



User Guide

QoS VPN Router

Shenzhen Tenda Technology Co., Ltd.

www.tendacn.com

Copyright Statement

© 2016 Shenzhen Tenda Technology Co., Ltd. All rights reserved.

Tenda is a registered trademark legally held by Shenzhen Tenda Technology Co., Ltd. Other brand and product names mentioned herein are trademarks or registered trademarks of their respective holders. Copyright of the whole product as integration, including its accessories and software, belongs to Shenzhen Tenda Technology Co., Ltd. No part of this publication can be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the prior written permission of Shenzhen Tenda Technology Co., Ltd.

Disclaimer

Pictures, images and product specifications herein are for references only. To improve internal design, operational function, and/or reliability, Tenda reserves the right to make changes to the products without obligation to notify any person or organization of such revisions or changes. Tenda does not assume any liability that may occur due to the use or application of the product described herein. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information and recommendations in this document do not constitute the warranty of any kind, express or implied.

Preface



Thank you for choosing Tenda! Please read this user guide before you start. This user guide instructs you to configure the product G3.

Conventions

Typographical conventions in this User Guide:

Item	Presentation	Example
Menu	『 』	The menu "Status" will be simplified as 『Status』 .
Continuous Menus	>	Go to 『System』 > 『Live Users』 .

Symbols in this User Guide:

Symbol	Meaning
 Note	This format is used to highlight information of importance or special interest. Ignoring this type of note may result in ineffective configurations, loss of data or damage to device.
 Tip	This format is used to highlight a procedure that will save time or resources.

For More Documents

For more documents, please go to our website <http://www.tendacn.com> and search for the appropriate product model to get the latest documents.

Technical Support

If you need more help, please contact us with any of the following ways. We will be glad to assist you as soon as possible.

Tenda website: <http://www.tendacn.com>

Global Hotline: (86) 755-27657180

United States Hotline: 1-800-570-5892

Technical Support: support@tenda.com.cn

HongKong Hotline: 00852-81931998

Canada Hotline: 1-888-998-8966

Email: support@tenda.com.cn

Website: <http://www.tendacn.com>

Skype: tendasz

Document Overview

The structure of the user guide is described as following:

Chapter	Content
1 Product Overview	About router appearance, packaging, functional characteristics, etc.
2 Device Installation	About router installation steps and installation notes.
3 Internet Access Setup	About steps for setting Internet access parameters of the router.
4 Device Management	About the router management page and the use of the functions in the page.
Appendix	About computer IP address settings, production specifications, FAQs, and declaration on toxic and harmful substances.

Table of Contents

Product Overview	- 1 -
1.1 Overview	- 2 -
1.2 Feature.....	- 2 -
1.3 Appearance.....	- 3 -
1.4 Package Contents	- 5 -
Device Installation	- 6 -
2.1 Installation Notes.....	- 7 -
2.2 Installing the Router	- 8 -
2.3 Connecting the Router.....	- 9 -
Internet Access Setup	- 11 -
Step 1: Log in to the router management page	- 12 -
Step 2: Set Internet access parameters.....	- 13 -
Device Management.....	- 17 -
4.1 Overview of Page.....	- 19 -
4.2 Network	- 20 -
4.3 Filter Management	- 32 -
4.4 Bandwidth Control.....	- 50 -
4.5 VPN	- 54 -
4.6 Security	- 72 -
4.7 AC Management	- 78 -
4.8 Captive Portal	- 83 -
4.9 PPPoE Authentication	- 92 -

Table of Contents

4.10 Virtual Server	- 104 -
4.11 USB.....	- 116 -
4.12 Maintenance.....	- 127 -
4.13 System status.....	- 140 -
Appendix	- 145 -
1 Obtain IP address autimatically	- 146 -
2 Product Specification	- 151 -
3 FAQs.....	- 152 -
4 Safety and emission statement	- 153 -



1

Product Overview

Overview

Main Features

Appearance

Package Contents

1.1 Overview

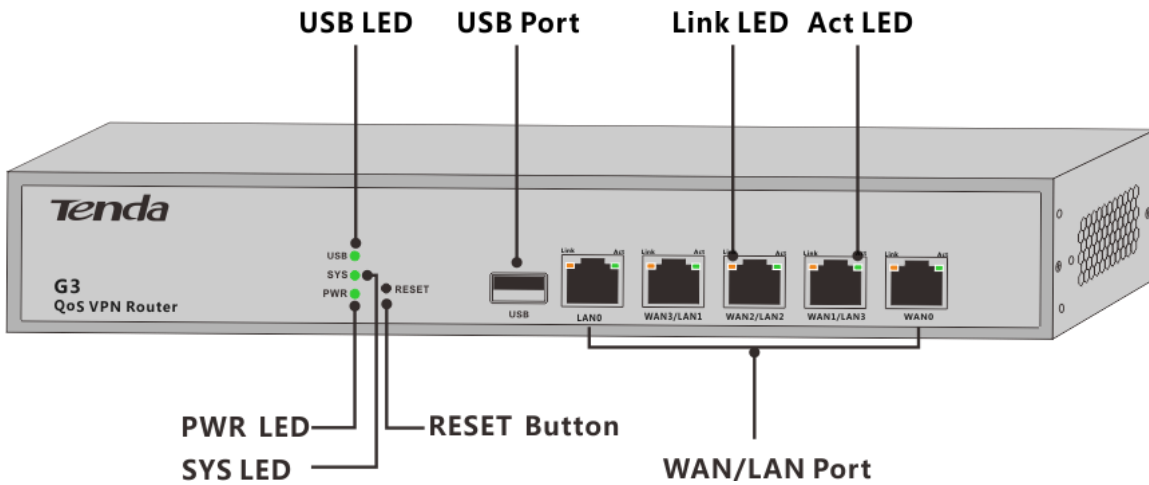
G3 are multi-WAN routers specially designed by Tenda for small and medium-sized enterprises and chain hotels. Use a high performance processor with a dominant frequency up to 800 MHz, support a maximum of 4 WAN ports, and integrate load balancing, flow control, and user authentication functions. Support IPSec/PPTP/L2TP VPN, a maximum of 15 concurrent tunnels. In addition, provide the AC management function to manage all models of APs of Tenda. G3 provides a 200-people standard device quantity and can manage up to 16 APs. Meet the requirements of enterprises and hotels for establishing an efficient, safe and manageable network.

1.2 Main Features

- Default 2 WAN ports and 3 LAN ports.
- Support multi-WAN policies to effectively prevent network congestion.
- Support intelligent bandwidth management to ensure rational use of network resources.
- Support PPTP/L2TP server and client modes. The server mode is mainly deployed in an enterprise's headquarters. The client mode is mainly deployed in an enterprise's branch.
- Support IPSec VPN service to ensure data integrity check, anti-data replay, and data encryption.
- Support AC function to manage APs in the network.
- Support the Captive Portal and PPPoE authentication functions that allow only legitimate users to have the right to Internet access.
- Rich website classification libraries and APP application libraries to effectively control the staff's Internet access behavior and improve the staff's work efficiency.
- Support USB print and file sharing to simply set the sharing of printers and file servers in an enterprise.
- Support software online upgrade.

1.3 Appearance

1.3.1 Front Panel

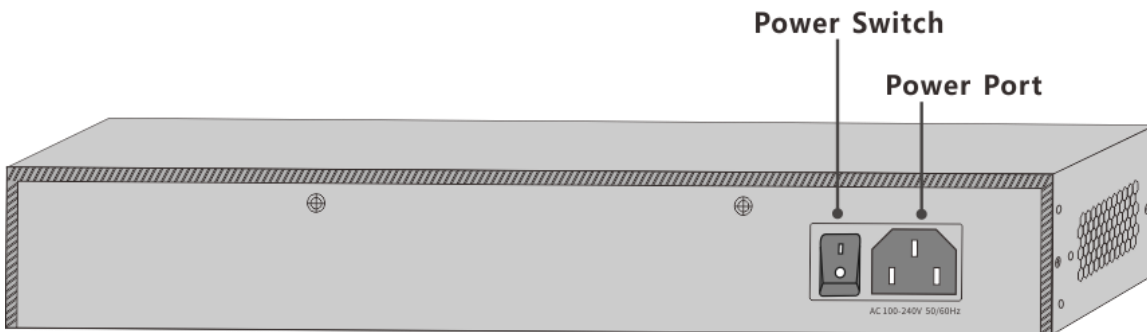


After the device is energized, the indicator states are described as follows:

Indicators	Color	Description
PWR	Green	<p>Solid indicates normal power-on.</p> <p>Off indicates abnormal power-on. Please check whether the power cord is loose.</p>
USB	Green	<p>Solid indicates that a USB device is connected.</p> <p>Blinking indicates that a USB device and this USB port have data transmission.</p> <p>Off indicates that no USB device is connected or connection is abnormal.</p>
SYS	Green	<p>Blinking indicates that the system operates normally.</p> <p>Solid or off indicates that the system fails.</p>
Link	Orange	<p>Solid indicates that a device is connected to the port.</p> <p>Off indicates that no device is connected to the port or connection is abnormal.</p>
Act	Green	<p>Solid indicates that there is no data transmission on the port.</p> <p>Blinking indicates that there is data transmission on the port.</p>

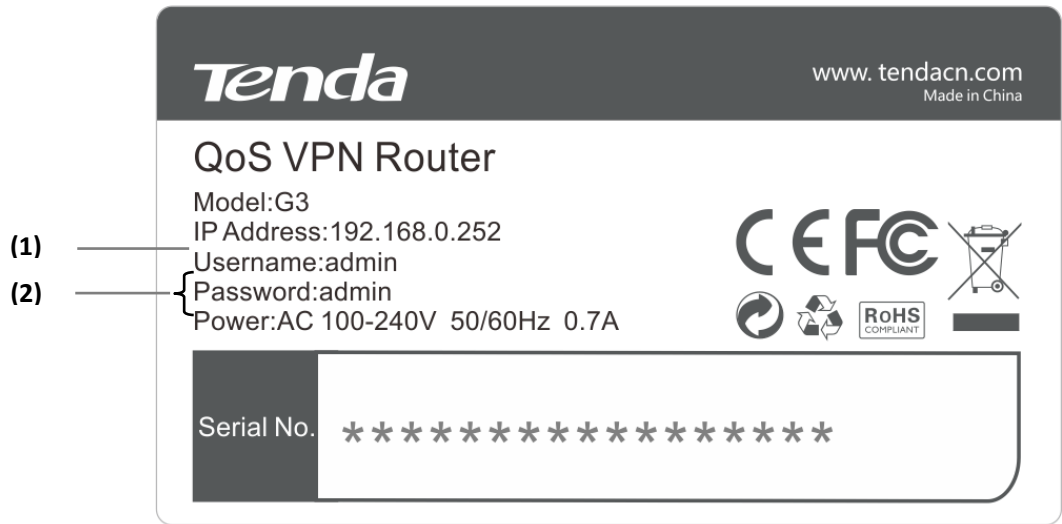
Port and Button	Description
RESET	In power-on state, press and hold the button with a spike for 8s and release it, and the device will be restored to factory state.
USB	USB3.0 Connects USB devices such as USB disks, mobile hard disks, and printers.
LAN0	Intranet port that connects devices such as switches and computers.
WAN3/LAN1, WAN2/LAN2, WAN1/LAN3	<p>Multiplexing for Intranet and Extranet ports.</p> <ul style="list-style-type: none"> WAN3/LAN1 and WAN2/LAN are Intranet (LAN) ports by default. WAN1/LAN3 is an Extranet (WAN) port by default. <p>The router enables 2 WAN ports by default. If you need to modify the number of WAN ports, please go to Network > Internet Setup and select the number of WAN ports.</p>
WAN0	Extranet port that connects Extranet cables. Extranet cables may be network cables from ADSL, fiber, and cable television cats, or broadband network cables directly provided by the broadband operator.

1.3.2 Rear Panel



- **Power port:** Connects the power cord. Please use the supporting power cord in the product packing box for connection.
- **Power switch:** After the power cord of the device is connected, press this button for power supply to the device.

1.3.3 Label at the Bottom

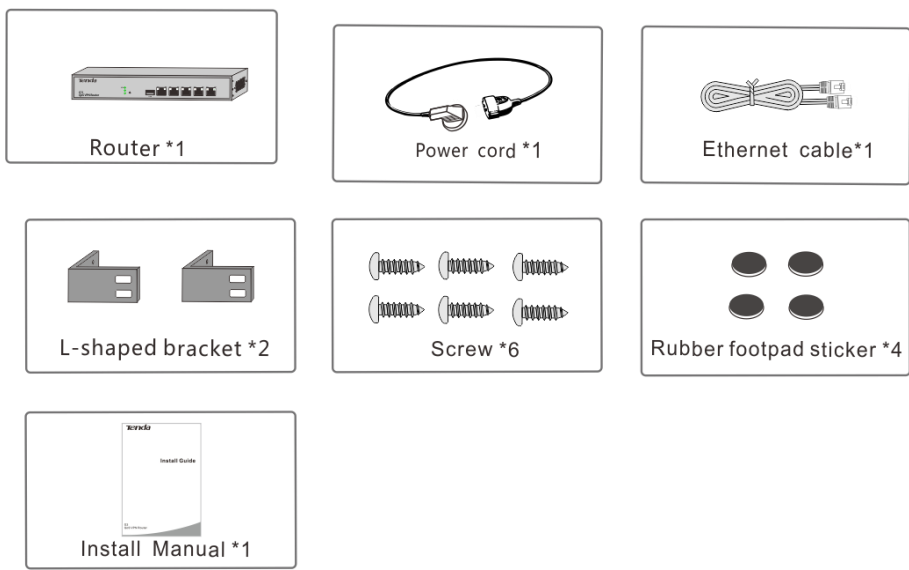


(1): The login IP address for router. This IP address can be used to go to the web login page of this router.

(2): Default login user name and password, it can be used to go to the web login page of this router.

1.4 Package Contents

Unpack the package. Your box should contain the following items:



If any item is incorrect, missing or damaged, please keep the original package and contact the vendor for replacement immediately.



2

Device Installation

Installation Notes

Installing the Router

Connecting the Router

2.1 Installation Notes

Follow the following notes to avoid device damage or personal injury due to improper use.

2.1.1 Safety Measures

- It is necessary to wear antistatic gloves in the installation process and the device must not be powered on.
- Use the power cord in the product packaging box for power supply to the device.
- Ensure that any input voltage range is consistent with the input voltage range indicated on the device.
- Ensure that the installation location of the device is well ventilated.
- Do not open or remove the device shell.
- Do not cut off the power supply when cleaning the device. Do not use any liquid to scrub the device.
- Keep the device away from power lines, electric lamps, power grids or any places where there is a potential risk of touching a strong-current power grid.



Note

A tamper protection seal is attached to one installation screw on the device shell. When maintaining the device, an agent must keep its seal intact. If you want to open the device shell, contact your local agent. Otherwise, you are held liable provided that the device cannot be maintained due to unauthorized action.

2.1.2 Environmental Requirements

Temperature and humidity requirements

Environment description	Temperature	Humidity
Operating environment	0°C ~ 40°C	10% - 90% RH (non-condensing)
Storage environment	-40°C ~ 70°C	5% - 90% RH (non-condensing)

Cleanliness requirement

To avoid any electrostatic effect on normal action of the device, pay attention to the following: Keep room air clean and regularly remove dust on the device. Perform correctly grounding of the device to ensure that static electricity is transferred smoothly.

Anti-lightning requirement

To avoid any damage to the device due to strong transient current generated from thunder and lightning, take the following lightning protection measures:

- Confirm that the power socket, rack, and worktable contact the ground well.
- The cabling shall be reasonable to avoid inducing lightning internally. When outdoor cabling is required, it is recommended to use the signal lightning arrester.

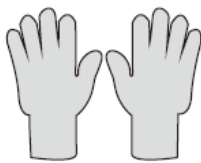
🔪 Requirements for the mounting table

Regardless of whether the device is installed in the rack or other work tables, pay attention to the following:

- Confirm that the rack or work table is stable and firm.
- Keep well ventilated. Leave 10 cm heat dissipation space around the device.
- Do not place any weight on the device.
- The vertical distance between devices shall not be smaller than 1.5 cm during rack installation.

2.1.3 Preparing Installation Tools

The following installation tools may be used in the device installation process. Please prepare them.



Antistatic gloves



Phillips screwdriver

2.2 Installing the Router

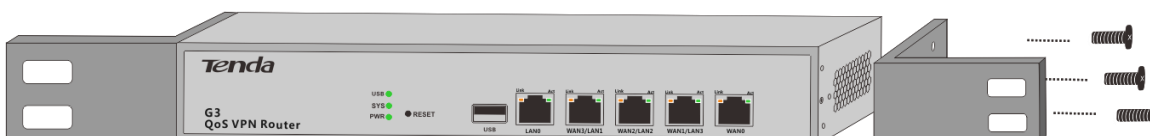
This device supports rack installation and tabletop installation. Please select a suitable installation mode according to your installation environment.

2.2.1 Rack Installation

The device is provided with L-shaped supports and screws and supports standard 19-inch rack installation.

Step 1: Ensure that the rack is stable and grounded.

Step 2: Fix two L-shaped supports on both sides of the device respectively with screws provided in the packaging box.



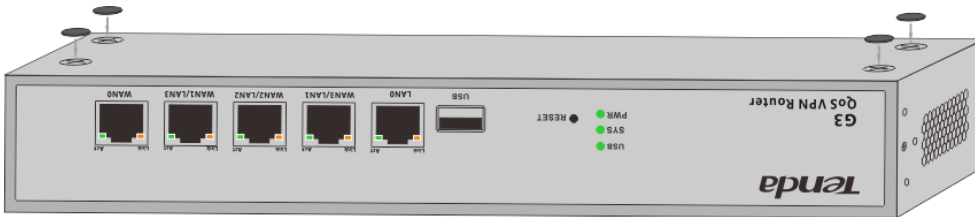
Step 3: Fix the device on the rack with screws (provided by the user).



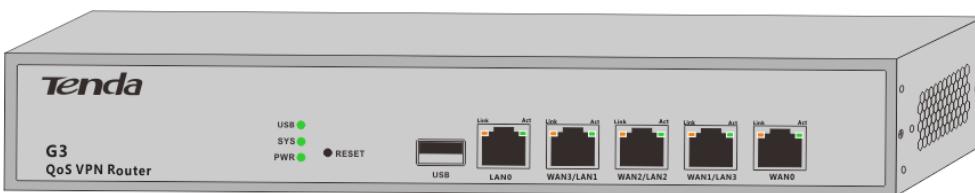
2.2.2 Tabletop Installation

If the user does not have a 19-inch standard cabinet, the tabletop installation mode can be used.

Step 1: Place the device on the tabletop with the bottom upward and paste 4 foot pads into the round groove at the bottom of the shell.



Step 2: Turn over the device so that it is placed on the tabletop with its front upward.

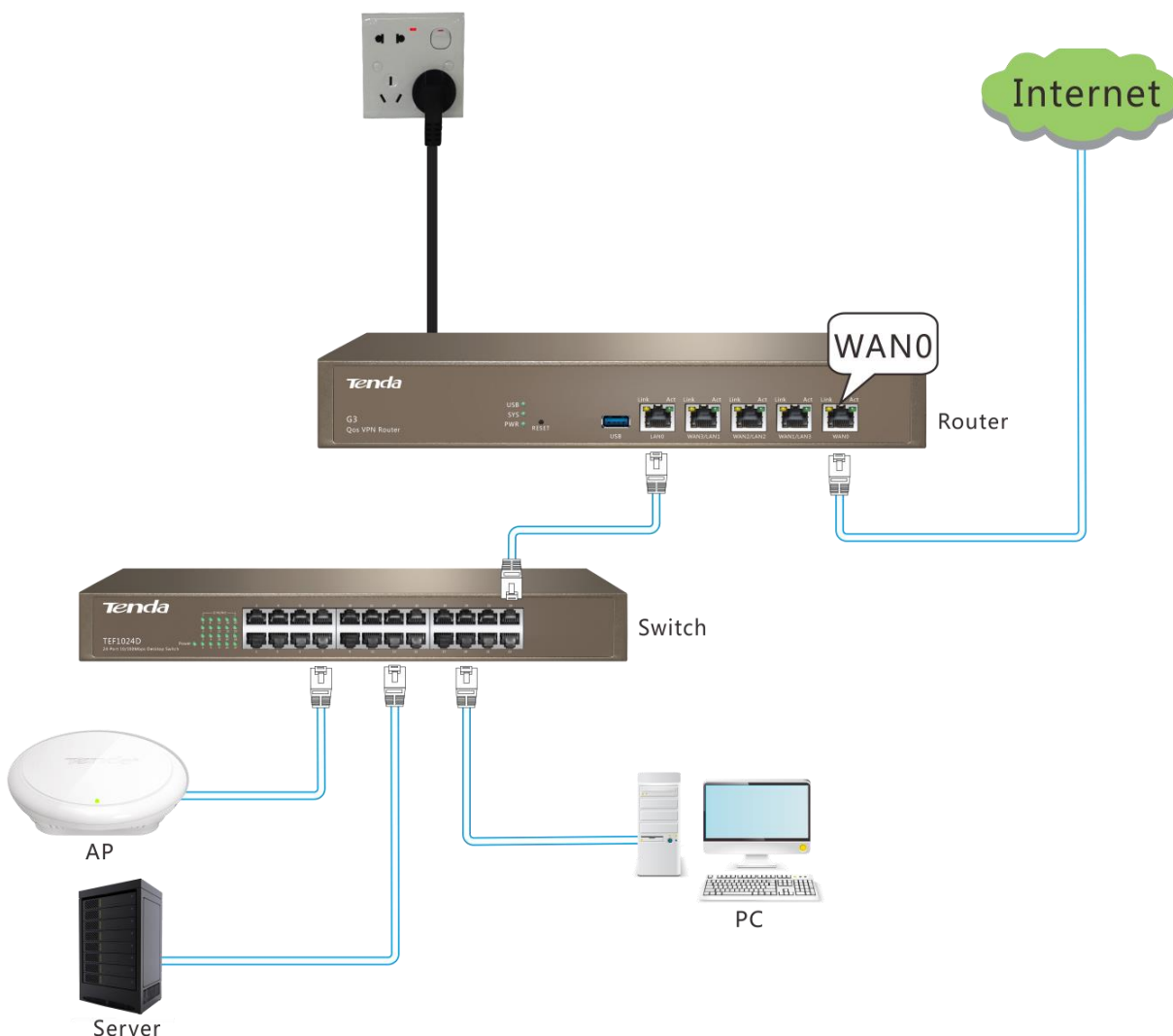


2.3 Connecting the Router

Step 1: Connect the Extranet cable to the WAN port of the device.



Step 2: Connect switches and other network devices (such as APs, servers, and computers) with network cables. After checking that the network topological graph is correct, connect the router to the power socket with the power cord in the product packaging box and press the power switch to power on the router.





3

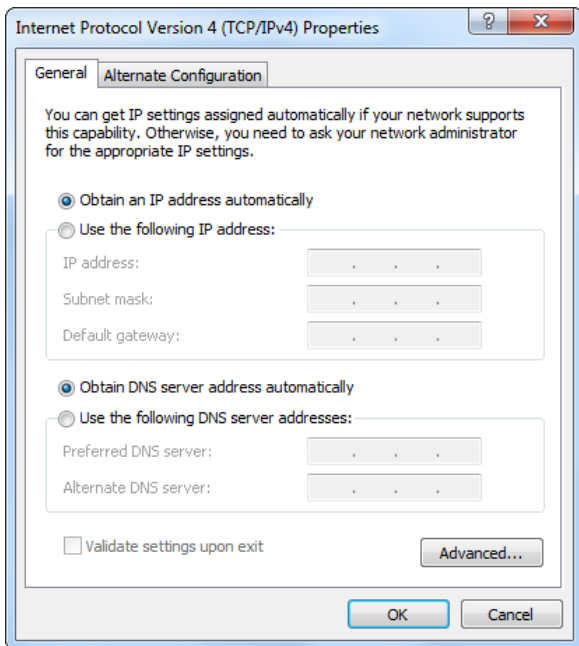
Internet Access Setup

Step 1: Log in to the router management page

Step 2: Set Internet access parameters

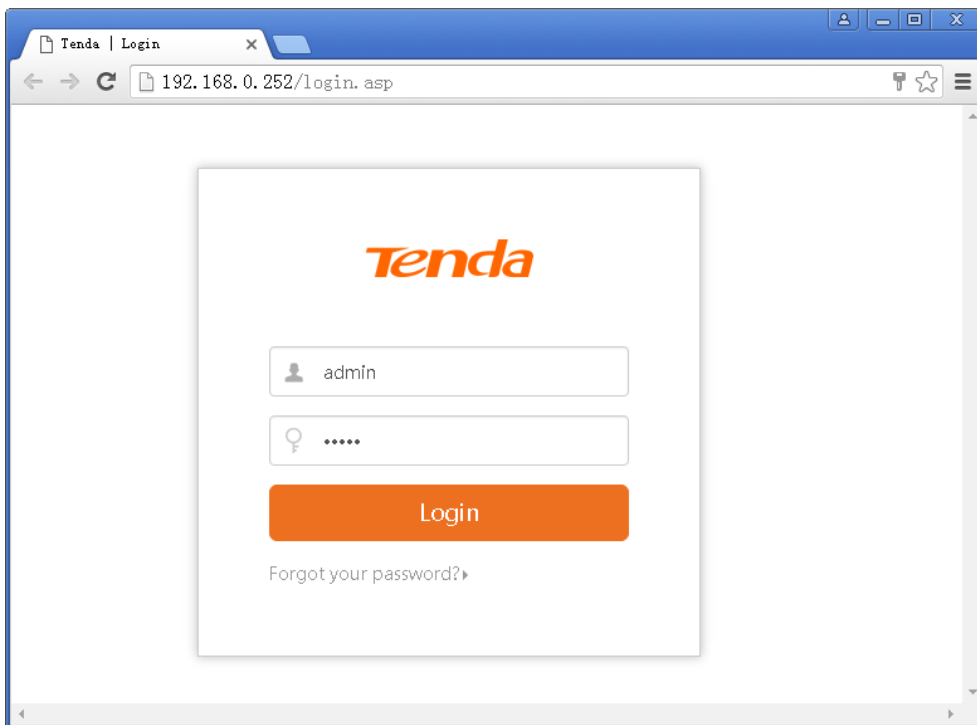
Step 1: Log in to the router management page

Step 1: Set the local connection of the computer to obtain an IP address automatically and Obtain DNS server address automatically. For detailed steps, refer to [1 Configure your computer](#).



