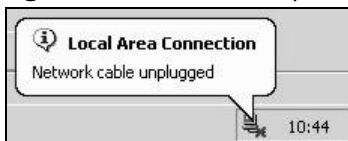


Do not turn off the Router while configuration file upload is in progress.

After the Router configuration has been restored successfully, the login screen appears. Login again to restart the Router.

The Router automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 85 Network Temporarily Disconnected



If you restore the default configuration, you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1).

If the upload was not successful, an error screen will appear. Click **OK** to go back to the **Configuration** screen.

Reset to Factory Defaults

Click the **Reset** button to clear all user-entered configuration information and return the Router to its factory defaults. The following warning screen appears.

Figure 86 Reset Warning Message

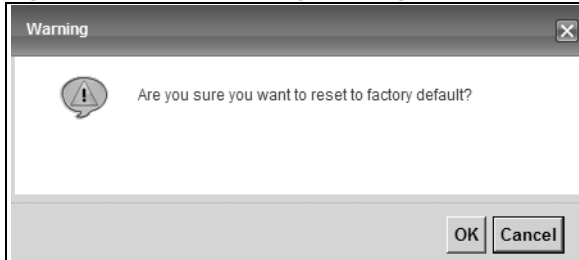
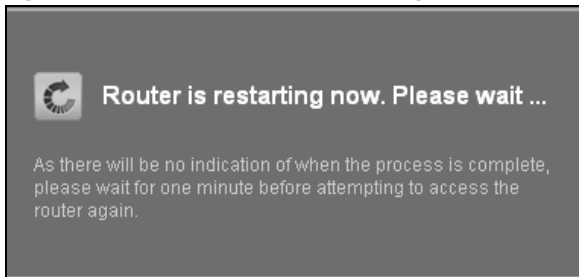


Figure 87 Reset In Process Message



You can also press the **Reset** button on the back panel to reset the factory defaults of your Router. Refer to [Chapter 1 on page 9](#) for more information on the **Reset** button.

26.2 The Reboot Screen

System restart allows you to reboot the Router remotely without turning the power off. You may need to do this if the Router hangs, for example.

Click **Maintenance > Reboot**. Click the **Reboot** button to have the Router reboot. This does not affect the Router's configuration.

27.1 The General Screen

Remote management allows you to determine which services/protocols can access which Router interface (if any) from which computers.

Click **Maintenance > Remote MGMT** to display the **General** screen. Select **Enable** to activate remote management on the Router.

Figure 88 Maintenance > Remote MGMT > General



Active Enabled Disabled

Apply Undo

27.2 The WWW Screen

Use the **WWW** screen to specify how to connect to the Router from a web browser. Click **Maintenance > Remote MGMT > WWW** screen.

Maintenance > Remote MGMT > WWW

Server Port:

Server Access:

Secured Client IP Address:

All

From: To:

Range

From: To:

From: To:

Remote MGMT enables to access this device remotely from a WAN and/or LAN connection by HTTPS.

Server Port:

Server Access:

Secured Client IP Address: Lan

All

From: To:

Range

From: To:

From: To:

Secured Client IP Address: Wan

All

From: To:

Range

From: To:

From: To:

From: To:

Note:

- 1: For UPnP to function normally, the HTTP and HTTPS service must be available for LAN computers using UPnP.
- 2: The session will be reset after apply.
- 3: The Range IP could be IPv4 or IPv6.

Table 78 Maintenance > Remote MGMT > WWW

LABEL	DESCRIPTION
Server Port	This displays the service port number for accessing the Router using HTTP or HTTPS. If the number is grayed out, it is not editable.
Server Access	Select the interfaces through which a computer may access the Router using this service. Note: It is recommended if you are allowing WAN access even temporarily to change the default password (in Maintenance > User Account). To allow access from the WAN, you will need to configure a WAN to Router firewall rule.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to communicate with the Router using this service. Select All to allow any computer to access the Router using this service. Choose Range to just allow the computers with an IP address in the range that you specify to access the Router using this service.

27.3 Telnet Screen

You can use Telnet to access the Device's command line interface. Specify which interfaces allow Telnet access and from which IP address the access can come.

Click **Maintenance > Remote MGMT > Telnet** tab to display the screen as shown.

