

User Guide

www.tenda.cn



D840R ADSL2+ Router

Copyright Statement

Tenda[®] the registered trademark of Shenzhen Tenda Technology Co., Ltd. Other trademark or trade name mentioned herein are the trademark or registered trademark of the company. Copyright of the whole product as integration, including its accessories and software, belongs to Shenzhen Tenda Technology Co., Ltd. Without the permission of Shenzhen Tenda Technology Co., Ltd, individual or party is not allowed to copy, plagiarize, imitate or translate it into other languages.

All the photos and product specifications mentioned in this manual are for references only, as the upgrading of software and hardware, there will be changes. And if there are changes, Tenda is not responsible for informing in advance. If you want to know more about our products information, please visit our website at www.tenda.cn

CONTENTS

Chapter 1 Overview	1
1.1 Product Introduction	1
1.2 Product Features	1
1.3 Supporting Protocol.....	1
1.4 Data Encapsulation.....	3
Chapter 2 Hardware Installation	4
2.1 ADSL Router Connection	4
2.2 USB Installation.....	4
Chapter 3 Before Web Management Configuration.....	5
3.1 Network Configuration of Your Computer.....	5
3.2 Verifying the Connection	8
3.3 Logging in to the Router.....	9
Chapter 4 Quick Installation Guide	10
4.1 Configure the PPPoE	11
4.2 Configure the PPPoA	13

4.3 Configure the MER	15
4.4 Configure the IPoA	18

Chapter 5 Configuration Description20

5.1 Device Information.....	20
5.2 Advanced Settings.....	23
5.2.1 WAN	23
5.2.2 LAN.....	48
5.2.3 NAT	50
5.2.4 Security	56
5.2.5 Routing.....	64
5.2.6 DNS.....	66
5.2.7 DSL.....	71
5.3 DHCP	72
5.4 System Tool	73
5.4.1 Settings.....	73
5.4.2 System Log	75
5.4.3 Internet Time.....	77
5.4.4 Access Control.....	78
5.4.5 Software Update	81

5.4.6 Save/Reboot	81
Chapter 6 Appendix	82
Appendix 1: Troubleshooting	82
Appendix 2: FAQ	84

Chapter 1 Overview

1.1 Product Introduction

D840R ADSL2+ Router complies with ADSL, ADSL2 and ADSL2+ standards. Supporting up to 24Mbps downstream rate and 1Mbps upstream rate, it supports multiple network protocols and provides NAT Router, Bridge and switch functions. Built-in 4-port switch can add more end users without purchasing hub or switch. In addition, the intelligent software, Setup Wizard, can assist you to access the Internet fast and easily. Powerful and exquisite, it is the best choice for SOHO and small enterprise users to share the Internet.

1.2 Product Features

- Provides up to 24Mbps downstream rate and 1Mbps upstream rate
- Supports DHCP, NAT, IGMP, ICMP, ARP
- Four 10/100M Auto-Negotiation RJ-45 Ethernet ports for network adapter, Hub and switch

connectivity

- One RJ-11 port and Voice Splitter included
- One USB port support for connecting PC's USB port
- Provides Web-based management and firmware upgrade
- Complies with ADSL, ADSL2 and ADSL2+ standards
- Provides NAT Router, Bridge and switch functions
- Compatible with all mainstream DSLAM (CO)
- Provides PPPOE, PPPOA, CLIP protocols
- Supports firewall and hacker attack prevention
- Supports Internet Multi Media
- Provides static and dynamic routes
- Up to 6.5km transmission distance
- Setup Wizard support for fast and easy configurations

1.3 Supporting Protocol

Supports full-rate ADSL2+ standard

- ANSI T1. 413 Issue 2
- ITU-T G. 992. 1 (G. dmt)
- ITU-T G. 992. 2 (G. Lite)

- ITU-T G. 992. 3
- ITU-T G. 992. 5

1.4 Data Encapsulation

- Supports RFC 1483 Bridge、RFC 1483 Router
- Supports Classical IP over ATM (RFC 1577)
- Supports PPP over ATM(RFC 2364)
- Supports PPP over Ethernet (RFC 2516)

Chapter 2 Hardware Installation

2.1 ADSL Router Connection

1. Connect one end of the telephone line to the LINE port of the D810R and the other end to the MODEM port of the voice splitter.
2. Connect the power adapter to the PWR port of the D810R.
3. Use an Ethernet cable to connect the LAN port with the NIC of your computer.

2.2 USB Installation

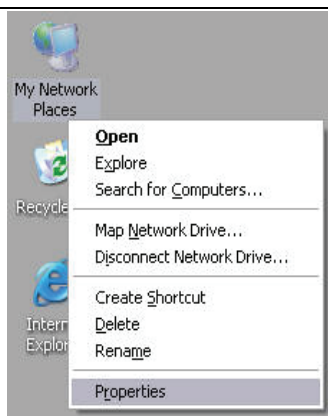
To connect the device to the USB interface of the computer, please follow the steps below:

1. Connect to the USB port of the D810R through a USB cable.
2. Connect the other end of the cable to the computer's USB port.
3. Set up the USB driver provided by the CD-ROM.

Chapter 3 Before Web Management Configuration

3.1 Network Configuration of Your Computer

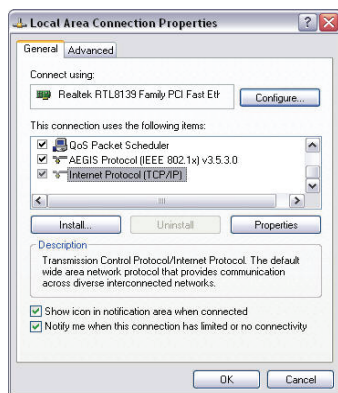
1. On the desktop of your computer, right-click "My Network Places", and then select "Properties" in the shortcut menu.



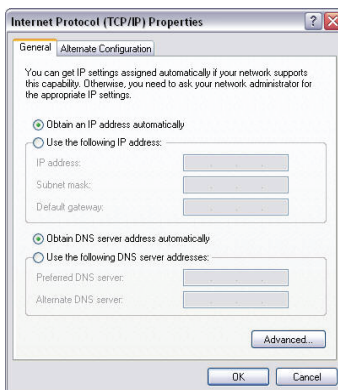
2. In the window that appears, right-click "Local Area Connection", and then select "Properties".



3. In the pop-up dialog box, check "Internet Protocol (TCP/IP)" and then click "Properties".



4. In the window that appears, select "Obtain an IP address automatically (O)" or "Use the following IP address (S)".
- 1) When "Obtain an IP address automatically (O)" is selected, the window is as shown in the right figure.



2) "Use the following IP address":

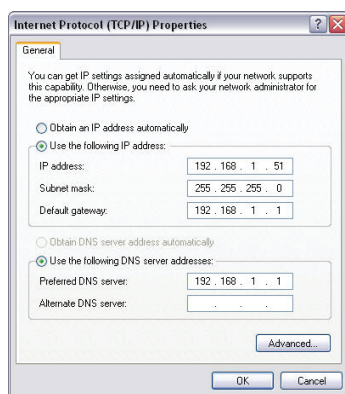
IP address: 192.168.1.XXX
(XXX ranges 2 ~ 254)

Subnet mask:
255.255.255.0

Default gateway:
192.168.1.1

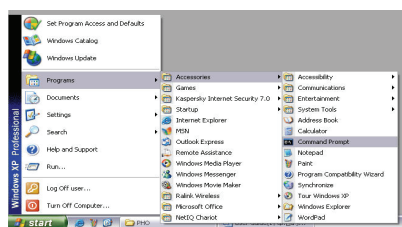
DNS server: Enter the local DNS server address (for this address, you can consult your ISP) or the router's default gateway as the DNS server.