Step 2: Open the browser on the computer, enter **192.168.0.252** in the address bar, and press **Enter** on the keyboard.

Step 3: Go to the web login page of the device. Enter the user name **admin** and password **admin**, and click **Login**.



 **Tip**

If you cannot log in to the router management page, refer to [Question 1](#) of **FAQs**.

You will successfully go to the web management page of the device.

Network

Internet Setup

WAN Parameters

LAN Setup

Port Mirroring

Static Route

Hotel Mode

Filter Management

Bandwidth Control

VPN

Security

AC Management

Captive Portal

PPPoE Authentication

Virtual Server

USB

Maintenance

System

Internet Setup ?

WAN ports: WAN ports: 2

WAN0

Connection Type: ADSL Dynamic IP Static IP

PPPoE Username:

PPPoE Password:

Link Speed: Uplink: Mbps Downlink: Mbps

Connection Status: No response from server

WAN1

Connection Type: ADSL Dynamic IP Static IP

Link Speed: Uplink: Mbps Downlink: Mbps

Connection Status: Disconnected

Step 2: Set Internet access parameters

Set Internet access information. Select one connection method from Methods 1, 2, and 3 according to actual situations. Try to surf the Internet after settings are finished.

Click 『Network』 to go to the **Internet Setup** page.



Tip

- This router provides 2 WAN ports by default. Take WAN0 settings as an example below. WAN1 port settings are consistent with WAN0 port settings.
- The default connection method of the router WAN0 is **ADSL**. The default connection method of WAN1 is **Dynamic IP**.
- All Internet access setting parameters are provided by the broadband operator. If you have any question, consult your broadband operator.
- If there is any prompt dialog box appearing in the setting process, take corresponding measures according to the contents of the prompt dialog box.

Method 1: There is a broadband user name and password provided by operators such as China Telecom and China Unicom. The connection method is ADSL. Perform settings by referring to the figure below.

Internet Setup

WAN ports: 2

LAN0 LAN1 LAN2 LAN Mode WAN1 WAN0 WAN Mode

WAN0

Connection Type: ADSL Dynamic IP Static IP

PPPoE Username: zhangsan

PPPoE Password:

Link Speed: Uplink: 10 Mbps Downlink: 2 Mbps

Connection Status: Connected

WAN1

Connection Type: ADSL Dynamic IP Static IP

Link Speed: Uplink: Mbps Downlink: Mbps

Connection Status: Disconnected

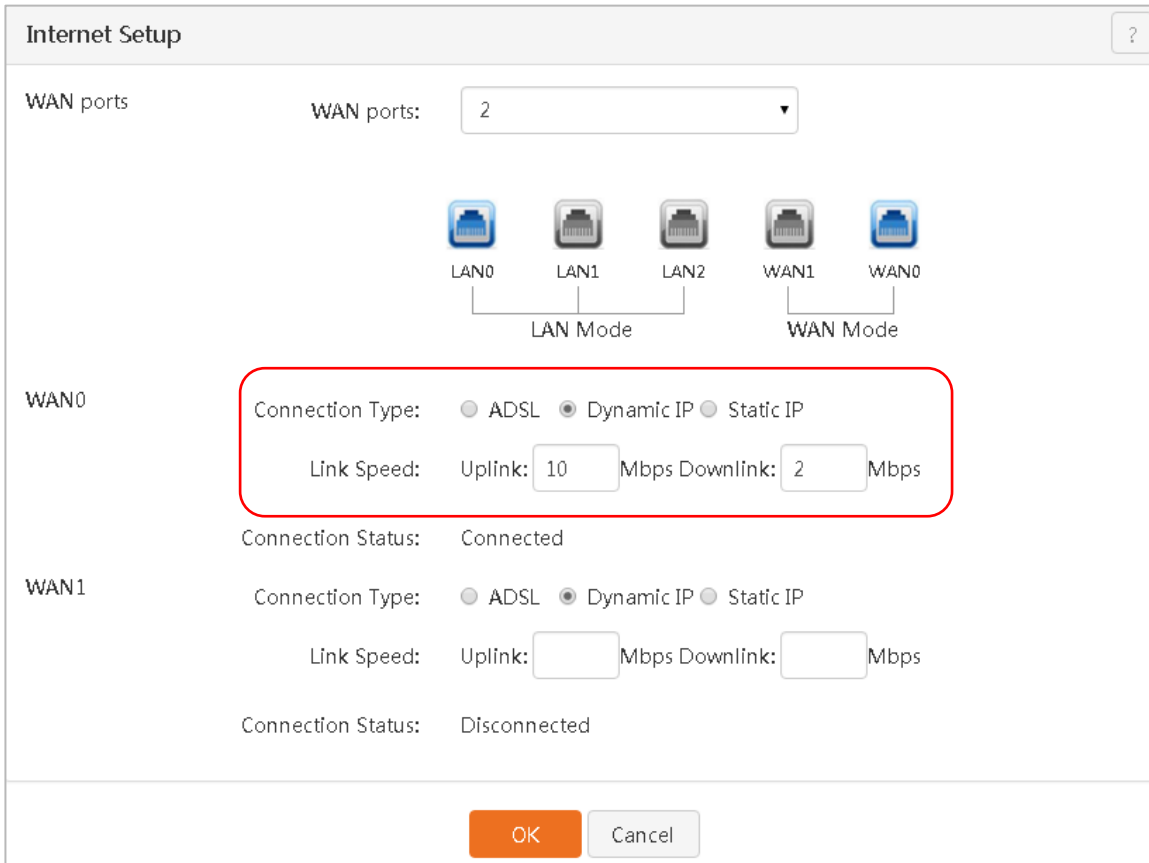
OK Cancel

Configuration steps:

- 1 Connection Type:** Click to select ADSL.
- 2 PPPoE Username/Password:** Enter the broadband user name and password information provided by operators such as China Telecom and China Unicom.
- 3 Operator:** Select an operator that handles the broadband.
- 4 Line Bandwidth:** Enter the size of broadband.
- 5** Click **OK** to finish settings.

Wait a moment. When **Connection Status** is displayed as **Connected**, you can try to surf the Internet.

Method 2: For users whose computers need only to be connected with a broadband network cable for Internet access when the router is not used, the connection method is Dynamic IP. Perform settings by referring to the figure below.



Configuration steps:

- 1 **Connection Type:** Click to select Dynamic IP.
- 2 **Operator:** Select an operator that handles the broadband.
- 3 **Line Bandwidth:** Enter the size of broadband.
- 4 Click **OK** to finish settings.

Wait a moment. When **Connection Status** is displayed as **Connected**, you can try to surf the Internet.

Method 3: For users who have fixed IP addresses provided by operators for Internet access, the connection method is Static IP. Perform settings by referring to the figure below.

The screenshot shows the 'Internet Setup' window. At the top, 'WAN ports' is set to 2. Below this, a diagram shows LAN ports (LAN0, LAN1, LAN2) grouped under 'LAN Mode' and WAN ports (WAN1, WAN0) grouped under 'WAN Mode'. The 'WAN0' section is highlighted with a red rounded rectangle. It shows 'Connection Type' set to 'Static IP' (selected with a radio button). Below this are input fields for 'IP Address', 'Subnet Mask', 'Default Gateway', 'Preferred DNS', and 'Alternate DNS'. At the bottom of the highlighted area are 'Link Speed' fields for 'Uplink' and 'Downlink' in Mbps. Below the highlighted area, 'WAN1' is shown with 'Connection Type' set to 'Dynamic IP' and 'Connection Status' as 'Disconnected'. At the bottom of the window are 'OK' and 'Cancel' buttons.

Configuration steps:

- 1 **Connection Type:** Click to select Static IP.
- 2 **IP Address, Subnet Mask, Default Gateway, and Preferred/Alternate DNS:** Enter fixed IP address information provided by the broadband operator.
- 3 **Operator:** Select an operator that handles the broadband.
- 4 **Line Bandwidth:** Enter the size of broadband.
- 5 Click **OK** to finish settings.

Wait a moment. When Connection Status is displayed as Connected, you can try to surf the Internet.



4

Device Management

Overview of Page

Network

Filter Management

Bandwidth Control

VPN

Security

AC Management

Captive Portal

PPPoE Authentication

Virtual Server

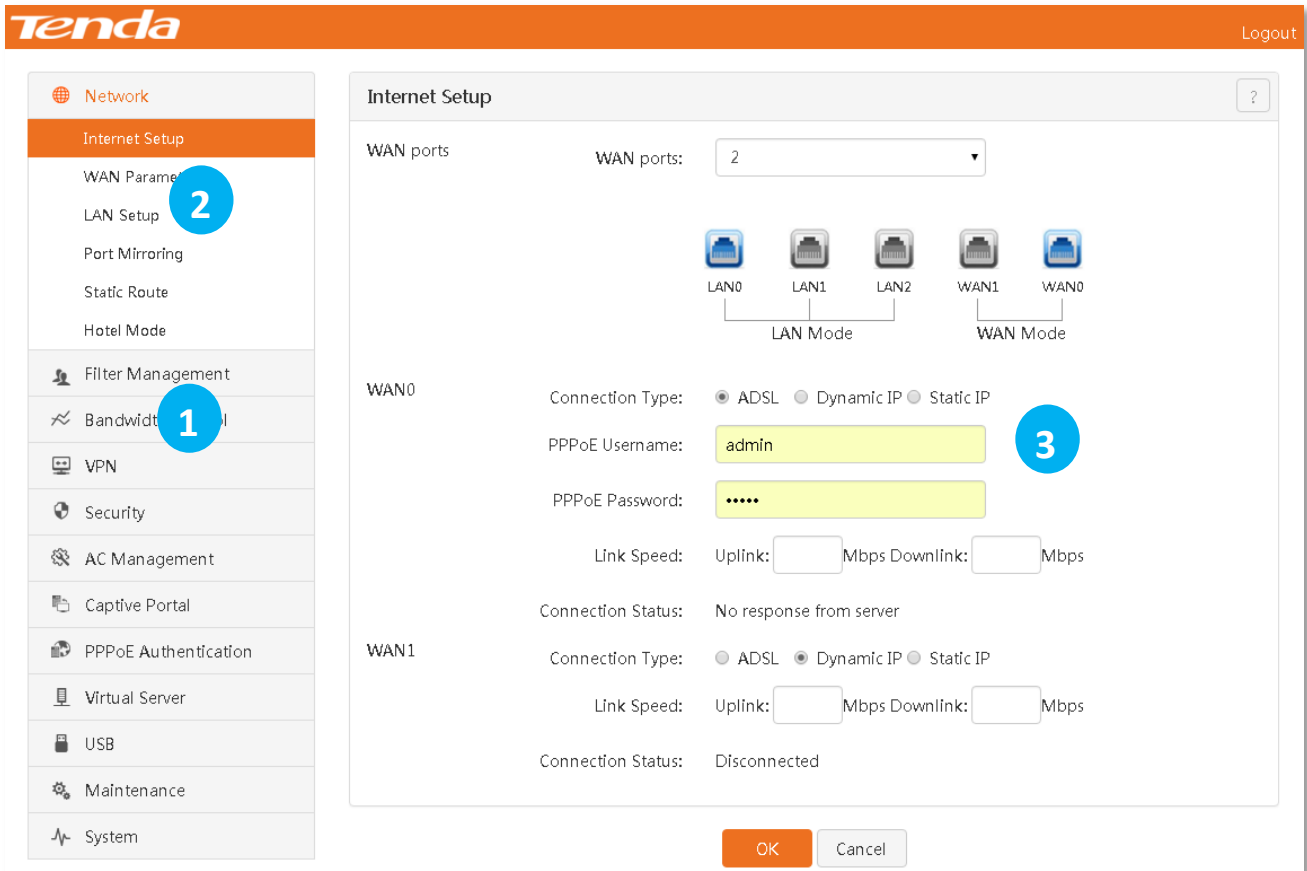
USB

Maintenance

System

4.1 Overview of Page

Go to the management page of the router. The web management page is divided into three parts: primary navigation bar, secondary navigation bar and configuration area, described as follows.



S/N	Name	Description
1	Primary Navigation bar	The navigation bar organizes the router's menu of all functions in the form of a navigation tree. You can choose the function menu from the navigation bar with selection result shown in the Secondary area.
2	Secondary Navigation bar	The navigation bar organizes the router's menu of all functions in the form of a navigation tree. You can choose the function menu from the navigation bar with selection result shown in the configuration area.
3	Configuration area	The area for users to configure and view.

Commonly used buttons and links

S/N	Name	Description
	OK	Click the button to apply your settings.
	Cancel	Click the button to cancel or clear the settings you are editing.
	Logout	Click this link to back to the router login page.

4.2 Network

Network includes the following contents:

[Internet Setup](#): Set router Internet access information.

[WAN Parameters](#): Modify WAN port parameters including WAN Speed, MTU, and MAC Address.

[LAN Setup](#): Modify relevant parameters of LAN IP and DHCP server.

[Port Mirroring](#): Set the router port mirroring function.

[Static Route](#): View router route forwarding information and configure static routing.

[Hotel Mode](#): Enable/Disable the router hotel mode. It is generally used for hotels. It allows you to set any IP address for clients in the router to surf the Internet.

4.2.1 Internet Setup

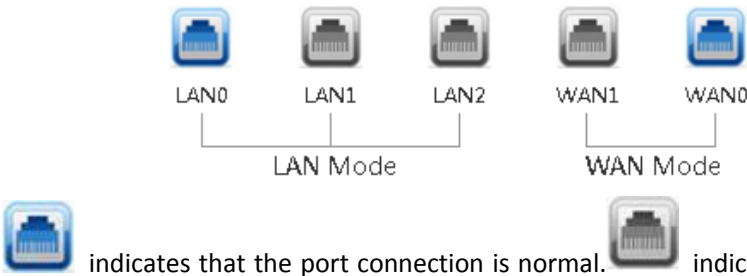


After setting Internet access parameters and logging in to the router web page, you will automatically log in to the Internet setup page. You can also click 『Network』 to go to the Internet Setup page. For detailed configuration steps, refer to [Step 2: Set Internet access parameters](#).

The screenshot displays the Tenda router's web interface for Internet Setup. The top navigation bar includes the Tenda logo and a 'Logout' link. A sidebar on the left lists various network management options, with 'Internet Setup' currently selected. The main content area is titled 'Internet Setup' and contains the following configuration details:

- WAN ports:** A dropdown menu is set to '2'.
- Port Diagram:** A visual representation shows LAN ports (LAN0, LAN1, LAN2) grouped under 'LAN Mode' and WAN ports (WAN1, WAN0) grouped under 'WAN Mode'.
- WAN0 Configuration:**
 - Connection Type: ADSL Dynamic IP Static IP
 - PPPoE Username:
 - PPPoE Password:
 - Link Speed: Uplink: Mbps Downlink: Mbps
 - Connection Status: No response from server
- WAN1 Configuration:**
 - Connection Type: ADSL Dynamic IP Static IP
 - Link Speed: Uplink: Mbps Downlink: Mbps
 - Connection Status: Disconnected

At the bottom of the configuration area, there are 'OK' and 'Cancel' buttons.

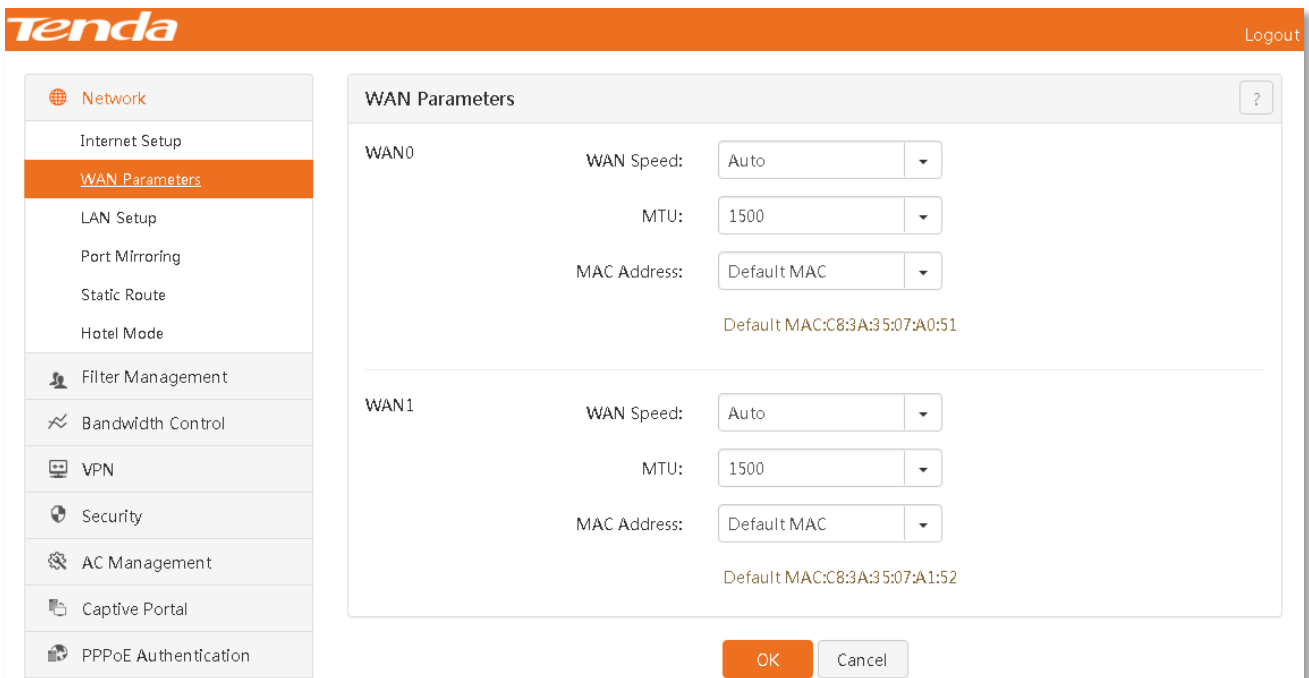
Parameter description in the page:

Parameter	Description
WAN ports	<p>Set the number of WAN ports and view RJ45 port status (connection status. The role is WAN or LAN port). The device enables 2 WAN ports by default. After the number of WAN ports is modified, the RJ45 port status diagram will also be changed as follows:</p> <p>WAN ports: <input type="text" value="2"/></p>  <p>The diagram shows five RJ45 port icons. LAN0, LAN1, and LAN2 are grouped under 'LAN Mode'. LAN0 has a blue icon, while LAN1 and LAN2 have grey icons. WAN1 and WAN0 are grouped under 'WAN Mode'. WAN1 has a grey icon, while WAN0 has a blue icon. Below the diagram, a legend shows a blue icon indicating normal connection and a grey icon indicating no device or abnormal connection.</p> <p> indicates that the port connection is normal.  indicates that no device is connected to the port or connection is abnormal.</p>
Connection Type	<p>Router connection method. Three connection methods are described as follows:</p> <ul style="list-style-type: none"> • ADSL: Broadband operators such as China Telecom and China Unicom provide a PPPoE username and password. When surfing the Internet without using the router, you need to perform dial-up access on the computer. • Dynamic IP: Broadband operators such as China Telecom and China Unicom do not provide any Internet access information. When surfing the Internet without using the router, you can surf the Internet by connecting the computer with a broadband network cable. • Static IP: Broadband operators such as China Telecom and China Unicom a fixed IP address. When surfing the Internet without using the router, you need to set a static IP address on the computer for Internet access.
PPPoE Username and PPPoE Password	Valid when the connection method is ADSL. Consult your broadband operator.
IP Address, Subnet Mask, Default Gateway, and Preferred/Alternate DNS	Valid when the connection method is Static IP. Consult your broadband operator.

Parameter	Description
Line Bandwidth	<p>Handle the size of bandwidth. Consult a corresponding broadband operator.</p> <p>Note</p> <p>If this item is empty, it will affect the "Intelligent Bandwidth Control" and "Smart Load Balancing" functions. Please fill in it.</p>
Connection Status	<p>Display the connection status of a WAN port. The states mainly include:</p> <ul style="list-style-type: none"> Connected or authenticated: The router has been successfully connected to the Internet. Connecting...: The router is being connected to the Internet. Disconnected: Disconnection or connection failure. Please check Internet access information or consult a corresponding broadband operator. <p>If other status information is displayed, take corresponding measures according to the prompt message about connection status.</p>

4.2.2 WAN Parameters

If you cannot access the Internet after performing Internet setup, you can solve this problem by modifying WAN parameters. Click 『Network』 > 『WAN Parameters』 to go to the configuration page.



Configuration steps for MAC address clone:

- 1 MAC Address:** Click the dropdown list and select Clone Local MAC or Manual Input. Enter a MAC address to be cloned in the MAC input box when selecting Manual Input MAC.
- 2** Click **OK**.

**Tip**

Please use a correct MAC address to perform the clone action! A correct MAC address is a MAC address of a computer on which a technician performs commissioning to surf the Internet during broadband installation.

Parameter description in the page:

Parameter	Description
WAN Speed	Router WAN port speed. The default is Auto. Do not change it unless necessary.
MTU	Maximum transmission unit. It is the maximum packet transmitted in the network device. It is recommended to maintain the default setting.
Mac Address	<p>MAC address of the WAN port. If the router cannot be connected to the Internet after perform "Internet Setup", the reason may be that the broadband operator binds Internet access information to a MAC address. At this point, perform MAC address clone and try to surf the Internet.</p> <ul style="list-style-type: none"> • Current MAC: Current MAC address of the router's WAN port. • Default MAC: Set the MAC address of the router WAN port to the factory default. • Clone Local MAC: Clone the MAC address of the computer that logs in to the router to the router's WAN port. • Manual Input: Manual enter a MAC address to be cloned to the router WAN port.

4.2.3 LAN Setup

This section describes how to set the IP address and DHCP server parameters of the router LAN port. Click 『Network』 > 『LAN Setup』 to go to the configuration page.

The LAN port IP address is a management IP address of the router.

The DHCP server can automatically assign Internet access information such as IP address, subnet mask, gateway, and DNS to clients that are successfully connected to the router. If this function is turned off, you can surf the Internet only by manually configuring IP address information on the client. Keep the DHCP server enabled in the absence of exceptional circumstances.

Configuration steps for modifying a LAN port IP address:

- 1 **LAN IP:** Modify an IP address such as 192.168.10.1.
- 2 Click **OK**.

After clicking **OK**, wait a moment. After the progress bar is over, if login fails, ensure that the method for obtaining a computer IP address is **Obtain an IP address automatically**. Repair a computer IP address. Retry using a new IP address.

Steps for setting DHCP server parameters:

- 1 **DHCP Server:** Click Enable.
- 2 **Start /End IP:** Set the last bit of start and end IP addresses that are automatically assigned to the client by the DHCP server.
- 3 Click **OK**.



Tip

1. The router enables the DHCP server function by default. After this function is disabled, you must manually set IP address information for every client under the router.
2. If there is no professional advice, maintain the default settings of the DHCP server to avoid any effect on normal Internet access.

