LR-25G001

Dual-Band Wireless Gigabit Router

User Manual

TABLE OF CONTENTS

1. Introduction

Congratulations on your purchase of this outstanding product: LR-25G001 Dual-band wireless router. Wireless router LR-25G001 with Gigabit Ethernet switch embedded provides the perfect throughput, which allows to enjoy the unmatched Torrent download speed and multicast stream IPTV quality. Dual-band wireless module of LR-25G001 (802.11ac/b/g/n) provides the ability of concurrent 2.4GHz/5GHz operation, fully compatible with the most of end-user devices, such as cellphones, laptops, etc (regardless of the OS onboard). Thereby LR-25G001 reaches the best performance of wireless data transfer as well, allowing to minimize radio interference using 5GHz frequency for clients responsive to connection quality (especially for IPTV, VoIP services and so on)

1.1. Package List

- (1) WiFi Router LR-25G001:

- (1) Quick User Guide:

LAVA TELECOM

LR-25G001

Dual-Band Wireless Gigabit Router

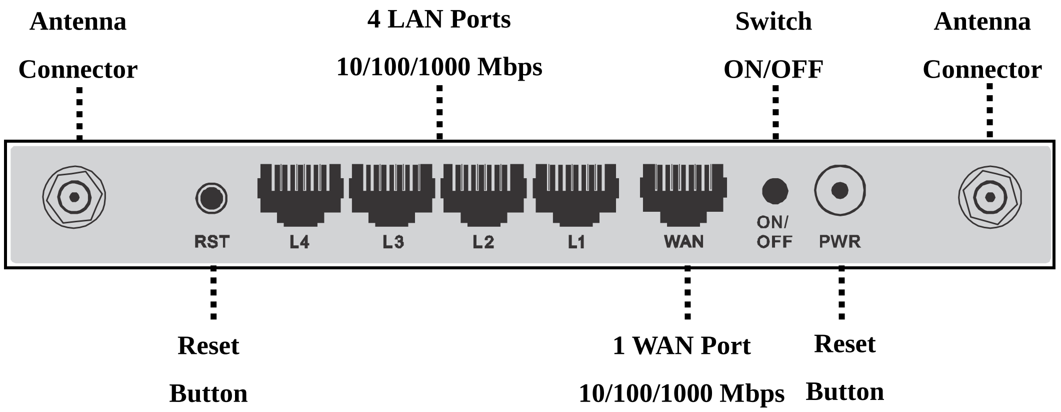
Quick Installation Guide

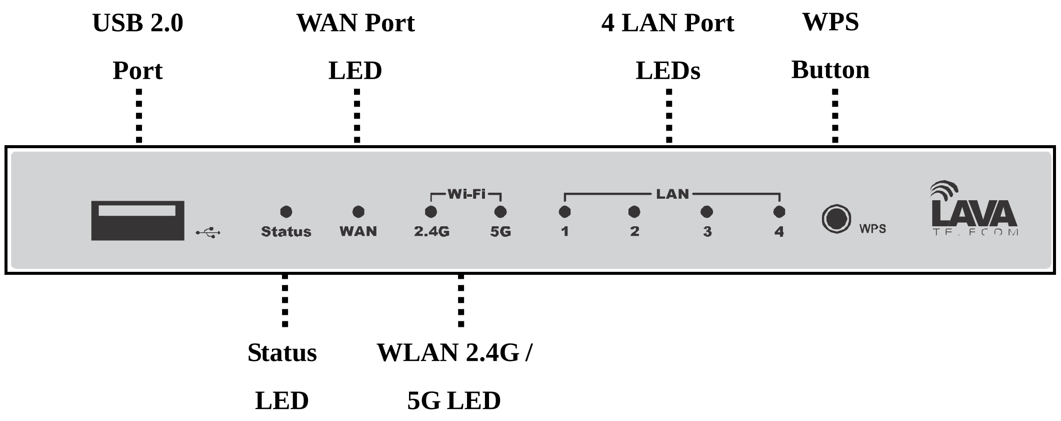
- (1) CD with User Manual:

- (1) Power Adapter:

1.2. Hardware Installation

1.2.1. Hardware configuration





1.2.2. LED indicators

- **Status / USB:**
  Lights up green: USB storage attached
  Blinks green: powered on / data access
  Blinks green frequently: reset mode

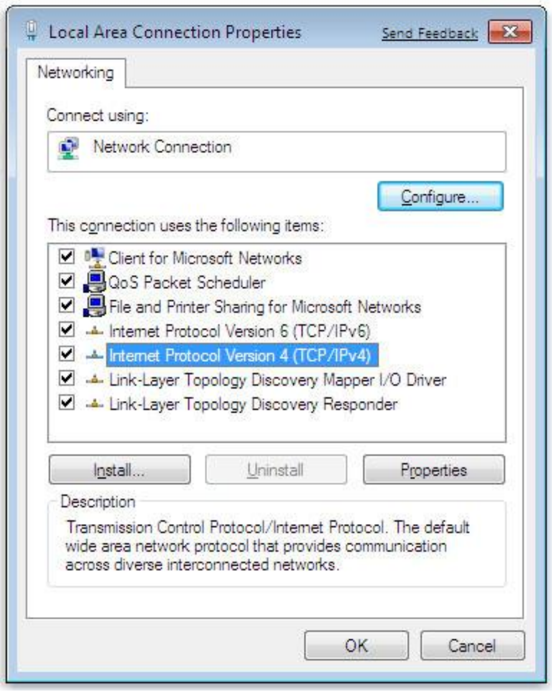
- **WAN / LAN 1-4 / WLAN 2.4G / 5G:**
  Lights up green: WiFi is on
  Blinks green: data access

1.2.3. How to Connect

- Connect your PC to LR-25G001 LAN 1~4 port
- Connect the WAN port of your LR-25G001 router to Internet with Ethernet cable provided by your ISP
- Plug the power jack into power socket
- Connect your USB storage or 3G dongle (if 3G WAN needed) to USB port of LR-25G001

2. Basic Configuration

Configure your network on PC for DHCP or Static IP on the 192.168.1.x subnet



Local Area Connection Properties

Send Feedback

Networking

Connect using:

Network Connection

Configure...

This connection uses the following items:

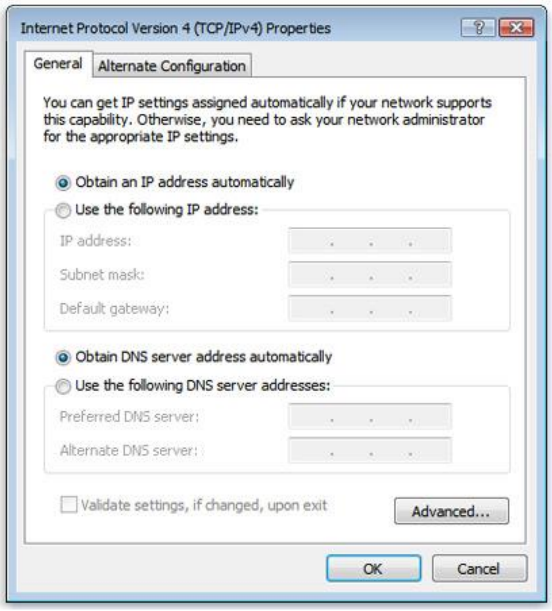
- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Install... Uninstall Properties

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

OK Cancel



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

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

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

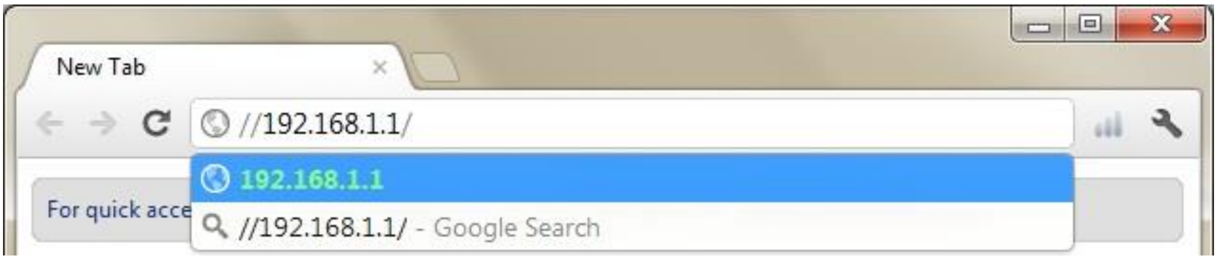
Alternate DNS server: . . .

□ Validate settings, if changed, upon exit

Advanced...

OK Cancel

Open your Internet browser and enter IP address http://192.168.1.1 into address bar



New Tab

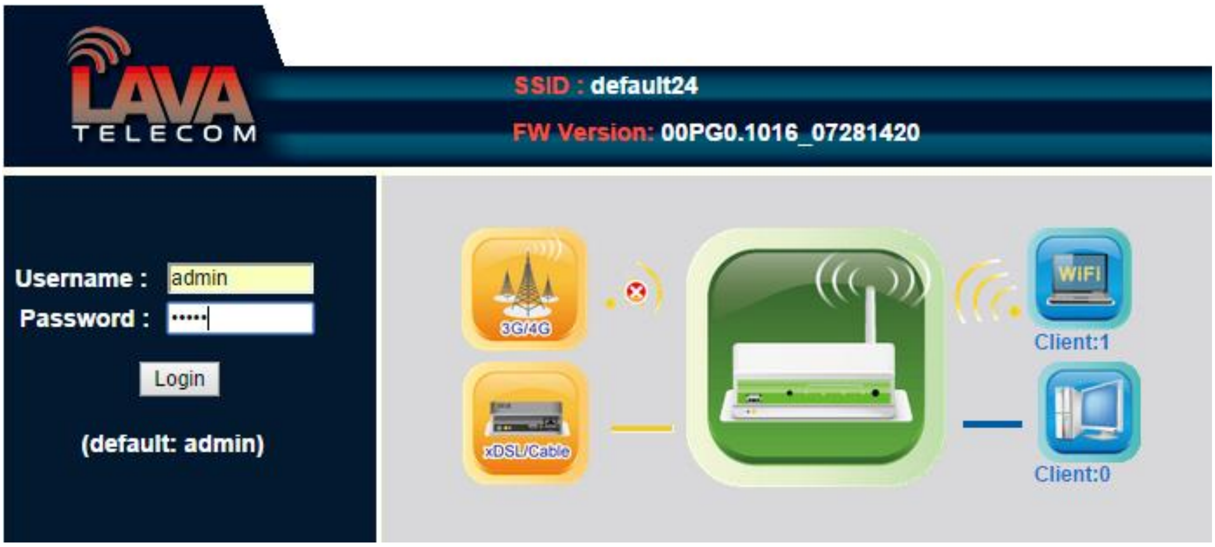
//192.168.1.1/

192.168.1.1

//192.168.1.1/ - Google Search

For quick acce

Use “admin”/”admin” in both username and password fields



SSID : default24

FW Version: 00PG0.1016_07281420

Username : admin

Password : •••••

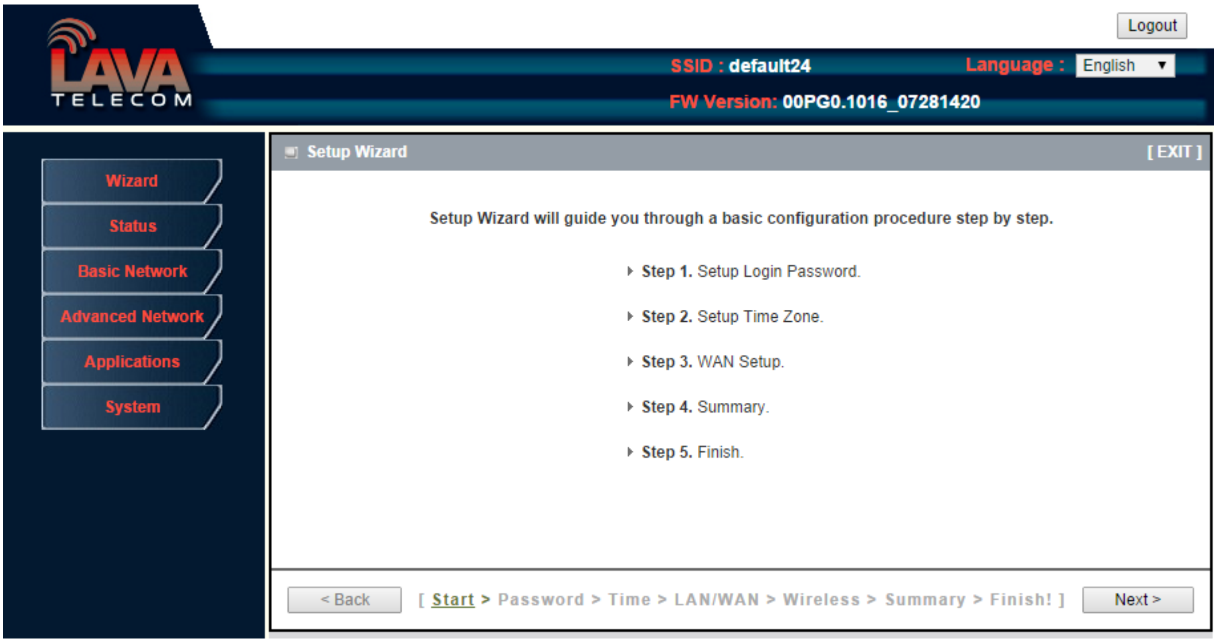
Login

(default: admin)

2.1. Configuration via WEB UI (automatically)

Configuration via Wizard is the simplest way to make the basic settings.

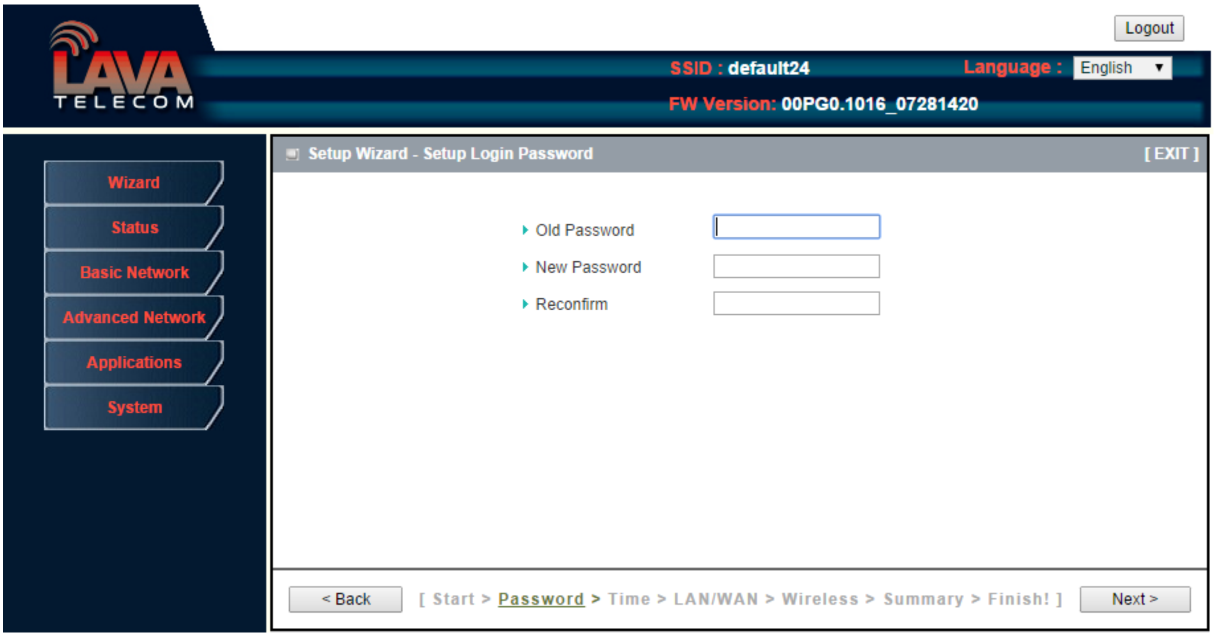
Select Wizard and press Next. Consistently fill the required fields. System will prompt you to change default password, set the time zone, configure WAN connection according to your ISP requirements, configure Wireless network.



Setup Wizard will guide you through a basic configuration procedure step by step.

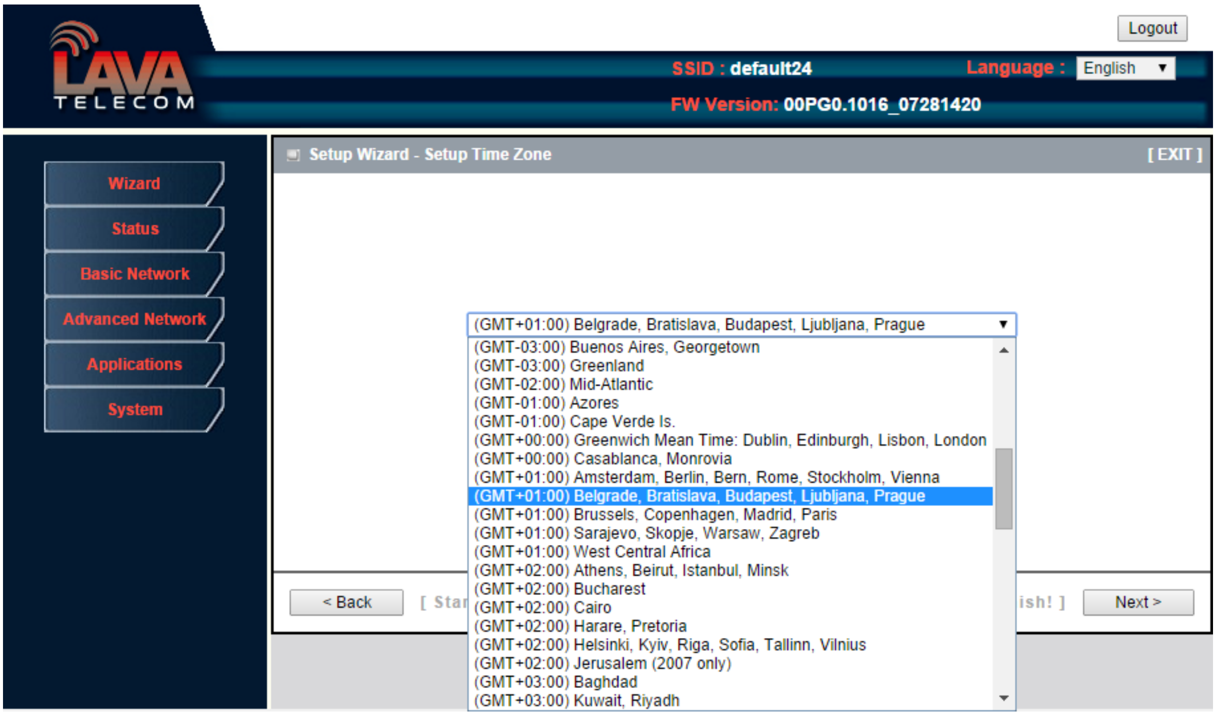
- **Step 1.** Setup Login Password.
- **Step 2.** Setup Time Zone.
- **Step 3.** WAN Setup.
- **Step 4.** Summary.
- **Step 5.** Finish.

Firstly, we kindly recommend you to change the system password after you receive this device. This password is used for web GUI login. You need to input old password first, and edit new password twice to confirm.


Logout
SSID : default24
Language : English
FW Version: 00PG0.1016_07281420
Wizard
Status
Basic Network
Advanced Network
Applications
System
Setup Wizard - Setup Login Password
[EXIT]
< Back
[Start > Password > Time > LAN/WAN > Wireless > Summary > Finish!]
Next >

- Old Password
- New Password
- Reconfirm

Select Time Zone according to your location



SSID : default24

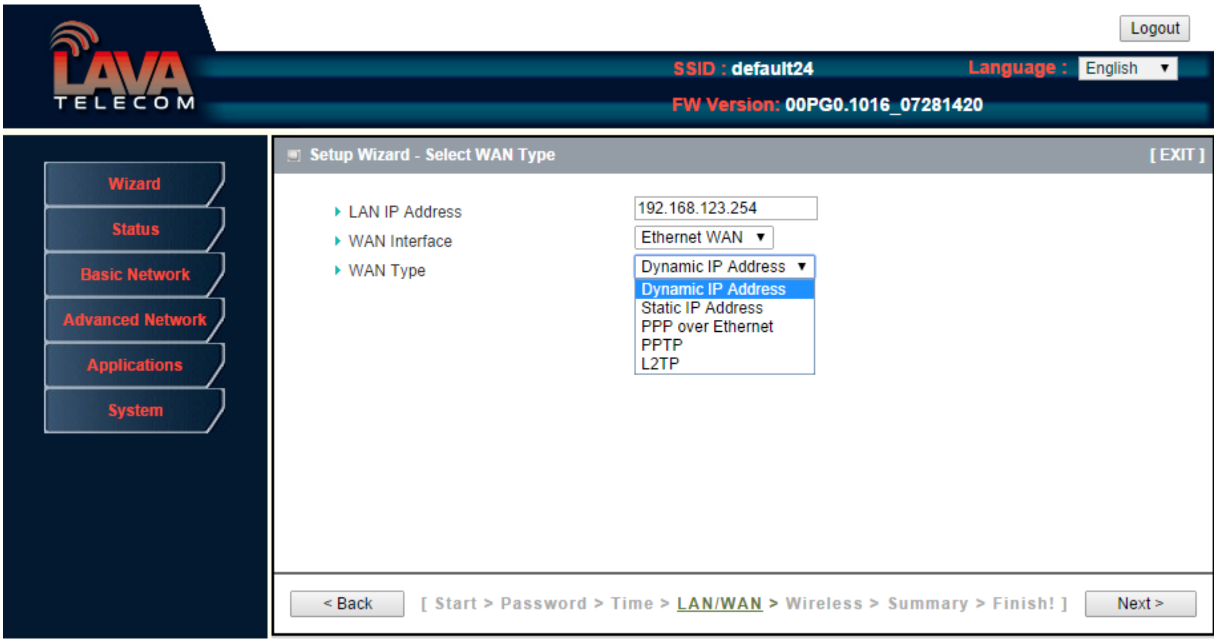
FW Version: 00PG0.1016_07281420

Setup Wizard - Setup Time Zone

(GMT+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague

(GMT-03:00) Buenos Aires, Georgetown
(GMT-03:00) Greenland
(GMT-02:00) Mid-Atlantic
(GMT-01:00) Azores
(GMT-01:00) Cape Verde Is.
(GMT+00:00) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
(GMT+00:00) Casablanca, Monrovia
(GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
(GMT+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
(GMT+01:00) Brussels, Copenhagen, Madrid, Paris
(GMT+01:00) Sarajevo, Skopje, Warsaw, Zagreb
(GMT+01:00) West Central Africa
(GMT+02:00) Athens, Beirut, Istanbul, Minsk
(GMT+02:00) Bucharest
(GMT+02:00) Cairo
(GMT+02:00) Harare, Pretoria
(GMT+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius
(GMT+02:00) Jerusalem (2007 only)
(GMT+03:00) Baghdad
(GMT+03:00) Kuwait, Riyadh

Select interface which will be used as WAN (Ethernet / Wireless) and WAN Type, provided by ISP



SSID : default24

FW Version: 00PG0.1016_07281420

Setup Wizard - Select WAN Type

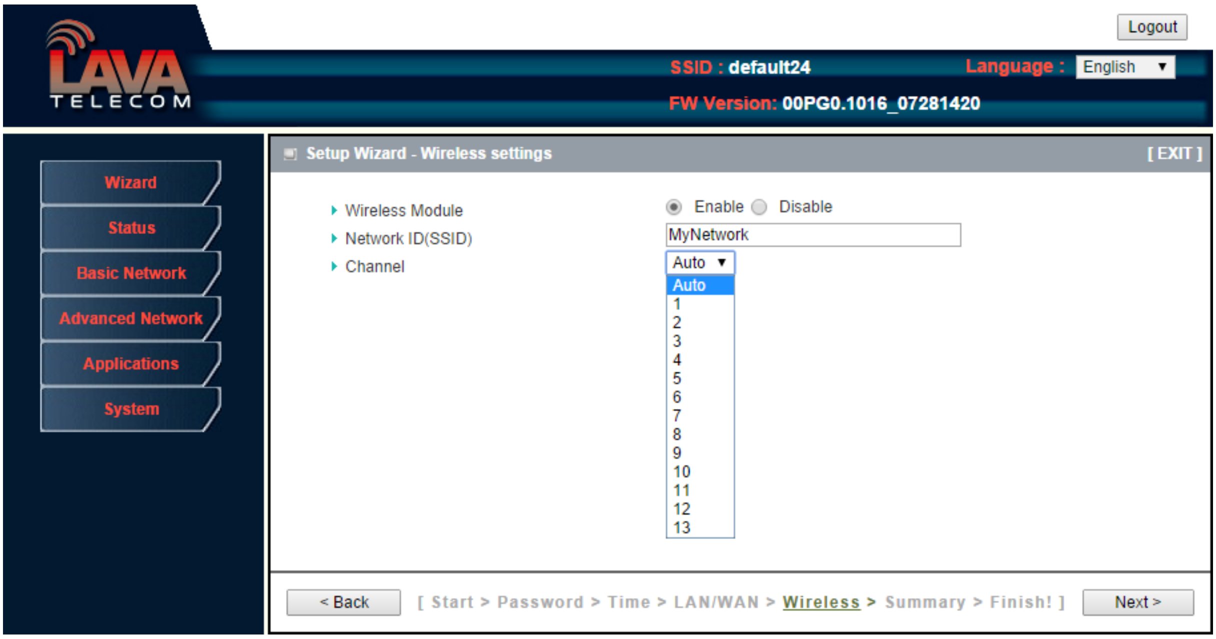
- LAN IP Address: 192.168.123.254
- WAN Interface: Ethernet WAN
- WAN Type: Dynamic IP Address

Dynamic IP Address
Static IP Address
PPP over Ethernet
PPTP
L2TP

[Start > Password > Time > LAN/WAN > Wireless > Summary > Finish!]

Host Name and ISP registered MAC Address are optional (if you don’t have such information, just press Next)

In the next page you have to choose if you need Wireless Module to be enabled or not. Select Enable, if you need Wi-Fi access, and then type your wireless network name (Network ID(SSID)) and Channel (you can use Auto channel selection, or set it manually according to information about adjacent wireless network.



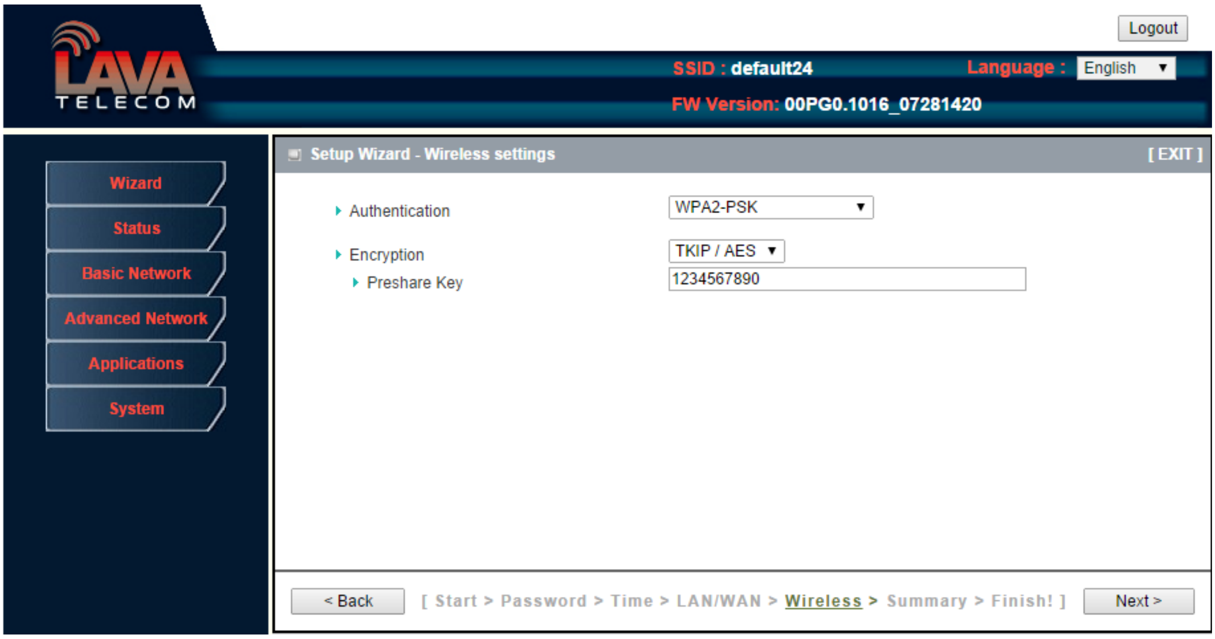
SSID : default24

FW Version: 00PG0.1016_07281420

Setup Wizard - Wireless settings

- Wireless Module: ● Enable ○ Disable
- Network ID(SSID): MyNetwork
- Channel: Auto

Select Authentication and Encryption types; enter the password which will be used for connection to your wireless network.



SSID : default24

FW Version: 00PG0.1016_07281420

Setup Wizard - Wireless settings

- Authentication: WPA2-PSK
- Encryption: TKIP / AES
  - Preshare Key: 1234567890

Press Next, and check all information. If everything is correct, press Apply Settings. Please wait a minute while system is applying the settings. Then press Finish.

2.2. Configuration via WEB UI (manually)

Manual settings allow you to do more flexible configuration of devise.

2.2.1. Status

On Status page You can see all the status of LR-25G001. Here you can find two items:

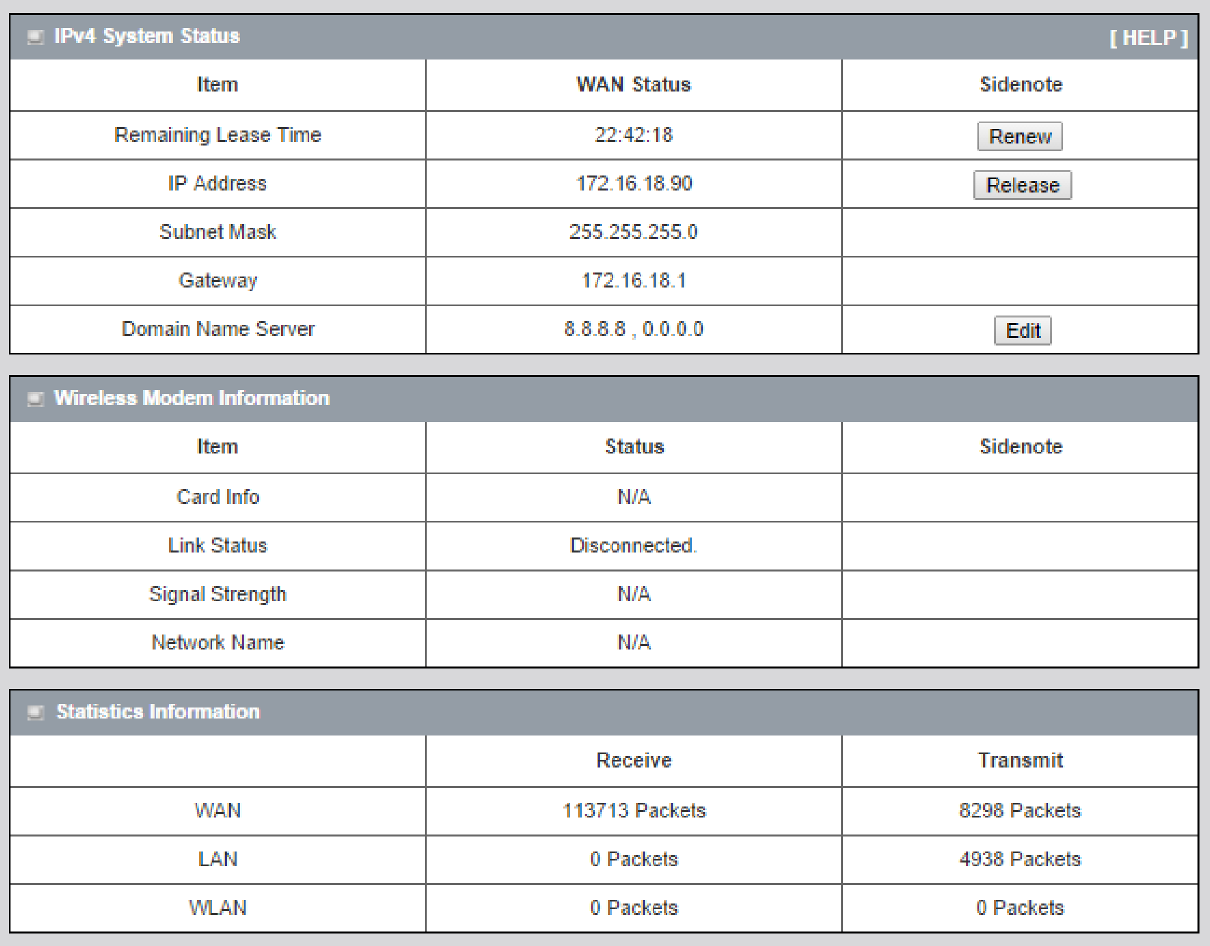
◤ System Status

IPv4 System Status: IPv4 Items will display WAN type, WAN IP address, DNS Server and Connection Scheme.

IPv6 System Status: IPv6 Items will display WAN Link-Local address, Global IPv6 address, LAN IPv6 Link-Local address and Link Status.

◤ Wireless Status

Wireless Status: Wireless Items will display Wireless Mode, SSID, Channel, Security and Wireless MAC address.