Figure 89 Maintenance > Remote MGMT > Telnet

Server Port: 23

Server Access: Disable

Secured Client IP Address: All

Range

From: 0.0.0.0 To: 0.0.0.0

From: 0.0.0.0 To: 0.0.0.0

From: 0.0.0.0 To: 0.0.0.0

Note :

1. The session will be reset after apply.

2. The Range IP could be IPv4 or IPv6.

Apply Undo

Table 79 Maintenance > Remote MGMT > Telnet

LABEL	DESCRIPTION
Server Port	This displays the service port number for accessing the Router. If the number is grayed out, it is not editable.
Server Access	Select the interfaces through which a computer may access the Router using this service. Note: It is recommended if you are allowing WAN access even temporarily to change the default password (in Maintenance > User Account). To allow access from the WAN, you will need to configure a WAN to Router firewall rule.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to communicate with the Router using this service. Select All to allow any computer to access the Router using this service. Choose Range to just allow the computers with an IP address in the range that you specify to access the Router using this service.

27.4 FTP Screen

You can use FTP (File Transfer Protocol) to upload and download the Router's firmware and configuration files. To use this feature, your computer must have an FTP client.

Use this screen to specify which interfaces allow FTP access and from which IP address the access can come. To change your Router's FTP settings, click **Maintenance > Remote MGMT > FTP**. The screen appears as shown.

Figure 90 Maintenance > Remote MGMT > FTP

Server Port: 21

Server Access: LAN

Secured Client IP Address: All

Range

From: 0.0.0.0 To: 0.0.0.0

From: 0.0.0.0 To: 0.0.0.0

From: 0.0.0.0 To: 0.0.0.0

Note :

1. The session will be reset after apply.

2. The Range IP could be IPv4 or IPv6.

Apply Undo

Table 80 Maintenance > Remote MGMT > FTP

LABEL	DESCRIPTION
Server Port	This displays the service port number for accessing the Router. If the number is grayed out, it is not editable.
Server Access	Select the interfaces through which a computer may access the Router using this service.
Secured Client IP Address	<p>A secured client is a “trusted” computer that is allowed to communicate with the Router using this service.</p> <p>Select All to allow any computer to access the Router using this service.</p> <p>Choose Range to just allow the computers with an IP address in the range that you specify to access the Router using this service.</p>

27.5 SNMP Screen

To change your Router's SNMP settings, click **Maintenance > Remote MGMT > SNMP** tab. The screen appears as shown.

Figure 91 Maintenance > Remote MGMT > SNMP

Server Port: 161

Server Access: Disable

SNMPv3: Enable Disable

Secured Client IP Address: All

Range

From: 0.0.0.0 To: 0.0.0.0

From: 0.0.0.0 To: 0.0.0.0

From: 0.0.0.0 To: 0.0.0.0

SNMP Setup

Get Community: public

Set Community: public

Trap Community: public

IPv4 Trap Destination: 0.0.0.0

IPv6 Trap Destination: ::1

Note :

- 1.The session will be reset after apply.
- 2.The Range IP could be IPv4 or IPv6.

Apply Undo

Table 81 Maintenance > Remote MGMT > SNMP

LABEL	DESCRIPTION
Server Port	This displays the port the SNMP agent listens on. If the number is grayed out, it is not editable.
Server Access	Select the interfaces through which a computer may access the Router using this service.
SNMPv3	Select Enable to activate the SNMPv3 feature.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to access the SNMP agent on the Router. Select All to allow any computer to access the SNMP agent. Choose Range to just allow the computers with an IP address in the range that you specify to access the Router using this service.

Table 81 Maintenance > Remote MGMT > SNMP (continued)

LABEL	DESCRIPTION
Get Community	Enter the Get Community , which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the Set community , which is the password for incoming Set requests from the management station. The default is public and allows all requests.
Trap Community	Type the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
IPv4 Trap Destination	Type the IPv4 IP address of the station to send your SNMP traps to.
IPv6 Trap Destination	Type the IPv6 IP address of the station to send your SNMP traps to.

27.6 DNS Screen

Use this screen to set from which IP address the Router will accept DNS queries and on which interface it can send them your Router's DNS settings. This feature is not available when the Router is set to bridge mode. Click **Maintenance > Remote MGMT > DNS** to change your Router's DNS settings.

Figure 92 Maintenance > Remote MGMT > DNS

Server Port: 53

Server Access: LAN

Secured Client IP Address: All Range

From: 0.0.0.0 To: 0.0.0.0

From: 0.0.0.0 To: 0.0.0.0

From: 0.0.0.0 To: 0.0.0.0

Note:
1.The Range IP could be IPv4 or IPv6.

Apply Undo

Table 82 Maintenance > Remote MGMT > DNS

LABEL	DESCRIPTION
Server Port	This displays the service port number for accessing the Router. If the number is grayed out, it is not editable.

