TP-LINK®

User Guide

TD-W8960N

300Mbps Wireless N ADSL2+ Modem Router



Rev: 4.0.0 1910010506

COPYRIGHT & TRADEMARKS

Specifications are subject to change without notice. **TP-LINK**[°] is a registered trademark of TP-LINK TECHNOLOGIES CO., LTD. Other brands and product names are trademarks or registered trademarks of their respective holders.

No part of the specifications may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from TP-LINK TECHNOLOGIES CO., LTD. Copyright © 2011 TP-LINK TECHNOLOGIES CO., LTD. All rights reserved.

http://www.tp-link.com

FCC STATEMENT

FC

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

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

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

- 1) This device may not cause harmful interference.
- 2) This device must accept any interference received, including interference that may cause undesired operation.

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

Note: The manufacturer is not responsible for any radio or tv interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate the equipment.

FCC RF Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

"To comply with FCC RF exposure compliance requirements, this grant is applicable to only Mobile Configurations. The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter."

CE Mark Warning

€€1588①

This is a class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

National Restrictions

This device is intended for home and office use in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

Country	Restriction	Reason/remark
Bulgaria	None	General authorization required for outdoor use and public service
France	Outdoor use limited to 10 mW e.i.r.p. within the band 2454-2483.5 MHz	Military Radiolocation use. Refarming of the 2.4 GHz band has been ongoing in recent years to allow current relaxed regulation. Full implementation planned 2012
Italy	None	If used outside of own premises, general authorization is required
Luxembourg	None	General authorization required for network and service supply(not for spectrum)
Norway	Implemented	This subsection does not apply for the geographical area within a radius of 20 km from the centre of Ny-Ålesund
Russian Federation	None	Only for indoor applications

Note: Please don't use the product outdoors in France.

This device has been designed to operate with the antennas listed below, and having a maximum gain of 3 dBi. Antennas not included in this list or having a gain greater than 3 dBi are strictly prohibited for use with this device. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that permitted for successful communication.

DECLARATION OF CONFORMITY

For the following equipment:

Product Description: 300Mbps Wireless N ADSL2+ Modem Router

Model No.: TD-W8960N

Trademark: **TP-LINK**

We declare under our own responsibility that the above products satisfy all the technical regulations applicable to the product within the scope of Council Directives:

Directives 1999/5/EC

The above product is in conformity with the following standards or other normative documents

ETSI EN 300 328 V1.7.1: 2006

ETSI EN 301 489-1 V1.8.1:2008& ETSI EN 301 489-17 V2.1.1:2009

EN 61000-3-2:2006+A1:2009+A2:2009

EN 61000-3-3:2008

EN60950-1:2006+A11:2009

Recommendation 1999/519/EC

EN62311:2008

Directives 2004/108/EC

The above product is in conformity with the following standards or other normative documents

EN 55022:2006 +A1:2007

EN 55024:1998+A1:2001+A2:2003

EN 61000-3-2:2006+A1:2009+A2:2009

EN 61000-3-3:2008

Directives 2006/95/EC

The above product is in conformity with the following standards or other normative documents

EN60950-1:2006+A11:2009

Person is responsible for marking this declaration:

Yang Hongliang

Product Manager of International Business

Pad	ckage	Contents	1
Ch	apter	1. Product Overview	2
1.1	Overv	view of the Router	2
1.2	Main	Features	3
1.3	Panel	Layout	4
	1.3.1	The Front Panel	. 4
	1.3.2	The Back Panel	. 5
Ch	apter	2. Connecting the Router	6
2.1	Syste	m Requirements	6
2.2	Install	ation Environment Requirements	6
2.3	Conne	ecting the Router	6
Ch	apter	3. Quick Installation Guide	8
	-	guring the PC	
		Installation Guide	
Ch	ontor	4. Configuring the Router1	6
	-	4. Configuring the Router	
	-		
		e Info1	
		Setup1	
4.4		nced Setup	
		Layer2 Interface	
	4.4.3	LAN	
	4.4.4	MAC Clone	
	4.4.5	NAT	-
	4.4.6	Security	40
	4.4.7	Parental Control	45
	4.4.8	Quality of Service	48
	4.4.9	Traffic Control	51
	4.4.10	Routing	54
	4.4.11	DNS	57
	4.4.12	DSL	59

CONTENTS

	4.4.13	UPnP	60
	4.4.14	Interface Grouping	61
	4.4.15	LAN Ports	63
	4.4.16	IPSec	63
4.5	Wirel	ess	67
	4.5.1	Basic	
	4.5.2	Security	
	4.5.3	MAC Filter	85
	4.5.4	Wireless Bridge	
	4.5.5	Advanced	
	4.5.6	Station info	89
4.6	Diagn	nostics	
4.7	Mana	gement	
	4.7.1	Settings	
	4.7.2	System Log	
	4.7.3	SNMP Agent	
	4.7.4	TR-069 client	
	4.7.5	Access Control	
	4.7.6	Update Firmware	
	4.7.7	Reboot	
Ар	pendi	x A: FAQ	100
Ap	pendi	x B: Configuring the PC	103
Ар	Appendix C: Specifications110		
Ар	Appendix D: Glossary111		
Ар	Appendix E: Technical Support115		

Package Contents

The following contents should be found in your package:

- > One TD-W8960N 300Mbps Wireless N ADSL2+ Modem Router
- > One power Adapter for TD-W8960N 300Mbps Wireless N ADSL2+ Modem Router
- Quick Installation Guide
- > One RJ45 cable
- Two RJ11 cables
- > One ADSL splitter
- > One Resource CD for TD-W8960N 300Mbps Wireless N ADSL2+ Modem Router, including:
 - This User Guide
 - Other Helpful Information

Note:

Make sure that the package contains the above items. If any of the listed items are damaged or missing, please contact your distributor.

Chapter 1. Product Overview

Thank you for choosing the TD-W8960N 300Mbps Wireless N ADSL2+ Modem Router.

1.1 Overview of the Router

The TD-W8960N 300Mbps Wireless N ADSL2+ Modem Router integrates 4-port Switch, Firewall, NAT-Router and Wireless AP. Powered by 2x2 MIMO technology, the Wireless N Router delivers exceptional range and speed, which can fully meet the need of Small Office/Home Office (SOHO) networks and the users demanding higher networking performance.

The TD-W8960N 300Mbps Wireless N ADSL2+ Modem Router utilizes integrated ADSL2+ transceiver and high speed MIPS CPU. The Router supports full-rate ADSL2+ connectivity conforming to the ITU and ANSI specifications.

In addition to the basic DMT physical layer functions, the ADSL2+ PHY supports dual latency ADSL2+ framing (fast and interleaved) and the I.432 ATM Physical Layer.

Incredible Speed

The router provides up to 300Mbps wireless connection with other 802.11n wireless clients. The incredible speed makes it ideal for handling multiple data streams at the same time, which ensures your network stable and smooth. The performance of this 802.11n wireless Router will give you the unexpected networking experience at speed 650% faster than 802.11g. It is also compatible with all IEEE 802.11g and IEEE 802.11b products.

Multiple Security Protections

With multiple protection measures, including SSID broadcast control and wireless LAN 64/128 WEP encryption, Wi-Fi protected Access (WPA2-PSK, WPA-PSK), as well as advanced Firewall protections, the TD-W8960N 300Mbps Wireless N ADSL2+ Modem Router provides complete data privacy.

Flexible Access Control

The Router provides flexible access control, so that parents or network administrators can establish restricted access policies for children or staff. It also supports Virtual Server and DMZ host for Port Triggering, and then the network administrators can manage and monitor the network in real time with the remote management function.

Simple Installation

Since the Router is compatible with virtually all the major operating systems, it is very easy to manage. Quick Setup Wizard is supported and detailed instructions are provided step by step in this user guide. Before installing the Router, please look through this guide to know all the Router's functions.

1.2 Main Features

- Complies with IEEE 802.11n to provide a wireless data rate of up to 300Mbps
- One RJ11 LINE port, four 10/100M Auto-Negotiation RJ45 LAN ports, supporting Auto MDI/MDIX
- > Quick response semi-conductive surge protect circuit, reliable surge-protect function
- > AFE to support Annex A and L deployments
- Provides external splitter
- > Multi-user sharing a high-speed Internet connection
- > Connecting the internet on demand and disconnecting from the Internet when idle for PPPoE
- > Provides WPA/WPA2, WPA-PSK/WPA2-PSK data security, TKIP/AES encryption security
- > Provides 64/128-bit WEP encryption security and wireless LAN ACL (Access Control List)
- Adopts Advanced DMT modulation and demodulation technology
- Adopts 300M wireless LAN transmission technology
- Supports access control, parents and network administrators can establish restricted access policies based on time of day for children or staff
- Supports Virtual Server, Port Triggering and DMZ host
- Supports UPnP, Dynamic DNS, Static Routing
- Supports bridge mode and Router function
- Supports Web management
- Supports firmware upgrade
- Supports Flow Statistics
- Supports QSS (Quick Secure Setup)
- > Built-in firewall supporting IP address filtering, MAC address filtering and parental control
- Built-in DHCP server

1.3 Panel Layout

1.3.1 The Front Panel

The Router's LEDs are located on the front panel.

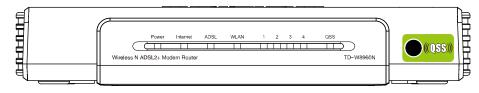


Figure 1-1

The Router's LEDs and the QSS button are located on the front panel (View from left to right).

LED Explanation:

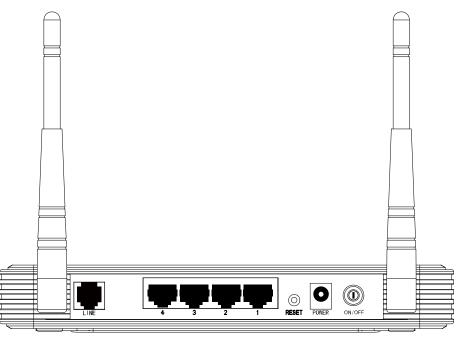
Name	Status	Indication	
	On	The modem router is powered on.	
Power	Off	The modem router is off. Please ensure that the power adapter is connected correctly.	
	On	The network is available with a successful Internet connection.	
Internet	Flash	There is data being transmitted or received via the Internet.	
	Off	There is no successful Internet connection or the modem router is operating in Bridge mode. Please refer to <u>Note 2</u> for troubleshooting.	
	On	ADSL line is synchronized and ready to use.	
ADSL	Flash	The ADSL negotiation is in progress.	
	Off	ADSL synchronization fails. Please refer to Note 1 for troubleshooting.	
	On	Wireless is enabled but no data is being transmitted.	
WLAN	Flash	The modem router is sending or receiving data over the wireless network.	
	Off	Wireless function is disabled.	
	On	There is a device connected to this LAN port.	
LAN 1,2,3,4	Flash	The modem router is sending or receiving data over this LAN port.	
	Off	There is no device connected to this LAN port.	
QSS	On	A wireless device has been successfully added to the network by QSS function.	
	Flash	QSS handshaking is in process and will continue for about 2 minutes. Please press the QSS button on other wireless devices that you want to add to the network while the LED is flashing.	
	Off	The QSS function is disabled or the wireless device fails to be added to the network in 2 minutes after QSS function is enabled. Please refer to $4.5.2.1$ QSS (WPS) Setup for more information.	

Note:

- If the ADSL LED is off, please check your Internet connection first. Refer to <u>2.3 Connecting</u> the Router for more information about how to make Internet connection correctly. If you have already made a right connection, please contact your ISP to make sure if your Internet service is available now.
- If the Internet LED is off, please check your ADSL LED first. If your ADSL LED is also off, please refer to Note 1. If your ADSL LED is GREEN ON, please check your Internet configuration. You may need to check this part of information with your ISP and make sure everything have been input correctly. Refer to <u>4.2 Device Info</u> for more information.

1.3.2 The Back Panel

The Router's ports, where the cables are connected, and RESET button are located on the back panel.





- > LINE: Connect to the Modem Port of Splitter or to the telephone line.
- > 1, 2, 3, 4 (LAN): The ports (1, 2, 3, 4) connect the Router to the local PC(s).
- > **RESET:** There are two ways to reset the Router's factory defaults.
- 1) Use the **Restore Default** function on **Management** -> **settings** -> **Restore Default** page in the router's Web-based Utility.
- 2) Use the Factory Default **RESET** button: With the Router powered on, use a pin to press and hold the **RESET** button for at least 5 seconds. And the Router will reboot to its factory default settings.
- > **POWER:** The Power plug is where you will connect the power adapter.
- > **ON/OFF:** The switch for the power.
- > Wireless Antennas: To receive and transmit the wireless data.

Chapter 2. Connecting the Router

2.1 System Requirements

- > Broadband Internet Access Service (DSL/Cable/Ethernet).
- > PCs with a working Ethernet Adapter and an Ethernet cable with RJ45 connectors.
- > TCP/IP protocol on each PC.
- > Web browser, such as Microsoft Internet Explorer, Mozilla Firefox or Apple Safari.

2.2 Installation Environment Requirements

- > Place the Router in a well ventilated place far from any heater or heating vent
- > Avoid direct irradiation of any strong light (such as sunlight)
- > Keep at least 2 inches (5 cm) of clear space around the Router
- ➢ Operating temperature: 0℃~40℃ (32°F~104°F)
- > Operating Humidity: 10% ~ 90% RH (non-condensing)

2.3 Connecting the Router

Back to LED Explanation

Before installing the Router, please make sure your broadband service provided by your ISP is available. If there is any problem, please contact your ISP. After that, please install the Router according to the following steps. Don't forget to pull out the power plug and keep your hands dry.

- 1. Locate an optimum location for the Router. The best place is usually at the center of your wireless network.
- 2. Adjust the direction of the antenna. Normally, upright is a good direction.
- 3. Connect your PC and Switch/Hub in your LAN to the LAN Ports of the Router. (If you have a wireless NIC and want to have wireless connection, please skip this step.)
- 4. Connect the telephone line to the Line port on the Router. Or you can access the Internet and make calls at the same time by using a separate splitter to divide the data and voice. The external splitter has three ports:
 - LINE: Connect to the wall jack
 - PHONE: Connect to the phone sets
 - MODEM: Connect to the ADSL LINE port of device

Plug one end of the twisted-pair ADSL cable into the ADSL LINE port on the rear panel of device. Connect the other end to the MODEM port of the external splitter.

- 5. Connect the power adapter to the power plug of the Router, and the other end into an electrical outlet. The electrical outlet shall be installed near the device and shall be easily accessible.
- 6. Turn on the ON/OFF switch to power the device. It will start to work automatically.

TD-W8960N 300Mbps Wireless N ADSL2+ Modem Router User Guide

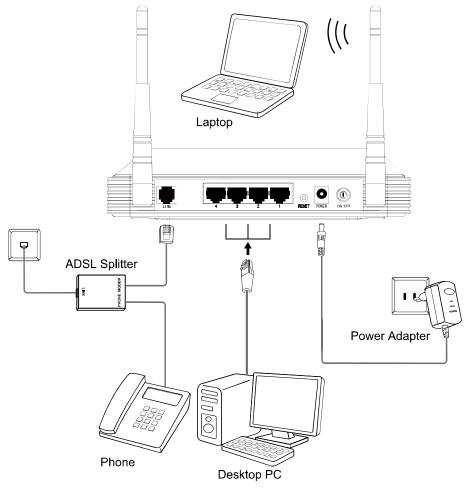


Figure 2-1

Chapter 3. Quick Installation Guide

This chapter will show you how to configure the basic functions of your **TD-W8960N 300Mbps Wireless N ADSL2+ Modem Router** using **Quick Setup Wizard** within minutes.

3.1 Configuring the PC

After you directly connect your PC to the **TD-W8960N** or connect your adapter to a Hub/Switch which has connected to the Router, you need to configure your PC's IP address. Follow the steps below to configure it. Here takes Windows XP for example. For more details, please refer to <u>Appendix B</u>.

Step 1: Click the Start menu on your desktop, right click My Network Places, and then select **Properties** (shown in Figure 3-1).

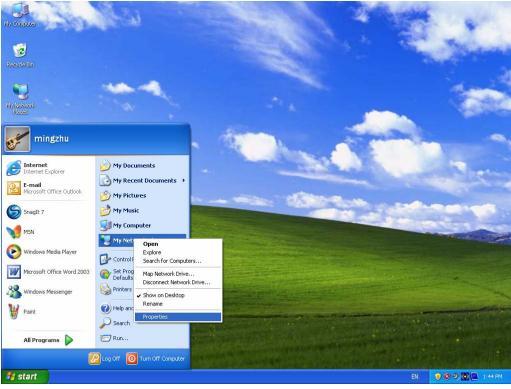


Figure 3-1

Step 2: Right click Local Area Connection (LAN), and then select Properties.

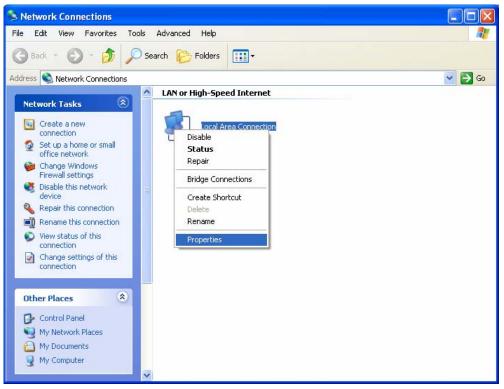


Figure 3-2

Step 3: Select General tab, highlight Internet Protocol (TCP/IP), and then click the Properties button.

🕹 Local Area Connection Properties 🛛 🔹 💽
General Authentication Advanced
Connect using:
Bealtek RTL8139 Family PCI Fast Etł
This connection uses the following items:
 Client for Microsoft Networks File and Printer Sharing for Microsoft Networks QoS Packet Scheduler Internet Protocol (TCP/IP)
□ <u>Install</u> <u>Uninstall</u> <u>Properties</u>
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
Sho <u>w</u> icon in notification area when connected Notify <u>me</u> when this connection has limited or no connectivity
OK Cancel

Figure 3-3

Step 4: Configure the IP address as Figure 3-4 shows. After that, click OK.

Internet Protocol (TCP/IP) Proper	rties 🛛 🕐 🔀
General	
You can get IP settings assigned autom this capability. Otherwise, you need to a the appropriate IP settings.	
Obtain an IP address automatically	,
Use the following IP address	
<u>I</u> P address:	192.168.1.2
S <u>u</u> bnet mask:	255 . 255 . 255 . 0
<u>D</u> efault gateway:	192.168.1.1
O <u>D</u> tain DNS server address autom	atically
• Use the following DNS server add	resses:
Preferred DNS server:	192.168.1.1
<u>A</u> lternate DNS server:	· · ·
	Ad <u>v</u> anced
	OK Cancel

Figure 3-4

Note:

You can configure the PC to get an IP address automatically, select "Obtain an IP address automatically" and "Obtain DNS server address automatically" in the screen above.

Now, you can run the Ping command in the command prompt to verify the network connection. Please click the **Start** menu on your desktop, select **run** tab, type **cmd or command** in the field and press **Enter**. Type **ping 192.168.1.1** on the next screen, and then press **Enter**.

If the result displayed is similar to the screen below, the connection between your PC and the Router has been established.

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = Oms, Maximum = Oms, Average = Oms