IPv4 System Status [HELP]

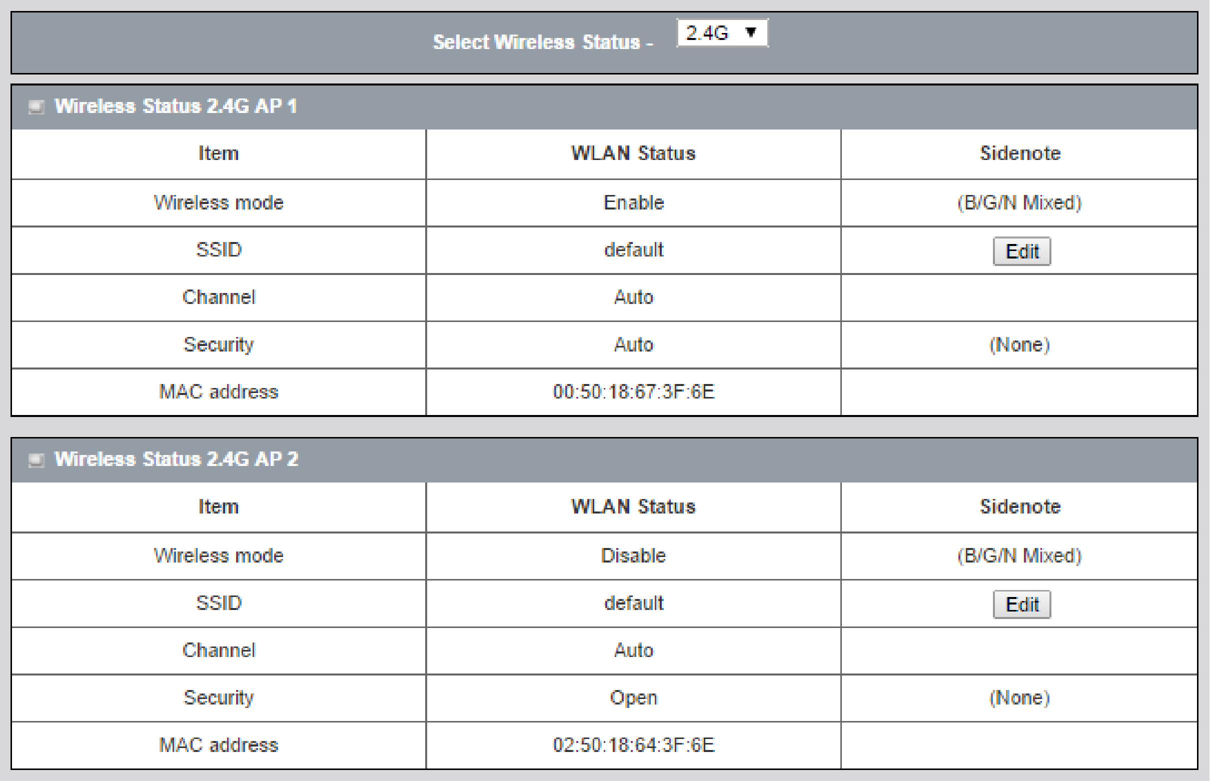
Item	WAN Status	Sidenote
Remaining Lease Time	22:42:18	Renew
IP Address	172.16.18.90	Release
Subnet Mask	255.255.255.0	
Gateway	172.16.18.1	
Domain Name Server	8.8.8.8 , 0.0.0.0	Edit

Wireless Modem Information

Item	Status	Sidenote
Card Info	N/A	
Link Status	Disconnected.	
Signal Strength	N/A	
Network Name	N/A	

Statistics Information

	Receive	Transmit
WAN	113713 Packets	8298 Packets
LAN	0 Packets	4938 Packets
WLAN	0 Packets	0 Packets



Select Wireless Status - 2.4G ▼

Wireless Status 2.4G AP 1

Item	WLAN Status	Sidenote
Wireless mode	Enable	(B/G/N Mixed)
SSID	default	Edit
Channel	Auto	
Security	Auto	(None)
MAC address	00:50:18:67:3F:6E	

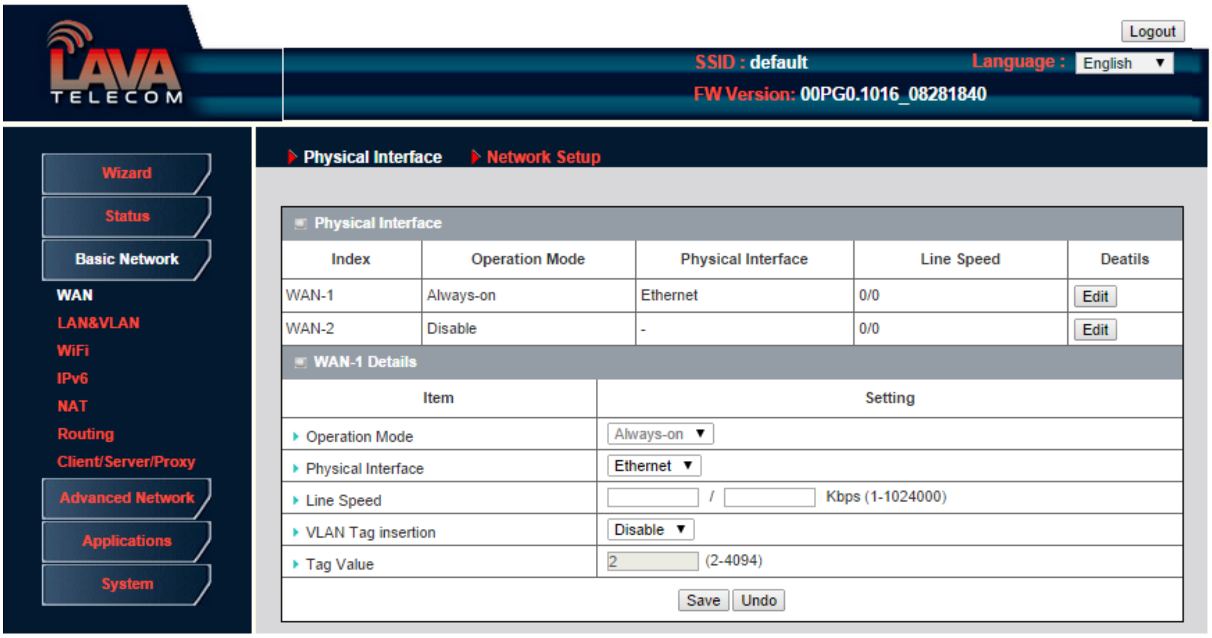
Wireless Status 2.4G AP 2

Item	WLAN Status	Sidenote
Wireless mode	Disable	(B/G/N Mixed)
SSID	default	Edit
Channel	Auto	
Security	Open	(None)
MAC address	02:50:18:64:3F:6E	

2.2.2. Basic Network

2.2.2.1. WAN – Physical Interface

Click on the “Edit” button for each WAN interface and you can get the detail physical interface settings and then configure the settings as well.



SSID : default
Language : English ▼
FW Version: 00PG0.1016_08281840

Physical Interface

Index	Operation Mode	Physical Interface	Line Speed	Deatils
WAN-1	Always-on	Ethernet	0/0	Edit
WAN-2	Disable	-	0/0	Edit

WAN-1 Details

Item	Setting
Operation Mode	Always-on ▼
Physical Interface	Ethernet ▼
Line Speed	/ Kbps (1-1024000)
VLAN Tag insertion	Disable ▼
Tag Value	2 (2-4094)

Save Undo

◤ WAN-1: The operation mode of this interface is forced to “Always-on” mode, and operates as the primary internet connection. You can click on the respective “Edit” button and configure the rest items for this interface.

◤ WAN-2: The operation mode of this interface is disabled by default, you can click on the respective “Edit” button and configure the second WAN interface to operate as “fail over” mode, so that when the WAN-1 connection broken, the device will try to failover the internet connection to WAN-2.

◤ Physical Interface: Select the WAN interface from the available list. For this device, there are “Ethernet” and “3G/4G” items. If you would like the RJ45 WAN port to operate as the primary internet connection, Please choose “Ethernet”; Otherwise, choose “3G/4G” for configuring the embedded 3G/4G modem as primary WAN connection.

◤ Line Speed (Kbps): You can specify the downstream / upstream speed for the corresponding WAN connection. Such information will be referred in QoS and load balance function to manage the traffic load for each WAN connection.

◤ VLAN Tag Insertion, Tag Value: If your ISP required a VLAN tag been inserted into the WAN packets, you can enable this setting, and enter the specified tag value.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

2.2.2.2. WAN – Network Setup

For each WAN interfaces, you can configure it one by one to get proper internet connection setup. It includes the Wireless WAN - the remote wireless ISP such as 3G (WCDMA, HSxPA, HSPA+, CDMA2000, EV-DO, TD-SCDMA), and the Ethernet WAN - the DSL ISP such as Dynamic IP, Static IP, PPPoE, PPTP and L2TP

Wireless WAN -3G/4G

Click on the “**Edit**” button for the 3G/4G WAN interface and you can get the detail WAN settings and then configure the settings as well.

◤ **WAN Type**: Choose “3G” from the drop list

◤ **Dial-up Profile**: Choose “Auto-Detection” or “Manual”. If you select “Auto-Detection”, then system will check the information automatically. If you select “Manual”, then you have to specify more ISP-related settings, such as Country, Service Provider, and APN, to get the 3G/4G service. The “Auto-Detection” option is suggested.

◤ **PIN Code**: Enter the PIN Code for your SIM card(Optional)

◤ **Dialed Number**: Enter the dialed number that is provided by your ISP.

◤ **Account, Password**: Enter the account / Password that is provided by your ISP(Optional).

◤ **Authentication**: Choose “auto”, “PAP”, or “CHAP” according your ISP’s authentication approach.

◤ **Primary / Secondary DNS**: Enter the Domain Name Server settings (Optional)

◤ **Connection Control**: Select your connection control scheme from the drop list; “auto-reconnect (always-on)” option is recommended.

◤ **Allowed Connection Time**: You can select “Always” or “By Schedule” for connection method. If you choose “By Schedule” rule, you have to add a new schedule for this connection.

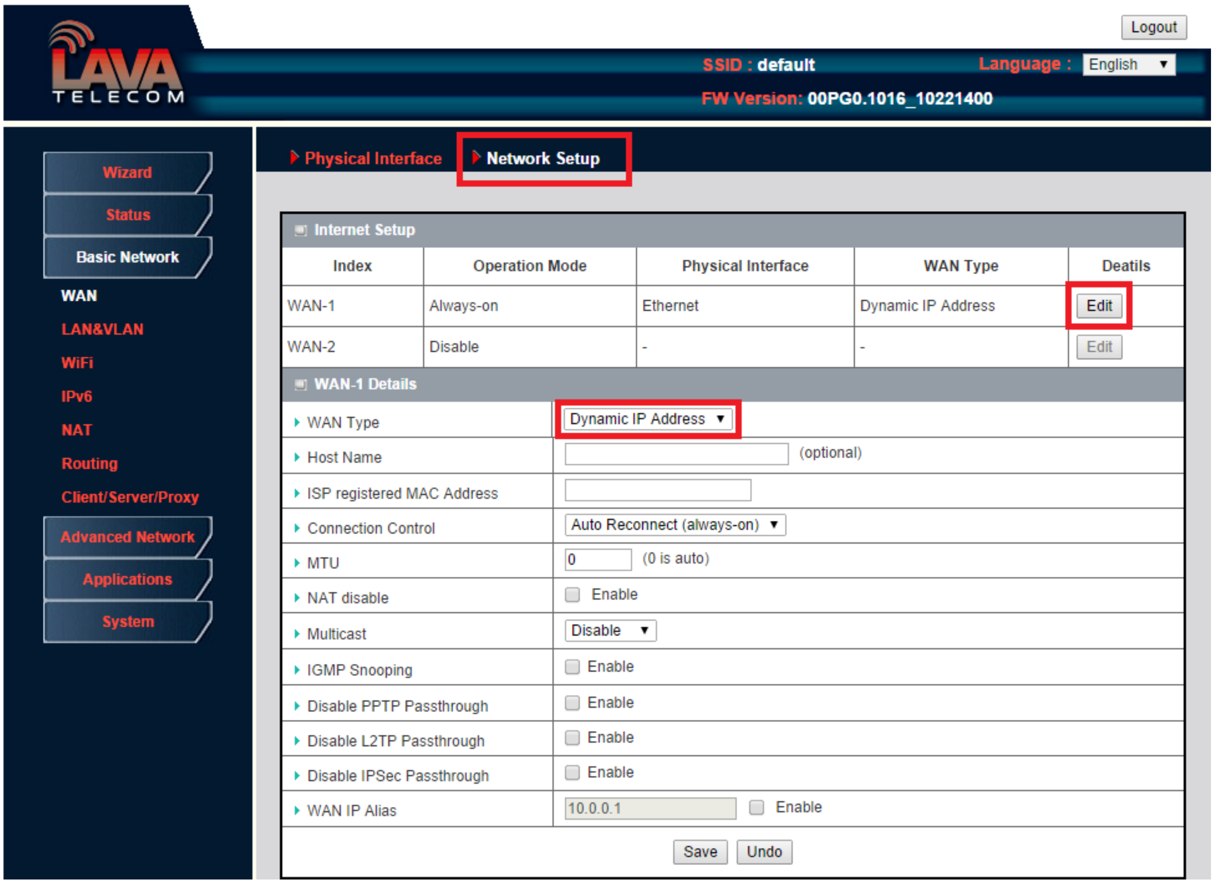
- **MTU**: Most ISP offers MTU value to users. The default value is o (auto).
- **Keep Alive**: You can do preferred settings by using this feature to prevent the built-in 3G modem from some sort of auto-timeout and disconnects from the internet after a period of inactivity.
- **Multicast**: Enable or disable multicast traffics from the internet. You may enable as auto mode or select by IGMP v1, IGMP v2, IGMP v3.
- **IGMP Snooping**: Enable or disable IGMP snooping function. If you enable the IGMP snooping function, this device will detect all IGMP messages exchanged on the link and will maintain a table indicating for each of the interfaces, what multicast groups should be forwarded. This simple solution easily prevents multicast flooding on an Ethernet link.
- **Disable PPTP / L2TP / IPSec Passthrough**: By default, the device allows the PPTP / L2TP / IPSec VPN traffic that initiated from local VPN client to pass through to Internet. If you want to disable such function, just change the setting to disable it.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

Ethernet WAN

Click on the “Edit” button for the Ethernet WAN interface and you can get the detail WAN settings and then configure the settings as well.

Dynamic IP Address



SSID : default   Language : English

FW Version: 00PG0.1016_10221400

Internet Setup

Index	Operation Mode	Physical Interface	WAN Type	Deatils
WAN-1	Always-on	Ethernet	Dynamic IP Address	Edit
WAN-2	Disable	-	-	Edit

WAN-1 Details

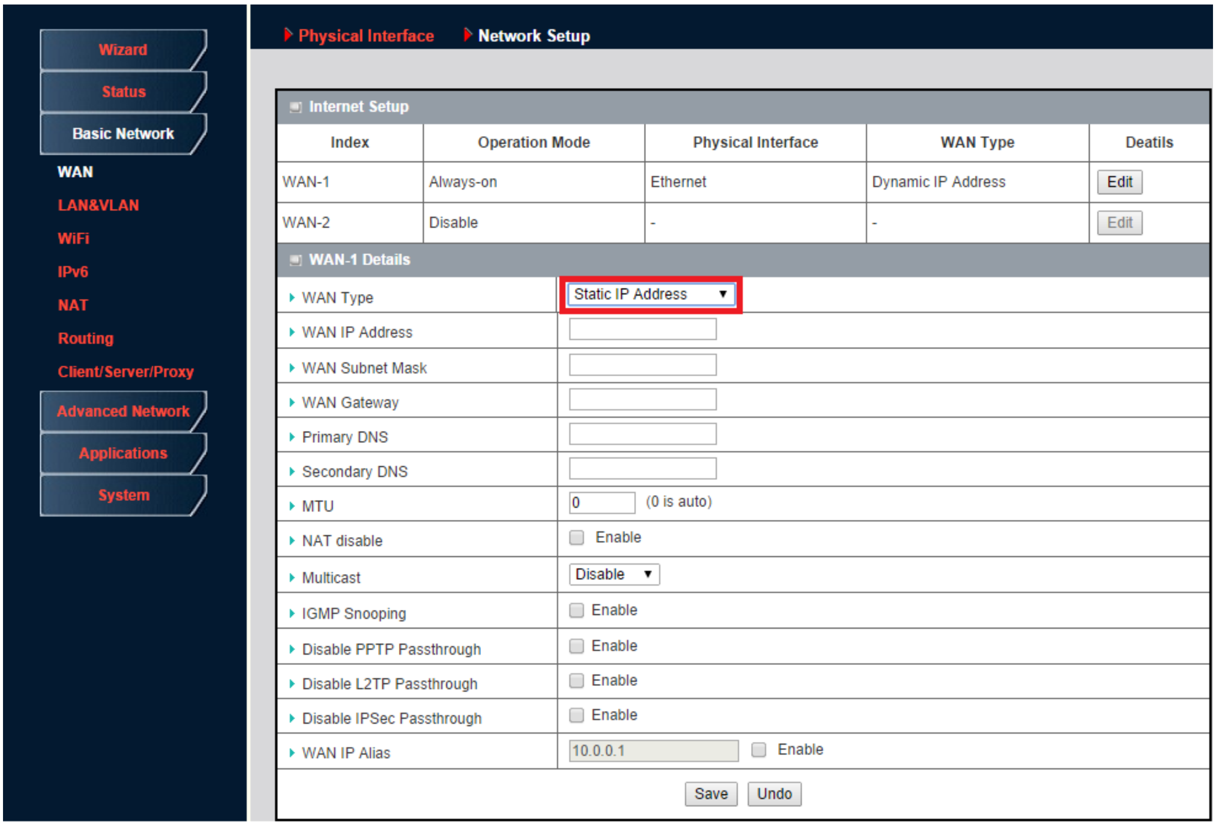
WAN Type	Dynamic IP Address
Host Name	(optional)
ISP registered MAC Address	
Connection Control	Auto Reconnect (always-on)
MTU	0 (0 is auto)
NAT disable	□ Enable
Multicast	Disable
IGMP Snooping	□ Enable
Disable PPTP Passthrough	□ Enable
Disable L2TP Passthrough	□ Enable
Disable IPSec Passthrough	□ Enable
WAN IP Alias	10.0.0.1 □ Enable

- **WAN Type**: choose “Dynamic IP Address” from the drop list
- **Host Name**: Optional, required by some ISPs, for example, @Home.
- **ISP registered MAC Address**: Enter the WAN MAC address of this device. (Optional)
- **MTU**: Most ISP offers MTU value to users. The default value is o (auto)
- **NAT disable**: If you enable this option, it will act with a non-NAT function.
- **Multicast**: Enable or disable multicast traffics from the internet. You may enable as auto mode or select by IGMP v1, IGMP v2, IGMP v3.
- **IGMP Snooping**: Enable or disable IGMP snooping function. If you enable the IGMP snooping function, this device will detect all IGMP messages exchanged on the link and will maintain a table indicating for each of the interfaces, what multicast groups should be forwarded. This simple solution easily prevents multicast flooding on an Ethernet link.
- **Disable PPTP / L2TP / IPSec Passthrough**: By default, the device allows the PPTP / L2TP / IPSec VPN traffic that initiated from local VPN client to pass through to Internet. If you want to disable such function, just change the setting to disable it.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

Static IP Address

Select this option to give your static IP information. You will need to enter in the IP address, subnet mask, and gateway address, provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which is four IP octets separated by a dot (x.x.x.x). The Router will not accept the IP address if it is not in this format.



Internet Setup

Index	Operation Mode	Physical Interface	WAN Type	Deatils
WAN-1	Always-on	Ethernet	Dynamic IP Address	Edit
WAN-2	Disable	-	-	Edit

WAN-1 Details

WAN Type	Static IP Address ▾
WAN IP Address	
WAN Subnet Mask	
WAN Gateway	
Primary DNS	
Secondary DNS	
MTU	0 (0 is auto)
NAT disable	□ Enable
Multicast	Disable ▾
IGMP Snooping	□ Enable
Disable PPTP Passthrough	□ Enable
Disable L2TP Passthrough	□ Enable
Disable IPSec Passthrough	□ Enable
WAN IP Alias	10.0.0.1 □ Enable

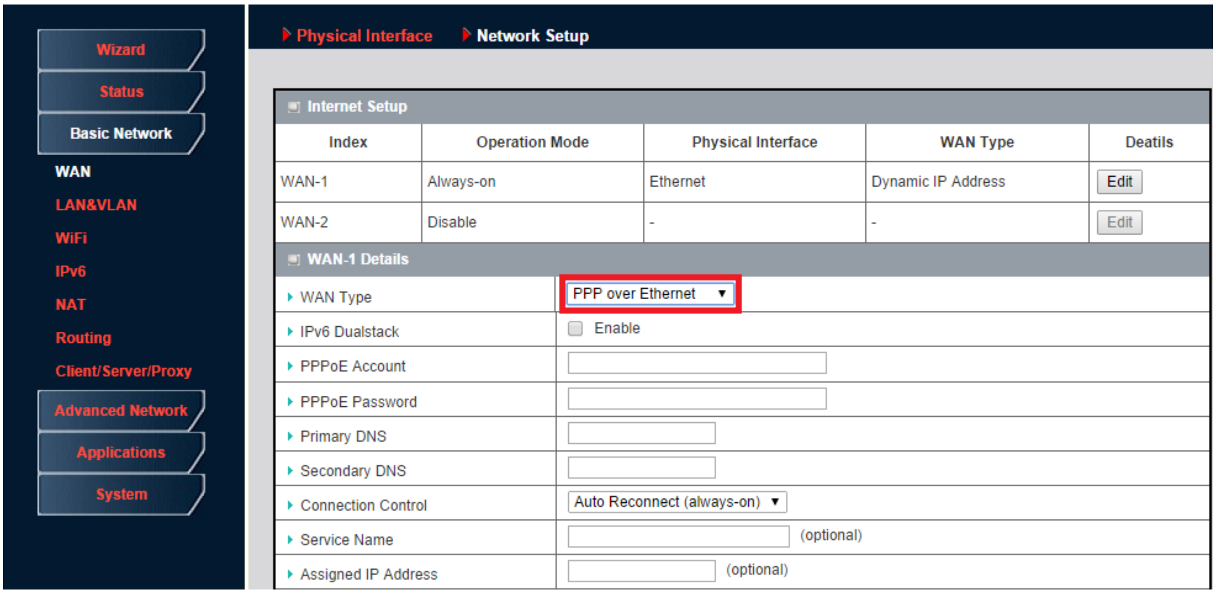
Save Undo

- **WAN Type:** Choose “Static IP Address” from the drop list
- **WAN IP address/ Subnet Mask/ Gateway: Enter the IP address, subnet mask, and gateway address, provided to you by your ISP.**
- **Primary DNS/ Secondary DNS**: input the Primary/Secondary DNS if necessary.
- **MTU**: Most ISP offers MTU value to users. The default value is o (auto)
- **NAT disable**: If you enable this option, it will act with a non-NAT function.
- **Multicast**: Enable or disable multicast traffics from the internet. You may enable as auto mode or select by IGMP v1, IGMP v2, IGMP v3.
- **IGMP Snooping**: Enable or disable IGMP snooping function. If you enable the IGMP snooping function, this device will detect all IGMP messages exchanged on the link and will maintain a table indicating for each of the interfaces, what multicast groups should be forwarded. This simple solution easily prevents multicast flooding on an Ethernet link.
- **Disable PPTP / L2TP / IPSec Passthrough**: By default, the device allows the PPTP / L2TP / IPSec VPN traffic that initiated from local VPN client to pass through to Internet. If you want to disable such function, just change the setting to disable it.
- **WAN IP alias**: The device supports 2 WAN IP address, one is for primary connection that provides users/devices in the LAN to access Internet; the other is a virtual connection that let remote user to manage this device.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

PPP over Ethernet

Select this option if your ISP requires you to use a PPPoE connection. This option is typically used for DSL services.

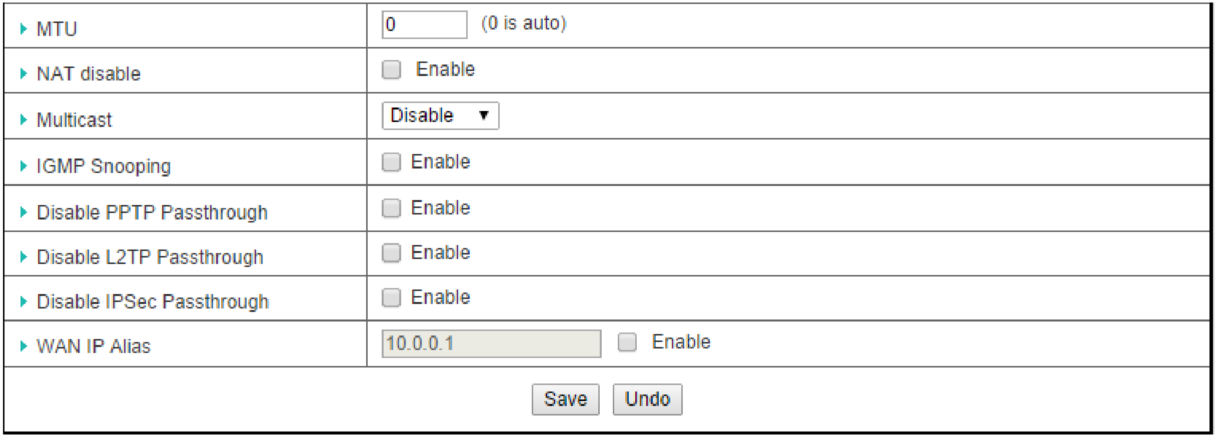


Internet Setup

Index	Operation Mode	Physical Interface	WAN Type	Deatils
WAN-1	Always-on	Ethernet	Dynamic IP Address	Edit
WAN-2	Disable	-	-	Edit

WAN-1 Details

WAN Type	PPP over Ethernet ▼
IPv6 Dualstack	□ Enable
PPPoE Account	
PPPoE Password	
Primary DNS	
Secondary DNS	
Connection Control	Auto Reconnect (always-on) ▼
Service Name	(optional)
Assigned IP Address	(optional)



MTU	0 (0 is auto)
NAT disable	□ Enable
Multicast	Disable ▾
IGMP Snooping	□ Enable
Disable PPTP Passthrough	□ Enable
Disable L2TP Passthrough	□ Enable
Disable IPSec Passthrough	□ Enable
WAN IP Alias	10.0.0.1 □ Enable

◤ **WAN Type**: Choose "PPP Over Ethernet" from the drop list

◤ **IPv6 Dualstack**: You can enable / disable the function of IPv4/IPv6 dual stack.

◤ **PPPoE Account and Password**: The account and password your ISP assigned to you. For security, this field appears blank. If you don't want to change the password, leave it blank.

◤ **Primary DNS / Secondary DNS: Input the Primary/Secondary DNS if necessary.**

◤ **Service Name / Assigned IP Address**: Input the Service Name and Assigned IP address if necessary.

◤ **MTU**: Most ISP offers MTU value to users. The default MTU value is 0 (auto)

◤ **NAT disable** : If you enable this option, it will act with a non-NAT function.

◤ **Multicast**: Enable or disable multicast traffics from the internet. You may enable as auto mode or select by IGMP v1, IGMP v2, IGMP v3.

◤ **IGMP Snooping**: Enable or disable IGMP snooping function. If you enable the IGMP snooping function, this device will detect all IGMP messages exchanged on the link and will maintain a table indicating for each of the interfaces, what multicast groups should be forwarded. This simple solution easily prevents multicast flooding on an Ethernet link.

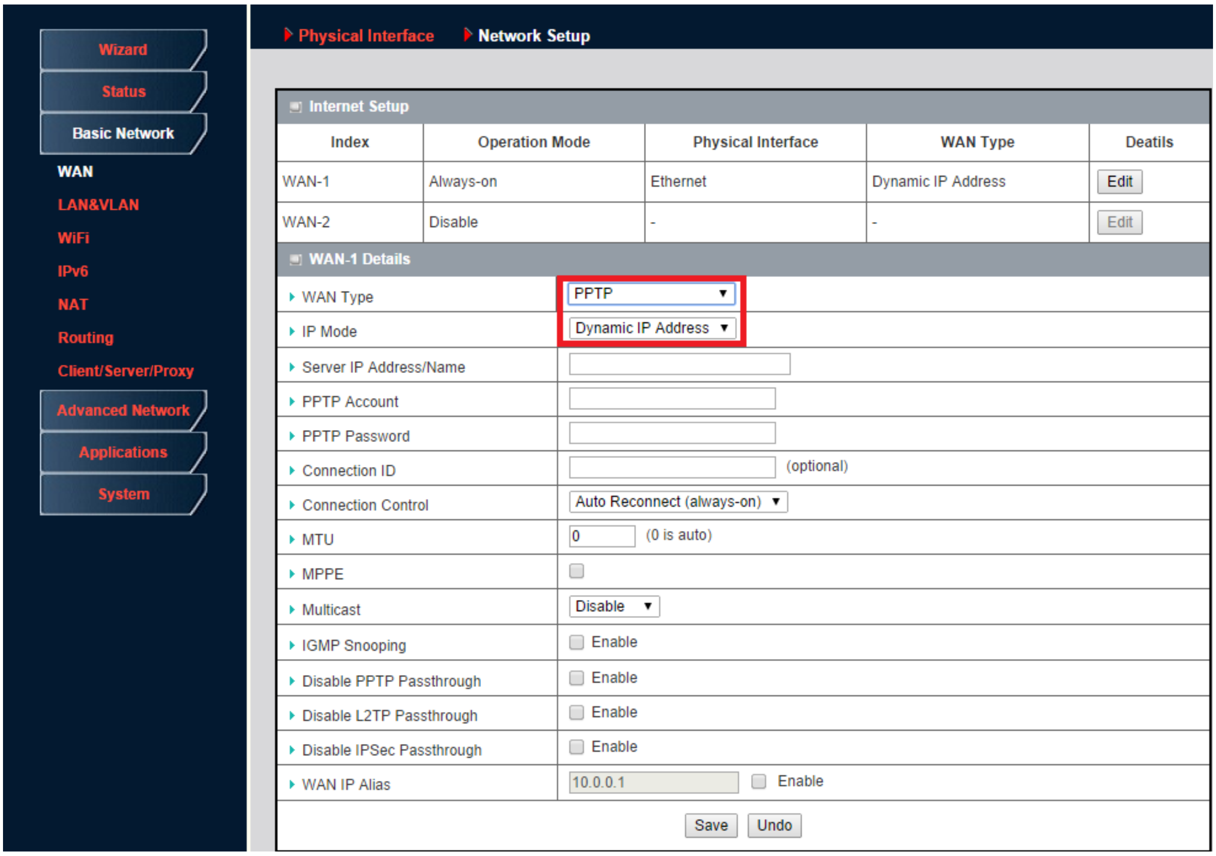
◤ **Disable PPTP / L2TP / IPSec Passthrough**: By default, the device allows the PPTP / L2TP / IPSec VPN traffic that initiated from local VPN client to pass through to Internet. If you want to disable such function, just change the setting to disable it.

◤ **WAN IP alias**: The device supports 2 WAN IP address, one is for primary connection that provides users/devices in the LAN to access Internet; the other is a virtual connection that let remote user to manage this device.

Afterwards, click on "Save" to store your settings or click "Undo" to give up the changes.

PPTP

Choose PPTP (Point-to-Point Tunneling Protocol) if your ISP used a PPTP connection. Your ISP will provide you with a username and password. This option is typically used for DSL services.



Internet Setup

Index	Operation Mode	Physical Interface	WAN Type	Deatils
WAN-1	Always-on	Ethernet	Dynamic IP Address	Edit
WAN-2	Disable	-	-	Edit

WAN-1 Details

WAN Type	PPTP
IP Mode	Dynamic IP Address
Server IP Address/Name	
PPTP Account	
PPTP Password	
Connection ID	(optional)
Connection Control	Auto Reconnect (always-on)
MTU	0 (0 is auto)
MPPE	□
Multicast	Disable
IGMP Snooping	□ Enable
Disable PPTP Passthrough	□ Enable
Disable L2TP Passthrough	□ Enable
Disable IPSec Passthrough	□ Enable
WAN IP Alias	10.0.0.1 □ Enable

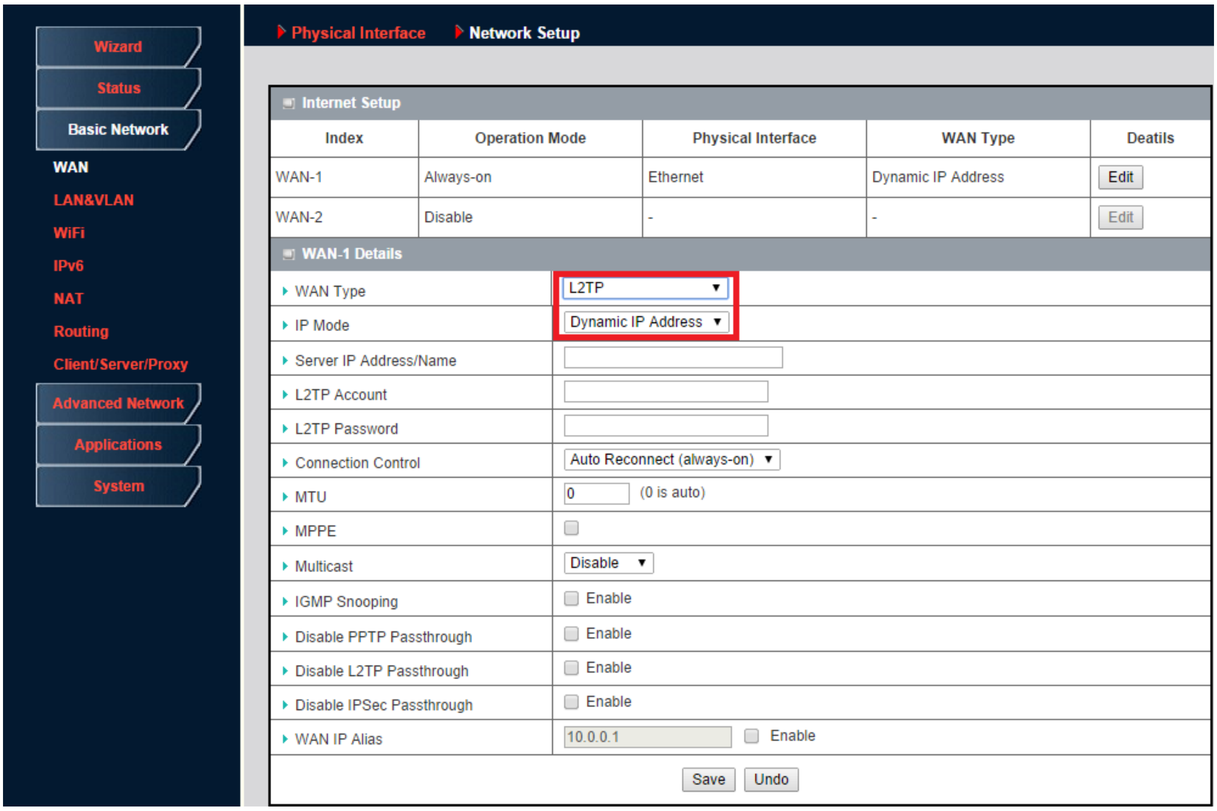
- **WAN Type**: Choose “PPTP” from the drop list
- **IP Mode**: Please check the IP mode your ISP assigned, and select “Static IP Address” or “Dynamic IP Address” accordingly. If you select “Static IP Address” option, you have to specify additional “My IP Address”, “My Subnet Mask”, and “Gateway IP” settings provided by your ISP.
- **Server IP Address / Name**: The IP address of the PPTP server and designated Gateway provided by your ISP.
- **PPTP Account and Password**: The account and password your ISP assigned to you. For security, this field appears blank. If you don't want to change the password, leave it blank**.**
- **Connection ID**: Optional, input the connection ID if your ISP requires it.
- **MTU** : Most ISP offers MTU value to users. The default MTU value is 0 (auto)
- **MPPE (Microsoft Point-to-Point Encryption)**: Enable or disable this function.
- **Multicast**: Enable or disable multicast traffics from the internet. You may enable as auto mode or select by IGMP v1, IGMP v2, IGMP v3.
- **IGMP Snooping**: Enable or disable IGMP snooping function. If you enable the IGMP snooping function, this device will detect all IGMP messages exchanged on the link and will maintain a table indicating for each of the interfaces, what multicast groups should be forwarded. This simple solution easily prevents multicast flooding on an Ethernet link.
- **Disable PPTP / L2TP / IPSec Passthrough**: By default, the device allows the PPTP / L2TP / IPSec VPN traffic that initiated from local VPN client to pass through to Internet. If you want to disable such function, just change the setting to disable it.