Table 82 Maintenance > Remote MGMT > DNS (continued)

LABEL	DESCRIPTION
Access Status	Select the interfaces through which a computer may send DNS queries to the Router.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to send DNS queries to the Router. Select All to allow any computer to send DNS queries to the Router. Choose Range to just allow the computers with an IP address in the range that you specify to send DNS queries to the Router.

27.7 ICMP Screen

To change your Router’s security settings, click **Maintenance > Remote MGMT > ICMP**. The screen appears as shown.

If an outside user attempts to probe an unsupported port on your Router, an ICMP response packet is automatically returned. This allows the outside user to know the Router exists. Your Router supports anti-probing, which prevents the ICMP response packet from being sent. This keeps outsiders from discovering your Router when unsupported ports are probed.

 If you want your device to respond to pings and requests for unauthorized services, you will also need to configure the firewall accordingly by disabling SPI.

Figure 93 Maintenance > Remote MGMT > ICMP

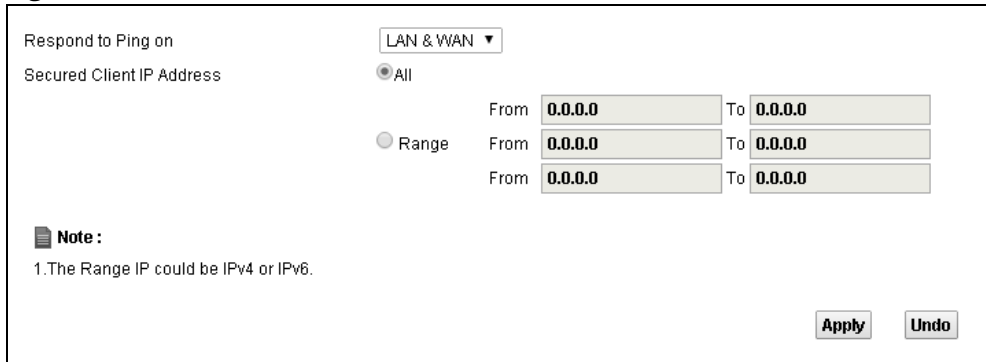


Table 83 Maintenance > Remote MGMT > ICMP

LABEL	DESCRIPTION
Respond to Ping on	The Router will not respond to any incoming Ping requests when Disable is selected. Select LAN to reply to incoming LAN Ping requests. Select WAN to reply to incoming WAN Ping requests. Otherwise select LAN & WAN to reply to both incoming LAN and WAN Ping requests.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to send Ping requests to the Router. Select All to allow any computer to send Ping requests to the Router. Choose Range to just allow the computers with an IP address in the range that you specify to send Ping requests to the Router.

27.8 SSH Screen

You can use Secure SHell (SSH) to securely access the Router’s command line interface. Specify which interfaces allow SSH access and from which IP address the access can come. SSH is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network.

Click **Maintenance > Remote MGMT > SSH** tab to display the screen as shown.

Figure 94 Maintenance > Remote MGMT > SSH

Server Port: 22

Server Access: LAN & WAN

Secured Client IP Address:Lan: All

Secured Client IP Address:Wan: All Range

From 192.168.1.33 To 192.168.1.254

From 172.20.25.1 To 172.20.25.254

From 172.20.45.1 To 172.20.45.254

From 80.58.63.129 To 80.58.63.190

From 172.20.25.1 To 172.20.25.254

From 172.20.45.1 To 172.20.45.254

From 193.152.37.193 To 193.152.37.206

Note :
1.The Range IP could be IPv4 or IPv6.

Apply Undo

Table 84 Maintenance > Remote MGMT > SSH

LABEL	DESCRIPTION
Server Port	This displays the service port number for accessing the Router. If the number is grayed out, it is not editable.
Server Access	Select the interfaces through which a computer may access the Router using this service. Note: It is recommended if you are allowing WAN access even temporarily to change the default password (in Maintenance > User Account). To allow access from the WAN, you will need to configure a WAN to Router firewall rule.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to communicate with the Router using this service. Select All to allow any computer to access the Router using this service. Choose Range to just allow the computers with an IP address in the range that you specify to access the Router using this service.

28.1 The Diagnostic Screen

Ping and traceroute help check availability of remote hosts and also help troubleshoot network or Internet connections. Click **Maintenance > Diagnostic** to open the **Diagnostic** screen shown next.