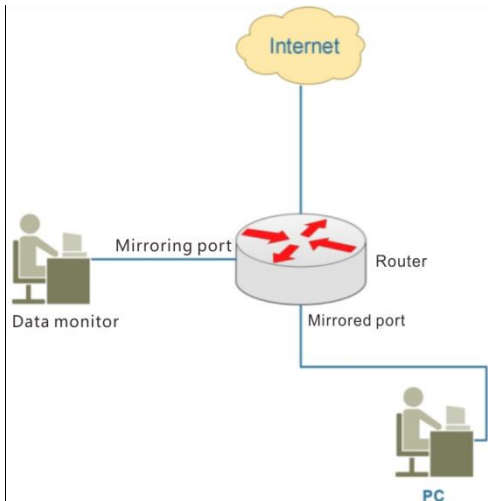
4.2.4 Port Mirroring

Overview

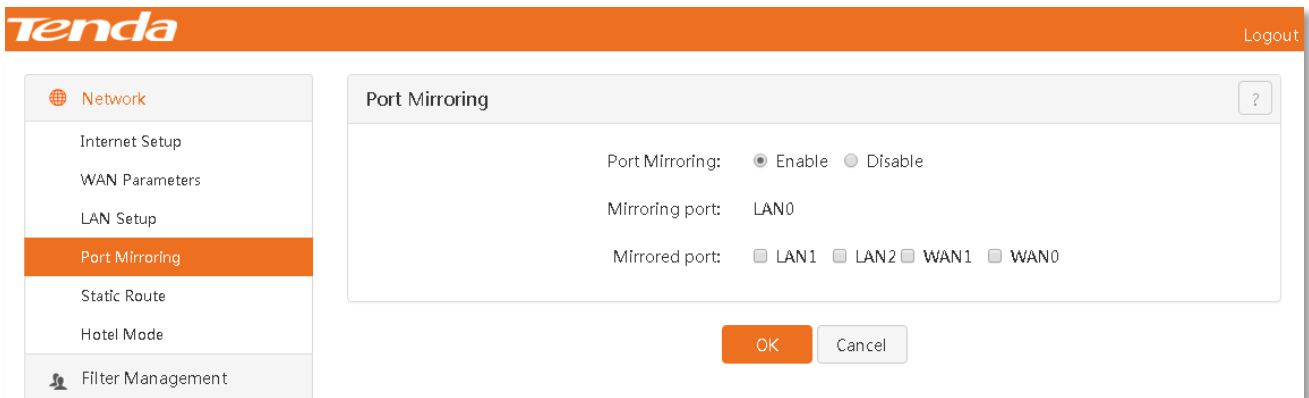
Port mirroring is to copy packets of one or more ports to one monitoring port of the device. The network

administrator may perform network monitoring and troubleshooting using these detected data.

Topological graph for port mirroring:



This device supports monitoring communication of other ports (mirrored ports) through the LAN0 port (mirroring port). Click 『Network』>『Port Mirroring』 to go to the configuration page. The port mirroring function is disabled by default.



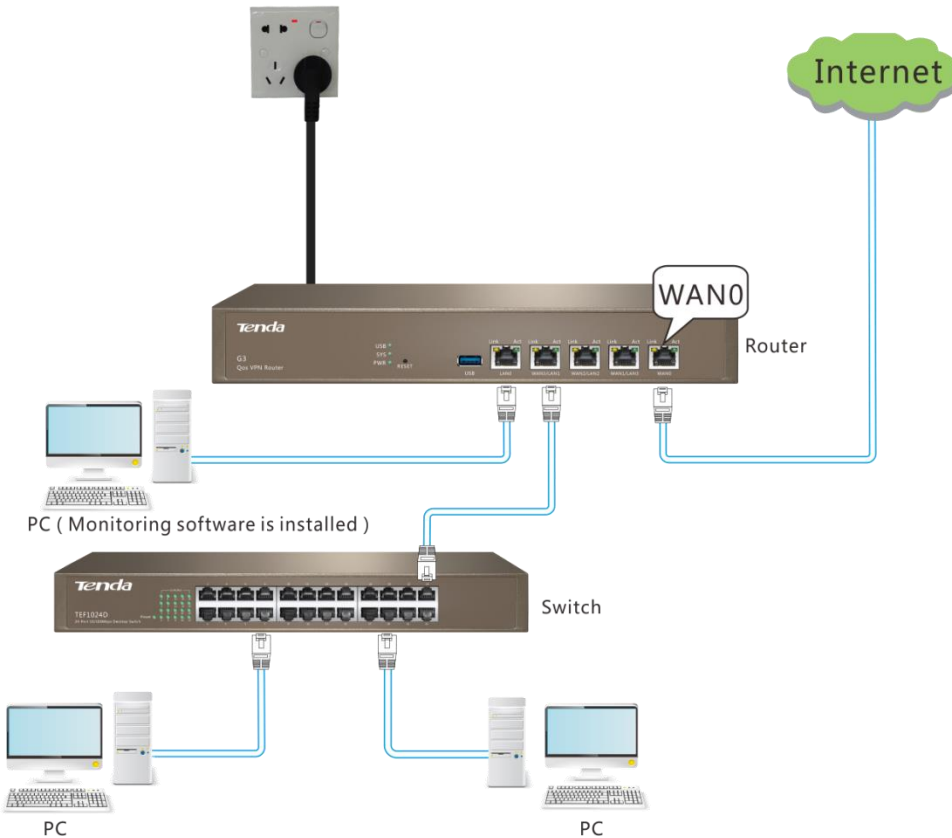
Parameter description in the page:

Parameter	Description
Port Mirroring	Enable/Disable the port mirroring function. The default is Disable.
Mirroring port	Monitoring port. Clients under this port must be installed with monitoring software. The default is LAN0 and cannot be changed.
Mirrored port	Mirrored port. After the port mirroring function is enabled, packets of a mirrored port will be automatically copied to the a mirroring port.

Example of port mirroring

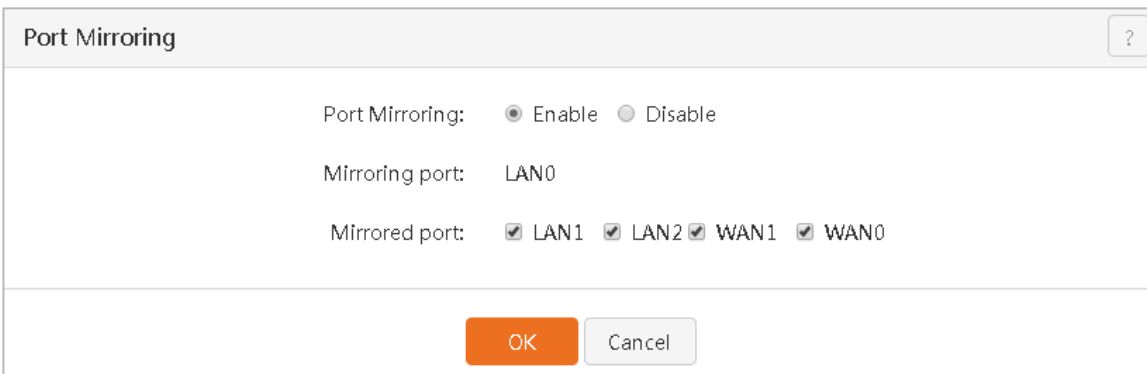
- Example:** An enterprise purchases a G3 enterprise router to establish a network. Recently, the network in the company is abnormal so that Internet access often fails. The port mirroring function can be used to capture WAN and LAN port data for analysis. Monitoring software is installed on the computer under LAN0. Other ports are set to mirrored ports.

The reference application scenario is as follows:



Configuration steps:

- 1 **Port Mirroring:** Click Enable.
- 2 **Mirrored port:** Click to select monitored ports such as LAN1, LAN2, WAN1, and WAN0.
- 3 Click **OK**.



After settings are finished, the computer installed with monitoring software (connected to the LAN0 port of the router) can monitor packets of other ports.

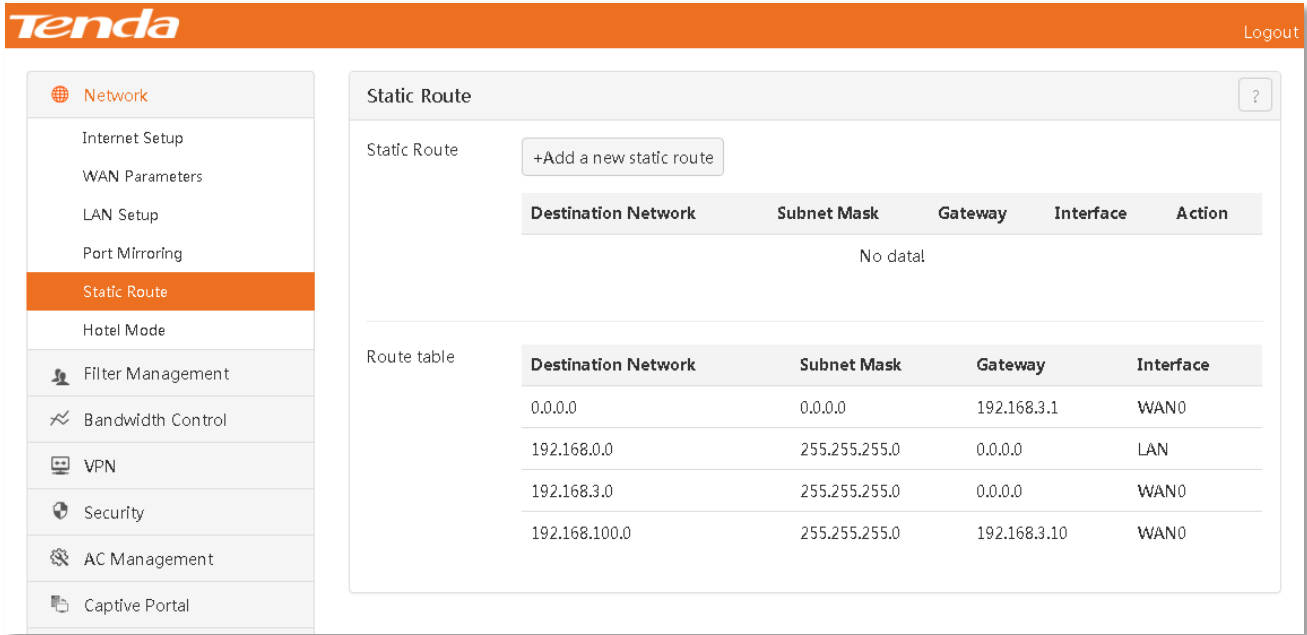
4.2.5 Static Route

Overview

Routing is a behavior to select one optimal path to transmit data from a source address to a destination address. Static route is a special route manually configured. It is characterized by simpleness, high efficiency, and reliability. A suitable static route may reduce route selection problems and the overload of route selection data stream and

increase the packet forwarding speed.

Click 『Network』 > 『Static Route』 to go to the configuration page.



Parameter description in the page:

Parameter	Description
Static Route	Manually add a static route.
Route table	Current route table information of the router, including default routes and added static routes.
Destination Network	Destination network address, i.e. IP address where packets reach.
Subnet Mask	Subnet mask of a destination network address.
Gateway	Entry IP address of the next-hop route after packets leave from a router port.
Interface	Port where packets leave from the router. Select a corresponding WAN port as needed.

Example of static route

- Example:** An enterprise purchases a G3 enterprise router to establish a network. The Intranet and Internet are located in different networks. The router has been connected to the Internet through the WAN0 port and to the Intranet through the WAN1 port. Now, it must be realized that the client under the router needs to access both the Internet and Intranet. This can be by achieved by setting a static route on the router.

Assume that basic information is as follows:

Intranet information assigned by the company:

IP Address	192.168.58.190	Gateway	192.168.58.1
Subnet mask	255.255.255.0	Master DNS	192.168.58.1

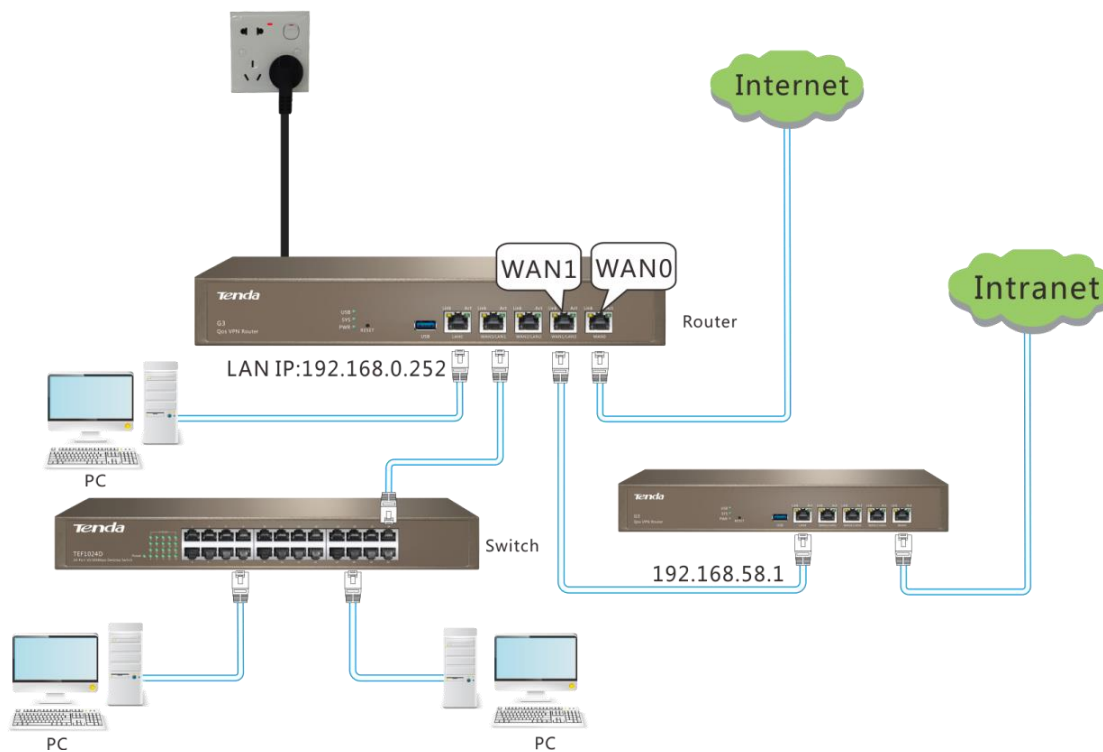
Internet access information assigned by the company:

Username	tenda
Password	tenda

Intranet server information is as follows:

IP Address	172.16.0.0
Subnet mask	255.255.0.0

The reference topological graph is as follows:



Configuration steps:

Step 1: Set a WAN port according to information assigned by the company (The Internet is connected to the WAN0 port. The Intranet is connected to the WAN1port), as shown in the figure below. For detailed configuration steps, refer to [Step 2: Set Internet access parameters.](#)

Internet Setup ?

WAN ports: WAN ports:

LAN0 LAN1 LAN2 WAN1 WAN0

LAN Mode WAN Mode

WAN0

Connection Type: ADSL Dynamic IP Static IP

PPPoE Username:

PPPoE Password:

Link Speed: Uplink: Mbps Downlink: Mbps

Connection Status: Connected

WAN1

Connection Type: ADSL Dynamic IP Static IP

IP Address:

Subnet Mask:

Default Gateway:

Preferred DNS:

Alternate DNS:

Link Speed: Uplink: Mbps Downlink: Mbps

Connection Status: Connected

Step 2: Set static router rules.

- 1 Click +Add a new static route.

Static Route ?

Static Route +Add a new static route

Destination Network	Subnet Mask	Gateway	Interface	Action
No data!				

- 2 Set static router rules.

- **Destination Network/ Subnet Mask:** Enter a destination network address and subnet mask.
- **Gateway:** Enter a gateway address to the Intranet.
- **Interface:** Select a router port that a destination network is connected to.
- Click **OK**.

Add a new static route ×

Destination Network:

Subnet Mask:

Gateway:

Interface: WAN0 WAN1

After settings are finished, newly added static router rules will be displayed in the route table.

Static Route ?

Static Route +Add a new static route

Destination Network	Subnet Mask	Gateway	Interface	Action
172.16.0.0	255.255.0.0	192.168.58.1	WAN1	

Route table

Destination Network	Subnet Mask	Gateway	Interface
0.0.0.0	0.0.0.0	192.168.3.1	WAN0
172.16.20.0	255.255.255.0	0.0.0.0	WAN1
192.168.0.0	255.255.255.0	0.0.0.0	LAN
192.168.3.0	255.255.255.0	0.0.0.0	WAN0
172.16.0.0	255.255.0.0	192.168.58.1	WAN1

4.2.6 Hotel Mode

The client under the router can generally surf the Internet by obtaining an IP address automatically or by manually setting correct IP address, gateway and DNS information. However, a hotel generally has a great flow of people. The configurations of computer network cards of many customers are different. Some computers obtain an IP address automatically. Some computers have an IP address that has been statically set. In addition, many customers do not know how to configure a computer network card. In this case, hotel personnel must help them to perform configurations and customers will also think that this is inconvenient.

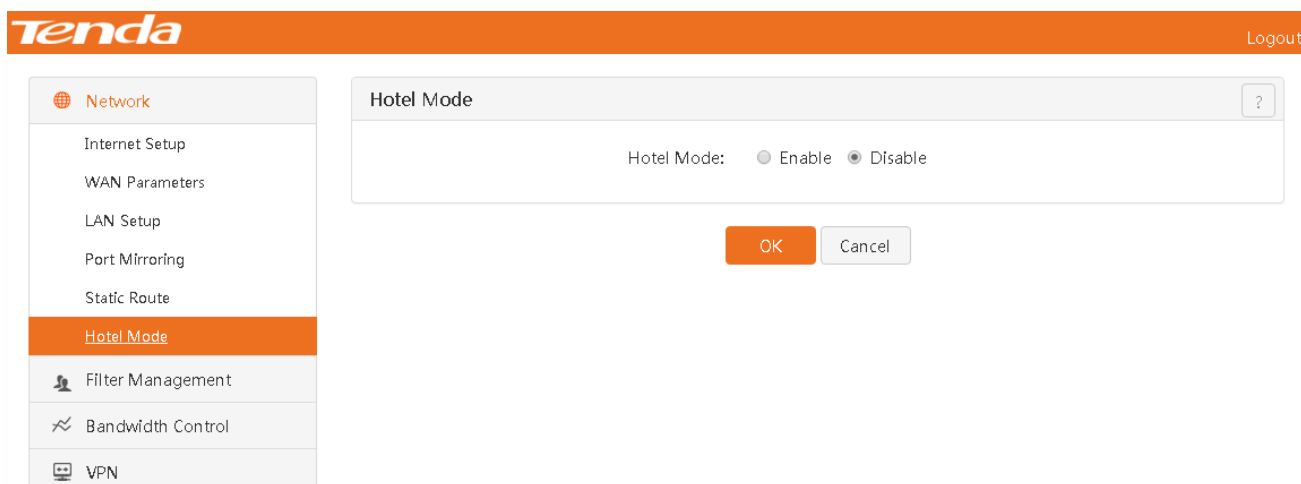
To realize Internet access by plugging a network cable by customers, Tenda develops the hotel mode function. After this function is enabled, customers can surf the Internet by plugging a network cable regardless of IP address settings of customers' computer network cards, thus being convenient and simple.



Tip

When the hotel mode is enabled, it has no effect on Internet access of clients by obtaining an IP address automatically. Clients in the LAN can also access the Internet by configuring any **IP address** (including IP addresses other than IP groups), **gateway**, and **DNS**.

Click 『Network』 > 『Hotel Mode』 to go to the configuration page. The hotel mode is disabled by default.



4.3 Filter Management

Filter Management includes the following contents:

[IP Group & Time Group](#): Set an IP group and time group. Applications such as Port Filter, Web Filter, and Multi-WAN Policy will be used.

[MAC Filter](#): Set limitations on a specified client from surfing the Internet.

[Port Filter](#): Set limitations on a client from accessing a specified port.

[Web Filter](#): Set application filter and QQ filter rules.

[Multi-WAN Policy](#): Set WAN port policies of the router.

4.3.1 IP Group & Time Group

Overview

This section describes how to add an IP group and time group. Most filter management functions of this router are set based on IP group and time group.

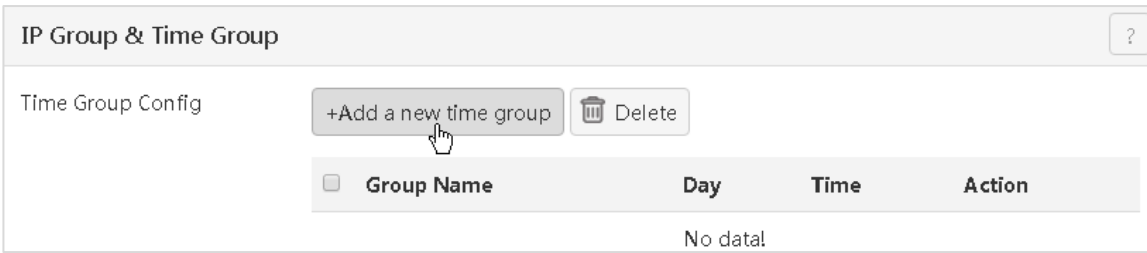
Click 『Filter Management』 to go to the IP Group & Time Group configuration page.

The screenshot displays the Tenda router's web interface for IP Group & Time Group management. The top navigation bar includes the Tenda logo and a 'Logout' link. The left sidebar lists various configuration categories, with 'Filter Management' expanded to show 'IP Group & Time Group' as the active selection. The main content area is titled 'IP Group & Time Group' and contains two configuration sections:

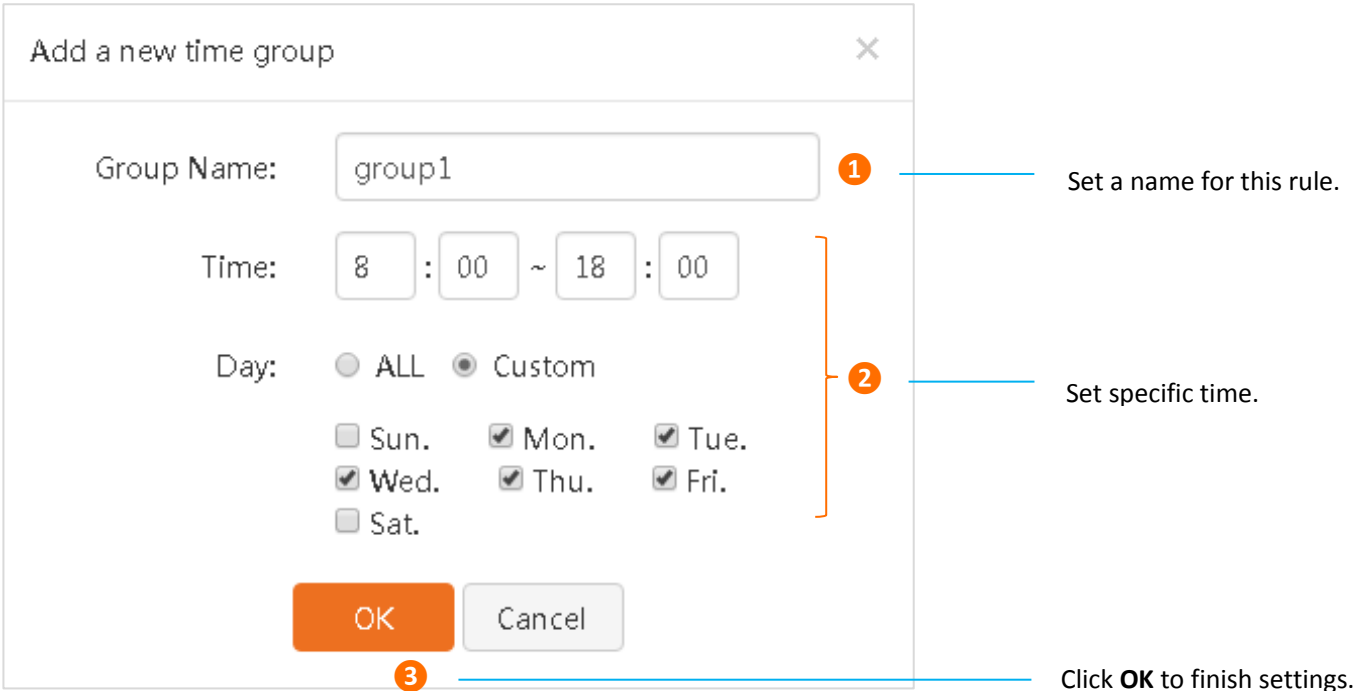
- Time Group Config:** Features a '+Add a new time group' button and a 'Delete' button. Below is a table with columns: Group Name, Day, Time, and Action. The table currently contains 'No data!'.
- IP Group Config:** Features a '+Add a new IP group' button and a 'Delete' button. A note states: 'Note: The IP excluded from the IP group will be forbidden from accessing the Internet.' Below is a table with columns: IP Group Name, IP, and Action. The table currently contains 'No data!'.

Steps for Adding a Time Group

Click .