- **WAN IP alias**: The device supports 2 WAN IP address, one is for primary connection that provides users/devices in the LAN to access Internet; the other is a virtual connection that let remote user to manage this device.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

L2TP

Choose L2TP (Layer 2 Tunneling Protocol) if your ISP used a L2TP connection. Your ISP will provide you with a username and password. This option is typically used for DSL services.



Internet Setup

Index	Operation Mode	Physical Interface	WAN Type	Deatils
WAN-1	Always-on	Ethernet	Dynamic IP Address	Edit
WAN-2	Disable	-	-	Edit

WAN-1 Details

WAN Type	L2TP
IP Mode	Dynamic IP Address
Server IP Address/Name	
L2TP Account	
L2TP Password	
Connection Control	Auto Reconnect (always-on)
MTU	0 (0 is auto)
MPPE	□
Multicast	Disable
IGMP Snooping	□ Enable
Disable PPTP Passthrough	□ Enable
Disable L2TP Passthrough	□ Enable
Disable IPSec Passthrough	□ Enable
WAN IP Alias	10.0.0.1 □ Enable

Save Undo

- **WAN Type**: Choose “L2TP” from the drop list
- **IP Mode**: Please check the IP mode your ISP assigned, and select “Static IP Address” or “Dynamic IP Address” accordingly. If you select “Static IP Address” option, you have to specify additional “IP Address”, “Subnet Mask”, and “WAN Gateway IP” settings provided by your ISP.
- **Server IP Address / Name**: The IP address of the PPTP server and designated Gateway provided by your ISP.
- **L2TP Account and Password**: The account and password your ISP assigned to you. For security, this field appears blank. If you don't want to change the password, leave it blank.
- **MTU** : Most ISP offers MTU value to users. The default MTU value is 0 (auto)
- **MPPE (Microsoft Point-to-Point Encryption)**: Enable or disable this function.
- **Multicast**: Enable or disable multicast traffics from the internet. You may enable as auto mode or select by IGMP v1, IGMP v2, IGMP v3.
- **IGMP Snooping**: Enable or disable IGMP snooping function. If you enable the IGMP snooping

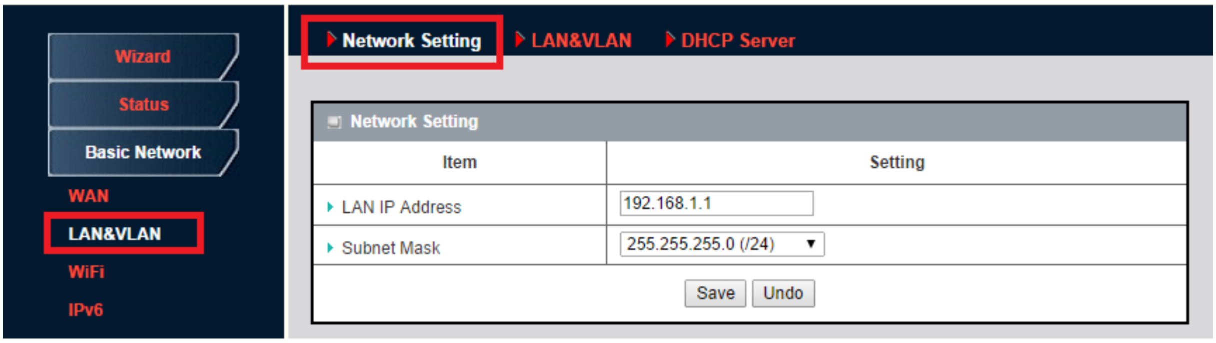
function, this device will detect all IGMP messages exchanged on the link and will maintain a table indicating for each of the interfaces, what multicast groups should be forwarded. This simple solution easily prevents multicast flooding on an Ethernet link.

◤ **Disable PPTP / L2TP / IPSec Passthrough**: By default, the device allows the PPTP / L2TP / IPSec VPN traffic that initiated from local VPN client to pass through to Internet. If you want to disable such function, just change the setting to disable it.

◤ **WAN IP alias**: The device supports 2 WAN IP address, one is for primary connection that provides users/devices in the LAN to access Internet; the other is a virtual connection that let remote user to manage this device.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

2.2.2.3. LAN & VLAN - Network Setting



Network Setting

Item	Setting
LAN IP Address	192.168.1.1
Subnet Mask	255.255.255.0 (/24)

Please follow the following instructions to do IPv4 Network Setup.

◤ **LAN IP Address**: The local IP address of this device. The computer on your network must use the LAN IP address of this device as their Default Gateway. You can change it if necessary.

◤ **Subnet Mask**: Input your Subnet mask. (All devices in the network must have the same subnet mask.) The default subnet mask is 255.255.255.0

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

2.2.2.4. LAN & VLAN

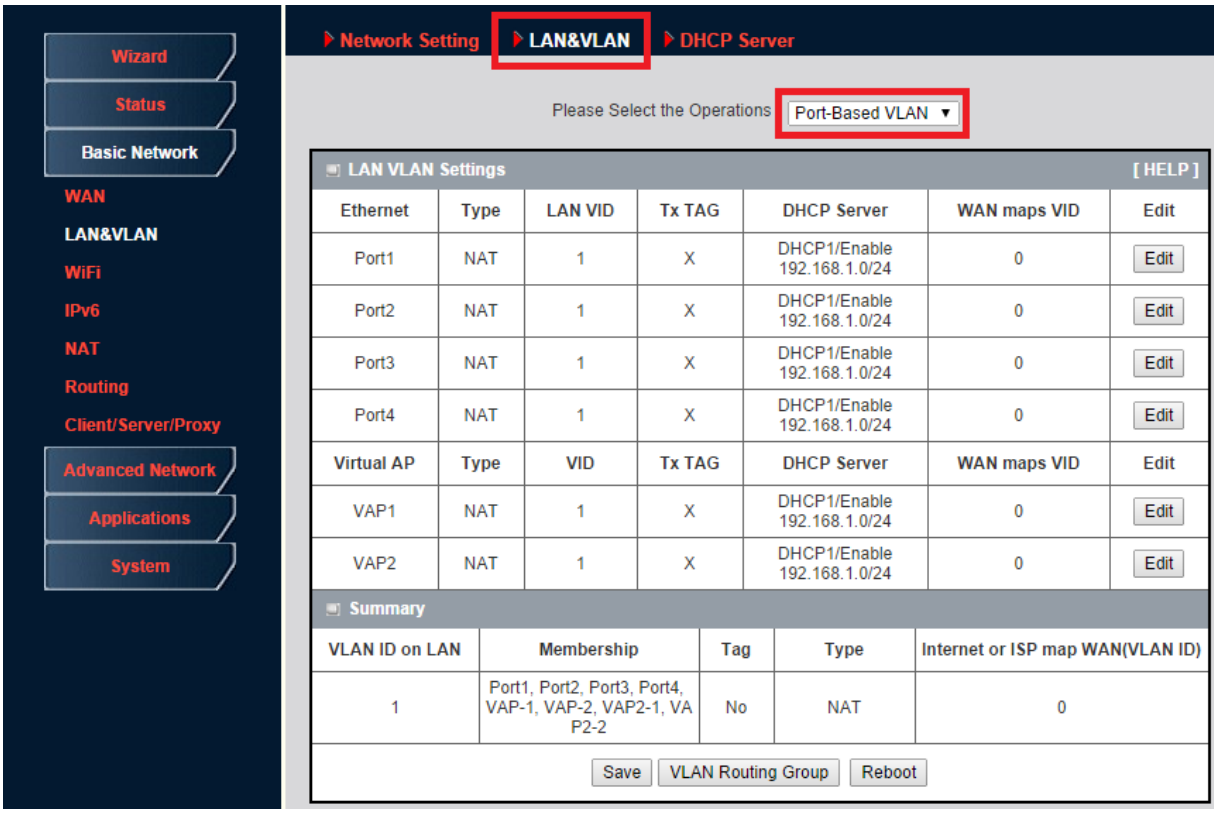
This section provides a brief description of VLANs and explains how to create, and modify virtual LANs which are more commonly known as VLANs. A VLAN is a group of ports that form a logical network under a certain switch or router device. The ports of a VLAN form an independent traffic domain in which the traffic generated by the nodes remains within the VLAN.

The VLAN function allows you to divide local network into different “virtual LANs”. In some cases, ISP may need router to support “VLAN tag” for certain kinds of services (e.g. IPTV) to work properly.

This Device supports port-based VLAN and tag-based VLAN. You can select either one operation mode and then configure according to your network configuration.

Port-Based VLAN

A port-based VLAN is a group of ports on a Ethernet switch or router that form a logical Ethernet segment. There are four LAN ports and up to eight virtual APs in this device, so you can have various VLAN configurations to organization the available LAN ports and virtual APs if required.



Please Select the Operations: Port-Based VLAN

LAN VLAN Settings [HELP]

Ethernet	Type	LAN VID	Tx TAG	DHCP Server	WAN maps VID	Edit
Port1	NAT	1	X	DHCP1/Enable 192.168.1.0/24	0	Edit
Port2	NAT	1	X	DHCP1/Enable 192.168.1.0/24	0	Edit
Port3	NAT	1	X	DHCP1/Enable 192.168.1.0/24	0	Edit
Port4	NAT	1	X	DHCP1/Enable 192.168.1.0/24	0	Edit
Virtual AP	**Type**	**VID**	**Tx TAG**	**DHCP Server**	**WAN maps VID**	**Edit**
VAP1	NAT	1	X	DHCP1/Enable 192.168.1.0/24	0	Edit
VAP2	NAT	1	X	DHCP1/Enable 192.168.1.0/24	0	Edit

Summary

VLAN ID on LAN	Membership	Tag	Type	Internet or ISP map WAN(VLAN ID)
1	Port1, Port2, Port3, Port4, VAP-1, VAP-2, VAP2-1, VAP2-2	No	NAT	0

Save | VLAN Routing Group | Reboot

By default, all the 4 LAN ports and 8 virtual APs belong to one VLAN, and this VLAN is a NAT type network, all the local device IP addresses are allocated by DHCP server 1. If you want to divide them into different VLANs, click on the "Edit" button related to each port.

- **Type**: Select "NAT" or "Bridge" to identify if the packets are directly bridged to the WAN port or processed by NAT mechanism.
- **LAN VID**: Specify a VLAN identifier for this port. The ports with the same VID are in the same VLAN.
- **Tx TAG**: If ISP requests a "VLAN Tag" with your outgoing data, please check the checkbox of "Tx TAG".
- **DHCP Server**: Specify a DHCP server for the configuring VLAN. This device provides up to 4 DHCP servers to serve the DHCP requests from different VLANs.
- **WAN Maps VID**: The VLAN Tag ID that come from the ISP service. For NAT type VLAN, no WAN VLAN tag is allowed, and the value is forced to "0"; For Bridge type VLAN, You have to specify the VLAN Tag value that is provided by your ISP.

Afterwards, click on "Save" to store your settings or click "Undo" to give up the changes.

Tag-Based VLAN

The second type of VLAN is the tag-based VLAN. VLAN membership in a tagged VLAN is determined by information within the frames that are received on a port. This differs from a port-based VLAN, where the port VIDs assigned to the ports determine VLAN membership

When the device receives a frame with a VLAN tag, referred to as a tagged frame, the device forwards the frame only to those ports that share the same VID.

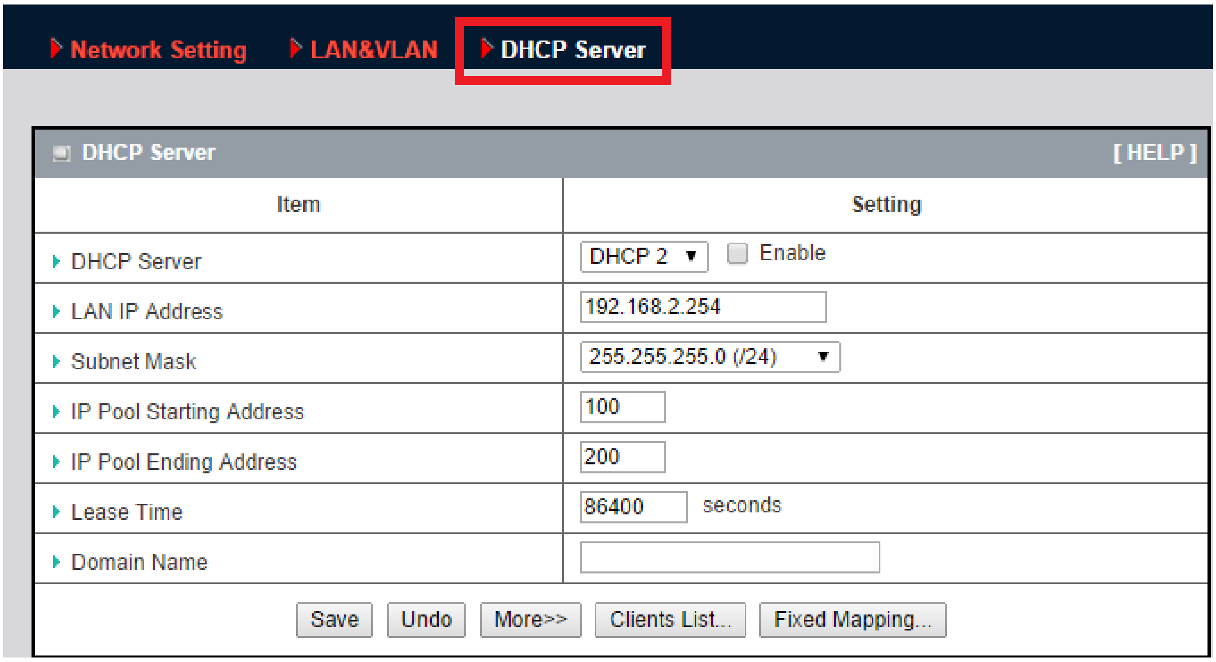
By default, all the 4 LAN ports and 8 virtual APs belong to one VLAN, and this VLAN ID is forced to “1”. It is a special tag based VLAN for device to operated, there is no tag required for this default VLAN ID.

If you want to configure your own tag-based VLANs, click on the “Edit” checkbox on a new VLAN ID row.

- **VLAN ID**: Specify a VLAN tag for this VLAN group. The ports with the same VID are in the same VLAN.
- **Internet**: Specify whether this VLAN can access Internet or not. If it is checked, all the packet will be un-tagged before it is forward to Internet, and all the packets from Internet will be tagged with the VLAN ID before it is forward to the destination belongs to this configuring VLAN group.
- **Port 1 ~ Port 4, VAP1 ~ VAP8**: Specify whether it is belong to the VLAN group or not. You just have to check the checkbox of the selected ports.
- **DHCP Server**: Specify a DHCP server for the configuring VLAN. This device provides up to 4 DHCP servers to serve the DHCP requests from different VLANs.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

2.2.2.5. DHCP Server



DHCP Server

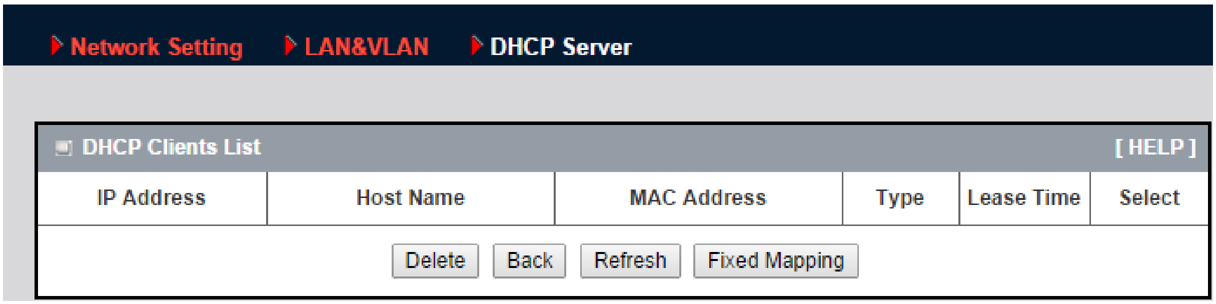
Item	Setting
DHCP Server	DHCP 2 ▼ □ Enable
LAN IP Address	192.168.2.254
Subnet Mask	255.255.255.0 (/24) ▼
IP Pool Starting Address	100
IP Pool Ending Address	200
Lease Time	86400 seconds
Domain Name	

- **DHCP Server**: Choose DHCP Server to Enable. If you enable the DHCP Server function, the following settings will be effective. This device provides up to 4 DHCP servers to serve the DHCP requests from different VLANs.
- **IP Pool Starting/Ending Address**: Whenever there is a request, the DHCP server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting / ending address of the IP address pool.
- **Lease Time**: DHCP lease time to the DHCP client.
- **Domain Name**: Optional, this information will be passed to the clients.

Press "More>>" and you can find more settings.

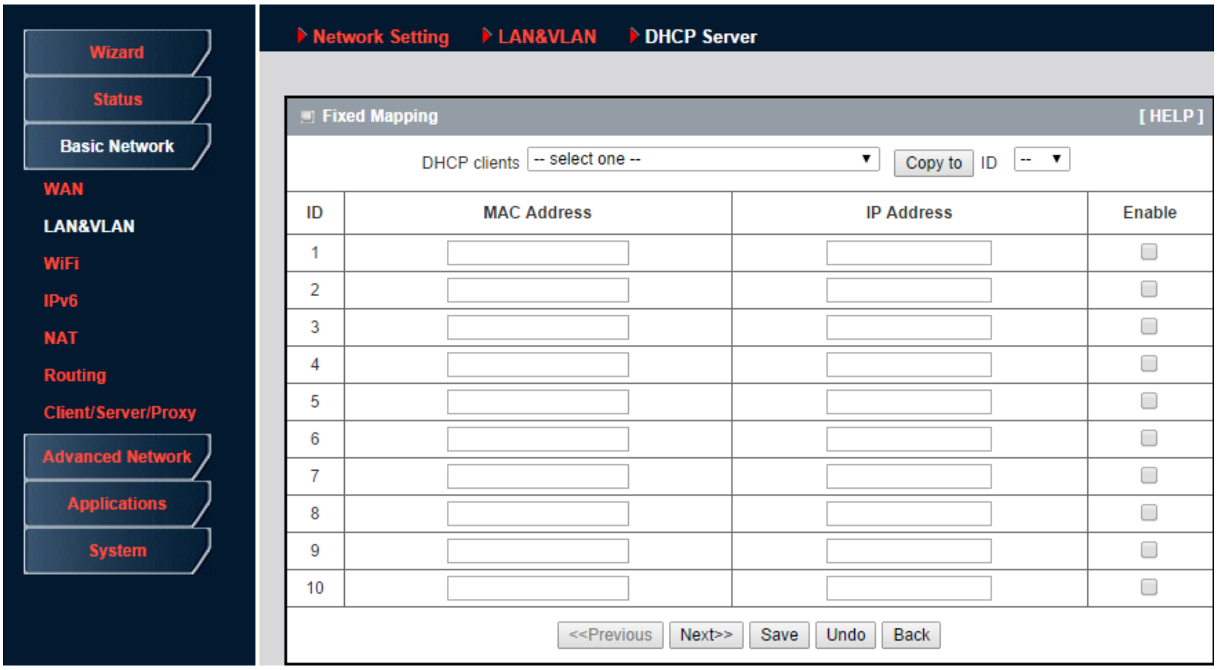
- **Primary DNS/Secondary DNS**: Optional. This feature allows you to assign a DNS Servers
- **Primary WINS/Secondary WINS**: Optional. This feature allows you to assign a WINS Servers
- **Gateway**: Optional. Gateway Address would be the IP address of an alternate Gateway. This function enables you to assign another gateway to your PC, when DHCP server offers an IP to your PC.

Press "**Clients List**" and the list of DHCP clients will be shown consequently.



IP Address	Host Name	MAC Address	Type	Lease Time	Select

Press "**Fixed Mapping**" and you can specify a certain IP address for designated local device (MAC address), so that the DHCP Server will reserve the special IP for designated devices.



DHCP clients: -- select one -- ID: --

ID	MAC Address	IP Address	Enable
1			□
2			□
3			□
4			□
5			□
6			□
7			□
8			□
9			□
10			□

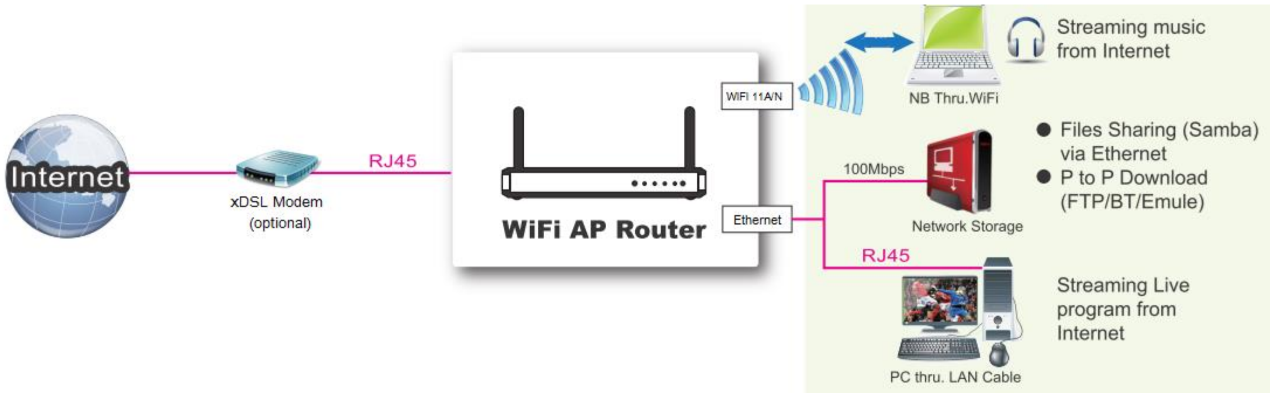
2.2.2.6. Wireless Setup

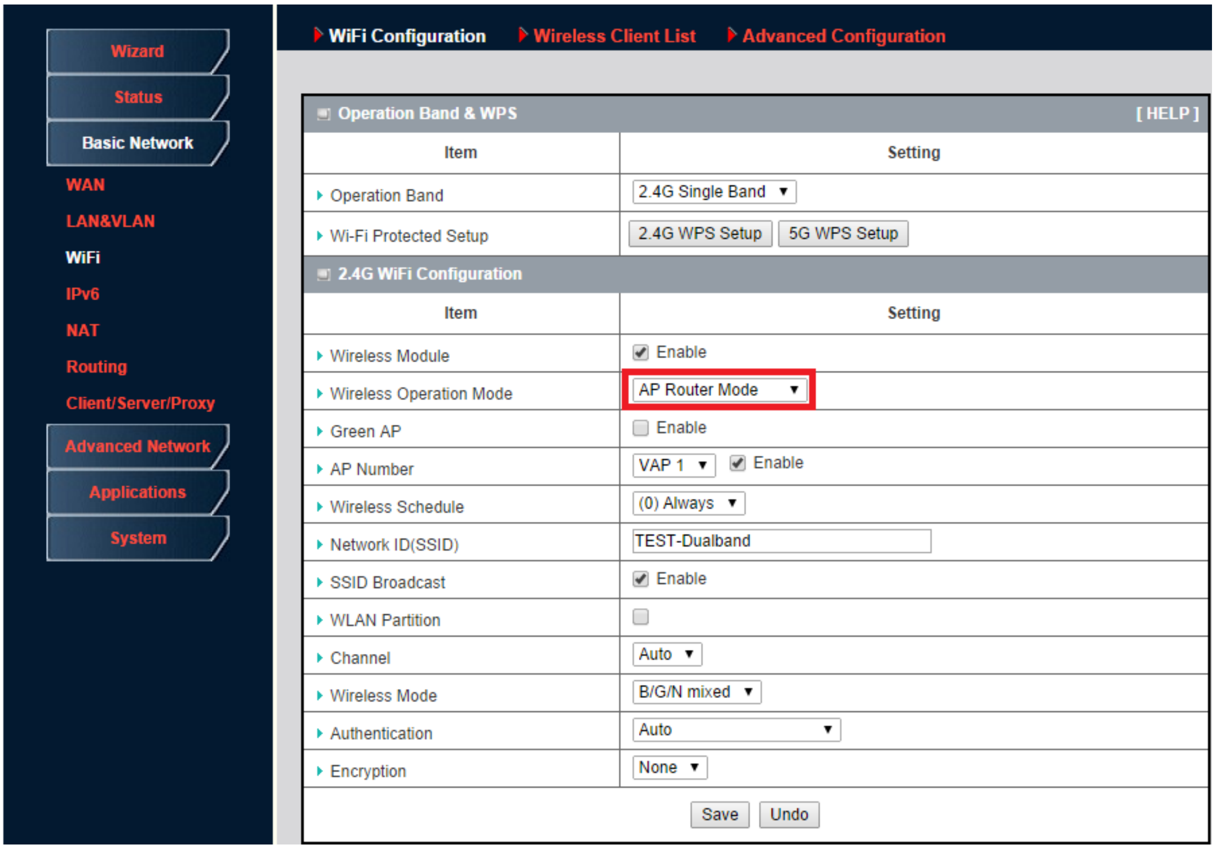
Wireless settings allow you to set the WLAN (WiFi) configuration items. When the wireless configuration is done your WiFi LAN is ready to support your local WiFi devices such as your laptop PC, wireless printer and some portable wireless devices.

There are several wireless operation modes provided by this device. They are: “AP Router Mode”, “AP Only Mode”, “WDS Hybrid Mode”, “WDS Only Mode”, and “Universal Repeater Mode”. You can choose the expected mode from the list on 2.4GHz /5GHz separately.

AP Router Mode

This mode allows you to get your wired and wireless devices connected with NAT.





Operation Band & WPS

Item	Setting
Operation Band	2.4G Single Band ▼
Wi-Fi Protected Setup	2.4G WPS Setup 5G WPS Setup

2.4G WiFi Configuration

Item	Setting
Wireless Module	☑ Enable
Wireless Operation Mode	AP Router Mode ▼
Green AP	☐ Enable
AP Number	VAP 1 ▼ ☑ Enable
Wireless Schedule	(0) Always ▼
Network ID(SSID)	TEST-Dualband
SSID Broadcast	☑ Enable
WLAN Partition	☐
Channel	Auto ▼
Wireless Mode	B/G/N mixed ▼
Authentication	Auto ▼
Encryption	None ▼

- **Wireless Module**: Enable the wireless function.
- **Wireless Operation Mode**: Choose “AP Router Mode” from the list.
- **Green AP**: Enable the Green AP function to reduce the power consumption when there is no wireless traffics.
- **AP Number**: This device supports up to 8 SSIDs for you to manage your wireless network. You can select AP1 ~ AP8 and configure each wireless network if it is required.
- **Wireless Schedule**: The wireless radio can be turn off according to the schedule rule you specified. By default, the wireless radio is always turned on when the wireless module is enabled.
- **Network ID (SSID)**: Network ID is used for identifying the Wireless LAN (WLAN). Client stations can roam freely over this device and other Access Points that have the same Network ID. (The factory default setting is “default”)
- **SSID Broadcast**: The router will broadcast beacons that have some information, including SSID so that wireless clients can know how many AP devices by scanning the network. Therefore, if this setting is configured as “Disable”, the wireless clients can not find the device from beacons.
- **WLAN Partition**: You can check the WLAN Partition function to separate the wireless clients. The wireless clients can’t communicate each other, but they can access the internet and other Ethernet LAN devices.
- **Channel**: The radio channel number. The permissible channels depend on the Regulatory Domain. The factory default setting is auto channel selection.
- **Wireless Mode**: Choose “B/G mixed”, “B only”, “G only”, “N only”, “G/N mixed” or “B/G/N mixed”. The factory default setting is “B/G/N mixed”.
- **Authentication & Encryption**: You may select one of the following authentications to secure your wireless network: Open, Shared, Auto, WPA-PSK, WPA, WPA2-PSK, WPA2, WPA-PSK/WPA2-PSK, or WPA /WPA2.

Open

Open system authentication simply consists of two communications. The first is an authentication request by the client that contains the station ID (typically the MAC address). This is followed by an authentication response from the AP/router containing a success or failure message. An example of when a failure may occur is if the client's MAC address is explicitly excluded in the AP/router configuration.

Shared

Shared key authentication relies on the fact that both stations taking part in the authentication process have the same "shared" key or passphrase. The shared key is manually set on both the client station and the AP/router. Three types of shared key authentication are available today for home or small office WLAN environments.

Auto

The AP will Select the Open or Shared by the client’s request automatically.

WPA-PSK

Select Encryption mode and enter the Pre-share Key. You can fill in 64 hexadecimal (0, 1, 2…8, 9, A, B…F) digits, or 8 to 63 ASCII characters as the pre-share key.

WPA

Select Encryption mode and enter RADIUS Server related information. You have to specify the IP address, and port number for the RADIUS Server, and then fill in 64 hexadecimal (0, 1, 2…8, 9, A, B…F) digits, or 8 to 63 ASCII characters as the shared key. The key value is shared by the RADIUS server and this router. This key value must be consistent with the key value in the RADIUS server.

WPA2-PSK

Select Encryption mode and enter the Pre-share Key. You can fill in 64 hexadecimal (0, 1, 2…8, 9, A, B…F) digits, or 8 to 63 ASCII characters as the pre-share key.

WPA2

Select Encryption mode and enter RADIUS Server related information. You have to specify the IP address, and port number for the RADIUS Server, and then fill in 64 hexadecimal (0, 1, 2…8, 9, A, B…F) digits, or 8 to 63 ASCII characters as the shared key. The key value is shared by the RADIUS server and this router. This key value must be consistent with the key value in the RADIUS server.

WPA-PSK/WPA2-PSK

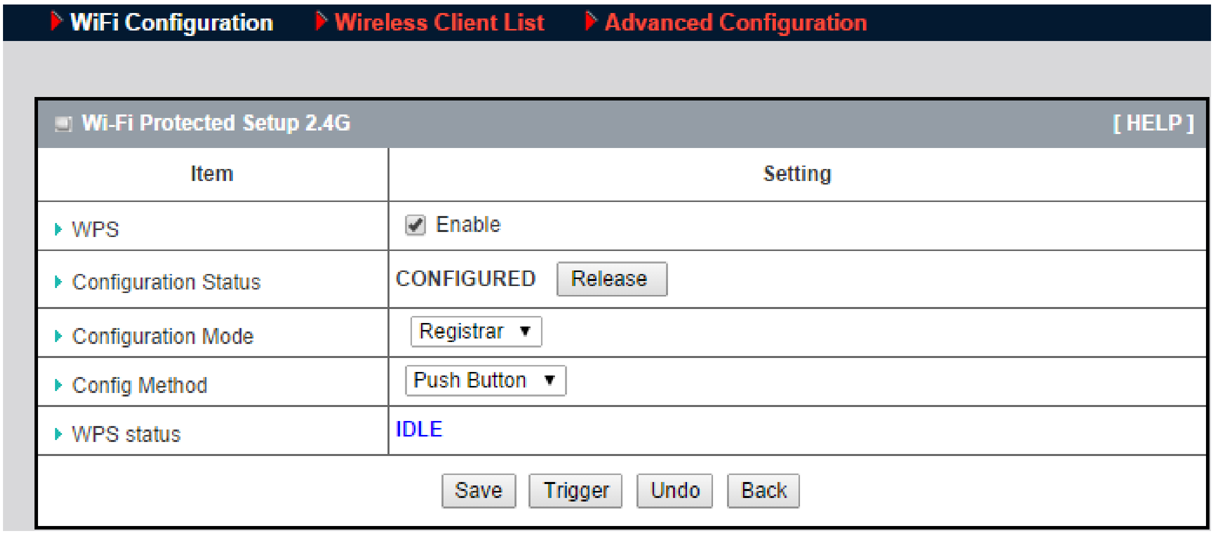
Select Encryption mode and enter the Pre-share Key. You can fill in 64 hexadecimal (0, 1, 2…8, 9, A, B…F) digits, or 8 to 63 ASCII characters as the pre-share key.

WPA/WPA2

Select Encryption mode and enter RADIUS Server related information. You have to specify the IP address, and port number for the RADIUS Server, and then fill in 64 hexadecimal (0, 1, 2…8, 9, A, B…F) digits, or 8 to 63 ASCII characters as the shared key. The key value is shared by the RADIUS server and this router. This key value must be consistent with the key value in the RADIUS server.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

Press “**WPS Setup**”, you can configure and enable the easy setup feature WPS (Wi-Fi Protection Setup) for your wireless network.

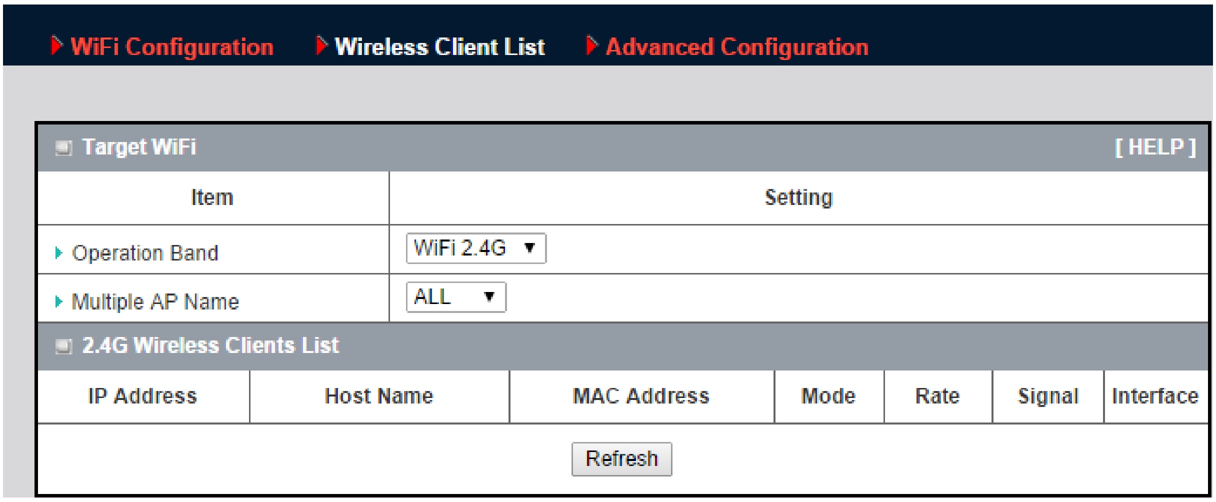


Wi-Fi Protected Setup 2.4G [HELP]

Item	Setting
WPS	☑ Enable
Configuration Status	CONFIGURED Release
Configuration Mode	Registrar ▼
Config Method	Push Button ▼
WPS status	IDLE

- **WPS**: You can enable this function by selecting “Enable”. WPS offers a safe and easy way to allow the wireless clients connected to your wireless network.
- **Config Mode**: Select your configuration Mode from “Registrar” or “Enrollee”. For a AP router or AP, it should be in “Registrar” mode, so that other wireless clients in “Enrollee” mode can connect to the discovered “Registrar”.
- **Config Status**: It shows the status of your configuration.
- **Config Method**: You can select the Configuration Method here from “Pin Code” or “Push Button”.
- **WPS status**: According to your setting, the status will show “Start Process” or “No used”.