Figure 95 Maintenance > Diagnostic

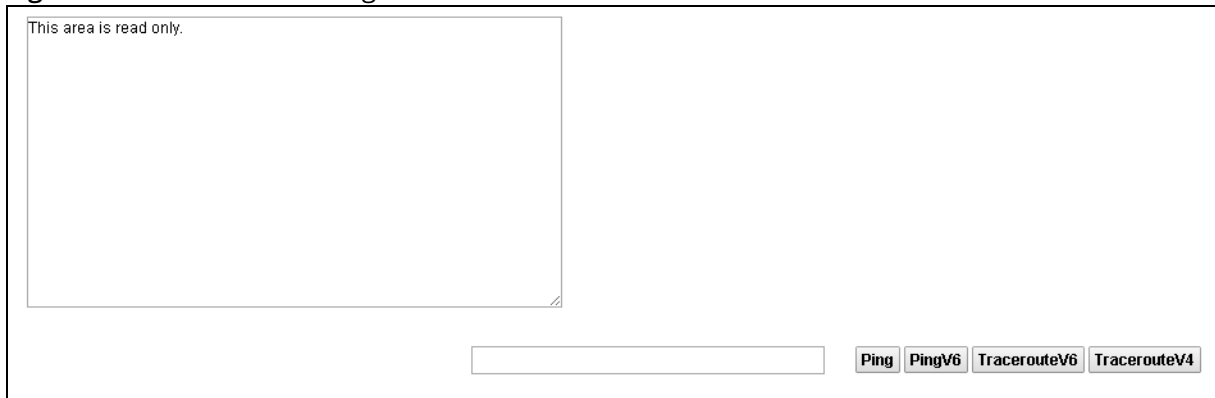


Table 85 Maintenance > Diagnostic

LABEL	DESCRIPTION
Ping	Type the IP address of a computer that you want to ping in order to test a connection. Click Ping and the ping statistics will show in the diagnostic .
PingV6	Click this to ping the IPv6 address that you entered.
TraceRouteV6	Click this to show the path that packets take from the system to the IPv6 address that you entered.
TraceRouteV4	Click this button to perform the traceroute function. This determines the path a packet takes to the specified host.

29.1 Overview

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- [Power, Hardware Connections, and LEDs](#)
- [Router Access and Login](#)
- [Internet Access](#)
- [Wireless Internet Access](#)
- [Phone Calls and VoIP](#)
- [UPnP](#)
- [UPnP](#)

29.2 Power, Hardware Connections, and LEDs



The Router does not turn on. None of the LEDs turn on.

- 1 Make sure the Router is turned on.
- 2 Make sure you are using the power adaptor or cord included with the Router.
- 3 Make sure the power adaptor or cord is connected to the Router and plugged in to an appropriate power source. Make sure the power source is turned on.
- 4 Turn the Router off and on.
- 5 If the problem continues, contact the vendor.



One of the LEDs does not behave as expected.


- 1 Make sure you understand the normal behavior of the LED. See [Section 1.3 on page 10](#).
- 2 Check the hardware connections. See [Section 1.2 on page 9](#).

- 3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.
- 4 Turn the Router off and on.
- 5 If the problem continues, contact the vendor.

29.3 Router Access and Login

 I forgot the IP address for the Router.

- 1 The default IP address is 192.168.1.1.
- 2 If you changed the IP address and have forgotten it, you might get the IP address of the Router by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the Router (it depends on the network), so enter this IP address in your Internet browser.
- 3 If this does not work, you have to reset the device to its factory defaults. See [Section 1.2 on page 9](#).

 I forgot the password.

- 1 The default admin password is **1234** and the default user password is **1234**.
- 2 If you can't remember the password, you have to reset the device to its factory defaults. See [Section 1.2 on page 9](#).

 I cannot see or access the **Login** screen in the web configurator.

- 1 Make sure you are using the correct IP address.
 - The default IP address is 192.168.1.1.
 - If you changed the IP address ([Section 8.1 on page 60](#)), use the new IP address.
 - If you changed the IP address and have forgotten it, see the troubleshooting suggestions for [I forgot the IP address for the Router](#).
- 2 Check the hardware connections, and make sure the LEDs are behaving as expected. See [Section 1.2 on page 9](#).
- 3 Make sure your Internet browser does not block pop-up windows and has JavaScript and Java enabled.
- 4 Reset the device to its factory defaults, and try to access the Router with the default IP address. See [Section 1.2 on page 9](#).

- 5 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Try to access the Router using another service, such as Telnet. If you can access the Router, check the remote management settings and firewall rules to find out why the Router does not respond to HTTP.
- If your computer is connected wirelessly, use a computer that is connected to a **ETHERNET** port.



I can see the **Login** screen, but I cannot log in to the Router.

- 1 Make sure you have entered the user name and password correctly. These fields are case-sensitive, so make sure [Caps Lock] is not on.
- 2 You cannot log in to the web configurator while someone is using Telnet to access the Router. Log out of the Router in the other session, or ask the person who is logged in to log out.
- 3 Turn the Router off and on.
- 4 If this does not work, you have to reset the device to its factory defaults. See [Section 29.2 on page 154](#).



