# TP-LINK®

# **User Guide**

# **TD-W8961ND**

# Wireless N ADSL2+ Modem Router



Rev: 1.0.1 1910010351

# **COPYRIGHT & TRADEMARKS**

Specifications are subject to change without notice. **TP-LINK**<sup>®</sup> 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 © 2010 TP-LINK TECHNOLOGIES CO., LTD. All rights reserved.

http://www.tp-link.com

# **FCC STATEMENT**



This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to pro-vide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not in-stalled 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**

# **CE1588**

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.

# **DECLARATION OF CONFORMITY**

For the following equipment:

Product Description: Wireless N ADSL2+ Modem Router

Model No.: TD-W8961ND

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 EN60950-1:2006 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 EN 61000-3-3:1995+A1:2001+A2:2005 Directives 2006/95/EC The above product is in conformity with the following standards or other normative documents EN 60950-1:2006

Directive (ErP) 2009/125/EC

Audio/Video, information and communication technology equipment- Environmentally conscious design

### EN62075:2008

Person is responsible for marking this declaration:

### Yang Hongliang

**Product Manager of International Business** 

TP-LINK TECHNOLOGIES CO., LTD. South Building, No.5 Keyuan Road, Central Zone, Science & Technology Park, Nanshan, Shenzhen, P. R. China

CONT	ENTS
------	------

Package Co	ontents	1
Chapter 1	Introduction	2
1.1	Product Overview	2
1.2	Main Features	2
1.3	Conventions	3
Chapter 2	Hardware Installation	4
2.1	The Front Panel	4
2.2	The Back Panel	5
2.3	Installation Environment	5
2.4	Connecting the Router	6
Chapter 3	Quick Installation Guide	8
3.1	Configure PC	8
3.2	Login	11
Chapter 4	Software Configuration	14
4.1	Status	14
	4.1.1 Device Info	14
	4.1.2 System Log	15
	4.1.3 Statistics	16
4.2	Quick Start	18
4.3	Interface Setup	18
	4.3.1 Internet	19
	4.3.2 LAN	24
	4.3.3 Wireless	27
4.4	Advanced Setup	
	4.4.1 Firewall	
	4.4.2 Routing	38
	4.4.3 NAT	39
	4.4.4 QoS	42
	4.4.5 VLAN	
	4.4.6 ADSL	46
4.5	Access Management	
	4.5.1 ACL	47
	4.5.2 Filter	48

	4.5.3	SNMP	. 56
	4.5.4	UPnP	. 56
	4.5.5	DDNS	. 57
	4.5.6	CWMP	. 57
4.6	Maint	enance	. 58
	4.6.1	Administration	. 58
	4.6.2	Time Zone	. 59
	4.6.3	Firmware	. 60
	4.6.4	System Restart	. 62
	4.6.5	Diagnostic	. 62
4.7	Help.		. 63
Appendix A	: Spec	cifications	. 65

# **Package Contents**

The following contents should be found in your package:

- > One TD-W8961ND Wireless N ADSL2+ Modem Router
- > One Power Adapter for TD-W8961ND Wireless N ADSL2+ Modem Router
- Quick Installation Guide
- > One RJ45 cable
- ➢ Two RJ11 cables
- > One ADSL splitter
- > One Resource CD, which includes this User Guide

### Solution 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 Introduction

Thank you for choosing the TD-W8961ND Wireless N ADSL2+ Modem Router.

# **1.1 Product Overview**

The device is designed to provide a simple and cost-effective ADSL Internet connection for a private Ethernet or IEEE 802.11n/ IEEE 802.11g/ IEEE 802.11b wireless network.

The TD-W8961ND connects to an Ethernet LAN or computers via standard Ethernet ports. The ADSL connection is made using ordinary telephone line with standard connectors. Multiple workstations can be networked and connected to the Internet using a single Wide Area Network (WAN) interface and single global IP address. The advanced security enhancements, **IP/MAC Filter**, **Application Filter** and **URL Filter** can help to protect your network from potentially devastating intrusions by malicious agents from the outside of your network.

**Quick Start** of the Web-based Utility is supplied and friendly help messages are provided for the configuration. Network and Router management is done through the Web-based Utility which can be accessed through local Ethernet using any web browser.

# ADSL

The TD-W8961ND 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.

# Wireless

In the most attentive wireless security, the Router provides multiple protection measures. It can be set to turn off the wireless network name (SSID) broadcast so that only stations that have the SSID can be connected. The Router provides wireless LAN 64/128-bit WEP encryption security, WPA-PSK/WPA2-PSK authentication, as well as TKIP/AES encryption security.

# 1.2 Main Features

- > Four 10/100Mbps Auto-Negotiation RJ45 LAN ports (Auto MDI/MDIX), one RJ11 port.
- > Provides external splitter.
- > Adopts Advanced DMT modulation and demodulation technology.
- > Supports bridge mode and Router function.
- > Multi-user sharing a high-speed Internet connection.
- Downstream data rates up to 24Mbps, upstream data rates up to 3.5Mbps (With Annex M enabled).
- Supports long transfers, the max line length can reach to 6.5Km.
- > Supports remote configuration and management through SNMP and CWMP.
- > Supports PPPoE, it allows connecting the internet on demand and disconnecting from the

Internet when idle.

- Provides reliable ESD and surge-protect function with quick response semi-conductive surge protection circuit.
- > High speed and asymmetrical data transmit mode, provides safe and exclusive bandwidth.
- > Supports All ADSL industrial standards.
- > Compatible with all mainstream DSLAM (CO).
- > Provides integrated access of internet and route function which face to SOHO user.
- > Real-time Configuration and device monitoring.
- Supports Multiple PVC (Permanent Virtual Circuit).
- ➢ Built-in DHCP server.
- > Built-in firewall, supporting IP/MAC filter, Application filter and URL filter.
- Supports Virtual Server, DMZ host and IP Address Mapping.
- > Supports Dynamic DNS, UPnP and Static Routing.
- > Supports system log and flow Statistics.
- > Supports firmware upgrade and Web management.
- > Provides WPA-PSK/WPA2-PSK data security, TKIP/AES encryption security.
- > Provides 64/128-bit WEP encryption security and wireless LAN ACL (Access Control List).

# 1.3 Conventions

The Router or device mentioned in this User Guide stands for TD-W8961ND without any explanations.

Parameters provided in the pictures are just references for setting up the product, which may differ from the actual situation.

# Chapter 2 Hardware Installation

# 2.1 The Front Panel



Figure 2-1

The LEDs locate on the front panel, they indicate the device's working status. For details, please refer to LED Explanation.

# LED Explanation:

Name	Status	Indication
Devuer	On	Power is on.
Power	Off	Power is off.
	Flash	The ADSL negotiation is in progress.
ADSL	On	The LINE port is linked up.
	Off	The LINE port is linked down.
	Off	There is no successful PPP connection or the Router works on Bridge mode.
Internet	On	A successful PPP connection has been built.
	Flash	Data is being transferred over the Internet.
	On	The wireless function is enabled but no data is being transmitted.
WLAN	Flash	There is wireless data being transmitted.
	Off	The wireless function is disabled.
	Flash	Data is being transferred over the 1-4 (LAN) port.
LAN(1-4)	On	There is a successful connection on the corresponding 1-4 (LAN) port but no activity.
	Off	There is no connection on the corresponding 1-4 (LAN) port or the connection is abnormal.
	Slow Flash	A wireless device is connecting to the network by QSS function. This process will last in the first 2 minutes.
QSS	On	A wireless device has been successfully added to the network by QSS function.
	Quick Flash	A wireless device failed to be added to the network by QSS function.

### P Note:

After a device is successfully added to the network by QSS function, the QSS LED will keep on for about 5 minutes and then turn off.

# 2.2 The Back Panel

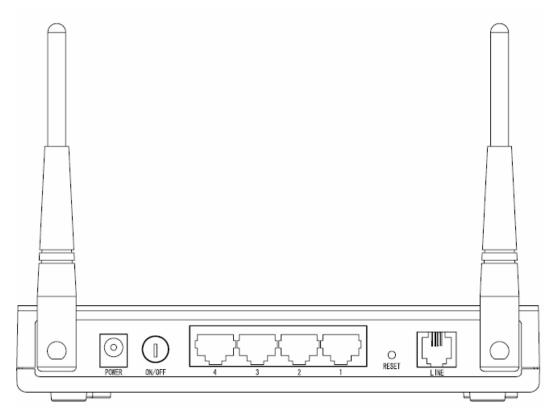


Figure 2-2

- > **POWER**: The Power plug is where you will connect the power adapter.
- 1, 2, 3, 4 (LAN): Through the port, you can connect the Router to your PC or the other Ethernet network devices.
- RESET: There are two ways to reset the Router's factory defaults.
   Method one: 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.
   Method two: Restore the default setting from "Maintenance-SysRestart" of the Router's Web-based Utility.
- LINE: Through the port, you can connect the router with the telephone. Or you can connect them by an external separate splitter. For details, please refer to 2.4.
- > Antenna: Used for wireless operation and data transmit.

# 2.3 Installation Environment

- > The Product should not be located where it will be exposed to moisture or excessive heat.
- Place the Router in a location where it can be connected to the various devices as well as to a power source.

- Make sure the cables and power cord are safely placed out of the way so they do not create a tripping hazard.
- > The Router can be placed on a shelf or desktop.
- Keep away from the strong electromagnetic radiation and the device of electromagnetic sensitive.

# 2.4 Connecting the Router

Before installing the device, please make sure your broadband service provided by your ISP is available. If there is any problem, please contact your ISP. Before cable connection, cut off the power supply and keep your hands dry. You can follow the steps below to install it.

**Step 1:** Connect the ADSL Line.

**Method one:** Plug one end of the twisted-pair ADSL cable into the ADSL LINE port on the rear panel of TD-W8961ND, and insert the other end into the wall socket.

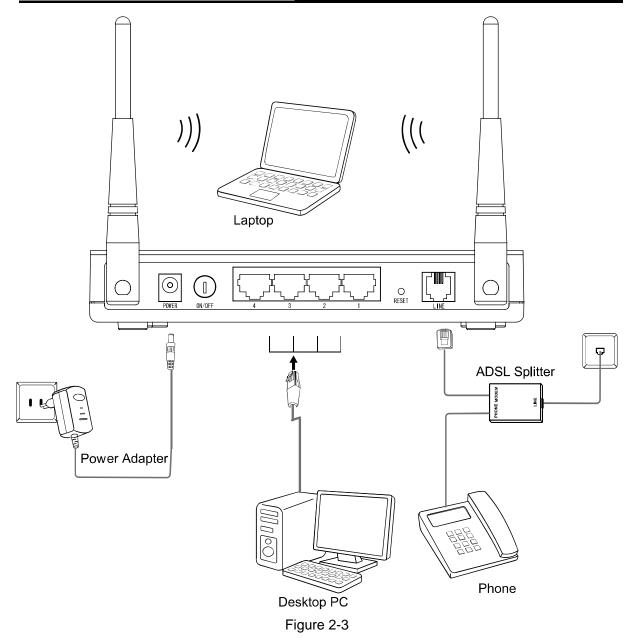
**Method two:** You can use a separate splitter. External splitter can divide the data and voice, and then you can access the Internet and make calls at the same time. The external splitter has three ports:

- LINE: Connect to the wall jack
- PHONE: Connect to the phone sets
- MODEM: Connect to the ADSL LINE port of TD-W8961ND

Plug one end of the twisted-pair ADSL cable into the ADSL LINE port on the rear panel of TD-W8961ND. Connect the other end to the MODEM port of the external splitter.

- Step 2: Connect the Ethernet cable. Attach one end of a network cable to your computer's Ethernet port or a regular hub/switch port, and the other end to the LAN port on the TD-W8961ND.
- Step 3: Power on the computers and LAN devices.
- **Step 4:** Attach the power adapter. Connect the power adapter to the power connector on the rear of the device and plug in the adapter to a wall outlet or power extension.

TD-W8961ND Wireless N ADSL2+ Modem Router User Guide



# Chapter 3 Quick Installation Guide

# 3.1 Configure PC

After you directly connect your PC to the TD-W8961ND 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.