Press “**Wireless Clients List**”, and the list of connected wireless clients will be shown consequently.



Target WiFi [HELP]

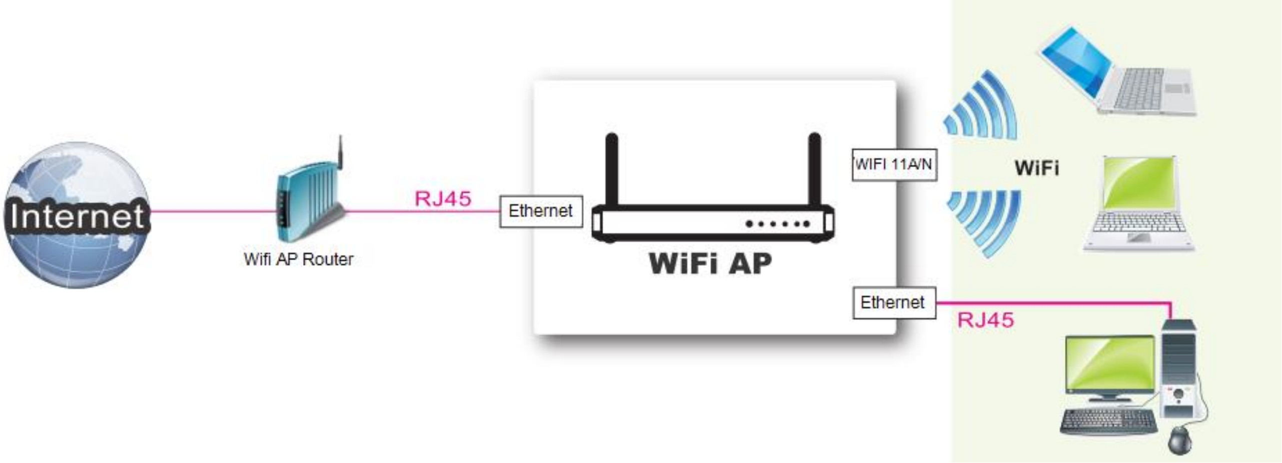
Item	Setting
Operation Band	WiFi 2.4G ▼
Multiple AP Name	ALL ▼

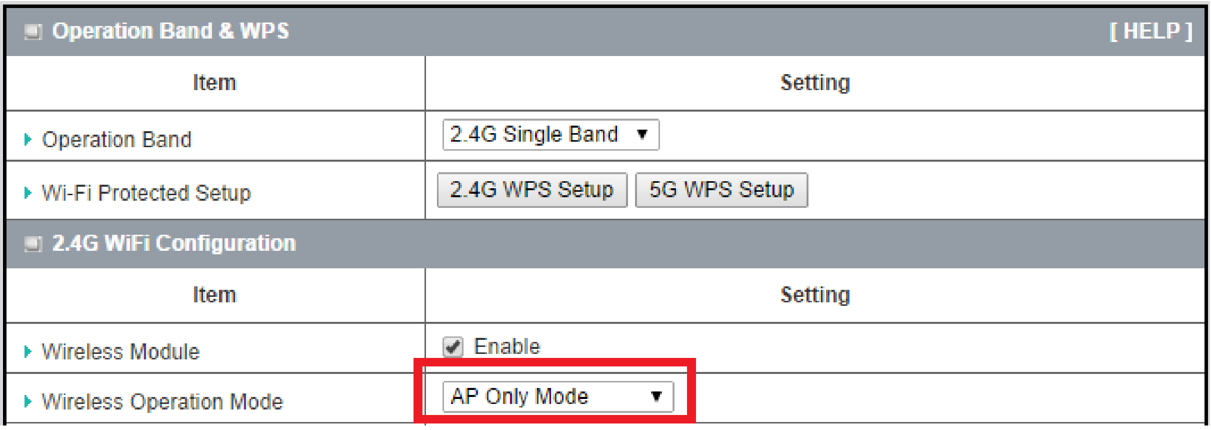
2.4G Wireless Clients List

IP Address	Host Name	MAC Address	Mode	Rate	Signal	Interface

AP Only Mode

When acting as an access point, this device connects all the wireless stations to a wired network and the WAN Port is disabled consequently.





Operation Band & WPS [HELP]

Item	Setting
Operation Band	2.4G Single Band ▼
Wi-Fi Protected Setup	2.4G WPS Setup 5G WPS Setup

2.4G WiFi Configuration

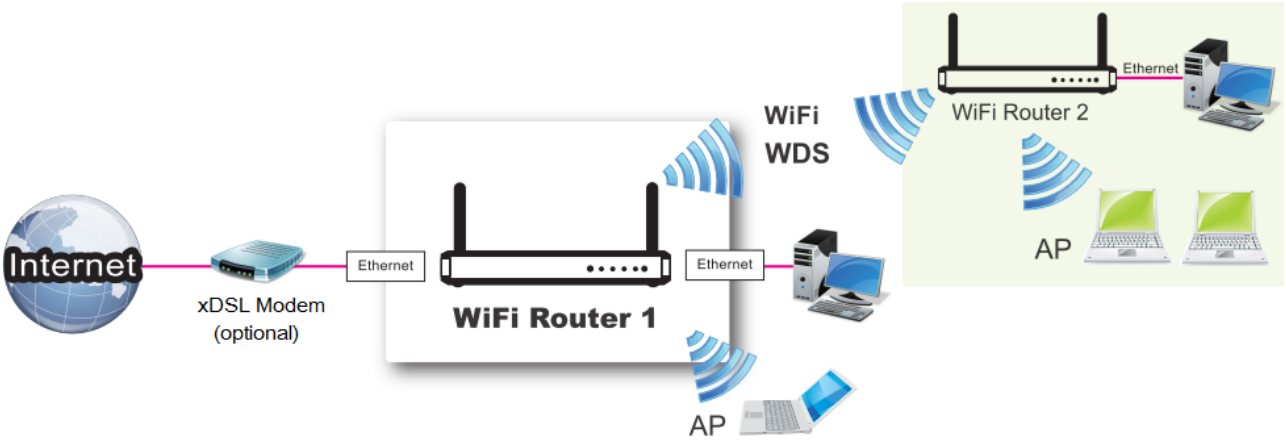
Item	Setting
Wireless Module	☑ Enable
Wireless Operation Mode	AP Only Mode ▼

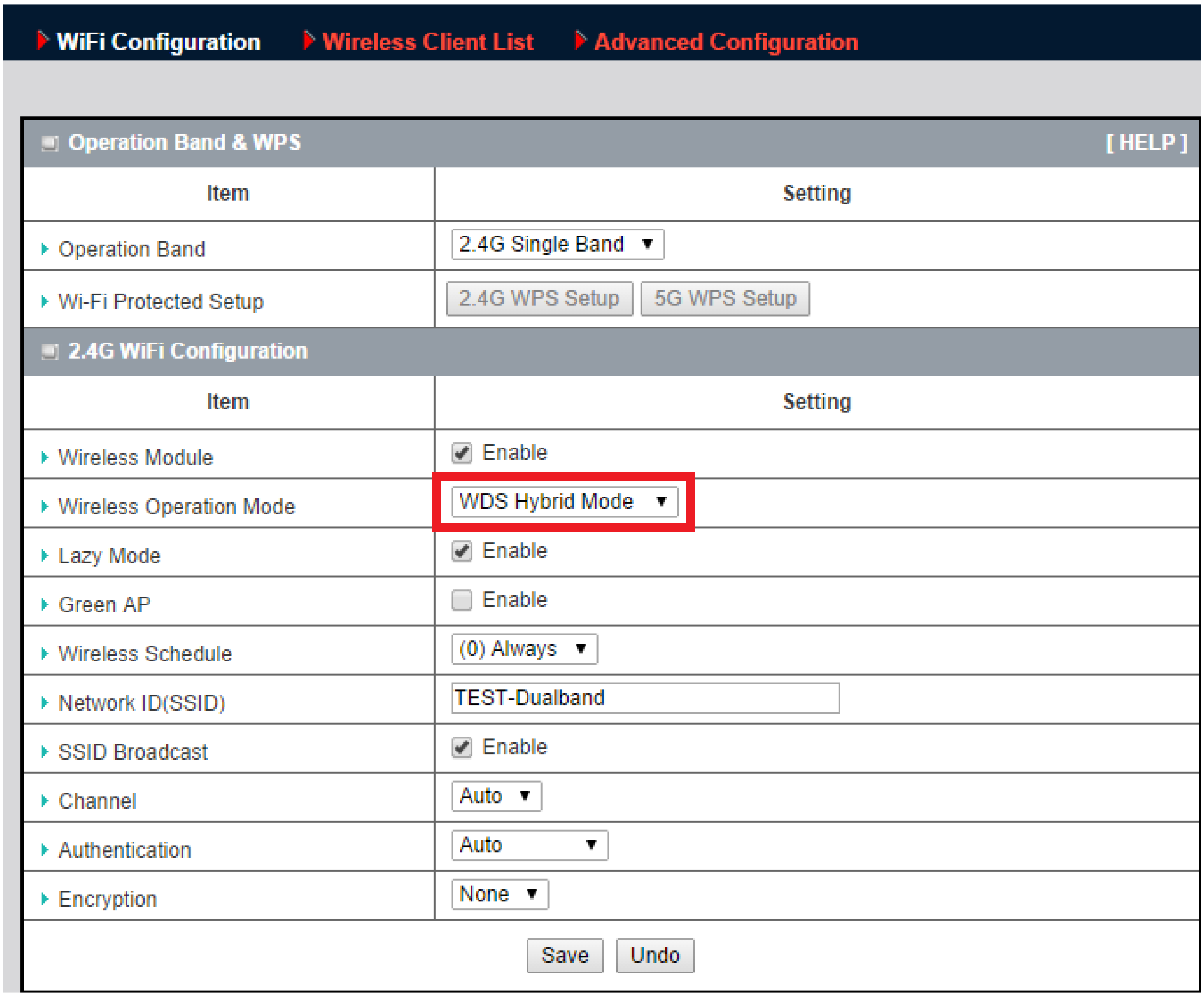
- **Wireless Module**: Enable the wireless function.
- **Wireless Operation Mode**: Choose “AP Only Mode” from the list.
- **Green AP**: Enable the Green AP function to reduce the power consumption when there is no wireless traffics.
- **AP Number**: This device supports up to 8 SSIDs for you to manage your wireless network. You can select AP1 ~ AP8 and configure each wireless network if it is required.
- **Wireless Schedule**: The wireless radio can be turn off according to the schedule rule you specified. By default, the wireless radio is always turned on when the wireless module is enabled.
- **Network ID (SSID)**: Network ID is used for identifying the Wireless LAN (WLAN). Client stations can roam freely over this device and other Access Points that have the same Network ID. (The factory default setting is “default”)
- **SSID Broadcast**: The device will broadcast beacons that have some information, including SSID so that wireless clients can know how many AP devices by scanning the network. Therefore, if this setting is configured as “Disable”, the wireless clients can not find the device from beacons.
- **WLAN Partition**: You can check the WLAN Partition function to separate the wireless clients. The wireless clients can’t communicate each other, but they can access the internet and other Ethernet LAN devices.
- **Channel**: The radio channel number. The permissible channels depend on the Regulatory Domain. The factory default setting is auto channel selection.
- **Wireless Mode**: Choose “B/G mixed”, “B only”, “G only”, “N only”, “G/N mixed” or “B/G/N mixed”. The factory default setting is “B/G/N mixed”.
- **Authentication & Encryption**: You may select one of the following authentications to secure your wireless network: Open, Shared, Auto, WPA-PSK, WPA, WPA2-PSK, WPA2, WPA-PSK/WPA2-PSK, or WPA /WPA2.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

WDS Hybrid Mode

While acting as a wireless Bridge, Wireless Router 1 and Wireless Router 2 can communicate with each other through wireless interface (with WDS). Thus All Stations can communicate each other and are able to access Internet if Wireless Router 1 has the Internet connection.





Operation Band & WPS

Item	Setting
Operation Band	2.4G Single Band ▼
Wi-Fi Protected Setup	2.4G WPS Setup / 5G WPS Setup

2.4G WiFi Configuration

Item	Setting
Wireless Module	☑ Enable
Wireless Operation Mode	WDS Hybrid Mode ▼
Lazy Mode	☑ Enable
Green AP	□ Enable
Wireless Schedule	(0) Always ▼
Network ID(SSID)	TEST-Dualband
SSID Broadcast	☑ Enable
Channel	Auto ▼
Authentication	Auto ▼
Encryption	None ▼

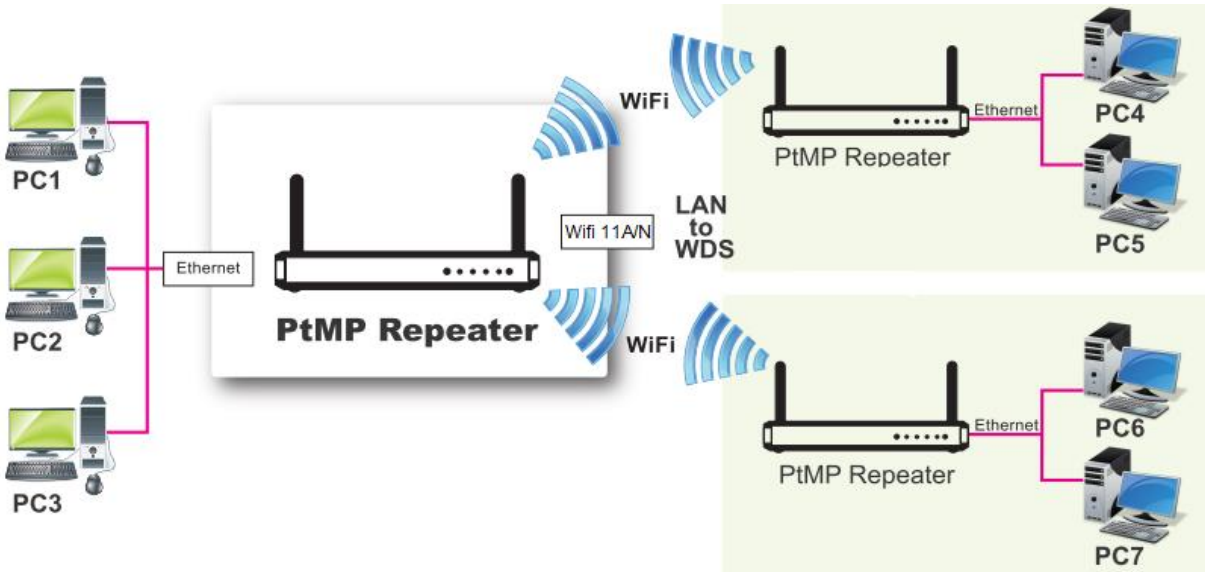
◤ **Lazy Mode**: This device support the Lazy Mode to automatically learn the MAC address of WDS peers, you don’t have to input other peer AP's MAC address. However, not all the APs can be set to enable the Lazy mode simultaneously; at least there must be one AP with all the WDS peers’ MAC address filled.

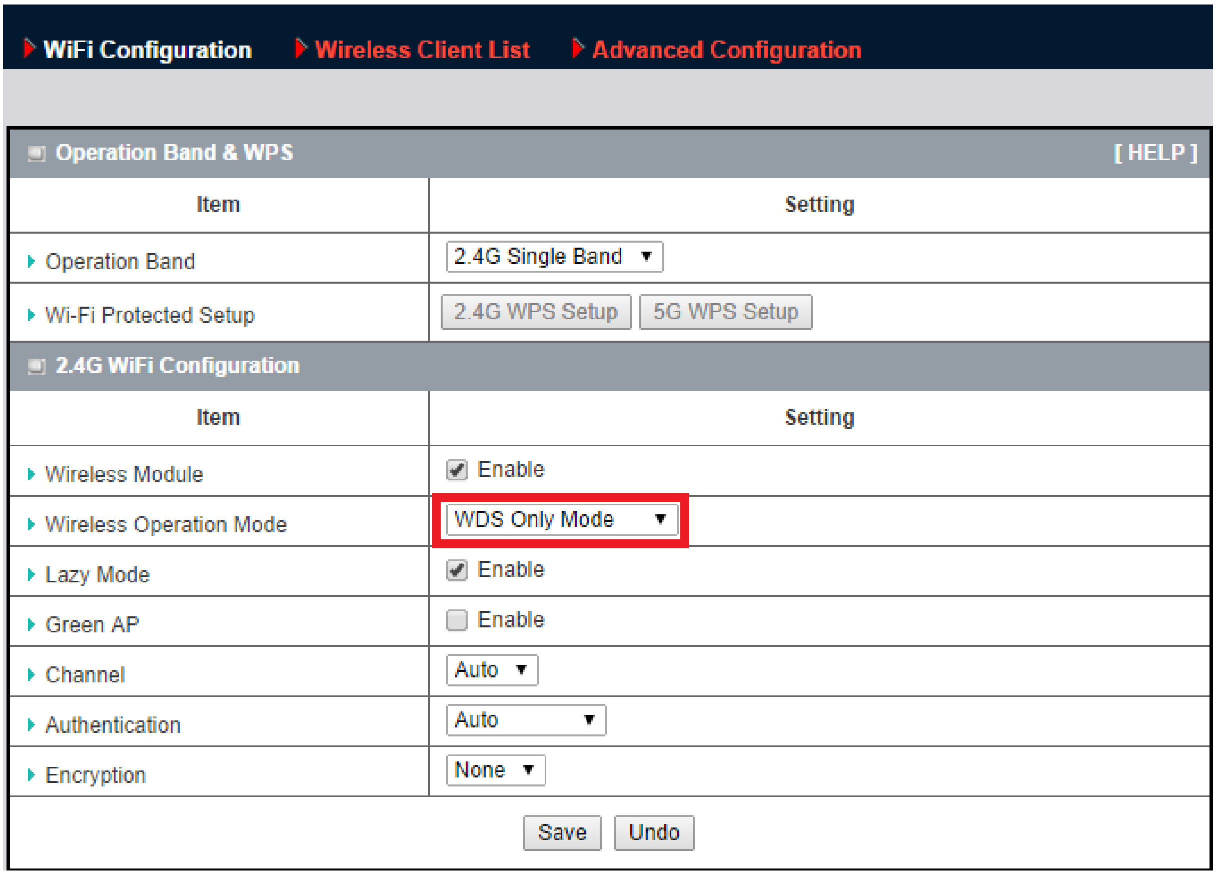
- **Green AP**: Enable the Green AP function to reduce the power consumption when there is no wireless traffics.
- **Wireless Schedule**: The wireless radio can be turn off according to the schedule rule you specified. By default, the wireless radio is always turned on when the wireless module is enabled.
- **Network ID (SSID)**: Network ID is used for identifying the Wireless LAN (WLAN). Client stations can roam freely over this device and other Access Points that have the same Network ID. (The factory default setting is "default")
- **SSID Broadcast**: The device will broadcast beacons that have some information, including SSID so that wireless clients can know how many AP devices by scanning the network. Therefore, if this setting is configured as "Disable", the wireless clients can not find the device from beacons.
- **WLAN Partition**: You can check the WLAN Partition function to separate the wireless clients. The wireless clients can't communicate each other, but they can access the internet and other Ethernet LAN devices.
- **Channel**: The radio channel number. The permissible channels depend on the Regulatory Domain. The factory default setting is auto channel selection.
- **Authentication & Encryption**: You may select one of the following authentications to secure your wireless network: Open, Shared, Auto, WPA-PSK, WPA, WPA2-PSK, WPA2, WPA-PSK/WPA2-PSK, or WPA /WPA2.
- **Remote AP MAC 1 ~ Remote AP MAC 4**: If you do not enable the Lazy mode, you have to enter the wireless MAC address for each WDS peer one by one.

Afterwards, click on "Save" to store your settings or click "Undo" to give up the changes.

WDS Only Mode

WDS (Wireless Distributed System) function let this access point acts as a wireless LAN access point and repeater at the same time. Users can use this feature to build up a large wireless network in a large space like airports, hotels and schools …etc.





Operation Band & WPS [HELP]

Item	Setting
Operation Band	2.4G Single Band ▾
Wi-Fi Protected Setup	2.4G WPS Setup 5G WPS Setup

2.4G WiFi Configuration

Item	Setting
Wireless Module	☑ Enable
Wireless Operation Mode	WDS Only Mode ▾
Lazy Mode	☑ Enable
Green AP	□ Enable
Channel	Auto ▾
Authentication	Auto ▾
Encryption	None ▾

◤ **Lazy Mode**: This device support the Lazy Mode to automatically learn the MAC address of WDS peers, you don’t have to input other peer AP's MAC address. However, not all the APs can be set to enable the Lazy mode simultaneously; at least there must be one AP with all the WDS peers’ MAC address filled.

◤ **Green AP**: Enable the Green AP function to reduce the power consumption when there is no wireless traffics.

◤ **Channel**: The radio channel number. The permissible channels depend on the Regulatory Domain. The factory default setting is auto channel selection.

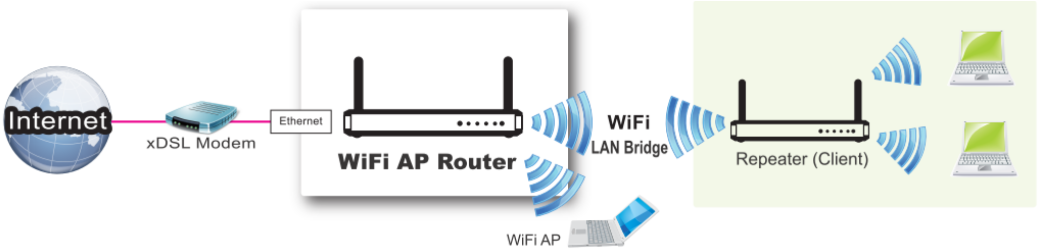
◤ **Authentication & Encryption**: You may select one of the following authentications to secure your wireless network: Open, Shared, Auto, WPA-PSK, WPA, WPA2-PSK, WPA2, WPA-PSK/WPA2-PSK, or WPA /WPA2.

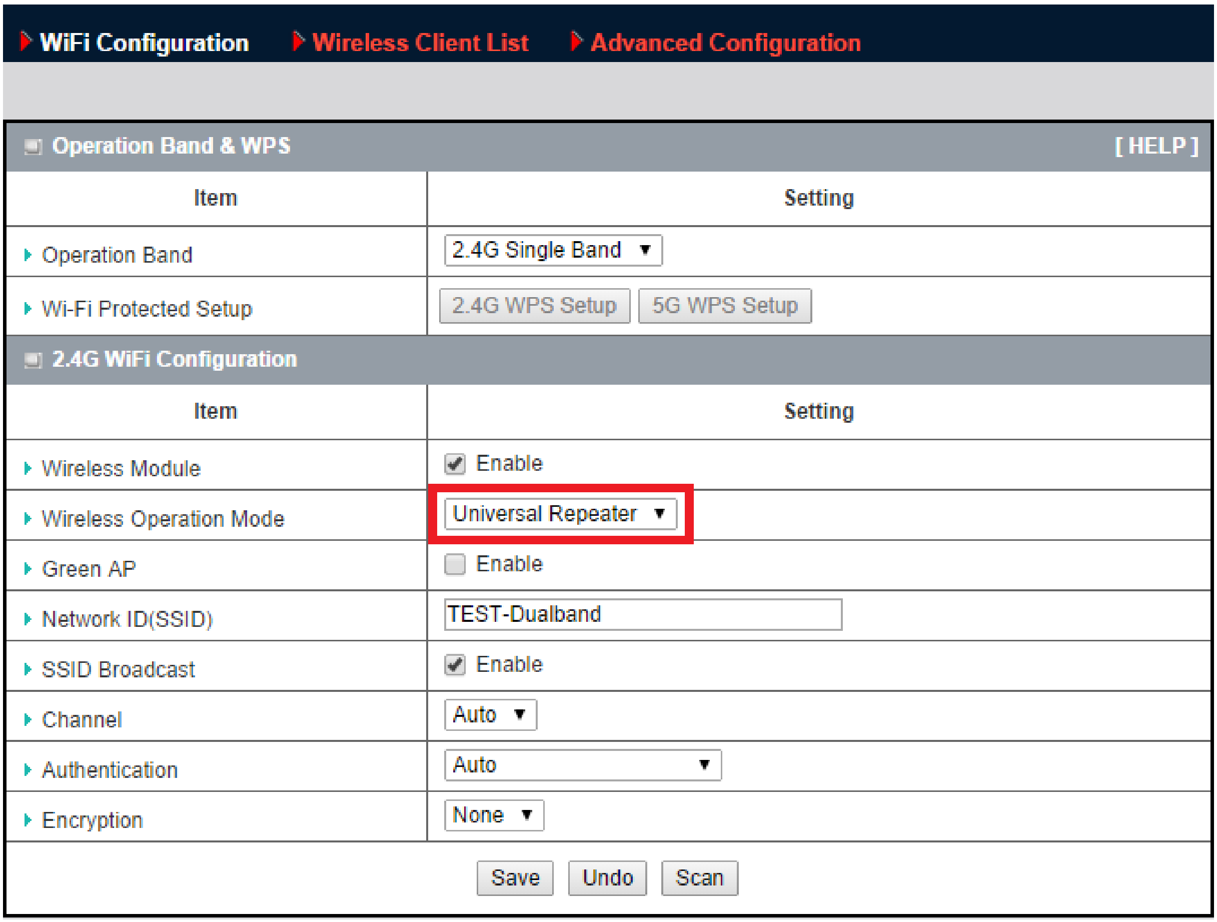
◤ **Remote AP MAC 1 ~ Remote AP MAC 4**: If you do not enable the Lazy mode, you have to enter the wireless MAC address for each WDS peer one by one.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

Universal Repeater Mode

Universal Repeater is a technology used to extend wireless coverage. It provides the function to act as Adapter (Client) and AP at the same time and can use this function to connect to a Root AP and use AP (SSID name must be the same as that of Root AP) function to service all wireless stations within its coverage. All the stations within the coverage of this access point can be bridged to the Root AP.





Operation Band & WPS [HELP]

Item	Setting
Operation Band	2.4G Single Band ▼
Wi-Fi Protected Setup	2.4G WPS Setup 5G WPS Setup

2.4G WiFi Configuration

Item	Setting
Wireless Module	☑ Enable
Wireless Operation Mode	Universal Repeater ▼
Green AP	□ Enable
Network ID(SSID)	TEST-Dualband
SSID Broadcast	☑ Enable
Channel	Auto ▼
Authentication	Auto ▼
Encryption	None ▼

Save Undo Scan

◤ **Green AP**: Enable the Green AP function to reduce the power consumption when there is no wireless traffics.

◤ **Network ID (SSID)**: Network ID is used for identifying the Wireless LAN (WLAN). Client stations can roam freely over this device and other Access Points that have the same Network ID. (The factory default setting is “default”)

◤ **SSID Broadcast**: The device will broadcast beacons that have some information, including SSID so that wireless clients can know how many AP devices by scanning the network. Therefore, if this setting is configured as “Disable”, the wireless clients can not find the device from beacons.

◤ **WLAN Partition**: You can check the WLAN Partition function to separate the wireless clients. The wireless clients can’t communicate each other, but they can access the internet and other Ethernet LAN devices.

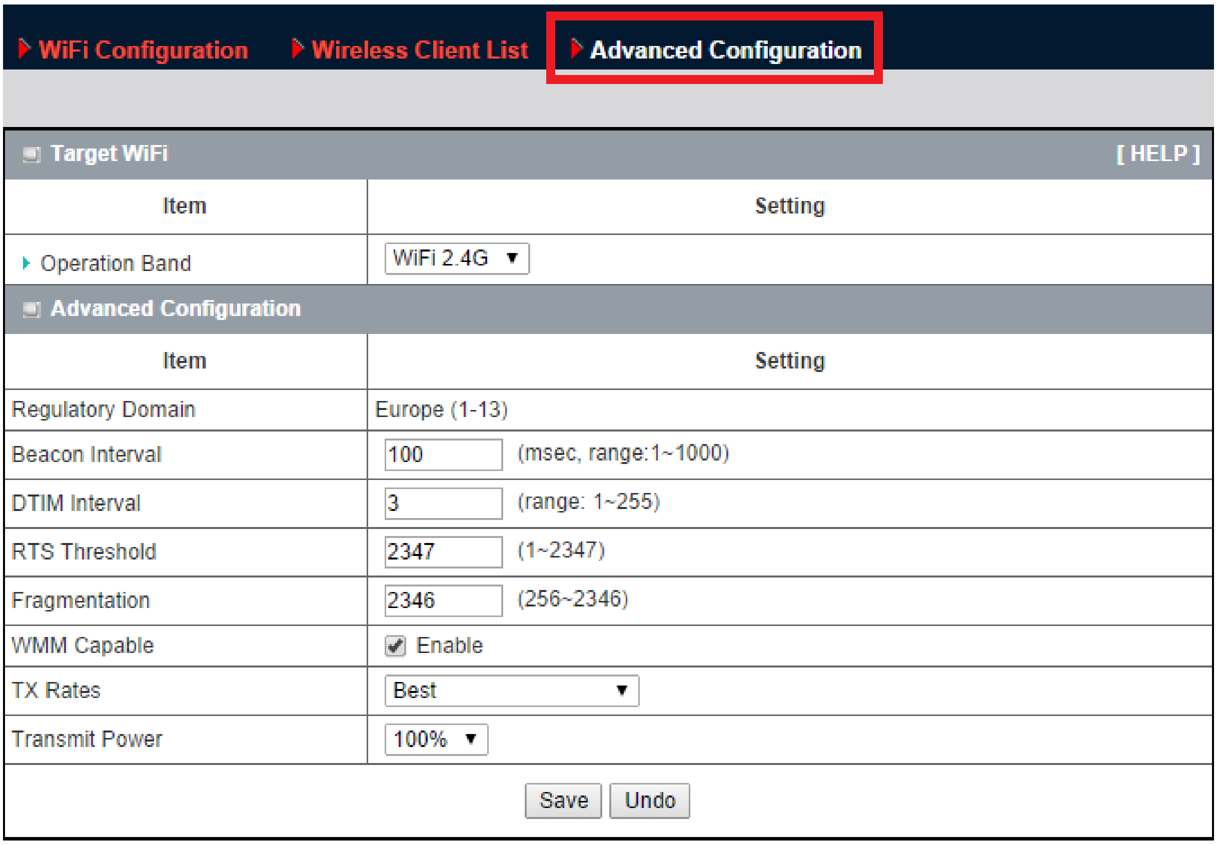
◤ **Channel**: The radio channel number. The permissible channels depend on the Regulatory Domain. The factory default setting is auto channel selection.

- **Authentication & Encryption**: You may select one of the following authentications to secure your wireless network: Open, Shared, Auto, WPA-PSK, WPA, WPA2-PSK, WPA2, WPA-PSK/WPA2-PSK, or WPA /WPA2.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

2.2.2.7. Advanced Configuration

This device provides advanced wireless setup for professional user to optimize the wireless performance under the specific installation environment.



Target WiFi

Item	Setting
Operation Band	WiFi 2.4G ▼

Advanced Configuration

Item	Setting
Regulatory Domain	Europe (1-13)
Beacon Interval	100 (msec, range:1~1000)
DTIM Interval	3 (range: 1~255)
RTS Threshold	2347 (1~2347)
Fragmentation	2346 (256~2346)
WMM Capable	☑ Enable
TX Rates	Best ▼
Transmit Power	100% ▼

- **Beacon interval**: Beacons are packets sent by a wireless router to synchronize wireless devices.
- **Transmit Power**: Normally the wireless transmission power operates at 100% out power specification of this device. You can lower down the power ratio to prevent transmissions from reaching beyond your corporate/home office or designated wireless area.
- **RTS Threshold**: If an excessive number of wireless packet collision occurred, the wireless performance will be affected. It can be improved by adjusting the RTS/CTS (Request to Send/Clear to Send) threshold value.
- **Fragmentation**: Wireless frames can be divided into smaller units (fragments) to improve performance in the presence of RF interference and at the limits of RF coverage.
- **DTIM interval**: A DTIM is a countdown informing clients of the next window for listening to

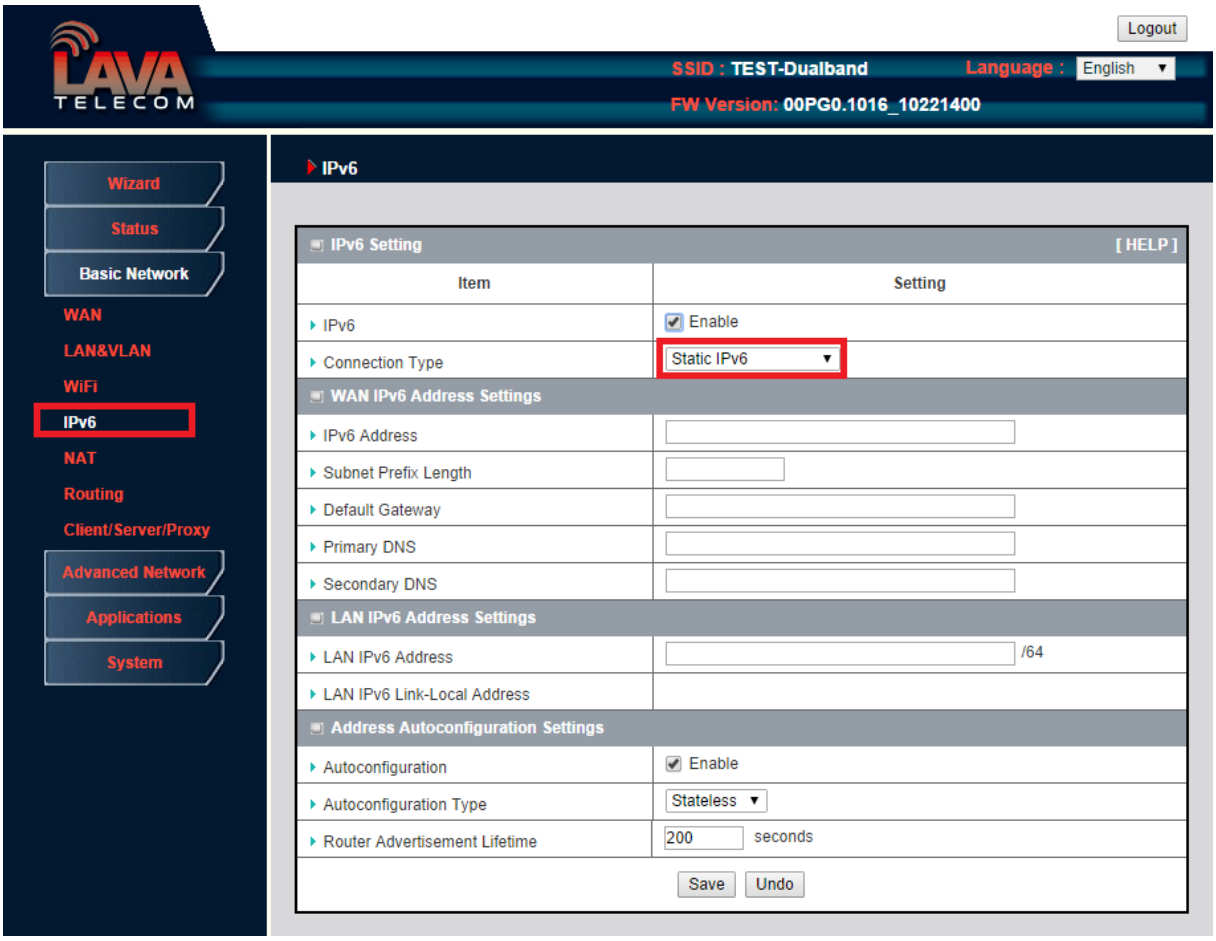
broadcast and multicast messages. When the wireless router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value.