Figure 3-5

If the result displayed is similar to the screen shown below, it means that your PC has not connected to the Router.

```
Pinging 192.168.1.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figure 3-6

You can check it following the steps below:

1) Is the connection between your PC and the Router correct?

The LEDs of LAN port which you link to the device and the LEDs on your PC's adapter should be lit.

2) Is the TCP/IP configuration for your PC correct?

If the Router's IP address is 192.168.1.1, your PC's IP address must be within the range of $192.168.1.2 \sim 192.168.1.254$.

3.2 Quick Installation Guide

With a Web-based utility, it is easy to configure and manage the TD-W8960N 300Mbps Wireless N ADSL2+ Modem Router. The Web-based utility can be used on any Windows, Macintosh or UNIX OS with a Web browser, such as Microsoft Internet Explorer, Mozilla Firefox or Apple Safari.

1. To access the configuration utility, open a web-browser and type the default address http://192.168.1.1 in the address field of the browser.

Address http://192.168.1.1

Figure 3-7

•

After a moment, a login window will appear, similar to the Figure 3-8. Enter **admin** for the User Name and Password, both in lower case letters. Then click the **OK** button or press the **Enter** key.

Connect to 192.1	68.1.1	? 🔀
	G	
Wireless N ADSL2	+ Modem Router TD-W8960	N
<u>U</u> ser name:	🖸 admin	*
Password:	•••••	
	Remember my password	д
	ОК	Cancel

Figure 3-8

P Note:

- 1) Do not mix up the user name and password with your ADSL account user name and password which are needed for PPP connections.
- If the above screen does not pop up, it means that your Web-browser has been set to a proxy. Go to Tools menu→Internet Options→Connections→LAN Settings, in the screen that appears, cancel the Using Proxy checkbox, and click OK to finish it.
- 2. After your successful login, you will see the Login screen as shown in Figure 3-9. Click **Quick Setup** menu to access **Quick Setup Wizard**.

Device Info Quick Setup	Device Info			
Advanced Setup				
Wireless				
Diagnostics	Firmware Version:	1.4.0 Bui	ld 110422 Rel.61740n	
Management	Hardware Version: TD-W8960N v3 0x00000002			
	This information reflects	the current s	tatus of your DSL connection.	
	Line Rate - Upstream (Kbps):			
	Line Rate - Downstream (Kbps):			
	LAN IP Address: 192.168.1.1			
	Default G	iateway:	0.0.0.0 ()	
	Primary DNS Server:			
	Secondary DNS	Server:		
	System Runni	ng time:	0 day(s) 00:02:00	

Figure 3-9

3. Change the VPI or VCI values which are used to define a unique path for your connection. If you have been given specific settings for this to configuration, type in the correct

values assigned by your ISP. Here we select PPPoE WAN Link Type for example, enter the Username and Password given by your ISP, and then click Next.

Device Info	Quick Setup WAN Configurations	
Quick Setup	Quick Setup - WAN Configurations	
Advanced Setup		
Wireless	You can configure an ATM PVC identifier (VPI and VCI), select your WAN Link Type.	
Diagnostics	VPI: [0-255] 8	
Management	VCI: [32-65535] 35	
	WAN Link Type: PFPoE 🗸	
	Encapsulation Mode: LLC/SNAP-BRIDGING 💙 (optional)	
	PPP Username:	
	PPP Password:	
	PPPoE Service Name: (optional)	
	MTU Size	
	Dial on demand (with idle timeout timer)	
	Use Static IPv4 Address (optional)	
	DNS Settings: Obtain Automatically O Set DNS Manually	
	Primary DNS:	
	Secondary DNS: (optional)	
	Next	

Figure 3-10

P Note:

The Quick Setup Wizard will guide you to configure the WAN Service over ATM interface.

4. On the **Wireless Configurations** screen, we use the default SSID, select Network Authentication (take **Mixed WPA2/WPA-PSK Personal** for example), set a Pre-Shared Key, and then click **Save** to continue.

Device Info Quick Setup	Quick Setup - W	/ireless Configuratior	IS
Advanced Setup			
Wireless	Note: The all existed ATM & WAN Service will be clean after you click the "Save" button on this Quick Setup page.		
Diagnostics			
Management	You can configure SSID and y	your WLAN Authentication type.	
	Wireless Network Name:	TP-LINK_010001	(Also called SSID)
		ork from hackers and unauthorized users, it is highly recommended you wireless network security settings.	
	Network Authentication:	Mixed WPA2/WPA-PSK Persona	al (adaptive) 🔽
	Wireless NetWork Key:	(Also cal	ed WPA Pre-Shared Key)
		(You can enter ASCII characters betw Hexadecimal characters.)	
		Back Sa	/e

Figure 3-11

P Note:

All the existed **ATM&WAN** service will be cleared after clicking the **Save** button on this Quick Setup page.

5. You will see the **Finish** screen below, click **Reboot** to save these settings.

Device Info	Quick Setup - Finish
Quick Setup	
Advanced Setup	
Wireless	
Diagnostics	Congratulations! The Router is now connecting you to the Internet.
Management	For detail settings, please click other menus if necessary. The change of wireless config will not take effect until the Router reboot. Click the button below to reboot the router. Finish Reboot

Figure 3-12

6. Now, your ADSL Modem Router has been configured and is rebooting. Please do not power off the Router while it's rebooting.

Device Info	Restart
Quick Setup	
Advanced Setup	
Wireless	The DSL Router has been configured and is rebooting.
Diagnostics	
Management	Restarting
	7%

Figure 3-13

 You will see the current configuration has been added to Layer2 Interface list (<u>4.4.1 Layer2</u> <u>Interface</u>) shown in Figure 3-14 and WAN Service list (<u>4.4.2 WAN Service</u>) shown in Figure 3-15.

Device Info	^		тм	Int	erface Co	onfigur	ation						
Quick Setup		2027	DSL ATM Interface Configuration										
Advanced Setup													
-Layer2 Interface		Choose Add	Choose Add, or Remove to configure DSL ATM interfaces.										
 ATM Interface 		Interface	Interface VPI VCI DSL Latency Category Link Type Connection Mode QoS Remove										
 ETH Interface 		atm0	atm0 0 35 Path0 UBR EoA DefaultMode Disabled										
• WAN Service													
• LAN													
• MAC Clone			Add Remove										
+NAT						Indd	Tremove	ļ					
					Figuro	2 11							

Figure 3-14

Device Info	Wide Area Network (WAN) Service Setup											
Quick Setup	inde /											
Advanced Setup												
+Layer2 Interface												
• WAN Service		Choose Add, or Remove to configure a WAN service over a selected interface. ETH and PTM/ATM service can not coexist.										
+ LAN	ETH and PT											
• MAC Clone	Interface	Description	Туре	Vlan8021p	VlanMuxId	Connld	IGMP	NAT	SPI Firewall	Bomovo		
+NAT	Interface	Description		•		connu	IGMF	NAI	SFIFIewan	Kelliove		
+Security	pppO	pvc_quick_setup	PPPoE	N/A	N/A	N/A	Enabled	Enabled	Enabled			
+Parental Control												
+Quality of Service												
+Routing				(Add Remo	ove						

Figure 3-15

P Note:

More detailed configurations please refer to <u>4.4.1 Layer2 Interface</u> and <u>4.4.2 WAN Service</u>.

Chapter 4. Configuring the Router

This chapter will show each Web page's key function and the configuration way.

4.1 Login

After your successful login, you will see the six main menus on the left of the Web-based utility. On the right, there are the corresponding explanations and instructions.

Device Info
Quick Setup
Advanced Setup
Wireless
Diagnostics
Management

The detailed explanations for each Web page's key function are listed below.

4.2 Device Info

Choose "Device Info" menu, there are six submenus under the main menu: Summary, WAN, Statistics, Route, ARP and DHCP. This Device Info section mainly introduces the elementary information about the Router and its current settings in use. Click any of them, and you will be able to view the corresponding information.

Choose "**Device Info**" \rightarrow "**Summary**", you will see the Summary screen (shown in Figure 4-1). The first table indicates the information about the version including Software and Hardware. The second table displays the current status of the TD-W8960N connection. This information will vary depending on the settings of the Router configured on the Advanced Setup screen.

Device Info Quick Setup Advanced Setup	Device Info		
Wireless			
Diagnostics	Firmware Version:	1.4.0 Build	d 110422 Rel.61740n
Management	Hardware Version:	TD-W896	0N v3 0x00000002
	This information reflects	the current sta	atus of your DSL connection.
	Line Rate - Upstream	(Kbps):	
	Line Rate - Downstream	(Kbps):	
	LAN IP A	ddress:	192.168.1.1
	Default G	ateway:	0.0.0.0 ()
	Primary DNS	Server:	
	Secondary DNS	Server:	
	System Runni	ng time:	0 day(s) 00:02:00

Figure 4-1

P Note:

Click the other submenus under the main menu **Device Info**, and you will be able to view the corresponding information about **WAN**, **Statistics**, **Route**, **ARP** and **DHCP**.

4.3 Quick Setup

Please refer to Section 3.2 Quick Installation Guide.

4.4 Advanced Setup

Choose "Advanced Setup", there are many submenus under the main menu. Among the submenus, Layer2 Interface, WAN Service, LAN etc. are default menus, while NAT, IP/MAC filtering of the Security, Quality of Service and DNS will appear only when you select some corresponding functions. Click any one of them, and you will be able to configure the corresponding function.

Advanced Setup + Layer2 Interface + WAN Service + LAN + MAC Clone + NAT + Security + Parental Control + Quality of Service + Traffic Control + Routing + DNS + DNS + DNS + DSL + UPnP + Interface Grouping + LAN Ports + IP Sec	
• WAN Service • LAN • MAC Clone • NAT • Security • Parental Control • Quality of Service • Traffic Control • Routing • DNS • DSL • UPnP • Interface Grouping • LAN Ports	Advanced Setup
 LAN MAC Clone NAT Security Parental Control Quality of Service Traffic Control Routing DNS DSL UPnP Interface Grouping LAN Ports 	+Layer2 Interface
 MAC Clone NAT Security Parental Control Quality of Service Traffic Control Routing DNS DSL UPnP Interface Grouping LAN Ports 	•WAN Service
+NAT + Security + Parental Control + Quality of Service + Traffic Control + Routing + DNS + DNS + DSL + UPnP + Interface Grouping + LAN Ports	• LAN
 Security Parental Control Quality of Service Traffic Control Routing DNS DSL UPnP Interface Grouping LAN Ports 	MAC Clone
 Parental Control Quality of Service Traffic Control Routing DNS DSL UPnP Interface Grouping LAN Ports 	+NAT
+Quality of Service +Traffic Control +Routing +DNS •DSL •UPnP •Interface Grouping •LAN Ports	+ Security
 Traffic Control Routing DNS DSL UPnP Interface Grouping LAN Ports 	+Parental Control
+Routing +DNS •DSL •UPnP •Interface Grouping •LAN Ports	+Quality of Service
+ DNS • DSL • UPnP • Interface Grouping • LAN Ports	+Traffic Control
• DSL • UPnP • Interface Grouping • LAN Ports	+Routing
• UPnP • Interface Grouping • LAN Ports	+DNS
 Interface Grouping LAN Ports 	•DSL
• LAN Ports	• UPnP
	 Interface Grouping
• IP Sec	LAN Ports
	• IP Sec

This Advanced Setup section mainly introduces how to configure the Router for adequate use. The detailed explanations for each subsection are provided below.

P Note:

To completely configure the WAN Interface, you need to first select the Layer2 Interface (<u>4.4.1</u> <u>Layer2 Interface</u>) according to the connection ISP provides you, and then to select the type of the connection (<u>4.4.2 WAN Service</u>) for the further configuration.

4.4.1 Layer2 Interface

Choose "Advanced Setup"→"Layer2 Interface", and you can select WAN Service Interface (layer2 interface) over ATM interfaces or ETH interface.

- ATM Interface: Configure the Router to access Internet as an ADSL user. ISP provides you VPI (Virtual Path Identifier), VCI (Virtual Channel Identifier) settings and the DSL Interface with RJ11 connector. (Figure 2-1)
- **ETH Interface:** Configure the Router to access Internet as an Ethernet user. ISP provides you Broadband Internet Service and the Ethernet Interface with RJ45 connector.

4.4.1.1 ATM interface

Choose "Advanced Setup"→"Layer2 Interface→ATM interface", you can Configure ATM interfaces on the screen below.

Device Info	DSL A	тм	Inte	erface Co	nfigura	tion							
Quick Setup													
Advanced Setup													
-Layer2 Interface	Choose Add, or Remove to configure DSL ATM interfaces.												
ATM Interface	Interface	Interface VPI VCI DSL Latency Category Link Type Connection Mode QoS Remove											
• ETH Interface	atm0	0	32	Path0	UBR	EoA	DefaultMode	Disabled					
• WAN Service	atm1	1	33	Path0	UBR	EoA	DefaultMode	Disabled					
• LAN	aurri	I	33	Patrio	UBR	EUA	Delaulimode	Disapled					
• MAC Clone	atm2	0	35	Path0	UBR	EoA	DefaultMode	Disabled					
+ Security	atm3	0	100	Path0	UBR	EoA	DefaultMode	Disabled					
+Parental Control	atm4	8	35	Path0	UBR	EoA	DefaultMode	Dischlad					
•Quality of Service	atrri4	0	30	Faulo	UBR	EUA	Delaulimode	Disabled					
+Traffic Control	atm5	8	81	Path0	UBR	EoA	DefaultMode	Disabled					
+Routing	atm6	0	200	Path0	UBR	EoA	DefaultMode	Disabled					
+DNS													
• DSL													
• UPnP					Add	Remove							
 Interface Grouping 					Indd								

Figure 4-2

Remove: Select the check box in the table on the screen above and then click the Remove button, the corresponding interface will be deleted in the table.

P Note:

If the interface is used by the configuration of the <u>4.4.2 WAN Service</u>, you need to remove the corresponding WAN Service entry first before you can remove it here.

> Add: Click the button, and you can add a new interface in the next screen.

Device Info	ATM PVC Configuration
Quick Setup	
Advanced Setup	
-Layer2 Interface	This screen allows you to configure an ATM PVC identifier (VPI and VCI), select DSL latency, select a
ATM Interface	service category. Otherwise choose an existing interface by selecting the checkbox to enable it.
• ETH Interface	VPI: [0-255] 0
• WAN Service	VCI: [32-65535] 35
• LAN	
• MAC Clone	Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.) EoA
+ Security	O PPPoA
+Parental Control	O IPoA
+Quality of Service	
+ Traffic Control	Encapsulation Mode: LLC/SNAP-BRIDGING
+Routing	Service Category: UBR Without PCR 🗸
+DNS	
• DSL	Select Connection Mode
• UPnP	O Default Mode - Single service over one connection
Interface Grouping	VLAN MUX Mode - Multiple Vlan service over one connection
LAN Ports	MSC Mode - Multiple Service over one Connection
• IP Sec	
Wireless	Enable Quality Of Service
Diagnostics	Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS
Management	cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of
	PVCs will be reduced. Use Advanced Setup/Quality of Service to assign priorities for the applications.
	Enable Quality Of Service.
	Back Apply/Save

Figure 4-3

- VPI/VCI: the VPI and VCI values provided by your ISP. Do not change them unless it was required by your ISP.
- DSL Link Type: Select a DSL Link Type which is provided by your ISP. The options include EoA (it is for PPPoE, IPoE, and Bridge), PPPoA (PPP over ATM) and IPoA (IP over ATM).
- Encapsulation Mode: The mode of the data processing over the Link Type you have selected. Uses the default setting, if you are not sure.
- Service Category: Select the type of the service assigned by your ISP in the drop-down list. The default type is UBR Without PCR.
- Connection Mode: Select the connection mode for EoA option of DSL Link Type. The options include Default mode for single service over one connection, VLAN MUX Mode for multiple Vlan service over one connection, and MSC Mode for Multiple Service over one connection.
- Enable Quality of Service: If you want to adopt QoS (Quality of Service) for the connection, please select check box.

P Note:

Enabling packet level QoS for PVC improves performance for selected classes of applications. While QoS consumes system resources; therefore the number of PVC(s) will be reduced. Besides

this, it cannot be set for the connection type of CBR and Real-time VBR. If you select the QoS service, the Quality of Service menu will be added to the Web-based Utility, the detailed configuration will be described in **4.4.8 Quality of Service**.

4.4.1.2 ETH interface

Choose "Advanced Setup"→"Layer2 Interface→ETH Interface", you can configure ETH WAN interfaces on the screen below.

Device Info	ETH WAN Interface Configuration									
Quick Setup		and e e e e e e e e e e e e e e e e e e e								
Advanced Setup										
-Layer2 Interface	Choose Add, or Remove to con	figure ETH WAN interfaces.								
 ATM Interface 	Allow one ETH as layer 2 wan i	Allow one ETH as layer 2 wan interface.								
• ETH Interface	Interface/(Name)	Connection Mode	Remove							
• WAN Service										
• LAN										
• MAC Clone		Add Remove								



P Note:

To make sure the ETH port available, you should first choose "Advanced Setup" \rightarrow "LAN Ports" to enable the Virtual LAN Ports feature.

> Add: Click the Add button, and you can add a new interface in the next screen.

Device Info	ETH WAN Configuration
Quick Setup	
Advanced Setup	
-Layer2 Interface	This screen allows you to configure a ETH port.
• ATM Interface	
• ETH Interface	Select a ETH port: eth0. 2/LAN4 🗸
• WAN Service	
• LAN	Select Connection Mode
• MAC Clone	Oefault Mode - Single service over one connection
+Security	VLAN MUX Mode - Multiple Vian service over one connection
+Parental Control	MSC Mode - Multiple Service over one Connection
+Quality of Service	
+Traffic Control	
+Routing	Back Apply/Save

Figure 4-5

> ETH port: Select an ETH port to configure as the WAN port.

> Select Connection Mode: Choose a connection mode for the port.

Click Apply/Save to save your settings and then you will see the screen similar to Figure 4-6.

Device Info	ETH WAN Interfa	ace Configuration	
Quick Setup		ace comganance	
Advanced Setup			
-Layer2 Interface	Choose Add, or Remove to con	nfigure ETH WAN interfaces.	
• ATM Interface	Allow one ETH as layer 2 wan i	nterface.	
• ETH Interface	Interface/(Name)	Connection Mode	Remove
• WAN Service	eth0.2/LAN4	DefaultMode	
• LAN		I	
• MAC Clone			
+Security		Remove	
+Parental Control			

Figure 4-6

Remove: Select the check box in the table on the screen above and then click the Remove button, the corresponding interface will be deleted in the table.

P Note:

One ETH is allowed to configure as the layer 2 WAN Interface.

4.4.2 WAN Service

Choose "Advanced Setup"→"WAN Service", and you will see the WAN Port Information Table in the screen similar to Figure 4-7, which describes the WAN port settings and the relevant manipulation to each interface. After you add a new Lay2 Interface, please follow the instructions below to complete the further configuration of WAN Interface. There are five different configurations for the connection types, which are PPPoE, IPoE, Bridge, PPPoA, and IPoA. You can select the corresponding types according to your needs.

Device Info	Wide 4	rea Net	work		Service	Setu	In				
Quick Setup	Wide F		worr		O CI VICC	. 0010	P P				
Advanced Setup											
+Layer2 Interface											
• WAN Service		, or Remove to	-		ce over a sele	cted interfa	ace.				
• LAN	ETH and PT	M/ATM service	can not o	coexist.							
• MAC Clone	Interface	Description	Туре	Vlan8021n	VlanMuxId	Connld	IGMP	NAT	SPI Firewall	Remove	Edit
Security		-		•							
Parental Control	atm0	br_0_0_32	Bridge	N/A	N/A	N/A	Disabled	Disabled	Disabled		Edit
Quality of Service	atm1	br_0_1_33	Bridge	N/A	N/A	N/A	Disabled	Disabled	Disabled		Edit
Traffic Control	atm2	br_0_0_35	Bridge	N/A	N/A	N/A	Disabled	Disabled	Disabled		Edi
Routing	atm3	br_0_0_100	Bridge	N/A	N/A	N/A	Disabled	Disabled	Disabled		Edi
)SL	atur (hr 0 0 05	Deidaa	NUA	N/A	N/A	Dischlad	Disabled	Dischlad		_
JPnP	atm4	br_0_8_35	Bridge	N/A	N/A	IN/A	Disabled	Disabled	Disabled		Edi
nterface Grouping	atm5	br_0_8_81	Bridge	N/A	N/A	N/A	Disabled	Disabled	Disabled		Edi
_AN Ports PSec	atm6	br_0_0_200	Bridge	N/A	N/A	N/A	Disabled	Disabled	Disabled		Edi
ireless	<u> </u>			1							
iagnostics											
 lanagement	Add Remove										

Figure 4-7

PNote:

- The following section adopts different VPI, VCI to introduce further configuration for the different connection types, if you need to change the configuration of ATM PVC (VPI/VCI), you should go to the previous section (<u>4.4.1 Laver2 Interface</u>) to configure them again.
- 2) ETH and ATM service can not coexist. If the ETH Interface had configured, you cannot configure any other WAN service over the ATM Interface until the ETH Interface is deleted.

4.4.2.1 ATM-EoA-PPPoE

If your ISP provides a **PPPoE** connection and you need to use an ATM Interface, follow the steps below to add a WAN service over a selected ATM interface:

- 1. Add a new ATM interface and select EoA option for DSL Link Type (4.4.1.1 ATM interface).
- 2. Click the **Add** button on the screen Figure 4-7 and you will enter the next screen as shown in Figure 4-8. Click **Next**.

Device Info	WAN Service Interface Configuration						
Quick Setup	WAN Service Interface Configuration						
Advanced Setup							
+Layer2 Interface							
• WAN Service	Select a layer 2 interface for this service						
• LAN	Note: For ATM interface, the descriptor string is (portId_vpi_vci) For PTM interface, the descriptor string is (portId high low)						
• MAC Clone	Where portid=0> DSL Latency PATH0 portid=1> DSL Latency PATH1 portid=4> DSL Latency PATH0&1						
+ Security							
+Parental Control	low =0> Low PTM Priority not set low =1> Low PTM Priority set						
+Quality of Service	high =0> High PTM Priority not set high =1> High PTM Priority set						
+Traffic Control							
+Routing							
• DSL	Select WAN Service Interface: atm7/(0_0_38) 🗸						
• UPnP							
 Interface Grouping 							
LAN Ports	Back Next						

Figure 4-8

 Select the WAN service type in Figure 4-9. If your ISP provides a PPPoE connection, select PPPoE option. You can create a service name for the Service Description or leave it the default name. Click Next.

Device Info	WAN Service Configuration		
Quick Setup		g	
Advanced Setup			
+Layer2 Interface	Select WAN service type:		
• WAN Service		PPP over Ethernet (PPPoE)	
• LAN		O IP over Ethernet	
MAC Clone		O Bridging	
+ Security	Enter Service Description:	pppoe_0_0_38	
+Parental Control			
+Quality of Service			
+Traffic Control		Back	
+Routing			

Figure 4-9

4. Enter the following parameters and then click **Next**.

Device Info	PPP Username a	nd Password	
Quick Setup			
Advanced Setup			
+Layer2 Interface			
•WAN Service	PPP usually requires that you have enter the user name and passy		sword to establish your connection. In the boxes below, ided to you
• LAN	enter the user hame and passy		10eu 10 you.
• MAC Clone	PPP Username:	pppuser	
+ Security	PPP Password:	•••••	
+Parental Control	PPPoE Service Name:		
+Quality of Service	Authentication Method:	AUTO 🗸	
+Traffic Control			
+Routing	MTU Size		
+DNS	MTU (bytes) [576-1492]:	1480	(The default is 1480, do not change unless
• DSL		necessary.)	
• UPnP	Enable Fullcone NAT		
 Interface Grouping 	🔲 Dial on demand (with idle ti	imeout timer)	
LAN Ports	📃 PPP IP extension (do not ch	noose unless necessary)	
• IP Sec	🔲 Use Static IPv4 Address		
Wireless			
Diagnostics	📃 Enable PPP Debug Mode		
Management	Multicast Proxy		
	Enable IGMP Multicast Prox	Ŋ	
	🔲 Enable MLD Multicast Proxy	(
		Back	Next

Figure 4-10

- PPP Username/Password: Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- PPPoE Service Name: Enter the Service Name if it was provided by your ISP. If you leave it blank, the default name will be the same as the Service Description on the previous screen.
- Authentication Method: Select the Authentication Method from the drop-down list, the default method is AUTO, and you can leave it as a default setting.

Note:

If you are not sure about the **PPP IP extension** and **PPP Debug Mode** etc. below, please don't select these options.

- MTU Size: Maximum Transmission Unit Size. Check this box then you can change the MTU size. The default MTU value is 1480 Bytes. It is not recommended that you change the default value unless required by your ISP.
- > Enable Fullcone NAT: It is a type of NAT, if not enabled, the default NAT will act.
- Dial on demand (with idle timeout timer): The Router will cut off the Internet connection after it has been inactive for a specific period of time (idle timeout), and it will automatically re-establish the connection as soon as you attempt to access the Internet again. If your Internet is charged by time you may want to select this option in order to save money.
- > **PPP IP extension**: Select this option to get the public IP address from the PPP server to your

PC, and the NAT and SPI Firewall will be closed. Sometimes you can think it as bridge while PPP dialing in the router. It's a special feature deployed by some ISP. Unless your ISP specifically requires this setup, do not select it.

- Use Static IPv4 Address: If your ISP gives you a static WAN, Gateway and DNS IP address, select this option to enter them manually.
- Enable PPP Debug Mode: Select this option to debug the PPP function and you can see many PPP log information in the System Log. Only PPP has this debug Mode.
- Bridge PPPoE Frames Between WAN and Local Ports: Select this option to start PPP connection in your local PC.
- Enable IGMP Multicast Proxy: IGMP (Internet Group Management Protocol) is used to manage multicasting on TCP/IP networks. Some ISPs use IGMP to perform remote configuration for client devices, such as the Router. The default value is disabled, and if you are not sure, please contact your ISP or just leave it.
- 5. Select a preferred wan interface as the system default gateway in Figure 4-11 and click **Next**.

Device Info	Routing Default Gateway
Quick Setup	
Advanced Setup	
+Layer2 Interface	
• WAN Service	Select a preferred wan interface as the system default gateway.
• LAN	
• MAC Clone	Selected WAN Interface: pppoe_0_0_38/ppp0 v
+Security	
+Parental Control	Back
+Quality of Service	Dack Wext

Figure 4-11

6. Configure the DNS Server Addresses on the screen below and click Next.

••••••••••••••••••••••••••••••••••••••	
Device Info	DNS Server Configuration
Quick Setup	2 com com gan anon
Advanced Setup	
+Layer2 Interface	
WAN Service	Get DNS server information from the selected WAN interface OR enter static DNS server IP addresses. If only a single PVC with IPoA or static MER protocol is configured, you must enter static DNS server IP addresses.
• LAN	single rive within the of status wells protocorts configured, you must enter status DNG server in addresses.
• MAC Clone	Obtain DNS info from a WAN interface:
+Security	WAN Interface selected: pppoe_0_0_38/ppp0 v
+Parental Control	O Use the following Static DNS IP address:
+Quality of Service	Primary DNS server:
+Traffic Control	
+Routing	Secondary DNS server:
+DNS	
• DSL	
• UPnP	Back Next
	Figure 4-12

- Obtain DNS info from a WAN Interface: You can select this option to automatically get DNS server information from the selected WAN interface.
- Use the following Static DNS IP Address: You can select this option to manually enter the primary and /or optional secondary DNS server IP addresses provided by your ISP.

P Note:

If only single PVC with IPoA is configured, you must enter static DNS server IP addresses.

7. On the next screen you will see the detailed settings you've made. Please click the **Apply/Save** button to save these settings.

evice Info	WAN Setup - Summary		
uick Setup			
dvanced Setup			
Layer2 Interface			
WAN Service	Make sure that the settings below match t	e settings provided by your ISP.	
LAN			
MAC Clone	PORT / VPI / VCI:	0/0/38	
Security	Connection Type:	PPPoE	
Parental Control	Service Name:	pppoe_0_0_38	
Quality of Service	Service Category:	UBR	
Traffic Control	IP Address:	Automatically Assigned	
Routing	Service State:	Enabled	
DSL	NAT:	Enabled	
UPnP	Full Cone NAT:	Disabled	
Interface Grouping	SPI Firewall:	Enabled	
LAN Ports	IGMP Multicast:	Disabled	
IPSec	Quality Of Service:	Disabled	
ireless		be effective. Click "Back" to make any modifications.	
agnostics	onex caressppy to have this intenace to	so encourse, onex back to make any moundations.	
anagement			

Figure 4-13

8. On the next screen you will see the WAN Port Information Table with the new configuration.

Device Info	Wide A	Area Netw	ork (WAN) S	Service	Setun					
Quick Setup						ootup					
Advanced Setup	I										