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

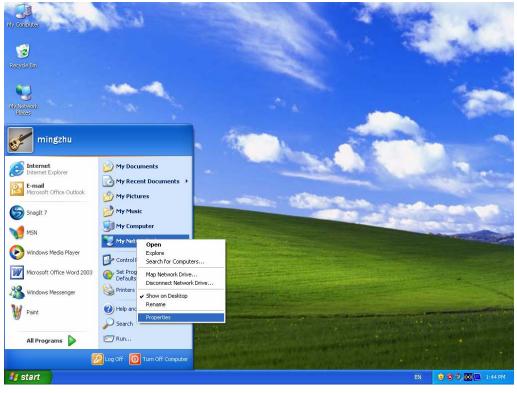


Figure 3-1

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

Network Connections		
le Edit View Favorites Tools	Advanced Help	
3 Back 👻 🕥 - 🏂 🔎 See	arch 🎼 Folders 🛄 -	
dress 🔕 Network Connections		💌 🄁 Go
Network Tasks	LAN or High-Speed Internet	
Create a new	Local Area Connection	
Set up a home or small office network	C Disable Status	
Change Windows Firewall settings	Repair Bridge Connections	
Disable this network device	Create Shortcut	
Repair this connection	Delete	
Rename this connection	Rename	
View status of this connection	Properties	
Change settings of this connection		
Other Places		
Control Panel		
My Network Places		
My Documents		
😼 My Computer		
V		



**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:
Realtek RTL8139 Family PCI Fast Etł <u>C</u> onfigure
This connection uses the following items:
<ul> <li>Client for Microsoft Networks</li> <li>Elia and Brinter Sharing for Microsoft Networks</li> </ul>
<ul> <li>File and Printer Sharing for Microsoft Networks</li> <li>QoS Packet Scheduler</li> </ul>
✓ Treatment Protocol (TCP/IP)
I <u>n</u> stall Uninstall Properties
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

Figure 3-3

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

Internet Protocol (TCP/IP) Proper	ties 🛛 🛛 🔀
General	
You can get IP settings assigned autom this capability. Otherwise, you need to a the appropriate IP settings.	
Obtain an IP address automatically	,
O 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 D <u>b</u> tain DNS server address autom	atically
OUse 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	
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64	
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64	
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	