I cannot Telnet to the Router.

See the troubleshooting suggestions for [I cannot see or access the Login screen in the web configurator](#). Ignore the suggestions about your browser.



I cannot use FTP to upload / download the configuration file. / I cannot use FTP to upload new firmware.

See the troubleshooting suggestions for [I cannot see or access the Login screen in the web configurator](#). Ignore the suggestions about your browser.

29.4 Internet Access



I cannot access the Internet.

- 1 Check the hardware connections, and make sure the LEDs are behaving as expected. See [Section 1.3 on page 10](#).
- 2 Make sure you entered your ISP account information correctly. These fields are case-sensitive, so make sure [Caps Lock] is not on.

- 3 If you are trying to access the Internet wirelessly, make sure the wireless settings in the wireless client are the same as the settings in the AP.
- 4 If you are trying to access the Internet wirelessly, make sure you have enabled the wireless LAN by the **Wifi/WPS** button or the **Network Setting > Wireless > General** screen.
- 5 Disconnect all the cables from your device, and follow the directions in [Section 1.2 on page 9](#). again.
- 6 If the problem continues, contact your ISP.



I cannot access the Internet anymore. I had access to the Internet (with the Router), but my Internet connection is not available anymore.

- 1 Check the hardware connections, and make sure the LEDs are behaving as expected. See [Section 1.3 on page 10](#).
- 2 Turn the Router off and on.
- 3 If the problem continues, contact your ISP.



The Internet connection is slow or intermittent.

- 1 There might be a lot of traffic on the network. Look at the LEDs, and check [Section 1.3 on page 10](#). If the Router is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
- 2 Turn the Router off and on.
- 3 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Check the settings for QoS. If it is disabled, you might consider activating it. If it is enabled, you might consider raising or lowering the priority for some applications.

29.5 Wireless Internet Access



What factors may cause intermittent or unstabled wireless connection? How can I solve this problem?

The following factors may cause interference:

- Obstacles: walls, ceilings, furniture, and so on.
- Building Materials: metal doors, aluminum studs.

- Electrical devices: microwaves, monitors, electric motors, cordless phones, and other wireless devices.

To optimize the speed and quality of your wireless connection, you can:

- Move your wireless device closer to the AP if the signal strength is low.
- Reduce wireless interference that may be caused by other wireless networks or surrounding wireless electronics such as cordless phones.
- Place the AP where there are minimum obstacles (such as walls and ceilings) between the AP and the wireless client.
- Reduce the number of wireless clients connecting to the same AP simultaneously, or add additional APs if necessary.
- Try closing some programs that use the Internet, especially peer-to-peer applications. If the wireless client is sending or receiving a lot of information, it may have too many programs open that use the Internet.



What wireless security modes does my Router support?

Wireless security is vital to your network. It protects communications between wireless stations, access points and the wired network.

The available security modes in your Router are as follows:

- **WPA2-PSK:** (recommended) This uses a pre-shared key with the WPA2 standard.
- **WPA-PSK:** This has the device use either WPA-PSK or WPA2-PSK depending on which security mode the wireless client uses.
- **WPA2:** WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA. It requires the use of a RADIUS server and is mostly used in business networks.
- **WPA:** Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. It requires the use of a RADIUS server and is mostly used in business networks.
- **WEP:** Wired Equivalent Privacy (WEP) encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private.

29.6 Phone Calls and VoIP



The telephone port won't work or the telephone lacks a dial tone.


- 1 Check the telephone connections and telephone wire.



I can access the Internet, but cannot make VoIP calls.

- 1 The **Telf** light should come on. Make sure that your telephone is connected to the **Telf1** port.
- 2 You can also check the VoIP status in the **System Info** screen.
- 3 If the VoIP settings are correct, use speed dial to make peer-to-peer calls. If you can make a call using speed dial, there may be something wrong with the SIP server, contact your VoIP service provider.


29.7 UPnP

 When using UPnP and the Router reboots, my computer cannot detect UPnP and refresh **My Network Places > Local Network**.

- 1 Disconnect the Ethernet cable from the Router's LAN port or from your computer.
- 2 Re-connect the Ethernet cable.

 The **Local Area Connection** icon for UPnP disappears in the screen.

Restart your computer.

 I cannot open special applications such as white board, file transfer and video when I use the MSN messenger.

- 1 Wait more than three minutes.
- 2 Restart the applications.

Safety Warnings

A Appendix

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.
- This product is for indoor use only (utilisation intérieure exclusivement).

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.