+Layer2 Interface											
• WAN Service		Choose Add, or Remove to configure a WAN service over a selected interface.									
• LAN	ETH and PT	M/ATM service ca	n not coe	xist.							
• MAC Clone	Interface	Description	Туре	Vlan8021p	VlanMuxId	Connld	IGMP	NAT	SPI Firewall	Remove	Edit
+ Security											
+Parental Control	atm0	br_0_0_32	Bridge	N/A	N/A	N/A	Disabled	Disabled	Disabled		Edit
+Quality of Service	atm1	br_0_1_33	Bridge	N/A	N/A	N/A	Disabled	Disabled	Disabled		Edit
+Traffic Control	atm2	br_0_0_35	Bridge	N/A	N/A	N/A	Disabled	Disabled	Disabled		Edit
+Routing •DSL	atm3	br_0_0_100	Bridge	N/A	N/A	N/A	Disabled	Disabled	Disabled		Edit
•UPnP	atm4	br_0_8_35	Bridge	N/A	N/A	N/A	Disabled	Disabled	Disabled		Edit
 Interface Grouping 	atm5	br_0_8_81	Bridge	N/A	N/A	N/A	Disabled	Disabled	Disabled		Edit
LAN Ports			_								
• IP Sec	atm6	br_0_0_200	Bridge	N/A	N/A	N/A	Disabled	Disabled	Disabled		Edit
Wireless	ppp0	pppoe_0_0_38	PPPoE	N/A	N/A	N/A	Disabled	Enabled	Enabled		Edit
Diagnostics		1		1						1	
Management											
		Add Remove									

Figure 4-14

Remove: Select the check box in the table above and then click Remove, the corresponding interface will be deleted in the table.

4.4.2.2 ATM-EoA-IPoE

If your ISP provides an **IPoE** connection and you need to use an ATM Interface, follow the steps below to add a WAN service over a selected ATM interface:

- 1. Add a new ATM interface and select EoA option for DSL Link Type (4.4.1.1 ATM interface).
- 2. Click the **Add** button on the screen (as shown Figure 4-7). Select WAN Service Interface over ATM PVC on the next screen (as shown Figure 4-8).
- 3. If your ISP provides an IPoE connection, select **IPoE** option for the **WAN service type** on the screen (as shown Figure 4-9), and click **Next** button to continue.
- 4. Enter parameters in the following blanks to configure the WAN IP Address and click Next.

Device Info	WAN IP Settings
Quick Setup	WAN IF Oettings
Advanced Setup	
+Layer2 Interface	
• WAN Service	Enter information provided to you by your ISP to configure the WAN IP settings. Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in MER mode.
• LAN	If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway.
• MAC Clone	
+ Security	Obtain an IP address automatically
+Parental Control	Option 60 Vendor ID:
+Quality of Service	Option 61 IAID: (8 hexadecimal digits)
+Traffic Control	Option 61 DUID: (hexadecimal digit)
+Routing	Option 125: Disable Enable
•DSL	O Use the following Static IP address:
• UPnP	WAN IP Address:
Interface Grouping	WAN Subnet Mask:
LAN Ports	WAN gateway IP Address:
• IP Sec	
Wireless	
Diagnostics	Back Next

Figure 4-15

Obtain an IP address automatically: Select this option, the Router will be able to obtain IP network information dynamically from a DHCP server provided by your ISP.

PNote:

- The response message from a DHCP server typically contains a number of configuration parameters (DHCP options) for the Router. The DHCP options include IP network information, and also the vendor-specific options. In some cases, the Router is implemented to perform user-defined operations (as shown below). You can implement your own treatment of all such options.
- 2) If the Router is functioning as a DHCP client, it must identify itself in option 61 (client-identifier) in every DHCP message. DUID/IAID is portion of option 61.
 - Option 60 Vendor ID: The option code 60 used to identify Vendor class.
 - Option 61 IAID: IAID (Identity Association ID) assigns an Identity Association ID to individual interfaces. In cases where the device is functioning with a single DHCP client identity, it must use value 1 for IAID for all DHCP interactions. In cases where the device is functioning with multiple DHCP client identities, the values of IAID have to start at 1 for the first identity and be incremented for each subsequent identity. For example, the device may use IAID value 1 for the first physical interface and value 2 for the second.

Alternatively, the device may use IAID value 1 for the virtual circuit corresponding to the first connection object in the data model and value 2 for the second connection object in the data model.

- **Option 61 DUID:** Specifies the name of the interface whose link-layer address the server is to use as its DUID (DHCP Unique Identifier). You must enter a value for this parameter or the server will not start. When the server starts, the DUID is written to the system log.
- **Option 125:** The option 125 allows DHCP server to be pre-configured with policy for handling classes of devices in a certain way without requiring DHCP server to be able to parse the unique format used in client-identifier option.
- Use the following IP Address: If you are provided with a static IP/gateway Address, please select this option, and then enter the WAN IP Address, WAN Subnet Mask and WAN gateway IP Address manually.
- 5. You will see the next screen as below. You can enable the **NAT**, **SPI Firewall**, and **IGMP Multicast**, if you are not sure about the settings, just leave the default settings. Click **Next**.

Device Info Quick Setup	Network Address Translation Settings		
Advanced Setup			
+Layer2 Interface			
• WAN Service	Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (LAN).		
• LAN	computers on your Eddar Area Network (EAN).		
• MAC Clone	Enable NAT		
+ Security			
+Parental Control	Enable SPI Firewall		
+Quality of Service	IGMP Multicast		
+Traffic Control	Enable IGMP Multicast		
+Routing			
• DSL			
• UPnP	Back		
 Interface Grouping 			

Figure 4-16

- Enable NAT: This technology translates the IP addresses of a local area network to a different IP address for the Internet. If this Router is hosting your network's connection to the Internet, please select the check box. If another Router exists in your network, you don't need to select the option.
- Enable SPI Firewall: A SPI firewall enhances network's security. Select the option to use a firewall, or else without a firewall.
- Enable IGMP Multicast: This is disabled by default. This setting will not allow IGMP (Internet Group Management Protocol) packets to be forwarded to the LAN. IGMP is used to manage multicasting on TCP/IP networks. Most users will not need to enable this. Some ISPs use IGMP to perform remote configuration for client devices, such as the Router. If you are unsure, check with your ISP.

P Note:

If you select the **Enable NAT** checkbox, the **NAT** menu will be added to the Web-based Utility. We will describe the detailed configuration in <u>4.4.5 NAT</u>.

6. Select a preferred **WAN** interface as the system default gateway and click **Next**.

Device Info	Routing Default Gateway		
Quick Setup	······································		
Advanced Setup			
+Layer2 Interface			
• WAN Service	Select a preferred wan interface as the system default gateway.		
• LAN			
• MAC Clone	Selected WAN Interface: ipoe_0_0_38/atm7 🗸		
+ Security			
+Parental Control	Back		
+Quality of Service	Dack Next		



7. Configure the DNS Server Addresses on the screen as follows.

Device Info	DNS Server Configuration
Quick Setup	
Advanced Setup	
+Layer2 Interface	
• WAN Service	Get DNS server information from the selected WAN interface OR enter static DNS server IP addresses. If only a single PVC with IPoA or static MER protocol is configured, you must enter static DNS server IP addresses.
• LAN	Single Five with in the of static with protocol is configured, you must enter static Dive server in addresses.
• MAC Clone	Obtain DNS info from a WAN interface:
+ Security	WAN Interface selected: ipoe 0 0 38/atm7 v
+Parental Control	Use the following Static DNS IP address:
+Quality of Service	Primary DNS server:
+Traffic Control	
+Routing	Secondary DNS server:
+DNS	
• DSL	
• UPnP	Back Next

Figure 4-18

P Note:

If only single PVC with IPoA is configured, you must enter static DNS server IP addresses.

8. On the next screen (as shown Figure 4-19) you will see the detailed settings you've made. Please click the **Apply/Save** button to save these settings.

Device Info	WAN Setup - Summ	arv
Quick Setup	mar coup cann	
Advanced Setup		
+Layer2 Interface		
• WAN Service	Make sure that the settings below ma	tch the settings provided by your ISP.
• LAN		
MAC Clone	PORT / VPI / VCI:	0/0/38
+ Security	Connection Type:	IPoE
+Parental Control	Service Name:	ipoe_0_0_38
+Quality of Service	Service Category:	UBR
+Traffic Control	IP Address:	Automatically Assigned
+Routing	Service State:	Enabled
• DSL	NAT:	Disabled
• UPnP	Full Cone NAT:	Disabled
 Interface Grouping 	SPI Firewall:	Disabled
LAN Ports	IGMP Multicast:	Disabled
• IP Sec	Quality Of Service:	Disabled
Wireless		e to be effective. Click "Back" to make any modifications.
Diagnostics	onex curer oppy to have the interfac	e to be encerve. Once back to make any modifications.
Management		
		Back Apply/Save

Figure 4-19

4.4.2.3 ATM-EoA-Bridging

If you want to adopt the **Bridge** service and you need to use an ATM Interface, follow the steps below to add a WAN service over a selected ATM interface:

- 1. Add a new ATM interface and select **EoA** option for DSL Link Type (see <u>4.4.1.1 ATM</u> <u>interface</u>).
- 2. Click the **Add** button on the screen Figure 4-7. Select WAN Service Interface over ATM PVC on the next screen (as shown Figure 4-8).
- 3. Select **Bridging** option for the **WAN service type** on the screen (as shown Figure 4-9), and click **Next** button to continue.
- 4. On the screen (as shown Figure 4-13) you will see the detailed settings you've made. Please click the **Apply/Save** button to save these settings.

4.4.2.4 ATM-PPPoA

If your ISP provides a **PPPoA** connection and you need to use an ATM Interface, follow the steps below to add a WAN service over a selected ATM interface:

- 1. Add a new ATM interface and select **PPPoA** option for DSL Link Type (see <u>4.4.1.1 ATM</u> <u>interface</u>).
- Click the Add button on the screen Figure 4-7 and the next configuration is similar to PPPoE, (see section <u>4.4.2.1 ATM-EoA-PPPoE</u>). The difference is that you don't need to set the PPPoE Service Name and Bridge PPPoE Frames Between WAN and Local Ports on the screen of Figure 4-10.

4.4.2.5 ATM-IPoA

If your ISP provides an **IPoA** connection and you need to use an ATM Interface, follow the steps below to add a WAN service over a selected ATM interface.

- 1. Add a new ATM interface and select **IPoA** option for DSL Link Type (see <u>4.4.1.1 ATM</u> <u>interface</u>).
- Click the Add button on the screen Figure 4-7 and the next configuration is similar to IPoE (see section <u>4.4.2.2 ATM-EoA-IPoE</u>). The difference is that you have to manually set the Static IP Address on the screen of Figure 4-15, and the Static IP Address for DNS Server on the screen of Figure 4-18.

P Note:

ETH and ATM service can not coexist. If the ATM Interface had configured, you cannot configure any other WAN service over the ETH Interface until the ATM Interface is deleted.

4.4.2.6 ETH-PPPoE

If your ISP provides a **PPPoE** connection and you need to use an **ETH** Interface, follow the steps below to add a WAN service over a selected ETH interface:

- 1. Add a new **ETH** interface on the screen of <u>4.4.1.2 ETH interface</u>.
- Click the Add button on the screen Figure 4-7 and the following configuration is similar to PPPoE over ATM interface (see section <u>4.4.2.1 ATM-EoA-PPPoE</u>).

4.4.2.7 ETH-IPoE

If your ISP provides an **IPoE** connection and you want to use an **ETH** Interface, follow the steps below to add a WAN service over a selected ETH interface:

- 1. Add a new **ETH** interface on the screen of <u>4.4.1.2 ETH interface</u>.
- Click the Add button on the screen Figure 4-7 and the next configuration is similar to IPoE over ATM interface (see section <u>4.4.2.2 ATM-EoA-IPoE</u>).

4.4.2.8 ETH-Bridge

If you want to adopt the **Bridge** service and you need to use an **ETH** Interface, follow the steps below to add a WAN service over a selected ETH interface:

- 1. Add a new **ETH** interface on the screen of <u>4.4.1.2 ETH interface</u>.
- Click the Add button on the screen Figure 4-7 and the next configuration is similar to Bridge over ATM interface (see section <u>4.4.2.3 ATM-EoA-Bridg</u>).

PNote:

For ETH-PPPoE, ETH-IPoE and ETH-Bridge, the Bridging option will display in the screen of Figure 4-20 only when VLAN MUX Mode is selected for Connection Mode on the screen of Figure 4-5. You have to set the **802.1P Priority** and **802.1Q VLAN ID**.

Device Info	WAN Service Conf	iguration
Quick Setup		
Advanced Setup	Select WAN service type:	
•		PPP over Ethernet (PPPoE)
+Layer2 Interface		🔘 IP over Ethernet
•WAN Service		O Bridging
+ LAN	Enter Service Description:	pppoe_eth0.3
• MAC Clone	Enter 802.1P Priority [0-7]:	0
+ Security	Enter 802.1Q VLAN ID [0-4094]:	0
+Parental Control		
+Quality of Service		Back Wayt
+ Traffic Control		Back
n	Figure 4	-20

4.4.3 LAN

Choose "Advanced Setup" \rightarrow "LAN", and you will see the LAN screen (shown in Figure 4-21), the section allows you to configure the Router's LAN ports settings.

Device Info	Local Area Netwo	ork (LAN) Setup		
Quick Setup	Eoodi Alou Notwo			
Advanced Setup	7			
+Layer2 Interface	Configure the DSL Modem Rout	er IP Address and Subnet Mas	k for LAN interface. GroupName D	efault 🗸
• WAN Service				
• LAN	IP Address:	192.168.1.1		
 MAC Clone 	Subnet Mask:	255.255.255.0		
+ Security				
+Parental Control	-			
+Quality of Service	🔲 Enable IGMP Snooping			
Traffic Control	💿 Standard Mode			
+Routing	O Blocking Mode			
+DNS	0			
• DSL				
• UPnP			ll not able to manage the Router. P	
 Interface Grouping 	-	I to manage the Router on "S	ecurity->IP Filtering->Incoming" pa	ge.
LAN Ports	📃 Enable LAN side firewall			
• IP Sec				
Wireless	O Disable DUOD Games			
Diagnostics	O Disable DHCP Server			
Management	Enable DHCP Server			
	Start IP Address:	192.168.1.100		
	End IP Address:	192.168.1.200		
	Leased Time (hour):	24		
	Static IP Lease List: (A maximu	ım 32 entries can be configu	ed)	
	MAC Address	IP Address	Remove	
	[Add Entries Re	nove Entries	
	-			
	Configure the second IP Ac	idress and Subnet Mask for L	AN interface	
		Save/Apply	·	



- > **IP Address:** You can configure the Router's IP Address and Subnet Mask for LAN Interface.
 - **IP Address:** Enter the Router's local IP Address, then you can access to the Web-based Utility via the IP Address, the default value is 192.168.1.1.
 - Subnet Mask: Enter the Router's Subnet Mask, the default value is 255.255.255.0.
- Enable IGMP Snooping: If you select the option, please choose the IGMP Mode: Standard Mode or Blocking Mode.
- DHCP Server: These settings allow you to configure the Router's Dynamic Host Configuration Protocol (DHCP) server function. The DHCP server is enabled by default for the Router's Ethernet LAN interface. DHCP service will supply IP settings to computers which are configured to automatically obtain IP settings that are connected to the Router though the Ethernet port. When the Router is set for DHCP, it becomes the default gateway for DHCP client connected to it. Keep in mind that if you change the IP address of the Router, you must change the range of IP addresses in the pool used for DHCP on the LAN.

- Start IP Address: Enter a value for the DHCP server to start with when issuing IP addresses. Because the default IP address for the Router is 192.168.1.1, the default Start IP Address is **192.168.1.2**, and the Start IP Address must be 192.168.1.2 or greater, but smaller than 192.168.1.254.
- End IP Address: Enter a value for the DHCP server to end with when issuing IP addresses. The End IP Address must be smaller than 192.168.1.254. The default End IP Address is **192.168.1.254**.
- Leased Time (hour): The Leased Time is the amount of time in which a network user will be allowed connection to the Router with their current dynamic IP address. Enter the amount of time, in hours, then the user will be "leased" this dynamic IP address. After the dynamic IP address has expired, the user will be automatically assigned a new dynamic IP address. The default is **24** hours.
- Static IP Lease List: The function allows you to specify a reserved IP address for a PC on the LAN, that PC will always obtain the assigned IP address each time when it accesses the DHCP server. Reserved IP addresses should be assigned to servers that require permanent IP settings. Click the Add Entries button, and then you will set the rule in the screen as below.

Device Info	DHCP Static IP Lease
Quick Setup	
Advanced Setup	
+Layer2 Interface	Enter the Mac address and Static IP address then click "Save/Apply".
• WAN Service	
+ LAN	MAC Address:
• MAC Clone	IP Address:
+ Security	
+Parental Control	
+Quality of Service	Save/Apply

Figure 4-22

- MAC Address: The MAC address of the computer on the LAN which you want to reserve an IP.
- IP Address: The IP address you want to reserved to the computer.
- Configure the second IP Address and Subnet Mask: You can configure the Router's second IP Address and Subnet Mask for LAN Interface through which you can also access to the Web-based Utility as the default IP Address and Subnet Mask.

UPnP, DHCP Server and the second IP Address are not available for the connection type of **Bridging** here, they won't display on the preceding screen since only Bridging is selected.

4.4.4 MAC Clone

Choose menu "Advanced Setup" \rightarrow "MAC Clone", you can configure the MAC address of the WAN Interface as shown below.

The WAN Interface List displays the Lay2 Interfaces you have configured on the section <u>4.4.1</u> <u>Layer2 Interface</u> and its default MAC Address. If you have not configured corresponding WAN Service for the interface on the section <u>4.4.2 WAN Service</u>, the blank for MAC Address will display "Need a corresponding WAN Service".

The last one of WAN Interface List displays your PC's current address.

etup		
rface Set the special MAC Add	dress to the selected WAN interfact	e
ce atm0 MAC Address:	00:25:86:c7:99:ab	Restore Default
atm1 MAC Address:	00:25:86:c7:99:ac	Restore Default
atm2 MAC Address:	00:25:86:c7:99:ad	Restore Default
atm3 MAC Address:	00:25:86:c7:99:ae	Restore Default
Service atm4 MAC Address:	00:25:86:c7:99:af	Restore Default
atm5 MAC Address:	00:25:86:c7:99:b0	Restore Default
atm6 MAC Address:	00:25:86:c7:99:b1	Restore Default
Current PC MAC	00:19:66:80:53:BD	Clone to atm0 🗸
uping		
Note: Only the WAN p with each other.	orts can using MAC Address Clone	e. All the clone MAC Address MUST NOT



Type the new value for the WAN Interface who's MAC Address you want to change, and click **Save/Apply**.

You can select corresponding WAN Interface from the drop-down list and click **Clone** button to clone your current PC MAC, and then click **Save/Apply**.

Click **Restore Default** button to restore the WAN Interface's default MAC Address.

PNote:

Only the WAN Ports can use MAC Address Clone function. All the clone MAC addresses must not be the same with each other.

4.4.5 NAT

NAT (Network Address Translation) allows you to share one WAN (Wide Area Network) IP address for multiple computers on your LAN (Local Area Network).

P Note:

When you select **PPPoA** or **PPPoE** for the WAN Setup, or when you select **Enable NAT** for the type of **IPoA** and **IPoE** connection (<u>4.4.2 WAN Service</u>), you will see the **NAT** menu in the Web-based Utility (shown in Figure 4-24).

Choose "Advanced Setup" \rightarrow "NAT", there are three submenus under the main menu: Virtual Servers, Port Triggering and DMZ Host. Click any of them, and you will be able to configure the corresponding function.

Device Info	NAT Virtual Servers Setup
Quick Setup	
Advanced Setup	
+Layer2 Interface	Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The
• WAN Service	Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.
• LAN	
• MAC Clone	Add Remove
-NAT	
 Virtual Servers 	Server Name External Port Start External Port End Protocol Internal Port Start Internal Port End Server IP Address WAN Interface Remove
 Port Triggering 	
• DMZ Host	
+ Security	

Figure 4-24

4.4.5.1 Virtual Servers

Choose "Advanced Setup" \rightarrow "NAT" \rightarrow "Virtual Servers", you can set up virtual servers on the screen below (shown in Figure 4-25).

Virtual servers can be used for setting up public services on your LAN, such as DNS, Email and FTP. A virtual server is defined as a service port, and all requests from the Internet to this service port will be redirected to the computer specified by the server IP. Any PC that was used for a virtual server must have a static or reserved IP Address because its IP Address may change when using the DHCP function.

Device Info	NAT Virtual Servers Setup													
Quick Setup														
Advanced Setup														
+Layer2 Interface		irtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The												
• WAN Service	configured.	nternal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured												
• LAN	_													
• MAC Clone		Add Remove												
-NAT														
Virtual Servers	Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	Remove					
 Port Triggering 	Mail (SMTP)	25	25	TCP	25	25	192.168.1.222	pppO						
• DMZ Host	1		1		1	1	1	1						
+ Security														
+Parental Control														

Figure 4-25

- > Virtual Server Table: The table indicates the information about the Virtual Server entries.
 - Server Name: This is the name of the Virtual Server. It is exclusive and must be filled in.
 - External Port Start: The base number of External Ports. You can type a service port or leave it blank.
 - External Port End: The end number of External Ports. You can type a service port or leave it blank.
 - Protocol: The protocol used for this application, TCP, UDP, or TCP/UDP.
 - Internal Port Start: The base number of Internal Ports. You can type a service port or leave it blank.
 - Internal Port End: The end number of Internal Ports. You can type a service port or leave it blank.
 - Server IP Address: The IP Address of the PC providing the service application.
 - WAN Interface: The WAN Service Interface providing the service application.
- Add: Click the Add button to add a new entry.

Remove: Select the check box in the table (shown in Figure 4-25) and then click the Remove button, then the corresponding entry will be deleted in the table.

To add a virtual server entry:

1. Click the **Add** button on the preceding screen Figure 4-25, and then you will see the new Virtual Server in the next screen as shown in Figure 4-26.

Device Info			_					
Quick Setup	NAT V	irtual	Serve	ers				
Advanced Setup								
+Layer2 Interface	Select the convic		and onter t	a conver IP adv	droop and cliv	ek "Appl	"Sove" to feeward IP pag	kets for this service to the
•WAN Service	specified server		and enter ti	le server in au	aress and cir	ck Appi	yoave to to ward in pac	Rets for this service to the
• LAN								e as "External Port End". alue as "Internal Port Start'
MAC Clone	Remaining num	-				tena v	vill be set to the same va	aue as internal Port Start
-NAT		Use Inte			38/ppp0	1		
Virtual Servers	Service Name:							
• Port Triggering	⊙ Se	elect a Se	rvice:	Mail (SMTF	²)		*	
• DMZ Host	0 0	ustom Se	rvice:					
+ Security	Ŭ	ver IP Ad		192,168,1		=		
+Parental Control	36	Ver IP Au	uress.	192.168.1.				
+Quality of Service								
+Traffic Control								
+Routing	External Port	Start	Externa	al Port End	Protocol		Internal Port Start	Internal Port End
+DNS	25		25		TCP	*	25	25
• DSL					TCP	*		
• UPnP					TCP	*		
 Interface Grouping 					TCP	~		
LAN Ports					TCP	~		
• IP Sec					TCP	~		
Vireless					TCP	~		
lagnostics					TCP	~		
lanagement			_		TCP	~		
			-		TCP	~		
			_		TCP	*		
		_			TCP	~		
					TUP	×		
					Apply/	Save		
					- Abbialy	Jave		



- 2. Select the Interface which you want to use from the drop-down list.
- 3. Select the service which you want to use from the drop-down list. If the list does not have the service you need, type the name of the custom service in the text box.
- 4. Type the IP Address of the computer in the **Server IP Address** text box.
- 5. Enter the External Port Start, External Port End, Internal Port Start and Internal Port End in the table, and then select the protocol used for this Virtual Server, **TCP**, **UDP** or **All**.
- 6. Click **Save/Apply** to enable virtual server and then you will see your setting as shown in Figure 4-25.

If you select the service from the drop-down list, the External Port Start, External Port End, Internal Port Start, Internal Port End and the Protocol will be added in the table automatically. You only need to enter the Server IP Address for the Virtual Server.

4.4.5.2 Port Triggering

Choose "Advanced Setup" \rightarrow "NAT" \rightarrow "Port Triggering", you can set Port Triggering on the screen (shown in Figure 4-27).

Some applications require that specific ports in the Router's firewall should be opened for access by remote devices. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote device using the triggering ports. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the open ports. A maximum 32 entries can be configured.

Device Info Quick Setup Advanced Setup	NAT Port T	riggerin	g Set	up					
+Layer2 Interface •WAN Service •LAN	Some applications requi dynamically opens up thu- remote party using the "T back to the application or	e 'Open Ports' i riggering Ports	n the firev . The Ro	wall whe uter allov	n an applicati ws the remote	on on the l party fron	LAN initiat h the WAN	es a TCP/UDP conne side to establish nev	ection to a
• MAC Clone	back to the application of	IT THE LAIN SIDE	using the	; open r	ons . A maxin	num 52 er	ines can	be configured.	
-NAT				Add	Remov	/e			
Virtual Servers									
Port Triggering		Trigger			Open				
DMZ Host	Application Name	Destand	Port R	ange	Destand	Port Ra	ange	WAN Interface	Remove
+ Security		Protocol	Start	End	Protocol	Start	End		
+Parental Control	ICQ	TCP	4000	4000	TCP	20000	20059	ррр0	
+Quality of Service									
+ Traffic Control									
+Routing									

Figure 4-27

- > **Port Triggering Table:** The table indicates the information about the Port Triggering entries.
 - Application (Name): This is the name of the Port Triggering. It is exclusive and must be filled.
 - Trigger: It includes the Protocol and the Start and End value of the Trigger Ports.
 - **Open:** It includes the Protocol and the Start and End value of the Open Ports.
 - WAN Interface: The WAN Service Interface setting the Port Triggering.
- > Add: Click the button to add a new entry.
- Remove: Select the check box in the table (shown in Figure 4-27) and then click the Remove button, then the corresponding entry will be deleted in the table.

To add a new Port Triggering:

1. Click the **Add** button in Figure 4-27, and then you will see the new Port Triggering in the next screen as shown in Figure 4-28.

Device Info Quick Setup	NAT	Port	Triggeri	ng								
Advanced Setup												
+Layer2 Interface	-											
• WAN Service			ch as games, v e opened for ac									
• LAN	selecting an existing application or creating your own (Custom application)and click "Save/Apply" to add it.											
MAC Clone	Remaining number of entries that can be configured: 31 Use Interface: pppoe_0_0_38/ppp0 v											
-NAT			Interface:	pppo	e_0_0_38	s/ppp0	*					
Virtual Servers	Application			ICQ			~					
• Port Triggering	 Sel 	lect an app	plication:	lica			×					
• DMZ Host	○ c	ustom app	olication:									
+ Security												
+Parental Control	Talaasa Da	the Character	Talaana Daat	Fad	Tatanan	Destant		Ctout	Onen Dert	Final	0	at a set
+Quality of Service	Trigger Po 4000	ort Start	Trigger Port	End	Trigger F	rotoco	Open Port	Start	Open Port 20059	End	Open Pr TCP	otocol
Traffic Control	4000		4000		TCP	~	20000]	20059			~
Routing]			TCP	
DNS					TCP	~					ТСР	~
DSL					TCP	*					TCP	~
JPnP					TCP	*]			TCP	*
nterface Grouping]			TCP	*]			ТСР	~
AN Ports]			TCP	~]			ТСР	~
		1			TCP	~		1			ТСР	~
IPSec												
• IP Sec Wireless Diagnostics												



- 2. Select the application from the drop-down list. If the list does not have the application that you want, select the **Custom application** radio button, and type the name of the custom application in the text box.