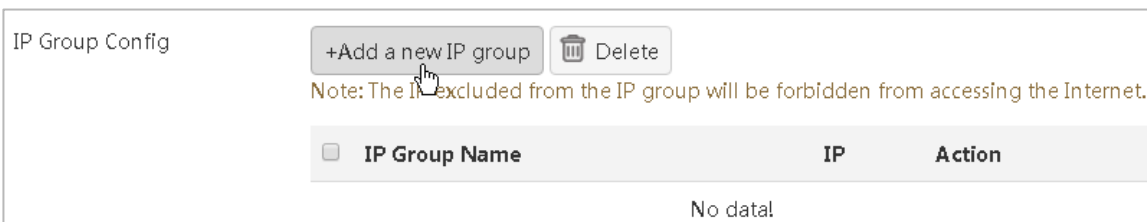


Set time group rule contents in the window that appears.

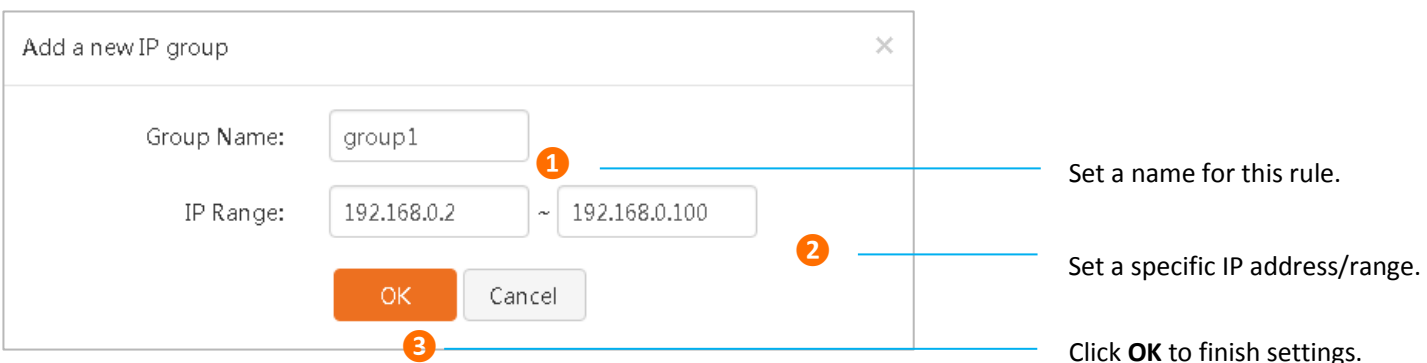


Steps for adding an IP group

Click .



Set IP group rule contents in the window that appears.

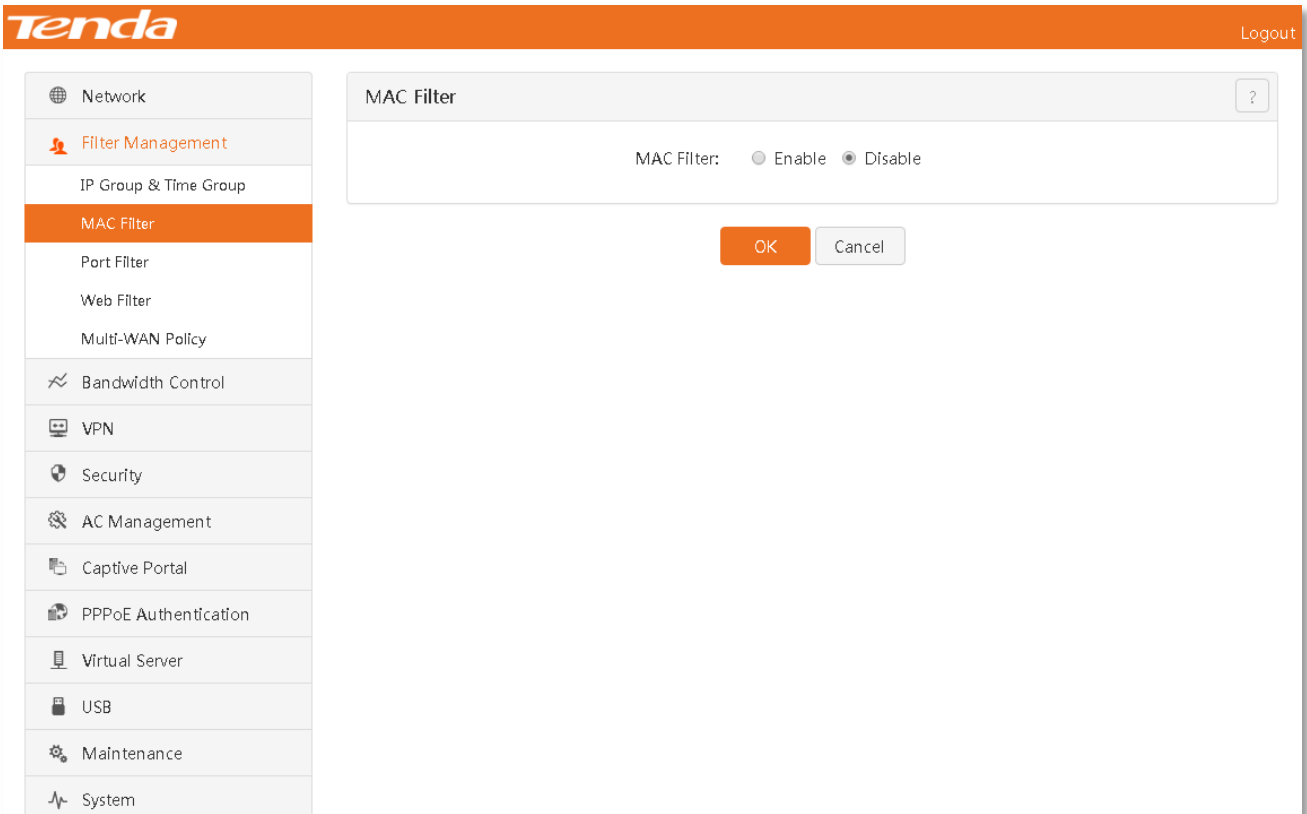


4.3.2 MAC Filter

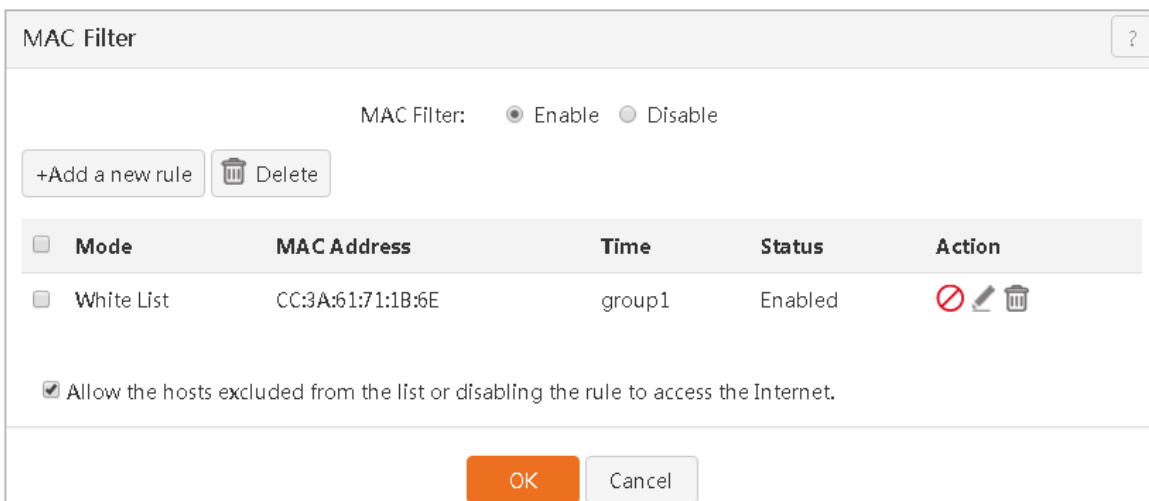
Overview

Computers and laptops that people often use have respective MAC addresses. You can control LAN clients' access to the Internet through the MAC Filter function. MAC Filter has two access control modes: Allow_Internet and Forbid_Internet.


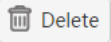
Click 『Filter Management』 > 『MAC Filter』 to go to the configuration page.



After the rule is set successfully, the page is shown in the figure below.



Parameter description in the page:

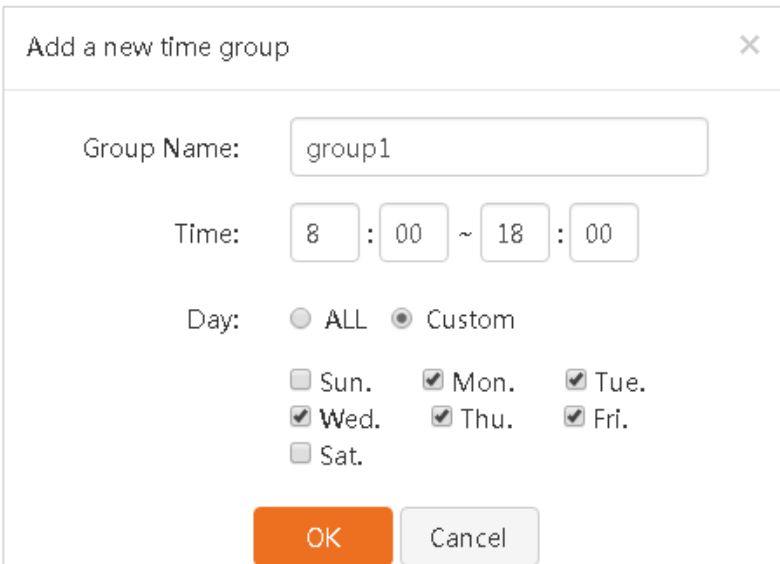
Parameter	Description
MAC Filter	Enable/Disable the MAC filter function. The default is Disable .
	Click this button to add a MAC filter rule.
	Click this button to delete a selected rule.
Mode	<ul style="list-style-type: none"> White List: Allow a device with this MAC address to access the Internet. Black List: Forbid a device with this MAC address from accessing the Internet.
MAC Address	MAC address of client device.
Time	Time to forbid or allow a corresponding device in the list to access the Internet.
Status	Current status of a rule, including Enabled and Disabled.
Action	Perform the enable/disable, edit, and delete actions on a rule.
Allow the hosts excluded from the list or disabling the rule to access the Internet.	<ul style="list-style-type: none"> When this item is enabled, all devices excluded from the list or disabling the rule in the list can access the Internet. When this item is disabled, only the rule in the list is valid and all devices excluded from the list or disabling the rule in the list cannot access the Internet.

Example of MAC filter

- **Example:** An enterprise uses a G3 enterprise router to establish a network. The staffs are forbidden from surfing the Internet in office hours, but recruiters are allowed to do so in office hours (8:00 - 18:00). This can be achieved through the MAC filter function. The MAC address for Internet access is CC:3A:61:71:1B:6E.

Configuration steps:

Step 1: Set a time group (8:00 - 18:00) as follows. For detailed configuration steps, refer to [Steps for adding a time group](#).

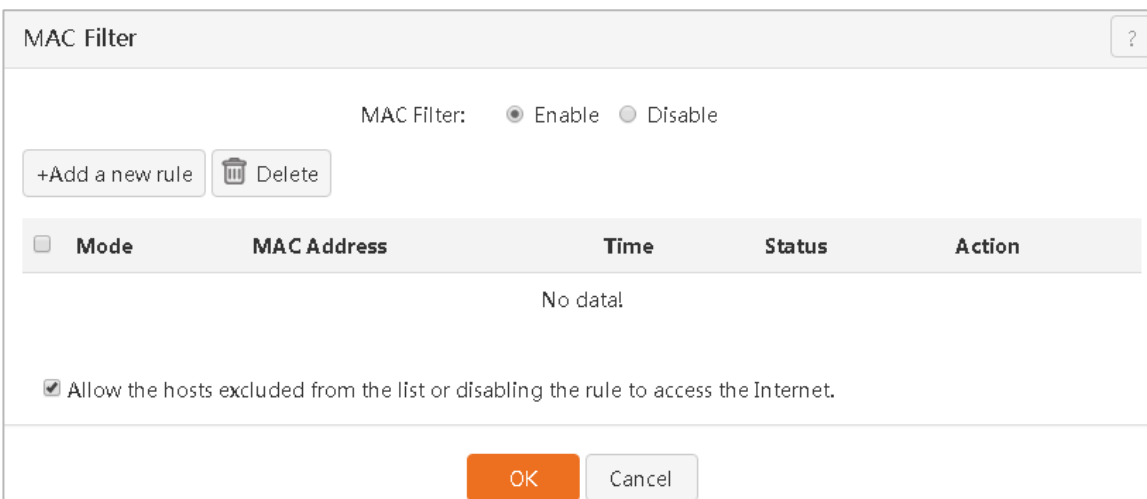


The screenshot shows a dialog box titled "Add a new time group" with a close button (X) in the top right corner. The dialog contains the following fields and options:

- Group Name:** A text input field containing "group1".
- Time:** A time range selector showing "8 : 00 ~ 18 : 00".
- Day:** Radio buttons for "ALL" and "Custom". The "Custom" option is selected.
- Days of the week:** Checkboxes for Sun., Mon., Tue., Wed., Thu., Fri., and Sat. The checkboxes for Mon., Tue., Wed., Thu., and Fri. are checked.
- Buttons:** "OK" (orange) and "Cancel" (grey).

Step 2: Enable the MAC filter function.

Click **Enable** and **OK**.

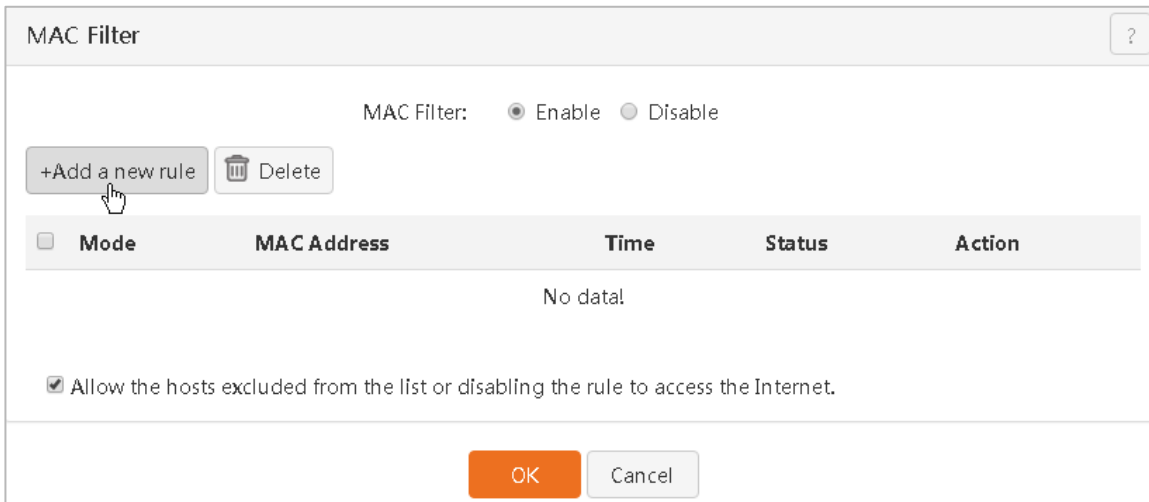


The screenshot shows a window titled "MAC Filter" with a help icon (?) in the top right corner. The window contains the following elements:

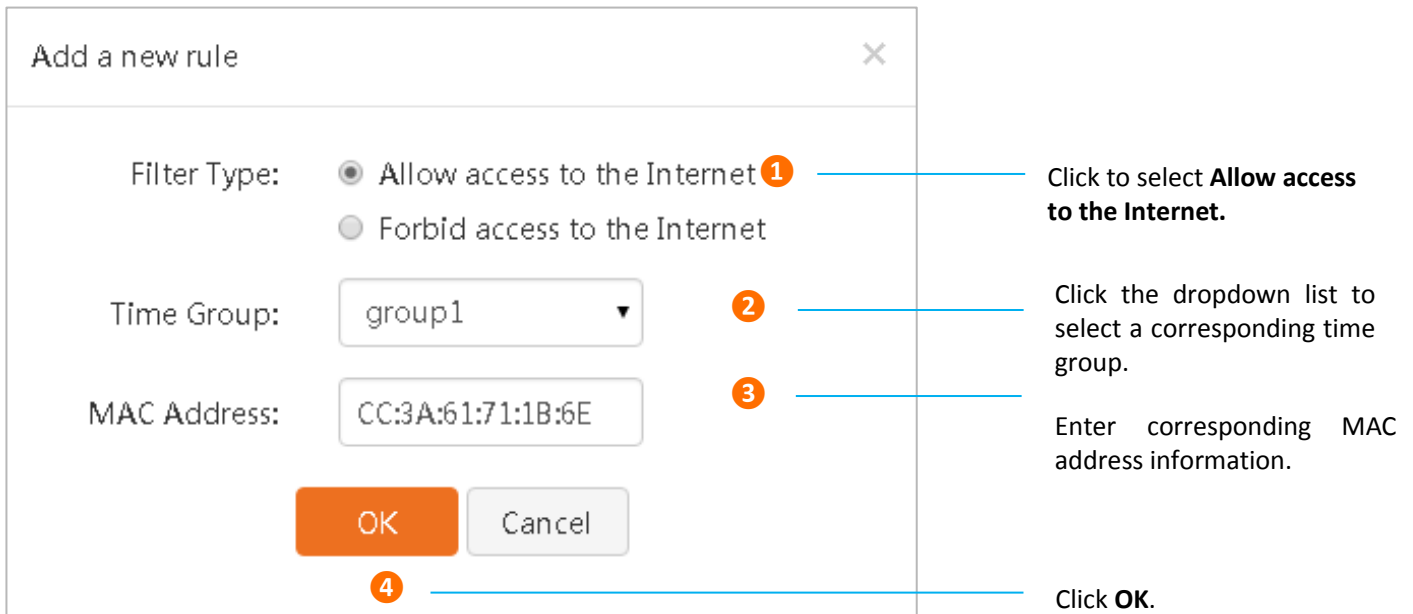
- MAC Filter:** Radio buttons for "Enable" and "Disable". The "Enable" option is selected.
- Buttons:** "+Add a new rule" and "Delete" (with a trash icon).
- Table:** A table with columns: Mode, MAC Address, Time, Status, and Action. The table is currently empty, displaying "No data".
- Checkbox:** A checked checkbox with the text "Allow the hosts excluded from the list or disabling the rule to access the Internet."
- Buttons:** "OK" (orange) and "Cancel" (grey).

Step 3: Set MAC Filter rule contents.

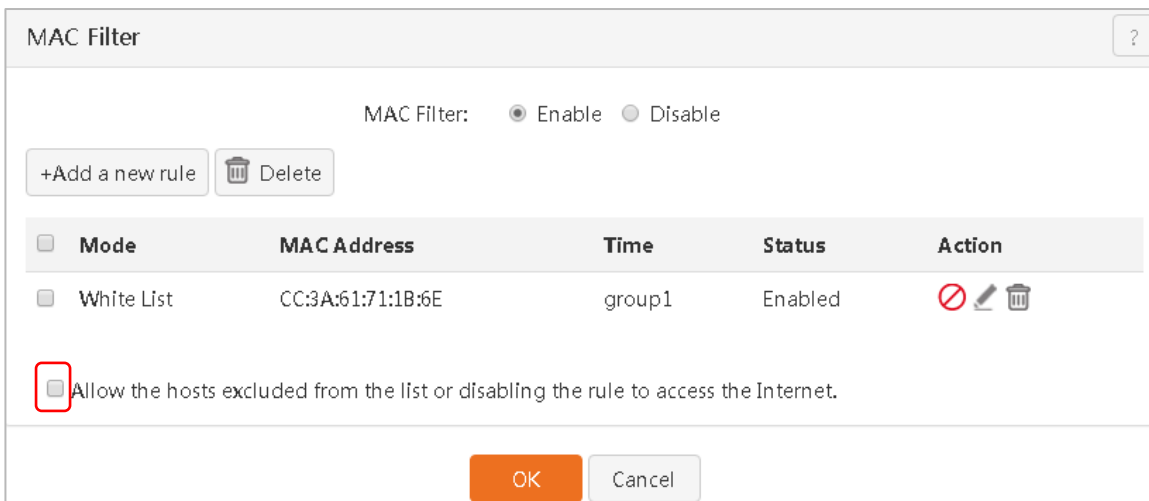
Click .



Set rule contents in the window that appears.



Step 4: Back to the MAC Filter page, disable Allow the hosts excluded from the list or disabling the rule to access the Internet, and click OK.

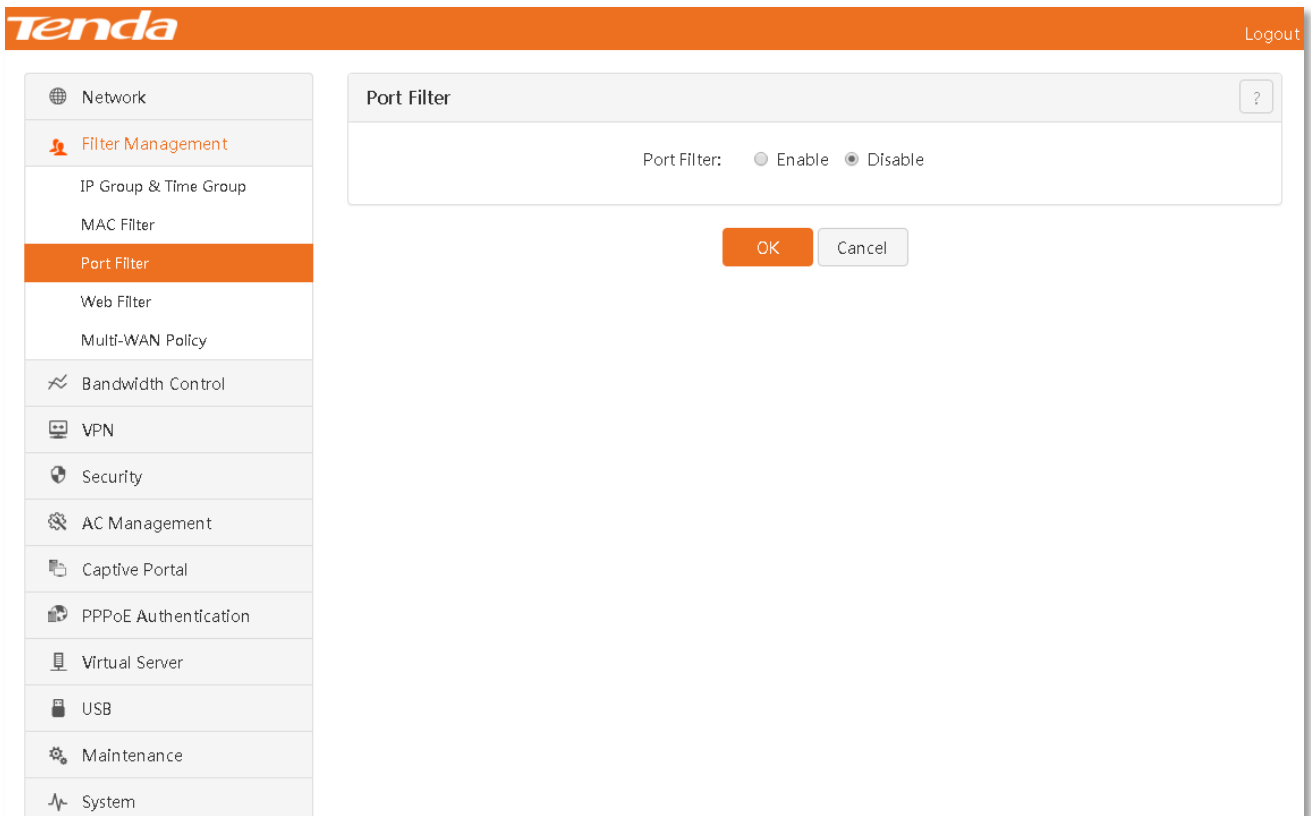


4.3.3 Port Filter

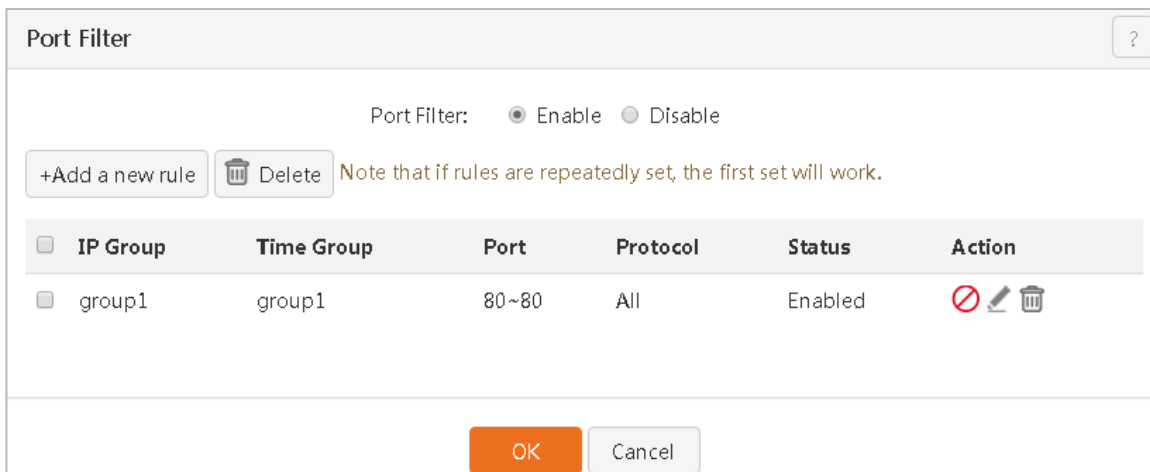
Overview

Network protocols involved by many services in the Internet have specific port numbers. 0-1023 are the port numbers of typical ports. These port numbers are generally assigned to specific services. To facilitate further management on clients in the LAN, the access of clients in the LAN to some ports in the Internet can be controlled by setting the port filter function.