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),
```



You can check it follow the steps below:

- 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 ~ 192.168.1.254.

# 3.2 Login

Once your host PC is properly configured, please proceed as follows to use the Web-based Utility: Start your web browser and type the private IP address of the Router in the URL field: **192.168.1.1**.



After that, you will see the screen shown below, enter the default User Name **admin** and the default Password **admin**, and then click **OK** to access to the **Quick Setup** screen. You can follow the steps below to complete the Quick Setup.



Figure 3-7

# Step 1: Select the Quick Start tab, then click RUN WIZARD, and you will see the next screen. Click the NEXT button.

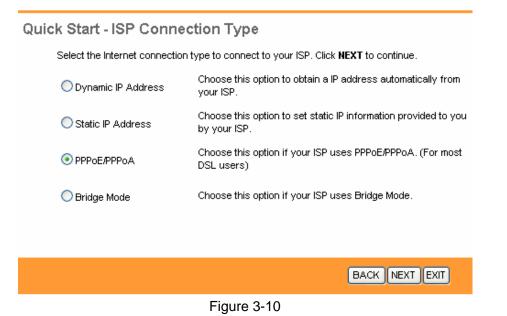
Quick Start	
The Wizard will guide you through these four quick steps. Begin by clicking on NEXT.	
Step 1. Choose your time zone	
Step 2. Set your Internet connection	
Step 3. Wireless network configuration	
Step 4. Save settings of this ADSL Router	
NEXTEXIT	
Figure 3-8	

**Step 2:** Configure the time for the Router, and then click the **NEXT** button.

Quick Start - Time Zone
Select the appropriate time zone for your location and click <b>NEXT</b> to continue.
(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London
BACK NEXT EXIT



**Step 3:** Select the connection type to connect to the ISP (We select **PPPoE/PPPoA** mode for example here), and then click the **NEXT** button.



Step 4: Configure the following options provided by your ISP: Username, Password, VPI, VCI and Connection Type. Then click Next.

Quick Start - PPPoE/PPPoA
Enter the PPPoE/PPPoA information provided to you by your ISP. Click NEXT to continue.
Username: Password:
VPI: 8 (0~255) VCI: 35 (1~65535)
Connection Type: PPPoE LLC
BACK NEXT EXIT
Figure 3-11

**Step 5:** Configure the rules for the WLAN, and click **NEXT**.

Quick Start - Wlan
You may enable/disable Wian,change the Wian SSID and Authentication type in this page.Click <b>Next</b> to continue.
Access Point : 💿 Activated 🔘 Deactivated
SSID: TP-LINK_012345
Broadcast SSID: 💿 Yes 🔘 No
Authentication Type : Disabled
BACK NEXT EXIT
Figure 3-12

### P Note:

If the Access Point is activated, the wireless function will be available even without the external antenna because of an additional printed antenna. To adopt the wireless security protection measures, please refer to section 4.3.3.

Step 6: Click NEXT to finish the Quick Start.

Quick Start Complete !!	
The Setup Wizard has completed. Click on <b>BACK</b> to modify ch to save the current settings.	anges or mistakes. Click <b>NEXT</b>
	BACK NEXT EXIT

Figure 3-13

# Chapter 4 Software Configuration

This User Guide recommends using the "Quick Installation Guide" for first-time installation. For advanced users, if you want to know more about this device and make use of its functions adequately, maybe you will get help from this chapter to configure the advanced settings through the Web-based Utility.

After your successful login, you can configure and manage the device. There are main menus on the top of the Web-based Utility; submenus will be available after you click one of the main menus. On the center of the Web-based Utility, there are the detailed configurations or status information. To apply any settings you have altered on the page, please click the **SAVE** button.

# 4.1 Status

Choose "**Status**", you can see the next submenus: **Device Info**, **System Log** and **Statistics**. Click any of them, and you will be able to configure the corresponding function.

Quick Start		face tup	Advance Setup	d Access Management	Maintenance	Status	Help
Device Info		Syste	em Log	Statistics			
Figure 4-1							

Click any of them, and you will be able to view the corresponding information.

# 4.1.1 Device Info

Choose "**Status** $\rightarrow$ **Device Info**" menu, and you will be able to view the device information, including LAN, WAN and ADSL. The information will vary depending on the settings of the Router configured on the Interface Setup screen.

Status Device Information	Devi			Setup	Manageme	nt Maintenanc	e Status	Help		
Device Information		ce Info	Syster	n Log	Statistics					
Device Information										
Device information										
	Firmware Version : 1.0.0 Build 100413 Rel.33291									
	MAC Address : 00:aa:bb:01:23:45									
LAN	LAN									
	IP Address : 192.168.1.1									
				sk : 255.255.25	5.0					
			DHCP Serv	er : Enabled						
WAN										
	PVC	VPIAVCI	IP Address	s Subn	et GateV	/ay DNS Server	Encapsulation	Status		
	PVC0	8/35	N/A	N/A	. N/A	. N/A	Bridge	Down		
	PVC1	0/33	N/A	N/A	. N/A	N/A	Bridge	Down		
	PVC2	0/35	N/A	N/A			Bridge	Down		
	PVC3	0/100	N/A	N/A			Bridge	Down		
	PVC4	1/32	N/A	N/A			Bridge	Down		
	PVC5	8/48	N/A	N/A			Bridge	Down		
	PVC6	0/38	N/A	N/A	. N/A	N/A	Bridge	Down		
ADSL ADSL Firmware Version : FwVer:3.11.2.175_TC3086 HwVer:T14.F7_6.0 Line State : Down Modulation : N/A Annex Mode : N/A										
	Downstream Upstream SNR Margin : N/A N/A db Line Attenuation : N/A N/A db Data Rate : N/A N/A kbps POWER : N/A N/A dbm CRC : N/A N/A									

Figure 4-2

# P Note:

Click the other submenus **System Log** or **Statistics** in Figure 4-2, and you will be able to view the system log and traffic statistics about the Router.

# 4.1.2 System Log

Choose "Status→System Log" menu, and you will be able to query the logs of the Router.

Status		erface Advan Setup Setu		Maintenance	Status	Help	
	Device Info	System Log	Statistics				
System Log							
	1/1/2000 0:	):2> main: inj	t completed.		~		
	1/1/2000 0:	):2> No DNS se	rver available				
	1/1/2000 0:	):2> Last erro	rlog repeat 10 Ti	imes			
	1/1/2000 0:	):2> adjTimeTa	sk fail: no serve	er available			
	1/1/2000 0:	):2> adjtime t	ask pause 60 seco	onds			
	1/1/2000 0:	:2> No DNS se	rver available				
	1/1/2000 0:	):2> Last erro	rlog repeat 10 Ti	imes			
	1/1/2000 0:	):2> adjTimeTa	sk fail: no serve	er available			
	1/1/2000 0:	/1/2000 0:0:2> adjtime task pause 60 seconds					
	1/1/2000 0:	):2> No DNS se	rver available				
	1/1/2000 0:	):2> Last erro	orlog repeat 10 Ti	imes			
	1/1/2000 0:	):2> adjTimeTa	ask fail: no serve	er available			
	1/1/2000 0:	):2> adjtime t	ask pause 1 day				
			rver available				
	1/1/2000 0:1:2> Last errorlog repeat 10 Times						
	1/1/2000 0:1:2> adjTimeTask fail: no server available						
		-	ask pause 60 secc	onds			
	1/1/2000 0:	l:2> No DNS se	rver available				
			orlog repeat 10 Ti				
		-	ask fail: no serve				
		-	ask pause 60 seco	onds			
			erver available				
			orlog repeat 10 Ti				
		-	ask fail: no serve	er available 💄	-		
	1/1/2000 0:	l:2> adjtime t	ask pause 1 day		*		
						_	
		CLE	AR LOG SAVE LOG				
		E:-	ure 4-3				

Figure 4-3

The Router can keep logs of all traffic. You can query the logs to find what happened to the Router.

Click the CLEAR LOG button to clear the logs.

Click the **SAVE LOG** button to save the logs.

### 4.1.3 Statistics

Choose "**Status** $\rightarrow$ **Statistics**" menu, and you will be able to view the network traffic over Ethernet, ADSL and WLAN.

Status	Quick Start	Interface Setup	Advanced Setup	Acce Manage		laintenance	Status	Help
	Device	Info Sys	tem Log 💦 🍾	Statistics				
Traffic Statistics								
		Interface	e : 💿 Ethernet (		LAN			
	Transmit Statistics		tistics		R	leceive Statistic	CS	
	Transmi	t Frames		156	Receive Fra	mes		348
	Transmi	t Multicast Frame	5	733	Receive Mul	ticast Frames		724
	Transmi	t total Bytes		891164	Receive tota	al Bytes		798447
	Transmi	t Collision		0	Receive CR	C Errors		0
	Transmi	t Error Frames		0	Receive Und	der-size Frames		0
			REFRESH	ļ				

Figure 4-4

- Interface: You can select Ethernet, ADSL and WLAN to view the corresponding network traffic over different ports.
- > Select **Ethernet**, and you will see the statistics table as below.

Interface : 💿 Ethernet 🔘 ADSL 🔵 WLAN

Transmit Statistics		Receive Statistics	
Transmit Frames	156	Receive Frames	348
Transmit Multicast Frames	733	Receive Multicast Frames	724
Transmit total Bytes	891164	Receive total Bytes	798447
Transmit Collision	0	Receive CRC Errors	0
Transmit Error Frames	0	Receive Under-size Frames	0

### **Statistics Table:**

	Transmit Frames	The frames transmitted over the Ethernet port.
	Transmit Multicast Frames	The multicast frames transmitted over the Ethernet port.
Transmit	Transmit total Bytes	The total bytes transmitted over the Ethernet port.
Statistics	Transmit Collision	The collision occurred over the Ethernet port when data is being transmitted.
	Transmit Error Frames	The error frames over the Ethernet port when data is being transmitted.
	Receive Frames	The frames received over the Ethernet port.
	Receive Multicast Frames	The multicast frames received over the Ethernet port.
Receive	Receive total Bytes	The total bytes received over the Ethernet port.
Statistics	Receive CRC Errors	The CRC errors occurred over the Ethernet port when data is being received.
	Receive Under-size Frames	The Under-size frames received over the Ethernet port.

> Select **ADSL**, and you will see the statistics table as below.

Interface : OEthernet 💿 ADSL OWLAN

Transmit Statistics		Receive Statistics	
Transmit total PDUs	0	Receive total PDUs	0
Transmit total Error Counts	0	Receive total Error Counts	0

### Statistics Table:

Transmit	Transmit total PDUs	The total PDUs transmitted over the ADSL port.
Statistics	Transmit total Error Counts	The total errors occurred over the ADSL port when data
Statistics		is being transmitted.
Receive	Receive total PDUs	The total PDUs transmitted over the ADSL port.
Statistics	Receive total Error Counts	The total errors occurred over the ADSL port when data
Statistics		is being received.

> Select **WLAN**, and you will see the statistics table as below.

Interface : 🔘 Ethernet 🔘 ADSL 💿 WLAN

Transmit Statistics		Receive Statistics	
Tx Frames Count	1227	Rx Frames Count	6060
Tx Errors Count	0	Rx Errors Count	590
Tx Drops Count	0	Rx Drops Count	0

### Statistics Table:

	Tx Frames Count	The frames transmitted over the WLAN when wireless data is
	TX Frames Count	being transmitted.
Transmit	Tx Errors Count	The errors occurred over the WLAN when wireless data is being
Statistics	TX EITOIS Count	transmitted.
	Tx Drops Count	The drops occurred over the WLAN when wireless data is being
	TX Drops Count	transmitted.
	Rx Frames Count	The frames received over the WLAN when wireless data is being
		transmitted.
Receive	Rx Errors Count	The terrors occurred over the WLAN when wireless data is being
Statistics		received.
	Px Drops Count	The drops occurred over the WLAN when wireless data is being
	Rx Drops Count	received.

Click the **Refresh** button to refresh immediately.

# 4.2 Quick Start

Please refer to "3.2: Login".

# 4.3 Interface Setup

Choose "Interface Setup", you can see the next submenus: Internet and LAN.

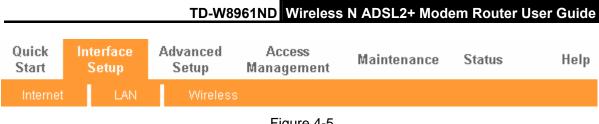


Figure 4-5

Click any of them, and you will be able to configure the corresponding function.

# 4.3.1 Internet

Choose "Interface Setup→Internet" menu, you can configure the parameters for WAN ports in the next screen (shown in Figure 4-6).

Interface	Quick Start	Interface Setup	Advanced Setup	Access Management	Maintenance	Status	Help
	Internet	LAN	Wireless				
ATM VC							
		Virtual Circuit		PVCs Summary			
			: 💿 Activated 🤇	· · · · · · · · · · · · · · · · · · ·			
		VPI		ge: 0~255)			
			· · ·	ge: 0~200) ge: 1~65535)			
QoS			(rang	JC. 1 00000)			
		ATM QoS	: UBR 💌				
		PCR	: 0 cells	/second			
		SCR	: 0 cells	/second			
		MBS	: 0 cells				
Encapsulation							
		ISP	: Opynamic IP /	Address			
			O Static IP Ade				
			💿 PPPoA/PPPo	E			
			🔘 Bridge Mode	•			
PPPoE/PPPoA							
		Servicename	:		]		
		Username	:				
		Password	:		Ī		
		Encapsulation	: PPPoE LLC	~	-		
	E	Bridge Interface	CActivated	Deactivated			
Connection Setting			-				
		Connection	: 💽 Always On				
			-	-Demand (Close if idle	for minutes	)	
	,	CD MSS Option	Connect Ma				
IP Address		ICP INISS OPLION	: TCP MSS(defau	t:1400) 1400 byte	8		
		Get IP Address	: 🔘 Static 💿 Dy	namic			
		tatic IP Address					
		IP Subnet Mask	: 0.0.0.0				
		Gateway	: 0.0.0.0				
		NAT	: Enable 🔽				
		Default Route	: 💽 Yes 🔘 No				
	1		TCP MTU(defaul		s		
		Dynamic Route		Direction : Both	*		
			: Disabled 💌				
		MAC Spoofing	Enabled O:00:00:00:00:00:00:00:00:00:00:00:00:00				
			00:00:00:00:00	00			
				_			
			SAVE DELE	TE			

Figure 4-6

- ATM VC: ATM settings are used to connect to your ISP. Your ISP provides VPI (Virtual Path Identifier), VCI (Virtual Channel Identifier) settings to you. In this Device, you can totally setup 8 VCs on different encapsulations, if you apply 8 different virtual circuits from your ISP. You need to activate the VC to take effect. For PVCs management, you can use ATM QoS to setup each PVC traffic line's priority.
  - Virtual Circuit: Select the VC number you want to setup, PVC0~PVC7.
  - Status: If you want to use a designed VC, you should activate it.
  - **VPI:** Identifies the virtual path between endpoints in an ATM network. The valid range is from 0 to 255. Please input the value provided by your ISP.
  - VCI: Identifies the virtual channel endpoints in an ATM network. The valid range is from 32 to 65535 (1 to 31 is reserved for well-known protocols). Please input the value provided by your ISP.
  - **PVCs Summary:** Click the button, and you can view the summary information about the PVCs.
  - QoS: Select the Quality of Service types for this Virtual Circuit, including CBR (Constant Bit Rate), UBR (Unspecified Bit Rate) and VBR (Variable Bit Rate). These QoS types are all controlled by the parameters specified below, including PCR (Peak Cell Rate), SCR (Sustained Cell Rate) and MBS (Maximum Burst Size), please configure them according to your needs.
- Encapsulation: There are four connection types: Dynamic IP Address, Static IP Address, PPPoA/PPPoE and Bridge Mode. Please choose the designed type that you want to use. After that, you should follow the configuration below to proceed.

### 1) Dynamic IP Address

Select this option if your ISP provides you an IP address automatically. This option is typically used for Cable services. Please enter the Dynamic IP information accordingly.

ISP :	<ul> <li>Dynamic IP Address</li> <li>Static IP Address</li> <li>PPPoA/PPPoE</li> <li>Bridge Mode</li> </ul>
Encapsulation :	1483 Bridged IP LLC
Bridge Interface :	Activated  Deactivated
NAT :	Enable 💙
Default Route :	⊙ Yes ◯ No
TCP MTU Option :	TCP MTU(default:1500) 1500 bytes
Dynamic Route :	RIP2-B 💙 Direction : Both 💌
Multicast :	Disabled 💌
MAC Spoofing :	C Enabled 💿 Disabled
	00:00:00:00:00:00

Figure 4-7

- Encapsulation: Select the encapsulation mode for the Dynamic IP Address, you can leave it default.
- NAT: Select this option to Enable/Disable the NAT (Network Address Translation) function for this VC. The NAT function can be activated or deactivated per PVC basis.