- 3. Enter the **Trigger Port Start**, **Trigger Port End**, **Open Port Start** and **Open Port End** in the table, and then select the **Trigger protocol** and **Open protocol**, **TCP**, **UDP** or **All**.
- 4. Click **Save/Apply** to enable the settings and then you will see you settings as shown in Figure 4-27.

If you select the application from the drop-down list, the External Port Start, External Port End, Internal Port Start, Internal Port End and the Protocol will be added in the table automatically.

4.4.5.3 DMZ Host

Choose "**Advanced Setup**"→"**NAT**"→"**DMZ Host**", you can set up DMZ Host on the screen (shown in Figure 4-29).

The DMZ host feature can make a local host be exposed to the Internet for a special-purpose service, such as online gaming or video conferencing.

Device Info	NAT DMZ Host
Quick Setup	
Advanced Setup	
+Layer2 Interface	The DSL Modem Router will forward IP packets from the WAN that do not belong to any of the applications
• WAN Service	configured in the Virtual Servers table to the DMZ host computer.
• LAN	Enter the computer's IP address and click "Save/Apply" to activate the DMZ host.
• MAC Clone	
-NAT	Clear the IP address field and click "Apply" to deactivate the DMZ host.
Virtual Servers	
• Port Triggering	DMZ Host IP Address: 192.168.1.222
DMZ Host	
+ Security	Save/Apply
+Parental Control	Save/ Apply

Figure 4-29

To add a new DMZ Host:

You can enter the computer's IP address and then click **Save/Apply** to activate the DMZ host you set on this page.

P Note:

DMZ host forwards all the ports at the same time. Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP Address assigned to it because its IP Address may change while using the DHCP function.

4.4.6 Security

Choose "Advanced Setup" \rightarrow "Security", and you will see the security screen including IP Filtering and MAC Filtering (only effective in Bridging mode) submenus.

Device Info	Outgoin	a IP Fil	terina	l Setu	b						
Quick Setup	je nigeni,	,									
Advanced Setup											
+Layer2 Interface	By default, all ou	utgoing IP tr	affic from L	AN is allo	wed, bu	it some IP traffic	can be l	BLOCKED by set	ting up 1	filters.	
• WAN Service											
• LAN	Choose Add or	Remove to	configure c	outgoing If	^o filters.						
• MAC Clone	Filter Name	Protocol	Source /	Address	Mask	Source Port	Dest. A	Address / Mask	Dest.	Port	Remove
+NAT											
-Security											
+IP Filtering					Add	l Remove	n i				
+MAC Filtering					Inde		J				

Figure 4-30

4.4.6.1 IP Filtering

The IP address filtering feature makes it possible for administrators to control user's access to the Internet, which is based on user's IP. The IP address filtering includes **Outgoing** and **Incoming**, the detailed descriptions are provided below.

IP Filtering - Outgoing

Choose "Advanced Setup" \rightarrow "Security" \rightarrow "IP Filtering" \rightarrow "Outgoing", you can configure Outgoing Filtering rules on the screen (shown in Figure 4-31).

The Outgoing IP Filtering feature allows you to control some IP traffic from LAN to access to some specifically addresses. By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters.

Device Info	Outgoin	a IP Fi	Itering Setup					
Quick Setup	- angenne	9	g ootop					
Advanced Setup								
+Layer2 Interface	By default, all o	utgoing IP tr	affic from LAN is allowe	d, but :	some IP traffic	can be <mark>BLOCKED</mark> by sett	ing up filters.	
•WAN Service								
• LAN	Choose Add or	Remove to	configure outgoing IP filf	ters.				
• MAC Clone	Filter Name	Protocol	Source Address / Ma	ask S	Source Port	Dest. Address / Mask	Dest. Port	Remove
+NAT	sendmail- filter	TCP or UDP	192.168.1.222/ 255.255.255.0			210.17.188.204/ 255.255.255.0	25	
-Security			233.233.233.0			200.200.200.0		
-IP Filtering								
Outgoing								
• Incoming		Add Remove						
+MAC Filtering					,			

Figure 4-31

Set up an Outgoing IP Filtering rule:

1. Click the **Add** button in Figure 4-31, and you will see the next screen as shown in Figure 4-32.

Device Info	Add IP Filter Outgo	oina	
Quick Setup			
Advanced Setup			
+Layer2 Interface			affic by specifying a new filter name and
• WAN Service	at least one condition below. All of the take effect. Click 'Save/Apply' to save ar		ilter rule must be satisfied for the rule to
• LAN	Filter Name:	sendmail-filter	1
• MAC Clone			1
+NAT	Protocol:	TCP/UDP 🖌 🗸	
-Security	Source IP address:	192.168.1.222]
-IP Filtering	Source Subnet Mask:	255.255.255.0]
Outgoing	Source Port (port or port:port):]
• Incoming	Destination IP address:	210.17.188.204]
+MAC Filtering	Destination Subnet Mask:	255.255.255.0]
+Parental Control	Destination Port (port or port:port):	25]
+Quality of Service			
+Traffic Control			
+Routing		Save/Apply	
+DNS			

Figure 4-32

- 2. Enter the Filter name for the rule, it is exclusive and must be filled.
- 3. Select the **protocol: TCP/UDP**, **TCP**, **UDP** or **ICMP** in the drop-down list for the connection between the Source IP address and Destination IP address.
- 4. Enter a **Source IP Address** in dotted-decimal notation format and then type the **Source Subnet Mask** and **Source Port** (port or port: port) in the text boxes separately.
- 5. Enter a **Destination IP Address** in dotted-decimal notation format and then type the **Destination Subnet Mask** and **Destination Port** (port or port: port) in the text boxes separately.
- 6. Click **Save/Apply** to save this entry.

When you add an Outgoing IP Filtering entry, you must configure at least one condition on the preceding screen except the Filter name. If you leave the Protocol blank, it means that the rule is effective to all protocols, if you leave the Source IP Address and/or Destination IP Address blank, it suggests that all Source IP Addresses and/or Destination IP Addresses are controlled by the rule, if you leave the Source Port and/or Destination Port blank, it suggests that all Source Ports and/or Destination Port blank, it suggests that all Source Ports and/or Destination Ports blank, it suggests that all Source Ports and/or Destination Port blank, it suggests that all Source Ports and/or Destination Ports are controlled by the rule.

IP Filtering - Incoming

Choose "Advanced Setup" \rightarrow "Security" \rightarrow "IP Filtering" \rightarrow "Incoming", you can configure Incoming Filtering rules on the screen as shown in Figure 4-33.

The Incoming IP Filtering feature allows some IP traffic from WAN to access some local addresses. By default, all incoming IP traffic from the WAN is blocked when the firewall is enabled. However, some IP traffic can be **ACCEPTED** by setting up filters.

Device Info	Incoming	ı IP Filt	erina S	Setup					
Quick Setup		,	•g ·						
Advanced Setup									
+Layer2 Interface		Vhen the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is BLOCKED. However, some IP traffic can be							
• WAN Service	ACCEPTED by s	etting up filter	rs.						
• LAN	Choose Add or	Remove to co	onfigure inc	oming IP filters.					
• MAC Clone				<i>-</i>					
+NAT									
-Security	Filter Name	Interfaces	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove	
-IP Filtering	recvmail-filter	ppp0,br0	TCP or UDP	210.17.188.2047			110		
• Outgoing									
• Incoming									
+MAC Filtering									
+Parental Control				Add	emove				

Figure 4-33

Set up an Incoming IP Filtering rule:

1. Click the **Add** button in Figure 4-33, and then you will see Figure 4-34.

Device Info	Add IP Filter Incom	ing
Quick Setup		
Advanced Setup		
+Layer2 Interface		rule to identify incoming IP traffic by specifying a new filter name and at least one
•WAN Service	condition below. All of the specified cor 'Save/Apply' to save and activate the filt	nditions in this filter rule must be satisfied for the rule to take effect. Click er.
• LAN	Filter Name:	recvmail-filter
• MAC Clone		
+NAT	Protocol:	TCP/UDP
- Security	Source IP address:	210.17.188.204
-IP Filtering	Source Subnet Mask:	255.255.255.0
Outgoing	Source Port (port or port:port):	
• Incoming	Destination IP address:	
+ MAC Filtering	Destination Subnet Mask:	
+Parental Control	Destination Port (port or port:port):	110
+Quality of Service	WAN Interfaces (Configured in Routin	g mode and with firewall enabled only)
+Traffic Control	Select one or more WAN/LAN interface	
+Routing	Select All	
+DNS	✓ pppoe_0_0_38/ppp0	
• DSL	✓ br0/br0	
• UPnP		
 Interface Grouping 		
LAN Ports		Save/Apply

Figure 4-34

- 2. Enter the **Filter name** for the rule, it is exclusive and must be filled in.
- 3. Select **Protocol** in the drop-down list, enter **Source IP address**, **Source Subnet Mask**, **Source Port**, **Destination IP address**, **Destination Subnet Mask**, and **Destination Port** for the rule.
- 4. Select at least one WAN interfaces displayed below to apply this rule.
- 5. Click **Save/Apply** to save this entry.

When you add an Incoming IP Filtering entry, you must configure at least one condition on the preceding screen except the Filter name. If you leave **Protocol** blank, it means that the rule is effective to all protocols, if you leave the Source IP address and/or Destination IP address blank, it suggests that all Source IP addresses and/or Destination IP addresses are controlled by the rule, if you leave the Source Port and/or Destination Port blank, it suggests that all Source Ports and/or Destination Ports blank, it suggests that all Source Ports and/or Destination Ports blank, it suggests that all Source Ports and/or Destination Port blank, it suggests that all Source Ports and/or Destination Ports are controlled by the rule.

4.4.6.2 MAC Filtering

Choose "Advanced Setup" \rightarrow "Security" \rightarrow "MAC Filtering", you can configure MAC Filtering rules on the screen as shown in Figure 4-35. The section allows you to control access to the Internet by users on your local network based on their MAC Address.

P Note:

MAC Filtering is only effective on ATM PVC(s) configured in Bridging mode.

vice Info	MAC Fil	tering S	etup					
Setup								
Setup								
ice								
e				d in Bridge mode. FORW of the specified rules in th				
				natching with any of the s				
	MAC Filtering	2		n interface will cause al	I defined rules for that in	terface to be		
				e new rules for the new p		terrace to be		
g	Interface		Policy		Change			
	atm0		FORWARD					
/ice	atm1		FORWARD					
d								
	atm2		FORWARD					
	atm3		FORWARD					
	atm4		FORWARD					
ping								
	atm5		FORWARD					
	atm6		FORWARD					
	1		1		1			
			C	hange Policy				
	Choose Add o	or Remove to a	onfigure MAC filtering r	ules.				
	Interface	Protocol	Destination MAC	Frame Direction	Remove			
	atm0	IGMP	00:11:22:33:44:AA	вотн				
	1	1	1	1	1			
			Ac	ld Remove				



- Change Policy: There are two policies for the MAC filters: FORWARDED and BLOCKED. Select the Change checkbox and click the Change Policy button to change from one policy to another. When you set FORWARDED, it means that all MAC layer frames will be forwarded except those matching with any of the specified rules in the table (shown in Figure 4-35). While BLOCKED means that all MAC layer frames will be blocked except those matching with any of the specified rules in the preceding table.
- Add: Click the Add button, and then you can add a new MAC Filter in the next screen (shown in Figure 4-35).
- Remove: Select the check box in the table (shown in Figure 4-35) and then click the Remove button, and then the corresponding entry will be deleted in the table.

To add a MAC Filtering rule:

1. Click the **Add** button in Figure 4-35, and you will see the next screen similar to in Figure 4-36.

Device Info Quick Setup	Add MAC Filter
Advanced Setup	
+Layer2 Interface	
• WAN Service	Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click "Apply" to save and activate the filter.
• LAN	specified, an ormerintane effect. Onco, Apply to save and activate the lifter.
MAC Clone	Protocol Type: IGMP
+NAT	
- Security	Destination MAC Address: 00:11:22:33:44:AA
+IP Filtering	Source MAC Address: 00:11:22:33:44:BB
-MAC Filtering	Frame Direction: LAN<=>WAN v
+Parental Control	WAN Interfaces (Configured in Bridge mode only) br_0_0_32/atm0
+Quality of Service	
+Traffic Control	
+Routing	Save/Apply

Figure 4-36

- 2. Select **Protocol Type** in the drop-down list for the rule.
- 3. Enter **Destination MAC Address** and **Source MAC Address** in the text box.
- 4. Select Frame Direction in the drop-down list for the rule.
- 5. Select the **WAN interfaces** from the drop-down list.
- 6. Click **Save/Apply** to save this entry and then you will see your settings as shown in Figure 4-35.

4.4.7 Parental Control

Choose "Advanced Setup" \rightarrow "Parental Control". You can configure the Parental Control on the screen as shown in Figure 4-37. Time Restriction allows you to control the Internet activities of the child by restricting the time of surfing. URL Filter limits every computer connected to the router to access certain websites. These two features work independently.

Device Info	Access T	ime R	estric	tion	A m	naxim	num	16 e	entrie	s can	be co	onfigured.
Quick Setup												
Advanced Setup												
+Layer2 Interface												
• WAN Service	Username	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove
• LAN			1	1		1	1	1	1	1	1	
• MAC Clone												
+NAT					Ac	id Re	emove					
+ Security					_							
-Parental Control												

Figure 4-37

4.4.7.1 Time Restriction

This feature allows you add time of day restriction to a special LAN device connected to the Router.

Device Info	Access	Time Restrict	ion	Am	axim	um	16 e	entri	ies c	an b	e cor	nfigured.
Quick Setup	/100000				a, iii							ingaroar
Advanced Setup												
+Layer2 Interface												
• WAN Service	Username	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove
• LAN	child 1	00:11:22:33:44:CC	x	x	x	x	x			18:0	21:0	
• MAC Clone												
+ NAT												
+ Security				Ad	d Re	emove	1					
-Parental Control							J					
Time Restriction												

Figure 4-38

To add a Time Restriction entry:

1. Click the **Add** button in Figure 4-38, and then you will see the next screen as shown in Figure 4-39.

Device Info Quick Setup Advanced Setup +Layer2 Interface • WAN Service • LAN	Time of Day This page adds time of automatically displays t click the "Other MAC Ad of a Windows based PC	day restric he MAC ad dress" butt	tion to a sp Idress of th ton and ent	ie LAN dev er the MAC	ice where t address c	he brows of the othe	er is runnii	ng. To res	strict other LAN device,
• MAC Clone • NAT • Security - Parental Control		User Name: child_1 Browser's MAC Address MAC Address: 40.61:86:FC:74:93							
• Time Restriction • URL Filter	Other MAC Address Other MAC Address(xx		xx:xx):	00:11:2	2:33:44:CC	;			1
+Quality of Service	Days of the week: Click to select:	Mon	Tue	Wed	Thu	Fri	Sat	Sun	
+Traffic Control	Start Blocking Time (hl		18:00	V					
+Routing +DNS •DSL	End Blocking Time (hl		21:00						
+ UPnP + Interface Grouping				Sa	ave/Apply				



- 2. Enter the User Name of the LAN device connected to the Router.
- To restrict the device where the browser is running, select the Browser's MAC Address radio button. The MAC Address has been automatically displayed in the text box. To restrict other LAN devices, click Other MAC Address radio button and enter the MAC address of the other LAN device.
- 4. Select the day to allow the rule to take effect in the table.
- 5. Enter the **Start Blocking Time** and **End Blocking Time** in the text box separately, and then the device controlled will then be unable to connect to the internet during that time.
- 6. Click **Save/Apply** to save this entry and then you will see your settings as shown in Figure 4-38.

The Time Restriction will not work correctly before the time of the device is set in "Management → Internet Time".

4.4.7.2 URL Filter

This feature allows you to configure the filter rules based on URL to control all the computers in the LAN to access the specified port, and it is independent with Time Restriction feature.



There are two policies for the URL Filter.

- **Exclude**: Block the PCs to access the specified URL.
- > Include: Only allow the PCs to access the specified URL.
- > **Disable**: URL Filter function will not take effect.

To add a URL Filter entry:

- 1. Check the **Exclude** or **Include** radio button. Here we take **Exclude** for example.
- 2. Click the **Add** button in Figure 4-40 and then you will see the next screen as shown in Figure 4-41. Enter the URL Address and Port Number.

Device Info	Parental Control	- URL Filter Add	1
Quick Setup			-
Advanced Setup			
+Layer2 Interface	Enter the URL address and port	number then click "Save/Appl	ly" to add the entry to the URL filter.
• WAN Service			_
• LAN	URL Address:	www.google.com	
• MAC Clone	Port Number:	80	(Default 80 will be applied if leave blank.)
+NAT			
+ Security			
-Parental Control		Save/App	ly
 Time Restriction 			
• URL Filter			

Figure 4-41

3. Click **Save/Apply** to save this entry and then you will see your settings as shown in Figure 4-40. Every computer connected to the router will not access this URL address on the port.

4.4.8 Quality of Service

Choose "Advanced Setup" \rightarrow "Quality of Service", you can enable QoS (Quality of Service) on the screen shown in Figure 4-42. 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 priority. This is useful when there are certain types of data you want to give higher priority, such as voice data packets give higher priority than Web data packets. This option will provide better service of selected network traffic over various technologies.

Device Info	QoS Queue Management Configuration
Quick Setup	
Advanced Setup	
+Layer2 Interface	If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without
• WAN Service	reference to a particular classifier. Click 'Apply/Save' button to save it. Note: If Enable Oos checkbox is not selected, all OoS will be disabled for all interfaces.
• LAN	Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.
• MAC Clone	· · · · · · · · · · · · · · · · · · ·
+NAT	🗹 Enable QoS
+ Security	Select Default DSCP Mark: No Change (-1)
+Parental Control	
-Quality of Service	
• Queue Config	Save/Apply

Figure 4-42

Select the **Enable QoS** checkbox to enable all QoS for all interfaces.

Select a **Default DSCP make** from drop-down list to automatically mark incoming traffic without reference to a particular classifier.

Click **Save/Apply** to save the current configuration.

P Note:

The default DSCP mark is used to mark all egress packets that do not match any classification rules.

4.4.8.1 Queue Config

Choose "Advanced Setup"→"Quality of Service"→"Queue Config", you can set up virtual servers on the screen below.

Quick Setup								
Advanced Setup								
+Layer2 Interface	If you disable WMM fu					II not take effects		
WAN Service	The QoS function has	s been (
• LAN	Name	Key	Interface	Precedence	DSL Latency	PTM Priority	Enable	Remov
MAC Clone	WMM Voice Priority	1	wI0	1			Enabled	
+NAT	WMM Voice Priority	2	wI0	2			Enabled	
+ Security	WMM Video Priority	3	wI0	3			Enabled	
+Parental Control	WMM Video Priority	4	wI0	4			Enabled	
-Quality of Service	WMM Best Effort	5	wl0	5			Enabled	
Queue Config	WMM Background	6	wI0	6			Enabled	
QoS Classification	WMM Background	7	wI0	7			Enabled	
+Traffic Control	WMM Best Effort	8	wI0	8			Enabled	
+Routing								
+DNS								
• DSL								

Figure 4-43

Click the **Add** button in Figure 4-43, and you can configure the QoS queue entry on the next screen as shown in Figure 4-44.

Device Info	QoS Queue Conf	iguration
Quick Setup		
Advanced Setup		
+Layer2 Interface		ure a QoS queue entry and assign it to a specific network interface. Each of the
• WAN Service	queues can be configured for a : to place ingress packets approp	specific precedence. The queue entry configured here will be used by the classifier riately.
• LAN	Note: Lower integer values for j	precedence imply higher priority for this queue relative to others.
• MAC Clone	Click 'Apply/Save' to save and ac	tivate the queue.
+NAT		
+ Security	Name:	queue1
+Parental Control	Enable:	Disable 😽
-Quality of Service	Interface:	ррр0(0_0_38) 🐱
Queue Config	Precedence:	3 🗸
 QoS Classification 	DSL Latency:	Path0 🗸
Traffic Control		
+ Routing		
+DNS		Save/Apply

Figure 4-44

- > Name: Set a name for the entry.
- **Enable**: Select Enable option to take this entry effect.
- > Interface: Assigned a specific Wan Service for this QoS queue entry.
- > **Precedence**: Specify precedence for this QoS queue entry.
- DSL Latency: Select latency path for the type of data transmission, only Path0 is available for this Router.

After you specify the condition, click **Save/Apply** to save the entry and then you will see you settings as shown in Figure 4-43.

- 1) Lower integer values for precedence imply higher priority for this queue relative to others.
- 2) The queue entry configured here will be used by the classifier to place ingress packets appropriately.

4.4.8.2 QoS Classification

This section will guide you to create a traffic class rule to classify the upstream traffic, assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP byte.

A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect.

Quick Setup	400 0.0	551110	ation	ootap		ım 32 entri	ob our b	e comig	ai e a.									
dvanced Setup																		
.ayer2 Interface																		
WAN Service	Choose Add or					o wireless will not ta	to effecte											
LAN	If you disable vi	MM NUNCS	ion in wires	433 (*934, c18)	sincason related a	o wireless will not ta	Na eserta											
MAC Clone								ION CRITERIA						CLASSIFICA	TION RESULTS	\$		
NAT	Class Name	Örder	Class Intf	Ether Type	SecMAC/ Mask	DstMAC/ Mask	SrclP/ Mask	DatlP/ Mask	Proto S	re Port Dat P	at DSCP Chec	802.1P Check	Queue Key	DSCP Mark	802.1P Mark	Vianit Tag	Enable	Remove
in curity			Clark IIII	carer rype				Cont / Ender		and the part	in both since		ausac ney		Startt Batt	think rug		
arental Control	ftp-class	1. J.				00:11:22:33:44:AA							34	AF12			2	
uality of Service																		
Queue Config																		
GoS Classification									-									
Routing								Ad	d Ena	ble Remov	1.5							

Figure 4-45

Click the Add button Figure 4-45, and you can configure the QoS on the next screen.

and the interface and optional	ass rule to classify the u lly overwrite the IP head specified conditions in	upstream traffic, assign queue which de er DSCP byte. A rule consists of a class this classification rule must be satisfier	name and at least
P Interface Service The screen creates a traffic cl and the interface and optional one condition below. All of the effect. Click 'Save/Apply' to sav ity tal Control Rule Order: Pule Status:	lly overwrite the IP heads e specified conditions in /e and activate the rule. ftp-class Last	er DSCP byte. A rule consists of a class	name and at least
Service The screen creates a traffic cl and the interface and optional one condition below. All of the effect. Click 'Save/Apply' to sav ity Traffic Class Name: tal Control Rule Order: Rule Status:	Ily overwrite the IP heads e specified conditions in /e and activate the rule. ftp-class Last	er DSCP byte. A rule consists of a class	name and at least
and the interface and optional one condition below. All of the effect. Click 'Save/Apply' to sav Traffic Class Name: tal Control Rule Order:	Ily overwrite the IP heads e specified conditions in /e and activate the rule. ftp-class Last	er DSCP byte. A rule consists of a class	name and at least
ity tal Control One Condition below. All of the effect. Click 'Save/Apply' to sav	specified conditions in ve and activate the rule. ftp-class Last		
ty Traffic Class Name: Rule Order:	ftp-class Last		
r Rule Order: I Control Rule Status:	Last 🗸		
ontrol Rule Order:	Last 🗸		
trol			
Rule Status:	Enable 🐱		
ervice			
onfig Specify Classification C	riteria		
A blank criterion indicates it is	not used for classificati	on.	
trol Class Interface:		*	
Ether Type:		*	
Source MAC Address:			
Source MAC Mask:			
Destination MAC Address:	00:11:22:33:44	I:AA	
Destination MAC Mask:			
Specify Classification R	lesults		
Must select a classification qu	Jeue. A blank mark or ta	a value means no change.	
	ssification Queue:	ppp0&Prec3&Path0	*
Mark Differentiated Service (Code Point (DSCP):	AF12(001100)	*
Mark 802.1p priority:		*	
Tag VLAN ID [0-4094]:			
103 VEALD [0-4034].			
		we/Apply	

Figure 4-46

After you specify the condition, click **Save/Apply** to save the entry.

4.4.9 Traffic Control

Choose "Advanced Setup" \rightarrow "Traffic Control" and then you will see the screen as shown in Figure 4-47. This page allows you to enable this function and to configure the value of Egress/Ingress Total Rate.

Device Info Quick Setup	TC Traffic Control
Advanced Setup	
+Layer2 Interface	The Egress/Ingress Total Rate must be configured here; otherwise TC rules can not be added. The recommanded Ingress/Egress Total Rate is Line Upstream/Downstream Rate. Click 'Apply/Save' button to save it.
• WAN Service	Note:
• LAN	If Enable checkbox is not selected, all TC rules will be disactived. Make sure that Ingress/Egress Total Rate is not greater than Line Upstream/Downstream Rate, otherwise TC rules will not take effect.
• MAC Clone	
+NAT	Enable
+ Security	
+Parental Control	Egress Total Rate (Kbps): 0 Line Rate - Upstream (Kbps):
+Quality of Service	Ingress Total Rate(Kbps): 0 Line Rate - Downstream (Kbps):
-Traffic Control	
 Traffic Control Rule 	
+Routing +DNS	Save/Apply

Figure 4-47

- **Enable**: Check this box to enable the Traffic Control function.
- > Egress Total Rate (Kbps): Enter the upload speed through the WAN port.
- > Ingress Total Rate (Kbps): Enter the download speed through the WAN port.
- > Line Rate-Upstream (Kbps): This field displays the upload speed assigned by your ISP.
- Line Rate-Downstream (Kbps): This field displays the download speed assigned by your ISP.
- Save/Apply: Click this button to make the configuration take effect.

Solution Note:

- 1) The Egress Total Rate and Ingress Total Rate are required to be configured. Otherwise TC rules cannot be added.
- 2) Only when the Router is configured to work in DSL connection does the Line Rate field display the upload/download speed assigned by your ISP. Otherwise there will be empty.

4.4.9.1 Traffic Control Rule

Choose "Advanced Setup" \rightarrow "Traffic Control" \rightarrow "Traffic Control Rule" and then you will see the screen as shown in Figure 4-48. This page allows you to view and configure TC rules.

TC rule list										
TO THE ISC										
Choose Add, Remove, Enable or	Edit to configure Traff	fic Control rul	es.							
Key IP Address	Protocol	Port	Precedence		ate (Kbps)	Ingress F	late (Kbps)	Enable	Edit	Remove
in Address	FIGUE	Port	riecedence	Min	Max	Min	Max	Chable	Cult	Nemove
				Fachia Dara						
			Add	Enable Rem	ove					
	TC rule list Choose Add, Remove, Enable of Key IP Address	Choose Add, Remove, Enable or Edit to configure Trat	Choose Add, Remove, Enable or Edit to configure Traffic Control ru	Choose Add. Remove, Enable or Edit to contigure Traffic Control rules. Key IP Address Protocol Port Precedence	Choose Add, Remove, Enable or Edit to configure Traffic Control rules. Key IP Address Protocol Port Precedence Egress R	Choose Add. Remove. Enable or Edit to configure Traffic Control rules. Key IP Address Protocol Port Precedence Egress Rate (Kbps)	Choose Add, Remove, Enable or Edit to configure Traffic Control rules. Key IP Address Protocol Port Precedence Egress Rate (Kbps) Ingress R	Choose Add. Remove, Enable or Edit to configure Traffic Control rules. Key IP Address Protocol Port Precedence Egress Rate (Kbps) Ingress Rate (Kbps) Min Max Min Max	Choose Add. Remove. Enable or Edit to contigure Traffic Control rules. Key IP Address Protocol Port Precedence Egress Rate (Kbps) Ingress Rate (Kbps) Enable	Choose Add. Remove, Enable or Edit to contigure Traffic Control rules. Key IP Address Protocol Port Precedence Egress Rate (Kbps) Ingress Rate (Kbps) Enable Edit

Figure 4-48