At the end of the setting, click "OK" to submit the settings. And then click "OK" in the "Local Area Connection Properties" window.

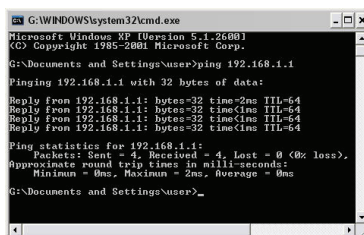


3.2 Verifying the Connection

1. Select "Start→Programs→Accessories→Comm and Prompt".

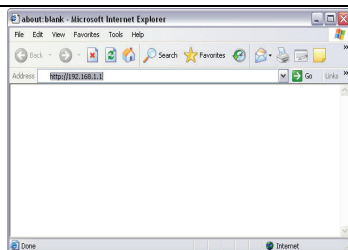


According to the format shown in the right figure, enter "Ping 192.168.1.1" and press Enter. If the system gives the result shown in the right figure, the connection between your computer and the router is OK.



3.3 Logging in to the Router

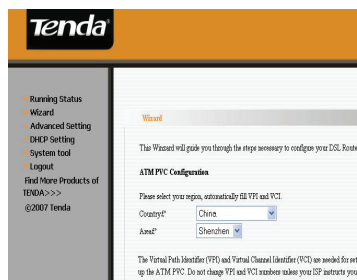
1. Open the web browser, and enter "http://192.168.1.1" in the address field, and then press Enter.



2. In the pop-up login window, enter the user name ("admin") and password ("admin"), and click "OK" (both user name and password are "admin" by default).



3. If the user name and password entered are correct, the browser displays the administrator window shown right.



Chapter 4 Quick Installation Guide

In the Wizard page, Select the required your "Country" and "Area" from the drop-down lists. If you can not find your country and city in these lists, you can consult your ISP and manually enter the VPI and VCI values of your area. After that, click "Next".

The screenshot shows the 'Wizard' page for 'ATM PVC Configuration'. It includes instructions to select a region and fill in VPI and VCI. The 'Country' dropdown is set to 'China' and the 'Area' dropdown is set to 'Shenzhen'. Below, the 'VPI' is set to 8 and the 'VCI' is set to 35. There is a section for 'Enable Quality Of Service' with a checkbox that is currently unchecked. A 'Next' button is at the bottom.

Wizard

This Wizard will guide you through the steps necessary to configure your DSL Router.

ATM PVC Configuration

Please select your region, automatically fill VPI and VCI.

Country: China

Area: Shenzhen

The Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) are needed for setting up the ATM PVC. Do not change VPI and VCI numbers unless your ISP instructs you otherwise.

VPI: [0-255] 8

VCI: [32-65535] 35

Enable Quality Of Service

Enabling QoS for a PVC improves performance for selected classes of applications. However, since QoS also consumes system resources, the number of PVCs will be reduced consequently. Use **Advanced Setup/Quality of Service** to assign priorities for the applications.

Enable Quality Of Service ☐

Next

4.1 Configure the PPPoE

1. Select "PPP over Ethernet (PPPoE)". Click "Next".

Connection Type

Select the type of network protocol for IP over Ethernet on WAN interface

☐ PPP over ATM (PPPoA)

☒ PPP over Ethernet (PPPoE)

☐ MAC Encapsulation Routing (MER)

☐ IP over ATM (IPoA)

☐ Bridging

Encapsulation Mode

LLC/SNAP-BRIDGING

Back Next

2. Enter the PPP user name and password provided by the ISP. If the ISP also provides the PPPoE service name, you can enter the corresponding value; otherwise, keep this field null. Use the default values for other options. For their more settings, refer to the detailed description in the Advanced Settings.

PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username: tende@163.gd

PPP Password: *****

PPPoE Service Name:

Authentication Method: AUTO

☒ Dial on demand (with idle timeout timer)

Inactivity Timeout (minutes) [1-4320]: 50

☐ PPP IP extension

☒ Use Static IP Address

IP Address: 51.219.66.7

☐ Retry PPP password on authentication error

☒ Bridge PPPoE Frames Between WAN and Local Ports (Default Enabled)

3. Click "Next" and check to enable the WAN service (enabled by default).

Enable IGMP Multicast, and WAN Service

Enable IGMP Multicast ☐

Enable WAN Service ☒

Service Name

4. Click "Next" to display the window shown the summary of your settings.

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

VPI / VCI:	8 / 35
Connection Type:	PPPoE
Service Name:	pppoe_8_35_1
Service Category:	USB
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.

NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.

5. Click "Save/Reboot" to activate your settings. The system automatically establishes connection in a few minutes.

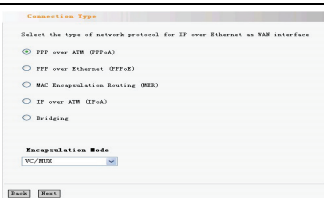
DSL Router Reboot

The DSL Router has been configured and is rebooting.

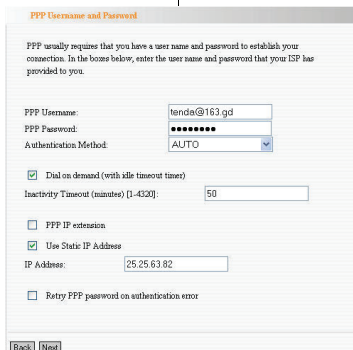
Rebooting, please waiting 35seconds

4.2 Configure the PPPoA

1. Select "PPP over ATM (PPPoA)". Click "Next".



2. Enter the PPP user name and password provided by the ISP. If the ISP also provides the PPPoA service name, you can enter the corresponding value; otherwise, keep this field null. Use the default values for other options. For their more settings, refer to the detailed description in the Advanced Settings.



3. Click "Next" and check to enable the WAN service (enabled by default).

Enable IGMP Multicast, and WAN Service

Enable IGMP Multicast ☐

Enable WAN Service ☒

Service Name

4. Click "Next" to display the window shown the summary of your settings.

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

VPI / VCI:	8 / 35
Connection Type:	PPPoE
Service Name:	pppoe_8_35_1
Service Category:	USB
IP Address:	Automatically Assigned
Service State:	Enabled
WAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.

NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.

5. Click "Save/Reboot" to activate your settings. The system automatically establishes connection in a few minutes.

DSL Router Reboot

The DSL Router has been configured and is rebooting



Rebooting, please waiting 35seconds

4.3 Configure the MER

1. Select "MAC Encapsulation Routing (MER)". Click "Next".

2. If your ISP provides the static IP address, you should enter the corresponding values in "WAN IP Address" and "WAN Subnet Mask".

3. If your ISP provides the dynamic IP address, you should select "Obtain an IP address automatically".

WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.
 Notice: DHCP can be enabled for PPP in MEER mode or IP over Ethernet as WAN interface if "Obtain an IP address automatically" is chosen. Changing the default gateway or the DNS affects the whole system. Configuring them with static values will disable the automatic assignment from DHCP or other WAN connections.
 If you configure static default gateway over this PPP in MEER mode, you must enter the IP address of the remote gateway in the "Use IP address". The "Use WAN interface" is optional.

☒ Obtain an IP address automatically
☐ Use the following IP address:

WAN IP Address:

WAN Subnet Mask:

☒ Obtain default gateway automatically
☐ Use the following default gateway:

☐ Use IP Address:

☐ Use WAN Interface: [HW](#)

☒ Obtain DNS server addresses automatically
☐ Use the following DNS server addresses:

Primary DNS server:

Secondary DNS server:

4. Click "Next". In the case of multiple computers share the Internet access service, it is recommended to enable NAT and firewall.