- **WMM Capable**: WMM can help control latency and jitter when transmitting multimedia content over a wireless connection.
- **TX Rate**: Can Fix TX Rate to transmit date.

2.2.2.8. IPv6 Setup

The growth of the Internet has created a need for more addresses than are possible with IPv4. IPv6 (Internet Protocol version 6) is a version of the Internet Protocol (IP) intended to succeed IPv4, which is the protocol currently used to direct almost all Internet traffic. IPv6 also implements additional features not present in IPv4. It simplifies aspects of address assignment (stateless address auto-configuration), network renumbering and router announcements when changing Internet connectivity providers. This router supports various types of IPv6 connection (Static IPv6 / DHCPv6 / PPPoE / 6 to 4 / IPv6 in IPv4 tunnel). Please ask your ISP of what type of IPv6 is supported before you proceed with IPv6 setup.

Static IPv6



IPv6 Setting

Item	Setting
IPv6	☑ Enable
Connection Type	Static IPv6 ▾
WAN IPv6 Address Settings	
IPv6 Address	
Subnet Prefix Length	
Default Gateway	
Primary DNS	
Secondary DNS	
LAN IPv6 Address Settings	
LAN IPv6 Address	/64
LAN IPv6 Link-Local Address	
Address Autoconfiguration Settings	
Autoconfiguration	☑ Enable
Autoconfiguration Type	Stateless ▾
Router Advertisement Lifetime	200 seconds

When “Static IPv6” is selected you need to do the following settings:

◤ **WAN IPv6 address settings:**

IPv6 address

Enter the IPv6 address here; IPv6 addresses have a size of 128 bits. Therefore, IPv6 has a vastly enlarged address space compared to IPv4. An example of an IPv6 address is “2001:0db8:85a3:0000:0000:8a2e:0370:7334”

Subnet Prefix Length

Enter the Prefix length of the Subnet Mask here; The subnet mask was the forerunner of the modern IP address prefix length. For example a subnet mask of 255.255.255.0 conveys exactly the same information as a prefix length of /24, a subnet mask of 255.255.255.240 is equivalent to a prefix length of /28.

Default Gateway

Enter the Default Gateway address here; A default gateway is the node on the computer network that the network software uses when an IP address does not match any other routes in the routing table.

Primary / Secondary DNS

You may select to obtain DNS server address automatically or use following DNS address. You may add IPv6 address Primary DNS address and secondary DNS address.

◤ **LAN IPv6 address settings**: Please enter “LAN IPv6 address” and ignore the “LAN IPv6 Link-Local address”.

◤ **Address auto configuration settings:**

Auto-configuration

Disable or enable this auto configuration setting.

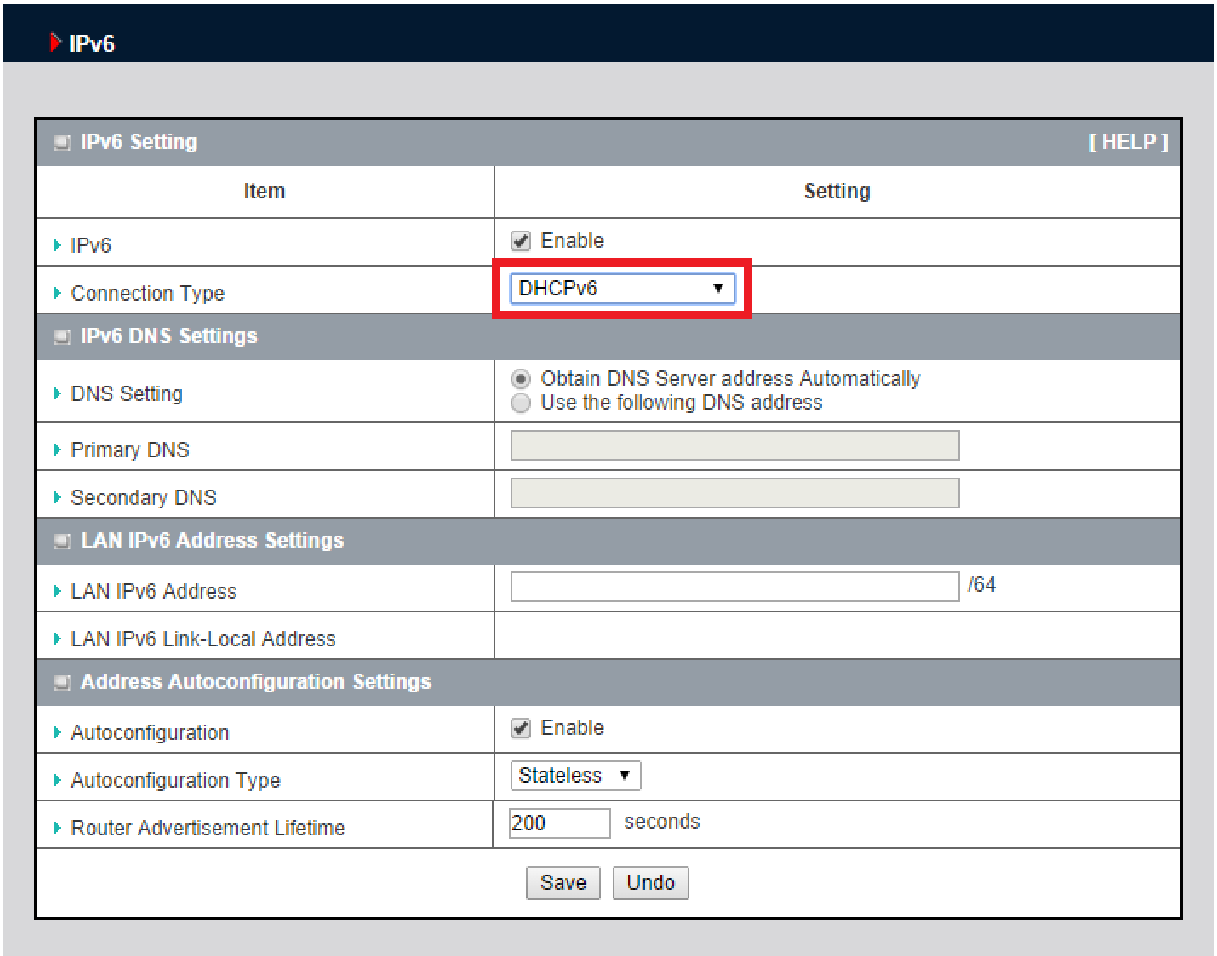
Auto-configuration type

You may set stateless or stateful (Dynamic IPv6).

Router advertisement Lifetime

You can set the time for the period that the router send (broadcast) its router advertisement. Each router periodically multicasts a Router Advertisement from each of its multicast interfaces, announcing the IP address(es) of that interface. Hosts discover the addresses of their neighboring routers simply by listening for advertisements. When a host attached to a multicast link starts up, it may multicast a Router Solicitation to ask for immediate advertisements, rather than waiting for the next periodic ones to arrive; if and only if no advertisements are forthcoming, the host may retransmit the solicitation a small number of times, but then must desist from sending any more solicitations. Any routers that subsequently start up, or that were not discovered because of packet loss or temporary link partitioning, are eventually discovered by reception of their periodic (unsolicited) advertisements.

DHCP v6



IPv6

IPv6 Setting	[HELP]
Item	Setting
IPv6	☑ Enable
Connection Type	DHCPv6 ▼
IPv6 DNS Settings	
DNS Setting	● Obtain DNS Server address Automatically ○ Use the following DNS address
Primary DNS	
Secondary DNS	
LAN IPv6 Address Settings	
LAN IPv6 Address	/64
LAN IPv6 Link-Local Address	
Address Autoconfiguration Settings	
Autoconfiguration	☑ Enable
Autoconfiguration Type	Stateless ▼
Router Advertisement Lifetime	200 seconds

When “DHCP v6” is selected you need to do the following settings:

◤ **IPv6 DNS (WAN IPv6 address) settings**: You may select to obtain DNS server address automatically or use following DNS address. You may add IPv6 address Primary DNS address and secondary DNS address.

◤ **LAN IPv6 address settings**: Please enter “LAN IPv6 address” and ignore the “LAN IPv6 Link-Local address”.

◤ **Address auto configuration settings:**

Auto-configuration

Disable or enable this auto configuration setting.

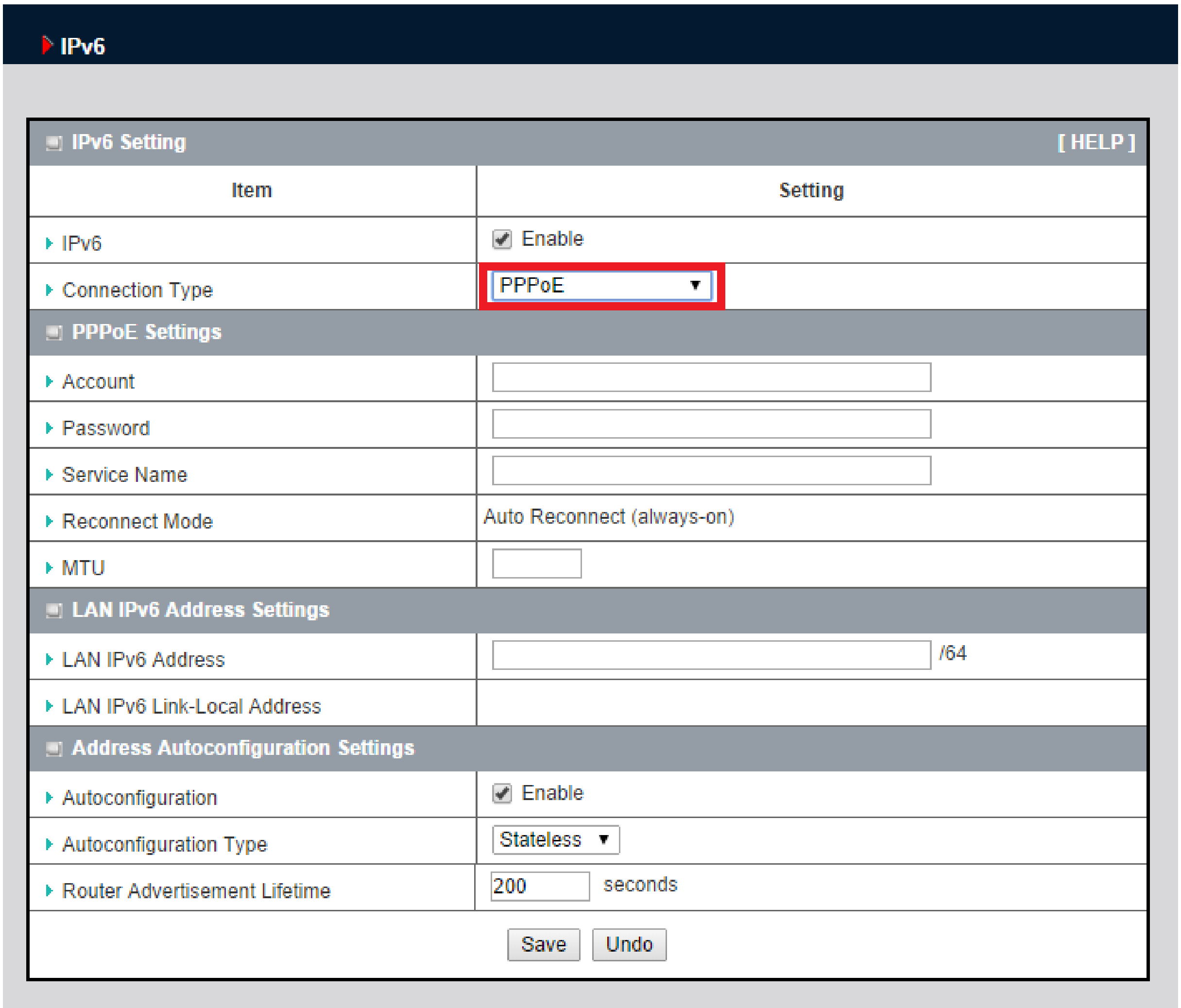
Auto-configuration type

You may set stateless or stateful (Dynamic IPv6).

Router advertisement Lifetime

You can set the time for the period that the router send (broadcast) its router advertisement. Each router periodically multicasts a Router Advertisement from each of its multicast interfaces, announcing the IP address(es) of that interface. Hosts discover the addresses of their neighboring routers simply by listening for advertisements. When a host attached to a multicast link starts up, it may multicast a Router Solicitation to ask for immediate advertisements, rather than waiting for the next periodic ones to arrive; if and only if no advertisements are forthcoming, the host may retransmit the solicitation a small number of times, but then must desist from sending any more solicitations. Any routers that subsequently start up, or that were not discovered because of packet loss or temporary link partitioning, are eventually discovered by reception of their periodic (unsolicited) advertisements.

PPPoE



IPv6

IPv6 Setting	[HELP]
Item	Setting
IPv6	☑ Enable
Connection Type	PPPoE ▼
PPPoE Settings	
Account	
Password	
Service Name	
Reconnect Mode	Auto Reconnect (always-on)
MTU	
LAN IPv6 Address Settings	
LAN IPv6 Address	/64
LAN IPv6 Link-Local Address	
Address Autoconfiguration Settings	
Autoconfiguration	☑ Enable
Autoconfiguration Type	Stateless ▼
Router Advertisement Lifetime	200 seconds

When "PPPoE" is selected you need to do the following settings:

◤ **WAN IPv6 address settings:**

Username: enter the Username that you got from your ISP

Password: enter the Password that you got from your ISP

Service Name: enter the Service Name that you got from your ISP

Reconnection Mode: leave the setting as "AutoReconnect (always-on)"

Max. Idle Time: give max. idle time that you want here

MTU (Maximum Transmission Unit): Most ISP offers MTU value to users. The default MTU value is 0 (auto).

- **LAN IPv6 address settings**: Please enter "LAN IPv6 address" and ignore the "LAN IPv6 Link-Local address".
- **Address auto configuration settings:**

Auto-configuration

Disable or enable this auto configuration setting.

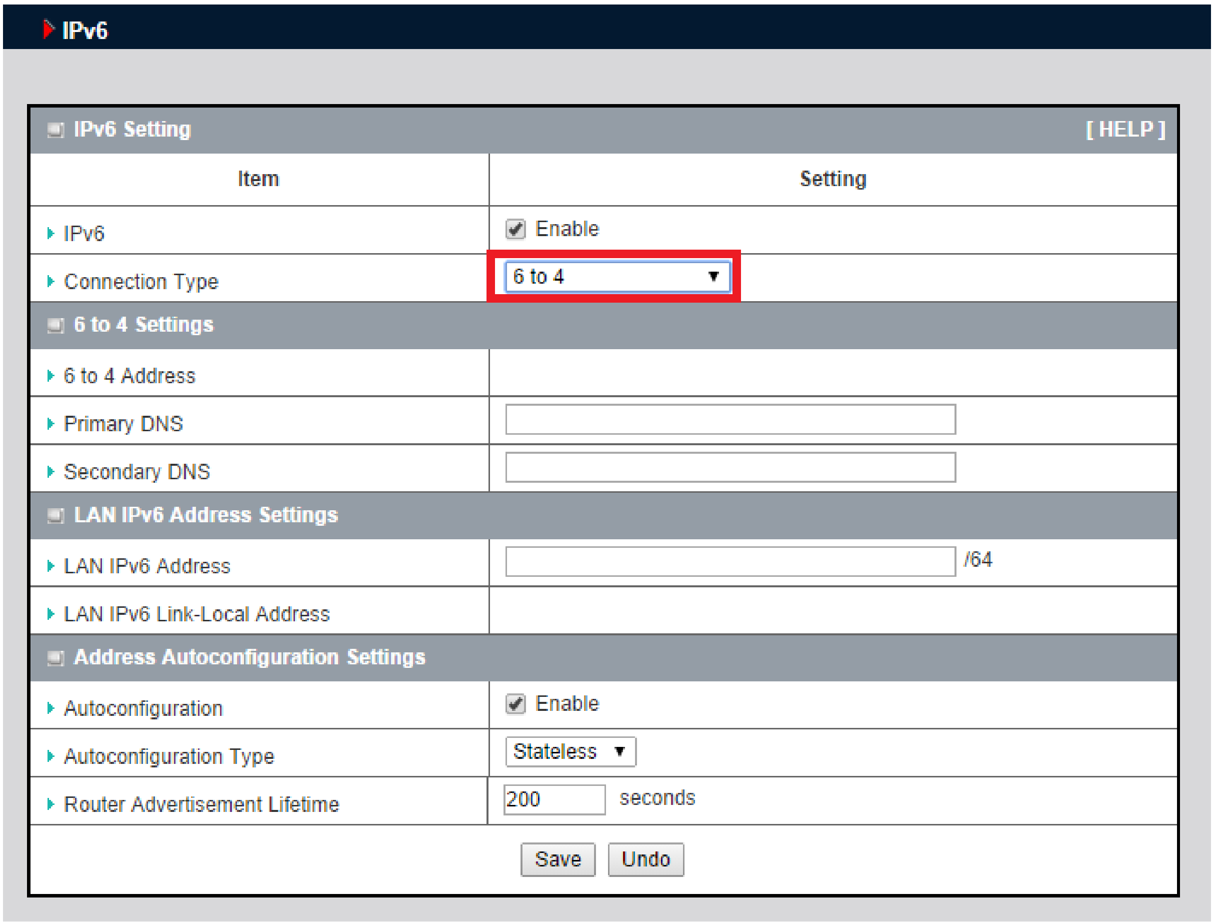
Auto-configuration type

You may set stateless or stateful (Dynamic IPv6).

Router advertisement Lifetime

You can set the time for the period that the router send (broadcast) its router advertisement. Each router periodically multicasts a Router Advertisement from each of its multicast interfaces, announcing the IP address(es) of that interface. Hosts discover the addresses of their neighboring routers simply by listening for advertisements. When a host attached to a multicast link starts up, it may multicast a Router Solicitation to ask for immediate advertisements, rather than waiting for the next periodic ones to arrive; if and only if no advertisements are forthcoming, the host may retransmit the solicitation a small number of times, but then must desist from sending any more solicitations. Any routers that subsequently start up, or that were not discovered because of packet loss or temporary link partitioning, are eventually discovered by reception of their periodic (unsolicited) advertisements.

6 to 4



IPv6

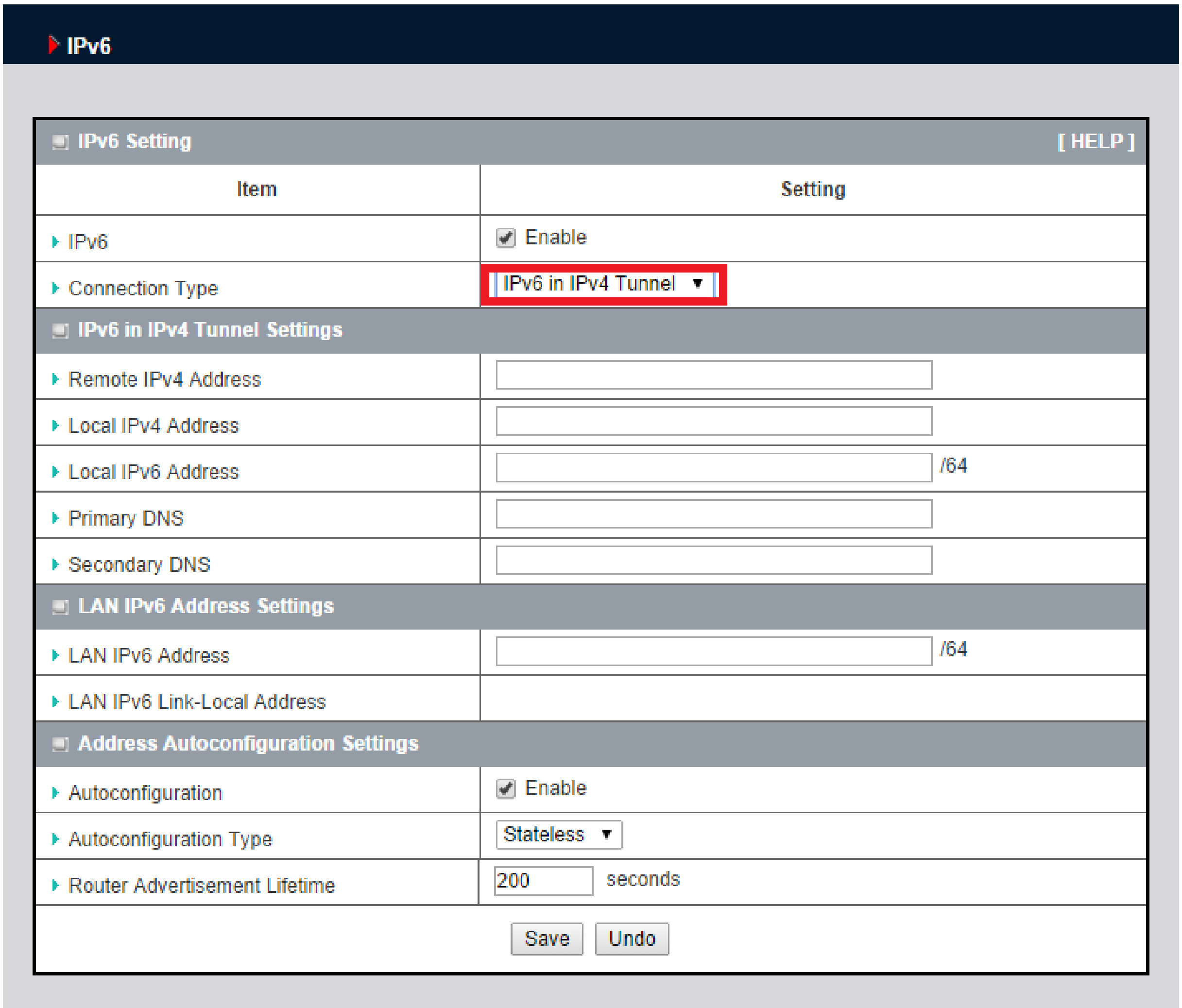
IPv6 Setting [HELP]

Item	Setting
IPv6	☑ Enable
Connection Type	6 to 4 ▼
6 to 4 Settings	
6 to 4 Address	
Primary DNS	
Secondary DNS	
LAN IPv6 Address Settings	
LAN IPv6 Address	/64
LAN IPv6 Link-Local Address	
Address Autoconfiguration Settings	
Autoconfiguration	☑ Enable
Autoconfiguration Type	Stateless ▼
Router Advertisement Lifetime	200 seconds

When “6 to 4 IPv6” is selected you need to do the following settings:

- **6 to 4 Settings**: You may obtain IPv6 DNS automatically or set DNS address manually for Primary DNS address and secondary DNS address.
- **LAN IPv6 address settings**: Enter “LAN IPv6 address” and “LAN IPv6 Link-Local address”.
- **Address auto configuration settings**: Disable or enable this auto configuration setting. You may set stateless or stateful (Dynamic IPv6), and also check if need to send Router advertisement messages periodically.

IPv6 in IPv4 Tunnel



IPv6

IPv6 Setting [HELP]

Item	Setting
IPv6	☑ Enable
Connection Type	IPv6 in IPv4 Tunnel ▼
IPv6 in IPv4 Tunnel Settings	
Remote IPv4 Address	
Local IPv4 Address	
Local IPv6 Address	/64
Primary DNS	
Secondary DNS	
LAN IPv6 Address Settings	
LAN IPv6 Address	/64
LAN IPv6 Link-Local Address	
Address Autoconfiguration Settings	
Autoconfiguration	☑ Enable
Autoconfiguration Type	Stateless ▼
Router Advertisement Lifetime	200 seconds

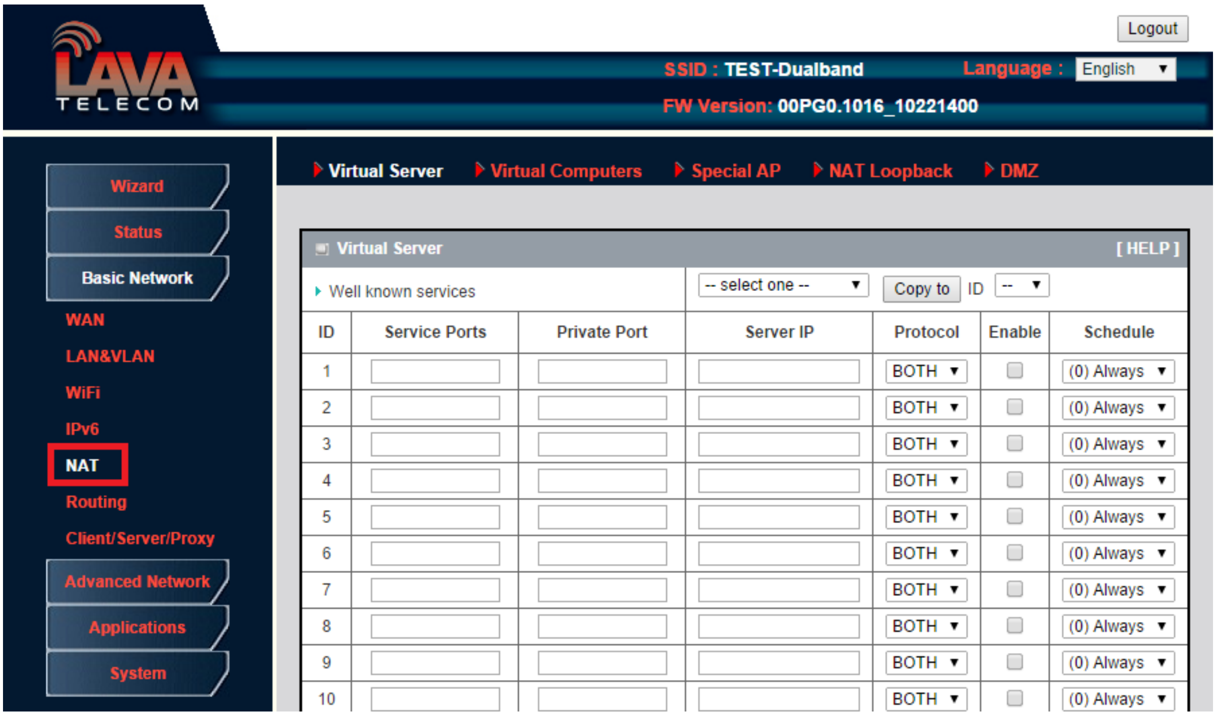
When “IPv6 in IPv4 Tunnel” is selected you need to do the following settings:

- **IPv6 in IPv4 Tunnel Settings**: you may add remote / local IPv4 address and local IPv6 address, then set DNS address manually for Primary DNS address and secondary DNS address.
- **LAN IPv6 address setting**: LAN IPv6 address and LAN IPv6 Link-Local address.
- **Address auto configuration setting**: Disable or enable this auto configuration setting. You may set stateless or stateful (Dynamic IPv6), and also check if need to send Router advertisement messages periodically.

2.2.2.9. NAT Setup - Virtual Server

This device’s NAT firewall filters out unrecognized packets to protect your Intranet, so all hosts behind this device are invisible to the outside world. If you wish, you can make some of them accessible by enabling the Virtual Server Mapping.

A virtual server is defined as a **Service Port**, and all requests to this port will be redirected to the computer specified by the **Server IP. Virtual Server** can work with Scheduling Rules, and give user more flexibility on **Access control**. For the details, please refer to Scheduling Rule.



Virtual Server

Well known services -- select one -- ID --

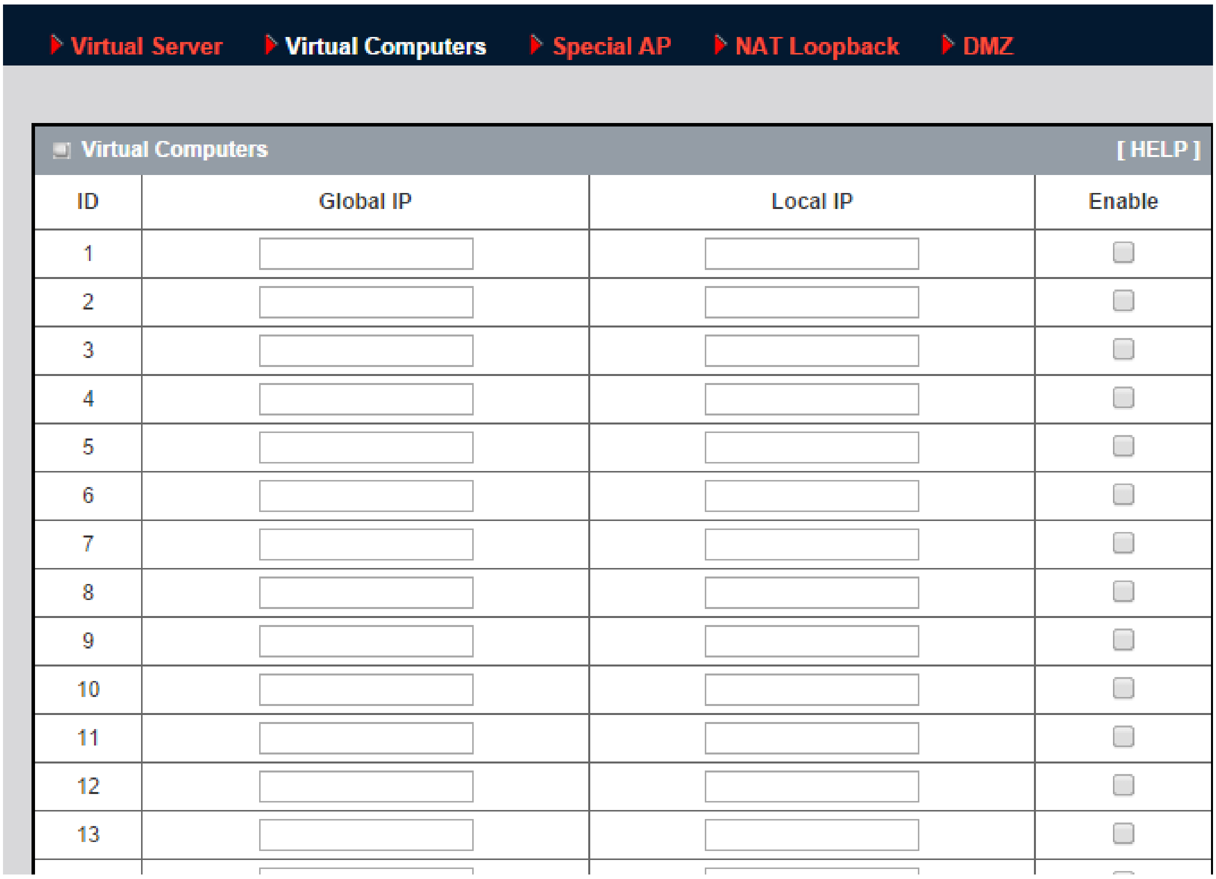
ID	Service Ports	Private Port	Server IP	Protocol	Enable	Schedule
1				BOTH	□	(0) Always
2				BOTH	□	(0) Always
3				BOTH	□	(0) Always
4				BOTH	□	(0) Always
5				BOTH	□	(0) Always
6				BOTH	□	(0) Always
7				BOTH	□	(0) Always
8				BOTH	□	(0) Always
9				BOTH	□	(0) Always
10				BOTH	□	(0) Always

For example, if you have an FTP server (Service port 21) at 192.168.123.1, a Web server1 (Service port 80) at 192.168.123.2, a Web server2 (Service Port 8080 and Private port 80) at 192.168.123.3, and a VPN server at 192.168.123.6, then you need to specify the following virtual server mapping table

Service Port	Private Port	Server IP	Enable
21		192.168.123.1	V
80		192.168.123.2	V
8080	80	192.168.123.3	v
1723		192.168.123.6	V

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

2.2.2.10. NAT - Virtual Computers



Virtual Computers [HELP]

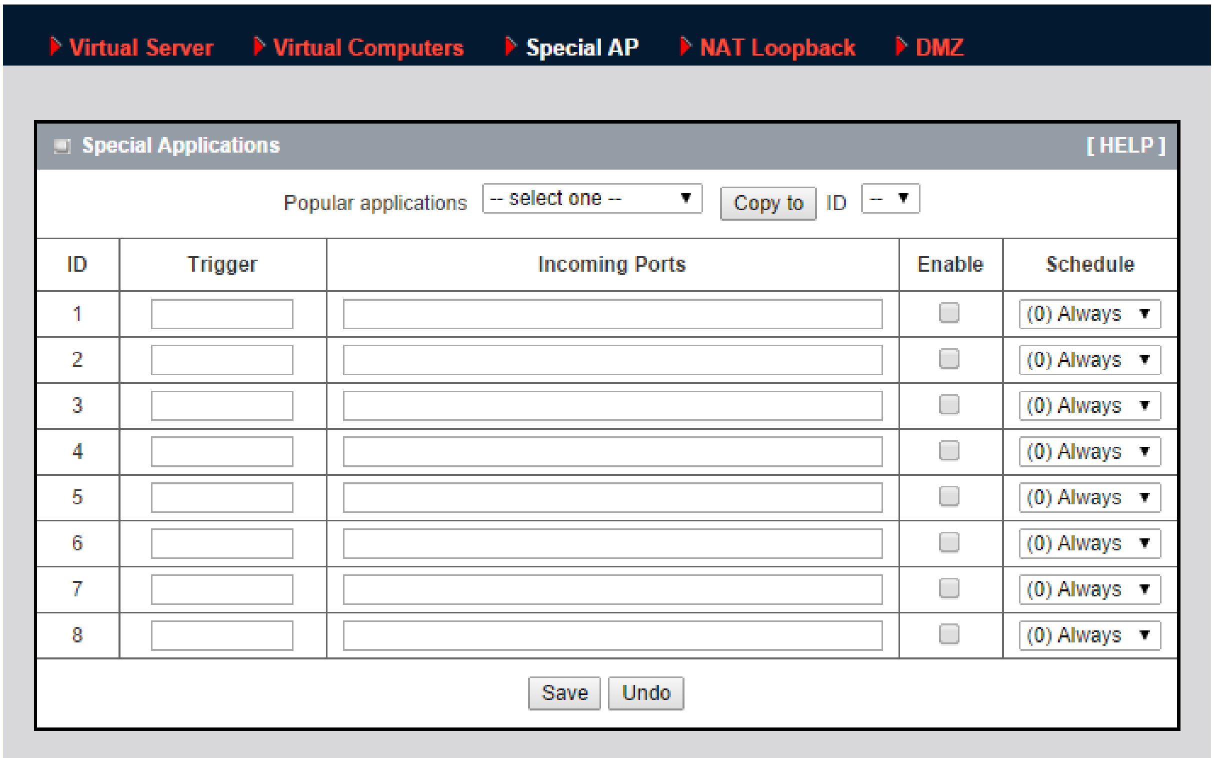
ID	Global IP	Local IP	Enable
1			□
2			□
3			□
4			□
5			□
6			□
7			□
8			□
9			□
10			□
11			□
12			□
13			□

Virtual Computer enables you to use the original NAT feature, and allows you to setup the one-to-one mapping of multiple global IP address and local IP address.