- Default Route: If enable this function, the current PVC will be considered as the default gateway to internet from this device.
- **TCP MTU Option:** Enter the TCP MTU as your desire.
- Dynamic Route: Select this option to specify the RIP (Routing Information protocol) version for WAN interface, including RIP1, RIP2-B and RIP2-M. RIP2-B and RIP2-M are both sent in RIP2 format, the difference is that RIP2-M using Multicast, while RIP2-B using Broadcast format.
  - Direction: Select this option to specify the RIP direction. None is for disabling the RIP function. Both means the ADSL Router will periodically send routing information and accept routing information, and then incorporate them into routing table. IN only means the ADLS router will only accept but will not send RIP packet. OUT only means the ADLS router will only send but will not accept RIP packet.
- Multicast: Select IGMP version, or disable the function. IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a multicast group. The ADSL ATU-R supports both IGMP version 1 (IGMP v1) and IGMP v2. Select "Disabled" to disable it.

### 2) Static IP Address

Select this option if your ISP provides static IP information to you. You should set static IP address, IP subnet mask, and gateway address in the screen below (shown in Figure 4-8).

ISP :	Opynamic IP Address				
	<ul> <li>Static IP Address</li> </ul>				
	O PPPoA/PPPoE				
	🔘 Bridge Mode				
Encapsulation :	1483 Bridged IP LLC				
Static IP Address :	0.0.0.0				
IP Subnet Mask :	0.0.0.0				
Gateway:	0.0.0.0				
Bridge Interface :	<ul> <li>Activated          <ul> <li>Deactivated</li> </ul> </li> </ul>				
NAT :	Enable 💌				
Default Route :	⊙ Yes ◯ No				
TCP MTU Option :	TCP MTU(default:1500) 1500 bytes				
Dynamic Route :	RIP2-B 💙 Direction : Both 💙				
Multicast :	Disabled 💌				
MAC Spoofing :	C Enabled 💿 Disabled				
	00:00:00:00:00:00				

Figure 4-8

### P Note:

Each IP address entered in the fields must be in the appropriate IP form, which is four IP octets separated by a dot (x.x.x.x), such as 192.168.1.100. The Router will not accept the IP address if it is not in this format.

### 3) PPPoA/PPPoE

Select this option if your ISP requires you to use a PPPoE connection. This option is typically used for DSL services. Select Dynamic PPPoE to obtain an IP address automatically for your PPPoE connection. Select Static PPPoE to use a static IP address for your PPPoE connection. Please enter the information accordingly.

ISP :	<ul> <li>Dynamic IP Address</li> <li>Static IP Address</li> <li>PPPoA/PPPoE</li> <li>Bridge Mode</li> </ul>
Servicename :	
Username :	
Password :	
Encapsulation :	PPPoE LLC
Bridge Interface :	O Activated 💿 Deactivated
Connection :	Always On (Recommended)     Connect On-Demand (Close if idle for
TCP MSS Option :	TCP MSS(default:1400) 1400 bytes
Get IP Address :	◯ Static ⊙ Dynamic
Static IP Address :	0.0.0.0
IP Subnet Mask :	0.0.0.0
Gateway :	0.0.0.0
NAT :	Enable 💙
Default Route :	⊙ Yes ◯ No
TCP MTU Option :	TCP MTU(default:1492) 1492 bytes
Dynamic Route :	RIP2-B V Direction : Both V
Multicast :	Disabled 💟
MAC Spoofing :	© Enabled

Figure 4-9

- Servicename: Enter a name to mark current connection, or you can leave it blank.
- **Username:** Enter your username for your PPPoE/PPPoA connection.
- **Password:** Enter your password for your PPPoE/PPPoA connection.
- Encapsulation: For both PPPoE/PPPoA connection, you need to specify the type of Multiplexing, either LLC or VC Mux.
- **Bridge Interface:** Activate the option, and the Router can also work in Bridge mode.
- Connection: For PPPoE/PPPoA connection, you can select Always on or Connect on-Demand or Connect Manually. Connect on demand is dependent on the traffic. If there is no traffic (or Idle) for a pre-specified period of time), the connection will tear down automatically. And once there is traffic send or receive, the connection will be automatically on.
- Static/Dynamic IP Address: For PPPoE/PPPoA connection, you need to specify the public IP address for this ADSL Router. The IP address can be either dynamically (via DHCP) or given IP address provided by your ISP. For Static IP, you need to specify the IP address, Subnet Mask and Gateway IP address.
- Default Route: You should select Yes to configure the PVC as the default gateway to internet from this device.

MAC Spoofing: Enable the MAC Spoofing, and enter a MAC address to configure the WAN port. It makes your inside network appear as a device with this MAC address to the outside world.

### 4) Bridge Mode

If you select this type of connection, the modem can be configured to act as a bridging device between your LAN and your ISP. Bridges are devices that enable two or more networks to communicate as if they are two segments of the same physical LAN.

ISP :	<ul> <li>Dynamic IP Address</li> <li>Static IP Address</li> <li>PPPoA/PPPoE</li> <li>Bridge Mode</li> </ul>
Encapsulation :	1483 Bridged IP LLC 🛛 🔽
	Figuro 4.10

Figure 4-10

# P Note:

After you finish the Internet configuration, please click SAVE to make the settings take effect.

# 4.3.2 LAN

Choose "Interface Setup $\rightarrow$ LAN" menu, and you will see the LAN screen (shown in Figure 4-11). Please configure the parameters for LAN ports according to the descriptions below.

Interface	Quick Start	Interface Setup	Advanced Setup	Access Management	Maintenance	Status	Help
	Internet	LAN	) Wireless	3			
Router Local IP							
		IP Address	: 192.168.1.1				
		IP Subnet Mask	: 255.255.255.0				
		Dynamic Route	: RIP2-8 💌	Direction : None	~		
			: Disabled 🔽				
		IGMP Snoop	: 💿 Disabled 🔘	Enabled			
DHCP							
		DHCP	: 🔘 Disabled 📀	Enabled 🔘 Relay			
DHCP Server							
	St	arting IP Address		Current Po	ool Summary		
		IP Pool Count					
		Lease Time		onds (0 sets to defai	ult value of 259200)		
		Physical Ports					
DNS			1 2 3 4	4			
DH3		DNS Relay	: Use Auto Disco	overed DNS Server On			
	Pri	mary DNS Server			.,		
		dary DNS Server					
			SAVE CAN	CEL			
			UANT CAN				



- Router Local IP: These are the IP settings of the LAN interface for the device. These settings may be referred to as Private settings. You may change the LAN IP address if needed. The LAN IP address is private to your internal network and cannot be seen on the Internet.
  - **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.
  - **IP Subnet Mask:** Enter the Router's Subnet Mask, the default value is 255.255.255.0.
  - **Dynamic Route:** Select this option to specify the RIP (Routing Information protocol) version for LAN interface, including **RIP1**, **RIP2-B** and **RIP2-M**. RIP2-B and RIP2-M are both sent in RIP2 format, the difference is that RIP2-M using Multicast, while RIP2-B using Broadcast format.
  - Direction: Select this option to specify the RIP direction. None is for disabling the RIP function. Both means the ADSL Router will periodically send routing information and accept routing information, and then incorporate them into routing table. IN only means the ADLS router will only accept but will not send RIP packet. OUT only means the ADLS router will only send but will not accept RIP packet.
  - Multicast: Select IGMP version, or disable the function. IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a multicast group. The ADSL ATU-R supports both IGMP version 1 (IGMP v1) and IGMP v2. Select "Disabled" to disable it.
  - **IGMP Snoop:** Enable the IGMP Snoop function if you need.
- DHCP Server: Select Enabled, then you will see the screen below (shown in Figure 4-12). The Router will work as a DHCP Server; it becomes the default gateway for DHCP client

connected to it. DHCP stands for Dynamic Host Control Protocol. The DHCP Server gives out IP addresses when a device is booting up and request an IP address to be logged on to the network. That device must be set as a DHCP client to obtain the IP address automatically. By default, the DHCP Server is enabled. The DHCP address pool contains the range of the IP address that will automatically be assigned to the clients on the network.

DHCP :	O Disabled 💿 Enabl	ed 🔘 Relay
Starting IP Address :	192.168.1.2	Current Pool Summary
IP Pool Count :	100	
Lease Time :	259200 seconds	(0 sets to default value of 259200)
Physical Ports :	Image: Weight of the second	
DNS Relay :	Use Auto Discovered	DNS Server Only 🔽
Primary DNS Server :	N/A	
Secondary DNS Server :	N/A	



- Starting IP Address: Enter the starting IP address for the DHCP server's IP assignment. 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 192.168.1.2or greater, but smaller than 192.168.1.254.
- **IP Pool Count:** The max user pool size.
- Lease Time: The length of time for the IP lease. After the dynamic IP address has expired, the user will be automatically assigned a new dynamic IP address. The default is **259200** seconds.
- Physical Ports: Specify the Physical Ports of the DHCP client.
- **DNS Relay:** If you want to disable this feature, you just need to set both Primary and secondary DNS IP to 0.0.0.0. If you want to use DNS relay, you can setup DNS server IP to 192.168.1.1 on their Computer. If not, the device will perform as no DNS relay.
- Primary DNS Server: Type in your preferred DNS server.
- Secondary DNS Server: Type in your preferred DNS server.
- **Current Pool Summary:** Click the button, then you can view the IP addresses that the DHCP Server gives out.

### P Note:

If **Use Auto Discovered DNS Server Only** is selected in DNS Relay, this router will accept the first received DNS assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s) during the connection establishment. If **Use User Discovered DNS Server Only** is selected in DNS Relay, it is necessary for you to enter the primary and optional secondary DNS server IP addresses. After type in the address, click SAVE button to save it and invoke it.

> DHCP Relay: Select Relay, then you will see the next screen (shown in Figure 4-13), and the

Router will work as a DHCP Relay. A DHCP relay is a computer that forwards DHCP data between computers that request IP addresses and the DHCP server that assigns the addresses. Each of the device's interfaces can be configured as a DHCP relay. If it is enabled, the DHCP requests from local PCs will forward to the DHCP server runs on WAN side. To have this function working properly, please run on router mode only, disable the DHCP server on the LAN port, and make sure the routing table has the correct routing entry.

DHCP :	🔘 Disabled 🔘 Enabled 💿 Relay
DHCP Server IP for Relay Agent	0.0.0.0



DHCP Server IP for Relay Agent: Enter the DHCP server IP Address runs on WAN side.

### P Note:

If you select **Disabled**, the DHCP function will not take effect.

### 4.3.3 Wireless

Choose "Interface Setup→Wireless" menu, and you will see the Wireless screen (shown in Figure 4-14). Please configure the parameters for wireless according to the descriptions below.

Interface		iterface Setup	Advanced Setup	Access Management	Maintenance	Status	Help
		LAN	Wireles	$\mathbf{b}$			
Access Point Settings							
	,	Access Point -	Activated (	Departmentand			
	·		UNITED STATE		Current Channel:		
	Beacon	Interval(ms):		ange: 20~1000)			
		S Threshold :					
		on Threshold .	2346 (range: 256~2346, even numbers only)				
		(bytes) DTIM(ms) :		ange: 1~255)	namboro onny)		
	W		802.11b+g+n				
11n Settings							
inistangs	Choros	el Bandwidth :	20/40 MHz 🗸	]			
			above the cont	rol channel			
		uard Interval :					
		MCS :	AUTO 🔽				
		VVMM :	• Enable O	Disable			
Multiple SSIDs Settings							
		SSID Index :	1 💙				
	Bro		💽 Yes 🔘 No				
		Use QSS :	💿 Yes 🔘 No				
QSS Settings							
			Unconfigured				
		QSS mode :	O PIN code	PBC			
	0	SS progress :	Start QSS				
			TP-LINK_01234	5	7		
	Authen	tication Type :		~			
WDS Settings							
		WDS Mode :	🔘 On 💿 Off				
	Мас		00:00:00:00:00	:00			
	Мас	Address #2 :	00:00:00:00:00	:00			
	Мас	Address #3 :	00:00:00:00:00	:00			
	Мас	Address #4 :	00:00:00:00:00	:00			
Wireless MAC Address Filter							
		Active :	O Activated	Deactivated			
				ion 🕙 the follow Wire	eless LAN station(s) as	sociation.	
	Мас	Address #1 :	00:00:00:00:00	00			
	Мас	Address #2 :	00:00:00:00:00	00			
	Mac	Address #3 :	00:00:00:00:00	00			
			00:00:00:00:00				
			00:00:00:00:00				
			00:00:00:00:00				
			00:00:00:00:00				
	Mac	: Address #8 :	00:00:00:00:00	00			
			SAVE CAN	CEL			
			Figure				

Figure 4-14

- Access point Settings: These are the settings of the access point. You can configure the rules to allow wireless-equipped computers and other devices to communicate with a wireless network.
  - Access point: Select Activated to allow wireless station to associate with the access point.
  - Channel: Select the channel you want to use from the drop-down List of Channel. 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.

- **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.
- RTS/CTS 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.
- **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.
- **DTIM:** 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.
- Wireless Mode: In the drop-down list you can select "802.11b", "802.11g", "802.11n", "802.11b+g", "802.11g+n" and "802.11b+g+n". "802.11b+g+n" allows both 802.11b, 802.11g and 802.11n wireless stations to connect to the Router.
- 11n Settings: These are the settings of the 11n parameters. If "802.11n", "802.11g+n" or "802.11b+g+n" is selected for Wireless mode, these settings will be displayed.
  - **Channel Bandwidth:** Select the Bandwidth you want to use from the drop-down List. There are two options, "20 MHz" and "20/40 MHz". If bigger bandwidth is selected, device could transmit and receive data with higher speed.
  - Extension Channel: If "20/40 MHz" is selected, this option will be displayed.
  - Guard Interval: Select the guard interval you want from the drop-down list.
  - MCS: Select the wireless transmission rate from the drop-down list. By default, the option is AUTO.
- > Multiple SSIDs Settings: These are the settings of the SSID.
  - **SSID Index:** The index of the SSID, and in this model, you can only leave it as a default value of 1.
  - **Broadcast SSID:** When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the Router. To broadcast the

Router's SSID, keep the default setting. If you don't want to broadcast the Router's SSID, select "No".

 Use QSS: Use QSS (Wi-Fi Protected Setup) function, you can add a new wireless device to an existing network quickly. To Use QSS, keep the default setting, and configure the parameters in QSS Settings. If you don't want to Use QSS, select "No", then you will see the screen as shown below.

Multiple SSIDs Settings				
	SSID Index :	1 🕶		
	Broadcast SSID :	💿 Yes 🔘 No		
	Use QSS :	🔘 Yes 💿 No		
	SSID :	TP-LINK_012345		
	Authentication Type :	Disabled	*	
WDS Settings				

Figure 4-15

- 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.