Settings - Backup

Network Address Translation Settings

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

Enable NAT: ☒

Enable Firewall: ☒

Enable IGMP Multicast, and WAN Service

Enable IGMP Multicast: ☐

Enable WAN Service: ☒

Service Name:

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

5. Click "Next" to display the window shown the summary of your settings.

VAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

VPI / VCI:	8 / 35
Connection Type:	WEB
Service Name:	ser_8_35
Service Category:	USB
IP Address:	192.168.1.1
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.

NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.

6. Click "Save/Reboot" to activate your settings. The system automatically establishes connection in a few minutes.

DSL Router Reboot

The DSL Router has been configured and is rebooting.

 Rebooting, please waiting 35seconds

4.4 Configure the IPoA

1. Select "IP over ATM (IPoA)". Click "Next".

2. Enter the fixed IP address and subnet mask in corresponding fields.

3. Click "Next". It is recommended to enable the NAT and firewall.

4. Click "Next" to display the window shown the summary of your settings.

VAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

VPI / VCI:	8 / 35
Connection Type:	PPPoE
Service Name:	ipoe_8_35
Service Category:	USB
IP Address:	58.251.70.7
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Disabled

Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.
NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.

[Back](#) [Save/Reboot](#)

5. Click "Save/Reboot" to activate your settings. The system automatically establishes connection in a few minutes.

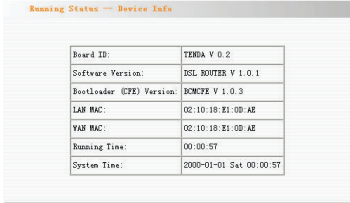
DSL Router Reboot

The DSL Router has been configured and is rebooting.

Rebooting, please waiting 35 seconds

Chapter 5 Configuration Description

5.1 Device Information

1) Click "Running Status" and "Summary" to display the "Device Info" and "DSL Info" window.															
2) The device information covers: a. Board ID b. Software version c. Boot version d. LAN MAC address e. WAN MAC address f. Running time g. System time	 <p>The screenshot shows a window titled "Running Status - Device Info". Inside, there is a table with the following data:</p> <table border="1"><tbody><tr><td>Board ID:</td><td>TENDA V 0.2</td></tr><tr><td>Software Version:</td><td>ISL ROUTER V 1.0.1</td></tr><tr><td>Bootloader (CFE) Version:</td><td>BOMCFE V 1.0.3</td></tr><tr><td>LAN MAC:</td><td>02:10:18:E1:0D:AE</td></tr><tr><td>WAN MAC:</td><td>02:10:18:E1:0D:AE</td></tr><tr><td>Running Time:</td><td>00:00:57</td></tr><tr><td>System Time:</td><td>2000-01-01 Sat 00:00:57</td></tr></tbody></table>	Board ID:	TENDA V 0.2	Software Version:	ISL ROUTER V 1.0.1	Bootloader (CFE) Version:	BOMCFE V 1.0.3	LAN MAC:	02:10:18:E1:0D:AE	WAN MAC:	02:10:18:E1:0D:AE	Running Time:	00:00:57	System Time:	2000-01-01 Sat 00:00:57
Board ID:	TENDA V 0.2														
Software Version:	ISL ROUTER V 1.0.1														
Bootloader (CFE) Version:	BOMCFE V 1.0.3														
LAN MAC:	02:10:18:E1:0D:AE														
WAN MAC:	02:10:18:E1:0D:AE														
Running Time:	00:00:57														
System Time:	2000-01-01 Sat 00:00:57														

3) The DSL information covers:

- a. Upstream link rate
- b. Downstream link rate
- c. LAN IP address
- d. Default gateway: In the pure bridge mode, there is no gateway; in other modes such as PPPoE and PPPoA, the gateway address is the IP address of the upstream device.
- e. Primary DNS server: In the PPPoA/PPPoE mode, the DNS address is obtained from the upstream device; in the pure bridge mode, it is not required to set the DNS address; in other modes, you can manually enter the DNS address.
- f. Secondary DNS server

Running Status — DSL Info

This information reflects the current status of your DSL connection.

Line Rate - Upstream (Kbps):	
Line Rate - Downstream (Kbps):	
LAN IP Address:	192.168.1.1
Default Gateway:	
Primary DNS Server:	192.168.1.1
Secondary DNS Server:	192.168.1.1

- 4) Click "WAN" in left menu to display the window shown in the right figure. From the table, you can know the general information on WAN.

Running Status - WAN

Interface	Mac	IP	Category	Service	Interface	Protocol	Ipip	QoS	State	Dynamic	IP Address
WAN	00E	1	WAN	pppoe_3_3_1	pppoe_3_3_1	PPPoE	Enabled	Enabled	Enabled	WAN Link Up	
WAN	00E	2	WAN	pppoe_3_3_2	pppoe_3_3_2	PPPoE	Enabled	Enabled	Enabled	WAN Link Down	

- 5) Click "Route" to display the window shown in the right figure, displaying the default information.

Running Status - Route

Flag: U - up, I - reject, O - gateway, H - host, R - redistribute
D - dynamic (redirect), M - modified (redirect)

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
192.168.1.0	0.0.0.0	255.255.255.0	U	0		wan

5.2 Advanced Settings

5.2.1 WAN

Click "WAN". If the WAN information has been set, you can edit or modify it in this window.

Caution: After modifying/adding new information, you need to reboot the device to activate the setting.

- 1) VPI (Virtual Path Identifier): Virtual path between two points in the ATM network. Its value ranges 0 ~ 255.
- 2) VCI (Virtual Channel Identifier): Virtual channel between two points in the ATM network. Its value ranges 32 ~ 65535 (1 ~ 31 are reserved for the well-known protocols).

The screenshot shows the 'WAN Configuration' page. It includes a title bar 'WAN Configuration' and a section 'ATM PVC Configuration'. Below this, there is explanatory text about configuring VPI and VCI. A form allows selecting a region (Country: China, Area: Shenzhen) and entering VPI (0-255) and VCI (32-65535) values. There are checkboxes for 'VLAN Wan' and 'Enable Quality Of Service'. A 'Service Category' dropdown is set to 'DDR Without PCR'. At the bottom, there are 'Back' and 'Next' buttons.

WAN Configuration

ATM PVC Configuration

This screen allows you to configure an ATM PVC identifier (VPI and VCI) and select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.

Please select your region, automatically fill VPI and VCI.

Country:

Area:

VPI: [0-255]

VCI: [32-65535]

VLAN Wan - Enable Multiple Protocols Over a Single PVC ☐

Service Category:

Enable Quality Of Service

Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use *Advanced Setup/Quality of Service* to assign priorities for the applications.

Enable Quality Of Service ☐

- | | |
|--|--|
| <p>3) Service category:
Selecting one from five
available service
categories.</p> <p>4) Enable Quality of Service
(QoS): check to enable it.</p> | |
|--|--|

PPPoA mode

- 1) Select "PPP over ATM (PPPoA)".
- Encapsulation Mode:
VC/MUX
LLC/ENCAPSULATION
- Once you select one mode, the system automatically changes the encapsulation mode into the one matching your setting. Therefore, it is recommended to keep the default setting unchanged.

The screenshot shows a web interface for configuring a network connection. The title is "Connection Type". Below the title, it says "Select the type of network protocol for IP over Ethernet as WAN interface". There are five radio button options: "PPP over ATM (PPPoA)" (which is selected), "PPP over Ethernet (PPPoE)", "MAC Encapsulation Routing (MER)", "IP over ATM (IPoA)", and "Bridging". Below these options is a section titled "Encapsulation Mode" with a dropdown menu currently showing "VC/MUX". At the bottom of the form are "Back" and "Next" buttons.