To add a TC rule, click the **Add** button and you can configure it in the screen as shown in Figure 4-49.

Device Info	The screen allows you to configure a TC rule entry. Each of the rules can be configured for a specific precedence. The rule entry configured
Quick Setup	here will be used to control the rates of ingress and egress packets.
Advanced Setup	Note: Min Egress/Ingress Rates must not be empty and not less than 10 Kbps. Max Egress/Ingress Rate should not be greater than the Egress/Ingress Total Rate, if empty or greater than the Egress/Ingress
+Layer2 Interface	Total Rate, the actual value will be set with Egress/Ingress Total Rate.
• WAN Service	Click 'Save/Apply' to save and activate the rule.
• LAN	
• MAC Clone	Rule Status: Enable 🗸
+NAT	
+ Security	IP Range: 192.168.1.101 - 192.168.1.103
+Parental Control	Port Range: 80 -
+Quality of Service	Protocol: TCP 🗸
-Traffic Control	
Traffic Control Rule	Precedence: Medium 🗸
+Routing	
+DNS	Min Rate (Kbps) Max Rate (Kbps)
• DSL	Egress Rate: 100 200
• UPnP	Ingress Rate: 400 800
 Interface Grouping 	
LAN Ports	
• IP Sec	Save/Apply

Figure 4-49

- **Rule Status**: Select the status of the rule from the drop-down list to enable or disable the rule.
- > **IP Range**: Enter a single IP address or a range of IP addresses.
- > **Port Range**: Enter a single port or a range of ports.
- Protocol: Select a protocol type from the drop-down list. TCP, UDP and ALL are available here.
- Precedence: Select precedence form the drop-down list. There are five options: Highest, High, Medium, Low and Lowest. The default precedence of the rule is Medium.
- > Egress Rate: Enter the min and max upload speed through the WAN port.
- > Ingress Rate: Enter the min and max download speed through the WAN port.

After completing the above configuration, click the **Save/Apply** button to make it take effect and then you will see the following list as shown in Figure 4-50. If you want to modify the rule, click the **Edit** button. If you want to delete the rule, check the **Remove** box first and then click the **Remove** button.

Device Info Quick Setup Advanced Setup	TC r	ule list										
+Layer2 Interface •WAN Service	Choose	Add, Remove, Enable or Edit to configure Traffic C	ontrol rules.									
+ LAN	Key	Lev IP Address Protocol Port Precedence Egress Rate (Kbps) Ingress Rate (Kbps)					Rate (Kbps)	Enable	Edit	Remove		
MAC Clone	ney	IF Address	PIOLOCOI POI	For	Frecedence	Min	Max	Min	Max	Chable	con	Remove
+NAT	1	192.168.1.101-192.168.1.103	TCP	80	Medium	100	200	400	1000	V	Edit	
+ Security												
+Parental Control												
+Quality of Service												
-Traffic Control					Add Enable	Remove						
Traffic Control Rule												

Figure 4-50

P Note:

The precedence, max egress/ingress rate and min egress/ingress rate work on allocation of surplus upload/download bandwidth. For rules with different precedence, the surplus bandwidth is firstly allocated to the rule with the highest precedence according to its max egress/ingress rate. If

there still has surplus bandwidth, it is allocated to the rule with hypo-high precedence. For rules with the same precedence, the surplus bandwidth is allocated to them according to their min egress/ingress rate. The greater a rule's min egress/ingress rate is, the more bandwidth it gets.

4.4.10 Routing

Choose "Advanced Setup"→"Routing", it includes three menus: Default Gateway, Static Route and RIP (shown in Figure 4-51). The detailed descriptions are provided below.

Device Info	Routing Default Gateway
Quick Setup	riouning Doluan Outomay
Advanced Setup	
+Layer2 Interface	
• WAN Service	Select a preferred wan interface as the system default gateway.
• LAN	Note: No configured WAN interface existed for system default gateway.
• MAC Clone	✓ Auto Gateway
+NAT	Auto Gateway
+ Security	
+Parental Control	Save/Apply
+Quality of Service	Save/Appiy
+Traffic Control	
-Routing	
Default Gateway	
Static Route	
• RIP	

Figure 4-51

4.4.10.1 Default Gateway

Choose "Advanced Setup" \rightarrow "Routing" \rightarrow "Default Gateway", you can see the Default Gateway screen. Deselect the checkbox before Auto Gateway, and then you will be able to select a WAN Interface from the drop-down list as the system default gateway. The Auto Gateway checkbox is selected by default.

Device Info	Routing Default Gateway
Quick Setup	Roading Donadic Calorray
Advanced Setup	
+Layer2 Interface	
• WAN Service	Select a preferred wan interface as the system default gateway.
• LAN	
• MAC Clone	Auto Gateway
+NAT	Selected WAN Interface pppoa_0_0_38/pppoa0 🗸
+ Security	
+Parental Control	
+Quality of Service	Save/Apply
+Traffic Control	
-Routing	
Default Gateway	
Static Route	

Figure 4-52

- 1) If changing the Automatic Assigned Default Gateway from unselected to selected, you have to reboot the Router to get the automatically assigned default gateway.
- 2) Default Gateway IP address should be specified since MER Interface is selected when you select the **Enable automatic Assigned Default Gateway** check box.

4.4.10.2 Static Route

Choose "Advanced Setup" \rightarrow "Routing" \rightarrow "Static Route". You can see the Static Route screen, this screen allows you to configure the static routes (shown in Figure 4-53). A static route is a pre-determined path that network information must travel to reach a specific host or network.

Quick Setup 🔥					
Advanced Setup	Routing S	static Route (A m	aximum 32 e	ntries can l	be configured)
+Layer2 Interface					
• WAN Service					
• LAN					
MAC Clone	Destination	Subnet Mask	Gateway	Interface	Remove
+NAT					
+ Security					
+Parental Control		A	dd Remove		
+Quality of Service					
+Traffic Control					
-Routing					
• Default Gateway 🗧					
Static Route					

Figure 4-53

To add static routing entries:

1. Click the Add button in Figure 4-53, and you will see the screen as shown in Figure 4-54.

Quick Setup	
Advanced Setup	Routing Static Route Add
+Layer2 Interface	
• WAN Service	
• LAN	Enter the destination petwork address, subset mask, actaway AND/OD sublished WAN interface than slick "Sour/Apply
• MAC Clone	Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Save/Apply to add the entry to the routing table.
+NAT	
+ Security	Destination Network Address: 210.17.155.203
+Parental Control	Subnet Mask: 255.255.255.0
+Quality of Service	Use Interface: pppoe_0_0_38/ppp0 v
+Traffic Control	
-Routing	· · · · · · · · · · · · · · · · · · ·
 Default Gateway 	Save/Apply
Static Route	

Figure 4-54

- 2. Enter the following data:
- Destination Network Address: The Destination Network Address is the address of the network or host that you want to assign to a static route.
- Subnet Mask: The Subnet Mask determines which portion of an IP Address is the network portion, and which portion is the host portion.

- Use Interface: Select the Interface name in the text box, or else, the default Use Interface will be adopted for the Static Route.
- Use Gateway IP Address: If you select the IPoE or IPoA mode for Use Interface, the screen above will display this item, you should type the Gateway address correctly, and the other option for Use Interface will adopt the default Gateway address for the Static Route.
- 3. Click **Save/Apply** to and then you will see you settings as shown in Figure 4-53.

To remove a static routing entry:

- 1. Select the **Remove** check box according to the entry in the Figure 4-53.
- 2. Click the **Remove** button, and the entry will be deleted.

PNote:

Gateway IP address should be correctly configured if IP based Interface (IPoE, IPoA) is selected.

4.4.10.3 RIP

Choose "Advanced Setup" \rightarrow "Routing" \rightarrow "RIP", you can see the RIP (Routing Information Protocol) screen which allows you to configure the RIP (shown in Figure 4-55).

Quick Setup						
Advanced Setup	Routing	RIP Configurati	on			
+Layer2 Interface						
• WAN Service						
• LAN	NOTE: RIP CANNO	T BE CONFIGURED on the \	NAN interface which has NAT enable	d (such as PPPoE)		
 MAC Clone 						
+NAT		To activate RIP for the WAN Interface, select the desired RIP version and operation and place a check in the 'Enabled' checkbox. To stop RIP on the WAN Interface, uncheck the 'Enabled' checkbox. Click the 'Save/Apply' button to star/stop				
+ Security	RIP and save the co					
+Parental Control			Operation			
+Quality of Service	Interface	Version	Enabled			
+ Traffic Control	atm0	2 🗸	Passive 🐱			
-Routing	atm1	2 🗸	Passive 🗸			
• Default Gateway 🚆						
Static Route	atm2	2 🗸	Passive 💙			
• RIP	atm3	2 🗸	Passive 🗸			
+DNS	atm4	2 ~	Passive V			
• DSL	aun4	2 2	Passive			
• UPnP	atm5	2 🗸	Passive 🐱			
 Interface Grouping 	atm6	2 🗸	Passive 🗸			
LAN Ports						
• IP Sec						
Wireless		_	O /A h			
Diagnostics			Save/Apply			

Figure 4-55

P Note:

RIP cannot be configured on the WAN Interface which has NAT enabled (such as PPPoE).

To activate RIP for the device, configure an individual interface, select the desired RIP version and operation, and select **Enabled** checkbox for the interface.

Click **Save/Apply** to save the configuration.

4.4.11 DNS

When you select the connection type **PPPoE**, **PPPoA** or **IPoA** for WAN configuration, you will see the **DNS** menu in the Web-based Utility (shown in Figure 4-56). It includes **DNS Server** and **Dynamic DNS** submenus.

Device Info	DNS Server Configuration
Quick Setup	DNS Server Comgulation
Advanced Setup	
+Layer2 Interface	Select the configured WAN interface for DNS server information OR enter the static DNS server IP Addresses for single
• WAN Service	PVC with IPoA, static IPoE protocol.
• LAN	El Auto DNS Sector
• MAC Clone	Auto DNS Server
+NAT	
+ Security	Apply/Cave
+Parental Control	Apply/Save
+Quality of Service	
+Traffic Control	
+Routing	
-DNS	
DNS Server	
Dynamic DNS	

Figure 4-56

4.4.11.1 DNS Server

Choose "Advanced Setup" \rightarrow "DNS" \rightarrow "DNS Server", and you can see the DNS Server Configuration screen. Deselect the checkbox before Auto DNS Server, and then you will be able to manually configure the DNS Server Addresses as shown in Figure 4-57.

Device Info	DNS Server Configuration
Quick Setup	Bito conver configuration
Advanced Setup	
+Layer2 Interface	Select the configured WAN interface for DNS server information OR enter the static DNS server IP Addresses for single
• WAN Service	PVC with IPoA, static IPoE protocol.
• LAN	Auto DNS Server
• MAC Clone	
+NAT	Obtain DNS info from a WAN interface:
+ Security	WAN Interface selected: pppoe_0_0_38/ppp0 🗸
+Parental Control	
+Quality of Service	Use the following Static DNS IP address:
+Traffic Control	Primary DNS server:
+Routing	Secondary DNS server:
-DNS	
DNS Server	
Dynamic DNS	Apply/Save
• DSL	



For PPPoA, PPPoE enabled PVC(s), please select the **Obtain DNS info from a WAN interface** checkbox, this Router will accept automatically the first received DNS assignment from the selected configured WAN interface during the connection establishment.

For single PVC with IPoA, static IPoE protocol, please select the **Use the following Static DNS IP address** checkbox, and enter the primary and /or optional secondary DNS server IP addresses provided by your ISP.

Click the **Apply/Save** button to save the new configuration.

4.4.11.2 Dynamic DNS

Choose "Advanced Setup" \rightarrow "DNS" \rightarrow "Dynamic DNS", you can see the Dynamic DNS screen, this screen allows you to configure the Dynamic DNS (shown in Figure 4-58).

The Router offers a Dynamic Domain Name System (**DDNS**) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP Address. The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your Router to be more easily accessed from various locations on the Internet.

Device Info	Dynamic DNS						
Quick Setup	-						
Advanced Setup							
+Layer2 Interface	The Dynamic DNS service allo						
•WAN Service	allowing your DSL Modem Ro	uter to be more easily acces	ssed from various	locations on the Int	ernet.		
• LAN	Choose Add or Remove to cor	nfigure Dynamic DNS.					
• MAC Clone							
+NAT	Hostname	Username	Service	Interface	Remove		
+ Security	Alsbot.homeunix.net	Alsbot.homeunix.net ailisa dyndns ppp0					
+Parental Control							
+Quality of Service							
+Traffic Control			Remove				
+Routing		Add Remove					
-DNS							
DNS Server							
Dynamic DNS							

Figure 4-58

To add a DDNS entry:

1. Click the **Add** button (pop-up Figure 4-58), and then you will set the DDNS in the next screen (shown in Figure 4-59).

Device Info	Add dynamic DNS	5
Quick Setup		
Advanced Setup		
+Layer2 Interface	This page allows you to add a Dy	namic DNS address from DynDNS.org or TZO.
• WAN Service		
• LAN	D-DNS provider:	DynDNS.org
• MAC Clone		
+NAT	Hostname:	Alsbot.homeunix.net
+ Security	Interface:	pppoe_0_0_38/ppp0 🖌
+Parental Control		
+Quality of Service	DynDNS Settings	
+Traffic Control	Username:	ailisa
+Routing	Password:	•••••
-DNS		
DNS Server		
Dynamic DNS		Save/Apply
		·

Figure 4-59

- 2. Select **D-DNS provider** in the drop-down list.
- 3. Enter the **Hostname** of the DNS Server, and select the corresponding **Interface** for the DDNS, you can leave it default.
- 4. Type the **User Name** and **Password** for your DDNS account.
- 5. Click **Save/Apply** to save the entry and then you will see your settings as shown in Figure 4-58.

4.4.12 DSL

Choose "Advanced Setup" \rightarrow "DSL", you can see the DSL Settings screen, this screen allows you to configure the DSL (shown in Figure 4-60).

Device Info	DSL Settings
Quick Setup	
Advanced Setup	
+Layer2 Interface	Select the modulation below
WAN Service	G.Dmt Enabled
• LAN	G.lite Enabled
MAC Clone	▼ T1.413 Enabled
+NAT	—
+ Security	ADSL2 Enabled
+Parental Control	AnnexL Enabled
+Quality of Service	ADSL2+ Enabled
+Traffic Control	AnnexM Enabled
+Routing	
+DNS	
• DSL	
• UPnP	Select the phone line pair below
 Interface Grouping 	 Inner pair
LAN Ports	Outer pair
• IP Sec	
Wireless	
Diagnostics	Capability
Management	
	V Bitswap Enable
	SRA Enable
	Save/Apply Advanced Settings

Figure 4-60

You can select the modulation type, phone line pair and the capability of Bitswap or SRA. After you set them up, click **Save/Apply** to save the configurations.

4.4.13 UPnP

Choose "**Advanced Setup**"→"**UPnP**", you can Enable or Disable the UPnP (Universal Plug and Play) protocol on the screen.

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

Device Info	UPnP Configuration
Quick Setup	
Advanced Setup	
+Layer2 Interface	
•WAN Service	Enable UPnP protocol.
• LAN	
• MAC Clone	
+NAT	Save/Apply
+ Security	
+Parental Control	
+Quality of Service	
+Traffic Control	
+Routing	
+DNS	
•DSL	
• UPnP	

Figure 4-61

Select the checkbox and click **Save/Apply** to enable the UPnP function.

4.4.14 Interface Grouping

Choose "Advanced Setup"→"Interface Grouping", you can configure multiple ports to PVC and bridging groups to perform as an independent network.

Device Info	Interface (Prouping	A maximi	um 16 entries c	an be configure
Quick Setup	interface	stouping		in to entries t	an be configure
Advanced Setup					
+Layer2 Interface					
• WAN Service					will perform as an independe LAN and WAN interfaces using
• LAN	the Add button. The	e Remove buttor	n will remove the group		d interfaces to the Default grou
• MAC Clone	Only the default gro	oup has IP interf	ace.		
+NAT	Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs
Security	Group Name	Remove			DHCP Vendor IDs
Parental Control			atm0	LAN(1-4)	
Quality of Service			atm1	Wireless0	
Traffic Control			atm2	Wireless0_Guest1	
Routing	Default		atm3	Wireless0_Guest2	
DNS	Dordan		atm4	Wireless0_Guest3	
DSL			atm5		
UPnP			atm6		
Interface Grouping			ррр0		
LAN Ports	<u>.</u>				
IPSec					
Vireless					
liagnostics			Add	Remove	

Figure 4-62

To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the **Add** button. The **Remove** button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

To create a new interface group:

1. Click the **Add** button. You can add a new interface group in the next screen.

Device Info Quick Setup Advanced Setup	Interface grouping Configuration
+Layer2 Interface •WAN Service •LAN •MAC Clone +NAT	To create a new interface group: 1. Enter the Group name and the group name must be unique and select either 2. (dynamic) or 3. (static) below: 2. If you like to automatically add LAN clients to a WAN Interface in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.
+ Security + Parental Control + Quality of Service + Traffic Control	3.Select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. Note that these clients may obtain public IP addresses
+Routing +DNS +DSL	4. Click Save/Apply button to make the changes effective immediately IMPORTANT If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.
• UPnP • Interface Grouping • LAN Ports • IPSec Wireless	Group Name: WAN Interface used in the grouping: br_0_0_32/atm0 v Grouped LAN Interfaces Available LAN Interfaces
Diagnostics Management	Wireless0 Wireless0_Gue Wireless0_Gue Wireless0_Gue
	Automatically Add Clients With the following DHCP Vendor IDs:
	Save/Apply

Figure 4-63

- 2. Enter a unique name for Group.
- 3. Select the Interface which you want to use from the drop-down list.

P Note:

If you like to automatically add LAN clients to a WAN Interface in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.

4. Select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports.

P Note:

These clients may obtain public IP addresses.

5. Click **Save/Apply** to make the entry effective immediately.

P Note:

If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.

4.4.15 LAN Ports

Choose "Advanced Setup"→"LAN Ports", you can Enable/Disable the Virtual LAN Ports feature by selecting the checkbox on the screen.

Device Info	LAN Ports Configuration
Quick Setup	
Advanced Setup	
+Layer2 Interface	
• WAN Service	Use this page to enable/disable the Virtual LAN Ports feature.
• LAN	
• MAC Clone	Enable virtual ports on LAN(1-4)
+NAT	LAN Port
+ Security	LAN(1-4)
+Parental Control	Wireless0
+Quality of Service	
+Traffic Control	
+Routing	Save/Apply
+DNS	
• DSL	
• UPnP	
 Interface Grouping 	
LAN Ports	

Figure 4-64

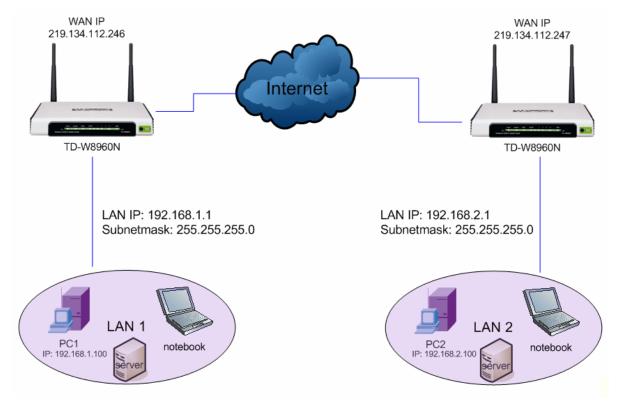
4.4.16 IPSec

Choose "**Advanced Setup**"→"**IPSec**", you can Add/Remove or Enable/Disable the IPSec tunnel connections on the screen as shown in Figure 4-65.

Device Info Quick Setup	IPSec Tunne	el Mode Coni	nections				
Advanced Setup							
+Layer2 Interface	Add, remove or enable/	disable IPSec tunnel c	onnections from this p	bage.			
• WAN Service							
• LAN	Connection Name	Remote Gateway	Local Addresses	Remote Addresses	Enable	Edit	Remove
• MAC Clone							
+NAT							
+ Security							
+Parental Control		Add	New Connection	Remove			
+Quality of Service							
+Traffic Control							
+Routing							
+DNS							
• DSL							
• UPnP							
 Interface Grouping 							
LAN Ports							
• IPSec							

Figure 4-65

This section will guide you to configure a VPN tunnel between two TD-W8960Ns. The topology is as follows.



PNote:

You could also use other VPN Routers to set VPN tunnels with TD-W8960N. TD-W8960N supports up to 10 VPN tunnels simultaneously.

Click **Add New Connection** in Figure 4-65 and then you will enter the screen shown in Figure 4-66.

Device Info	IPSec Settings	
Quick Setup	in occ octaings	
Advanced Setup		
+Layer2 Interface		
•WAN Service	IPSec Connection Name:	VPN1
•LAN	Remote IP Sec Gateway Address(URL):	219.134.112.247
MAC Clone		LIGHT INTELED
+NAT	Tunnel access from local IP addresses:	Subnet
+ Security		
+Parental Control	IP Address for VPN:	192.168.1.1
+Quality of Service	IP Subnetmask:	255.255.255.0
+Traffic Control		
+Routing	Tunnel access from remote IP addresses:	Subnet 🗸
+DNS	IP Address for VPN:	192.168.2.1
• DSL	IP Subnetmask:	255.255.255.0
• UPnP	ii Subicultusia	255,255,255,0
 Interface Grouping 	Key Exchange Method:	Auto(IKE) 🗸
LAN Ports		
• IP Sec	Authentication Method:	Pre-Shared Key
Wireless	Pre-Shared Key:	12345678
Diagnostics	Perfect Forward Secrecy:	Disable 🗸
Management		
	Advanced IKE Settings:	Show Advanced Settings
		Save/Apply



- > **IPSec Connection Name:** Enter a name for your VPN.
- Remote IPSec Gateway Address (IP or Domain Name): Enter the destination gateway IP address in the box which is the public WAN IP or Domain Name of the remote VPN server endpoint. (For example: Input 219.134.112.247 in Device1, Input 219.134.112.246 in Device 2)
- Tunnel access from local IP addresses: Choose Subnet if you want the Whole LAN to join the VPN network, or else choose Single Address if you want single IP to join the VPN network.
- IP Address for VPN: Enter the IP address of your LAN. (For example: Input 192.168.1.1 in Device1, Input 192.168.2.1 in Device2)
- IP Subnetmask: Enter the Subnet mask of your LAN. (For example: Input 255.255.255.0 in both Device1 and Device2)
- Tunnel access from remote IP addresses: Choose Subnet if you want the Remote Whole LAN to join the VPN network, or else choose Single Address if you want single IP to join the VPN network.
- IP Address for VPN: Enter the IP address of the Remote LAN. (For example: Input 192.168.2.1 in Device1,Input 192.168.1.1 in Device2)
- IP Subnetmask: Enter the subnetmask of the remote LAN. (For example: Input 255.255.255.0 in both Device1 and Device2)
- > Key Exchange Method: Select Auto (IKE) or Manual.
- > Authentication Method: Select Pre-Shared Key (recommended) or Certificate (X.509).

- > **Pre-Shared Key:** Input the Pre-Shared key for Authentication. (For example: Input 12345678)
- > **Perfect Forward Secrecy:** PFS is an additional security protocol.

We recommend you leave the Advanced Settings as default value.

After complete the basic settings and click Save/Apply in both **Device1** and **Device2**, PCs in LAN1 could communicate with PCs in remote LAN2. (For example: You can ping the IP address of PC2 which is 192.168.2.100 in PC1)

P Note:

The VPN Servers Endpoint from both ends must use the same pre-shared keys and Perfect Forward Secrecy settings.

Advanced IKE Settings:	Hide Advanced Settin	ngs
Phase 1		
Mode:	Main	*
My Identifier Type:	Local Wan IP	*
My Identifier:		
Remote Identifier Type:	Remote Wan IP	*
Remote Identifier:		
Encryption Algorithm:	3DES	*
Integrity Algorithm:	MD5 🗸	
Select Diffie-Hellman Group for Key Exchange:	1024bit 🗸	
Key Life Time:	3600	Seconds
Phase 2		
Encryption Algorithm:	3DES 🗸	
Integrity Algorithm:	MD5 🔽	
Select Diffie-Hellman Group for Key Exchange:	1024bit 🗸	
Key Life Time:	3600	Seconds

Click Show Advanced Settings and then you can configure the Advanced Settings.

- Main Mode: Select Main Mode to configure the standard negotiation parameters for IKE phase1.
- Aggressive Mode: Select Aggressive Mode to configure IKE phase1 of the VPN Tunnel to carry out negotiation in a shorter amount of time. (Not Recommended-Less Secure)

PNote:

The difference between the two is that aggressive mode will pass more information in fewer packets, with the benefit of slightly faster connection establishment, at the cost of transmitting the identities of the security firewall in the clear. When using aggressive mode, some configuration parameters such as Diffie-Hellman groups, and PFS can not be negotiated, resulting in a greater importance of having "compatible" configuration on both ends.

> Key Life Time:

Enter the number of seconds for the IPSec lifetime. It is the period of time to pass before establishing a new IPSec security association (SA) with the remote endpoint. The default value is 3600.

P Note:

If you want to change the default settings of **Advanced Settings**, please make sure that both VPN server endpoints use the same Encryption Algorithm, Integrity Algorithm, Diffie-Hellman Group and Key Life time in both **phase1** and **phase2**.

4.5 Wireless

Choose "**Wireless**", there are six submenus to configure Wireless LAN settings. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

Wireless
• Basic
• Security
• MAC Filter
• Wireless Bridge
• Advanced
Station Info

4.5.1 Basic

Choose "Wireless" \rightarrow "Basic", you will see the screen of Wireless--Basic settings shown as below. The basic settings for wireless networking are set on this screen.

Device Info	Wireless Basic		
Quick Setup			
Advanced Setup			
Wireless	This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless		
Basic	LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements.		
Security	Click "Apply/Save" to configure the basic wireless options.		
MAC Filter			
 Wireless Bridge 			
 Advanced 	Enable Wireless		
Station Info	Hide SSID Broadcast		
Diagnostics	Clients Isolation		
Management	Wireless Network Name: TP-LINK 010001 (Also called SSID)		
	Wireless Network Name: TP-LINK_010001 (Also called SSID)		
	BSSID: 02:10:18:01:00:01		
	Country: UNITED STATES		
	Apply/Save		

Figure 4-67

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on Region requirements.

- Enable Wireless: If you want to use wireless features, you must select "Enable Wireless". If you deselect "Enable Wireless" option, all the Wireless settings below will be disabled.
- Hide Access Point: When wireless clients survey the local area for wireless networks to associate with, you can select this option to avoided being surveyed.
- Clients Isolation: Select this option to enable AP isolation function so that stations associated to the AP will not be able to communicate with each other.
- SSID: Wireless network name shared among all points in a wireless network. The SSID must be identical for all devices in the wireless network. It is case-sensitive and must not exceed 32 characters (use any of the characters on the keyboard). Make sure this setting is the same for all stations in your wireless network. Type the desired SSID in the space provided.
- > **BSSID:** Show the MAC address of the Router.
- > **Country:** Restrict the channel set and transmit power.

Click Apply/Save to save your settings.

4.5.2 Security

Choose "Wireless" \rightarrow "Security", you will see the screen of Wireless--Security settings shown as below. You can configure security features of the wireless LAN interface by manually setting the network authentication or through QSS (Quick Security Setup) method.

Quick Setup Advanced Setup Wireless • Basic • Security • MAC Filter • Wireless Bridge • Advanced • Station Info Diagnostics Management Device PIN: • 54037137 Gen new PIN Help Help	Wireless Security		
Wireless This page allows you to configure security features of the wireless LAN interface. You may setup configuration manually or through Wi-Fi Protected Setup(WPS) • Security • MAC Filter • Wireless Bridge • Advanced • Station Info Enable QSS(WPS): Diagnostics Add Client (This feature is available only when WPA-PSK, WPA2-PSK or OPEN mode is configured) Management Push-Button © PIN			
• Basic • Security • MAC Filter • OSS(WPS) • Advanced • Enable OSS(WPS): • Station Info • Add Client (This feature is available only when WPA-PSK, WPA2-PSK or OPEN mode is configured) • Management • Push-Button © PIN			
• Basic • Security • MAC Filter • Wireless Bridge • Advanced • Station Info Diagnostics Management • Management			
MAC Filter Wireless Bridge Advanced Station Info Diagnostics Management Management GSS(WPS): Enabled ♥ Constant (This feature is available only when WPA-PSK, WPA2-PSK or OPEN mode is configured) OPush-Button ⊙ PIN Add Enrollee Help	You may setup configuration manually or through Wi-Fi Protected Setup(WPS)		
• Wireless Bridge OSS(WPS) • Advanced Enable OSS(WPS): • Station Info Add Client (This feature is available only when WPA-PSK, WPA2-PSK or OPEN mode is configured) • Management • Push-Button • PIN • Help • Help			
Wireless Bridge Advanced Enable OSS(WPS): Enabled Station Info Diagnostics Management Push-Button ③ PIN Add Enrollee Help			
Advanced Station Info Diagnostics Management Add Client (This feature is available only when WPA-PSK, WPA2-PSK or OPEN mode is configured) OPush-Button OPIN Add Enrollee Help	QSS(WPS)		
Diagnostics Add Client (This feature is available only when WPA-PSK, WPA2-PSK or OPEN mode is configured) Management OPush-Button OPIN Help			
Management Push-Button ⊙ PIN Add Enrollee Help			
Management Help			
Manual Setup AP			
	In order to protect your network from hackers and unauthorized users, it is highly recommended you choose		