- **Global IP**: Enter the global IP address assigned by your ISP.
- **Local IP**: Enter the local IP address of your LAN PC corresponding to the global IP address.
- **Enable**: Check this item to enable the Virtual Computer feature.

2.2.2.11. NAT - Special AP

Some applications require multiple connections, like Internet games, Video conferencing, Internet telephony, etc. Because of the firewall function, these applications cannot work with a pure NAT router. **The Special Applications** feature allows some of these applications to work with this product. If the mechanism of Special Applications fails to make an application work, try setting your computer as the DMZ host instead.



Special Applications [HELP]

Popular applications -- select one -- ▼ Copy to ID -- ▼

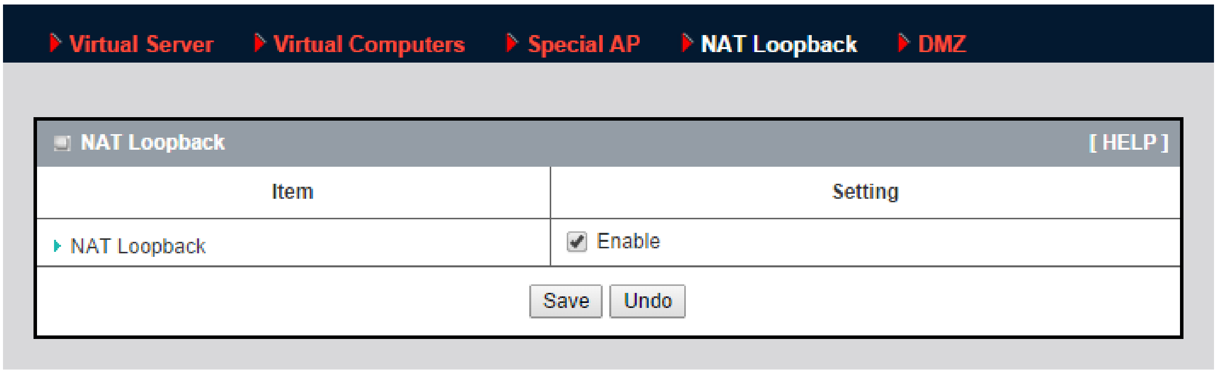
ID	Trigger	Incoming Ports	Enable	Schedule
1			☐	(0) Always ▼
2			☐	(0) Always ▼
3			☐	(0) Always ▼
4			☐	(0) Always ▼
5			☐	(0) Always ▼
6			☐	(0) Always ▼
7			☐	(0) Always ▼
8			☐	(0) Always ▼

This device provides some predefined settings. Select your application and click “Copy to” to add the predefined setting to your list.

- **Trigger**: The outbound port number issued by the application.
- **Incoming Ports**: When the trigger packet is detected, the inbound packets sent to the specified port numbers are allowed to pass through the firewall.
- **Enable**: Check this item to enable the Special AP feature.

Afterwards, Click on “Save” to store your settings or click “Undo” to give up the changes.

2.2.2.12. NAT Loopback

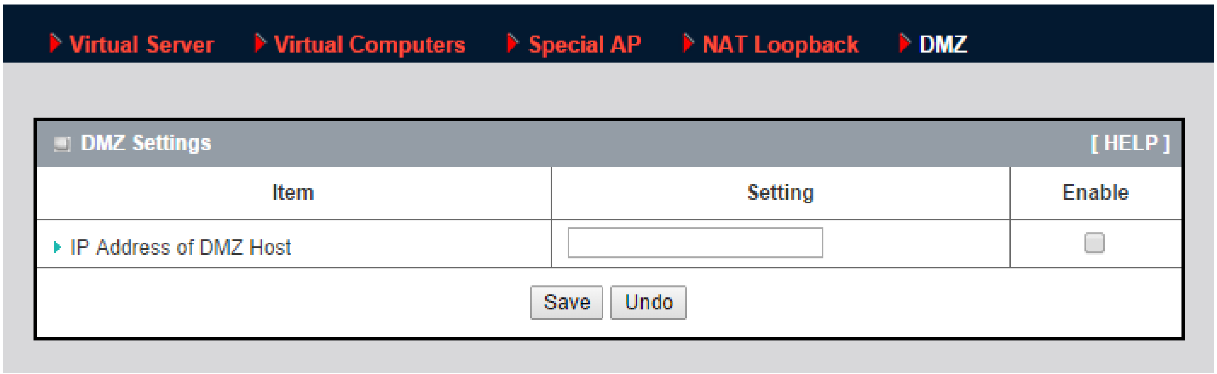


NAT Loopback [HELP]

Item	Setting
NAT Loopback	☑ Enable

Allow you to access the external IP address from inside your home or office network. This is useful when you run a server inside your network.

2.2.2.13. NAT - DMZ



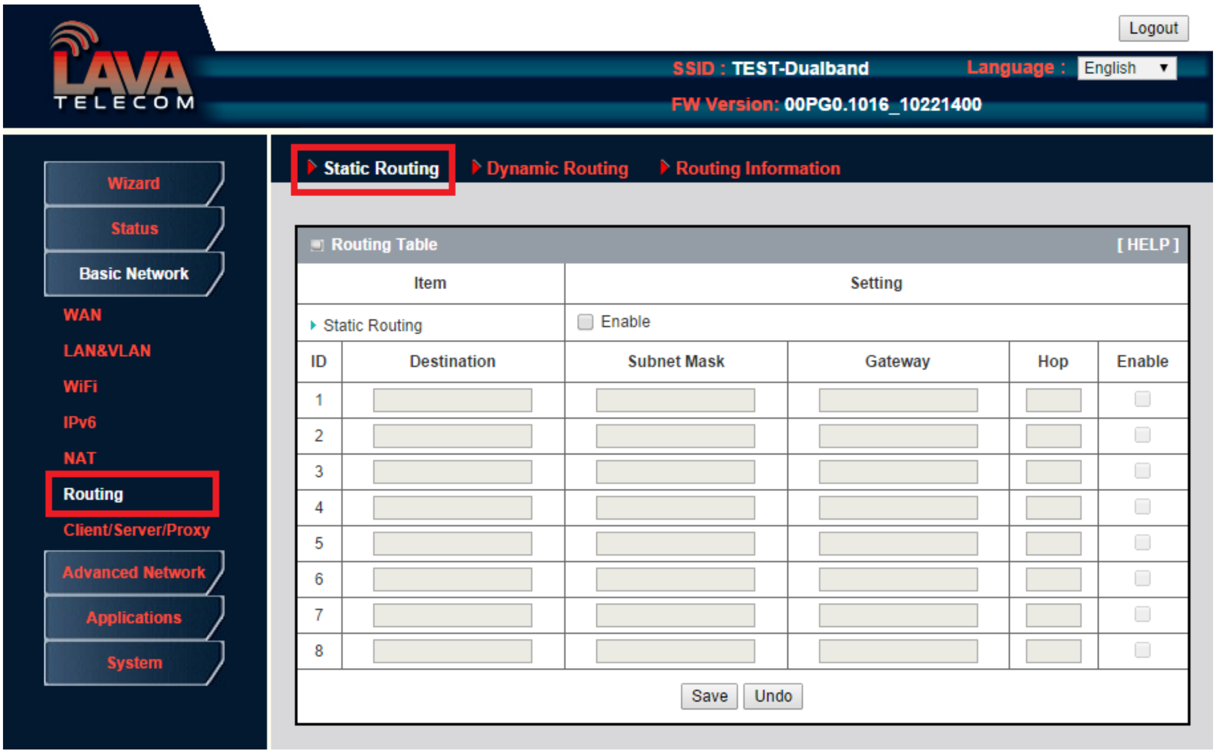
Item	Setting	Enable
IP Address of DMZ Host		□

DMZ (DeMilitarized Zone) Host is a host without the protection of firewall. It allows a computer to be exposed to unrestricted 2-way communication for Internet games, Video conferencing, Internet telephony and other special applications.

NOTE: This feature should be used only when needed.

2.2.2.14. Routing - Static Routing

If you have more than one routers and subnets, you will need to enable routing function to allow packets to find proper routing path and allow different subnets to communicate with each other..



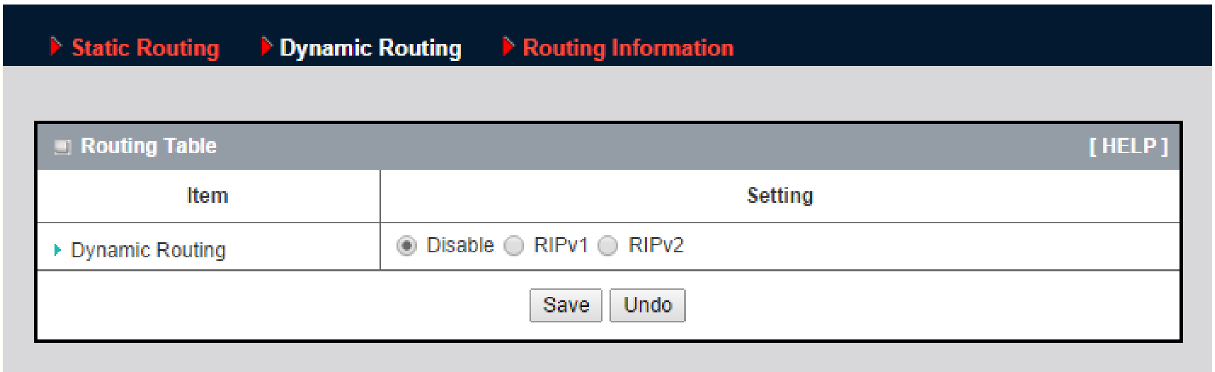
SSID : TEST-Dualband
Language : English
FW Version: 00PG0.1016_10221400

Item	Setting
Static Routing	□ Enable

ID	Destination	Subnet Mask	Gateway	Hop	Enable
1					□
2					□
3					□
4					□
5					□
6					□
7					□
8					□

For static routing, you can specify up to 32 routing rules. The routing rules allow you to determine which physical interface addresses are utilized for outgoing IP data grams. You can enter the destination IP address, subnet mask, gateway, and hop for each routing rule, and then enable or disable the rule by checking or un-checking the Enable checkbox.

2.2.2.15. Routing - Dynamic Routing



Routing Table [HELP]

Item	Setting
Dynamic Routing	● Disable ○ RIPv1 ○ RIPv2

◤ **Dynamic Routing**: Routing Information Protocol (RIP) will exchange information about destinations for computing routes throughout the network. Please select RIPv2 only if you have different subnets in your network. Otherwise, please select RIPv1 if you need this protocol.

When you finished setting, click on “Save” to store your settings or click “Undo” to give up the changes.

2.2.2.16. Routing - Routing Information

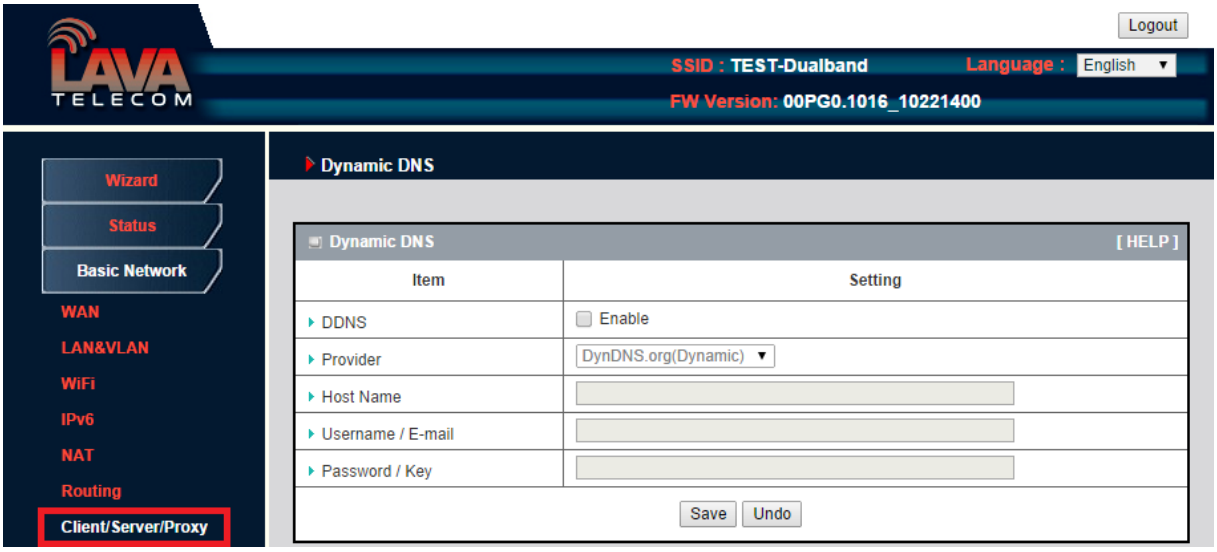
A routing table, or routing information base (RIB), is a data table stored in a router or a networked computer that lists the routes to particular network destinations, and in some cases, metrics (distances) associated with those routes. The routing table contains information about the topology of the network immediately around it.

This page displays the routing table maintained by this device. It is generated according to your network configuration.

2.2.2.17. Client/Server/Proxy - Dynamic DNS

To host your server on a changing IP address, you have to use dynamic domain name service (DDNS). Therefore, anyone wishing to reach your host only needs to know the name of it. Dynamic DNS will map the name of your host to your current IP address, which changes each time you connect your Internet service provider.

Before you enable Dynamic DNS, you need to register an account on one of these Dynamic DNS servers that we list in Provider field.



SSID : TEST-Dualband

Language : English

FW Version: 00PG0.1016_10221400

Dynamic DNS

Item	Setting
DDNS	□ Enable
Provider	DynDNS.org(Dynamic) ▼
Host Name	
Username / E-mail	
Password / Key	

- **DDNS**: Select enable if you would like to trigger this function.
- **Provider**: The DDNS provider supports service for you to bind your IP(even private IP) with a certain Domain name. You could choose your favorite provider.
- **Host Name**: Register a domain name to the DDNS provider. The fully domain name is concatenated with hostname(you specify) and a suffix(DDNS provider specifies).
- **Username/E-mail**: Input username or E-mail based on the DDNS provider you select.
- **Password/Key**: Input password or key based on the DDNS provider you select**.**

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3. Advanced Configuration

3.1. Advanced Network

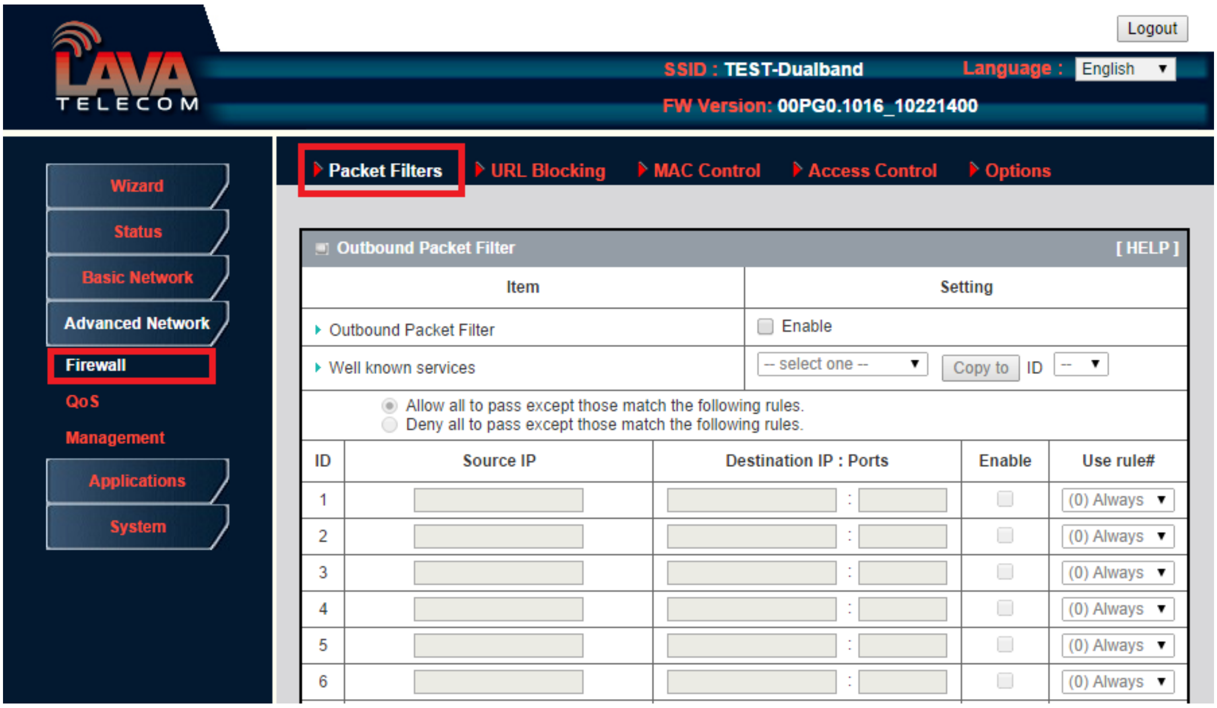
This router also supports many advanced network features, such as Firewall, QoS, Security, Redundancy, and Management. You can finish those configurations in this section.

3.1.1. Firewall - Packet Filters

The firewall functions include Packet Filters, URL Blocking, Web Content Filter, L7 Application Filter, IPS, MAC Address Control and Others

Packet Filters include both outbound filter and inbound filter. And they have the same way to setting. It enables you to control what packets are allowed to pass the router. Outbound filter applies on all outbound packets. However, inbound filter applies on packets that destined to virtual servers or DMZ host only. You can select one of the two filtering policies:

- Allow all to pass except those match the specified rules.
- Deny all to pass except those match the specified rules.



SSID : TEST-Dualband   Language : English ▼

FW Version: 00PG0.1016_10221400

Outbound Packet Filter

Item	Setting
Outbound Packet Filter	□ Enable
Well known services	-- select one -- ▼ Copy to ID -- ▼

● Allow all to pass except those match the following rules.
○ Deny all to pass except those match the following rules.

ID	Source IP	Destination IP : Ports	Enable	Use rule#
1		:	□	(0) Always ▼
2		:	□	(0) Always ▼
3		:	□	(0) Always ▼
4		:	□	(0) Always ▼
5		:	□	(0) Always ▼
6		:	□	(0) Always ▼

You can specify rules for each direction: inbound or outbound. For each rule, you can define the following:

- Source IP address or range
- Destination IP address or range
- Destination port
- Protocol: TCP or UDP or both.
- Use Rule Schedule#

For source or destination IP address, you can define a single IP address (4.3.2.1) or a range of IP addresses (4.3.2.20~30). An empty implies all IP addresses.

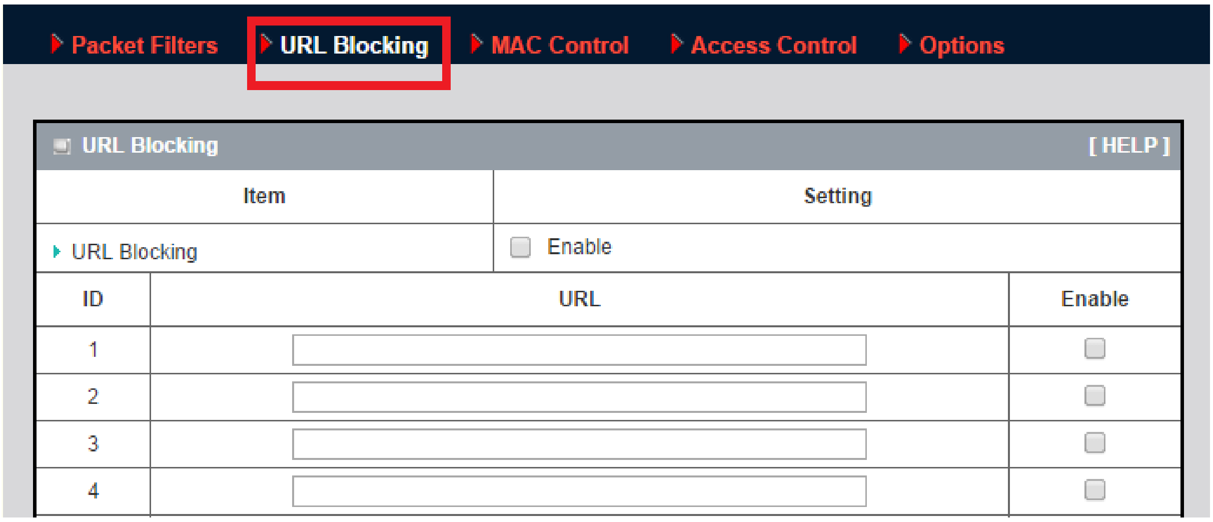
For destination port, you can define a single port (80) or a range of ports (1000-1999). Add prefix "T" or "U" to specify TCP or UDP protocol. For example, T80, U53, U2000-2999, No prefix indicates both TCP and UDP are defined. An empty implies all port addresses. Packet Filter can work with **Scheduling Rules**, and give user more flexibility on Access control. For more details, please refer to the **Scheduling Rule** section.

Each rule can be enabled or disabled individually.

Afterwards, click on "Save" to store your settings or click "Undo" to give up the changes.

3.1.2. Firewall - URL Blocking

URL Blocking will block the webs containing pre-defined key words. This feature can both filter domain input suffix (like .com or .org, etc) and a keyword "bct" or "mpe".



URL Blocking [HELP]

Item	Setting
URL Blocking	□ Enable

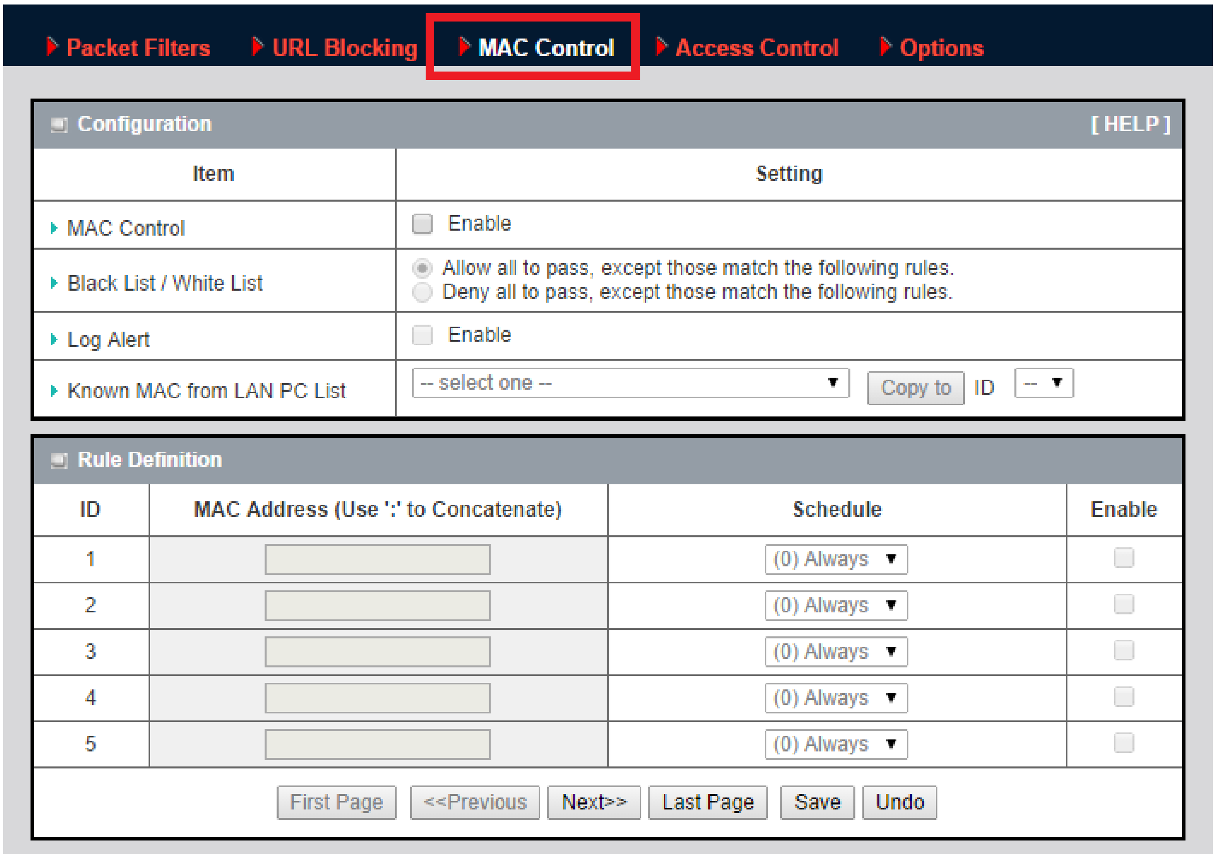
ID	URL	Enable
1		□
2		□
3		□
4		□

- **URL Blocking**: Check if you want to enable URL Blocking.
- **URL**: If any part of the Website's URL matches the pre-defined word, the connection will be blocked. You can enter up to 10 pre-defined words in a rule and each URL keyword is separated by ",", e.g., "abc, bt, org"; In addition to URL keywords, it can also block the designated domain name, like "www.xxx.com", "www.123aaa.org, mma.com".
- **Enable**: Check to enable each rule.
- **Schedule**: The rule can be turn off according to the schedule rule you specified. By default, it is always turned on when the rule is enabled.

Afterwards, click on "Save" to store your settings or click "Undo" to give up the changes.

3.1.3. Firewall - MAC Address Control

MAC Address Control allows you to assign different access right for different users and to assign a specific IP address to a certain MAC address.



Configuration

Item	Setting
MAC Control	□ Enable
Black List / White List	● Allow all to pass, except those match the following rules. ○ Deny all to pass, except those match the following rules.
Log Alert	□ Enable
Known MAC from LAN PC List	-- select one -- ▼ Copy to ID -- ▼

Rule Definition

ID	MAC Address (Use ':' to Concatenate)	Schedule	Enable
1		(0) Always ▼	□
2		(0) Always ▼	□
3		(0) Always ▼	□
4		(0) Always ▼	□
5		(0) Always ▼	□

◤ **MAC Address Control**: Check “Enable” to enable the “MAC Address Control”. All of the settings in this page will take effect only when “Enable” is checked.

◤ **Connection control**: Check "Connection control" to enable the control of which wired and wireless clients can connect to this device. If a client is denied to connect to this device, it means the client can't access to the Internet consequently. Choose "allow" or "deny" to allow or deny the clients, whose MAC addresses are not in the "Control table", to connect to this device.

◤ **Association control**: Check "Association control" to enable the control of which wireless client can associate to the wireless LAN. If a client is denied to associate to the wireless LAN, it means the client can't send or receive any data via this device. Choose "allow" or "deny" to allow or deny the clients, whose MAC addresses are not in the "Control table", to associate to the wireless LAN.

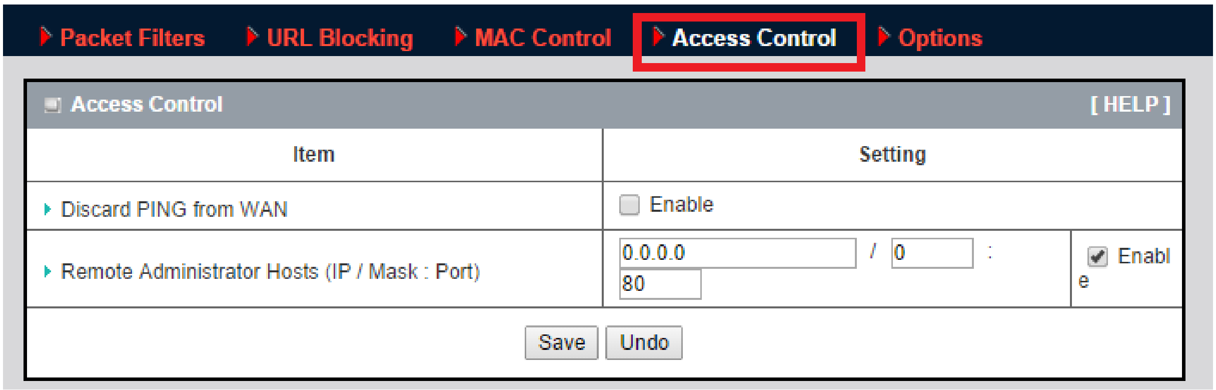
Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.1.4.Firewall – Access Control

◤ **Remote Administrator Host/Port**: In general, only local clients (LAN users) can browse the device’s built-in web pages for device administration setting. This feature enables you to perform administration task from a certain remote host. If this feature is enabled, only the specified IP address can perform remote administration. If the specified IP address is 0.0.0.0, any host can connect with this product to perform administration task. You can use subnet mask bits "/nn" notation to specified a group of trusted IP addresses for example, "10.1.2.0/24".

NOTE: When Remote Administration is enabled, the web server port will be shifted to 80. You can change web server port to other port, too.

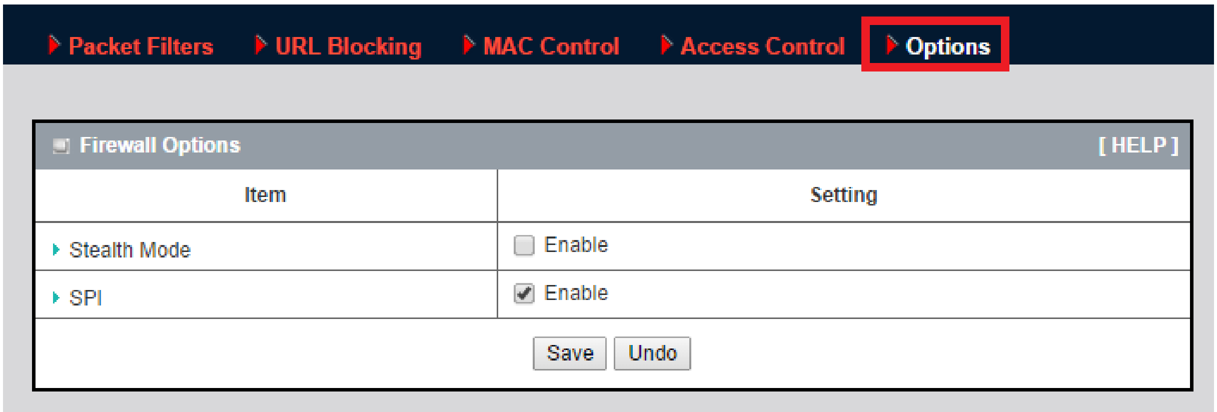
- **Discard PING from WAN side**: When this feature is enabled, any host on the WAN side cannot ping this product.



Access Control

Item	Setting
Discard PING from WAN	□ Enable
Remote Administrator Hosts (IP / Mask : Port)	0.0.0.0 / 0 : 80 ☑ Enable

3.1.5. Firewall – Options



Firewall Options

Item	Setting
Stealth Mode	□ Enable
SPI	☑ Enable

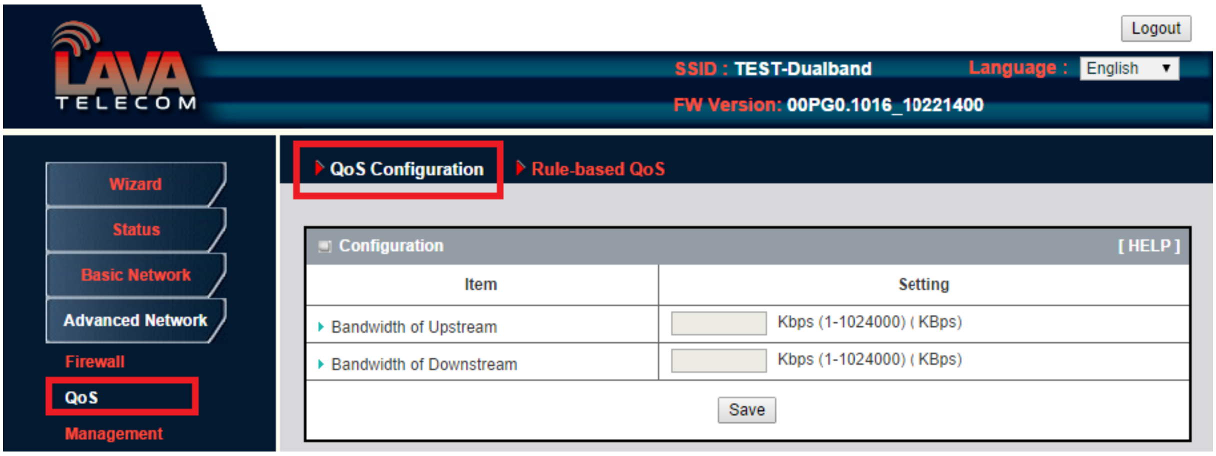
- **SPI**: SPI ("stateful packet inspection" also known as "dynamic packet filtering") helps to prevent cyber attacks by tracking more state per session. It validates that the traffic passing through that session conforms to the protocol
- **Stealth mode**: If enabled, the router will not respond to port scans from the WAN, thus making it less susceptible to discovery and attacks.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.1.6. QoS(Quality of Service) (Optional)

The main goal of QoS (Quality of Service) is prioritizing incoming data, and preventing data loss due to factors such as jitter, delay and dropping. Another important aspect of QoS is ensuring that prioritizing one data flow doesn’t interfere with other data flows.

QoS helps to prioritize data as it enters your router. By attaching special identification marks or headers to incoming packets, QoS determines which queue the packets enter, based on priority. This is useful when there are certain types of data you want to give higher priority to, such as voice packets given higher priority than Web data packets.