2) Click “Next” to display the window shown in the right figure.

a. Authentication Method:
AUTO/PAP/CHAP/MSCHAP. Usually, “AUTO” is selected.

b. Dial on demand:
If you check this option, you need to manually enter the timeout time. If no flow is detected when the timeout time is up, the device will disconnect the network connection automatically. And when a flow is detected, the device automatically makes dial-up connection again.
If you disable this option, the device is always in online status until device power-off, connection failure or other failures occur.

PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:

PPP Password:

Authentication Method:

☒ Dial on demand (with idle timeout timer)

Inactivity Timeout (minutes) [1-4320]:

☐ PPP IP extension

☒ Use Static IP Address

IP Address:

☐ Retry PPP password on authentication error

C. PPP IP extension:

When the integrated gateway is connected with a computer, the IP address obtained through the upstream link is directly allocated to this computer connecting with the device. After the PPP IP extension is enabled, you can enable the advanced DMZ. At this time, you need to enter your DMZ host and subnet mask.

d. Use Static IP Address:

After this option is checked, the device uses this IP address as the WAN IP address and does not need to obtain it through the upstream link.

e. Retry PPP password on authentication error

f. Enable PPP debugging mode.

3) Click "Next" to display the window shown in the right figure.

- a. Enable IGMP Multicast:
IGMP agent. For example, to enable the IPTV in the PPPoE mode, you need to check this option.
- b. Enabled WAN Service:
Checked by default. It is recommended to keep this default setting, unless you do not need to activate your WAN.

Enable IGMP Multicast, and WAN Service

Enable IGMP Multicast	<input checked="" type="checkbox"/>
Enable WAN Service	<input checked="" type="checkbox"/>
Service Name	<input type="text" value="pppoe_8_35_1"/>

- 4) Click "Next" to display the window shown in the right figure. This window shows the general information set.

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

VPI / VCI:	8 / 35
Connection Type:	PPPoE
Service Name:	pppoe_8_35_1
Service Category:	UNR
IP Address:	61.187.22.9
Service State:	Enabled
NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Enabled
Quality Of Service:	Disabled

Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.

NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.

[Back](#) [Save/Reboot](#)

- 5) Click "Save/Reboot" to activate your settings.

DSL Router Reboot

The DSL Router has been configured and is rebooting.



Rebooting, please waiting 35 seconds

PPPoE mode

- 1) Select "PPP over Ethernet (PPPoE)".
Encapsulation Mode:
VC/MUX
LLC/SNAP-BRIDGING
Once you select one mode, the system automatically changes the encapsulation mode into the one matching your setting. Therefore, it is recommended to keep the default setting unchanged.

Connection Type

Select the type of network protocol for IP over Ethernet as WAN interface

☐ PPP over ATM (PPPoA)

☒ PPP over Ethernet (PPPoE)

☐ MAC Encapsulation Routing (MER)

☐ IP over ATM (IPoA)

☐ Bridging

Encapsulation Mode

LLC/SNAP-BRIDGING

Back Next

2) Click “Next” to display the window shown in the right figure.

a. Authentication

Method:

AUTO/PAP/CHAP/MSCHAP. Usually, “AUTO” is selected.

b. Dial on demand:

If you check this option, you need to manually enter the timeout time. If no flow is detected when the timeout time is up, the device will disconnect the network connection automatically. And when a flow is detected, the device automatically makes dial-up connection again.

If you disable this

PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method:

☒ Dial on demand (with idle timeout timer)

Inactivity Timeout (minutes) [1-4320]:

☐ PPP IP extension

☒ Use Static IP Address

IP Address:

☐ Retry PPP password on authentication error

☒ Bridge PPPoE Frames Between WAN and Local Ports (Default Enabled)

option, the device is always in online status until device power-off, connection failure or other failures occur.

c. PPP IP extension:

When the device is connected with a computer, the IP address obtained through the upstream link is directly allocated to this computer connecting with the device. After the PPP IP extension is enabled, you can enable the advanced DMZ. At this time, you need to enter your DMZ host and subnet mask.

d. Use Static IP Address:

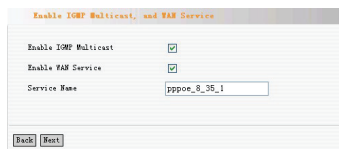
After this option is checked, the device

uses this IP address as the WAB IP address and does not need to obtain it through the upstream link.

- e. Retry PPP password on authentication error
- f. Enable PPP debugging mode.

8) Click “Next” to display the window shown in the right figure.

- a. Enable IGMP Multicast:
IGMP agent. For example, to enable the IPTV in the PPPoE mode, you need to check this option.
- b. Enabled WAN Service:
Checked by default. It is recommended to keep this default setting, unless you do not need to activate your WAN.



Enable IGMP Multicast, and WAN Service	
Enable IGMP Multicast	<input checked="" type="checkbox"/>
Enable WAN Service	<input checked="" type="checkbox"/>
Service Name	<input type="text" value="pppoe_8_35_1"/>
<input type="button" value="Back"/> <input type="button" value="Next"/>	

8) Click "Next" to display the window shown in the right figure. This window lists your settings.

VDSL Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

VPI / VCI:	8 / 35
Connection Type:	PPPoE
Service Name:	pppoe_8_35_1
Service Category:	USB
IP Address:	51.219.66.7
Service State:	Enabled
NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Enabled
Quality Of Service:	Disabled

Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.
NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.

8) Click "Save/Reboot" to activate your settings.

DSL Router Reboot

The DSL Router has been configured and is rebooting.

Rebooting, please waiting 35 seconds

MER mode

- 1) Select "MAC Encapsulation Routing(MER)".
Encapsulation Mode:
VC/MUX
LLC/SNAP-BRIDGING
Once you select one mode, the system automatically changes the encapsulation mode into the one matching your setting. Therefore, it is recommended to keep the default setting unchanged.

The screenshot shows the router's configuration page. At the top, there's a header "Connection Type". Below it, a sub-header reads "Select the type of network protocol for IP over Ethernet as WAN interface". There are five radio button options: "PPP over ATM (PPPoA)", "PPP over Ethernet (PPPoE)", "MAC Encapsulation Routing (MER)", "IP over ATM (IPoA)", and "Bridging". The "MAC Encapsulation Routing (MER)" option is selected. Below this, there's a section titled "Encapsulation Mode" with a dropdown menu currently set to "LLC/SNAP-BRIDGING". At the bottom of the form are "Back" and "Next" buttons.

2) Click "Next" to display the window shown in the right figure.

a. Obtain an IP address automatically:

If your device automatically obtains the IP address, the IP address and other parameters will be from your ISP automatically.

b. Use the following IP address:

To manually specify an address, you need to check this option and enter your static IP address and subnet mask.

c. Obtain default gateway automatically:

If this option is checked, the device

WAN IP Settings

WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.
Notice: DHCP can be enabled for PVC in MER mode or IP over Ethernet as WAN interface if "Obtain an IP address automatically" is chosen. Changing the default gateway or the DNS effects the whole system. Configuring them with static values will disable the automatic assignment from DHCP or other WAN connection.

If you configure static default gateway over this PVC in MER mode, you must enter the IP address of the remote gateway in the "Use IP address". The "Use WAN interface" is optional.