You can set the network authentication method, selecting data encryption, specify whether a network key is	one of the following wireless network security settings. You can set the network authentication method, selecting data encryption, specify whether a network key is		
required to authenticate to this wireless network and specify the encryption strength. Warning: we suggest you not to set WEP encryption to "Enabled" when the device runs in 11n mode. The	required to authenticate to this wireless network and specify the encryption strength.		
device's wireless highest speed is 54Mbps in that encryption type.			
Tips: 11n only mode are not supported when WEP encryption is "Enabled" or WPA Encryption type is "TKIP". Tips: "WPA Encryption" are not allowed to set to "TKIP" when the device runs in 11n mode.	Tips: 11n only mode are not supported when WEP encryption is "Enabled" or WPA Encryption type is "TKIP".		
Click "Apply/Save" when done.			
Network Authentication: Open (insecurity)			
WEP Encryption: Disabled			
Apply/Save	Apply/Save		

Figure 4-68

4.5.2.1 QSS (WPS) Setup

Back to LED Explanation

This section will guide you to add a new wireless device to an existing network quickly by **QSS** (Quick Security Setup) method. It's also called WPS (Wi-Fi Protected Setup) in some cases.

PNote:

- 1) This feature is available only when OPEN, WPA-PSK, WPA2-PSK or Mixed WPA2/WPA-PSK mode is configured.
- 2) To build a successful connection by QSS, you should also do the corresponding configuration of the new device for QSS function meanwhile.
- 3) QSS (Quick Security Setup) is one kind of WPS (Wi-Fi Protected Setup) method.

I. By PBC

If the wireless adapter supports Quick Security Setup and the Push Button Configuration (PBC) method, you can add it to the network by PBC with the following two methods. Click **Push-Button**, you will see the screen as shown below.

Device Info	Wireless Security	
Quick Setup		
Advanced Setup		
Wireless	This page allows you to configure security features of the wireless LAN interface.	
• Basic	You may setup configuration manually or through Wi-Fi Protected Setup(WPS)	
Security		
• MAC Filter	000(11/00)	
• Wireless Bridge	QSS(WPS)	
Advanced	Enable QSS(WPS): Enabled	
 Station Info 		
Diagnostics	Add Client (This feature is a vail able only when WPA-PSK, WPA2-PSK or OPEN mode is configured)	
Management	OPush-Button PIN Add Enrollee Device PIN: 54037137 Gen new PIN Help	
	Device PIN: 54037137 Gen new PIN Help	
	Manual Setup AP	
	In order to protect your network from hackers and unauthorized users, it is highly recommended you choose one of the following wireless network security settings. You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Warning: we suggest you not to set WEP encryption to "Enabled" when the device runs in 11n mode. The device's wireless highest speed is 54Mbps in that encryption type. Tips: 11n only mode are not supported when WEP encryption is "Enabled" or WPA Encryption type is "TKIP". Tips: "WPA Encryption" are not allowed to set to "TKIP" when the device runs in 11n mode. Click "Apply/Save" when done.	
	Network Authentication: Open (insecurity) WEP Encryption: Disabled	
	Apply/Save	

Figure 4-69

Method One: Hardware push button.

Step 1: Press the QSS button on the front panel of the Router.



Step 2: Press and hold the QSS button of the adapter directly for 2 or 3 seconds.

QSS	

Step 3: Wait for a while until the next screen of adapter appears. Click **Finish** to complete the QSS configuration.

🥶 QSS for Wireless	
(((QSS)))	
Wireless Configuration Completed	
Your computer has successfully joined the TP-LINK network.	
< <u>B</u> ack Finish	Cancel

Figure 4-70

Method Two:

Step 1: Press the QSS button on the front panel of the Router.



Step 2: For the configuration of the wireless adapter, please choose "**Push the button on my** access point" in the configuration utility of the QSS as below, and click **Next**.

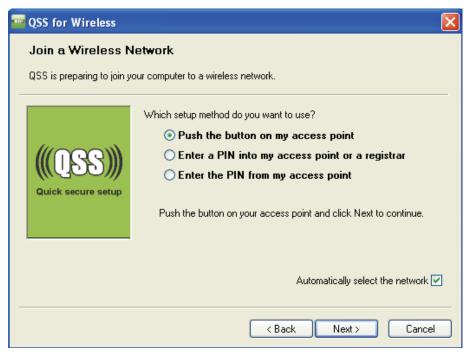


Figure 4-71

Step 3: Wait for a while until the next screen appears. Click **Finish** to complete the QSS configuration.



Figure 4-72

II. By PIN

If the new device supports Quick Security Setup and the PIN method, you can add it to the network by PIN with the following two methods.

Method One: Enter the PIN of wireless adapter into my Router.

Step 1: Select the **PIN** checkbox and enter the PIN code of the wireless adapter in the field under as shown below. Then click **Add Enrollee**.

Device Info	Wireless Security		
Quick Setup			
Advanced Setup			
Wireless	This page allows you to configure security features of the wireless LAN interface.		
• Basic	You may setup configuration manually or through Wi-Fi Protected Setup(WPS)		
• Security			
• MAC Filter			
•Wireless Bridge	QSS(WPS)		
• Advanced	Enable QSS(WPS): Enabled		
Station Info			
Diagnostics	Add Client (This feature is available only when WPA-PSK, WPA2-PSK or OPEN mode is configured)		
Management	Push-Buttor O PIN Add Enrollee		
	Device PIN: 54037137 Gen new PIN Help		
	Manual Setup AP		
	In order to protect your network from hackers and unauthorized users, it is highly recommended you choose one of the following wireless network security settings. You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Warning: we suggest you not to set WEP encryption to "Enabled" when the device runs in 11n mode. The device's wireless highest speed is 54Mbps in that encryption is "Enabled" or WPA Encryption type is "TKIP". Tips: 11n only mode are not supported when WEP encryption is "Enabled" or WPA Encryption type is "TKIP". Tips: "WPA Encryption" are not allowed to set to "TKIP" when the device runs in 11n mode. Click "Apply/Save" when done.		
	Network Authentication: Open (insecurity)		
	WEP Encryption: Disabled		
	Apply/Save		

Figure 4-73

P Note:

The PIN code of the adapter is always displayed on the QSS configuration screen.

Step 2: For the configuration of the wireless adapter, please choose "Enter a PIN into my access point or a registrar" in the configuration utility of the QSS as below, and click Next.

15	QSS for Wireless		×
	Join a Wireless N	letwork	
	QSS is preparing to join y	our computer to a wireless network.	
_	(((QSS))) Quick secure setup	 Which setup method do you want to use? Push the button on my access point Enter a PIN into my access point or a registrar Enter the PIN from my access point 	
_		Automatically select the network < Back Next > Cancel	9

Figure 4-74

PNote:

In this example, the default PIN code of this adapter is 16952898 as the preceding figure shown.

Method Two: Enter the PIN of my Router into the wireless adapter.

Step 1: Get the Current PIN code generated by the Router as shown below. You can click **Gen New PIN** to get a new PIN code for Router.

Device Info	Wireless Security	
Quick Setup	Whichess - Occurry	
Advanced Setup		
Wireless	This page allows you to configure security features of the wireless LAN interface.	
• Basic	You may setup configuration manually or through Wi-Fi Protected Setup(WPS)	
• Security		
• MAC Filter		
• Wireless Bridge	QSS(WPS)	
 Advanced 	Enable QSS(WPS): Enabled	
Station Info		
Diagnostics	Add Client (This feature is available only when WPA-PSK, WPA2-PSK or OPEN mode is configured)	
Management	○ Push-Button ④ PIN Add Enrollee	
	Device PIN: 12345670 Gen new PIN Help	
	Manual Setup AP	
	In order to protect your network from hackers and unauthorized users, it is highly recommended you choose one of the following wireless network security settings. You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Warning: we suggest you not to set WEP encryption to "Enabled" when the device runs in 11n mode. The device's wireless highest speed is 54Mbps in that encryption type. Tips: 11n only mode are not supported when WEP encryption is "Enabled" or WPA Encryption type is "TKIP". Tips: "WPA Encryption" are not allowed to set to "TKIP" when the device runs in 11n mode. Click "Apply/Save" when done.	
	Network Authentication: Open (insecurity) WEP Encryption: Disabled	
	Apply/Save	

Figure 4-75

Step 2: For the configuration of the wireless adapter, please choose "Enter a PIN from my access point" in the configuration utility of the QSS as below, and enter the PIN code of the Router into the field after "Access Point PIN". Then click Next.

(QSS for Wireless		×
	Join a Wireless N	etwork	
(QSS is preparing to join your computer to a wireless network.		
	(((QSS))) Quick secure setup	 Which setup method do you want to use? Push the button on my access point Enter a PIN into my access point or a registrar Enter the PIN from my access point 	ue.
		Access Point PIN: 12345670 Automatically select the network	
	< Back Next > Cancel		

Figure 4-76

4.5.2.2 Manual Setup AP

Follow the instructions below to configure security features of the wireless LAN interface manually. You can set the network authentication method, select data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.

Device Info	Wireless Security	
Quick Setup	White is a boot in the second se	
Advanced Setup		
Wireless	This page allows you to configure security features of the wireless LAN interface.	
• Basic	You may setup configuration manually or through Wi-Fi Protected Setup(WPS)	
Security		
MAC Filter	000(11/00)	
• Wireless Bridge	QSS(WPS)	
• Advanced	Enable QSS(WPS): Enabled	
 Station Info 		
Diagnostics	Add Client (This feature is available only when WPA-PSK, WPA2-PSK or OPEN mode is configured)	
Management	○ Push-Button ④ PIN Add Enrollee	
	Device PIN: 12345670 Gen new PIN Help	
	Device PIN: 12345670 Gen new PIN Help	
	Manual Setup AP	
	In order to protect your network from hackers and unauthorized users, it is highly recommended you choose one of the following wireless network security settings. You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Warning: we suggest you not to set WEP encryption to "Enabled" when the device runs in 11n mode. The device's wireless highest speed is 54Mbps in that encryption type. Tips: 11n only mode are not supported when WEP encryption is "Enabled" or WPA Encryption type is "TKIP". Tips: "WPA Encryption" are not allowed to set to "TKIP" when the device runs in 11n mode. Click "Apply/Save" when done.	
	Network Authentication: Open (insecurity)	
	Apply/Save	

Figure 4-77

Network Authentication: Select an authentication type from the drop-down list. Options available are: Open, Shared, WPA, WPA-PSK, WPA2, WPA2-PSK, Mixed WPA2/WPA, and Mixed WPA2/WPA-PSK.

P Note:

For most users, it is recommended to use the default Wireless LAN Performance settings. Any changes made to these settings may adversely affect your wireless network. Under certain circumstances, changes may benefit performance. Carefully consider and evaluate any changes to these wireless settings.

1. WEP

WEP is a basic encryption method offering two levels of encryption, 64-bit and 128-bit encryption. To configure the WEP encryption, there are two ways.

- Keep the Network Authentication of **Open (insecurity)** and select **Enabled** from the WEP Encryption drop-down list, as shown in Figure 4-78. **Open (insecurity)** allows any wireless station to associate with the access point.
- Select Shared (good) from the Network Authentication drop-down list, as shown in Figure 4-79. Shared (good) only allows stations using a shared key encryption to associate with it. Shared key requires additional configuration of the keys to be used. Follow the instructions

below to configure the Shared Keys.

Wireless					
• Basic					
Security	Manual Setup AP				
• MAC Filter	In order to protect your network from backars and unauthorized users, it is highly recommended you				
• Wireless Bridge		In order to protect your network from hackers and unauthorized users, it is highly recommended you choose one of the following wireless network security settings.			
Advanced		thentication method, selecting data encryption, specify whether a network key is this wireless network and specify the encryption strength.			
Station Info	Warning: we suggest you n	ot to set WEP encryption to "Enabled" or WPA encryption to "TKIP" when the			
Diagnostics	device runs in 11n mode. The device's wireless highest speed is 54Mbps in these two encryption types. Tips: 11n only mode are not supported when WEP encryption is "Enabled" or WPA Encryption type is				
Management	"TKIP".				
	Click "Apply/Save" when do	ne.			
	Network Authentication:	Open (insecurity)			
	WED Encomptions	Enabled V			
	WEP Encryption: Encryption Strength:	128-bit V			
	Current Network Key:				
	Network Key 1:				
	Network Key 2:				
	-				
	Network Key 3:				
	Network Key 4:	Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit			
		encryption keys			
		Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys			
		encrypuon keys			
		Apply/Save			
		hppiy/save			
	F	igure 4-78			
Device Info					
Quick Setup	Manual Setup AP				
Advanced Setup	In order to protect your pot	work from hackers and unauthorized users, it is highly recommended you			
Wireless	choose one of the following	g wireless network security settings.			
• Basic		thentication method, selecting data encryption, specify whether a network key is his wireless network and specify the encryption strength.			
Security	Warning: we suggest you n	ot to set WEP encryption to "Enabled" when the device runs in 11n mode. The			
	device's wireless highest s	need in 54Mbps in that approximation type			
• MAC Filter	Tips: 11n only mode are no Tips: "WPA Encryption" are i	t supported when WEP encryption is "Enabled" or WPA Encryption type is "TKIP". not allowed to set to "TKIP" when the device runs in 11n mode.			
• Wireless Bridge	Tips: 11n only mode are no	t supported when WEP encryption is "Enabled" or WPA Encryption type is "TKIP". not allowed to set to "TKIP" when the device runs in 11n mode.			
• Wireless Bridge • Advanced	Tips: 11n only mode are no Tips: "WPA Encryption" are i	t supported when WEP encryption is "Enabled" or WPA Encryption type is "TKIP". not allowed to set to "TKIP" when the device runs in 11n mode.			
+ Wireless Bridge + Advanced + Station Info	Tips: 11n only mode are no Tips: "WPA Encryption" are i	t supported when WEP encryption is "Enabled" or WPA Encryption type is "TKIP". not allowed to set to "TKIP" when the device runs in 11n mode.			
• Wireless Bridge • Advanced • Station Info Diagnostics	Tips: 11n only mode are no Tips: "WPA Encryption" are Click "Apply/Save" when doi Network Authentication:	t supported when WEP encryption is "Enabled" or WPA Encryption type is "TKIP". not allowed to set to "TKIP" when the device runs in 11n mode. ne. Shared (good)			
+ Wireless Bridge + Advanced + Station Info	Tips: 11n only mode are no Tips: "WPA Encryption" are Click "Apply/Save" when dor Network Authentication: WEP Encryption:	t supported when WEP encryption is "Enabled" or WPA Encryption type is "TKIP". not allowed to set to "TKIP" when the device runs in 11n mode. ne. Shared (good)			
• Wireless Bridge • Advanced • Station Info Diagnostics	Tips: 11n only mode are no Tips: "WPA Encryption" are Click "Apply/Save" when doi Network Authentication:	t supported when WEP encryption is "Enabled" or WPA Encryption type is "TKIP". not allowed to set to "TKIP" when the device runs in 11n mode. ne. Shared (good)			
• Wireless Bridge • Advanced • Station Info Diagnostics	Tips: 11n only mode are no Tips: "WPA Encryption" are Click "Apply/Save" when dor Network Authentication: WEP Encryption: Encryption Strength:	t supported when WEP encryption is "Enabled" or WPA Encryption type is "TKIP". not allowed to set to "TKIP" when the device runs in 11n mode. ne. Shared (good)			
• Wireless Bridge • Advanced • Station Info Diagnostics	Tips: 11n only mode are no Tips: "WPA Encryption" are Click "Apply/Save" when dor Network Authentication: WEP Encryption Encryption Strength: Current Network Key:	t supported when WEP encryption is "Enabled" or WPA Encryption type is "TKIP". not allowed to set to "TKIP" when the device runs in 11n mode. ne. Shared (good)			
• Wireless Bridge • Advanced • Station Info Diagnostics	Tips: 11n only mode are no Tips: "WPA Encryption" are Click "Apply/Save" when doi Network Authentication: WEP Encryption: Encryption Strength: Current Network Key: Network Key 1:	t supported when WEP encryption is "Enabled" or WPA Encryption type is "TKIP". not allowed to set to "TKIP" when the device runs in 11n mode. ne. Shared (good)			
• Wireless Bridge • Advanced • Station Info Diagnostics	Tips: 11n only mode are no Tips: "WPA Encryption" are Click "Apply/Save" when dor Network Authentication: WEP Encryption Encryption Strength: Current Network Key 1: Network Key 2: Network Key 3:	t supported when WEP encryption is "Enabled" or WPA Encryption type is "TKIP". not allowed to set to "TKIP" when the device runs in 11n mode. ne. Shared (good)			
• Wireless Bridge • Advanced • Station Info Diagnostics	Tips: 11n only mode are no Tips: "WPA Encryption" are Click "Apply/Save" when dor Network Authentication: WEP Encryption: Encryption Strength: Current Network Key 1: Network Key 2:	t supported when WEP encryption is "Enabled" or WPA Encryption type is "TKIP". not allowed to set to "TKIP" when the device runs in 11n mode. ne. Shared (good)			
• Wireless Bridge • Advanced • Station Info Diagnostics	Tips: 11n only mode are no Tips: "WPA Encryption" are Click "Apply/Save" when dor Network Authentication: WEP Encryption Encryption Strength: Current Network Key 1: Network Key 2: Network Key 3:	t supported when WEP encryption is "Enabled" or WPA Encryption type is "TKIP". not allowed to set to "TKIP" when the device runs in 11n mode. ne. Shared (good) Enabled 128-bit 1 Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys			
• Wireless Bridge • Advanced • Station Info Diagnostics	Tips: 11n only mode are no Tips: "WPA Encryption" are Click "Apply/Save" when dor Network Authentication: WEP Encryption Encryption Strength: Current Network Key 1: Network Key 2: Network Key 3:	t supported when WEP encryption is "Enabled" or WPA Encryption type is "TKIP". not allowed to set to "TKIP" when the device runs in 11n mode. ne. Shared (good) Enabled 128-bit 1 Encryption type is "TKIP". TKIP". Shared (good) Enabled Enabled Enabled Enabled TKIP". TKIP.			
• Wireless Bridge • Advanced • Station Info Diagnostics	Tips: 11n only mode are no Tips: "WPA Encryption" are Click "Apply/Save" when dor Network Authentication: WEP Encryption Encryption Strength: Current Network Key 1: Network Key 2: Network Key 3:	t supported when WEP encryption is "Enabled" or WPA Encryption type is "TKIP". not allowed to set to "TKIP" when the device runs in 11n mode. ne. Shared (good) Enabled 128-bit 1 Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit			
• Wireless Bridge • Advanced • Station Info Diagnostics	Tips: 11n only mode are no Tips: "WPA Encryption" are Click "Apply/Save" when dor Network Authentication: WEP Encryption Encryption Strength: Current Network Key 1: Network Key 2: Network Key 3:	t supported when WEP encryption is "Enabled" or WPA Encryption type is "TKIP". not allowed to set to "TKIP" when the device runs in 11n mode. ne. Shared (good) Enabled 128-bit 1 Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit			

Figure 4-79

- > Encryption strength: Select the appropriate level of encryption, 64-bit or 128-bit.
- > Current Network Key: To indicate which WEP key to use, select a transmission key number.
- Network Key 1-4: If you want to manually enter the WEP keys, then enter them in the network Key 1-4 fields.

Configure WEP Settings

- 1. Select **Shared (good)** from the **Network Authentication** drop-down list. The menu will change to offer the appropriate settings.
- 2. Select **64-bit** from the **WEP Encryption** drop-down list.
- 3. Select "1" from Current Network Key drop-down list.
- 4. Type in the password in the Network Key 1 field.
- 5. Click **Save/Apply** to save the new configuration.

Device Info		
Quick Setup	Manual Setup AP	
Advanced Setup	In order to protect your pet	work from hackers and unauthorized users, it is highly recommended you
Wireless	choose one of the followin	g wireless network security settings.
• Basic		thentication method, selecting data encryption, specify whether a network key is his wireless network and specify the encryption strength.
Security	Warning: we suggest you n	ot to set WEP encryption to "Enabled" when the device runs in 11n mode. The 👘
• MAC Filter	Tips: 11n only mode are no	peed is 54Mbps in that encryption type. t supported when WEP encryption is "Enabled" or WPA Encryption type is "TKIP".
• Wireless Bridge	Tips: "WPA Encryption" are Click "Apply/Save" when do	not allowed to set to "TKIP" when the device runs in 11n mode. ne
• Advanced	Cher Apply Dave when do	no.
 Station Info 	Network Authentication:	Shared (good)
Diagnostics	Network Authentication:	Shared (good)
Management	WEP Encryption:	Enabled 🐱
	Encryption Strength:	64-bit 🗸
	Current Network Key:	
	Network Key 1:	1234567890
	Network Key 2:	
	Network Key 3:	
	Network Key 4:	
		Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys
		Apply/Save

Figure 4-80

Note:

We use **Network Authentication** Shared (good), **Encryption Strength** 64-bit, **Current Network Key** "1" and enter 10 hexadecimal digits "1234567890" in the **Network Key 1** for example, as shown in Figure 4-80 above.

2. WPA

WPA security for wireless communication has been developed to overcome some of the shortcomings of WEP. WPA combines the key generation with the authentication services of a RADIUS server.

Device Info	Manual Setup AP		
Quick Setup			
Advanced Setup			uthorized users, it is highly recommended you
Wireless	choose one of the following wi You can set the network authen		settings. I data encryption, specify whether a network key is
• Basic	required to authenticate to this wireless network and specify the encryption strength.		
• Security	Warning: we suggest you not to set WEP encryption to "Enabled" when the device runs in 11n mode. The device's wireless highest speed is 54Mbps in that encryption type.		
• MAC Filter	Tips: 11n only mode are not supported when WEP encryption is "Enabled" or WPA Encryption type is "TKIP". Tips: "WPA Encryption" are not allowed to set to "TKIP" when the device runs in 11n mode.		
• Wireless Bridge	Click "Apply/Save" when done.		
• Advanced			
 Station Info 	Network Authentication:	WPA (good)	~
Diagnostics			
Management	WPA Group Rekey Interval:	0	(optional)
	RADIUS Server IP Address:	0.0.0.0	
	RADIUS Port:	1812	(1-65535)
	RADIUS Key: (optional)		
	(You can enter ASCII characters between 0 and 63 characters or 0 to 64 Hexadecimal characters.)		
	WPA Encryption:	ES 🗸	
	WEP Encryption:	Disabled 🗸	
		Apply/S	ave



- WPA Group ReKey Interval: Enter the Key Renewal period, which tells the Router how often it should change encryption keys.
- > RADIUS Server IP Address: The IP address of the RADIUS server.
- > **RADIUS Port:** The port of the RADIUS server. The default number is 1812.
- > **RADIUS key:** The password of the RADIUS Server.
- WPA Encryption: Select the encryption you want to use: TKIP or AES (AES is an encryption method stronger than TKIP).

Configure WPA settings

- 1. Select **WPA** from the **Network Authentication** drop-down list. The menu will change to offer the appropriate settings.
- 2. Change the WPA Group Rekey Interval as desired.
- 3. Type in the IP address of the RADIUS server used in the **RADIUS Server IP Address** field.
- 4. Change the **RADIUS Port** if necessary.
- 5. Type in the password in the **RADIUS Key** field.
- 6. Use the default setting **AES** of WPA Encryption.
- 7. Click **Save/Apply** to save the new configuration.

Device Info	Manual Setup AP				
Quick Setup					
Advanced Setup	In order to protect your network from hackers and unauthorized users, it is highly recommended you				
Wireless	choose one of the following wireless network security settings. You can set the network authentication method, selecting data encryption, specify whether a network key is				
• Basic	required to authenticate to this wireless network and specify the encryption strength.				
Security		Warning: we suggest you not to set WEP encryption to "Enabled" when the device runs in 11n mode. The device's wireless highest speed is 54Mbps in that encryption type.			
• MAC Filter	Tips: 11n only mode are not supported when WEP encryption is "Enabled" or WPA Encryption type is "TKIP". Tips: "WPA Encryption" are not allowed to set to "TKIP" when the device runs in 11n mode.				
• Wireless Bridge	Tips: "What Encryption" are not allowed to set to "TKIP" when the device runs in TTh mode. Click "Apply/Save" when done.				
• Advanced					
Station Info	Network Authentication:	WPA (good)	v		
Diagnostics					
Management	WPA Group Rekey Interval:	30	(optional)		
	RADIUS Server IP Address:	192.168.1.10			
	RADIUS Port:	1812	(1-65535)		
	RADIUS Key: (optional)				
	(You can enter ASCII characters between 0 and 63 characters or				
	0 to 64 Hexadecimal characters.) WPA Encryption:				
	WEP Encryption: Disabled v				
	Apply/Save				

Figure 4-82

3. WPA-PSK

WPA-PSK requires a shared key and does not use a separate server for authentication. PSK keys can be ASCII or Hex type.

Device Info		
Quick Setup	Manual Setup AP	
Advanced Setup	In order to protect your network from hackers and unauthorized users, it is highly recommended you choose one of	the
Wireless	following wireless network security settings.	
• Basic	You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.	
Security	Warning: we suggest you not to set WEP encryption to "Enabled" when the device runs in 11n mode. The device's wireles highest speed is 54Mbps in that encryption type.	ss
• MAC Filter	Tips: 11n only mode are not supported when WEP encryption is "Enabled" or WPA Encryption type is "TKIP".	
• Wireless Bridge	Tips: "WPA Encryption" are not allowed to set to "TKIP" when the device runs in 11n mode. Click "Applv/Save" when done.	
Advanced		
 Station Info 	Network Authentication: WPA-PSK (better)	
Diagnostics		
Management	WPA Pre-Shared Key:	
	Click here to display (You can enter ASCII characters between 8 and 63 characters or 8 to 64 Hexadecimal characters.)	
	WPA Group Rekey Interval: 30 (optional)	
	WPA Encryption: AES	
	WEP Encryption: Disabled	
	Apply/Save	

Figure 4-83

- WPA Pre-Shared Key: Enter the key shared by the Router and your other network devices. It must have 8-63 ASCII characters or 64 Hexadecimal digits.
- > Click here to display: Click it to show you the WPA Pre-Shared Key.

Configure WPA-PSK settings

- 1. Select **WPA-PSK**. The menu will change to offer the appropriate settings as the picture show above.
- 2. WPA-PSK requires a shared key. Type the key in the space provided. PSK keys can be ASCII or Hex type.
- 3. Change the Group Key Interval as desired or use the default setting.
- 4. Click Save/Apply to save the new configuration.

Device Info			
Quick Setup	Manual Setup AP		
Advanced Setup	In order to protect your network from hackers and unauthorized users, it is highly recommended you choose one of th		
Wireless	following wireless network security settings.		
• Basic	You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.		
Security	Warning: we suggest you not to set WEP encryption to "Enabled" when the device runs in 11n mode. The device's wireless highest speed is 54Mbps in that encryption type.		
• MAC Filter	Tips: 11n only mode are not supported when WEP encryption is "Enabled" or WPA Encryption type is "TKIP".		
• Wireless Bridge	Tips: "WPA Encryption" are not allowed to set to "TKIP" when the device runs in 11n mode. Click "Apply/Save" when done.		
• Advanced			
 Station Info 	Network Authentication: WPA-PSK (better)		
Diagnostics			
Management	WPA Pre-Shared Key:		
	Click here to display (You can enter ASCII characters between 8 and 63 characters or 8 to 64 Hexadecimal characters.)		
	WPA Group Rekey Interval: 30 (optional)		
	WPA Encryption: AES 🗸		
	WEP Encryption: Disabled		
	Apply/Save		

Figure 4-84

P Note:

If you click the option "Click here to display", the Figure 4-85 will pop-up, and it shows the password you have set.