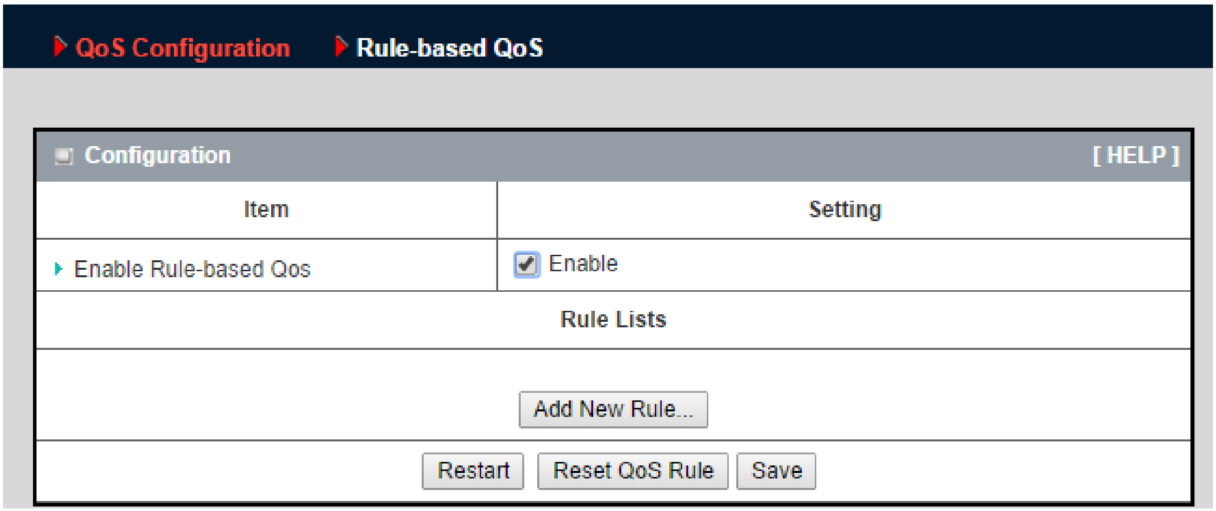
SSID : TEST-Dualband Language : English

FW Version: 00PG0.1016_10221400

Configuration [HELP]

Item	Setting
Bandwidth of Upstream	Kbps (1-1024000) (KBps)
Bandwidth of Downstream	Kbps (1-1024000) (KBps)

Rule-based QoS



Configuration [HELP]

Item	Setting
Enable Rule-based Qos	☑ Enable

Rule Lists

◤ **QoS**: You can enable/disable this QoS function.

◤ **Bandwidth of Upstream / Bandwidth of Downstream**: You can input the value of maximum upstream and downstream bandwidth from your ISP

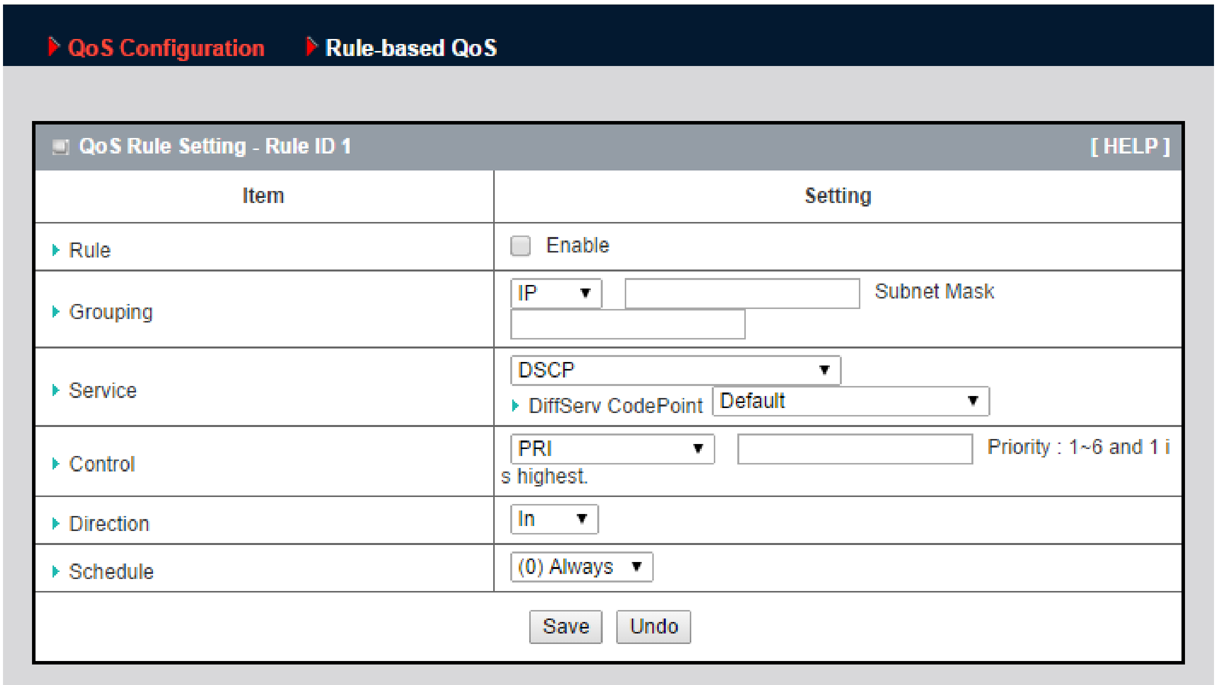
◤ **Flexible Bandwidth Management (FBM)**: When this management is enabled, system will share the bandwidth to normal applications

◤ **Guest Setting / Bandwidth Policy**: This device can allocate a designated internet bandwidth for the forth LAN port (Port4). If you want to enable this function, check the “Enable” checkbox and enter the allowed bandwidth.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

Create a QoS Rule:

You can click on the button “Add New Rule” shown in the icon above to create a new QoS rule.



QoS Configuration Rule-based QoS

QoS Rule Setting - Rule ID 1 [HELP]

Item	Setting
Rule	□ Enable
Grouping	IP ▾ Subnet Mask
Service	DSCP ▾ DiffServ CodePoint Default ▾
Control	PRI ▾ Priority : 1~6 and 1 is highest.
Direction	In ▾
Schedule	(0) Always ▾

◤ **Rule**: Enable the rule setting first.

◤ **Grouping**: Select the QoS grouping class from the drop list, and specify the grouping information accordingly.

Grouping	Description
IP	IP address based
MAC	MAC based

◤ **Service**: Set your own “Service” type to enable the QoS rule as below.

Service	Description
DSCP	DiffServ Code Point
Service Port	Mean TCP or UDP Port
Pre-defined Application profiles	Normal service Application
Connection Sessions	NAT Session

◤ **Control**: Set the corresponding control type for the selected service type.

Control	Description	Data
DSCP Marking	Priority as you select DiffServ CodePoint	CS1 ~ AF
PRI	Priority	1~6(1 is highest Priority)
MAXR	Maximum bandwidth Rate	KBps/MBps
MINR	Minimum bandwidth Rate	KBps/MBps
SESSION	Connection session	Number (1~20000)

- **Direction**: Select the traffic direction to be applied for this QoS rule.

Direction	
IN	In-bond
OUT	Out-bond
BOTH	In-bond & Out-bond

- **Schedule**: The QoS rule can be turn off according to the schedule you specified. By default, it is always turned on when the rule is enabled.

Afterwards, click on "Save" to store your settings or click "Undo" to give up the changes.

Example for adding a "DSCP" type QoS rule:

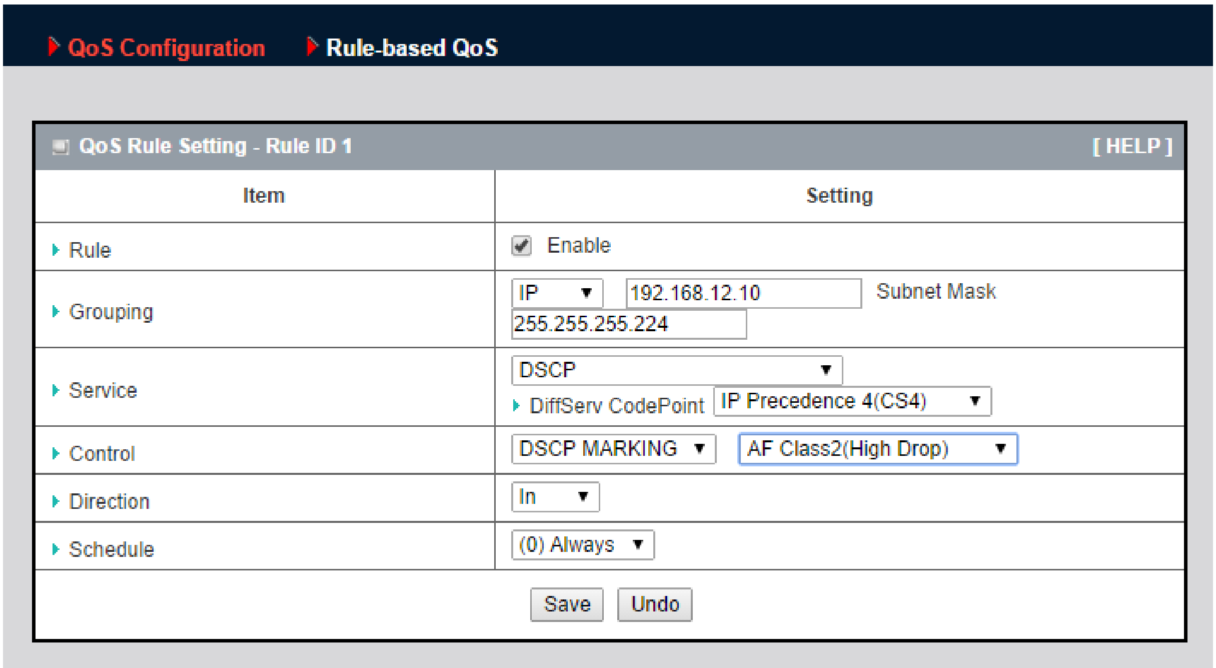
Grouping: Select "IP" and entry IP Range.

Service: Select "DSCP" and "Source Network Packets" which DiffServ are set as CS4.

Control: Select "DSCP Marking" and mark these Packets as "AF Class 2".

Direction: Select "IN" for In-bound traffic only.

Schedule: Leave the default value of "(0)Always" as it is.



QoS Configuration ▸ Rule-based QoS

QoS Rule Setting - Rule ID 1 [HELP]

Item	Setting
Rule	☑ Enable
Grouping	IP ▾ 192.168.12.10 Subnet Mask 255.255.255.224
Service	DSCP ▾ DiffServ CodePoint IP Precedence 4(CS4) ▾
Control	DSCP MARKING ▾ AF Class2(High Drop) ▾
Direction	In ▾
Schedule	(0) Always ▾

This Rule means IP Packets from WAN or other interfaces with DiffServ value of CS4 will be modified with DSCP Marking of "AF Class 2", then forward corresponding packets to the Clients whose IP address is in the range of 192.168.12.10~40.

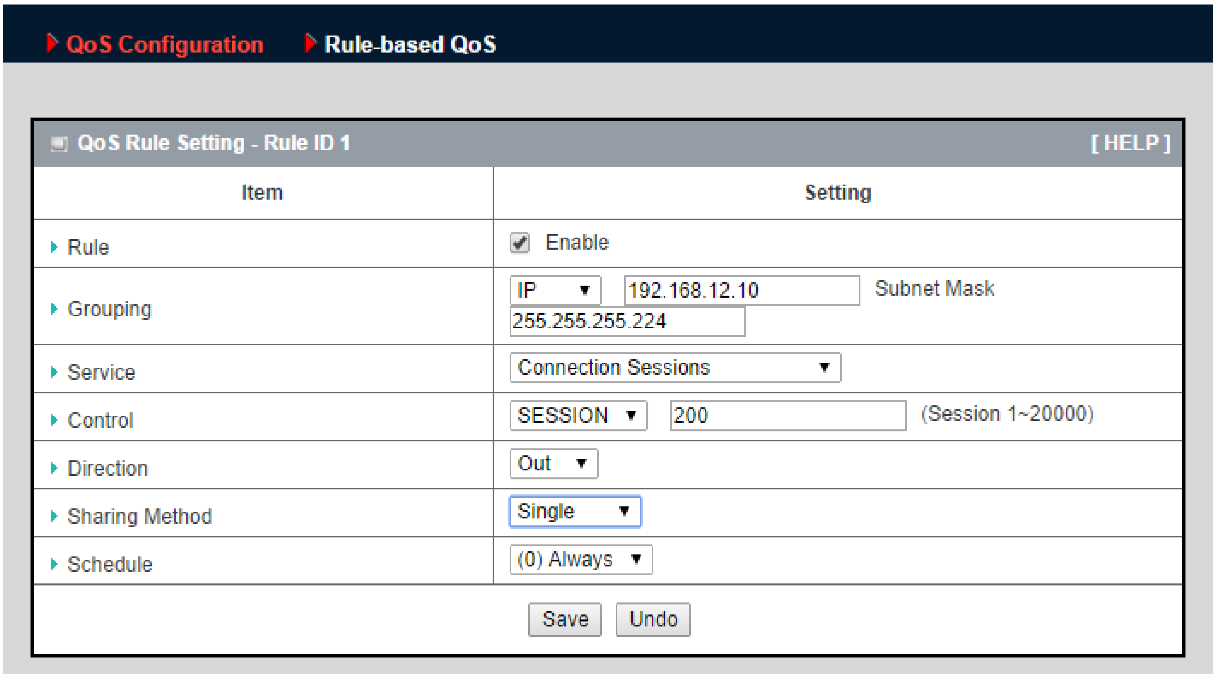
Example for adding a "Connection Sessions" type QoS rule:

Control: Set NAT session number as 200.

Direction: Select "Out" for Out-bound traffic only. It is for the client devices under the Gateway to establish session with servers on the Internet.

Sharing Method: Select “Single” or “Grouping” from the drop list. In this case, “Single” is selected.

Schedule: leave the default value of “(0)Always” as it is.



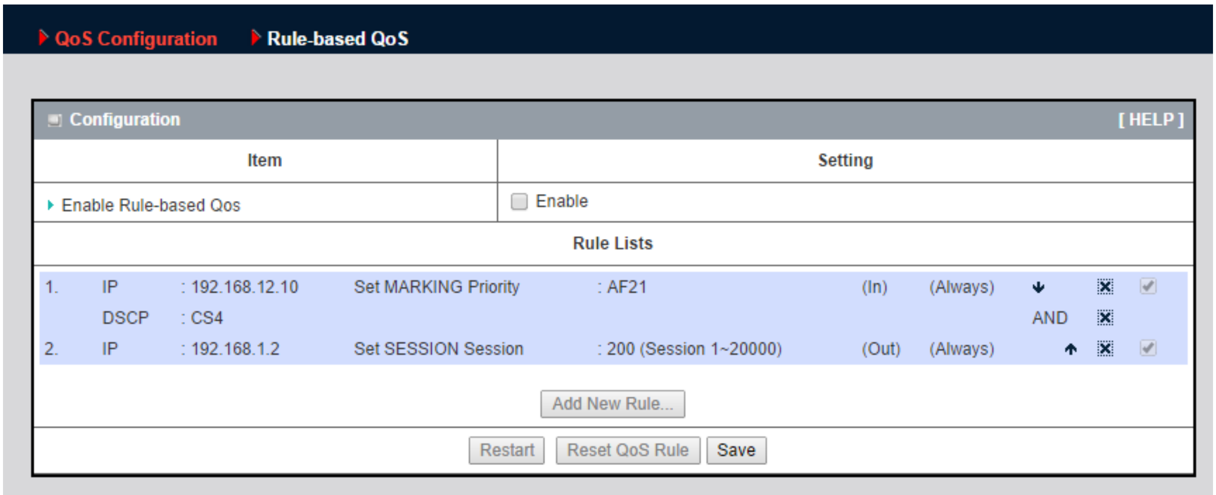
QoS Rule Setting - Rule ID 1

Item	Setting
Rule	☑ Enable
Grouping	IP ▼ 192.168.12.10 Subnet Mask 255.255.255.224
Service	Connection Sessions ▼
Control	SESSION ▼ 200 (Session 1~20000)
Direction	Out ▼
Sharing Method	Single ▼
Schedule	(0) Always ▼

This Rule defines that each single user, whose IP address is in the range of 192.168.12.10~40, can access to a remote server on the Internet, and keep a maximum 200 sessions at the same time.

Finishing QoS settings:

Once you saved the QoS rule, it will be displayed in the Rule List area as below.



Configuration

Item	Setting
Enable Rule-based Qos	☐ Enable

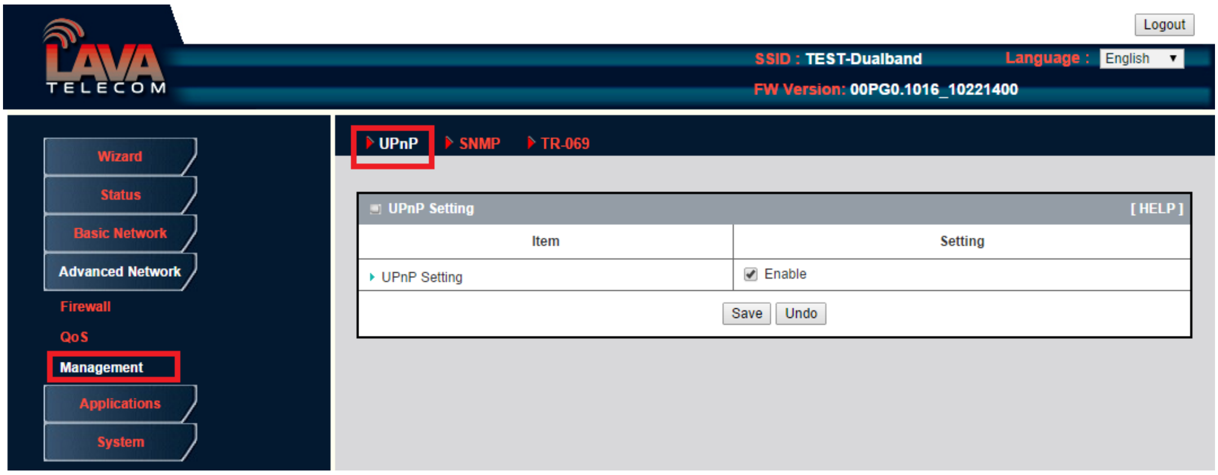
Rule Lists

1.	IP	: 192.168.12.10	Set MARKING Priority	: AF21	(In)	(Always)	↓	☒	☑
	DSCP	: CS4					AND	☒	
2.	IP	: 192.168.1.2	Set SESSION Session	: 200 (Session 1~20000)	(Out)	(Always)	↑	☒	☑

Besides, you can move up or down the priority of all rules by clicking on the ‘↑’or ’↓’ icon if you want to change the priority of rules. You can also unmark any rule in the list if you don’t want to enable it.

3.1.7. Management - UPnP

UPnP Internet Gateway Device (IGD) Standardized Device Control Protocol is a NAT port mapping protocol and is supported by some NAT routers. It is a common communication protocol of automatically configuring port forwarding. Applications using peer-to-peer networks, multiplayer gaming, and remote assistance programs need a way to communicate through home and business gateways. Without IGD one has to manually configure the gateway to allow traffic through, a process which is error prone and time consuming



SSID : TEST-Dualband Language : English
FW Version: 00PG0.1016_10221400

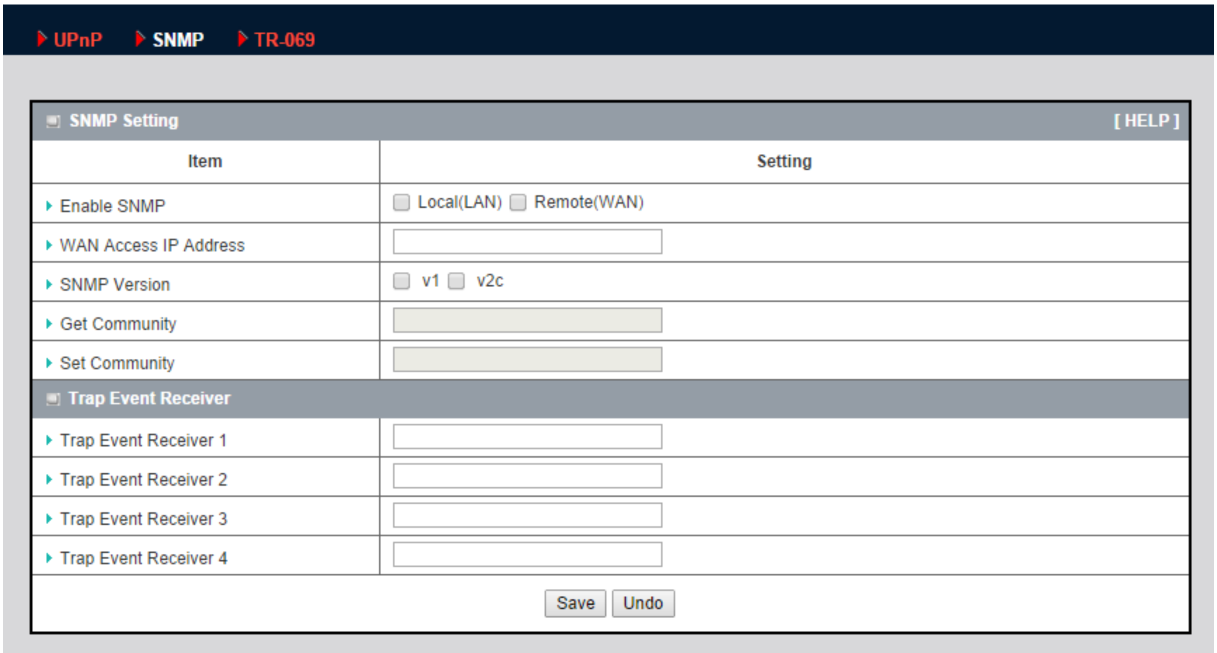
UPnP Setting [HELP]

Item	Setting
UPnP Setting	☑ Enable

This device supports the UPnP Internet Gateway Device (IGD) feature. By default, it is enabled.

3.1.8. Management - SNMP

In brief, SNMP, the Simple Network Management Protocol, is a protocol designed to give a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.



SNMP Setting [HELP]

Item	Setting
Enable SNMP	□ Local(LAN) □ Remote(WAN)
WAN Access IP Address	
SNMP Version	□ v1 □ v2c
Get Community	
Set Community	
Trap Event Receiver	
Trap Event Receiver 1	
Trap Event Receiver 2	
Trap Event Receiver 3	
Trap Event Receiver 4	

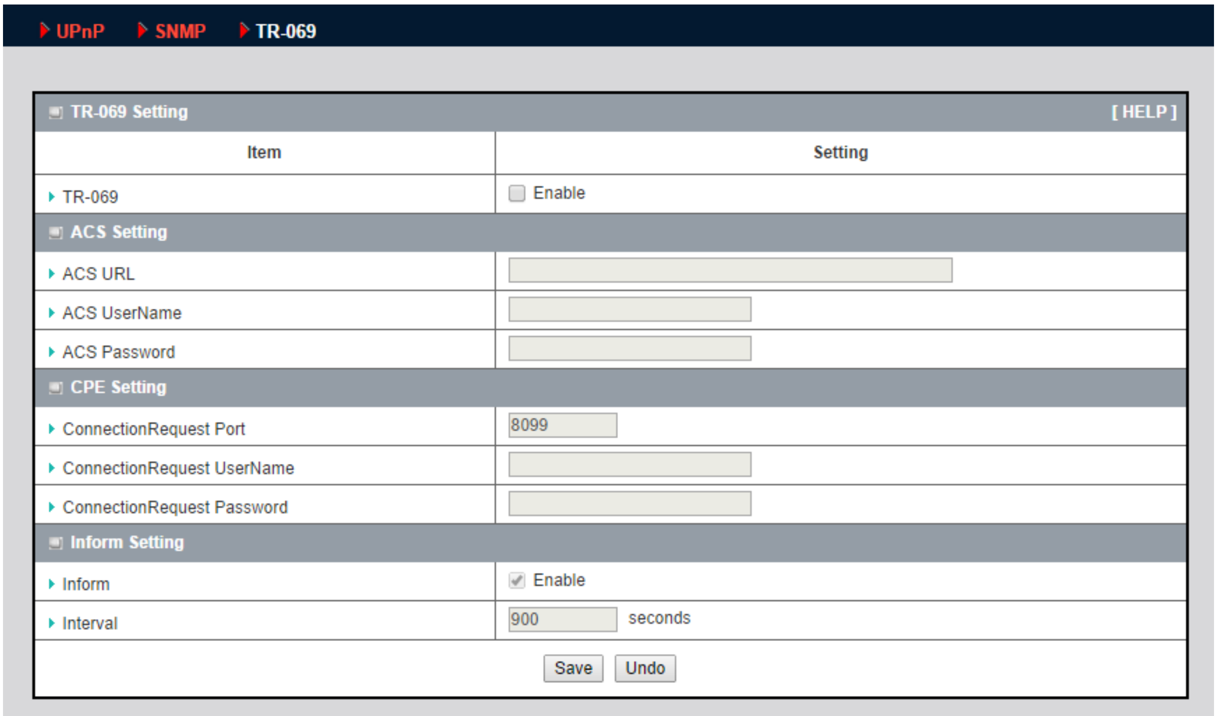
- **Enable SNMP**: You can check “Local”, “Remote” or both to enable SNMP function. If “Local” is checked, this device will respond to the request from LAN. If “Remote” is checked, this device will respond to be request from WAN.
- **WAN Access IP Address**: If you want to limit the remote SNMP access to specific computer, please enter the PC`s IP address. The default value is 0.0.0.0, and it means that any internet connected computer can get some information of the device with SNMP protocol.
- **SNMP Version**: Supports SNMP V1, V2c, and V3.
- **Get Community**: The community of GetRequest that this device will respond. This is a text password mechanism that is used to weakly authenticate queries to agents of managed network devices.
- **Set Community**: The community of SetRequest that this device will accept.
- **SNMPv3 Settings**: User 1/2: This device supports up to two SNMP management accounts. You can specify the account permission as “Read” or “Read/Write” respectively**.**
- **User 1/2 AUTH Mode**: Select MD5 or SHA as the method of password encryption for the specified level of access, or to disable authentication.
- **User 1/2 Privacy Mode**: You can configure the SNMP privacy mode. There are three modes for you to choose: “noAuthNoPriv” for both authentication and private key are not required, “authNoPriv” for no private key required, and “authPriv” for both authentication and private key required.
- **Username 1/2**: Use this field to identify the user name for the specified level of access.
- **Password 1/2**: Use this field to set the password for the specified level of access.
- **User 1/2 Priv Key**: Use this field to define the encryption key for the specified level of access.
- **Trap Event Receiver 1 ~ 4**: Enter the IP addresses or Domain Name of your SNMP Management PCs. You have to specify the IP address, so that the device can send SNMP Trap message to the management PCs consequently.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.1.9. Management - TR069

- **TR-069**: Disable or enable the TR-069 settings.
- **ACS setting**: you may add ACS URL/ Username/ Password.
- **CPE setting**: you may add CPE connection request port/ username /password.
- **Inform setting**: you may enable/disable the interval of informing CPE.
- **Interval** : you may input seconds for every interval.

Note: TR-069 is a customized feature for ISP, please contact with us once you get any problem to configure.

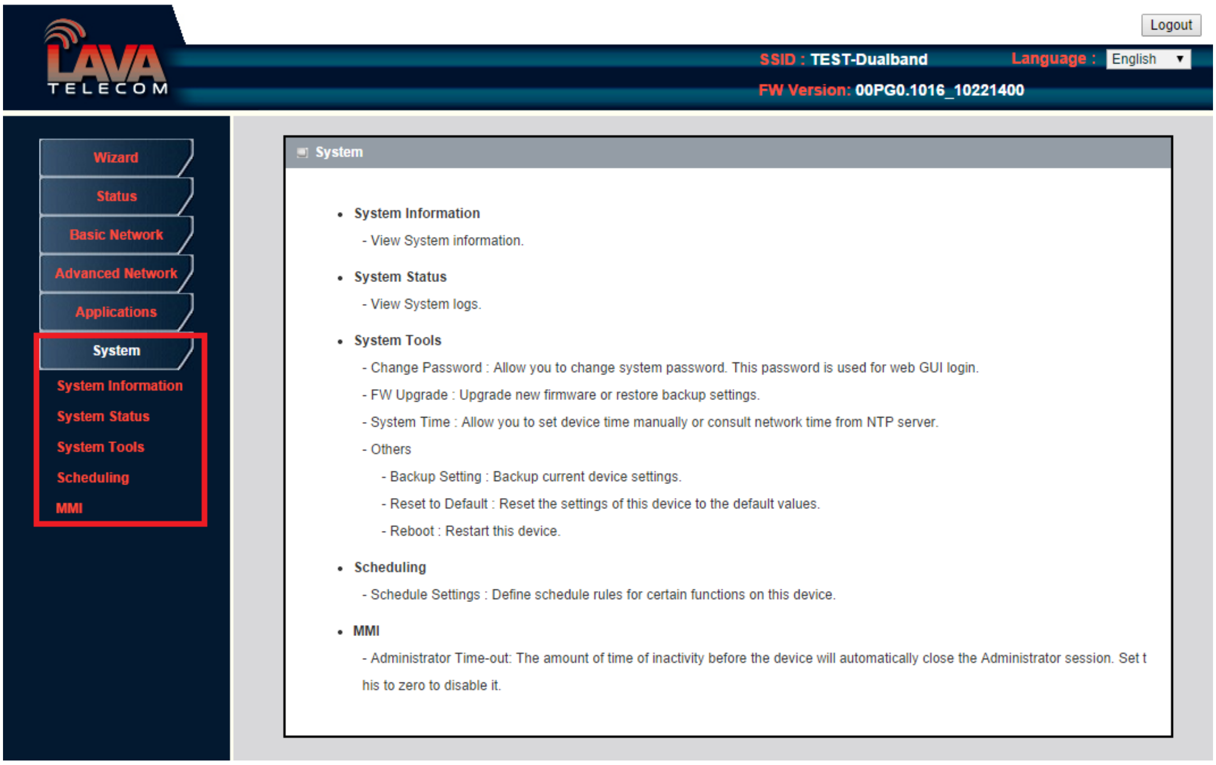


TR-069 Setting

Item	Setting
TR-069	□ Enable
ACS Setting	
ACS URL	
ACS UserName	
ACS Password	
CPE Setting	
ConnectionRequest Port	8099
ConnectionRequest UserName	
ConnectionRequest Password	
Inform Setting	
Inform	☑ Enable
Interval	900 seconds

3.2. System

In this section you can see system information, system logs, use system tools for system update and do service scheduling and system administration setting.



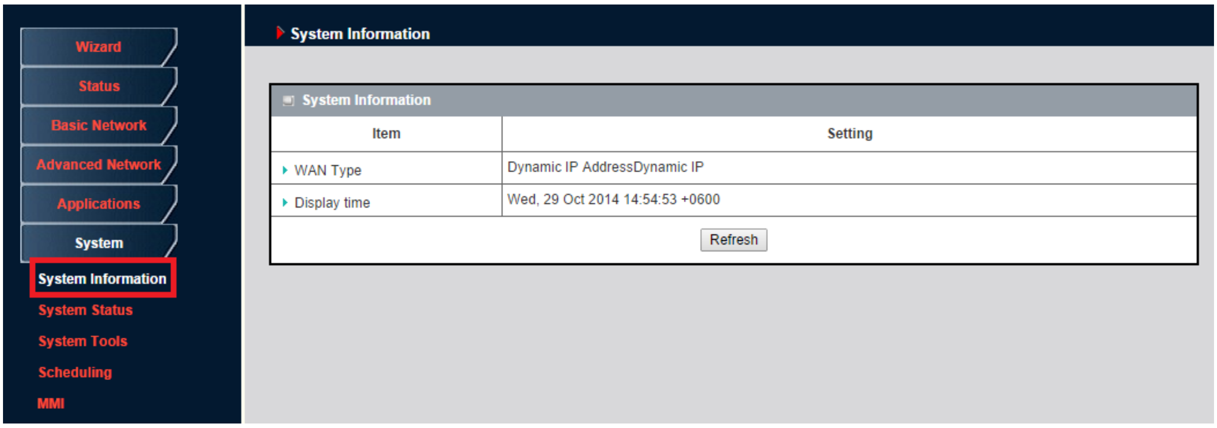
SSID : TEST-Dualband
Language : English
FW Version: 00PG0.1016_10221400

System

- **System Information**
  - View System information.
- **System Status**
  - View System logs.
- **System Tools**
  - Change Password : Allow you to change system password. This password is used for web GUI login.
  - FW Upgrade : Upgrade new firmware or restore backup settings.
  - System Time : Allow you to set device time manually or consult network time from NTP server.
  - Others
    - Backup Setting : Backup current device settings.
    - Reset to Default : Reset the settings of this device to the default values.
    - Reboot : Restart this device.
- **Scheduling**
  - Schedule Settings : Define schedule rules for certain functions on this device.
- **MMI**
  - Administrator Time-out: The amount of time of inactivity before the device will automatically close the Administrator session. Set t his to zero to disable it.

3.2.1. System Information

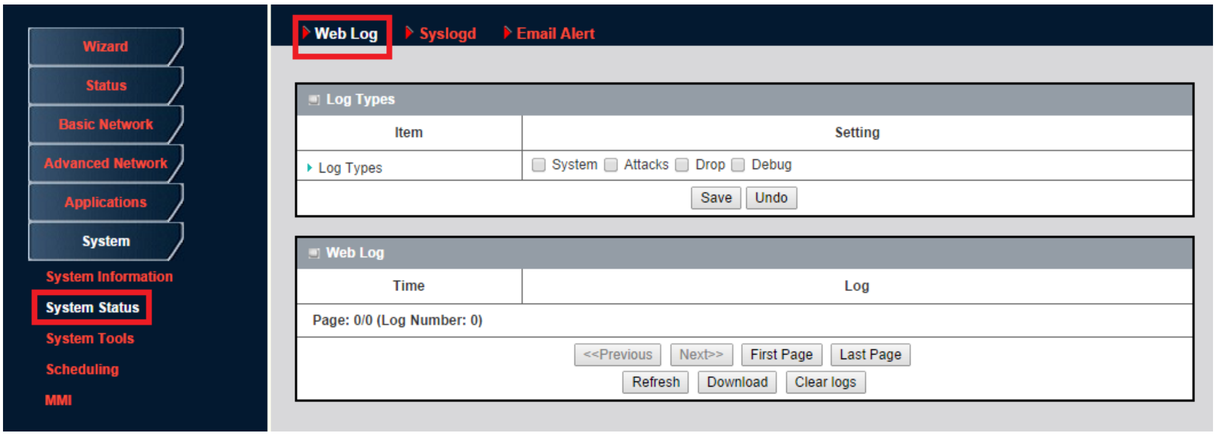
You can view the System Information in this page.