☒ Obtain an IP address automatically
☐ Use the following IP address:

WAN IP Address:
WAN Subnet Mask:

☒ Obtain default gateway automatically
☐ Use the following default gateway:

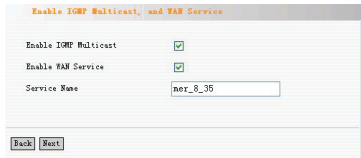
☐ Use IP Address:
☐ Use WAN Interface:

☒ Obtain DNS server addresses automatically
☐ Use the following DNS server addresses:

Primary DNS server:
Secondary DNS server:

automatically obtains the default gateway address from the upstream device.

- 3) Use the following default gateway: To manually enter a gateway, check this option.
 - a. Use IP Address:
After checking "Use the following default gateway", you can enter a value here.
 - b. Use WAN Interface:
For the broadband access device, you need to enter the IP address of the downstream link interface.
- 4) Obtain DNS server address automatically:
If this option is checked,

<p>the device automatically obtains the DNS address.</p> <p>5) Use the following DNS server address:</p> <p>To manually enter a DNS address, check this option.</p> <p>a. Primary DNS server</p> <p>b. Secondary DNS server</p>	
<p>6) Click “Next”.</p> <p>a. Enable IGMP Multicast: IGMP agent. For example, to enable the IPTV in the PPPoE mode, you need to check this option.</p> <p>b. Enable WAN Service: Checked by default. It is recommended to keep this default setting, unless you do not need to activate</p>	

your WAN.

- 7) Click "Next" to display the window shown in the right figure. This window lists your settings.

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

VPI / VCI:	8 / 35
Connection Type:	WEB
Service Name:	mer_8_35
Service Category:	WEB
IP Address:	Automatically Assigned
Service State:	Enabled
BAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Enabled
Quality Of Service:	Disabled

Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.

NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.

[Back](#) [Save/Reboot](#)

- 8) Click "Save/Reboot" to activate your settings.

DSL Router Reboot

The DSL Router has been configured and is rebooting.



Rebooting, please waiting 36seconds

IPoA mode

- 1) Select "IP over ATM (IPoA)".
Encapsulation Mode:
VC/MUX
LLC/SNAP-ROUTING
Once you select a mode, the system automatically changes the encapsulation mode into the one matching your setting. Therefore, it is recommended to keep the default setting unchanged.



Connection Type

Select the type of network protocol for IP over Ethernet at WAN interface

- ☐ PPP over ATM (PPPoA)
- ☐ PPP over Ethernet (PPPoE)
- ☐ MAC Encapsulation Routing (MER)
- ☒ IP over ATM (IPoA)
- ☐ Bridging

Encapsulation Mode

LLC/SNAP-ROUTING

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

2) Click "Next" to display the window shown in the right figure.

a. WAN IP Address:

Enter the IP address provided by your ISP.

b. WAN Subnet Mask:

Enter the subnet mask provided by your ISP.

c. Use the following default gateway:

You can check this option.

d. Use IP Address:

Enter the IP address provided by your ISP.

e. Use WAN Interface:

For the broadband access device, you need to enter the IP address of the downstream link interface.

3) Use the following DNS server address:

WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.

Notice: DHCP is not supported in IPoA mode. Changing the default gateway or the DNS affects the whole system. Configuring them with static values will disable the automatic assignment from other WAN connection.

WAN IP Address:

WAN Subnet Mask:

☒ Use the following default gateway:

☒ Use IP Address:

☒ Use WAN Interface:

☒ Use the following DNS server addresses:

Primary DNS server:

Secondary DNS server:

You can check this option.

- a. Primary DNS server
- b. Secondary DNS server

Caution: In the IPoA mode, DHCP is not supported, so you need to manually enter the WAN IP address, subnet mask, default gateway, DNS server and other settings.

- 4) Click "Next".
- a. Enable NAT:
NAT enables multiple computers in your LAN to use the same WAN IP address for Internet access. It is recommended to check this option.
- b. Enable Firewall
It is recommended to check this option to avoid some attacks.
- c. Enable IGMP Multicast:
IGMP agent. For example, to enable the IPTV in the PPPoE mode, you need to check this option.
- d. Enable WAN Service:
Checked by default. It is recommended to keep this default setting, unless you do not need to activate your WAN.

Settings - Backup

Network Address Translation Settings

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

Enable NAT ☒

Enable Firewall ☒

Enable IGMP Multicast, and WAN Service

Enable IGMP Multicast ☒

Enable WAN Service ☒

Service Name:

Back Next

e. Click "Next" to display the window shown in the right figure. This window lists your settings.

VLAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

VPI / VCI:	8 / 35
Connection Type:	IPoA
Service Name:	ipoa_8_35
Service Category:	VOIP
IP Address:	61.215.66.7
Service State:	Enabled
NAT:	Enabled
Firewall:	Enabled
IGMP Multicast:	Enabled
Quality Of Service:	Disabled

Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.
NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.

g. Click "Save/Reboot" to activate your settings.

DSL Router Reboot

The DSL Router has been configured and is rebooting.

 Rebooting, please waiting 35seconds

Bridging mode

1) Select "Bridging".

Encapsulation Mode:

VC/MUX

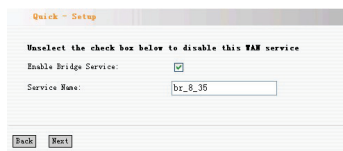
LLC/SNAP-BRIDGING

Once you select a mode, the system automatically changes the encapsulation mode into the one matching your setting. Therefore, it is recommended to keep the default setting unchanged.



2) Enable Bridge Service:

To select the bridge mode, you need to check this option. By default, this option is checked.



3) Click "Next" to display the window shown in the right figure. This window lists your settings.

VAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

VPI / VCI:	8 / 35
Connection Type:	Bridge
Service Name:	br_8_35
Service Category:	USB
IP Address:	Not Applicable
Service State:	Enabled
NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Not Applicable
Quality Of Service:	Disabled

Click "Save/Reboot" to save these settings and reboot router. Click "Back" to make any modifications.

NOTE: The configuration process takes about 1 minute to complete and your DSL Router will reboot.

4) Click "Save/Reboot" to activate your settings.

DSL Router Reboot

The DSL Router has been configured and is rebooting.

Rebooting, please waiting 35seconds

5.2.2 LAN

- 1). IP Address: IP address used by the router to connect to the LAN. This option is set to 192.168.1.1 upon device delivery. You can change it as required.

Caution: After changing this IP address, you need to use the new IP address to access the Web management window upon next login to the router. In addition, you must set the default gateway in each computer in your LAN to this IP address, to ensure normal Internet access.

- 2). Subnet Mask: Setting

Advanced Setting - LAN

Configure the DSL Router IP Address and Subnet Mask for LAN interface. Save button only saves the LAN configuration data. Save/Reboot button saves the LAN configuration data and reboots the router to make the new configuration effective.

IP Address:

Subnet Mask:

☐ Enable IGMP Snooping

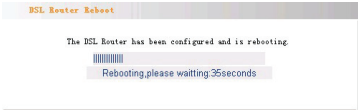
☒ Standard Mode

☐ Blocking Mode

☒ Configure the second IP Address and Subnet Mask for LAN interface

IP Address:

Subnet Mask:

<p>your subnet mask.</p> <p>3). Enable IGMP Snooping: Used in the bridge mode.</p> <p>4). Standard Mode</p> <p>5). Blocking Mode</p> <p>6). Configure the second IP Address and Subnet Mask for LAN interface.</p>	
<p>Click "Save/Reboot".</p>	

5.2.3 NAT

5.2.3.1. Virtual Server

- 1) Click “NAT” → “Virtual Server” to display the window shown in the right figure. Here, you can add or delete your virtual server settings. By default, the external networks cannot access the IP address of your internal network. However, if you need such access by the external networks (for example, you need to set up the server or support some special applications), you should enable this function to allow the access by external networks.