- Authentication Type: Select an authentication type from the drop-down list, which allows you to configure security features of the wireless LAN interface. Options available are: Disabled, WEP-64Bits, WEP-128Bits, WPA-PSK, WPA2-PSK, and WPA-PSK/ WPA2-PSK.

# 1) WEP-64Bits

To configure WPA-64Bits settings, select the WPA-64Bits option from the drop-down list. The menu will change to offer the appropriate settings. WPA-64Bits is a data privacy mechanism based on a 64-bit shared key algorithm, as described in the IEEE 802.11g standard.

Multiple SSIDs Settings		
	SSID Index :	1 💌
	Broadcast SSID :	● Yes ● No
	Use QSS :	🔿 Yes 💿 No
	SSID :	TP-LINK_012345
	Authentication Type :	WEP-64Bits
WEP		
		For each key, please enter either (1) 5 characters excluding symbols, or (2) 10 characters ranging from 0~9, a, b, c, d, e, f.
		For each key, please enter either (1) 13 characters excluding symbols, or (2) 26 characters ranging from 0~9, a, b, c, d, e, f.
	💽 Key#1 :	0x000000000
	◯ Key#2 :	0×000000000
	◯ Key#3 :	0×000000000
	🔘 Key#4 :	0x000000000
WDS Settings		

Figure 4-16

2) WEP-128Bits

To configure WPA-64Bits settings, select the WPA-64Bits option from the drop-down list. The menu will change to offer the appropriate settings. 128-bit is stronger than 64-bit.

Multiple SSIDs Settings		
	SSID Index :	1 💌
	Broadcast SSID :	● Yes ● No
	Use QSS :	🔿 Yes 💿 No
	SSID :	TP-LINK_012345
	Authentication Type :	WEP-128Bits
WEP		
		For each key, please enter either (1) 5 characters excluding symbols, or (2) 10 characters ranging from 0~9, a, b, c, d, e, f.
		For each key, please enter either (1) 13 characters excluding symbols, or (2) 26 characters ranging from 0~9, a, b, c, d, e, f.
	🧿 Key#1 ∶	0×000000000000000000000000000000000000
	◯ Key#2∶	0×000000000000000000000000000000000000
	◯ Key#3 :	0x000000000000000000000000000000000000
	○ Key#4 :	0×000000000000000000000000000000000000
WDS Settings		

Figure 4-17

### 3) WPA-PSK

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

Multiple SSIDs Settings			
	SSID Index :	1 💌	
	Broadcast SSID :	⊙ Yes ◯ No	
	Use QSS :	🔿 Yes 💿 No	
	SSID :	TP-LINK_012345	
	Authentication Type :	WPA-PSK	
WPA-PSK			
	Encryption :	TKIP/AES 🔽	
	Pre-Shared Key :	hexadecimal characters)	(8~63 ASCII characters or 64
WDS Settings			



- Encryption: Select the encryption you want to use: TKIP/AES, TKIP or AES (AES is an encryption method stronger than TKIP).
  - **TKIP** (Temporal Key Integrity Protocol) a wireless encryption protocol that provides dynamic encryption keys for each packet transmitted.
  - **AES** (Advanced Encryption Standard) A security method that uses symmetric 128-bit block data encryption.
- 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.

### 4) 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.

Multiple SSIDs Settings			
	SSID Index :	1 💙	
	Broadcast SSID :	⊙ Yes ◯ No	
	Use QSS :	🔿 Yes 💿 No	
	SSID :	TP-LINK_012345	
	Authentication Type :	WPA2-PSK	_
WPA2-PSK			
	Encryption :	TKIP/AES 💌	
	Pre-Shared Key :	hexadecimal characters)	(8~63 ASCII characters or 64
WDS Settings			

Figure 4-19

### 5) WPA-PSK/WPA2-PSK

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

Multiple SSIDs Settings			 
	SSID Index :	1 💌	
	Broadcast SSID :	Yes ○No     No	
	Use QSS :	🔿 Yes 💿 No	
	SSID :	TP-LINK_012345	
	Authentication Type :	WPA-PSK/WPA2-PSK 🔽	
WPA-PSK/WPA2-PSK Mixed			
Mode	Encryption :	TKIP/AES 💌	
	Pre-Shared Key :	hexadecimal characters)	(8~63 ASCII characters or 64
WDS Settings			 



- QSS Settings: QSS can help you to add a new wireless device to an existing network quickly. This section will guide you how to use QSS function.
  - **QSS state:** Display the current QSS state.
  - **QSS mode:** If the wireless adapter supports Wi-Fi Protected Setup (QSS), you can establish a wireless connection between wireless adapter and Router using either Push Button Configuration (PBC) method or PIN method, please select the one you want.

### 1) PBC

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

QSS Settings	
	QSS state : Unconfigured
	QSS mode : 🔘 PIN code 💿 PBC
	Start QSS
	QSS progress : Idle
	SSID: TP-LINK_012345
	Authentication Type : WPA-PSK/WPA2-PSK 💌
WPA-PSK/WPA2-PSK Mixed	
Mode	

Figure 4-21

### Method One:

Step 1: Press the QSS button on the front panel of the Router or click **Start QSS** button in Figure 4-21.

TP-LINK <sup>®</sup> TD-W8961ND	Power	ADSL	nternet	WLAN	1	2	3	4	ass QSS
Wireless N ADSL2+ Modern Router	¢	φ	Ø	8	. 🖸	Ø	Q		

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

(055)	

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

🧧 QSS for Wireless	X
(((QSS))) <sub>&gt;&gt;&gt;</sub>	
Wireless Configuration Completed	
Your computer has successfully joined the <b>TP-LINK</b> network.	
Karak Finish Ca	ancel

The QSS Configuration Screen of Wireless Adapter

### Method Two:

Step 1: Press the QSS button on the front panel of the Router or click **Start QSS** button in Figure 4-21.



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**.

🥶 QSS for Wireless		×
Join a Wireless N	etwork	
QSS is preparing to join y	our computer to a wireless network.	
(((QSS))) Quick secure setup	<ul> <li>Which setup method do you want to use?</li> <li>Push the button on my access point</li> <li>Enter a PIN into my access point or a registrar</li> <li>Enter the PIN from my access point</li> </ul> Push the button on your access point and click Next to continue.	
	Automatically select the network	

The QSS Configuration Screen of Wireless Adapter

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



The QSS Configuration Screen of Wireless Adapter

### 2) PIN code

If the wireless adapter supports Wi-Fi Protected Setup and the PIN method, you can add it to the network by PIN with the following two methods. Click **PIN code**, you will see the screen as shown below.

QSS Settings		
	QSS state :	Unconfigured
	QSS mode :	● PIN code ● PBC
	AP self PIN code :	00745659
	enrollee PIN code :	
		Start QSS
	QSS progress :	Idle
	SSID :	TP-LINK_012345
	Authentication Type :	WPA-PSK/WPA2-PSK 💙
WPA-PSK/WPA2-PSK Mixed		
Mode		

Figure 4-22

Method One: Enter the PIN into my Router

Step 1: 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, and get the PIN code on the screen as below, then click Next.

🧧 QSS for Wireless		×
Join a Wireless N	letwork	
QSS is preparing to join y	our computer to a wireless network.	
	Which setup method do you want to use?	_
	Enter a PIN into my access point or a registrar	
Quick secure setup	○ Enter the PIN from my access point	
	Enter the PIN <b>6952898</b> Into your access point or external registrar and click Next to continue.	
	Automatically select the network 🗹	
	< Back Next > Cancel	

The QSS Configuration Screen of Wireless Adapter

Step 2: For the Router, keep **PIN code** selected and enter the PIN code of the wireless adapter in the field after **enrollee PIN code** as shown below. Then click **Start QSS**.

QSS Settings	
	QSS state : Unconfigured
	QSS mode : 💿 PIN code 🔘 PBC
	AP self PIN code : 00745659
	enrollee PIN code 16952898
	Start QSS
	QSS progress : Idle
	SSID: TP-LINK_012345
	Authentication Type : WPA-PSK/WPA2-PSK 🔽
PA-PSK/WPA2-PSK Mixed	
Mode	

Figure 4-23

Method Two: Enter the PIN from my Router

- Step 1: Get the Current PIN code of the Router from AP self PIN code in Figure 4-23 (each Router has its unique PIN code. Here takes the PIN code 55924054 of this Router for example).
- 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 Network								
QSS is preparing to join y	our computer to a wireless network.							
(((QSS))) Quick secure setup	<ul> <li>Which setup method do you want to use?</li> <li>Push the button on my access point</li> <li>Enter a PIN into my access point or a registrar</li> <li>Enter the PIN from my access point</li> </ul>							
	Access Point PIN: 00745659							
	Automatically select the network 🗹							
	<pre></pre>							

The QSS Configuration Screen of Wireless Adapter

### P Note:

The default PIN code of the Router can be found in its label or the QSS configuration screen as Figure 4-23.

- **QSS progress:** Show the current QSS progress.
- **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.

- Authentication Type: Select an authentication type from the drop-down list, which allows you to configure security features of the wireless LAN interface. Options available are: Disabled, WEP-64Bits, WEP-128Bits, WPA-PSK, WPA2-PSK, and WPA-PSK/ WPA2-PSK.
- WDS Settings: Select On/Off to enable/disable WDS. With this function enabled, the Router can bridge two or more WLANs.
  - MAC Address: Enter the MAC Address you wish to bridge in the field.
- Wireless MAC Address Filter: Wireless access can be filtered by using the MAC addresses of the wireless devices transmitting within your network's RADIUS.
  - Active: If you wish to filter users by MAC Address, select "Activated", and "Deactived" for don't.
  - Action: To filter wireless users by MAC Address, select "Allow Association" or "Deny Association" the follow Wireless LAN station(s) association.
  - **MAC Address:** Enter the MAC Address you wish to filter in the field.

### 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.

## 4.4 Advanced Setup

Choose "Advanced Setup", you can see the next submenus:





Click any of them, and you will be able to configure the corresponding function.

## 4.4.1 Firewall

Choose "**Advanced Setup**→**Firewall**" menu, and you will see the next screen (shown in Figure 4-25).

Advanced	Quick Start	Interface Setup	Advanced Setup	Access Managemen	nt Main	tenance	Status	Help		
	Firewall	Routing	NAT	QoS	VLAN	ADSL				
Firewall			-	_						
	Firewall : ③ Enabled 〇 Disabled SPI : 〇 Enabled ④ Disabled									
		WARNING: If You enabled SPI, all traffics initiated from WAN would be blocked, including DMZ, Virtual Server, and ACL WAN side.)								
			Diviz, virtual Si	si ver, and ACE WA	N SIUC.)					
			SAVE CA	NCEL						

Figure 4-25

- Firewall: Select this option can automatically detect and block Denial of Service (DoS) attacks, such as Ping of Death, SYN Flood, Port Scan and Land Attack.
- SPI: If you enable SPI, all traffics initiated from WAN would be blocked, including DMZ, Virtual Server, and ACL WAN side.

## 4.4.2 Routing

Choose "Advanced Setup $\rightarrow$ Routing" menu, and you will see the routing information in the next screen (shown in Figure 4-26).

Advanced	Quick Start	Interface Setup	Advanced Setup	Access Manageme	nt Mai	ntenance	Status	\$	Help
	Firewall	Routing	NAT	QoS	VLAN	ADSL			
Routing Table List									
	#	Dest IP	Mask	Gateway IP	Metric	Device	Use	Edit	Drop
	1	192.168.1.0	24	192.168.1.1	1	enet0	937		
			ADD ROUT	E					

Figure 4-26

Click ADD ROUTE button to add a new route in the next screen (shown in Figure 4-27).

Static Route	1
	Destination IP Address : 0.0.0.0
	IP Subnet Mask : 0.0.0.0
	Gateway IP Address : 💿 0.0.0.0 🔿 PVC0 💌
	Metric : 0
	Announced in RIP : Yes 💌
	SAVE DELETE BACK CANCEL

Figure 4-27

- Destination IP Address: This parameter specifies the IP network address of the final destination.
- > **IP Subnet Mask:** Enter the subnet mask for this destination.
- Gateway IP Address: Enter the IP address of the gateway. The gateway is an immediate neighbor of your ADSL Router that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your Router; over Internet (WAN), the

gateway must be the IP address of one of the remote nodes.

- Metric: Metric represents the "cost" of transmission for routing purposes. IP Routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not to be precise, but it must between 1 and 15. In practice, 2 or 3 is usually a good number.
- Announced in RIP: This parameter determines if the ADSL router will include the route to this remote node in its RIP broadcasts. If set to Yes, the route to this remote node will be propagated to other hosts through RIP broadcasts. If No, this route is kept private and is not included in RIP broadcasts.

## 4.4.3 NAT

Choose "Advanced Setup $\rightarrow$ NAT" menu, you can setup the NAT (Network Address Translation) function for the Router (shown in Figure 4-28).

Advanced	Quick Start	Interface Setup	Advanced Setup	Access Managemen	nt Main	tenance	Status	Help	
	Firewall	Routing	NAT	QoS	VLAN	ADSL			
NAT									
		Virtual Circuit : PVC0 💌							
		NAT Status							
		Number of IPs	: 💿 Single 🔘	Multiple					
		0	DMZ						
		0	Virtual Serve	ſ					

Figure 4-28

- > Virtual Circuit: Enter Virtual Circuit Index that you plan to setup for the NAT function.
- NAT Status: This field shows the current status of the NAT function for the current VC. You can go to the previous screen (shown in Figure 4-6) to activate the function.
- Number of IPs; This field is to specify how many IPs are provided by your ISP for current VC. It can be single IP or multiple IPs. We select Multiple to explain.

## P Note:

For VCs with single IP, they share the same DMZ and Virtual servers; for VCs with multiple IPs, each VC can set DMZ and Virtual servers. Furthermore, for VCs with multiple IPs, they can define the Address Mapping rules; for VCs with single IP, since they have only one IP, there is no need to individually define the Address Mapping rule.

### 4.4.3.1 DMZ

Choose "Advanced Setup $\rightarrow$ NAT $\rightarrow$ DMZ" in Figure 4-28, you can configure the DMZ host in the next screen. A DMZ (demilitarized zone) is a host between a private local network and the outside public network. It prevents outside users from getting direct access to a server that has company data. Users of the public network outside the company can access to the DMZ host.

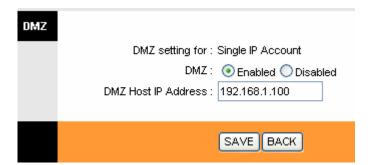


Figure 4-29

> DMZ Host IP Address: Enter the specified IP Address for DMZ host on the LAN side.

### 4.4.3.2 Virtual Server

Choose "Advanced Setup $\rightarrow$ NAT $\rightarrow$ Virtual Server" in Figure 4-28, you can configure the Virtual Server in the next screen.

The Virtual Server is the server or server(s) behind NAT (on the LAN), for example, Web server or FTP server, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single machine to the outside world.

Virtual Server											
	Virtua	I Server for :	Single IP Accou	Single IP Account							
		Rule Index :	3 💌								
		Application :	FTP		FTP	~					
		Protocol :	ALL 🔽								
	Start F	ort Number :	21								
	End F	ort Number :	21								
	Local	IP Address :	192.168.1.102								
Virtual Server Listing											
	Rule	Applie	cation	Protocol	Start Port	End Port	Local IP Address				
	1	F	TP	ALL	21	21	192.168.1.100				
	2	HTTP_	Server	ALL	80	80	192.168.1.101				



- Rule Index: The Virtual server rule index for this VC. You can specify 10 rules in maximum. All the VCs with single IP will use the same Virtual Server rules.
- > Application: The Virtual servers can be used for setting up public services on your LAN.
- > **Protocol:** The protocol used for this application.