System Information

Item	Setting
WAN Type	Dynamic IP AddressDynamic IP
Display time	Wed, 29 Oct 2014 14:54:53 +0600

3.2.2. System status - Web Log



Log Types

Item	Setting
Log Types	□ System □ Attacks □ Drop □ Debug

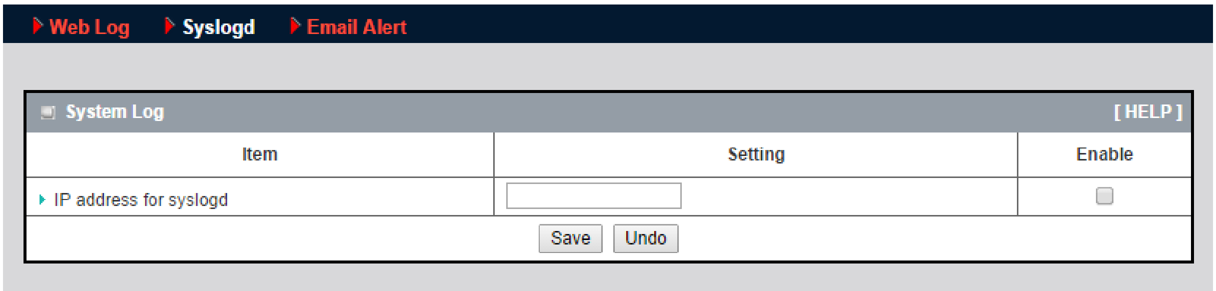
Web Log

Time	Log
Page: 0/0 (Log Number: 0)	

◤ **Log Types**: You can select the log types to be collected in the web log area. There are “System”, “Attacks”, “Drop”, and “Debug” types for you to select.

◤ **Web Log**: You can browse, refresh, download, and clear the log messages.

3.2.3. System status - Syslog



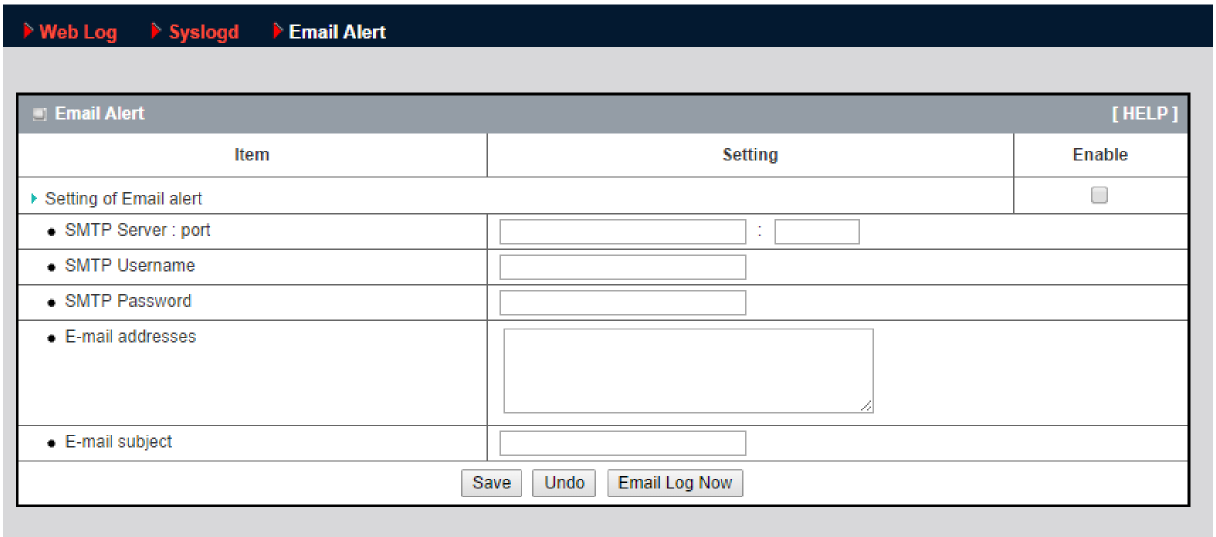
System Log

Item	Setting	Enable
IP address for syslogd		□

This device can also export system logs to specific destination by means of syslog (UDP) and SMTP(TCP). With enabled Syslog function, this device will send log to a certain host periodically. You need to install a syslog utility on a host to receive syslogs.

IP Address for syslogd: Host IP of destination where syslog will be sent to. Check Enable to enable this function.

3.2.4. System status - Email Alert



Email Alert [HELP]

Item	Setting	Enable
Setting of Email alert		□
● SMTP Server : port	:	
● SMTP Username		
● SMTP Password		
● E-mail addresses		
● E-mail subject		

This device can also export system logs via sending emails to specific recipients. The items you have to setup include:

- **Setting of Email alert**: Check if you want to enable Email alert (send syslog via email).
- **SMTP Server**: Port: Input the SMTP server IP and port, which are connected with ':'. If you do not specify port number, the default value is 25.

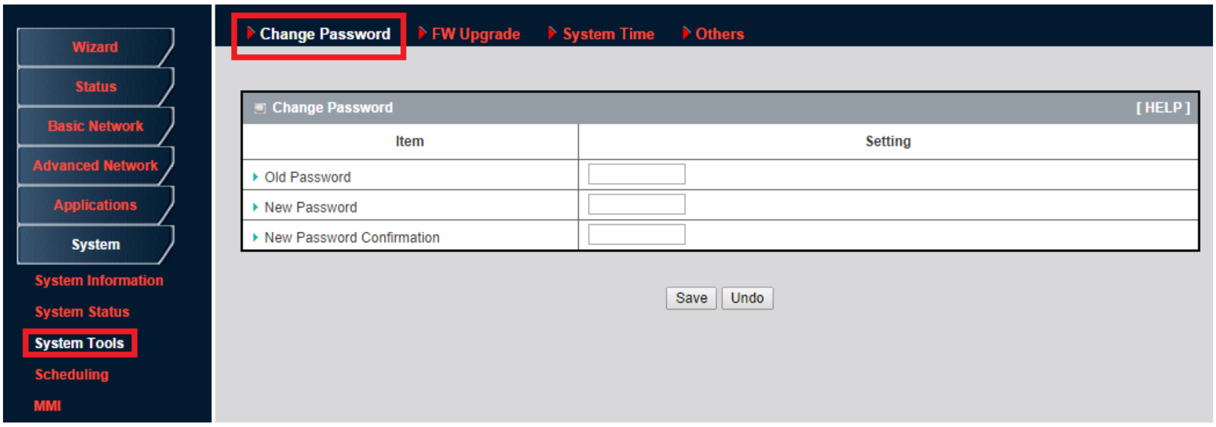
For example, "mail.your_url.com" or "192.168.1.100:26".

- **SMTP Username**: Enter the Username offered by your ISP.
- **SMTP Password**: Enter the password offered by your ISP.
- **E-mail Addresses**: The recipients are the ones who will receive these logs. You can assign more than 1 recipient, using ';' or ',' to separate these email addresses.
- **E-mail Subject**: The subject of email alert is optional.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.2.5. System Tools - Change Password

You can change the System Password here. We strongly recommend you to change the system password for security reason. Click on “Save” to store your settings or click “Undo” to give up the changes.



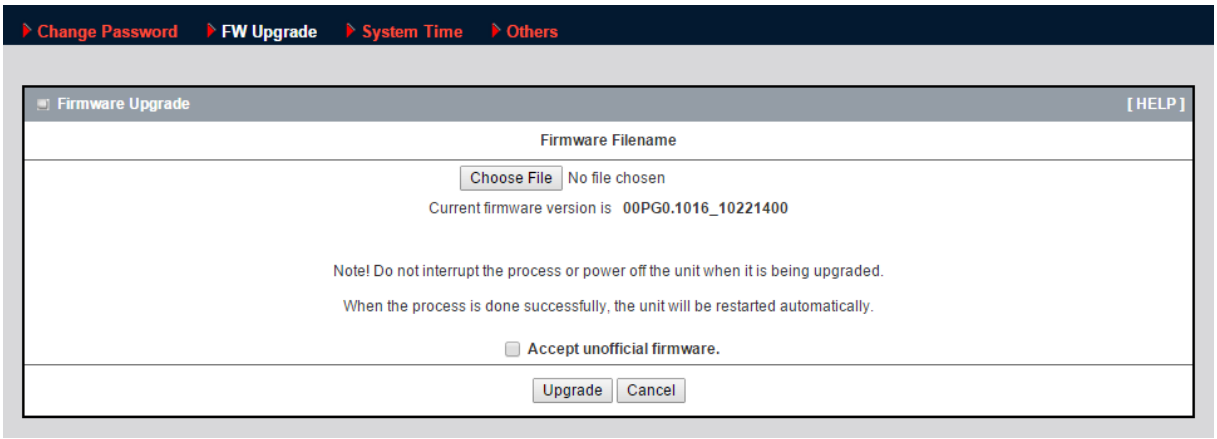
Change Password [HELP]

Item	Setting
Old Password	
New Password	
New Password Confirmation	

Save Undo

3.2.6. System Tools - FW Upgrade

If new firmware is available, you can upgrade router firmware through the WEB GUI here.



Firmware Upgrade [HELP]

Firmware Filename

Choose File No file chosen

Current firmware version is 00PG0.1016_10221400

Note! Do not interrupt the process or power off the unit when it is being upgraded.

When the process is done successfully, the unit will be restarted automatically.

□ Accept unofficial firmware.

Upgrade Cancel

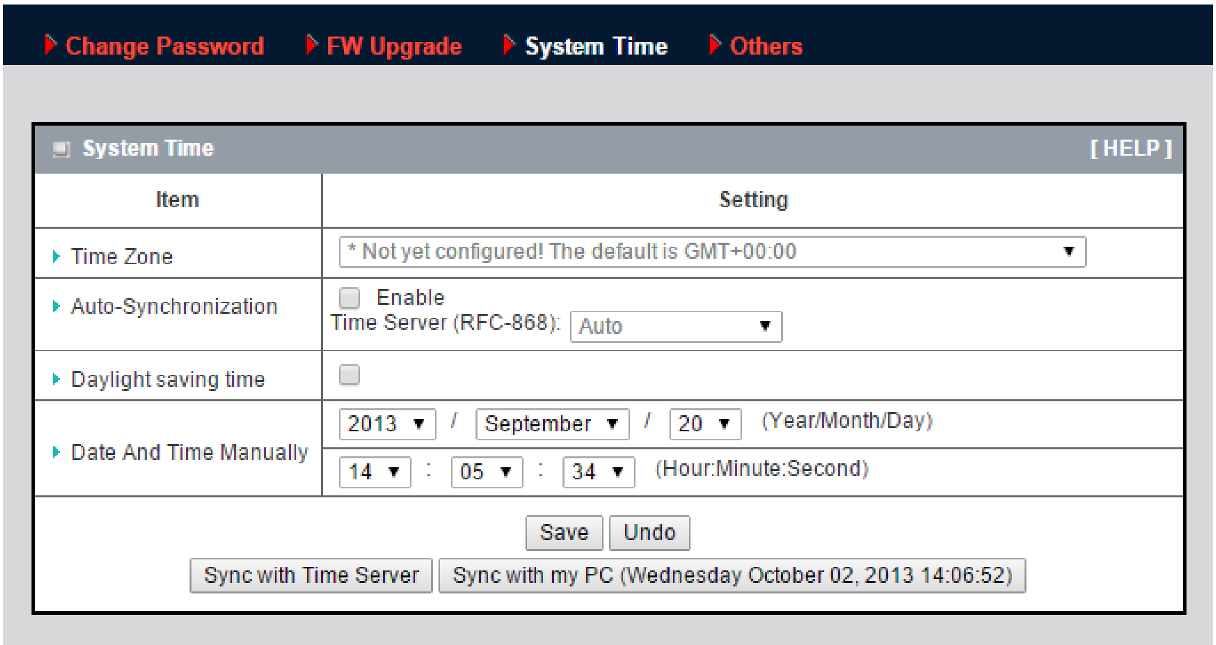
Press “browse” button to indicate the file name of new firmware, and then press Upgrade button to start to upgrade new firmware on this device. If you want to upgrade a firmware which is from GPL policy, please check “Accept unofficial firmware”.

NOTE. PLEASE DO NOT TURN THE DEVICE OFF WHEN UPGRADE IS PROCEEDING.

3.2.7. System Tools - System Time

If new firmware is available, you can upgrade router firmware through the WEB GUI here.

- **Time Zone**: Select a time zone where this device locates.
- **Auto-Synchronization**: Check the “Enable” checkbox to enable this function. Besides, you can select a NTP time server to consult UTC time.
- **Sync with Time Server**: Click on the button if you want to set Date and Time by NTP Protocol.
- **Sync with my PC**: Click on the button if you want to set Date and Time using the PC’s Date and Time.



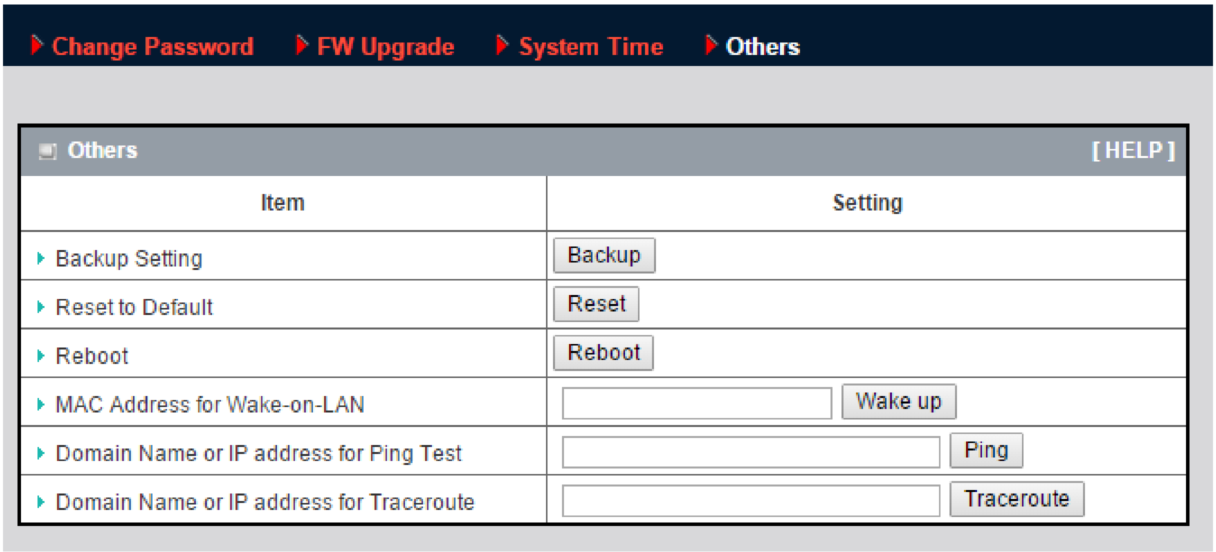
System Time [HELP]

Item	Setting
Time Zone	* Not yet configured! The default is GMT+00:00 ▼
Auto-Synchronization	□ Enable Time Server (RFC-868): Auto ▼
Daylight saving time	□
Date And Time Manually	2013 ▼ / September ▼ / 20 ▼ (Year/Month/Day) 14 ▼ : 05 ▼ : 34 ▼ (Hour:Minute:Second)

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.2.8. System Tools - Others

In this section you can do system backup, reset to default, system reboot settings and ping test.



Others [HELP]

Item	Setting
Backup Setting	Backup
Reset to Default	Reset
Reboot	Reboot
MAC Address for Wake-on-LAN	Wake up
Domain Name or IP address for Ping Test	Ping
Domain Name or IP address for Traceroute	Traceroute

◤ **Backup Setting**: You can backup your settings by clicking the “Backup” button and save it as a bin file. Once you want to restore these settings, please click Firmware Upgrade button and use the bin file you saved.

◤ **Reset to Default**: You can also reset this device to factory default settings by clicking the “Reset“ button.

◤ **Reboot**: You can also reboot this device by clicking the “Reboot“ button.

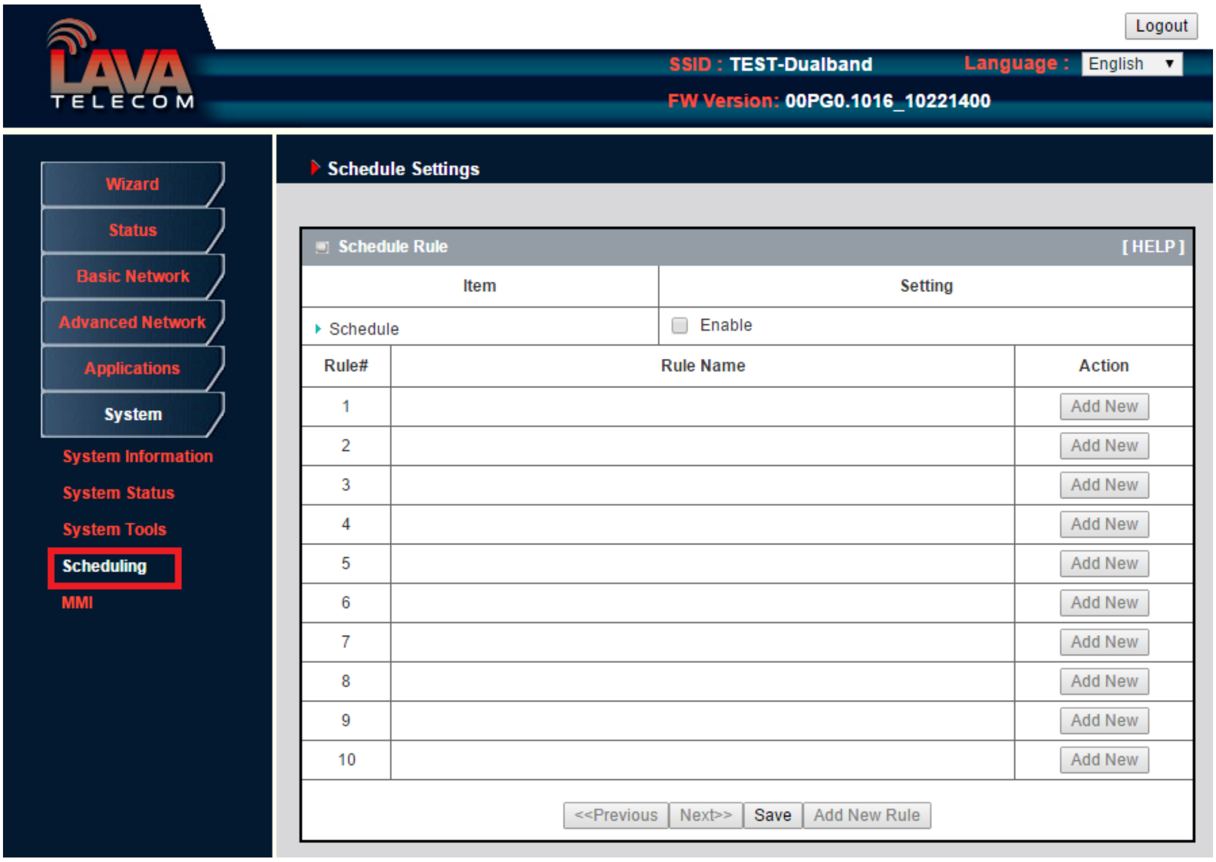
◤ **MAC Address for Wake-on-LAN**: Wake-on-LAN (WOL) is an Ethernet networking standard that allows a computer to be turned on or awakened by a network message. You can enter the MAC address of the computer, in your LAN network, to be remotely turned on.

◤ **Domain Name or IP address for Ping Test**: This allows you to configure an IP, and ping the device. You can ping a specific IP to test whether it is alive.

◤ **Domain Name or IP address for Traceroute**: Traceroute is a network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an IP network. Traceroute proceeds unless all (three) sent packets are lost more than twice, then the connection is lost and the route cannot be evaluated. Ping, on the other hand, only computes the final round-trip times from the destination point

3.2.9. Scheduling

You can set the schedule time to decide which service will be turned on or off. The added rules will be listed.



Schedule Rule [HELP]

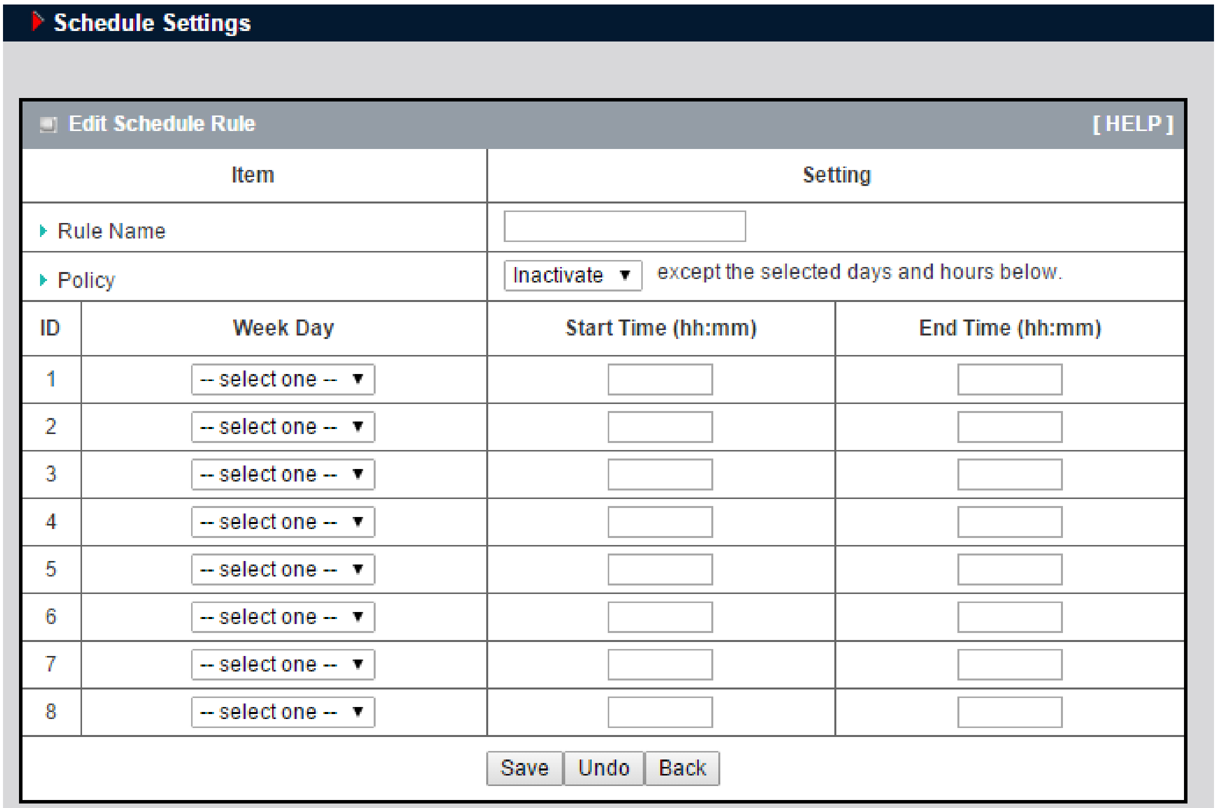
Item	Setting
Schedule	□ Enable

Rule#	Rule Name	Action
1		Add New
2		Add New
3		Add New
4		Add New
5		Add New
6		Add New
7		Add New
8		Add New
9		Add New
10		Add New

Add New Rule:

To create a schedule rule, click the “**Add New**” button or the “**Add New Rule**…” button at the bottom. When the next dialog popped out you can edit the Name of Rule, **Policy**, and set the schedule time (Week day, Start Time, and End Time).

Afterwards, click “save” to store your settings or click “Undo” to give up the changes.



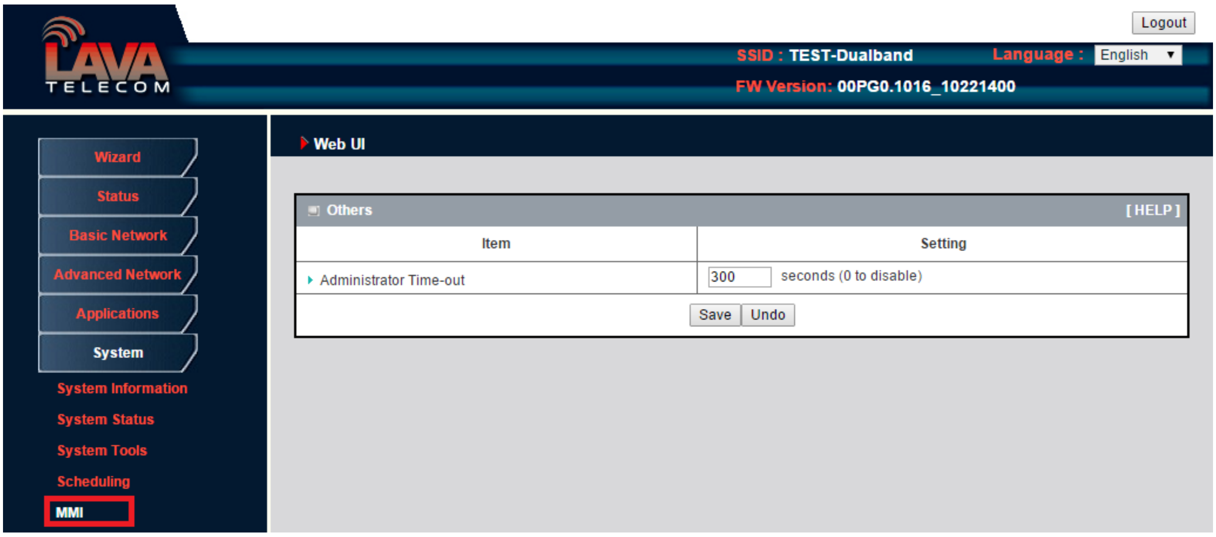
Schedule Settings

Edit Schedule Rule [HELP]

Item	Setting
Rule Name	
Policy	Inactivate ▼ except the selected days and hours below.

ID	Week Day	Start Time (hh:mm)	End Time (hh:mm)
1	-- select one -- ▼		
2	-- select one -- ▼		
3	-- select one -- ▼		
4	-- select one -- ▼		
5	-- select one -- ▼		
6	-- select one -- ▼		
7	-- select one -- ▼		
8	-- select one -- ▼		

3.2.10. MMI - Web UI



SSID : TEST-Dualband

Language : English ▼

FW Version: 00PG0.1016_10221400

Web UI

Others [HELP]

Item	Setting
Administrator Time-out	300 seconds (0 to disable)

You can set UI administration time-out duration give remote administration host port in this page. When the host port is given please remember to check the enable box and save your settings.

4. Troubleshooting

This Chapter provides solutions to problems for the installation and operation of the WiFi Broadband Router. You can refer to the following if you are having problems.

4.1. Why can’t I configure the router even the cable is plugged and the LED is lit?

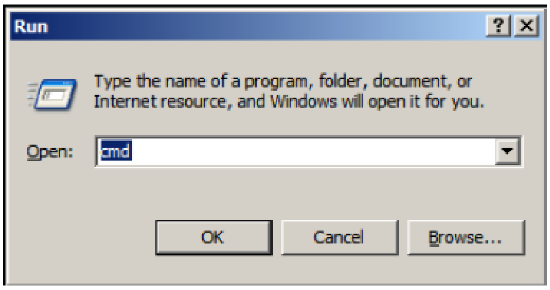
Do a Ping test to make sure that the WiFi

Note: It is recommended that you use an

Broadband Router is responding.

Go **to Start > Run.**

- Type **cmd.**

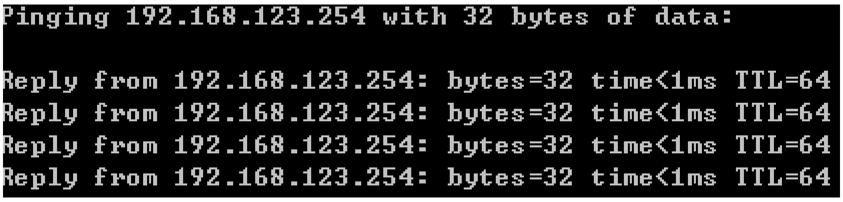


Run

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

Open: cmd

- Press **OK.**
- Type **ipconfig** to get the IP of default gateway**.**
- Type “**ping 192.168.123.254**”. Assure that you ping the correct IP Address assigned to the WiFi Broadband Router. It will show four replies if you ping correctly**.**



```
Pinging 192.168.123.254 with 32 bytes of data:

Reply from 192.168.123.254: bytes=32 time<1ms TTL=64
Reply from 192.168.123.254: bytes=32 time<1ms TTL=64
Reply from 192.168.123.254: bytes=32 time<1ms TTL=64
Reply from 192.168.123.254: bytes=32 time<1ms TTL=64
```

Ensure that your Ethernet Adapter is working, and that all network drivers are installed properly. Network adapter names will vary depending on your specific adapter. The installation steps listed below are applicable for all network adapters.

- Go to **Start > Right click on “My Computer” > Properties**.
- Select the **Hardware Tab**.
- Click **Device Manager**.
- Double-click on “**Network Adapters**”.

◤ Right-click on **Wireless Card bus Adapter** or your specific network adapter.

◤ Select **Properties** to ensure that all drivers are installed properly.

◤ Look under **Device Status** to see if the device is working properly.

◤ Click “**OK**”.

4.2. What can I do if my Ethernet connection does not work properly?

◤ Make sure the RJ45 cable connects with the router.

◤ Ensure that the setting on your Network Interface Card adapter is “Enabled”.

◤ If settings are correct, ensure that you are not using a crossover Ethernet cable, not all Network Interface Cards are MDI/MDIX compatible, and use a patch cable is recommended.

◤ If the connection still doesn’t work properly, then you can reset it to default.

4.3. Something wrong with the wireless connection?

4.3.1. Can’t setup a wireless connection?

◤ Ensure that the SSID and the encryption settings are exactly the same to the Clients.

◤ Move the WiFi Broadband Router and the wireless client into the same room, and then test the wireless connection.

◤ Disable all security settings such as **WEP**, and **MAC Address Control**.

◤ Turn off the WiFi Broadband Router and the client, then restart it and then turn on the client again.

◤ Ensure that the LEDs are indicating normally. If not, make sure that the power and Ethernet cables are firmly connected.

◤ Ensure that the IP Address, subnet mask, gateway and DNS settings are correctly entered for the network.

◤ If you are using other wireless device, home security systems or ceiling fans, lights in your home, your wireless connection may degrade dramatically. Keep your product away from electrical devices that generate RF noise such as microwaves, monitors, electric motors…

4.3.2. What can I do if my wireless client can not access the Internet?

◤ Out of range: Put the router closer to your client.

◤ Wrong SSID or Encryption Key: Check the SSID or Encryption setting.

◤ Connect with wrong AP: Ensure that the client is connected with the correct Access Point.

- Right-click on the **Local Area Connection** icon in the taskbar.
- Select **View Available Wireless Networks** in **Wireless Configure**. Ensure you have selected the correct available network.

  - Reset the WiFi Broadband Router to default setting

4.3.3. Why does my wireless connection keep dropping?

- Antenna Orientation.
  - Try different antenna orientations for the WiFi Broadband Router.
  - Try to keep the antenna at least 6 inches away from the wall or other objects.
- Try changing the channel on the WiFi Broadband Router, and your Access Point and Wireless adapter to a different channel to avoid interference.
- Keep your product away from electrical devices that generate RF noise, like microwaves, monitors, electric motors, etc.

4.4. What to do if I forgot my encryption key?

- Go back to advanced setting to set up your Encryption key again.
- Reset the WiFi Broadband Router to default setting

4.5. How to reset to default?

- Ensure the WiFi Broadband Router is powered on
- Find the **Reset** button on the right side
- Press the **Reset** button for 8 seconds and then release.
- After the WiFi Broadband Router reboots, it has back to the factory default settings.

5. Appendix A. Spec Summary Table

Device Interface		LR-25G001
Wireless WAN	USB 2.0 for external 3G/LTE modem	1
Ethernet WAN	RJ-45 port, 10/100/1000Mbps	1
Ethernet WAN/LAN	RJ-45 port, 10/100/1000Mbps	4
Antenna	2pcs x 3dBi 2.4GHz Detachable external antenna 1pcs x 5GHz internal antenna	3
WPS and Reset Button	WPS connection, Reset router setting to factory default	2
LED Indication	Status / WAN / LAN1 ~ LAN4/ WiFi2.4G / Wi-Fi 5G	●
Power Jack	DC Power Jack, powered via external DC 12V/1.5A switching power adapter	1
Wireless LAN (WiFi)		
Standard	IEEE 802.11ac, 11b/g/n compliance	●
SSID	SSID broadcast or in stealth mode	●
Channel	Auto-selection, manually	●
Security	WEP, WPA, WPA2, WPA-PSK, WPA2-PSK	●
WPS	WPS (Wi-Fi Protected Setup)	●
WMM	WMM (Wi-Fi Multimedia)	●
Functionality		
Ethernet WAN	PPPoE, DHCP client, Static IP	●
WAN Connection	Auto-reconnect, dial-on-demand, manually	●
One-to-Many NAT	Virtual server, special application, DMZ, IGMP v1v2 v3 pass-through	●
NAT Session	Support NAT session	20000
SPI Firewall	IP/Service filter, URL blocking, MAC control	●
DoS Protection	DoS (Deny of Service) detection and protection	●
Management	SNMP, UPnP IGD, syslog, Auto Backup Setting	●
Administration	Web-based UI, remote login, backup/restore setting	●
Environment & Certification		
Package Information	Device dimension (mm)	SP08
	Package dimension (mm)	TBD
	Package weight (g)	TBD
Operation Temp.	Temp.: 0~40oC, Humidity 10%~90% non-condensing	●
Storage Temp.	Temp.: -10~70oC, Humidity: 0~95% non-condensing	●
EMI Certification	CE/FCC compliance	●
RoHS	RoHS compliance	●

6. Appendix B. Licensing information

This product includes copyrighted third-party software licensed under the terms of the GNU General Public License. Please refer to the GNU General Public License below to check the detailed terms of this license.

The following parts of this product are subject to the GNU GPL, and those software packages are copyright by their respective authors.

Linux Kernel	GPLv2	Linux-2.6.21
busybox	GPLv2	busybox_1.3.2
bridge-utils	GPLv2	bridge-utils 1.1
udhcp server	GPLv2	udhcp-0.9.9
udhcp client		
fdisk	GPLv2	util-linux 2.12q
mke2fs, e2fsck	GPLv2	e2fsprogs v1.40.2
samba	GNUv2	samba 3.0.20
wireless tools	GPLv2	wireless tools
vsfptd	GPLv2	vsftpd-2.0.3
Transmission	MIT	Transmission-1.74
mt-daapd	GNUv2	mt-daapd-0.2.4
dnrd	GNUv2	DNRD-2.17
libcurl	cURL-7.19.6	
OpenSSL	BSD	openssl-1.00b3
ntfs-3g	GNUv2	ntfs-3g-2009.4.4
Zebra	GNUv2	zebra-0.95a
snmpd	CMU	snmp-4.1.2
pptp	GNUv2	pptp-1.7.1
pppoe	GPLv2	pppoe-3.8
pppd	BSD	ppp-2.4
l2tpd	GPLv2	l2tp-0.4
iptables	GNUv2	iptables-1.4.2
tc	GNUv2	iproute2-2.6.11
wget	GNUwget-1.7.1	

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Preamble

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

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

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

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

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

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

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

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

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

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

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

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

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

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

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

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

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

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

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

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

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

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

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

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

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.
7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

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

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

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

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

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

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

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

NO WARRANTY

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

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

END OF TERMS AND CONDITIONS