2) Click "Add" to display the window shown in the right figure.

a. Select a Service:
Selecting the service to be enabled.

b. Custom Server:
Manually entering the server name.

c. Server IP Address: LAN
IP address for the server.

Caution: After a service is selected, the system automatically opens the corresponding port. After you manually enter a customized service, you need to manually enter the port to be opened.

NAT - Virtual Servers

Select the service name, and enter the server IP address and click "Save/Apply" to forward IP packets for this service to the specified server. NOTE: The "Internal Port End" cannot be changed. It is the same as "External Port End" normally and will be the same as the "Internal Port Start" or "External Port End" if either one is modified.

Remaining number of entries that can be configured:

32

Server Name:

☒ Select a Service: FTP Server

☐ Custom Server:

Server IP Address: 192.168.1.100

Save/Apply				
External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
21	21	TCP	21	21
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		

- d. Click "Save/Apply" to display the service added, as shown in the right figure.

Advanced Setting >>> NAT >>> Virtual Server Setting

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External Port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number apply the service on the LAN side. A maximum 32 entries can be configured.

Service Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	Remove
FTP-Server	21	21	TCP	21	21	192.168.1.100	<input type="checkbox"/>

5.2.3.2 Port Triggering

- 1) Click "Port Triggering" to display the window shown in the right figure. Here, you can add or delete your port triggering service settings. For some special applications, you need to enable some application ports. Through the port triggering, you can enable the automatic opening of the ports required by applications.

Advanced Setting >>> NAT >>> Port Triggering Setting

Some applications require the specific ports in the Router's firewall to be opened for access by the remote parties. Port Trigger dynamically opens up the "Open Ports" in the firewall when an application on the LAN initiates a NAT-type connection to a remote party using the "Triggering Ports". The Router allows the remote party from the WAN side to establish any connection back to the application on the LAN side using the "Open Ports". A maximum 32 entries can be configured.

Application	Trigger	Open	Remove	
Name	Protocol	Port Range	Protocol	Port Range
	Start	End	Start	End

Add

Remove

- 2) Click "Add" to display the window shown in the right figure.

 - a. Select an application: Selecting the name of the service to be enabled.
 - b. Custom application: Manually entering the service name.

Caution: After a service is selected, the system automatically sets the corresponding port. After you manually enter a customized service, you need to manually enter the port to be triggered.

- 3) Click "Save/Apply" to display the service added, as shown in the right figure.

NAT — Port Triggering

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own. (Custom applications) click "Save/Apply" to add it.

Remaining number of entries that can be configured: 32

Application Name:

☒ Select an application: QuickTime 4 Client

☐ Custom application:

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
554	554	TCP	6970	32000	UDP
554	554	TCP	6970	7000	TCP/UDP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP

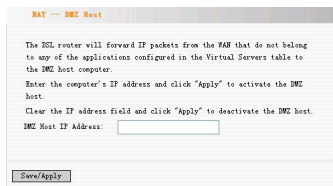
Advanced Setting — NAT — Port Triggering Setup

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger Setup dynamically opens up the "Open Port" in the firewall when an application on the LAN initiates a NAT connection to a remote party using the "Triggering Port". The browser allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the "Open Port". A maximum 32 entries can be configured.

Application	Trigger			Open		Remarks
Name	Protocol	Port Range	Protocol	Port Range		
		Start End		Start End		
QuickTime 4 Client	TCP	554 554	UDP	6970 32000		<input type="checkbox"/>
QuickTime 4 Client	TCP	554 554	TCP/UDP	6970 7000		<input type="checkbox"/>

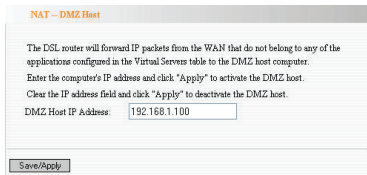
5.2.3.3 DMZ Host

1. Click "DMZ Host" to display the window shown in the right figure.



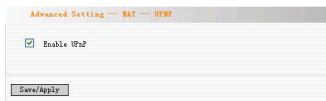
2. DMZ Host IP Address:
Entering the LAN IP address for the DMZ host.

Caution: Opening DMZ means to open all ports. In this case, your computer is totally exposed to the public network. Be cautious to use this function. Click "Save/Apply" to activate the settings.



5.2.3.4 UPNP

- 1) Click “UPNP” to display the window shown in the right figure. Enable UPnP: Check to Enable the UPnP (Universal Plug and Play) function. UPnP is a kind of architecture of common network connection between the computer and intelligent devices/instruments. It is especially common in the family application. Based on the Internet standards and technologies (such as TCP/IP, HTTP and XML), UPnP enables automatic connection and cooperation between such devices, thus to make more people can



access the network (especially the family network).

Click "Save/Apply" to activate the settings.

5.2.4 Security

5.2.4.1 IP Filtering

- 1) Click "Security" → "IP Filtering" to display the window shown in the right figure.

By default, all outgoing traffic is allowed. However, you can set IP filtering to restrict external network access by some computers in the internal network.



- 2) Click "Add" to display the window shown in the right figure.
- Filter Name: Setting the filtering name to facilitate identification.
 - Protocol: Selecting one from four available protocols: TCP/UDP; TCP; UDP; ICMP.
 - Source IP address: Entering the internal network IP address to be filtered.
 - Source Subnet Mask: Entering the subnet mask corresponding to the internal network IP address to be filtered.
 - Source Port: Entering the port number of the internal network IP

Add IP Filter - Outgoing

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

Filter Name:	<input type="text" value="tenda"/>
Protocol:	<input type="text" value="TCP/UDP"/>
Source IP address:	<input type="text" value="192.168.1.100"/>
Source Subnet Mask:	<input type="text" value="255.255.255.0"/>
Source Port (port or port port):	<input type="text" value="1500"/>
Destination IP address:	<input type="text" value="218.77.85.9"/>
Destination Subnet Mask:	<input type="text" value="255.255.0.0"/>
Destination Port (port or port port):	<input type="text" value="80"/>

<p>address to be filtered.</p> <p>f. Destination IP address: Entering the external network IP address to be filtered.</p> <p>g. Destination Subnet Mask: Entering the subnet mask corresponding to the external network IP address to be filtered.</p> <p>h. Destination Port: Entering the port number of the external network IP address to be filtered. Based on the above settings, you can add your filtering rules. You can select your WAN interface. However, it is recommended to keep the default setting unchanged.</p>	
--	--

3) Click "Save/Apply".

Security - Outgoing IP Filtering Setup

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **REJECTED** by setting up them.

Click on Add or Remove to configure outgoing IP filters.

Filter Name	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove
heals	TCP/UDP	192.168.1.100/255.255.255.0	1500	210.19.82.9/255.255.0.0	80	<input type="checkbox"/>

4) Click "Incoming" to display the window shown in the right figure.

By default, all incoming traffic is restricted. However, you can set IP filtering to allow internal network access by some external computers.

Security Incoming IP Filtering Setup

By default, all incoming IP traffic from the WAN is blocked when the firewall is enabled. However, some IP traffic can be **ACCEPTED** by setting up filters.

Click on Add or Remove to configure incoming IP filters.

Filter Name	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Remove
-------------	----------	-----------------------	-------------	----------------------	------------	--------

- 5) Click "Add" to display the window shown in the right figure.
- a. Filter Name: Setting the filtering name to facilitate identification.
- b. Protocol: Selecting one from four available protocols: TCP/UDP; TCP; UDP; ICMP.
- c. Source IP address: Entering the external network IP address to be filtered.
- d. Source Subnet Mask: Entering the subnet mask corresponding to the external network IP address to be filtered.
- e. Source Port: Entering the port number of the external network IP address to be filtered.