- Start & End port number: Enter the specific Start and End Port number you want to forward. If it is one port only, you can enter the End port number the same as Start port number. For example, if you want to set the FTP Virtual server, you can set the start and end port number to 21.
- **Local IP Address:** Enter the IP Address for the Virtual Server in LAN side.
- > Virtual Server Listing: This displays the information about the Virtual Servers you establish.

### To add a virtual server entry:

Step 1: Select the "Virtual Circuit" and select "Virtual Server".

### P Note:

For VCs with single IP, select Single; For VCs with multiple IPs, select Multiple for the option.

- **Step 2:** Select the Rule index for the rule as shown in Figure 4-30.
- Step 3: Select the application you want from drop-down list, then the protocol and port number will be added to the corresponding field automatically, you only need to configure the IP address for the virtual server; If the application list does not contain the service that you want, please configure the Port number, IP Address and Protocol manually.
- Step 4: After that, click SAVE to make the entry take effect.

### Other operations for the entries as shown in Figure 4-30:

Enter the index of assigned entry, and click the **DELETE** button to delete the entry.

Click the **BACK** button to return to the previous screen.

Click the **CANCEL** button to cancel the configuration which is made just now.

### 4.4.3.3 IP Address Mapping

Select Multiple for numbers of IPs in Figure 4-28, and choose "Advanced Setup $\rightarrow$ NAT $\rightarrow$ IP Address Mapping(for Multiple IP Service)". You can configure the Address Mapping Rule in the next screen. The IP Address Mapping is for those VCs that configured with multiple IPs. The IP Address Mapping rule is per-VC based (only for Multiple IPs' VCs).

IP Address Mapping							
	Address N	1apping R	ule : PVC0				
		Rule Ind	lex:1 🔽				
		Rule Ty	/pe : Many-to-Man	y Overlo	ad 🔽		
	L	.ocal Star	t IP : 0.0.0.0		(for all local l	IPs, enter 0.0.0.0 for S	tart IP)
		Local End	d IP : 255.255.255.2	255	(for all local IPs, enter 255.255.255.255 for End IP)		
	Р	ublic Star	t IP : 61.141.228.32	2			
	I	Public End	d IP : 61.141.228.25	54			
Address Mapping List							
	Rule	Туре	Local Start IP	Loc	al End IP	Public Start IP	Public End IP
	1	M-M Ov	0.0.0.0	255.2	55.255.255	61.141.228.32	61.141.228.254
			<b>—</b> :	~ 1			



- Rule Index: Select the Virtual server rule index for this VC. You can specify 8 rules in maximum.
- Rule Typ: There are four types: one-to-one, Many-to-One, Many-to-Many Overload and Many-to-Many No-overload.
- Local Start & End IP: Enter the local IP Address you plan to map to. Local Start IP is the starting local IP address and Local End IP is the ending local IP address. If the rule is for all local IPs, then the Start IP is 0.0.0.0 and the End IP is 255.255.255.255.
- Public Start & End IP: Enter the public IP Address you want to do NAT. Public Start IP is the starting public IP address and Public End IP is the ending public IP address. If you have a dynamic IP, enter 0.0.0.0 as the Public Start IP.
- > Address Mapping List: This displays the information about the Mapping addresses.

To add a mapping rule:

Step 1: Select the "Virtual Circuit" and Multiple for the "Number of IPs". Then select the tab IP Address Mapping (shown in Figure 4-28).

### P Note:

### **IP Address Mapping** is only available for VCs with Multiple IPs.

- Step 2: Select the Rule index for the rule as shown in Figure 4-31.
- Step 3: Select the rule type you want from the drop-down list.
- **Step 4:** Enter the local and public IP addresses in the corresponding fields.
- Step 5: After that, click SAVE to make the entry take effect.

### Other operations for the entries as shown in Figure 4-31:

Select the index of assigned entry, and click the **DELETE** button to delete the entry.

Click the **BACK** button to return to the previous screen.

Click the **CANCEL** button to cancel the configuration which is made just now.

## 4.4.4 QoS

Choose "Advanced Setup  $\rightarrow$  QoS", you can configure the QoS in the next screen. 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.

Advanced	Quick Interface Start Setup	Advanced Setup	Access Management	Maintenance	Status	Help
	Firewall Routing	NAT	(Q05) V	LAN ADSL		
Quality of Service						
	Qos	S: 💿 Activated (				
	Summar		ngs Summary			
Rule						
	Rule Inde:	<: 1 💌				
	Activ		<ol> <li>Deactivated</li> </ol>			
	Application	ו: 💌				
	Physical Port:	s: WLAN Enet		net4		
	Destination MA	::				
	I	P:				
	Mas	k:				
	Port Range	e:~				
	Source MAG	:				
	I	P:				
	Mas	k:				
	Port Range	e:~				
	Protocol II	): 🛛 👻				
	Vlan ID Rang	ə: ~				
	IPP/DS Field		DSCP			
	IP Precedence Range					
	Type of Service		~			
	DSCP Range		(Value Range: 0	~ 63)		
Action	802.1	0:				
Holdin	IPP/DS Fiel	a: O ipp/tos (	DSCP			
	IP Precedence Remarking					
	Type of Service Remarking	g :	~			
	DSCP Remarking	a: (Value	e Range: 0 ~ 63)			
	802.1p Remarking	a: 🔽	~			
	Queue ;	<b>#</b> : •				
		ADD DELET	ECANCEL			

Figure 4-32

- QoS: Select this option to Activate/Deactivate the IP QoS on different types (IP ToS and DiffServ).
- Summary: Click the button to view the configurations of QoS.
- Rule: Configure the rules for QoS. If the traffic complies with the rule, then the Router will take the corresponding action to deal with it.
  - **Rule Index:** Select the index for the rule you want to configure.
  - Active: Activate the rule. The rule can take effect only when it is activated.
  - **Application:** Select the application that the rule aimed at.
  - **Physical Ports:** Select the port whose traffic flow are controlled by the rule.
  - **Destination MAC & IP & Mask & Port Range:** Enter the IP information about the Destination host for the rule.
  - Source MAC & IP & Mask & Port Range: Enter the IP information about the Source host for the rule.
  - **Protocol ID:** Select one among TCP/UDP, TCP, UDP or ICMP protocols for the application.
  - Vian ID Range: Enter the Vian range, and the rule will be effective to the selected Vians.

• **IPP/DS Field:** Select the type of the action to assign the priority.

When you select IPP/TOS, you can assign the priority via IP information. IP QoS function is intended to deliver guaranteed as well as differentiated Internet services by giving network resource and usage control to the Network operator.

- **IP Precedence Range:** Enter the IP precedence range that the Router takes to differentiate the traffic.
- **Type of Service:** Select the type of service that the Router takes to deal with the traffic.
- **802.1p:** Select the priority range for the rule.

When you select DSCP, you can assign the priority via DHCP (the header of IP group). It maps the IP group into corresponding service class.

- **DSCP Range:** Enter the DSCP range to differentiate the traffic.
- **802.1p:** Select the priority range for the rule.
- Action: Configure the action that the Router takes to deal with the traffic which accord with the rule.
  - IPP/DS Field: Select the type for the action.
  - IP Precedence Remarking: Select the number to remark the priority for IP precedence.
  - **Type of Service Remarking:** Select the type to remark the service.
  - **DSCP Remarking:** Enter the number to remark the DSCP priority.
  - **802.1p Remarking:** Select the type to remark the 802.1p priority.
  - **Queue:** Select the priority type for the action.

## 4.4.5 VLAN

Choose "Advanced Setup→VLAN", you can activate the VLAN function in the next screen.

Virtual LAN (VLAN) is a group of devices on one or more LANs that are configured so that they can communicate as if they were attached to the same LAN, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, it is very flexible for user/host management, bandwidth allocation and resource optimization. There are two types of VLAN as follows:

Port-Based VLAN: Each physical switch port is configured with an access list specifying membership in a set of VLANs.

ATM VLAN: Using LAN Emulation (LANE) protocol to map Ethernet packets into ATM cells and deliver them to their destination by converting an Ethernet MAC address into an ATM address.

TD-W8961ND Wireless N ADSL2+ Modem Router User Guide

Advanced	Quick Start	Interface Setup	Advanced Setup	Access Management	Maintenance	Status	Help			
	Firewall	Routing	NAT	Q05 🤇	ADSL					
	1									
VLAN										
	VLAN Function : 💿 Activated 🔘 Deactivated									
		0	Assign VLAN	PVID for each Inter	face					
		0	Define VLAN	Group						

Figure 4-33

## 1) Assign VLAN PVID for each Interface

Click **Assign VLAN PVID for each Interface** in Figure 4-33, you can assign the PVID for each interface in the next screen (shown in Figure 4-34).

PVID Assign	
	ATM VC #0 : PVID 1
	VC #1 : PVID 1
	VC #2: PVID 1
	VC #3∶ p∨lD 1
	VC #4 : p∨iD 1
	VC #5∶ p∨ID 1
	VC #6 : p∨lD 1
	VC #7 : pviD 1
	Ethernet Port #1 : PVID 1
	Port #2 : pvip 1
	Port #3∶ p∨jp 1
	Port #4 : PVID 1
	Wireless LAN : PVID 1
	SAVE CANCEL NEXT

Figure 4-34

PVID: Each physical port has a default VID called PVID (Port VID). PVID is assigned to untagged frames or priority tagged frames (frames with null (0) VID) received on this port.

## 2) Define VLAN Group

Click **Define VLAN Group** in Figure 4-33, you can define VLAN groups in the next screen (shown in Figure 4-35).

VLAN Group Setting				
	N	/LAN Index	: 1 💌	
		Active	: 💿 Yes 🔘 No	
		VLAN ID	: 1 (Decimal)	
		ATM VCs	Tagged         Image         Image <t< th=""><th></th></t<>	
		Ethernet	Port # V V V 1 2 3 4	
	W	reless LAN	Tagged Port # 0	
VLAN Group Summary				
	Group Active	ID	VLAN Group Ports	VLAN Tagged Ports
	1 Yes	1	e4,e3,e2,e1,w,p0,p1,p2,p3,p4,p5,p6,p7	
	p:pvc, e:ethernet,	and w:wla	1	
			SAVE DELETE CANCEL	

Figure 4-35

- > VLAN Index: Select the VLAN index for this VC. You can specify 8 groups in maximum.
- > VLAN ID: This indicates the VLAN group.
- ATM VCs: Select the ATM VCs as members of VLAN, and if you leave the Tagged blank, the tag in frames will be deleted when transmitted from the VC.
- > Ethernet: Select the Ethernet port as a member of VLAN.
- Wireless LAN: Select the wireless LAN port as a member of VLAN, and if you leave the Tagged blank, the tag in frames will be deleted when transmitted from the port.
- > VLAN Group Summary: This displays the information about the VLAN Groups.

## 4.4.6 ADSL

Choose "Advanced Setup $\rightarrow$ ADSL", you can select the ADSL Type and ADSL Mode in the next screen. The ADSL feature can be selected when you meet the physical connection problem. Please check the proper settings with your Internet service provider.

Advanced	Quick Start	Interface Setup	Advanced Setup	Access Managemei	nt Mai	intenance	Status	Help
	Firewall	Routing	NAT	QoS	VLAN	ADSL		
ADSL								
		ADSL Mode ADSL Type						
		HEEL I JPC						
			🗹 Bitswap I 🗹 SRA Enat					
			SKA EHAL	ле				
			SAVE					

Figure 4-36

- > **ADSL Mode:** Select the ADSL operation mode which your ADSL connection uses.
- > **ADSL Type:** Select the ADSL operation type which your ADSL connection uses.

## 4.5 Access Management

Choose "Access Management", you can see the next submenus:



Figure 4-37

Click any of them, and you will be able to configure the corresponding function.

## 4.5.1 ACL

Choose "Access Management $\rightarrow$ ACL", you can see the next screen (shown in Figure 4-38). You can specify the client to access the ADSL Router once setting his IP as a Secure IP Address through selected applications.

Access	Quick Start	Interface Setup		nced tup	Access Management	Maintenance	Status	Help				
Management	ACL	Filter		SNMP	UPnP	L II IIMS	VMP (069)					
Access Control Setup												
Access Control Setup		A	CL: 💽 🗛	tivated (	Deactivated							
Access Control Editing			0.1.		Doublination							
		ACL Rule Index : 1										
	Se	Active : ⊙ Yes ◯ No Secure IP Address : 192.168.1.20 ~ 192.168.1.200 (0.0.0.0 ~ 0.0.0.0 means all IPs)										
		Applicati	on: Web	*		(0.0.0.0 0.0.	0.0 mound un n dy					
Access Control Listing		Interfa	e : Both	*								
-		Index 4	Active	Se	cure IP Address	Application	Interface					
		1	Yes	192.16	8.1.20-192.168.1.200	Web	Both					
			SAV	E DELE								

#### Figure 4-38

- ACL: If Activated, the IP addresses which are contained in the Access Control List can access to the Router. If Deactivated, all IP addresses can access to the Router.
- > ACL Rule Index: Select the ACL rule index for the entry.
- > **Active:** Enable the ACL rule.
- Secure IP Address: Select the IP addresses which are permitted to access to the Router remotely. With the default IP 0.0.0.0, any client would be allowed to remotely access the ADSL Router.
- Application: Select the application for the ACL rule, and then you can access the Router through it.
- > Interface: Select the interface for access: LAN, WAN or Both.
- > Access Control of Listing: This displays the information about the ACL Rules.

## 4.5.2 Filter

Choose "Access Management→Filter", you can see the Filter screen (the default is IP/MAC Filter screen shown in Figure 4-39). The filtering feature includes IP/MAC Filter, Application Filter, and URL Filter. The feature makes it possible for administrators to control user's access to the Internet, protect the networks.

### 4.5.2.1 IP Filter

Select **IP/Mac Filter** as the Filter type, and select **IP** as the Rule type (shown in Figure 4-39), then you can configure the filter rules based on IP address. The filtering includes **Outgoing** and **Incoming**, the detailed descriptions are provided below.

Access	Quick Start	Interface Setup	Advanc Setu		In a r	ntenance	Status	Help			
Management	ACL	Filter	SN	IMP UPnP	DDN		VMP (069)				
Filter											
Filter Type											
		Filter Type Selection	P /MAC	Filter) V							
IP / MAC Filter Set Editing		nter Type concentri									
	IP /	MAC Filter Set Index Interface Direction	PVC0								
/ MAC Filter Rule Editing											
	IP / N	AC Filter Rule Index	. 1 🗸								
		Rule Type	and the second s								
			: O Yes	O No							
		Source IP Address : 192.168.1.7 (0.0.0.0 means Don't care)									
		Subnet Mask	sk : 255.255.255.255								
		Port Number	: 0 (0 means Don't care)								
	Destination IP Address : 0.0.0.0 (0.0.0.0 means Don't care)										
		Subnet Mask	:: 0.0.0.0								
		Port Number	: 25	25 (0 means Don't care)							
		Protoco									
IP / MAC Filter Listing		Rule Unmatched	i: Next	~							
a chine chine choing	IP / MA	C Filter Set Index	1 🗸	Interface	PVC0		Direction	Both			
	# Acti	ve Src Address	Mask	Dest IP/Mask	Src Port	Dest Port	Protocol	Unmatched			
	1 Ye	255.255.25	5.255	0.0.0.0/ 0.0.0.0	0	25	TCP	Next			
	2 Ye	192.168. 255.255.25		0.0.0.0/ 0.0.0.0	0	110	TCP	Forward			
	3 Ye	192.168. 255.255.25		202.96.134.12/ 255.255.255.255	0	0	TCP	Forward			
	4 -	-		-	-	-	-	-			
	5 -				-		-	-			
	6 -			12		-	-				