Click 『Filter Management』 > 『Port Filter』 to enter the configuration page.



After the rule is set successfully, the page is shown in the figure below.



Parameter description in the page:

Parameter	Description
Port Filter	Enable/Disable the port filter function. The default is Disable.
	Click this button to add a port filter rule.
	Click this button to delete a selected rule.
IP Group	IP group where the rule is valid.
Time Group	Time when the rule is valid, i.e. time to forbid a device corresponding to an IP group in the rule to access a specified service.
Port	Port number of an unaccessible service.
Protocol	Protocol used by an unaccessible service. It is recommended to maintain the default settings.
Status	Current status of a rule, including Enabled and Disabled.
Action	Perform the enable/disable, edit, and delete actions on a rule.

Example of port filter

- Example:** An enterprise uses a G3 enterprise router to establish a network. Computers with IP addresses 192.168.0.2-192.168.0.100 in the LAN cannot browse a web page at 8:00-18:00 (office hours) of Monday to Friday. (The port for the service of browsing a web page is 80 by default.)

Configuration steps:

Step 1: Set a time group (8:00 - 18:00) as follows. For detailed configuration steps, refer to [Steps for adding a time group](#).

Add a new time group
✕

Group Name:

Time: : ~ :

Day: ALL Custom

Sun.

Mon.

Tue.

Wed.

Thu.

Fri.

Sat.

Step 2: Set an IP group (IP field is 192.168.0.2-192.168.0.100) as follows. For detailed configuration steps, refer to [Steps for adding an IP group](#).

Add a new IP group

Group Name:

IP Range: ~

Step 3: Enable the Port Filter function.

Click **Enable** and **OK**.

Port Filter

Port Filter: Enable Disable

Note that if rules are repeatedly set, the first set will work.

<input type="checkbox"/> IP Group	Time Group	Port	Protocol	Status	Action
No data					

Step 4: Set Port Filter rule contents.

1 Click .

Port Filter

Port Filter: Enable Disable

Note that if rules are repeatedly set, the first set will work.

<input type="checkbox"/> IP Group	Time Group	Port	Protocol	Status	Action
No data					

- 1 Set rule contents in the window that appears.
 - **IP Group**、 **Time Group**: Click the dropdown list and select a corresponding IP.
 - **Ports**: Set a service port unaccessible for the LAN that may be a single port or port segment.
 - **Protocol**: Set a protocol used by a forbidden service. It is recommended to maintain the default settings.
 - Click **OK** to finish settings.

Add a new rule
✕

IP Group:

Time Group:

Ports: ~

Protocol:

The rule addition is finished, as shown in the figure below:

Port Filter
?

Port Filter: Enable Disable

Note that if rules are repeatedly set, the first set will work.

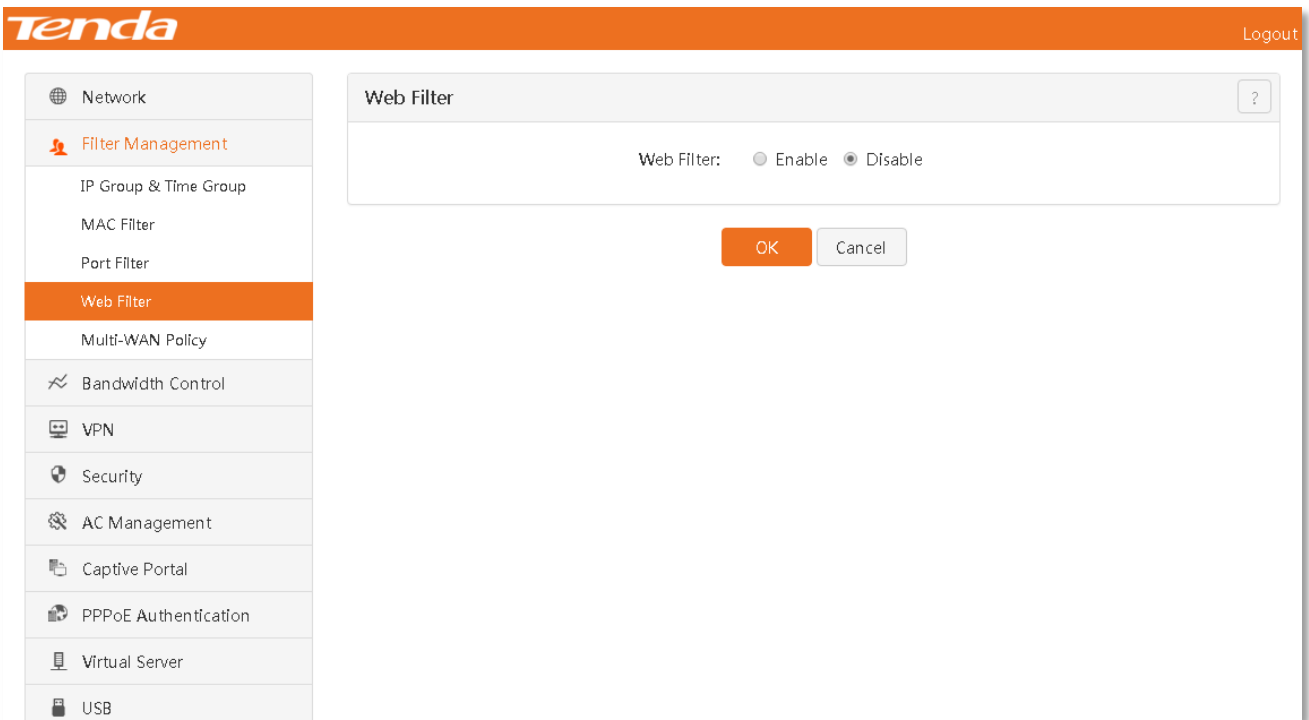
<input type="checkbox"/> IP Group	Time Group	Port	Protocol	Status	Action
<input type="checkbox"/> group1	group1	80~80	All	Enabled	<input type="checkbox"/> <input type="button" value="✖"/> <input type="button" value="✎"/> <input type="button" value="🗑️"/>

4.3.4 Web Filter

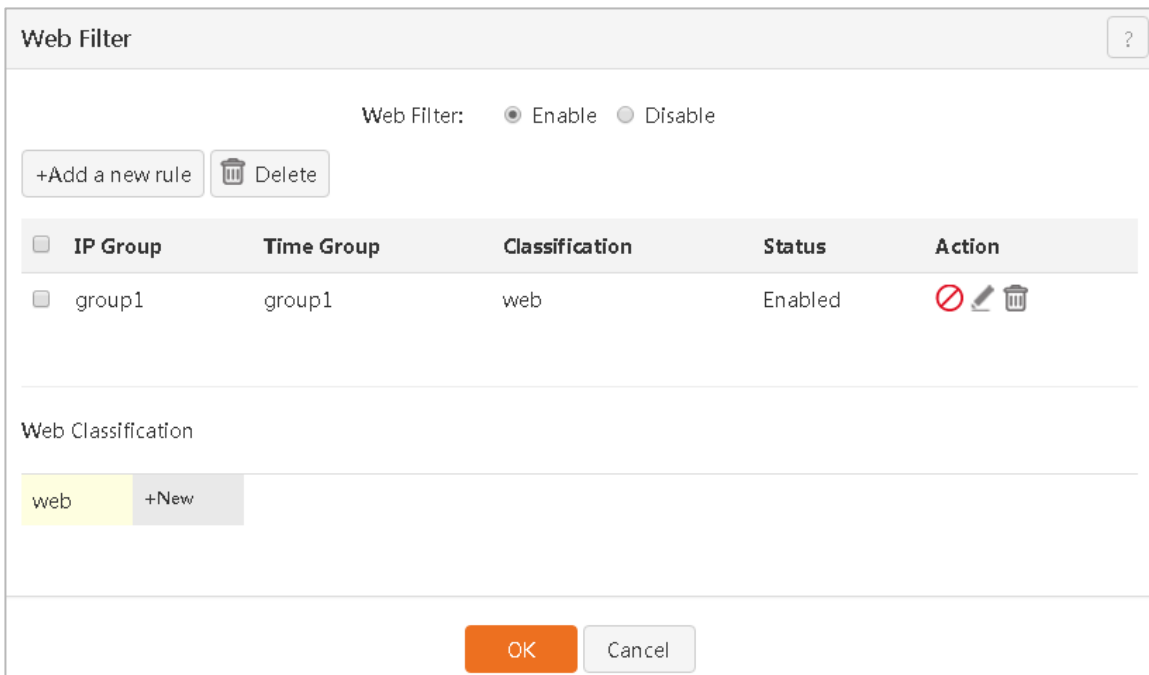
Overview

This describes how to set the web filter function. This router can forbid any specified client in the LAN from using any specified applications such as communication software, video software, and music software.


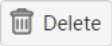

Click 『Filter Management』 > 『Web Filter』 to go to the configuration page. You must define a website before performing filter settings.



After the rule is set successfully, the page is shown in the figure below.



Parameter description in the page:

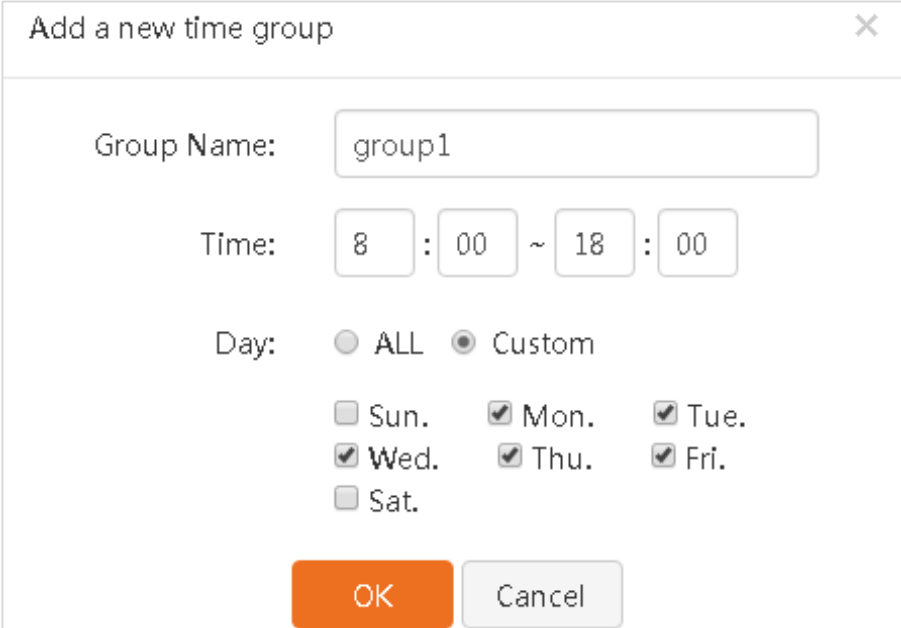
Parameter	Description
Web Filter	Enable/Disable the web filter function. The default is Disable .
	Click this button to add a web filter rule.
	Click this button to delete a selected rule.
IP Group	IP group where the rule is valid.
Time Group	Time when the rule is valid, i.e. time to forbid a client corresponding to an IP group in the rule from using a specified application.
Classification	Application that is forbidden from being used by a device corresponding to an IP group.
Status	Current status of a rule, including Enabled and Disabled.
Action	Perform the enable/disable, edit, and delete actions on a rule.
	Add website contents.

Example of web filter

- **Example:** An enterprise uses a G3 enterprise router to establish a network. Computers with IP addresses 192.168.0.2-192.168.0.100 in the LAN cannot access yahoo.com at 8:00-18:00 (office hours) of Monday to Friday.

Configuration steps:

Step 1: Set a time group (8:00 - 18:00) as follows. For detailed configuration steps, refer to [Steps for adding a time group](#).



Add a new time group

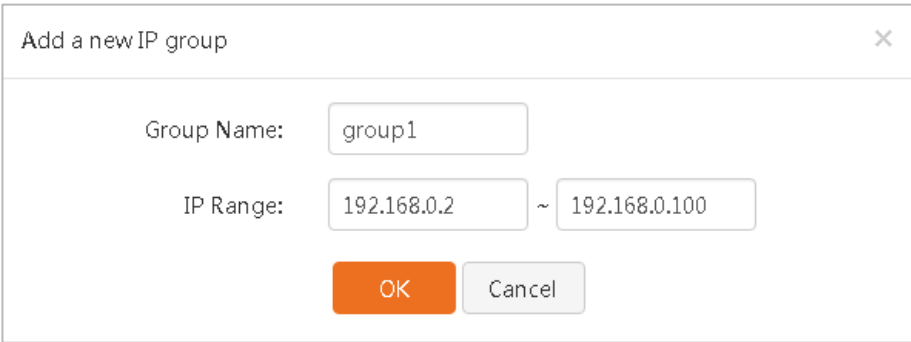
Group Name:

Time: : ~ :

Day: ALL Custom

Sun. Mon. Tue.
 Wed. Thu. Fri.
 Sat.

Step 2: Set an IP group (IP field is 192.168.0.2-192.168.0.100) as follows. For detailed configuration steps, refer to [Steps for adding an IP group](#).



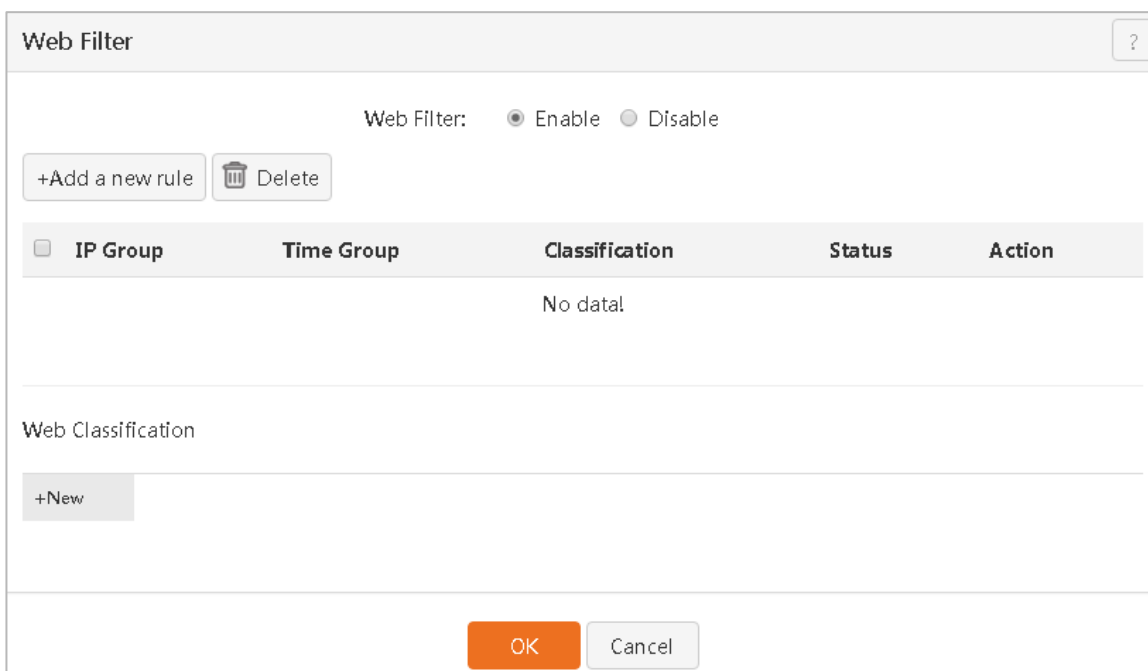
Add a new IP group

Group Name:

IP Range: ~

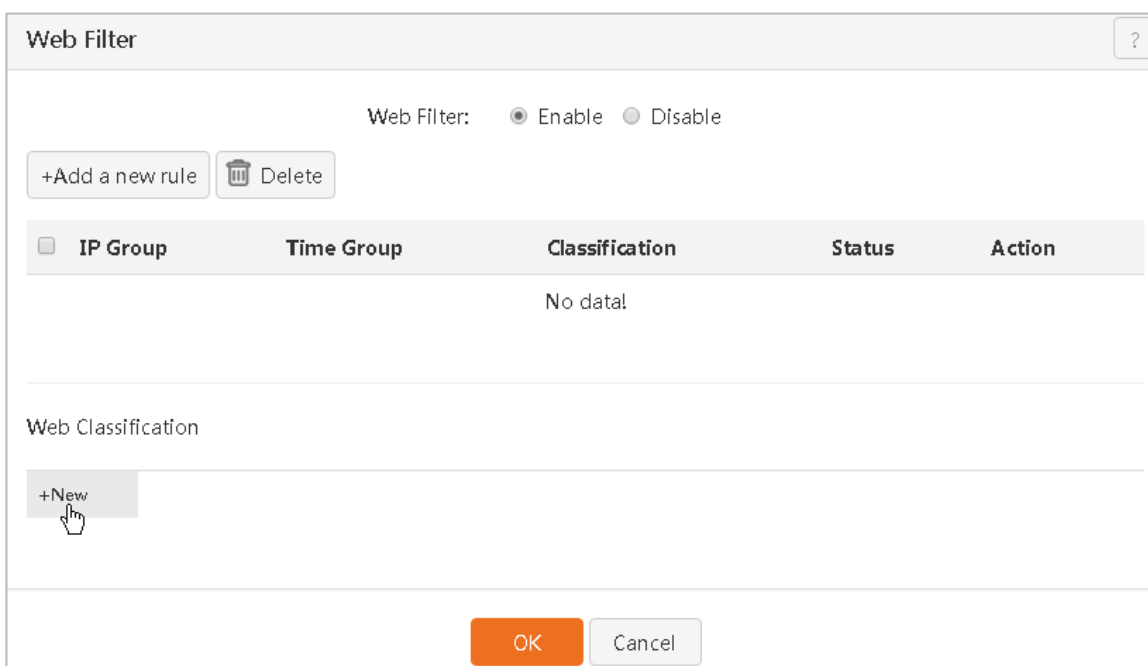
Step 3: Set the **Web Filter** function.

Click **Enable** and **OK** to enable the **Web Filter** function.



Add website contents to be filtered.

Click  .



Set rule contents in the window that appears.

The screenshot shows a 'New classification' dialog box with the following elements and callouts:

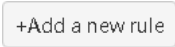
- 1**: Points to the 'Group Name' input field containing 'web'. A note to the right says 'Set a rule name.' Below the field is the text '20-character maximum for a group name'.
- 2**: Points to the 'URL' input field containing 'www.yahoo.com'. A note to the right says 'Set a website to be filtered.'
- 3**: Points to the 'URL' input field containing 'yahoo'. A note to the right says 'Set website description.'
- 4**: Points to the 'OK' button. A note to the right says 'Click **OK** to finish settings.'

The rule addition is finished, as shown in the figure below:

The screenshot shows the 'Web Filter' window with the following elements:

- At the top, 'Web Filter:' with radio buttons for 'Enable' (selected) and 'Disable'.
- Buttons for '+Add a new rule' and 'Delete'.
- A table with columns: IP Group, Time Group, Classification, Status, Action. The table is currently empty with 'No data!' below it.
- A section titled 'Web Classification' containing a list item 'web' with a '+New' button next to it. The 'web' item is highlighted with a red box.
- Buttons for 'OK' and 'Cancel' at the bottom.

Set website filter.

Click .

This is a close-up of the '+Add a new rule' button in the 'Web Filter' window. A mouse cursor is shown clicking on the button. The rest of the window's interface is visible in the background.

Set filter rule contents.

- **IP Group、 Time Group:** Click the dropdown list and select a corresponding IP group and time group.
- **Classification:** Select an application type that is forbidden from being used by a client. When adding multiple websites, you can quickly select them through **All** and **Invert**.
- Click **OK** to finish settings.

Add a new rule

IP Group: group1

Time Group: group1

Classification: Select All Invert

web

OK Cancel

After addition is successful, the page is shown in the figure below.

Web Filter

Web Filter: Enable Disable

+Add a new rule Delete

<input type="checkbox"/> IP Group	Time Group	Classification	Status	Action
<input type="checkbox"/> group1	group1	web	Enabled	<input type="checkbox"/> <input type="text"/> <input type="trash"/>

Web Classification

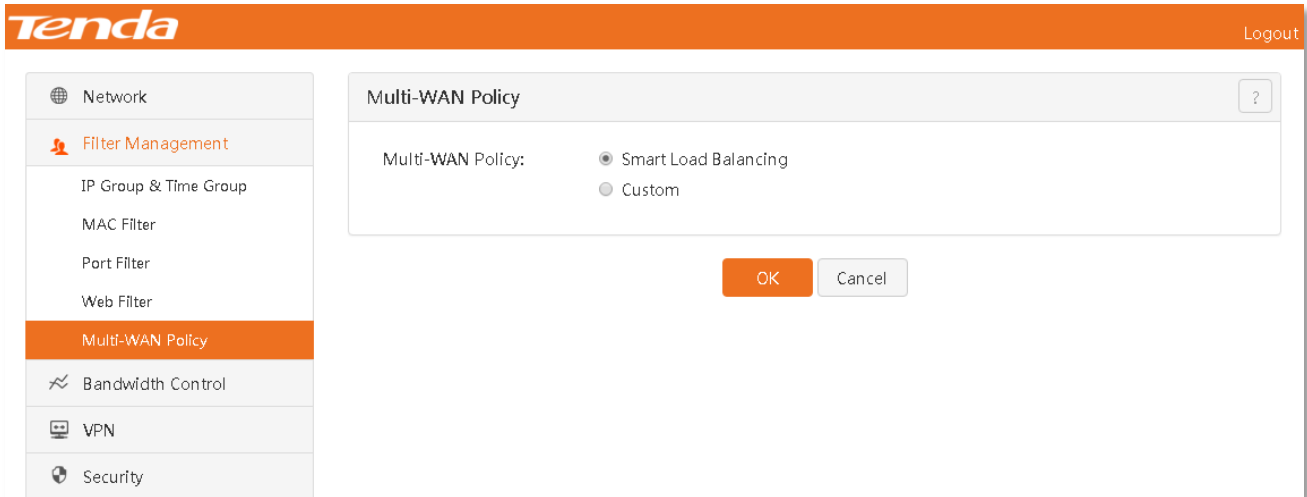
web +New

OK Cancel

4.3.5 Multi-WAN Policy

Overview

This section describes how to set a router WAN port policy. A router WAN port supports two operating modes: Smart Load Balancing (Auto) and Custom. Click 『Filter Management』 > 『Multi-WAN Policy』 to go to the configuration page.



- **Smart Load Balancing:** The system automatically searches a WAN port with the minimum traffic for communication. It needs no manual intervention and automatically assign traffic.
- **Custom:** You can specify a specific WAN port against a specific source address according to actual need.

Example of custom

- **Example:** An enterprise uses a G3 enterprise router to establish a network. Broadband services provided by both China Telecom and China Mobile are handled to meet enterprise network requirements. The Internet has been successfully accessed. Multi-WAN policy settings can be performed to manage the network better.

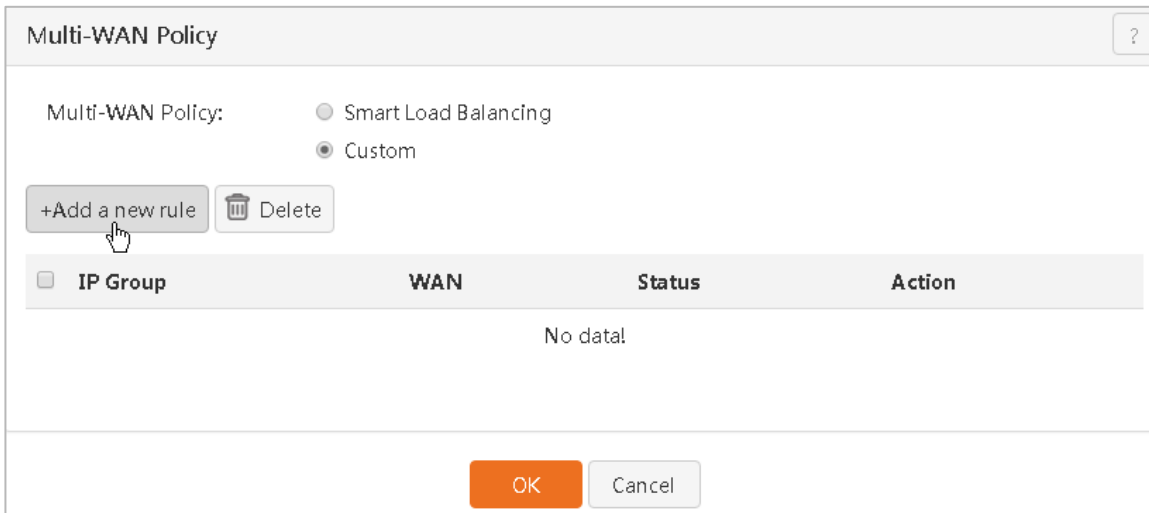
Configuration steps:

Step 1: Add an IP group applied to this WAN policy. For example, the IP range is 192.168.0.2-192.168.0.100. For detailed configuration steps, refer to [Steps for adding an IP group](#).