🖆 http://192.168.1.253/wlsecrefresh.wl?wlRefresh=0 📃 🗖 🗙		
	1234567890	
	🤵 Internet	

Figure 4-85

4. WPA2

To configure WPA2 settings, select the WPA2 option from the drop-down list. The menu will change to offer the appropriate settings. The steps of these settings are similar to WPA settings.

TD-W8960N 300Mbps Wireless N ADSL2+ Modem Router User Guide

• Security			
MAC Filter	Manual Setup AP		
• Wireless Bridge	In order to protect your petwo	rk from backore an	l unauthorized users, it is highly recommended you choose one of the
• Advanced	following wireless network se	curity settings.	
 Station Info 	You can set the network authen authenticate to this wireless ne		ecting data encryption, specify whether a network key is required to e encryption strength.
Diagnostics	Warning: we suggest you not to	set WEP encryption	to "Enabled" or WPA encryption to "TKIP" when the device runs in 11n
Management			ops in these two encryption types. encryption is "Enabled" or WPA Encryption type is "TKIP".
	Network Authentication:	WPA2 (better)	V
	WPA2 Preauthentication:	Disabled 🐱	
	Network Re-auth Interval:	36000	(optional)
	WPA Group Rekey Interval:	0	(optional)
	RADIUS Server IP Address:	0.0.0.0	
	RADIUS Port:	1812	(1-65535)
	RADIUS Key:		(optional)
		(You can enter AS Hexadecimal cha	CII characters between 0 and 63 characters or 0 to 64 racters.)
	WPA Encryption:	AES 🗸	
	WEP Encryption:	Disabled 👻	
			Apply/Save

Figure 4-86

- WPA2 Preauthentication: Select Enable from the drop-down list, Stations will authenticate with the AP during the scanning process, and once association is required, the station has been already authenticated.
- Network Re-auth Interval: Enter a value in seconds as the frequency interval to enable periodic Network Re-authentication function, while leave it blank or enter "0" to disable it.

5. WPA2-PSK

To configure WPA2-PSK settings, select the WPA2-PSK option from the drop-down list. The menu will change to offer the appropriate settings. WPA2-PSK requires a shared key and does not use a separate server for authentication. PSK keys can be ASCII or Hex type.

Security	Help
• MAC Filter	Device PIN: 11812777 Gen new PIN Help
• Wireless Bridge	
• Advanced	
 Station Info 	Manual Setup AP
Diagnostics	
Management	In order to protect your network from hackers and unauthorized users, it is highly recommended you choose one of the following wireless network security settings. You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Warning: we suggest you not to set WEP encryption to "Enabled" or WPA encryption to "TKIP" when the device runs in 11n mode. The device's wireless highest speed is 54Mbps in these two encryption types. Tips: 11n only mode are not supported when WEP encryption is "Enabled" or WPA Encryption type is "TKIP". Click "Apply/Save" when done.
	WPA Pre-Shared Key: Click here to display (You can enter ASCII characters between 8 and 63 characters or 8 to 64 Hexadecimal characters.)
	WPA Group Rekey Interval: 0 (optional)
	WPA Encryption: AES V WEP Encryption: Disabled V
	Apply/Save

Figure 4-87

6. Mixed WPA2/WPA

To configure Mixed WPA2/WPA settings, select the Mixed WPA2/WPA option from the drop-down list. The menu will change to offer the appropriate settings. The steps to these settings are similar to those for WPA-PSK.

Security			
• MAC Filter	Manual Setup AP		
• Wireless Bridge			l
• Advanced	following wireless network se		l unauthorized users, it is highly recommended you choose one of the
 Station Info 	You can set the network auther authenticate to this wireless ne		ecting data encryption, specify whether a network key is required to a securition strength
Diagnostics			to "Enabled" or WPA encryption to "TKIP" when the device runs in 11n
Management			ops in these two encryption types. encryption is "Enabled" or WPA Encryption type is "TKIP".
	Network Authentication: Mixed WPA2/WPA (adaptive)		
	WPA2 Preauthentication:	Disabled 🗸	
	Network Re-auth Interval:	36000	(optional)
	WPA Group Rekey Interval:	0	(optional)
	RADIUS Server IP Address:	0.0.0	
	RADIUS Port:	1812	(1-65535)
	RADIUS Key:		(optional)
	(You can enter ASCII characters between 0 and 63 characters or 0 to 64 Hexadecimal characters.)		
	WPA Encryption: AES		
	WEP Encryption:	Disabled 🗸	
			Apply/Save

Figure 4-88

7. Mixed WPA2/WPA-PSK

To configure Mixed WPA2/WPA-PSK settings, select the Mixed WPA2/WPA-PSK option from the drop-down list. The menu will change to offer the appropriate settings. The steps of this setting are the same with WPA-PSK.

Device Info		
Quick Setup	Manual Setup AP	
Advanced Setup	In order to protect your network from hac	ters and unauthorized users, it is highly recommended you choose one of the
Wireless	following wireless network security settin	gs.
• Basic	authenticate to this wireless network and s	nod, selecting data encryption, specify whether a network key is required to necify the encryption strength.
Security	Warning: we suggest you not to set WEP er highest speed is 54Mbps in that encryption	cryption to "Enabled" when the device runs in 11n mode. The device's wireless
• MAC Filter	Tips: 11n only mode are not supported whe	n WEP encryption is "Enabled" or WPA Encryption type is "TKIP".
• Wireless Bridge	Tips: "WPA Encryption" are not allowed to se Click "ApplwSave" when done.	et to "TKIP" when the device runs in 11n mode.
• Advanced		
 Station Info 	Network Authentication: Mixed W	PA2/WPA-PSK (adaptive) 🗸
Diagnostics	MERVOR Addrenic door.	ne, min ron (adaptivo)
Management	WPA Pre-Shared Key:	
	(You can e	to display enter ASCII characters between 8 and 63 characters or 8 to 64 nal characters.)
	WPA Group Rekey Interval: 30	(optional)
	WPA Encryption: AES	×
	WEP Encryption: Disable	d 🗸
		Apply/Save

Figure 4-89

4.5.3 MAC Filter

Choose "Wireless" \rightarrow "MAC Filter", you will see the screen of Wireless--MAC Filter settings shown as below.

Device Info	Wireless MAC Filter	
Quick Setup		
Advanced Setup		
Wireless	MAC Restrict Mode: 💿 Disabled 🔿 Allow 🔿 Deny	4
• Basic	<u> </u>	
• Security	MAC Address	Remove
• MAC Filter	00:13:0A:55:FF:09	
• Wireless Bridge		
• Advanced		
 Station Info 	Add R	emove

Figure 4-90

Wireless access can be filtered by using the MAC addresses of the wireless devices transmitting within your network's RADIUS. To filter wireless users by MAC Address, either permitting or blocking access. If you do not wish to filter users by MAC Address, select Disabled.

- > **Disabled:** Select this option to disable MAC Filter function.
- Allow: Select this option to enable MAC Filter function that allow wireless access by the devices listed on this screen.
- Deny: Select this option to enable MAC Filter function that block wireless access from the devices listed on this screen.
- > Add: Click this button to add the MAC Address.
- > Remove: Select the item of the MAC Address and click this button to remove it.

When you click the **Add** button, the pop-up picture shown below, and then you can type the MAC Address in the **MAC** Address field.

PNote:

The form of MAC Address must be "xx:xx:xx:xx:xx", like "00:13:0A:55:FF:09".

Device Info	Wireless MAC Filter
Quick Setup	
Advanced Setup	
Wireless	Enter the MAC address with 00:11:22:33:44:55 format and click "Apply/Save" to add the MAC address to the wireless MAC
• Basic	address filters.
Security	MAC Address: 00:13:0A:55:FF:09
MAC Filter	
• Wireless Bridge	
• Advanced	Apply/Save
 Station Info 	



When you finished making changes to the MAC Filter List screen, click **Save/Apply** to save the changes.

4.5.4 Wireless Bridge

Choose "Wireless"→"Wireless Bridge", you will see the screen of Wireless--Bridge settings shown as below. You can configure wireless bridge features of the wireless LAN interface and click Apply/Save button to save the current configuration.

Device Info	Wireless Bridge
Quick Setup	Lindge
Advanced Setup	
Wireless	This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge
• Basic	(also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP.
• Security	Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges
• MAC Filter	will be granted access.
• Wireless Bridge	Click "Refresh" to update the remote bridges. Wait for few seconds to update. Click "Apply/Save" to configure the wireless bridge options.
• Advanced	Tip: Only "Open" or "Shared" Network Authenticaion support Wireless Bridge. If you want remote wireless devices
 Station Info 	connect to this router by bridge Mode, set the Network Authentication to "Open" or "Shared" first!
Diagnostics	
Management	AP Mode: Access Point
	Bridge Restrict: Enabled
	Remote Bridges MAC Address:
	Refresh Apply/Save

Figure 4-92

- AP Mode: Select an AP Mode from the drop-down list. Options available are: Access Point and Wireless Bridge.
 - Access Point: Select this option to allow wireless stations including AP clients to access.
 - **Wireless Bridge**: Also known as WDS (Wireless Distribution System), it will bridges the wireless stations which also in bridge mode to connect two or more remote LANs.
- > Bridge Restrict:
 - **Disabled**: Select this option to disables wireless bridge restriction, that any wireless bridge will be granted access.
 - **Enabled**: Select this option (as shown below) to enables wireless bridge restriction, please enter the MAC address of the Remote Bridges that you want to connect with, and only these Remote Bridges are granted access.

AP Mode:	Access Point
Bridge Restrict:	Enabled 🗸
Remote Bridges MAC Address:	00:23:CD:ED:B3:F2
	Refresh Apply/Save

Figure 4-93

- Enabled (Scan): Select this option to enables wireless bridge restriction, and it will scan the environment for APs that exist around the device. Only those selected AP will be granted access.
- **Refresh:** Click this button to scan and display the APs.

Remote Bridges MAC Address: SSID BSSID TP-LINK 00:19:E0:94:51:F4
TP-LINK 00:19:E0:94:51:F4

Figure 4-94

P Note:

Only Open or Shared authentication method support wireless bridge, you should choose "**Wireless**"→"**Security**" to change authentication method to "open" or "shared" mode first.

4.5.5 Advanced

Choose "Wireless"→"Advanced", you will see the screen of Wireless--Advanced settings shown as below.

Device Info	Wireless Advan	ced
Quick Setup		
Advanced Setup		
Wireless		e advanced features of the wireless LAN interface. You can select a particular channel
• Basic	on which to operate, set the fragr save mode, set the beacon interv	nentation threshold, set the RTS threshold, set the wakeup interval for clients in power- val for the access point.
Security		", you couldn't set Wireless encryption type to "WEP" or "TKIP".
MAC Filter	Click "Apply/Save" to configure th	e advanced wheless options.
• Wireless Bridge		
Advanced	Channel:	Auto 🗸
 Station Info 	Mode:	11bgn v
Diagnostics	Bandwidth:	20MHz 🗸
Management	Control Sideband:	Lower 🗸
	Fragmentation Threshold:	2346
	RTS Threshold:	2347
	DTIM Interval:	1
	Beacon Interval:	100
	Transmit Power:	100% 🗸
	WMM(Wi-Fi Multimedia):	Enabled V
		Apply/Save
		Apply/Save

Figure 4-95

- Channel: Select the channel you want to use from the drop-down List. This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- Mode: In the drop-down list you can select "11b", "11bg", "11bgn" and "11n only". "11bgn" allows both 802.11b, 802.11g and 802.11n wireless stations to connect to the Router.
- Bandwidth: Select the Bandwidth you want to use from the drop-down List. If bigger bandwidth is selected, device could transmit and receive data with higher speed.
- Control Sideband: If bigger bandwidth is selected, this option will allow you select the Control Sideband you want.
- Fragmentation Threshold: This value specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor reduction of the default value is recommended. In most cases, it should remain at its default value of 2346.
- RTS Threshold: Should you encounter inconsistent data flow, only minor reduction of the default value 2347 is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. In most cases, keep its default value of 2347.
- DTIM Interval: This value, between 1 and 255, indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM

Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages. The default value is 1.

- Beacon Interval: Enter a value between 20-1000 milliseconds. The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the Router to synchronize the wireless network. The default value is 100.
- Transmit Power: This option will allow you to configure the wireless transmit power. High transmit power will extend the wireless signal range of the device and make the signal transmit more legible. Low transmit power with the smaller wireless signal range that will decrease the probability of interrupt by other Wi-Fi device.
- > WMM (Wi-Fi Multimedia): This function can guarantee the packets with high-priority messages being transmitted preferentially. It is strongly recommended.

4.5.6 Station info

Choose "Wireless" \rightarrow " Station Info", you will see the screen of Wireless--Authenticated Stations setting shown as below.

Device Info	Wireless Authenticated Stations						
Quick Setup							
Advanced Setup							
Wireless	This page shows authenticated wireless stations and their status.						
• Basic							
• Security							
• MAC Filter	MAC Associated Authorized SSID Interface						
• Wireless Bridge	MAC Associated Authorized SSID Interface						
• Advanced							
Station Info	(Peferel)						
Diagnostics	Refresh						
Management							

Figure 4-96

This page shows authenticated wireless stations and their status.

- > **MAC**: Displays the connected wireless station's MAC address.
- > **Associated**: Displays whether the wireless station has associated with the access point.
- > **Authorized**: Displays the information of Authentication.
- SSID: Displays the connected wireless station's SSID.
- > Interface: Displays the connected wireless station's Interface mode.

4.6 Diagnostics

Choose "**Diagnostics**", you will see the Diagnostics screen. This section describes the result of the test for the ENET (Ethernet) Connection, Wireless Connection and ADSL Synchronization. You can refer to the **Help** menu to get more information about the corresponding test.

uick Setup								
dvanced Setup								
lireless	Your modem is capable of testing your DSL c							
iagnostics	click "Rerun Diagnostic Tests" at the bottom o click "Help" and follow the troubleshooting pro		make sure the fa	il status is consi:	stent. If the test continu			
anagement								
	Test the connection to your local network							
	Test your LAN(1-4) Connection:			PASS	Help			
	Test your Wireless Connection:			PASS	Help			
	Test the connection to your DSL service pro	vider						
	Test xDSL Synchronization:							
	Test ATM OAM F5 segment ping:	DISABLED		Н	elp			
	Test ATM OAM F5 end-to-end ping:	DISABLED	elp					
	<u> </u>							
	Test the connection to your Internet service	-						
	Test PPP server connection:	DISABLED	Help					
	Test authentication with ISP:	DISABLED	Help					
	Test the assigned IP address:	DISABLED	<u>Help</u>					
	Ping default gateway:	FAIL	<u>Help</u>					
	Ping primary Domain Name Server:	FAIL	<u>Help</u>					
		st Te	st With OAM F	4				

4.7 Management

Choose "Management", there are eight submenus under the main menu. They are Settings, System Log, SNMP Agent, TR-069 Client, Access Control, Update Software and Reboot. Click any of them, and you will be able to configure the corresponding function.

Management
+Settings
• System Log
 SNMP Agent
• TR-069 Client
+Access Control
• Update Software
• Reboot

4.7.1 Settings

This section provides three important functions for managing the Router; they are **Backup**, **Update** and **Restore Default** (shown in Figure 4-98). The detailed manipulations are described below.

Device Info	Settings - Backup
Quick Setup	
Advanced Setup	
Wireless	Backup DSL Modem Router configurations. You may save your router configurations to a file on your PC.
Diagnostics	
Management	
-Settings	Backup Settings
• Backup	
• Update	
• Restore Default	

Figure 4-98

4.7.1.1 Export

Choose "**Management**" \rightarrow "**Settings**" \rightarrow "**Export**", you can see the **Export** screen, this screen (shown in Figure 4-99) allows you to save the current configuration of the Router as a backup file.

Device Info	Settings - Export
Quick Setup	
Advanced Setup	
Wireless	Backup DSL Modem Router configurations. You may save your router configurations to a file on your PC.
Diagnostics	
Management	
- Settings	Export Settings
•Export	
• Import	

Figure 4-99

To back up the Router's current settings:

1. Click the **Export Settings** button on the preceding screen (pop-up Figure 4-99), the following screen will then appear (shown in Figure 4-100).

File Dow	rnload - Security Warning 🛛 🛛 🔀				
Do you want to save this file?					
	Name: rom-0 Type: Unknown File Type, 16.0 KB From: 192.168.1.1 <u>S</u> ave Cancel				
١	While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not save this software. <u>What's the risk?</u>				

Figure 4-100

2. Click the **Save** button, and save the file as the appointed file (shown in Figure 4-101).

Save As						? 🔀
Savejn:	🚞 TD-W8960N		 v G	ø	۳ 📂	
My Recent Documents						
Desktop						
My Documents						
Wy Computer						
	File <u>n</u> ame:	rom-0			*	<u>S</u> ave
My Network	Save as <u>t</u> ype:	Document			*	Cancel

Figure 4-101

4.7.1.2 Import

Choose "**Management**" \rightarrow "**Settings**" \rightarrow "**Import**", you can see the **Import** screen, this screen (shown in Figure 4-102) allows you to update the Router's settings.

Device Info	Settings - Import
Quick Setup	5 1
Advanced Setup	
Wireless	Update DSL Modem Router settings. You may update your router settings using your saved files.
Diagnostics	Settings File Name: Browse
Management	
- Settings	
• Export	Import Settings
• Import	

Figure 4-102

To update the Router's settings:

- 1. Click the **Browse** button to locate the update file for the device, and you can also enter the exact path to the Setting file in the text box.
- 2. After you have selected the file for updating the settings, click the **Import Settings** button.

P Note:

The Router will reboot upon completion. This process will take a while, don't turn off the Router or press the **Reset** button while processing.

4.7.1.3 Restore Default

Choose "Management" \rightarrow "Settings" \rightarrow "Restore Default", you can see the Restore Default screen, this screen (shown in Figure 4-103) allows you to restore the Router's configuration to the factory defaults on the screen.

Device Info	Tools Restore Default Settings
Quick Setup	
Advanced Setup	
Wireless	Restore DSL Modern Router settings to the factory defaults.
Diagnostics	
Management	
– Settings	Restore Default Settings
• Backup	
• Update	
• Restore Default	



- Restore Default Settings: Click this button to restore the Router's configuration to the factory defaults, and then follow the on-screen instructions to complete it.
- > Account and Password: The default account name and its password are both admin.
- > The default IP Address: 192.168.1.1.
- > The default **Subnet Mask:** 255.255.255.0.

4.7.2 System Log

Choose "**Management**" \rightarrow "System Log", you can see the System Log screen, this screen (shown in Figure 4-104) allows you to view the system log and configure the system log options.

Device Info	System Log
Quick Setup	
Advanced Setup	
Wireless	The System Log dialog allows you to view the System Log and configure the System Log options.
Diagnostics	Click "View System Log" to view the System Log.
Management	Click "Configure System Log" to configure the System Log options.
+Settings	
• System Log	View System Log Configure System Log
 SNMP Agent 	
• TR-069 Client	

Figure 4-104

To View the System Log:

Click the **View System Log** button, you will see the screen (shown in Figure 4-105) which displays the Router's recent logs.

)ate/Time	Facility	Severity	Message
-----------	----------	----------	---------

Figure 4-105

- **Refresh:** Click the button, the information in the table will be updated.
- **Close:** Click the button, the screen will be closed.

To Configure the System Log Settings:

Click the **Configure System Log** button (shown in Figure 4-104), you will see the screen below (shown in Figure 4-106).

Device Info	System Log Configurati	ion					
Quick Setup							
Advanced Setup							
Wireless		n to log all the selected events. For the Log Level, all events above or equal to					
Diagnostics	the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the						
Management		remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.					
+Settings	Select the desired values and click 'Save/Apply'	to configure the system log options.					
• System Log	Log:	💿 Disable 🔘 Enable					
 SNMP Agent 	Log Level:	Debugging 😽					
• TR-069 Client	Display Level:	Error					
+Access Control	Mode:	Local 👻					
•Update Software	Server IP Address:						
• Reboot	Server UDP Port:						
		Save/Apply					

Figure 4-106

- Disable/Enable: Select the Enable to log the events, if you don't want to log these events, please select Disable.
- Log Level: Select the Log level in the drop-down list, for the Log level, all events above or equal to the selected level will be logged.
- Display Level: Select the Display level in the drop-down list, for the Display Level, all logged events above or equal to the selected level will be displayed.
- Mode: Select the mode to record the events. If the selected mode is Local, events will be recorded in the local memory. If the selected mode is Remote, events will be sent to the specified IP address and UDP port of the remote system log server. If the selected mode is Both, events will be sent to the local memory and the remote system log server.
- > Server IP Address: Type the address of the server you want to record the events.
- Server UDP Port: Type the UDP Port of the server.

4.7.3 SNMP Agent

Choose "**Management**"→"**SNMP Agent**", you can see the SNMP-Configuration screen as shown below.

SNMP (Simple Network Management Protocol) has been widely applied in the computer networks currently, which is used for ensuring the transmission of the management information between any two nodes. In this way, network administrators can easily search and modify the information on any node on the network. Meanwhile, they can locate faults promptly and implement the fault diagnosis, capacity planning and report generating.

An **SNMP Agent** is an application running on the Router that performs the operational role of receiving and processing SNMP messages, sending responses to the SNMP manager, and sending traps when an event occurs. So a Router contains SNMP "agent" software can be monitored and/or controlled by SNMP Manager using SNMP messages.

An **SNMP Manager** or SNMP Service is an application that performs the operational roles of generating SNMP messages/requests to modify and retrieve management information, and receiving the requested information and trap-event reports that are generated by the SNMP agent. SNMP Manager is the third-party management system. Monitor one is an SNMP Manager.

Device Info Quick Setup	SNMP - Configuration				
Advanced Setup					
Wireless	Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from				
Diagnostics	the SNMP agent in this device.				
Management	Select the desired values and click "Apply" to configure the SNMP options.				
+ Settings	The change of SNMP Community will not take effect until the Router reboot.				
• System Log	SNMP Agent:	⊙ Disable O Enable			
SNMP Agent	Read Community:	public			
• TR-069 Client	Set Community:	private			
+Access Control	System Name:	TP-LINK			
 Upgrade Firmware 	System Location:	unknown			
• Reboot	System Contact:	unknown			
	Trap Manager IP:	0.0.0.0			
		Save/Apply			

Figure 4-107

> **SNMP Agent:** You can select the checkbox to disable or enable the function.

P Note:

SNMP Community string provides a simple method of authentication between the Router (SNMP Agent) and a remote network manager (SNMP Manager). You can specify the community string as the password to authenticate the management station to the Router.

- Read Community: This field allows you to specify the SNMP Community string which provides read-only access to the Router that the community is only permitted to read the device configuration. The default value is "public".
- Set Community: This field allows you to specify the SNMP Community string which provides read and write access to the Router that the community has the authority to read and change the device configuration. The default value is "public".

- System Name: Enter alphanumeric string to specify an SNMP community string name. Your Router (SNMP agents) will expose management data on the managed systems as this "system name".
- > System Location: The person to notify when problems occur.
- > System contact: The location of the person that is identified as the system contact.
- Trap Manager IP: Enter the IP address of the SNMP Manager, where the SNMP Agent forwards trap notifications.

Select the desired values and click **Save/Apply** to configure the SNMP options.

4.7.4 TR-069 client

Choose "**Management**"→"**TR-069 client**", you can see the TR-069 client - Configuration screen as shown below.

TR-069 (WAN Management Protocol) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

Device Info	TR-069 client - Configuration					
Quick Setup						
Advanced Setup						
Wireless	WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration,					
Diagnostics	provision, collection, and diagnostics to this device.					
Management	Select the desired values and click "Save/Apply" to configure the TR-069 client options.					
+ Settings	Inform: 💿 Disable 🔘 Enable					
• System Log	Inform Interval: 300					
• SNMP Agent	ACS URL:					
• TR-069 Client	ACS User Name: admin					
+Access Control	ACS Password:					
• Update Software	WAN Interface used by TR-069 client: Any_WAN 🤜					
• Reboot	Disable 🔿 Enable					
	Connection Request Authentication					
	Connection Request User Name: admin					
	Connection Request Password:					
	Connection Request URL:					
	Save/Apply GetRPCMethods					

Figure 4-108

- > Inform: You can select the checkbox to disable or enable the Inform Interval.
- > Inform Interval: Type the interval time of your Router contact with the **ACS**.
- ACS URL: Please accept this information from your ISP. And through ACS (Auto-Configuration Server) you can perform auto-configuration, provision, collection, and diagnostics to this router.
- > ACS User Name: Please accept this User Name information from your ISP.
- > **ACS Password:** Please accept the Password information from your ISP.

P Note:

If you want to log on the ACS, you must own the ACS User Name and ACS Password.

- WAN Interface used by TR-069 Client: Please select the WAN Interface from the drop-down list to perform this function.
- > Connection Request User Name: Type the Connection Request User Name, set it yourself.
- > Connection Request Password: Type the Connection Request Password, set it yourself.

P Note:

The Connection Request User Name and Connection Request Password used for **ACS** log on the Router and manage it.

Select the desired values and click **Save/Apply** to configure the TR-069 client options.

4.7.5 Access Control

Choose "**Management**" \rightarrow "Access Control" \rightarrow "Password", you can see the screen (shown in Figure 4-109) which allows you to change the factory default password of the Router. The default password is the same as the user name, which is admin/admin, support/support, and user/user respectively.

Device Info	Access Control Password
Quick Setup	
Advanced Setup	
Wireless	Access to your DSL Modem Router is controlled through three user accounts: admin, support, and user.
Diagnostics	The user name "admin" has unrestricted access to change and view configuration of your DSL Router.
Management	The user name "support" is used to allow an ICP technisism to see as your DCI. Butter for maintenance and
+Settings	The user name "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics.