Add IP Filter -- Incoming

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

Filter Name:	tenda
Protocol:	TCP/UDP
Source IP address:	218.77.87.8
Source Subnet Mask:	255.255.0.0
Source Port (port or port port):	80
Destination IP address:	192.168.0.100
Destination Subnet Mask:	255.255.255.0
Destination Port (port or port port):	1500

WAN Interfaces (Configured in Routing mode and with firewall enabled only)
Select at least one or multiple WAN interfaces displayed below to apply this rule.

☒ Select All

☒ pppoe_8_35_1/ppp_8_35_1

Save/Apply

f. Destination IP address:
Entering the internal network IP address to be filtered.

h. Destination Subnet Mask: Entering the subnet mask corresponding to the internal network IP address to be filtered.

i. Destination Port:
Entering the port number of the internal network IP address to be filtered.

Based on the above settings, you can add your filtering rules.

You can select your WAN interface.

However, it is recommended to keep the default setting unchanged.

5) Click "Save/Apply".

Security > Incoming IP Filtering Setup

By default, all incoming IP traffic from the WAN is blocked when the firewall is enabled. However, some IP traffic can be **ALLOWED** by setting up filters.

Click on **Add** or **Remove** to configure incoming IP filters.

Filter Name	UT/PCI	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Action
Example	ALL	TCP/UDP	192.168.0.0 / 255.255.0.0	80	192.168.0.0 / 255.255.0.0	8080	<input type="checkbox"/>

Add Remove

5.2.4.2. Parent Control

1) Click "Time of Day Restriction" to display the window shown in the right figure.

Security > Time of Day Restriction > A window of restriction can be configured

Overview	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Action
<p>Add Remove</p>											

2) Click "Add" to display the window shown in the right figure. Here, you can set a specific period to restrict Internet access of a MAC address.

Time of Day Restriction

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

User Name:

☒ Browser's MAC Address:
☐ Other MAC Address: (xx:xx:xx:xx:xx:xx)

Days of the week: ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat ☐ Sun

Click to select: ☒ ☒ ☒ ☒ ☒ ☐ ☐

Start Blocking Time (hh:mm):

End Blocking Time (hh:mm):

Save/Apply

3) Click "Save/Apply".

Security -- Time of Day Restrictions -- X address is selected can be restricted

Interface	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Access
tenda	00:09:85:00:11:03	x	x	x	x	x			00:00	23:00	<input type="checkbox"/>

5.2.5 Routing

5.2.5.1 Default Gateway

- 1) Click "Routing" → "Default Gateway" to display the window shown in the right figure.

Enable Automatic Assigned Default Gateway:

You can check/uncheck this option. If you uncheck this option, you need to manually enter the default gateway address and WAN service. It is recommended to keep the default setting unchanged.

- 2) Click "Save/Apply".

Advanced Setting --> Routing --> Default Gateway

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

NOTE: If changing the Automatic Assigned Default Gateway from unselected to selected, You must reboot the router to get the automatic assigned default gateway.

☒ Enable Automatic Assigned Default Gateway

Save/Apply

5.2.5.2 Static Routing

- 1) Click “Static Route” to display the window shown in the right figure.

Here, you can add/delete the items of the static route.

Advanced Setting — Routing — Static Route

Routing — Static Route (A maximum 32 entries can be configured)

Destination	Subnet Mask	Gateway	Interface	Remove
-------------	-------------	---------	-----------	--------

Add Remove

- 1) Click “Add” to display the window shown in the right figure.

Destination Network Address: Entering the network or host for static route.

Subnet Mask: Entering the subnet mask corresponding to the network or host for static route.

Use Gateway IP Address:
Address: Entering the

Routing - Static Route Add

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

Destination Network Address: 192.168.0.1

Subnet Mask: 255.255.255.0

☒ Use Gateway IP Address 192.168.1.101

☒ Use Interface pppoe_8_35_1/ppp_8_35_1

Save/Apply

gateway address to be passed by the static route.

Use Interface:

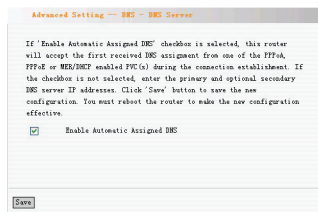
Selecting the interface corresponding to your connection mode.

Click "Save/Apply".

5.2.6. DNS

5.2.6.1 DNS Server

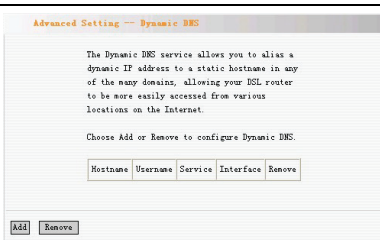
- 1) Click "DNS Server" to display the window shown in the right figure.
- 2) Enable Automatic Assigned DNS: After checking it, the DNS settings are activated. And the DHCP server of the router allocates the added DNS address to the



<p>client submitting the request.</p> <p>3) Primary DNS server: Entering the DNS address provided by the ISP.</p> <p>4) Secondary DNS server: If your ISP provides two DNS addresses, you can enter the other address here.</p>	
---	--

5.2.6.2 Dynamic DNS

- 1) Click "Dynamic DNS" to display the window shown in the right figure. Here, you can add/ delete the dynamic DNS settings. Dynamic DNS can make your applied domain name correspond to your IP address, so that the other users only need to remember your domain name for accessing your server.



- 2) Click "Add" to display the window shown in the right figure.

D-DNS provider:

Selecting a specific provider of dynamic DNS.

Hostname: Domain name applied by you.

Interface: Selecting one from two available interface modes.

Username: Your user name registered on the website of the dynamic DNS provider.

Password: Password corresponding to your user name registered on the website of the dynamic DNS provider.

The screenshot shows the 'Add dynamic DNS' configuration page. At the top, there is a title bar 'Add dynamic DNS'. Below it, a subtitle reads: 'This page allows you to add a Dynamic DNS address from DynDNS.org or TZO.' The form is divided into two main sections: 'D-DNS provider' and 'DynDNS Settings'. In the 'D-DNS provider' section, there is a dropdown menu currently set to 'DynDNS.org'. Below this are fields for 'Hostname' (containing 'tenda') and 'Interface' (a dropdown menu set to 'pppoe_8_35_1/ppp_8_35_1'). The 'DynDNS Settings' section contains fields for 'Username' (containing 'lyd') and 'Password' (masked with eight dots). At the bottom of the form is a 'Save/Apply' button.

Add dynamic DNS	
This page allows you to add a Dynamic DNS address from DynDNS.org or TZO.	
D-DNS provider	DynDNS.org ▼
Hostname	tenda
Interface	pppoe_8_35_1/ppp_8_35_1 ▼
DynDNS Settings	
Username	lyd
Password	●●●●●●●●
Save/Apply	

3) Click "Save/Apply".

Advanced Setting — Dynamic DNS

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your DSL router to be more easily accessed from various locations on the Internet.

Choose Add or Remove to configure Dynamic DNS.

Hostname	Username	Service	Interface	Remove
tenda	lyd	dyndns	ppp_8_35_1	<input type="checkbox"/>

5.2.7 DSL

Click “DSL” to display the window shown in the right figure. Here, you can enable a service as required. By default, the system checks the status of G.dmt, G.lite, T1.413, ADSL2, ADSL2+, AnnexL, Inner pair and Bitswap. The device can automatically negotiate with the upstream device.