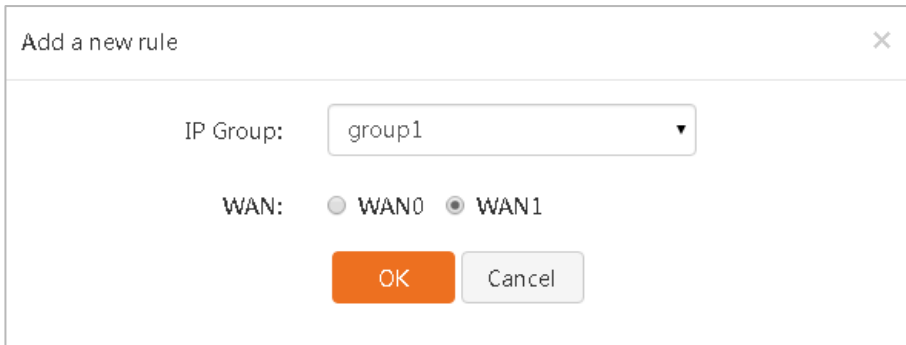
Step 2: Set a WAN policy rule.

- 1 **WAN policy:** Click to select Custom.
- 2 Click **OK**

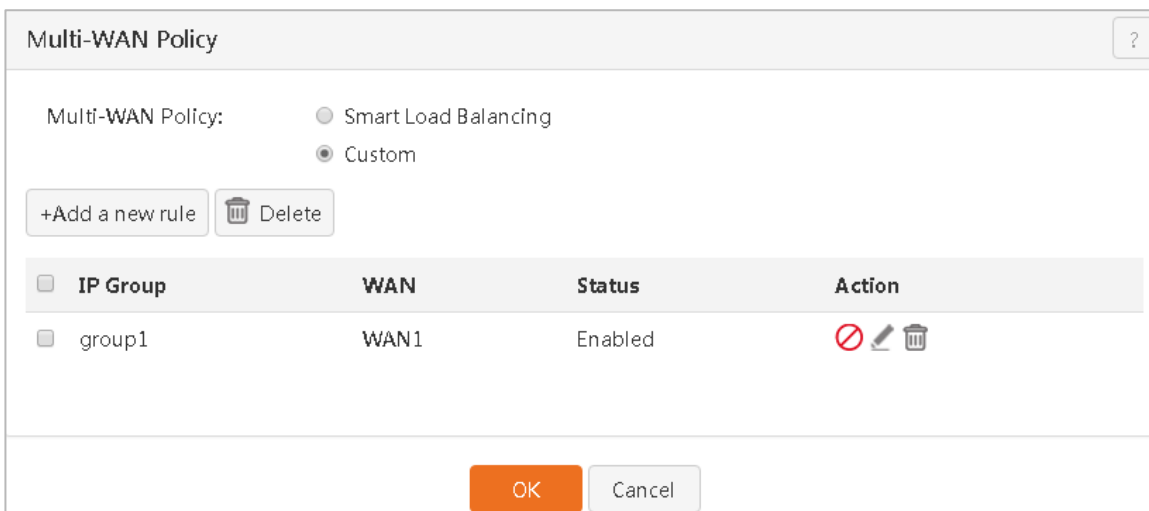
- 3 Click **Add a new rule**.



- 4 IP Group: Click the dropdown list to select a corresponding IP group.
- 5 WAN: Select a WAN port where the data traffic of the IP group passes.
- 6 Click **OK** to finish settings.



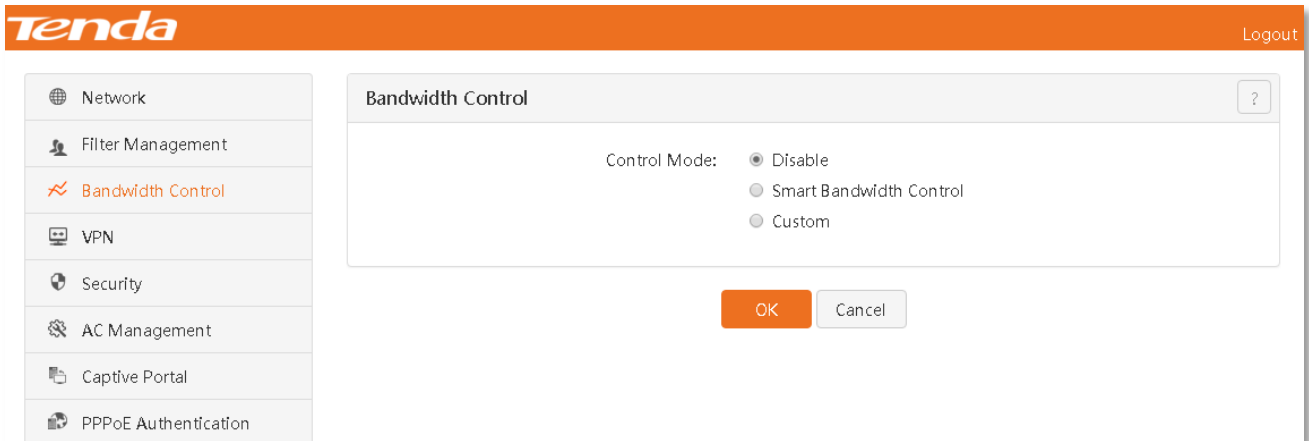
The rule addition is finished, as shown in the figure below:



4.4 Bandwidth Control

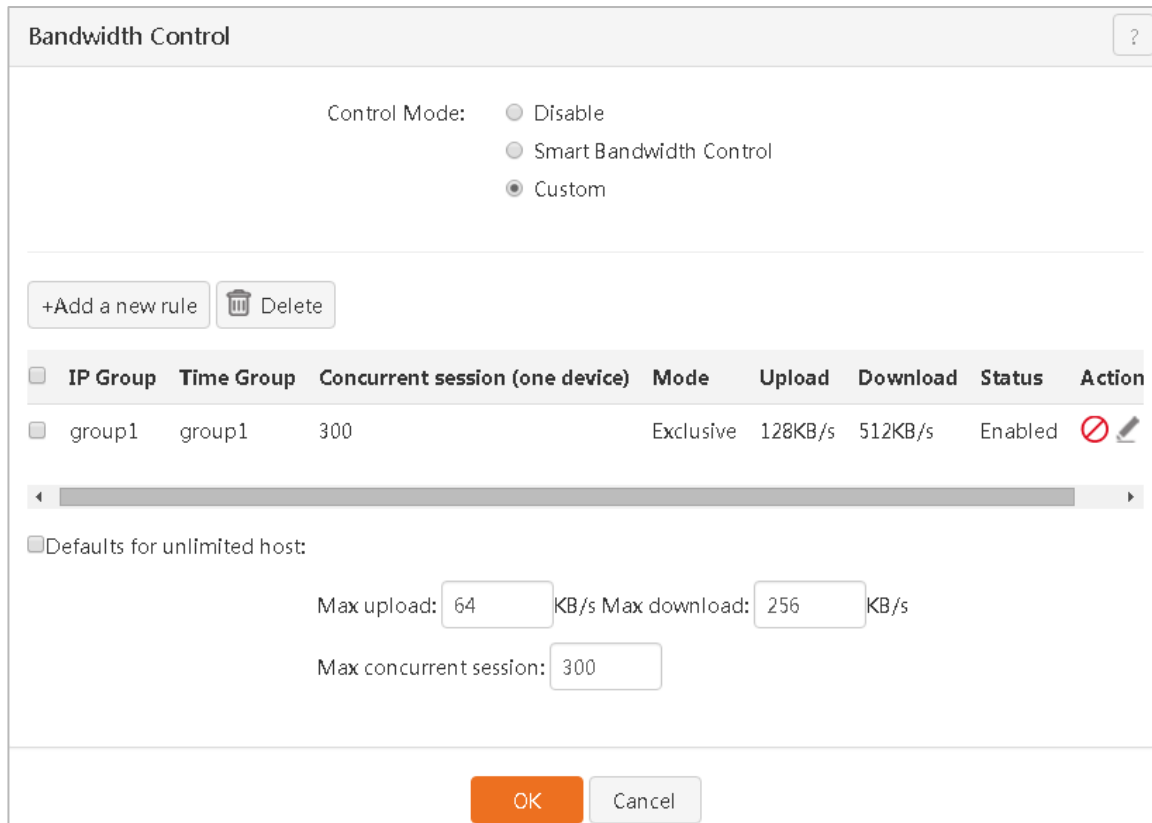
Overview

This section describes how to set the router traffic function. By setting corresponding limitation rules on various data traffic, bandwidth control on data transmission can be realized so that limited bandwidth resources are reasonably allocated to achieve the objective of effectively using the existing bandwidth. Click 『Bandwidth Control』 to go to the configuration page.



- **Disable:** Disable the bandwidth control function.
- **Smart Bandwidth Control:** The router smartly allocates bandwidth to a client according to actual situations.
- **Custom:** Manually set bandwidth for a client.

After the "custom rule" is set successfully, the page is shown in the figure below.



Parameter description in the page:

Parameter	Description
IP Group	IP group where the rule is valid.
Time Group	Time when the rule is valid, i.e. time to forbid a client corresponding to an IP group in the rule from accessing a specified website.
Concurrent session (one device)	Maximum total number of connections used by every computer in a controlled IP address range.
Mode	<ul style="list-style-type: none"> Shared: The sum of bandwidths of all IP addresses in a controlled address range is an uploading/downloading rate set by the current rule. Exclusive: Every IP address in a controlled address range applies an uploading/downloading rate set by the current rule.
Upload/Download	Uploading/Downloading rate of a client under a corresponding rule. 1 Mbps = 128 KB/s = 1,024 kb/s
Status	Current status of a rule, including Enabled and Disabled.
Action	Perform the enable/disable, edit, and delete actions on a rule.
Defaults for unlimited host:	<ul style="list-style-type: none"> When this item is enabled, the bandwidth parameters of devices excluded from the list or disabling the rule in the list are "default parameters". When this item is disabled, only the rule in the list is valid and no bandwidth of devices excluded from the list or disabling the rule in the list is restricted.

Enabling smart bandwidth control

Click Smart Bandwidth Control and click **OK**.

Example of custom

- Example:** An enterprise uses a G3 enterprise router to establish a network. The router LAN port IP address is 192.168.0.252. The subnet mask is 255.255.255.0. Bandwidth control on a client under the router needs to be set so that the client has a fixed bandwidth. The IP address is 192.168.0.2-192.168.0.100. The time group restricted for the broadband is 8:00-18:00.

Configuration steps:

Step 1: Set a time group (8:00 - 18:00) as follows. For detailed configuration steps, refer to [Steps for adding a time group](#).

Add a new time group
✕

Group Name:

Time: : ~ :

Day: ALL Custom

Sun.
 Mon.
 Tue.

Wed.
 Thu.
 Fri.

Sat.

OK
Cancel

Step 2: Set an IP group (IP field is 192.168.0.2-192.168.0.100) as follows. For detailed configuration steps, refer to [Steps for adding an IP group.](#)

Add a new IP group
✕

Group Name:

IP Range: ~

OK
Cancel

Step 3: Click **Custom** and **OK** to enable the "Custom" function.

Bandwidth Control
?

Control Mode: Disable Smart Bandwidth Control Custom

+Add a new rule
 Delete

<input type="checkbox"/>	IP Group	Time Group	Concurrent session (one device)	Mode	Upload	Download	Status	Action
No data!								

Defaults for unlimited host:

Max upload: KB/s
Max download: KB/s

Max concurrent session:

OK
Cancel

Step 4: Set "Custom" rule contents.

Click .

Bandwidth Control ?

Control Mode: Disable
 Smart Bandwidth Control
 Custom

<input type="checkbox"/>	IP Group	Time Group	Concurrent session (one device)	Mode	Upload	Download	Status	Action
No data.								

Defaults for unlimited host:

Max upload: KB/s Max download: KB/s

Max concurrent session:

Set rule contents in the window that appears.

- **IP Group, Time Group:** Click the dropdown list and select a corresponding IP group and time group.
- **Concurrent session:** It is recommended to set this parameter to 300 in the absence of exceptional circumstances.
- **Mode:** Select **Exclusive**.
- **Upload/ Download:** Set an uploading/downloading rate of a client.
- Click **OK** to finish settings.

Add a new rule ✕

IP Group:

Time Group:

Concurrent session (one device):

Mode: Shared Exclusive

Upload: KB/s

Download: KB/s

4.5 VPN

VPN includes the following contents:

[PPTP/L2TP Client](#): The router as a client is connected to the server.

[PPTP/L2TP Server](#): The router as a server allows a specified client to be connected to it.

[IPSec](#): Establish an IPSec tunnel to implement VPN transmission.

[Example of PPTP/L2TP configurations](#): Explain VPN application through the example of PPTP server/client.

[Example of IPSec configurations](#): Explain VPN application through the example of establishing an IPSec tunnel.

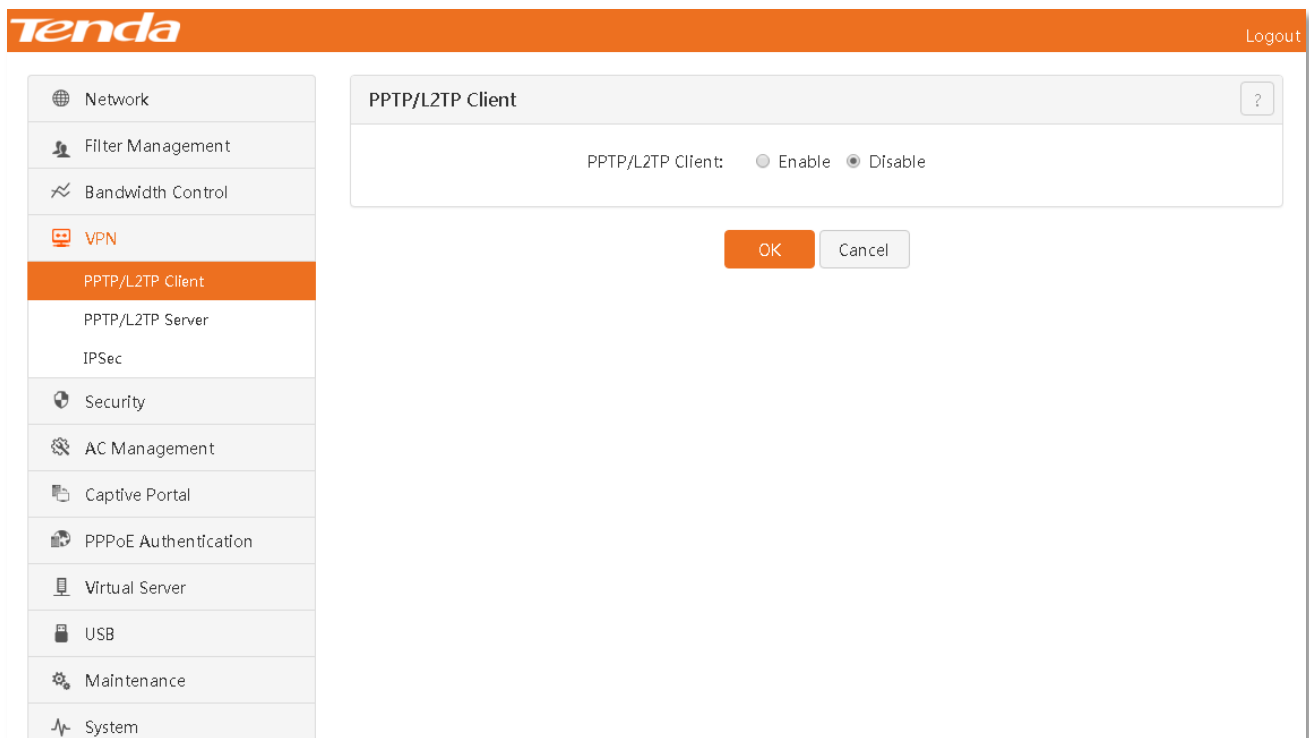
VPN (Virtual Private Network) is a private network established on the public network (generally the Internet). However, this private network logically exists only and has no actual physical line. Therefore, it is called VPN. VPN technology allows employees in a branch to conveniently share LAN resources of other employees or the headquarters without exposing these resources to users on the Internet.

VPN establishes a virtual private line between two sites using tunnel technology. It uses end-to-end authentication and encryption to ensure data security. Tunnel protocols supported by this router include Layer 2 tunneling protocols PPTP and L2TP and Layer 3 tunneling protocol IPSec.

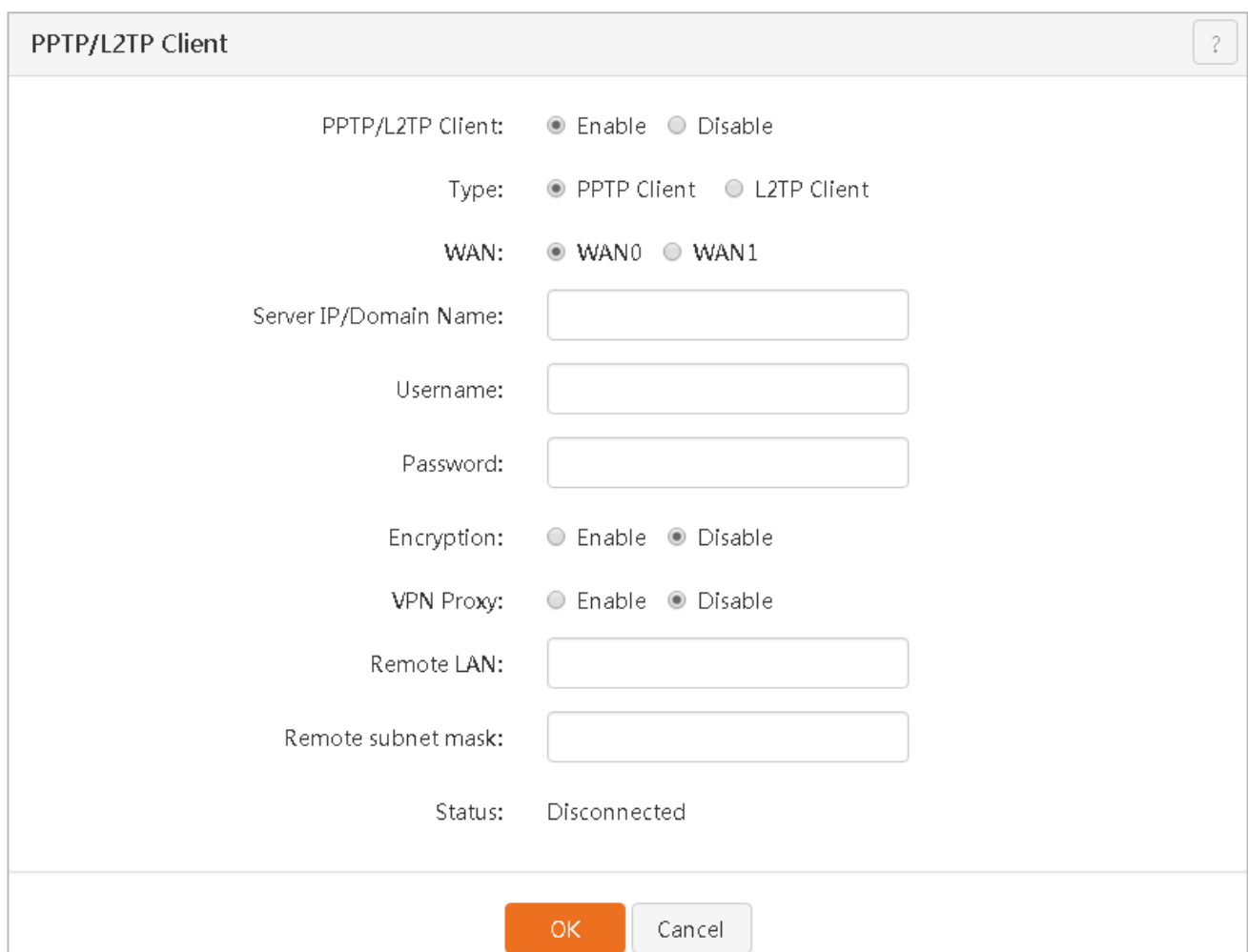
4.5.1 PPTP/L2TP Client

The PPTP/L2TP client supports connection from the VPN router client to the VPN router server. For example, information simple and safe access between the branch and the headquarters is required. This can be achieved by using the VPN server function in the router in the headquarters and the VPN client function in the router in the branch.

Click 『VPN』 to go to the PPTP/L2TP Client configuration page.



After PPTP/L2TP Client is enabled, the page is shown in the figure below.



Parameter description in the page:

Parameter	Description
PPTP/L2TP Client	Enable or disable the PPTP/L2TP client function. After this function is enabled, the router is used as a VPN client.
Type	Type of client that the router acts as, including PPTP Client and L2TP Client.
WAN	Select the current WAN port, i.e. the router port where the PPTP/L2TP client is enabled.
Server IP/Domain Name	Enter a VPN server IP address/domain name to be connected to, which is generally a WAN port IP address of the remote VPN router as a server where the "PPTP/L2TP Server" function is enabled.
Username/password	Enter a username/password assigned to the PPTP/L2TP client by the VPN server.
Encryption	Whether to enable data encryption. Server settings shall be consistent with client settings.
VPN Proxy	When this function is enabled after a VPN rule is established, the client router can surf the Internet through the server router.
Remote LAN	LAN segment under the VPN server.
Remote subnet mask	Subnet mask of LAN under the VPN server.
Status	Display the connection status of the current VPN client.

4.5.2 PPTP/L2TP Server

The PPTP/L2TP server allows specified users to dial into the server. For example, simple and safe access between the branch and the headquarters is required. This can be achieved by using the VPN server function in the router in the headquarters and the VPN client function in the router in the branch.

Click 『VPN』 > 『PPTP/L2TP Server』 to go to the configuration page.

Tenda Logout

- Network
- Filter Management
- Bandwidth Control
- VPN**
 - PPTP/L2TP Client
 - PPTP/L2TP Server**
 - IPSec
- Security
 - AC Management
 - Captive Portal
 - PPPoE Authentication
 - Virtual Server
 - USB
 - Maintenance
- System

PPTP/L2TP Server

PPTP/L2TP Server Status: Enable Disable

PPTP & L2TP User

<input type="checkbox"/>	Username	Password	Type	Network	Subnet Mask	Remark	Action
No data!							

After PPTP/L2TP Server is enabled, the page is shown in the figure below.