### Figure 4-39

- **Filter Type Selection:** Select the filter type for the configuration below.
- IP/MAC Filter Set Index: Select the Set index for the IP Filter entry. This index can match with six IP / MAC Filter Rule Indexes.
- > Interface: Select the interface for the entry.

### P Note:

If select PVC0~PVC7 as an interface, the filter will match the IP traffic of WAN port with specified IPs (Source IP Address and Destination IP Address). If select LAN as an interface, the filter will match the IP traffic of LAN port with specified IPs.

Direction: Select the direction for this IP Filter rule. There are three filtering directions: Both, Incoming, Outgoing.

### P Note:

Incoming means that IP traffic which is coming into the router, and the Outgoing means that IP traffic which is going out the router.

> IP/MAC Filter Rule Index: Select the Rule index for the IP Filter entry.

### P Note:

You should set the **IP/MAC Filter Set Index** and **IP/MAC Filter Rule Index** together to appoint the address (shown in the Filter List) for the IP Filter rule. For example, (1, 2), it means the rule will be shown in the row 2 IP/MAC Filter Set Index 1.

- > Rule Type: For IP Filter, please select IP here.
- > Active: Select "Yes" to make the rule to take effect.
- Source IP Address: Enter the source IP address for the rule. You can enter 0.0.0.0; it means that all IP addresses are controlled by the rule.
- Destination IP Address: Enter the destination IP address for the rule. You can enter 0.0.0.0, it means that all IP addresses are controlled by the rule. The set of Subnet Mask and Port Number are same as Source IP Address.
- Subnet Mask: Enter the Subnet Mask for the rule.
- Port Number: Enter the Port Number for the rule. You can enter 0, which means that all ports are controlled by the rule.
- > **Protocol:** Select the protocol: **TCP**, **UDP** or **ICMP** for the filter rule.
- Rule Unmatched: If the current rule can not match, and you select Forward, the router will skip the rule and transmit directly. If you select Next, the router will find the next filter rule (show in Filter list) to match.
- > **IP/MAC Filter Listing:** This displays the information about the IP Filter rules.

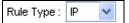
### To add an IP Address filtering entry:

**For example:** If you desire to block E-mail received and sent by the IP address 192.168.1.7 on your local network; And wish to make the PCs with IP address 192.168.1.8 unable to visit the website of IP address 202.96.134.12, while other PCs have no limit. You can configure the rules as follows. Presume the rules are both aimed at the interface PVC0, and their indexes are (1, 1), (1, 2) and (1, 3).

**Step 1:** Select the "IP/MAC Filter" as the Filer Type Selection (show in Figure 4-39).

Filter Type Selection : IP / MAC Filter 🛛 👻

Select the "IP" as the Rule Type on the Filter screen, then you can configure the specific rule for the example.



Step 2: Select the IP/MAC Filter Set Index and IP/MAC Filter Rule Index for the rule, then select the Interface "PVC0", and select the Direction "Both" for the first rule.

IP / MAC Filter Set Index :	1 💙
Interface :	PVC0 🔽
Direction :	Both 🔽
IP / MAC Filter Rule Index :	1 💌
Rule Type :	IP 🔽
Active :	💿 Yes 🔘 No

### P Note:

If you want to make the rule take effect, please select **Yes** to active the rule.

**Step 3:** Enter the "Source IP Address", "Destination IP Address", "Subnet Mask" and "Port Number" in the corresponding field.

Source IP Address :	192.168.1.7		(0.0.0.0 means Don't care)
Subnet Mask :	255.255.255.255		
Port Number :	0	(0 mea	ns Don't care)
Destination ID Address .	0000		
Destination IP Address :	0.0.0.0		(0.0.0.0 means Don't care)
Subnet Mask :	0.0.0.0		
Port Number :	25	(0 mea	ns Don't care)
Protocol :	тср 💌		
Rule Unmatched :	Next 💙		

- Step 4: Select the Protocol as "TCP" and select the Unmatched rule as "Next".
- Step 5: Finally, click the SAVE to save the entry.
- Step 6: Go to Step 2 to configure the next two rules: Block E-mail received by the IP address 192.168.1.7 on your local network; Make the PC with IP address 192.168.1.8 unable to visit the website of IP address 202.96.134.12.

### P Note:

After you complete the IP filter rules for the example, the Filter list will show as follows. You can enter the **IP / MAC Filter Set Index** to view the information about the rule.

#	Active	Src Address/Mask	Dest IP/Mask	Src Port	Dest Port	Protocol	Unmatched
1	Yes	192.168.1.7/ 255.255.255.255	0.0.0.0/ 0.0.0.0	0	25	ТСР	Next
2	Yes	192.168.1.7/ 255.255.255.255	0.0.0.0/ 0.0.0.0	0	110	ТСР	Forward
3	Yes	192.168.1.8/ 255.255.255.255	202.96.134.12/ 255.255.255.255	0	0	ТСР	Forward

#### Other operations for the entries as shown in Figure 4-39:

Select the IP / MAC Filter Set Index and IP/MAC Filter Rule Index to view or modify the entry.

Select the **IP / MAC Filter Set Index** and **IP/MAC Filter Rule Index** to locate the specific rule, and then click the **DELETE** button to delete the entry.

### 4.5.2.2 MAC Filter

Select **IP/Mac Filter** as the Filter type, and select **MAC** as the Rule type (shown in Figure 4-40), and then you can configure the filter rules based on MAC address.

Access	Quick Start	Interface Setup	Advanced Setup	Access Managemer	nt Maint	enance	Status	Help
Management		Filter	SNMP	UPnP	DDNS		VMP (069)	
Filter								
Filter Type								
	Fitt	er Type Selection :	IP / MAC Filter	<b>Y</b>				
IP / MAC Filter Set Editing								
IP / MAC Filter Set Editing								
	IP / MA	C Filter Set Index:						
		Interface						
		Direction	: Both 💌					
IP / MAC Filter Rule Editing								
	IP / MA	C Filter Rule Index :	1 🕶					
		Rule Type :						
		Active	: 💿 Yes 🔘 I	۹o				
		MAC Address	: 00:0a;eb:00:07	l'he				
		Rule Unmatched :		.be				
IP / MAC Filter Listing		Rule Ormatched						
in Annual Lioung	IP / MAC	Filter Set Index	1 💌	Interface	PVC0	I	Direction	Both
	# Active	Src Address	Mask D	est IP/Mask	Src Port	Dest Port	Protocol	Unmatched
	1 Yes	00:0a:eb:00:		-	-	-	-	Next
	2 Yes	00:0a:eb:00:	07:5f	-	-	-	-	Forward
	3 -	-		-	-	-	-	-
	4 - 5 -	-		-	•	-	-	-
	6 -			-		-	-	
	-	1						
			SAVE	ETE CANCEL	J			

Figure 4-40

- **Rule Type:** Select MAC for the MAC Filter rule.
- > Active: Select "Yes" to make the rule to take effect.
- > MAC Address: Enter the MAC address for the rule.
- Rule Unmatched: If the current rule can not match, and you select Forward, the router will skip the rule and transmit directly. If you select Next, the router will find the next filter rule (show in Filter list) to match.
- > **IP/MAC Filter Listing:** This displays the information about the MAC Filter rules.

#### To add a MAC Address filtering entry:

**For example:** If you want to block the PCs with MAC addresses 00-0A-EB-00-07-BE and 00-0A-EB-00-07-5F to access the Internet, you can configure as follows. Presume the rules are both aimed at the interface PVC0, and their indexes are (1, 1) and (1, 2).

**Step 1:** Select the "IP/MAC Filter" as the Filer Type Selection:

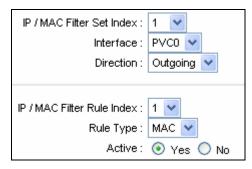
Filter Type Selection : IP / MAC Filter

Select the "MAC" as the Rule Type on the Filter screen (show in Figure 4-40).

Rule Type :	MAC	Y
-------------	-----	---

, Then you can configure the specific rule for the example.

Step 2: Select the IP/MAC Filter Set Index and IP/MAC Filter Rule Index for the rule, then select the Interface "PVC0", and select the Direction "Outgoing" for the first rule.



### P Note:

If you want to make the rule take effect, please select **Yes** to active the rule. **Step 3:** Enter the "MAC Address" and select the Unmatched rule as "Next".

MAC Address :	00:0A:EB:00:07:BE	
Rule Unmatched :	Next 💙	

**Step 4:** Finally, click the **SAVE** to save the entry.

Step 5: Go to Step 2 to configure the next rule: Block the PC with MAC address 00-0A-EB-00-07-5F to access the Internet.

### Note:

After you complete the MAC filter rules for the example, the Filter list will show as follows. You can enter the **IP / MAC Filter Set Index** to view the information about the rule.

#	Active	Src Address/Mask	Dest IP/Mask	Src Port	Dest Port	Protocol	Unmatched
1	Yes	00:0a:eb:00:07:be	-	-	-	-	Next
2	Yes	00:0a:eb:00:07:5f	-	-	-	-	Forward

Other operations for the entries as shown in Figure 4-39:

Select the IP / MAC Filter Set Index and IP/MAC Filter Rule Index to view or modify the entry.

Select the **IP / MAC Filter Set Index** and **IP/MAC Filter Rule Index** to locate the specific rule, and then click the **DELETE** button to delete the entry.

### 4.5.2.3 Application Filter

Select **Application Filter** as the Filter type (shown in Figure 4-41), and then you can configure the filter rules based on application.

TD-W8961ND Wireless N ADSL2+ Modem Router User Guide

Access	Quick Start	Interface Setup	Advanced Setup	Access Management	Maintenance	Status	Help
Management	ACL	Filter	SNMP	UPnP		WMP R069)	
Filter							
Filter Type							
	Fitt	er Type Selection	Application Filt				
Application Filter Editing		Application Filter	·     Activated	Deactivated			
			: O Allow O D				
			: 💿 Allow 🔘 D : 💿 Allow 🔘 D	•			
		Real Audio/Video	-	,			
			SAVE CAN	CEL			
				4 4 4			



- **Filter Type Selection:** Select the Application Filter for the next configuration.
- > **Application Filter:** Activate or deactivate the function.
- ICQ & MSN & YMSG & Real Audio/Video: Select Allow or Deny for these applications. If you select Allow, the Router will accept the application; if you select Deny, the Router will forbid the application.

### 4.5.2.4 URL

Select **Application Filter** as the Filter type (shown in Figure 4-42), and then you can configure the filter rules based on URL.

Filter Type											
	Filter Type	Selection : URL Filter									
RL Filter Editing											
		Active : 💿 Yes 🔿 No									
	l	JRL Index : 3 🔽									
		URL: www.sina.com									
& Filter Listing											
	Index	URL									
	1	www.baidu.com									
	2	www.cnw.com.cn									
	3	www.sina.com									
	4										
	5										
	6										
	7										
	8										
	9										
	10										
	11										
	12										
	13										
	14										
	15										
	16										

### Figure 4-42

- > Filter Type Selection: Select the URL Filter for the next configuration.
- > Active: Select "Yes" to make the rule to take effect.
- > **URL Index:** Select the index for the URL Filter entry.
- > **URL:** Enter the URL for this URL Filter.
- > URL Filter Listing: This displays the information about the URL Filter rules.

### To add a URL filter entry:

**For example:** If you want to forbid the user to access the website: <u>www.yahoo.com</u>. Presume the rule is aimed at the interface PVC0, and its index is "1".

Step 1: Select the "URL Filter" as the Filer Type Selection (show in Figure 4-42).

Step 2: Select the Index for the rule, and then enter the website in the URL field.

Step 3: Finally, Select Yes to active the rule, and then click the SAVE to save the entry.

### Other operations for the entries as shown in Figure 4-39:

Select the **URL Index** to view or modify the entry.

Select the **URL Index** to locate the specific rule, and then click the **DELETE** button to delete the entry.

### 4.5.3 SNMP

Choose "Access Management→SNMP", you can see the SNMP screen. The Simple Network Management Protocol (SNMP) is used for exchanging information between network devices.

Access	Quick Start	Interface Setup	Advanced Setup	Access Management	Maintenance	Status	Help
Management	ACL	Filter	SNMF	UPnP	DDNS	CWMP(TR069)	
SNMP							
		Get Community :	public				
		Set Community :	public				
			SAVE				
			<b>—</b> •	4 40			

Figure 4-43

- Get Community: Set the password for the incoming Get and Get next requests from the management station.
- > Set Community: Set the password for incoming Set requests from the management station.

### 4.5.4 UPnP

Choose "Access Management→UPnP", you can configure the UPnP in the screen (shown in Figure 4-44).

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.



Figure 4-44

- UPnP: Activate or Deactivate the UPnP function. Only when the function is activated, can the UPnP take effect.
- Auto-Configure: If you activate the function, then the UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions.

## 4.5.5 DDNS

Choose "Access Management $\rightarrow$ DDNS", you can configure the DDNS function in the screen (shown in Figure 4-45).

The router offers a Dynamic Domain Name System (**DDNS**) feature. The feature lets you use a static host name with a dynamic IP address. User should type the host name, user name and password assigned to your ADSL Router by your Dynamic DNS provider. User also can decide to turn on DYNDNS Wildcard or not.

Access	Quick Start	Interface Setup	Advanced Setup	Access Management	Maintenance	Status	Help
Management		Filter	SNMP	UPnP	L II IIMS	WMP R069)	
Dynamic DNS							
		Dynamic DNS : Service Provider : My Host Name : E-mail Address : Username : Password : Mildcard support :					
			SAVE				

Figure 4-45

- > **Dynamic DNS:** Activate the DDNS function or not.
- > Service Provider: This field displays the service provider of DDNS.
- > My Host Name: Enter your host name here.
- **E-mail Address:** Enter your E-mail address here.
- **Username & Password:** Type the "User Name" and "Password" for your DDNS account.
- > Wildcard support: Select the option to use Wildcard function

### 4.5.6 CWMP

Choose "Access Management $\rightarrow$ CWMP", you can configure the CWMP function in the screen (shown in Figure 4-46).

The router offers CWMP feature. The function supports TR-069 protocol which collects information, diagnoses the devices and configures the devices automatically via ACS (Auto-Configuration Server).

Access	Quick Start	Interface Setup	Advanced Setup	Access Management	Maintenance	Status	Help
Management	ACL	Filter	SNMP	UPnP		/MP 069)	
CWMP (TR069) Setup							
		CVVMP	🗧 🔘 Activated 🤇	Deactivated			
Login ACS							
		URL	:				
		User Name	:		7		
		Password	:		]		
Connection Request							
		Path	: /tr069				
		Port	: 7547				
		UserName	:				
		Password	:				
Periodic Inform							
		Periodic Inform	: 💿 Activated 🤇	Deactivated			
		Interval(s)	86400				
			SAVE CAN	CEL			

Figure 4-46

- > **CWMP:** Select activate the CWMP function.
- > URL: Enter the website of ACS which is provided by your ISP.
- > User Name/Password: Enter the User Name and password to login the ACS server.
- > **Path:** Enter the path that connects to the ACS server.
- > **Port:** Enter the port that connects to the ACS server.
- User Name/Password: Enter the User Name and Password that provided the ACS server to login the router.
- Periodic Inform: Activate or deactivate the function. If Activated, the information will be informed to ACS server periodically.
- > Interval: Enter the interval time here.

## 4.6 Maintenance

Choose "Maintenance", you can see the next submenus:



```
Figure 4-47
```

Click any of them, and you will be able to configure the corresponding function.

## 4.6.1 Administration

Choose "Maintenance $\rightarrow$ Administration", you can set new password for admin in the screen (shown in Figure 4-48).

Maintenance	Quick Start	Interface Setup	Advanced Setup	Access Management	Maintenand	ce Status	Help
	Administra	ation Tim	ne Zone	Firmware S	ysRestart	Diagnostics	
Administrator							
		Username New Password			1		
	Ca	onfirm Password	1:		j		
			SAVE CA	NCEL			



### P Note:

- 1) There is only one account that can access Web-Management interface. The default account is "admin", and the password is "admin". Admin has read/write access privilege.
- When you change the password, you should enter the new password twice, and then click SAVE to make the new password take effect.

### 4.6.2 Time Zone

Choose "**Maintenance** $\rightarrow$ **Time Zone**", you can configure the system time in the screen (shown in Figure 4-49).

The system time is the time used by the device for scheduling services. There are three methods to configure the time. You can manually set the time or connect to a NTP (Network Time Protocol) server. If a NTP server is set, you will only need to set the time zone. If you manually set the time, you may also set Daylight Saving dates and the system time will automatically adjust on those dates.

### 1) NTP Server automatically

Select NTP Server automatically as the Synchronize time, you only need to set the time zone.

Maintenance	Quick Start	Interface Setup	Advanced Setup	Access Managem	-	Maintena	nce	Status	Help
	Administr	ration <b>Tin</b>	ne Zone	Firmware	Sys	Restart	Diag	nostics	
Time Zone									
		Current Date/Time	e: 03/17/2010 15	5:57:30					
Time Synchronization									
	Sync	hronize time with	1 : 💿 NTP Servi	er automatically					
			🔵 PC's Cloci	k					
			🔘 Manually						
		Time Zone	e : (GMT) Green	wich Mean Time	: Dublin	, Edinburgh, Lis	bon, Loi	ndon 🔽	
		Daylight Saving	: OEnabled (	Disabled					
	NTE	Server Address	s: 0.0.0.0		0.0.0.0	): Default Value	)		
					-				
			SAVE CA	NCEL					
			Figure	4-49					

### P Note:

The ADSL Router built-in some NTP Servers, when the Router connects to the Internet, the

Router will get the system time automatically from the NTP Server. You can also configure the NTP Server address manually, and then the Router will get the time from the specific Server firstly.

### 2) PC's Clock

Select **PC's Clock** as the Synchronize time, you don't need to set any items.

Maintenance	Quick Start	Interface Setup	Advanced Setup	Access Managem		Maintena	nce	Status	Help
	Administr	ation Tim	ie Zone	Firmware	Sys	Restart	Diag	nostics	
Time Zone									
Time Synchronization	(	Current Date/Time	: 03/17/2010 15	:58:53					
Time Synchronization	Sync	hronize time with	: ONTP Serve	er automatically					
			📀 PC's Clock	c ·					
			O Manually		1				
		Date				/Date/Year)			
		Time	: 15 : 58	: <u>53 (</u> ł	nour:min	nsec)			
			SAVE CA	NCEL					

Figure 4-50

### 3) Manually

Select **Manually** as the Synchronize time, you need to set the date and time corresponding to the current time.

Maintenance	Quick Start	Interface Setup	Advanced Setup	Acces Manager		Maintena	ince	Status	Help
	Administ	ration Tim	ne Zone	Firmware	Sys	Restart	Diag	nostics	
Time Zone									
		Current Date/Time	e : 04/15/2009 10	):18:29					
Time Synchronization									
	Syne	chronize time with	n : 🔘 NTP Serve	er automatically					
			🔵 PC's Clock	ĸ					
			Manually						
		Date	e: 4 / 15	/ 2009	(Month/D	ate/Year)			
		Time	e: 10 ; 18	; 29 (h	our:min:s	ec)			
			SAVE CA	NCEL					

Figure 4-51

### 4.6.3 Firmware

Choose "**Maintenance** $\rightarrow$ **Firmware**", you can upgrade the firmware of the Router in the screen (shown in Figure 4-52). Make sure the firmware or romfile you want to use is on the local hard drive of the computer. Click **Browse** to find the local hard drive and locate the firmware or romfile to be used for upgrade.

Maintenance	Quick Start	Interface Setup	Advanced Setup	Access Management	Maintenance	Status	Help
	Administ	ration Tim	e Zone 🛛 🤇 🤇	irmware Sy	sRestart Diag	gnostics	
Firmware/Romfile Upgrade	New F	Firmware Version Firmware Location Romfile Location Romfile Backup	:		Browse		
		Status 1		veral minutes, don't pov	wer off it during upgrad	ding. Device will res	start after
			UPGRADE	1			

Figure 4-52

#### To upgrade the router's firmware, follow these instructions below:

- **Step 1:** Type the path and file name of the update file into the "New Firmware Location" field. Or click the **Browse** button to locate the update file.
- Step 2: Click the UPGRADE button.

#### P Note:

- 1) When you upgrade the router's firmware, you may lose its current configurations, so please back up the router's current settings before you upgrade its firmware.
- 2) Do not turn off the router or press the Reset button while the firmware is being upgraded.
- 3) The router will reboot after the upgrading has been finished.

### To back up the Router's current settings:

**Step 1:** Click the **ROMFILE SAVE** button (shown in Figure 4-52), click **Save** button in the next screen (shown in Figure 4-53) to proceed.

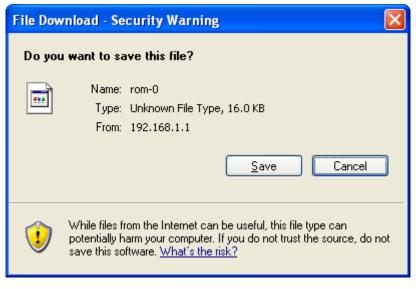


Figure 4-53

**Step 2:** Save the file as the appointed file (shown in Figure 4-54).

TD-W8961ND Wireless N ADSL2+ Modem Router User Guide

Save As						? 🔀
Save jn:	🚞 TD-W8961NI	C	<b>~</b> G	D 🖻 🛙	• 🖽 *	
My Recent Documents						
Desktop						
My Documents						
My Computer						
	File <u>n</u> ame:	rom-0			<b>~</b>	<u>S</u> ave
My Network	Save as <u>t</u> ype:	Document		-	~	Cancel

Figure 4-54

## To restore the Router's settings:

- **Step 1:** Click the **Browse** button to locate the update file for the device, or enter the exact path in "New Romfile Location" field.
- Step 2: Click the UPGRADE button to complete.

## 4.6.4 System Restart

Choose "Maintenance $\rightarrow$ SysRestart", you can select to restart the device with current settings or restore to factory default settings in the screen (shown in Figure 4-55).

Maintenance		rface Advan tup Setu			Maintenance	Status	Help
	Administration	Time Zone	Firmware	Sys	sRestart Dia	gnostics	
System Restart	System Re:	start with : 💿 Cur 🔘 Fac	rent Settings tory Default Setting	s			
		REST	ART				
		Figu	IND A EE				

Figure 4-55

## 4.6.5 Diagnostic

Choose "Maintenance $\rightarrow$ Diagnostic", you can view the test results for the connectivity of the physical layer and protocol layer for both LAN and WAN sides in the screen (shown in Figure 4-56).

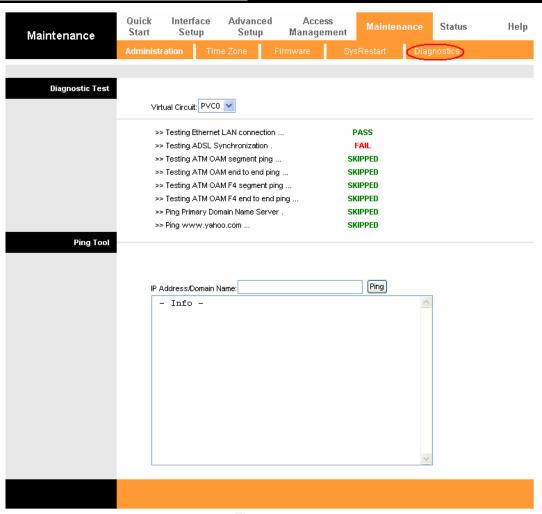


Figure 4-56

## 4.7 Help

Choose "Help", you can view the help information for configuration of any function.

Help	Quick Start	Interface Setup	Advanced Setup	Access Management	Maintenance	Status	Help
	1						
Quick Start		0	Quick Start				
Interface Setup							
			<ul> <li>Internet Setti</li> <li>LAN Settings</li> </ul>				
			Wireless LAN				
Advanced Setup							
		0	Firewall				
		0					
		0					
		0	QoS VLAN				
		-	ADSL				
Access Management							
		0	ACL				
		-	IP Filter				
			SNMP				
		-	UPnP				
		-	DDNS CWMP				
			CAAMAD				
Maintenance		•					
		0	Administratio	n			
		ŏ					
		ŏ					
		0	Diagnostics				
Status							
		0	Device Info				
		0	System Log				
		0	Statistics				

Figure 4-57

P Note:

Click the tab, and you will be able to get the corresponding information.

# **Appendix A: Specifications**

	General
	ANSI T1.413, ITU G.992.1, ITU G.992.2, ITU G.992.3, ITU G.992.5,
Standards and Protocols	IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.3, IEEE
	802.3u, TCP/IP, PPPoA, PPPoE, SNTP, HTTP, DHCP, ICMP, NAT
Safety & Emission	FCC、 CE
Ports	Four 10/100M Auto-Negotiation RJ45 ports (Auto MDI/MDIX)
FUIIS	One RJ11 port
LEDs	Power, ADSL, Internet, WLAN, 1,2,3,4(LAN), QSS
Network Medium	10Base-T: UTP category 3, 4, 5 cable
	100Base-TX: UTP category-5
	Max line length: 6.5Km
Data Rates	Downstream: Up to 24Mbps
	Upstream: Up to 3.5Mbps (With Annex M enabled)
System Requirement	Internet Explorer 5.0 or later, Netscape Navigator 6.0 or later
	Win 9x/ ME/ 2000/ XP/ Vista/Windows 7
	Physical and Environment
Working Temperature	0°C ~ 40°C
Working Humidity	10% ~ 90% RH (non-condensing)
Storage Temperature	-40°C ~ 70°C
Storage Humidity	5% ~ 90% RH (non-condensing)