• System Log	The user name "user" can access the DSL Router, view configuration settings and statistics, as well as,
 SNMP Agent 	update the router's software.
• TR-069 Client	Use the fields below to enter up to 16 characters and click "Apply" to change or create passwords. Note:
-Access Control	Password cannot contain a space.
Passwords	Username:
•Update Software	Old Password:
• Reboot	New Password: support
	Confirm Password:
	Save/Apply

Figure 4-109

To change the password:

- 1. Select the **Username** whose password you want to change.
- 2. Enter the **Old Password** in the text box.
- 3. Enter the **New Password** and **Confirm Password**. The Confirm Password should be the same as the New Password.
- 4. Click Save/Apply to make your change take effect.

P Note:

 Access to your DSL Modem Router is controlled through three user accounts: admin, support, and user. The user name "admin" has unrestricted access to change and view configuration of your DSL Modem Router. The user name "support" is used to allow an ISP technician to access your DSL Modem Router for maintenance and to run diagnostics. The user name "user" can access the DSL Modem Router, view configuration settings and statistics, as well as, update the Router's software.

- 2) Both of admin and support accounts can do remote management. For security reasons, please change the default password for these two accounts when remote access function is enabled.
- 3) The password cannot contain a space, and its maximum length is 16 characters.

4.7.6 Update Firmware

Choose "**Management**" \rightarrow "**Update Firmware**", you can see the screen (shown in Figure 4-110) which allows you to upgrade the latest version software to keep the Router up to date.

Device Info	Tools Update Firmware
Quick Setup	
Advanced Setup	
Wireless	
Diagnostics	Step 1: Obtain an updated firmware image file from our website (<u>www.tp-link.com</u>).
Management	Step 2: Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.
+ Settings	Step 3: Click the "Update Firmware" button once to upload the new image file.
• System Log	NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot.
SNMP Agent	Firmware File Name:
• TR-069 Client	
+Access Control	
Upgrade Firmware	Update Firmware
• Reboot	opade i iniware

Figure 4-110

- **Browse:** Click the button to locate the latest software for the device.
- > **Update Firmware:** After you have selected the latest software, click the button.

To update the Router's software:

- 1. Download the latest software upgrade file from the TP-LINK website (http://www.tp-link.com).
- 2. Click **Browse** to view the folders and select the image file or enter the exact path to the image file location in the text box.
- 3. Click the **Update Firmware** button.

P Note:

- 1) There is no need to upgrade the firmware unless the new firmware has a new feature you want to use. However, when experiencing problems caused by the Router itself, you can try to upgrade the firmware.
- 2) Before upgrading the Router's firmware, you should write down some of your customized settings to avoid losing important configuration settings of the Router.
- 3) Do not turn off the Router or press the **Reset** button while the software is being updated.
- 4) The Router will reboot after the Upgrading is finished.

4.7.7 Reboot

Choose "**Management**" \rightarrow "**Reboot**", you can see the screen (shown in Figure 4-111) which allows you to reboot the Router.

Device Info	Reboot router
Quick Setup	
Advanced Setup	
Wireless	
Diagnostics	Click the button below to reboot the router.
Management	
+ Settings	
• System Log	
 SNMP Agent 	Reboot
• TR-069 Client	
+Access Control	
• Update Software	
• Reboot	

Figure 4-111

P Note:

- 1) After you clicked the **Reboot** button, please wait for a while before reopening your web browser.
- 2) Do not turn off the Router or press the **RESET** button while the Router is rebooting.
- 3) If necessary, reconfigure your PC's IP address to match your new configuration.

Appendix A: FAQ

1. How do I configure the Router to access Internet by ADSL users?

- 1) First, configure the ADSL Modem configured in RFC1483 bridge model.
- 2) Connect the Ethernet cable from your ADSL Modem to the WAN port on the Router. The telephone cord plugs into the Line port of the ADSL Modem.
- 3) Log in to the Router, and configure the WAN connection type as PPPoE connection mode. The detailed steps please refer to section 4.4.2.1 ATM-EoA-PPPoE.
- 4) If your ADSL lease is in "pay-according-time" mode, select "Dial on Demand" for Internet connection mode on the screen of Figure 4-10.

P Note:

If you are a Cable user, please configure the Router following the above steps.

2. How do I configure the Router to access Internet by Ethernet users?

Log in to the Router, and configure the WAN connection type as IPoE connection mode. The detailed steps please refer to section 4.4.2.2 ATM-EoA-IPoE.

3. I want to use NetMeeting, what do I need to do?

- 1) If you start NetMeeting as a sponsor, you don't need to do anything with the Router.
- 2) If you start as a response, you need to configure Virtual Server or DMZ Host.
- 3) How to configure Virtual Server: Log in to the Router, click the "Advanced Setup-NAT" menu on the left of your browser, and click "Virtual Servers" submenu. On the "Virtual Servers" page, click Add, and enter "1720" for the service port, using 192.168.1.222 for Server IP Address, remember to click the Save/Apply button.

nced Setup										
er2 Interface	Select the service i	name, and	enter the	server IP add	fress and cli	ck "Appl	y/Save" to forward	d IP packe	ets for this servi	e to the
N Service	specified server.									
	NOTE: The "Intern However, if you m									
lone	Remaining numbe	-								
	ι	Use Interface:			_38/ppp0	1				
rs	Service Name:									
ring	 Sele 	ct a Servic	e:	Mail (SMTF	")			~		
	O Cust	tom Servic	e:							
	Ŭ	er IP Addre		192.168.1		=				
ntrol	Serve	a ir Audre	33.	192.100.1.						
rvice										
ntrol										
	External Port St	tart E	xternal	Port End	Protocol		Internal Por	t Start	Internal Po	rt End
	External Port St 25		E xternal 25	Port End	Protocol TCP	*	Internal Por 25	t Start	Internal Po 25	ort End
				Port End				t Start		ort End
				Port End	TCP	~		t Start		ort End
				Port End	TCP TCP	*		t Start		ort End
				Port End	TCP TCP TCP	*		t Start		ort End
				Port End	TCP TCP TCP TCP	*		t Start		
ing				Port End	TCP TCP TCP TCP TCP	*		t Start		
ing				Port End	TCP TCP TCP TCP TCP TCP TCP TCP	× × × × × × × × ×		t Start		
9				Port End	TCP TCP TCP TCP TCP TCP TCP TCP	× × × ×				
bing				Port End	TCP TCP TCP TCP TCP TCP TCP TCP TCP					
				Port End	TCP TCP					
puping				Port End	TCP TCP TCP TCP TCP TCP TCP TCP TCP					Image: Control

P Note:

Your opposite side should call your WAN IP, which is displayed on the "Status" page.

4) How to enable DMZ Host: Log in to the Router, click the "Advanced Setup-NAT" menu on the left of your browser, and click "DMZ Host" submenu. On the "DMZ" page, type your IP address into the "DMZ Host IP Address" field, using 192.168.1.222 as an example, remember to click the Save/Apply button.

Device Info	NAT DMZ Host				
Quick Setup					
Advanced Setup					
+Layer2 Interface	The DSL Modem Router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.				
• WAN Service					
• LAN	Enter the computer's IP address and click "Save/Apply" to activate the DMZ host.				
• MAC Clone					
-NAT	Clear the IP address field and click "Apply" to deactivate the DMZ host.				
Virtual Servers					
• Port Triggering	DMZ Host IP Address: 192.168.1.222				
DMZ Host					
+Security	Save/Apply				
+Parental Control	Save/ Appry				
+Quality of Service					

4. I want to build a WEB Server on the LAN, what should I do?

Log in to the Router, click the "Advanced Setup-NAT" menu on the left of your browser, and click

the "Virtual Servers" submenu. On the "Virtual Servers" page, click Add New, then on the "Add or Modify a Virtual Server" page, enter use "80" as service port, and your IP address next to the "Server IP Address", assuming 192.168.1.188 for an example, and remember to click the Save/Apply button.

Device Info								
	NAT Virtual	l Serv	ers					
Quick Setup								
Advanced Setup								
+Layer2 Interface	Select the service name, the specified server.	and enter	the server IP a	ddress and clic	k "Ap	ply/Save" to forward IP p	ackets for this servi	ce to
• WAN Service	NOTE: The "Internal Port							
•LAN	End". However, if you me Port Start".	odify "Inter	rnal Port Star	", then "Interna	I Po	t End" will be set to the	same value as "Int	ternal
• MAC Clone	Remaining number of er	ntries that	can be config	ured: 32				
-NAT	Use Inter	rface:	pppoe_0_0_38/ppp0 🗸					
Virtual Servers	Service Name:							
Port Triggering	🔘 Select a Sen	vice:	Select One			*		
DMZ Host	Oustom Ser	vice:	WEB Serv	er on the LAN	1			
+ Security + Parental Control	Server IP Add	Iress:	192 168 1 188					
+Quality of Service								
+Quality of Service +Traffic Control								
+Routing +DNS	External Port Start	_	I Port End	Protocol		Internal Port Start	Internal Port E	nd
•DNS	80	80			~	80	80	
•UPnP					*			
Interface Grouping				TCP	*			
LAN Ports				ТСР	*			
• IP Sec				TCP	*]
Wireless				TCP	~			1
Diagnostics				TCP	~			1
Management				TCP	~			1
Junagomon				TCP	~			1
				TCP	~			1
				TCP	~			
					~			1
				101				
				Apply/Sav				

Solution Note:

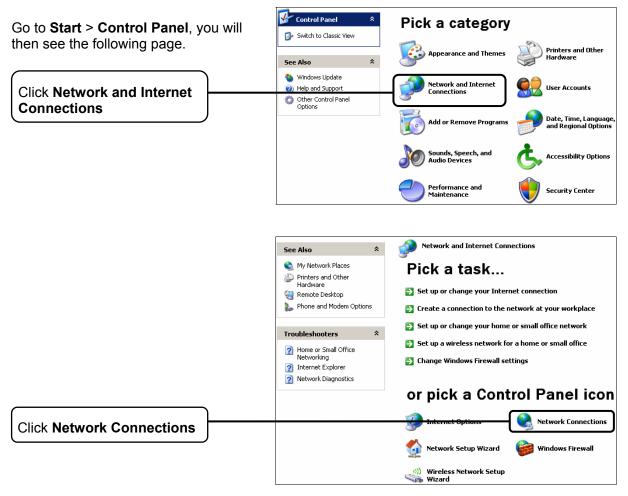
Because the WEB Server port 80 will interfere with the WEB management port 80 on the Router, you will be prompt to change the WEB management port number to avoid interference.



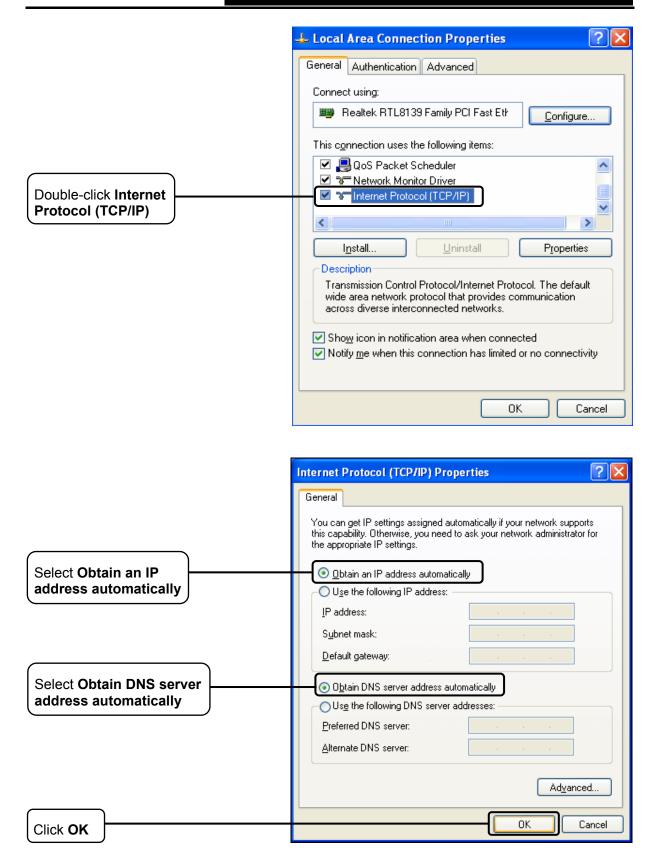
- 5. The wireless stations cannot connect to the Router.
- 1) Make sure the **"Enable Wireless Router Radio"** is checked.
- 2) Make sure that the wireless stations' SSID accord with the Router's SSID.
- 3) Make sure the wireless stations have right KEY for encryption when the Router is encrypted.
- If the wireless connection is ready, but you can't access the Router, check the IP Address of your wireless stations.

Appendix B: Configuring the PC

For Windows XP OS



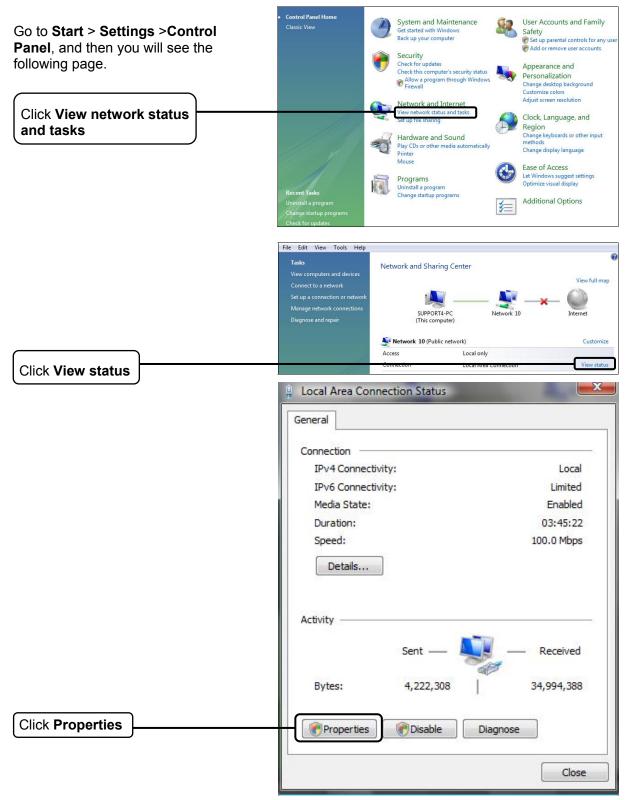
	LAN or High-Speed Internet	
Right-click Local Area	Create a new	
Connection	Connection Set up a home or small office network	F Disable Status
	Change Windows Firewall settings	Repair
	Sisable this network device	Bridge Connections
	🗞 Repair this connection	Create Shortcut
	Rename this connection	Delete
	View status of this connection	Rename Properties
Click Properties	Change settings of this connection	



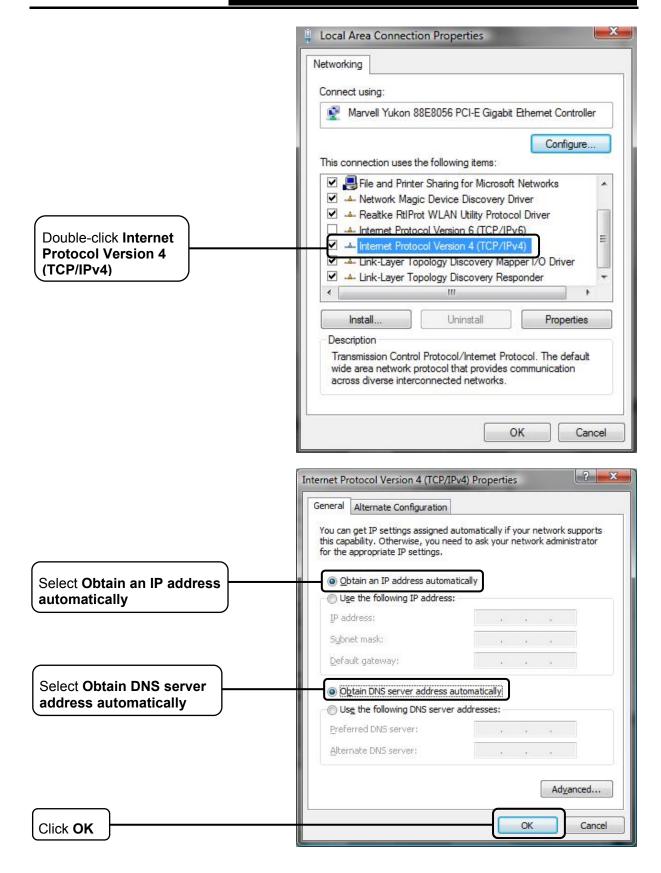
🕹 Local Area Connection Properties 🛛 🔹 💽
General Authentication Advanced
Connect using:
This connection uses the following items:
✓ % Network Monitor Driver ✓ % Internet Protocol (TCP/IP)
Install Uninstall Properties
Description Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
 Show icon in notification area when connected Notify me when this connection has limited or no connectivity
OK Cancel

Click OK

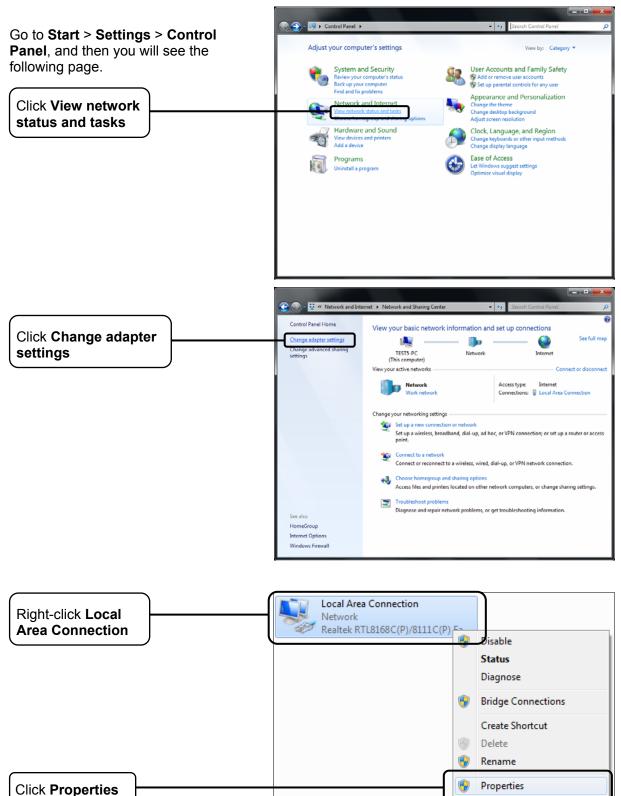
For Windows Vista OS



TD-W8960N 300Mbps Wireless N ADSL2+ Modem Router User Guide



For Windows 7 OS



TD-W8960N 300Mbps Wireless N ADSL2+ Modem Router User Guide

	📮 Local Area Connection Properties
	Networking
	Connect using:
	Realtek RTL8168C(P)/8111C(P) Family PCI-E Gigabit Eth
	Configure This connection uses the following items:
	Client for Microsoft Networks
Double click Internet	Generation Constants
Double-click Internet Protocol Version 4 (TCP/IPv4)	
	 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
	Internet Protocol Version 4 (TCP/IPv4) Properties
Select Obtain an IP	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.
Select Obtain an IP address automatically	General Alternate Configuration You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator
	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. Image: Configuration of the appropriate IP settings. Image: Configuration of the appropriate IP settings.
	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. Image: Optimized properties of the properties of t
	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. Image: Optimized properties of the properties of t
address automatically Select Obtain DNS server	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. • Qbtain an IP address automatically • Uge the following IP address: IP address: Subnet mask: Default gateway: Obtain DNS server address automatically
address automatically	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. Image: Configuration of the appropriate IP settings. Image: Configuratin the appropriate IP settings. <tr< th=""></tr<>
address automatically Select Obtain DNS server	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. Image: Configuration of the appropriate IP settings. Image: Configuratin the appropriate IP settings. <tr< th=""></tr<>
address automatically Select Obtain DNS server	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. Image: Configuration of the appropriate IP settings. Image: Configuratin the appropriate IP settings. <tr< th=""></tr<>
address automatically Select Obtain DNS server	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. Image: Configuration of the appropriate IP settings. Image: Configuratin the appropriate IP settings. <tr< th=""></tr<>
address automatically Select Obtain DNS server	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. • Qbtain an IP address automatically • Uge the following IP address: IP address: Subnet mask: Default gateway: O Dbtain DNS server address automatically Default gateway: Qbtain DNS server: Alternate DNS server: Alternate DNS server:

Appendix C: Specifications

General				
Standards	ANSI T1.413, ITU G.992.1, ITU G.992.2, ITU G.992.3, ITU G.992.5, IEEE 802.3, IEEE 802.3u, IEEE 802.11b , IEEE 802.11g , 802.11n			
Protocols	TCP/IP, IPoA , PPPoA , PPPoE, SNTP, HTTP, DHCP, ICMP, NAT			
Ports	LAN Ports: Four 10/100M Auto-Negotiation RJ45 ports (Auto MDI/MDIX)			
	Line Port: One RJ11 port			
Cabling Type		JTP category 3, 4, 5 cable (maximum 100m) ΞΙΑ/ΤΙΑ-568 100Ω STP (maximum 100m)		
		JTP category 5, 5e cable (maximum 100m) ΞΙΑ/ΤΙΑ-568 100Ω STP (maximum 100m)		
LED	1,2,3,4(LAN), WLAN, ADSL			
	Power, Internet, QSS			
Safety & Emissions	FCC, CE			

Wireless		
Frequency Band	2.4~2.4835GHz	
Radio Data Rate	 11n: up to 300Mbps (Automatic) 11g: 54/48/36/24/18/12/9/6Mbps (Automatic) 11b: 11/5.5/2/1Mbps (Automatic) 	
Frequency Expansion	DSSS(Direct Sequence Spread Spectrum)	
Modulation	DBPSK, DQPSK, CCK, OFDM, 16-QAM, 64-QAM	
Security	WEP/WPA/WPA2/WPA2-PSK/WPA-PSK	
Sensitivity @PER	270M: -62dBm@10% PER 130M: -64dBm@10% PER 54M: -68dBm@10% PER 11M: -85dBm@8% PER 6M: -88dBm@10% PER 1M: -90dBm@8% PER	

Environmental and Physical			
Temperature.	Operating:	0℃~40℃ (32°F~104°F)	
	Storage:	-40℃~70℃(-40°F~158°F)	
Humidity	Operating:	10% ~ 90% RH, Non-condensing	
	Storage:	5% ~ 90% RH, Non-condensing	

Appendix D: Glossary

- 802.11n 802.11n builds upon previous 802.11 standards by adding MIMO (multiple-input multiple-output). MIMO uses multiple transmitter and receiver antennas to allow for increased data throughput via spatial multiplexing and increased range by exploiting the spatial diversity, perhaps through coding schemes like Alamouti coding. The Enhanced Wireless Consortium (EWC) [3] was formed to help accelerate the IEEE 802.11n development process and promote a technology specification for interoperability of next-generation wireless local area networking (WLAN) products.
- 802.11b The 802.11b standard specifies a wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHz, and WEP encryption for security. 802.11b networks are also referred to as Wi-Fi networks.
- 802.11g specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology, using OFDM modulation and operating in the unlicensed radio spectrum at 2.4GHz, and backward compatibility with IEEE 802.11b devices, and WEP encryption for security.
- 2x to 3x eXtended Range[™] WLAN Transmission Technology The WLAN device with 2x to 3x eXtended Range[™] WLAN transmission technology make its sensitivity up to 105 dB, which gives users the ability to have robust, longer-range wireless connections. With this range-enhancing technology, a 2x to 3x eXtended Range[™] based client and access point can maintain a connection at as much as three times the transmission distance of traditional 802.11b and 802.11g products, for a coverage area that is up to nine times greater. A traditional 802.11b and 802.11g product transmission distance is about 300m, a 2x to 3x eXtended Range[™] based client and access point can maintain a connection at as much as three transmission distance is about 300m, a 2x to 3x eXtended Range[™] based client and access point can maintain a connection transmission distance may be up to 830m.
- Access Point A device that allows wireless-equipped computers and other devices to communicate with a wired network. Also used to expand the range of a wireless network.
- Ad-hoc Network An ad-hoc network is a group of computers, each with a wireless adapter, connected as an independent IEEE 802.11 wireless LAN. Ad-hoc wireless computers operate on a peer-to-peer basis, communicating directly with each other without the use of an access point. Ad-hoc mode is also referred to as an Independent Basic Service Set (IBSS) or as peer-to-peer mode, and is useful at a departmental scale or SOHO operation.
- AES (Advanced Encryption Standard) A security method that uses symmetric 128-bit block data encryption.
- ACS (Auto-Configuration Server) Through ACS (Auto-Configuration Server) you can perform auto-configuration, provision, collection, and diagnostics to the device.
- ATM (Asynchronous Transfer Mode) ATM is a cell based transfer mode that requires variable length user information to be segmented and reassembled to/from short, fixed length cells. It uses two different methods for carrying connectionless network interconnect traffic, routed and bridged Protocol Data Units (PDUs), over an ATM network.
- **Bridging -** A device that connects different networks.
- Browser An application program that provides a way to look at and interact with all the information on the World Wide Web.

- DDNS (Dynamic Domain Name System) Allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (e.g., www.xyz.com) and a dynamic IP address.
- > **Default Gateway -** A device that forwards Internet traffic from your local area network.
- DHCP A networking protocol that allows administrators to assign temporary IP addresses to network computers by "leasing" an IP address to a user for a limited amount of time, instead of assigning permanent IP addresses.
- DMZ (Demilitarized Zone) Removes the Router's firewall protection from one PC, allowing it to be "seen" from the Internet.
- DNS (Domain Name Server) The IP address of your ISP's server, which translates the names of websites into IP addresses.
- **Domain -** A specific name for a network of computers.
- DSL (Digital Subscriber Line) An always-on broadband connection over traditional phone lines.
- > **Dynamic IP Address -** A temporary IP address assigned by a DHCP server.
- EAP (Extensible Authentication Protocol) A general authentication protocol used to control network access. Many specific authentication methods work within this framework.
- **Encryption -** Encoding data transmitted in a network.
- Ethernet IEEE standard network protocol that specifies how data is placed on and retrieved from a common transmission medium.
- Firewall A set of related programs located at a network gateway server that protects the resources of a network from users from other networks.
- Gateway A device that interconnects networks with different, incompatible communications protocols.
- IEEE 802.11b The IEEE 802.11b standard specifies a wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHz, and WEP encryption for security. IEEE 802.11b networks are also referred to as Wi-Fi networks.
- IEEE 802.11g Specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology, using OFDM modulation and operating in the unlicensed radio spectrum at 2.4GHz, and backward compatibility with IEEE 8021b devices, and WEP encryption for security.
- Infrastructure Network An infrastructure network is a group of computers or other devices, each with a wireless adapter, connected as an IEEE 802.11 wireless LAN. In infrastructure mode, the wireless devices communicate with each other and to a wired network by first going through an access point. An infrastructure wireless network connected to a wired network is referred to as a Basic Service Set (BSS). A set of two or more BSS in a single network is referred to as an Extended Service Set (ESS). Infrastructure mode is useful at a corporation scale, or when it is necessary to connect the wired and wireless networks.
- > **IP Address** The address used to identify a computer or device on a network.
- IPoA (IP and ARP over ATM) A protocol that provides extensions to the IP Group for handling IP over ATM flows.
- > **ISP** (Internet Service Provider) A company that provides access to the Internet.

- > LAN The computers and networking products that make up your local network.
- MAC (Media Access Control) Address The unique address that a manufacturer assigns to each networking device.
- NAT (Network Address Translation) NAT technology translates IP addresses of a local area network to a different IP address for the Internet.
- MER (MAC Encapsulation Routing) MER allows IP packet to be carried as bridged frames. There are many applications, such as IPoA, DSL networks and other frame-based network. Depending on your equipment, they can be either bridged or routed within the network.
- Network A series of computers or devices connected for the purpose of data sharing, storage, and/or transmission between users.
- Ping (Packet Internet Groper) An Internet utility used to determine whether a particular IP address is online.
- Port The connection point on a computer or networking device used for plugging in cables or adapters.
- PPPoE (Point to Point Protocol over Ethernet) PPPoE stands for Point to Point protocol over Ethernet, this protocol is used as a type of broadband connection that provides authentication (username and password) in addition to data transport.
- PPPoA (Point to Point Protocol over ATM) PPPoA stands for Point to Point protocol over ATM, this protocol is also used as a type of broadband connection that provides authentication (username and password) in addition to data transport.
- RADIUS (Remote Authentication Dial-In User Service) A protocol that uses an authentication server to control network access.
- **RJ45** (Registered Jack-45) An Ethernet connector that holds up to eight wires.
- **Router -** A networking device that connects multiple networks together.
- RPC (Remote Procedure Calls) RPC is a powerful technique for constructing distributed, client-server based applications. It is based on extending the notion of convention, or local procedure calling, so that the called procedure need not exist in the same address space as the calling procedure. The two processes may be on the same system, or they may be on different systems with a network connecting them. By using RPC, programmers of distributed applications avoid the details of the interface with the network. The transport independence of RPC isolates the application from the physical and logical elements of the data communications mechanism and allows the application to use a variety of transports.
- Server Any computer whose function in a network is to provide user access to files, printing, communications, and other services.
- SOHO (Small Office/Home Office) Market segment of professionals who work at home or in small offices.
- SSID A Service Set Identification is a thirty-two character (maximum) alphanumeric key identifying a wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID. This is typically the configuration parameter for a wireless PC card. It corresponds to the ESSID in the wireless Access Point and to the wireless network name.
- Static IP Address A fixed address assigned to a computer or device that is connected to a network.

- > Static Routing Forwarding data in a network via a fixed path.
- Subnet Mask An address code that determines the size of the network.
- TCP (Transmission Control Protocol) A network protocol for transmitting data that requires acknowledgement from the recipient of data sent.
- TCP/IP (Transmission Control Protocol/Internet Protocol) A set of instructions PCs use to communicate over a network.
- TKIP (Temporal Key Integrity Protocol) a wireless encryption protocol that provides dynamic encryption keys for each packet transmitted.
- UDP (User Datagram Protocol) A network protocol for transmitting data that does not require acknowledgement from the recipient of the data that is sent.
- > VCI (Virtual Channel Identifier) The identifier of the VC contained in the ATM cell header.
- > **VPI** (Virtual Path Identifier) The identifier of the VP contained in the ATM cell header.
- > **Update -** To replace existing software or firmware with a newer version.
- VLAN (Virtual Local Air Network) Logical subgroups that constitute a Local Area Network (LAN). This is done in software rather than defining a hardware solution.
- VLAN ID (0-4095) Indicates the ID number of the VLAN being configured. Up to 256 VLANs can be created.
- > WAN (Wide Area Network) Networks that cover a large geographical area.
- > Web-based Utility The web page that allows you to manage the Router.
- WEP (Wired Equivalent Privacy) A data privacy mechanism based on a 64-bit or 128-bit or 152- bit shared key algorithm, as described in the IEEE 802.11g standard.
- Wi-Fi A trade name for the IEEE 802.11b wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see <u>http://www.wi-fi.net</u>), an industry standards group promoting interoperability among IEEE 802.11b devices.
- WLAN (Wireless Local Area Network) A group of computers and associated devices communicate with each other wirelessly, which network serving users are limited in a local area.
- WPA (Wi-Fi Protected Access) A wireless security protocol use TKIP (Temporal Key Integrity Protocol) encryption, which can be used in conjunction with a RADIUS server.

Appendix E: Technical Support

Technical Support

- For more troubleshooting help, go to: www.tp-link.com/support/faq.asp
- To download the latest Firmware, Driver, Utility and User Guide, go to: www.tp-link.com/support/download.asp
- For all other technical support, please contact us by using the following details:

<u>Global</u>

Tel: +86 755 26504400 E-mail: support@tp-link.com Service time: 24hrs, 7 days a week

Australia & New Zealand Tel: AU 1300 87 5465

NZ 0800 87 5465 E-mail: support@tp-link.com.au Service time: 24hrs, 7 days a week

Singapore

Tel: +65 62840493 E-mail: support.sg@tp-link.com Service time: 24hrs, 7 days a week

<u>UK</u>

Tel: +44 (0) 845 147 0017 E-mail: support.uk@tp-link.com Service time: 24hrs, 7 days a week

USA/Canada

Toll Free: +1 866 225 8139 E-mail: support.usa@tp-link.com Service time: 24hrs, 7 days a week

<u>Germany / Austria</u>

Tel: +49 1805 875465 (German Service) / +49 1805 TPLINK E-mail: support.de@tp-link.com Fee: 0.14 EUR/min from the German fixed phone network and up to 0.42 EUR/min from mobile phone Service time: Monday to Friday 9:00 AM to 6:00 PM GMT+ 1 or GMT+ 2

(Daylight Saving Time in Germany)

*Except bank holidays in Hesse

<u>Malaysia</u>

Tel: 1300 88 875465 (1300 88TPLINK) Email: support.my@tp-link.com Service time: 24hrs, 7 days a week

<u>Turkey</u>

Tel: 444 19 25 (Turkish Service) E-mail: support.tr@tp-link.com Service time: 9:00 AM to 6:00 PM 7 days a week

Italy

Tel: +39 02 66987799 E-mail: support.it@tp-link.com Service time: 9:00 AM to 6:00 PM Monday to Friday

Switzerland

Tel: +41 (0)848 800998 (German Service) E-mail: support.ch@tp-link.com Fee: 4-8 Rp/min, depending on rate of different time Service time: Monday to Friday 9:00 AM to 6:00 PM GMT+ 1 or GMT+ 2 (Daylight Saving Time)