PPTP/L2TP Server

PPTP/L2TP Server Status: Enable Disable

Type: PPTP Server L2TP Server

WAN: WAN0 WAN1

Encryption: Enable Disable

IP Pool: 10.1.0.100-200

Max Connections: 15

PPTP & L2TP User

<input type="checkbox"/>	Username	Password	Type	Network	Subnet Mask	Remark	Action
<input type="checkbox"/>	admin	admin	Network	192.168.1.0	255.255.255.0		

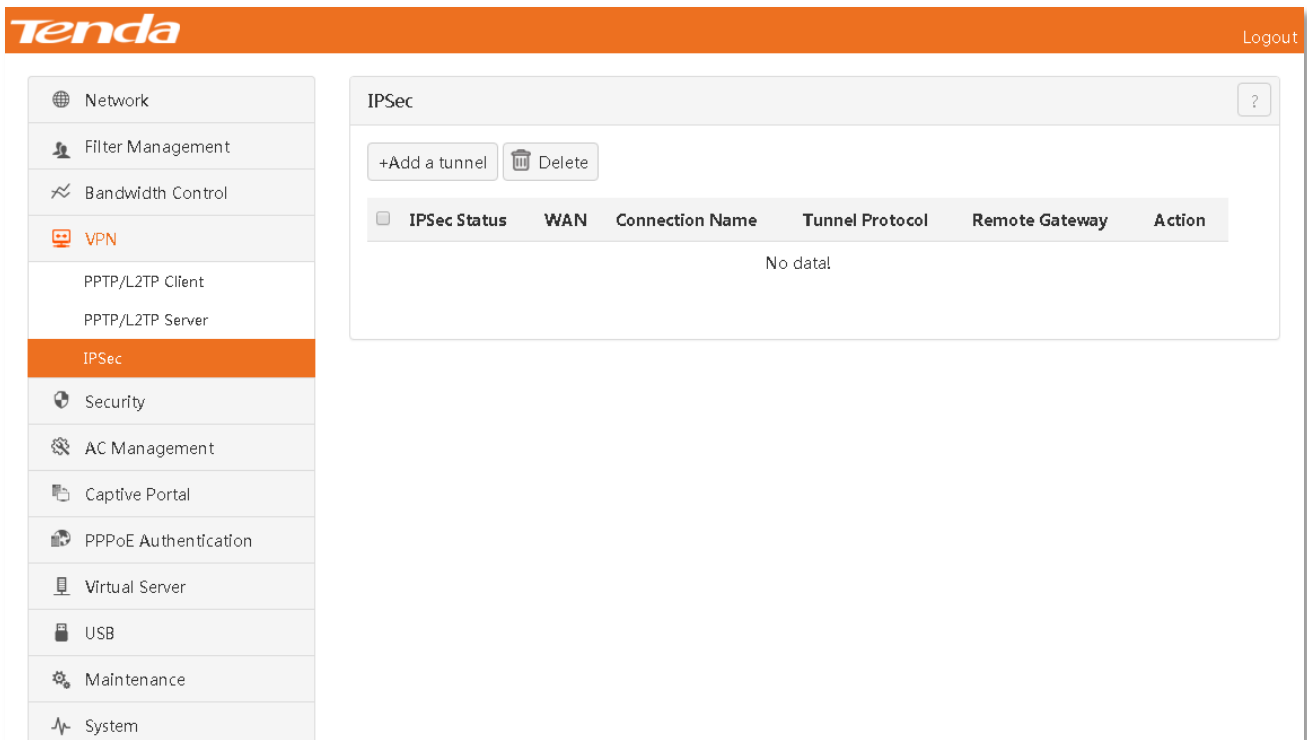
Parameter description in the page:

Parameter		Description
PPTP/L2TP Server	Status	Enable/Disable the PPTP/L2TP server function. After this function is enabled, the router is used as a VPN server.
	Type	Type of server that the router acts as, including PPTP Server and L2TP Server.
	WAN	Router port where the PPTP/L2TP server is enabled. The IP address of this port is "Server IP/Domain Name" information of the PPTP/L2TP client.
	Encryption	Whether to enable data encryption. Server settings shall be consistent with client settings.
	IP Pool	IP address field assigned to the PPTP/L2TP client by the server.
	Max Connections	Maximum number of PPTP/L2TP clients that are allowed to be connected. The system fixes this maximum number to 15.
PPTP/L2TP User	Username/Password	Set a user name/password assigned to the PPTP/L2TP client by the server. Username and password used when the PPTP/L2TP client is connected to the PPTP/L2TP server.
	Type	The client is a network or host. When the PPTP/L2TP client is a network, the LAN and mask of the PPTP/L2TP client must be set.
	Network	When the PPTP/L2TP client is a network, this item must be set. Set an IP LAN of the PPTP/L2TP client.
	Subnet Mask	When the PPTP/L2TP client is a network, this item must be set. Set a remote subnet mask of the PPTP/L2TP client.
	Remark	Description of this user. No description is displayed if it is not set when a rule is set.
	Action	Perform the edit and delete actions on users.

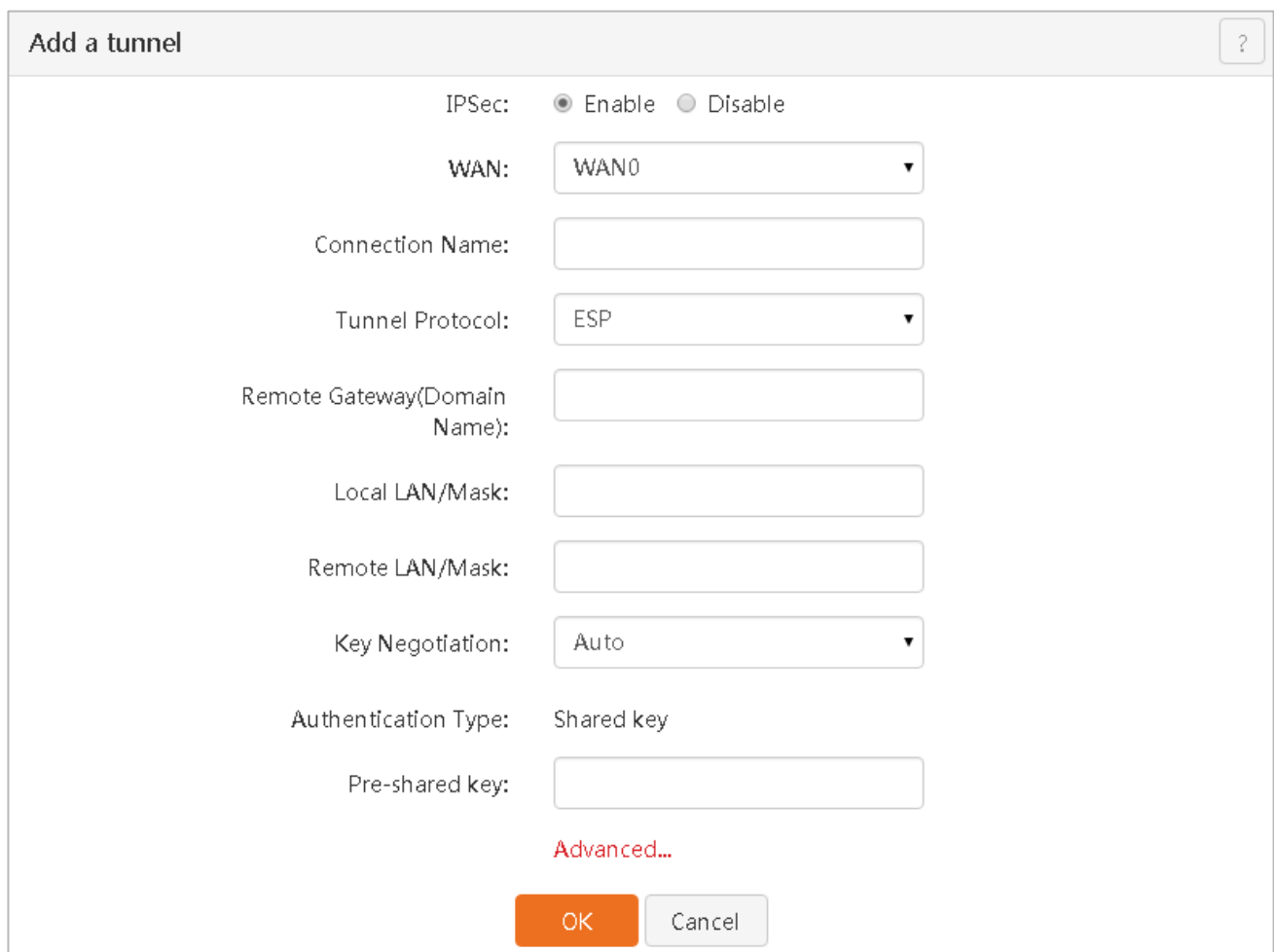
4.5.3 IPsec

IPsec (IP Security) is the set of a series of services and protocols that protects end-to-end communication security

and prevents any network attack in the IP network. Click 『VPN』 > 『IPSec』 to go to the configuration page.



After IPSec is enabled, the page is shown in the figure below.



Parameter description in the page:

Parameter	Description
IPSec	Enable/Disable the IPSec function.
WAN	Router port where IPSec is enabled. The IP address of this port is "Remote Gateway Address" information of the remote router.
Connection Name	Set a name for this IPSec connection to facilitate identification.
Tunnel Protocol	<p>Select ESP, AH or AH+ESP as needed.</p> <ul style="list-style-type: none"> AH (Authentication Header). The AH protocol is used to ensure data integrity. If data packets are falsified in the transmission process, the packet receiver will discard packets during integrity verification. ESP (Encapsulating Security Payload). The ESP protocol is used for data integrity check and data encryption. It is difficult for the third party to obtain true information even if encrypted packets are intercepted.
Remote Gateway Address	IP address or domain name of the remote router port.
Local LAN/Mask	IP LAN of the local router.
Remote LAN/Mask	IP LAN of the remote router.
Key Negotiation	The default is Auto. If you want to set it to Custom, refer to Key Negotiation — Custom .
Pre-shared key	Key that is mutually authenticated by both parties. The local and remote routers must have the same pre-shared key.

🔑 Key Negotiation — Auto

When key negotiation is Auto, the whole negotiation process is divided into two stages. Stage 1: Both parties of communication will negotiate security proposals such as exchange and verification algorithm and encryption algorithm, and establish an ISAKMP SA to securely exchange more information in Stage 2. Stage 2: Both parties of communication will negotiate parameters for the IPSec security protocol using ISAKMP SA established in Stage 1, and create IPSec SA to protect communication data of both parties.



Tip

1. **ISAKMP:** Internet Security Association and Key Management Protocol.
2. **SA:** Security Association.
3. **IKE:** Internet Key Exchange.

Description of IPSec tunnel **Advanced** parameters.

Click [Hide Advanced ...](#), and the page below appears:

[Hide Advanced...](#)

Period 1

Mode:

Encryption Algorithm:

Integrity Verification Algorithm:

Diffie-Hellman Group:

Key Life Cycle:

Period 2

PFS: Enable

Encryption Algorithm:

Integrity Verification Algorithm:

Diffie-Hellman Group:

Key Life Cycle:

Parameter description in the page:

Parameter	Description
Mode	<p>Set an exchange mode negotiated in Stage 1. This exchange mode must be the same as that of the remote end.</p> <p>There are two exchange modes as follows:</p> <ul style="list-style-type: none"> • MAIN: This mode allows both parties to exchange many packets, provides identity protection, and applies to situations with high requirements for identity protection. • AGGRESSIVE: Also called ACTIVE. This mode provides no identity protection, allows parties to exchange a small number of packets, has a fast negotiation speed, and applies to situations with low requirements for identity protection.
Encryption algorithm	<p>Select an encryption algorithm applied to an IKE session.</p> <p>The router supports the following encryption algorithms:</p> <ul style="list-style-type: none"> • DES (Data Encryption Standard): Encrypt 64-bit data using a 56-bit key. The last 8 bits of 64 bits are used for parity check. 3DES (Triple DES) performs encryption using three 56-bit keys. • AES (Advanced Encryption Standard): AES128/192/256 indicates performing encryption

	using a 128/192/256-bit key.
Parameter	Description
Integrity Verification Algorithm	<p>Select a verification algorithm applied to an IKE session.</p> <p>The router supports the following verification algorithms:</p> <ul style="list-style-type: none"> MD5 (Message Digest Algorithm): Generate a 128-bit message digest for a message to prevent this message from being falsified. SHA1 (Secure Hash Algorithm): Generate a 160-bit message digest for a message. It is more difficult to crack SHA1 than to crack MD5.
Diffie-Hellman Group	Diffie-Hellman algorithm group information that is used to generate a session key to encrypt an IKE tunnel.
Key Life Cycle	IPSec SA survival time.
PFS	<p>The PFS (Perfect Forward Secrecy) feature enables IKE Stage 2 negotiation to generate a new key material that has no association with any key material generated in Stage 1 negotiation. Therefore, the Stage 2 key is safe even if the IKE1 Stage 1 key is cracked. If PFS is not used, the Stage 2 key will be generated according to the key material generated in Stage 1. Once the Stage 1 key is cracked, the Stage 2 key used to protect communication data will also be placed in jeopardy. This will seriously threaten communication security of both parties.</p>

Key Negotiation — Custom

When key negotiation is **Custom**, the page is shown in the figure below.

Key Negotiation:

ESP Encryption Algorithm:

ESP Encryption Key:

ESP Authentication Algorithm:

ESP Outcoming SPI:

ESP Incoming SPI:

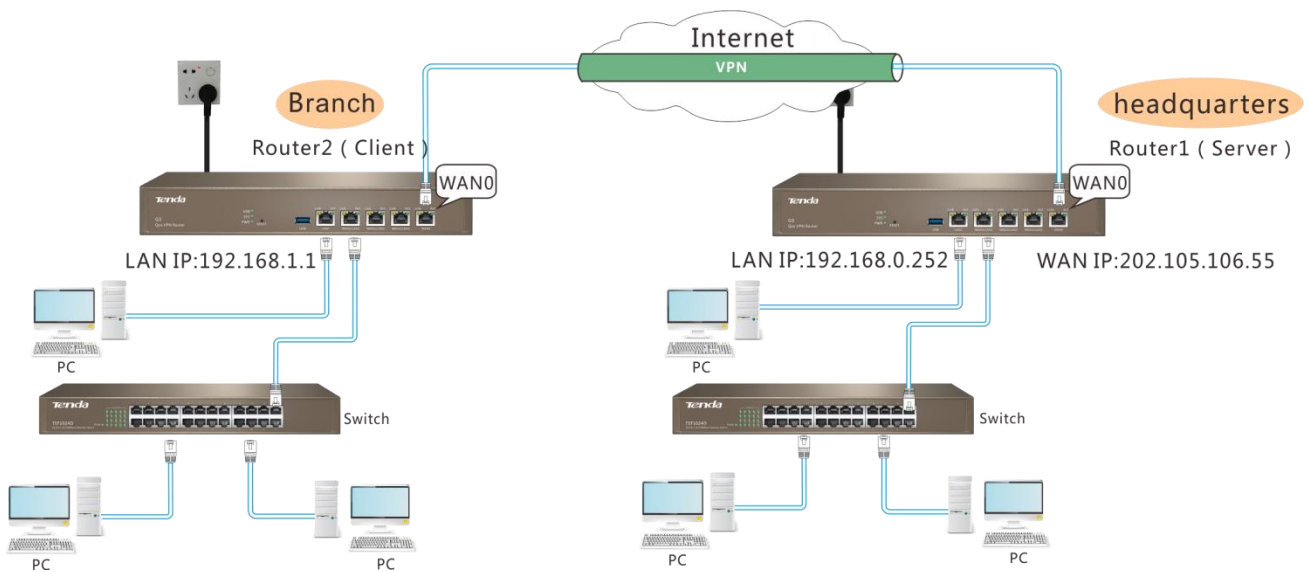
Parameter description in the page:

Parameter	Description
ESP Encryption Algorithm	<p>Set an ESP encryption algorithm when selecting an ESP security protocol.</p> <p>The router supports the following encryption algorithms:</p> <ul style="list-style-type: none"> • DES (Data Encryption Standard): Encrypt 64-bit data using a 56-bit key. The last 8 bits of 64 bits are used for parity check. 3DES (Triple DES) performs encryption using three 56-bit keys. • AES (Advanced Encryption Standard): AES128/192/256 indicates performing encryption using a 128/192/256-bit key.
ESP Encryption Key	<p>Set an ESP encryption key. Both parties of communication must keep the key consistent.</p>
ESP Authentication Algorithm	<p>Set an ESP authentication algorithm when selecting an ESP security protocol. Set an AH authentication algorithm when selecting an AH security protocol.</p> <p>The router supports the following verification algorithms:</p> <ul style="list-style-type: none"> • MD5 (Message Digest Algorithm): Generate a 128-bit message digest for a message to prevent this message from being falsified. • SHA1 (Secure Hash Algorithm): Generate a 160-bit message digest for a message. It is more difficult to crack SHA1 than to crack MD5.
ESP Outcoming SPI	<p>Set an SPI parameter. Three parameters including SPI, tunnel remote gateway address, and protocol type jointly identifies one IPSec security ally.</p> <p>The SPI parameter must be the same as the Incoming SPI value of the remote end of communication.</p>
ESP Incoming SPI	<p>Set an SPI parameter. Three parameters including SPI, tunnel remote gateway address, and protocol type jointly identifies one IPSec security ally.</p> <p>The SPI parameter must be the same as the Outcoming SPI value of the remote end of communication.</p>

4.5.4 Example of PPTP/L2TP configurations

- Example:** The headquarters and the branch use a G3 enterprise router to establish a network with successful access to the Internet. Employees in the branch need to access the company's resources via the Internet at any time. These resources include the company's internal data, office OA, ERP system, CRM system, project management system, etc. Remote users can access the company's server by setting the VPN service on the router. Take PPTP as an example. The setting method of L2TP is similar.

The reference topological graph is as follows:



Configuration steps:

Step 1: Set Router 1 that acts as a server.

Enable the "PPTP/L2TP Server" function.

- Status:** Click Enable.
- Type:** Click PPTP Server.
- WAN:** Select an enabled WAN port of Router 1 (VPN server) (In this example, WAN0).
- Encryption:** Click Enable to enable encryption.
- Click **OK**.

PPTP/L2TP Server

PPTP/L2TP Server

Status: Enable Disable

Type: PPTP Server L2TP Server

WAN: WAN0 WAN1

Encryption: Enable Disable

IP Pool: 10.1.0.100-200

Max Connections: 15

PPTP & L2TP User

+Add a user Delete

<input type="checkbox"/>	Username	Password	Type	Network	Subnet Mask	Remark	Action
No data!							

OK Cancel

Add a username and password whose access is allowed.

PPTP & L2TP User

+Add a user Delete

<input type="checkbox"/>	Username	Password	Type	Network	Subnet Mask	Remark	Action
No data!							

Click **Add a user**.

Add a user

Username:

Password:

Type: Network Host

Network:

Subnet Mask:

Remark (Optional):

OK Cancel

Set a username and password used when the client is connected to the server, such as admin.

Enter a client LAN and subnet mask.

Enter the description of this user (optional).

Click **OK**.

After settings are successfully finished, the page is shown in the figure below.

PPTP/L2TP Server
?

PPTP/L2TP Server

Status: Enable Disable

Type: PPTP Server L2TP Server

WAN: WAN0 WAN1

Encryption: Enable Disable

IP Pool: 10.1.0.100-200

Max Connections: 15

PPTP & L2TP User

+Add a user
 Delete

<input type="checkbox"/>	Username	Password	Type	Network	Subnet Mask	Remark	Action
<input type="checkbox"/>	admin	admin	Network	192.168.1.0	255.255.255.0		

OK
Cancel

Step 2: Set Router 2 that acts as a client.

- 1 **PPTP/L2TP Client:** Click Enable.
- 2 **Type:** Click PPTP client.
- 3 **WAN:** Select an enabled WAN port of Router 2 (VPN client) (In this example, WAN0).
- 4 **Server IP/Domain Name:** Enter an enabled WAN port IP address of the VPN server.
- 5 **Username/Password:** Enter a username/password assigned to the client by the server.
- 6 **Encryption:** Click Enable to enable encryption.
- 7 **Remote LAN:** Enter a server LAN.
- 8 **Remote subnet mask:** Enter a subnet mask of server LAN.
- 9 Click **OK**.

PPTP/L2TP Client ?

PPTP/L2TP Client: Enable Disable

Type: PPTP Client L2TP Client

WAN: WAN0 WAN1

Server IP/Domain Name:

Username:

Password:

Encryption: Enable Disable

VPN Proxy: Enable Disable

Remote LAN:

Remote subnet mask:

Status: Disconnected

After settings are successfully finished, the page is shown in the figure below. The connection is successful when the status is displayed as Connected and an IP address has been obtained.

PPTP/L2TP Client ?

PPTP/L2TP Client: Enable Disable

Type: PPTP Client L2TP Client

WAN: WAN0 WAN1

Server IP/Domain Name:

Username:

Password:

Encryption: Enable Disable

VPN Proxy: Enable Disable

Remote LAN:

Remote subnet mask:

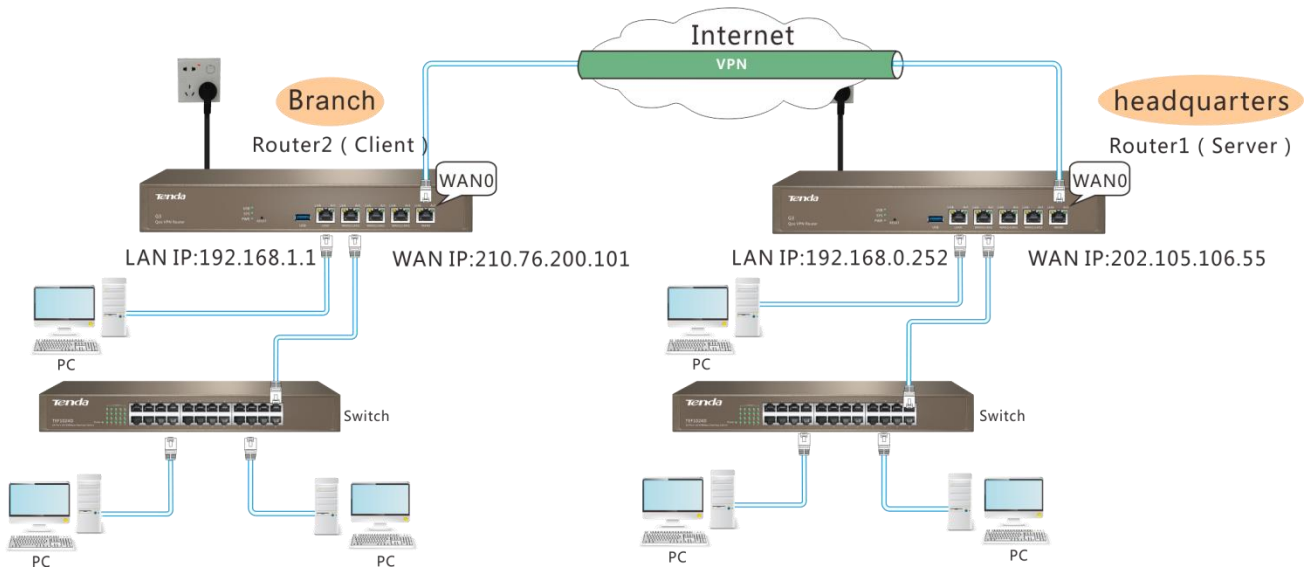
Status: **Connected**

IP Obtained: 10.1.0.100

4.5.5 Example of IPSec configurations

- Example:** The headquarters and the branch use a G3 enterprise router to establish a network with successful access to the Internet. Employees in the branch need to access the company's resources via the Internet at any time. These resources include the company's internal data, office OA, ERP system, CRM system, project management system, etc. Remote users can access the company's server by setting the VPN service on the router. Take IPSec as an example.

The reference topological graph is as follows:



Configuration steps:

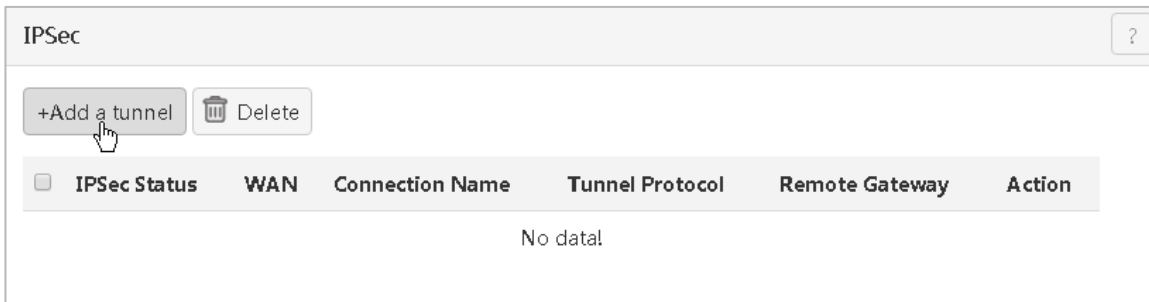
Assume that basic information about the IPSec tunnel of two routers is as follows:

Key Negotiation: Auto

Pre-shared key: 12345678

Step 1: Set Router 1.

Click .



Set rule contents.

- 1 **IPSec:** Click Enable.
- 2 **WAN:** Select an enabled WAN port of this tunnel (In this example, WAN0).
- 3 **Connection Name:** Set a name for this tunnel such as IPSec_1.
- 4 **Remote Gateway (Domain Name):** Enter an IP address of the enabled WAN port of the IPSec tunnel of the remote router (In this example, 210.76.200.101).
- 5 **Local LAN/Mask:** Enter a local LAN/subnet mask (In this example, 192.168.0.0/24).
- 6 **Remote LAN/Mask:** Enter a remote router LAN/subnet mask (In this example, 192.168.0.0/24).
- 7 **Pre-shared key:** Enter a pre-shared key (In this example, 12345678).
- 8 Click **OK**.

Add a tunnel
?

IPSec: Enable Disable

WAN:

Connection Name:

Tunnel Protocol:

Remote Gateway(Domain Name):

Local LAN/Mask:

Remote LAN/Mask:

Key Negotiation:

Authentication Type: Shared key

Pre-shared key:

Advanced...

OK
Cancel

After settings are successfully finished, the page is shown in the figure below.

IPSec
?