The screenshot shows the 'Advanced Setting - DSL' window. It contains the following settings:

- Select the modulation below:
 - ☒ G.Dmt Enabled
 - ☒ G.lite Enabled
 - ☒ T1.413 Enabled
 - ☒ ADSL2 Enabled
 - ☒ AnnexL Enabled
 - ☒ ADSL2+ Enabled
 - ☐ AnnexM Enabled
- Select the modulation below:
 - ☒ Inner pair
 - ☐ Outer pair
- Capability:
 - ☒ Bitswap Enable
 - ☐ SRA Enable

At the bottom, there are two buttons: 'Save/Apply' and 'Advanced Settings'.

5.3 DHCP

- i. Click “DHCP Server” to display the window shown in the right figure.
1. You can click “Disable DHCP Server” or “Enable DHCP Server”.
2. Start IP Address: Start address of the DHCP server IP pool
3. End IP Address: End address of the DHCP server IP pool
4. Leased Time: Validity period of the IP address obtained. Click “Save”.

DHCP Settings - DHCP Server

☐ Disable DHCP Server
☒ Enable DHCP Server

Start IP Address: 192.168.1.100
End IP Address: 192.168.1.254
Leased Time (hours): one day

Save

Click “DHCP Client List” to view the list of the clients with allocated DHCP service.

DHCP Setting - DHCP Client List

DHCP Leases			
Hostname	MAC Address	IP Address	Expires In
DD	00:04:61:44:8C:24	192.168.1.100	23 hours, 59 minutes, 55 seconds

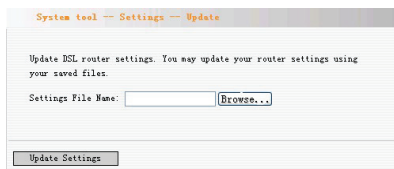
5.4 System Tool

5.4.1 Settings

1. Click "Backup" to display the window shown in the right figure. Here, you can back up the current settings of the router.



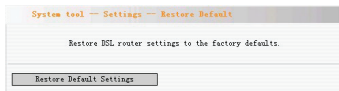
2. Click "Update" to display the window shown in the right figure. Here, you can restore the router settings from the backup file.



3. Click "Restore Default" to display the window shown in the right figure.

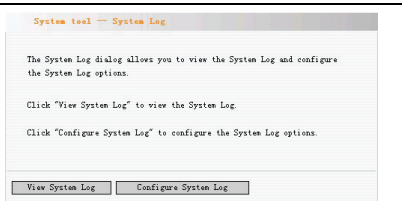
Click "Restore Default Settings" to restore the default settings before device delivery.

Caution: After restoring the default settings, you need to reboot the router to activate this modification.



5.4.2 System Log

1. Click "System Log" to display the window shown in the right figure.



2. Click "View System Log" to display the window shown in the right figure.



3. Click "Configure System Log" to display the window shown in the right figure.

- (1) Log: Enable; Disable
- (2) Log Level: Selecting the required level, Debugging by default.
- (3) Display Level: Error by default.
- (4) Mode: Local by default. If you select "Remote" or "Local/Remote", the system transmits the log UDP packets to your log server. Click "Save/Apply".

System Log -- Configuration

If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.

Select the desired values and click 'Save/Apply' to configure the system log options.

Log: ☐ Disable ☒ Enable

Log Level:

Display Level:

Mode:

5.4.3 Internet Time

1. Click "Internet Time" to display the window shown in the right figure. If you enable this function, the system can automatically obtain the time when accessing the Internet.

System tool — Internet Time

This page allows you to the router's time configuration.

☒ Automatically synchronize with Internet time servers

First NTP time server:

Second NTP time server:

Time zone offset:

5.4.4 Access Control

5.4.4.1 Service

- (1) Click "Access Control" to display the window shown in the right figure. You can enable or disable FTP/HTTP/ICMP/SNMP/SSH/TELNET/TFTP.
- (2) Click "Save/Apply" to activate the settings

System tool — Access Control — Services

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

Services	LAN	WAN
HTTP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable
ICMP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable
SNMP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable
TELNET	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable
TFTP	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Enable

Save/Apply

5.4.4.2 IP address

- (1) Click "IP Address" to display the window shown in the right figure. Here, you can add/delete items. Access Control Mode: Enable; Disable. When you enable it, the IP address allowed can access the management page.

System tool — Access Control — IP Address

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

Access Control Mode: ☒ Disable ☐ Enable

IP Address	Remove
------------	--------

Add Remove

- (2) Click "Add" to display the window shown in the right figure. You can enter an IP address, which is allowed by the system for access- ing the management page. Click "Save/Apply" to activate the settings.

Access Control — IP Address

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

IP Address:

Save/Apply

5.4.4.3 Password

- (1) Click "Password" to display the window shown in the right figure. Here, you can modify the password for logging in to the Management page. Enter the former login password, and then the new login password. If the former login password is correctly entered, you can click "Save/Apply" to successfully modify the login password.

Caution: For the sake of security, we highly recommend you to change the initial user name and password.

- (2) Click "Save/Apply" to activate the modification.

System tool — Access Control — Passwords

The user name "admin" has unrestricted access to change and view configuration of your DSL Router.

The user name "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics.

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

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

Access to your DSL router is controlled through three user accounts: admin, support, and user.

Username:

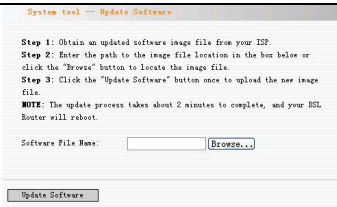
Old Password:

New Password:

Confirm Password:

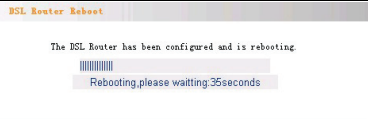
5.4.5 Software Update

1. Click "Update Software" to display the window shown in the right figure. Click "Browse" to select your update file, and then click "Update Software".



5.4.6 Save/Reboot

1. Click "Save/Reboot" to display the window shown in the right figure. Rebooting device can activate the changed settings. However, the ADSL connection is automatically interrupted before the reboot.



Chapter 6 Appendix

Appendix 1: Troubleshooting

Trouble Case	Troubleshooting
Power Indicator Off	<ul style="list-style-type: none">● Check if the power adapter is● Connected properly.● Check if the power adapter is matched.
ADSL Off	<ul style="list-style-type: none">● Check if the ADSL cable connection is OK.● Make sure the telephone line is OK you're your phone.● Check the phone line cabling is right.
LAN Off	<ul style="list-style-type: none">● Check the Ethernet cable is OK.● Make sure the PC's NIC indicator is ON.● Make sure the NIC works normally.

Can't access the Internet	<ul style="list-style-type: none">● Make sure the above troubles are clear.● Make sure the dial-up connection is established and set up.● Make sure the user name and password are right.● If the dial-up is OK, please make sure the IE proxy server is configured properly.● Please try opening multiple web pages
---------------------------	--

Appendix 2: FAQ

Q: What are VPI, VCI?

A: VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) are to identify ATM terminal (ADSL) for DSLAM, usually provided the local ISP.

Q: What related parameters are required from your ISP?

A: For dial user, Connection protocol, User name, Password, Value of VPI/VCI, Encapsulation mode and so on.

Q: The firmware upgrade fails and I can't enter the Web-based management interface?

A: Contact the technical engineer for support or after-sales service engineer.

Note: please download the upgrade packets from the Tenda website.

Q: Have completed all configurations, but can't dial through computer?

A: 1) Check the indicator of ADSL, it should be working in normally.

2) Check the accuracy of parameter of value of

VPI/VCI, Encapsulation mode and so on.

3) Make sure the dial-up connection is established.

4) You can check whether your ADSL Modem succeeds in connection through PING command.