+Add a tunnel
 Delete

<input type="checkbox"/>	IPSec Status	WAN	Connection Name	Tunnel Protocol	Remote Gateway	Action
<input type="checkbox"/>	Enable	WAN0	IPSec_1	ESP	210.76.200.101	

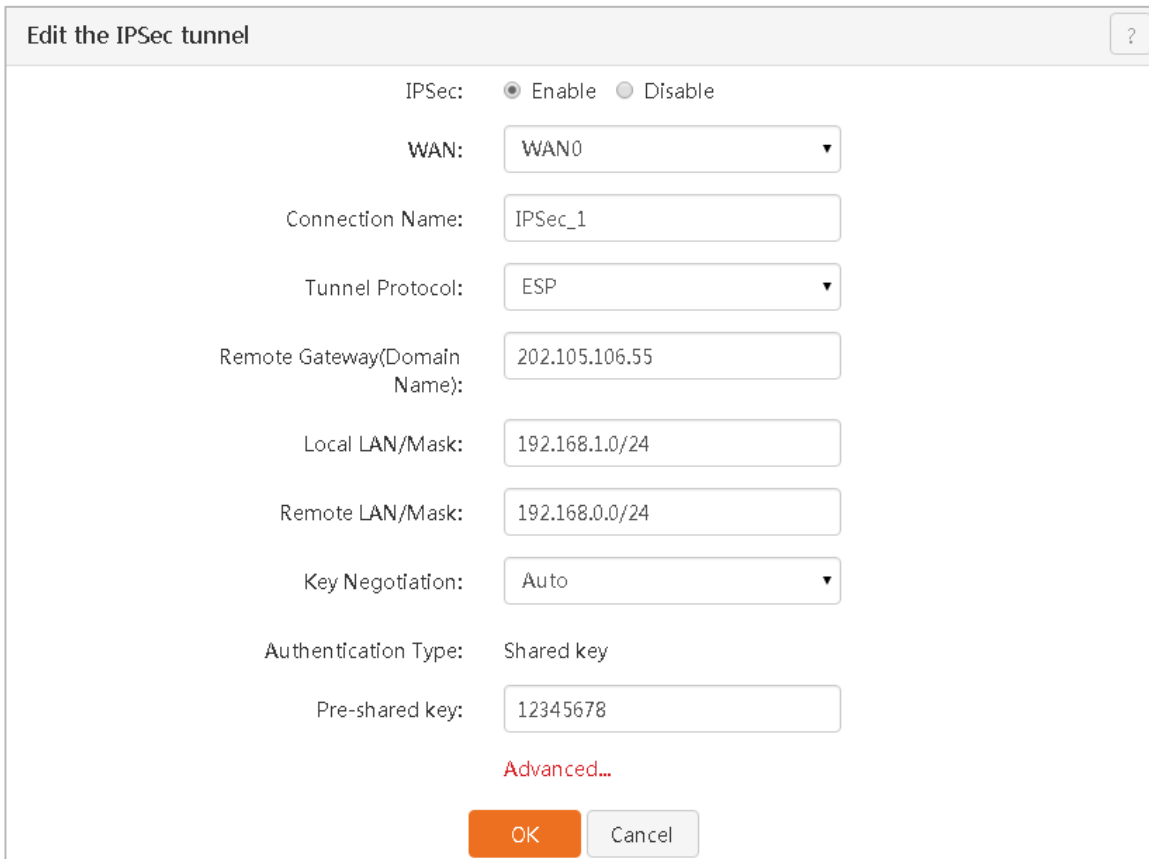
Step 2: Set Router 2.

Click +Add a tunnel.



Set rule contents.

- 1 IPsec: Click Enable.
- 2 WAN: Select an enabled WAN port of this tunnel (In this example, WAN0).
- 3 **Connection Name:** Set a name for this tunnel such as IPsec_1.
- 4 **Remote Gateway (Domain Name):** Enter an IP address of the enabled WAN port of the IPsec tunnel of the remote router (In this example, 202.105.106.55).
- 5 **Local LAN/Mask:** Enter a local LAN/subnet mask (In this example, 192.168.0.0/24).
- 6 **Remote LAN/Mask:** Enter a remote router LAN/subnet mask (In this example, 192.168.0.0/24).
- 7 **Pre-shared key:** Enter a pre-shared key (In this example, 12345678).
- 8 Click **OK**.



After settings are successfully finished, the page is shown in the figure below.

IPSec					
+Add a tunnel		Delete			
IPSec Status	WAN	Connection Name	Tunnel Protocol	Remote Gateway	Action
<input type="checkbox"/> Enable	WAN0	IPSec_1	ESP	202.105.106.55	

Step 3: Verify whether settings are successful.

Go to the management page of the router. Click 『System』 > 『Live Users』 to go to the page. When the number of connections is displayed in **IPSec**, settings are successful.

Live Users				
DHCP User	VPN User	PPPoE User	Captive Portal	IPSec
1	0	0	0	2
Item	IP Address	MAC Address	Uptime	Remaining
1	192.168.0.159	C8:3A:35:D5:75:A6	0d0h11min46s	19min



Tip

1. If you want to set the advanced option of the IPSec tunnel in the setting process, keep the setting parameters of two routers consistent.
2. When key negotiation is Custom, the encryption algorithm, encryption key, and authentication at both ends of IPSec shall be consistent. The outgoing SPI of Device 1 shall be consistent with the incoming SPI of Device 2. The incoming SPI of Device 1 shall be consistent with the outgoing SPI of Device 2.

4.6 Security

Security includes the following contents:

[IP-MAC Binding](#): Set the function that only the users bound to IP and MAC addresses in the list can access the Internet.

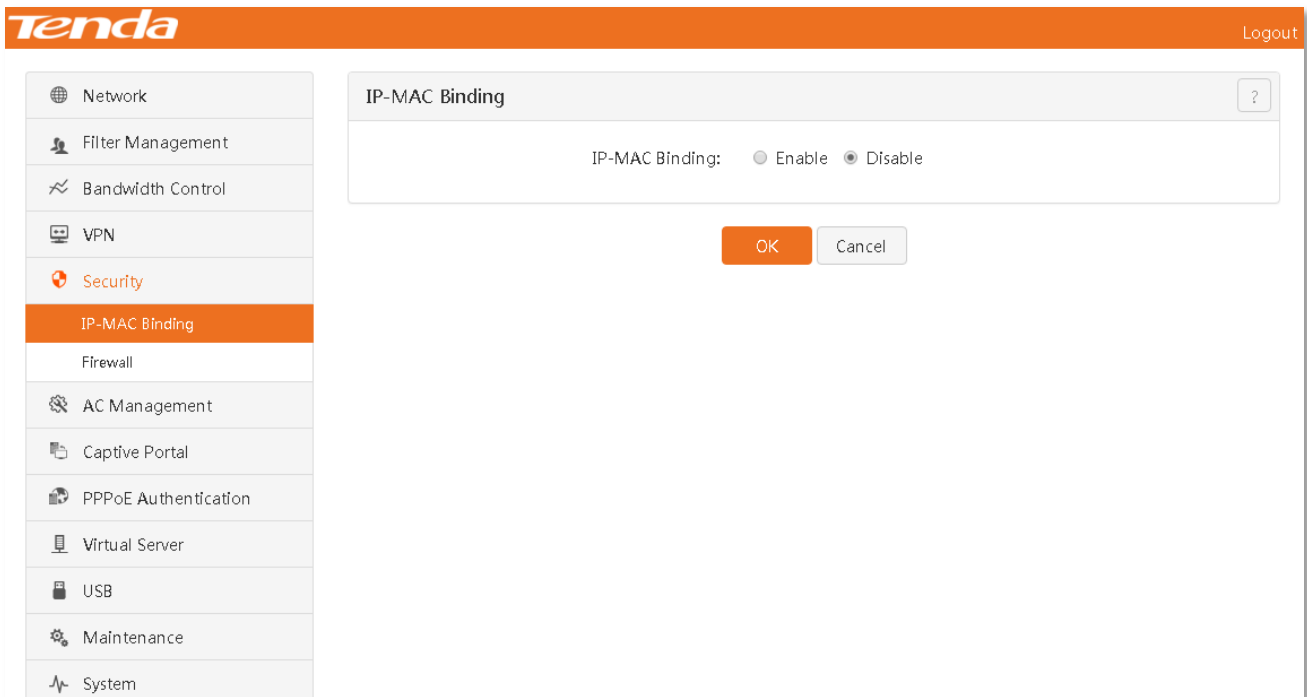
[Firewall](#): Set the defense function of the device. You can set this part under the guide of a professional.

4.6.1 IP-MAC Binding

Overview

The IP-MAC address binding function allows users bound to IP and MAC addresses in the list to access the Internet and forbids other users from accessing the Internet. This router supports manual binding and dynamic binding.

Click 『Security』 to go to the IP-MAC Binding configuration page.



After an "IP-MAC Binding" rule is added, the page is shown in the figure below.

IP-MAC Binding
?

IP-MAC Binding: Enable Disable

Binding List Note that a user mismatching with the IP-MAC binding rule cannot access the Internet.

<input type="checkbox"/>	IP Address	MAC Address	Remark	Action
<input type="checkbox"/>	192.168.0.159	c8:3a:35:d5:75:a6		

Dynamic Binding

<input type="checkbox"/>	IP Address	MAC Address	Action
<input type="checkbox"/>	192.168.0.159	c8:3a:35:d5:75:a6	Bind

Parameter description in the page:

Parameter	Description	
IP-MAC Binding	Enable/Disable the IP-MAC binding function. The default is Disable.	
Binding List	<input type="button" value="+Add"/>	Click this button to manually add bound IP and MAC addresses.
	<input type="button" value="Unbind"/>	Click this button to unbind a selected bound rule.
	IP Address	Displays a bound IP address.
	MAC Address	Displays a MAC address corresponding to a bound IP address.
	Remark	Displays the description of a corresponding rule. No remark information is displayed if it is not set during dynamic or manual binding.
Action	Perform the edit or delete action on a bound rule.	

Parameter		Description
Dynamic Binding	<input type="button" value="Bind"/>	Information about a client connected to the router is displayed in the dynamic list. Click this button to add a selected rule in the binding list.
	<input type="button" value="Bind All"/>	Click this button to add all rules in the dynamic list into the binding list.
	IP Address	Displays an IP address of a client connected to the router.
	MAC Address	Display a MAC address corresponding to an IP address of a client connected to the router.
	Action	Click Bind after a corresponding rule to quickly add this rule in the binding list.

Example of IP-MAC binding

- Example:** An enterprise uses a G3 enterprise router to establish a network. Only two employees in the recruitment team are allowed to access the Internet in office hours of the company. Other employees are forbidden from accessing the Internet. This can be achieved through the IP-MAC binding function. First of all, you must know the IP and MAC addresses of the recruiters who are allowed to access the Internet, i.e. 192.168.0.226, C8:3A:35:03:11:79 and 192.168.0.208, CC:3A:61:71:1B:6E.

Configuration steps:

- After going to the IP-MAC Binding page, Click **Enable** and **OK** to enable this function.

The screenshot shows the 'IP-MAC Binding' configuration interface. At the top, there is a toggle for 'IP-MAC Binding' which is currently set to 'Enable'. Below this, there is a 'Binding List' section with '+Add' and 'Unbind' buttons and a note: 'Note that a user mismatching with the IP-MAC binding rule cannot access the Internet.' The table below this is empty. In the 'Dynamic Binding' section, there are 'Bind' and 'Bind All' buttons. A table lists one dynamic binding rule with IP Address '192.168.0.159' and MAC Address 'c8:3a:35:d5:75:a6', and a 'Bind' button next to it. At the bottom of the page, the 'OK' button is highlighted with a red box.

- If a client to be bound has been connected to the router, find a corresponding device in the dynamic binding

list and click [Bind](#). If it is not connected to the router, click **Add**, enter IP and MAC address information to be bound, and click **OK**.

IP-MAC Binding
?

IP-MAC Binding: Enable Disable

Binding List Note that a user mismatching with the IP-MAC binding rule cannot access the Internet.

+Add
Unbind

<input type="checkbox"/>	IP Address	MAC Address	Remark	Action
No data!				

Dynamic Binding Bind Bind All

<input type="checkbox"/>	IP Address	MAC Address	Action
<input type="checkbox"/>	192.168.0.159	c8:3a:35:d5:75:a6	Bind

OK
Cancel

After addition is successful, the page is shown in the figure below.

IP-MAC Binding
?

IP-MAC Binding: Enable Disable

Binding List Note that a user mismatching with the IP-MAC binding rule cannot access the Internet.

+Add
Unbind

<input type="checkbox"/>	IP Address	MAC Address	Remark	Action
<input type="checkbox"/>	192.168.0.159	c8:3a:35:d5:75:a6		

Dynamic Binding Bind Bind All

<input type="checkbox"/>	IP Address	MAC Address	Action
<input type="checkbox"/>	192.168.0.159	c8:3a:35:d5:75:a6	Bind

OK
Cancel

4.6.2 Firewall

Firewall includes ARP Attack Defense, DDOS Defense, and IP Attack Defense.

ARP spoofing is that an attack host in the LAN sends ARP spoofing packets to replace records in the device ARP list with forged IP and MAC correspondence. This type of ARP attacks seriously affects internal communication in the LAN. Therefore, ARP protection technology is generated.

By sending a large number of request services to occupy excessive resources, DOS causes destination routers and servers to be busy in answering requests or waiting nonexistent connection replies so that legitimate user requests cannot be answered by servers. DDOS defense can prevent the WAN from performing port scanning and malicious attack on computers in the router or LAN to ensure their safe action.

IP attack defense allows the router to intercept packets with some special IP options as required and record the information about the host sending these packets in the IP option list.

Click 『Security』 > 『Firewall』 to go to the configuration page.

The screenshot displays the Tenda Firewall configuration interface. On the left is a navigation menu with 'Firewall' selected. The main content area is titled 'Firewall' and contains the following sections:

- ARP Attack Defense:**
 - Enable ARP Attack Defense: (ARP Attack Prevention/ARP Spoofing Prevention/ARP Broadcast Prevention)
 - ARP Broadcast Interval: s
- DDOS Defense:**
 - ICMP Flood Threshold: pps
 - UDP Flood Threshold: pps
 - SYN Flood Threshold: pps
- IP Attack Defense:**
 - IP Timestamp Option
 - IP Security Option
 - IP Stream Option
 - IP Record Route Option
 - IP Loose Source Route Option
 - Illegal IP Option
- Prohibit Ping WAN:**
 - Enable Disable

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

Parameter description in the page:

Parameter		Description
ARP Attack Defense	Enable ARP Attack Defense	Enable/Disable the ARP attack defense function.
	ARP Broadcast Interval	Time interval when the device sends ARP broadcast.
DDOS Defense	ICMP Flood Threshold	If a destination IP address receives ICMP request packets exceeding a specified quantity within 1s, it is supposed that this destination IP address is being attacked by ICMP Flood.
	UDP Flood Threshold	If a port of a destination IP address receives UDP packets exceeding a specified quantity within 1s, it is supposed that this port of this destination IP address is being attacked by UDP Flood.
	SYN Flood Threshold	If a port of a destination IP address receives TCP SYN packets exceeding a specified quantity within 1s, it is supposed that this port of this destination IP address is being attacked by SYN Flood.
IP Attack Defense	IP Timestamp Option	Whether to check that IP packets from a specified area contain the Internet Timestamp item.
	IP Security Option	Whether to check that IP packets from a specified area contain the Internet Security item.
	IP Stream Option	Whether to check that IP packets from a specified area contain the Stream ID item.
	IP Record Route Option	Whether to check that IP packets from a specified area contain the Record Route option.
	IP Loose Source Route Option	Whether to check that IP packets from a specified area contain the Loose Source option.
	Illegal IP Option	Whether to check the integrity or correctness of IP packets from a specified area.
Prohibit Ping WAN	After this item is enabled, other network devices in the network cannot ping a router WAN port successfully.	

4.7 AC Management

This router integrates the wireless controller function to manage Tenda APs.

AC Management includes the following contents:

[Discover AP](#): On this page, the router can discover compatible APs in the LAN network.

[Wireless Policy](#): On this page, you can add wireless policies for the managed APs. The parameters contain SSID-related parameters and radio parameters.

[Advanced Policy](#): On this page, you can add reboot policies and alarm policies for the managed APs. A reboot policy can make an AP reboot periodically or regularly, and enable or disable an AP's LED status. An alarm policy allows the system to send an AP's alarm information to a specified email address or to a specified IP address.

[AP Management](#): On this page, you can reboot, upgrade a firmware or reset the selected APs.

[Issue Policy](#): On this page, you can deliver the added policies to the selected APs.

[AP DHCP](#): On this page, you can set up the DHCP server for the managed APs. Note that the DHCP server and the device's LAN IP address must be on the same IP segment.

[User Status](#): On this page, you can see or export the information of online users that connect to the managed online APs.

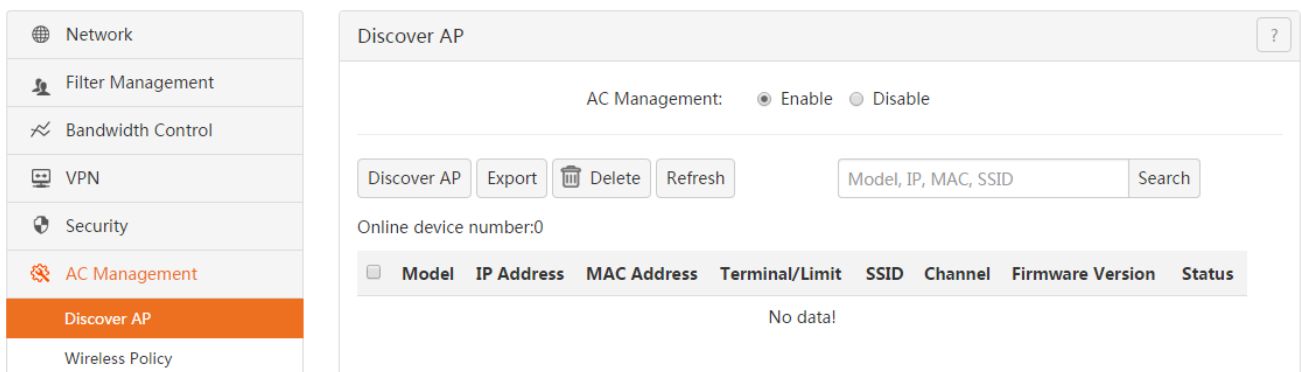
4.7.1 Discover AP

On this page, the router can discover compatible APs in the LAN network.

For the descriptions of button and parameters, click  on the upper right page.


To discover APs:

1. Log in to the device's web UI.
2. Go to **AC Management > Discover AP**.
3. Click **Discover AP**. The available APs will display in the list.



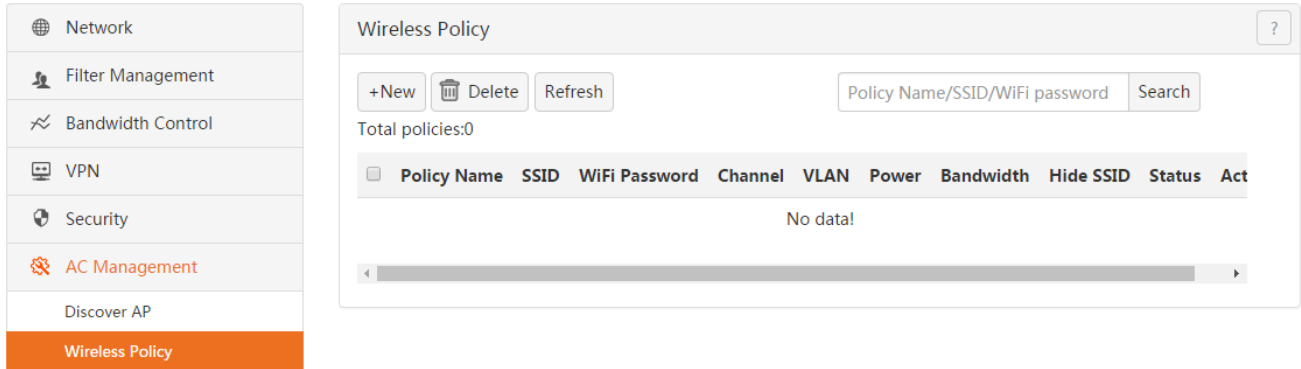
4.7.2 Wireless Policy

On this page, you can add wireless policies for the managed APs. The parameters contain SSID-related parameters and radio parameters.

For the descriptions of button and parameters, click  on the upper right page.

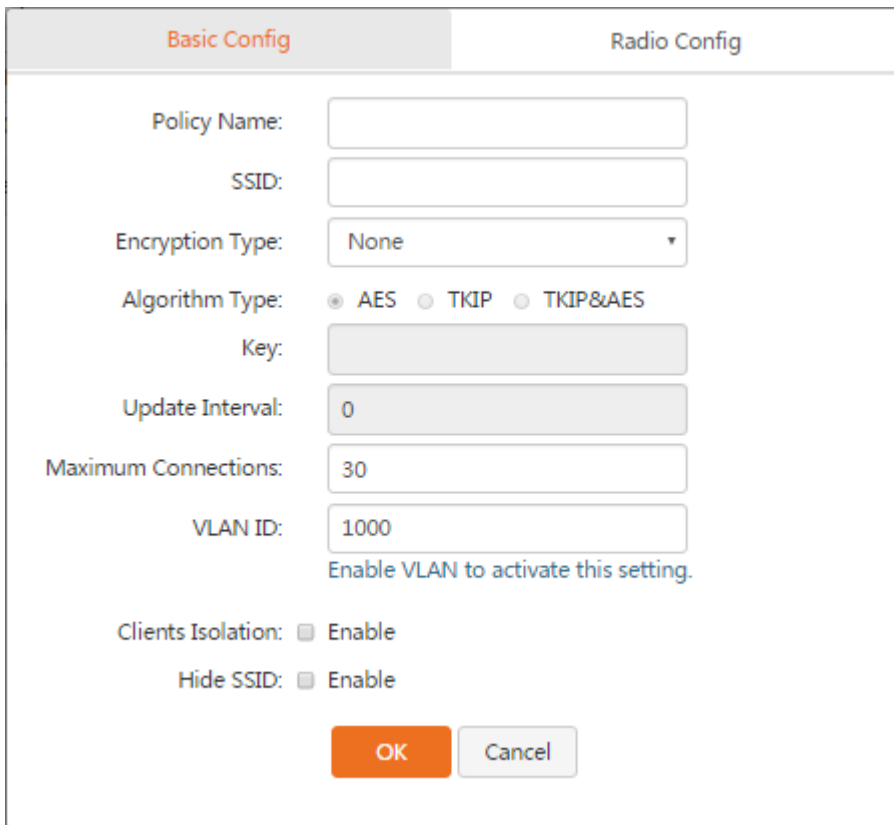
To add a wireless policy:

1. Log in to the device’s web UI.
2. Go to **AC Management > Wireless Policy**.
3. Click **New**.




4. On the pop-up window, set up the parameters and click **OK**. We recommend that you set up *Policy Name*, *SSID*, *Encryption Type*, and *Key*, and keep the default values of other parameters.

Note that if you set up *VLAN ID* for the policy, go to **Radio Config** page and check the box of *Enable VLAN*.



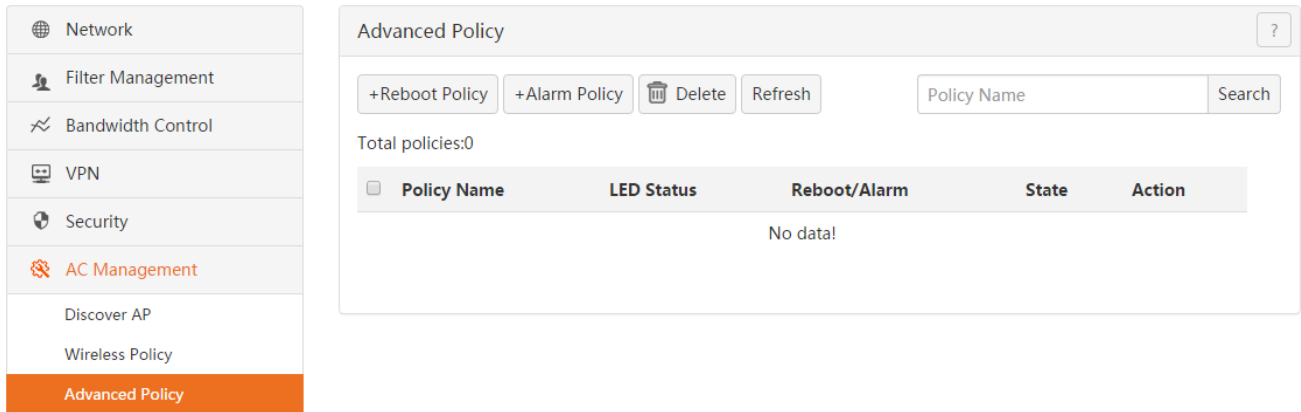
4.7.3 Advanced Policy

On this page, you can add reboot policies and alarm policies for the managed APs. A reboot policy can make an AP reboot periodically or regularly, and enable or disable an AP’s LED status. An alarm policy allows the system to send an AP’s alarm information to a specified email address or to a specified IP address.

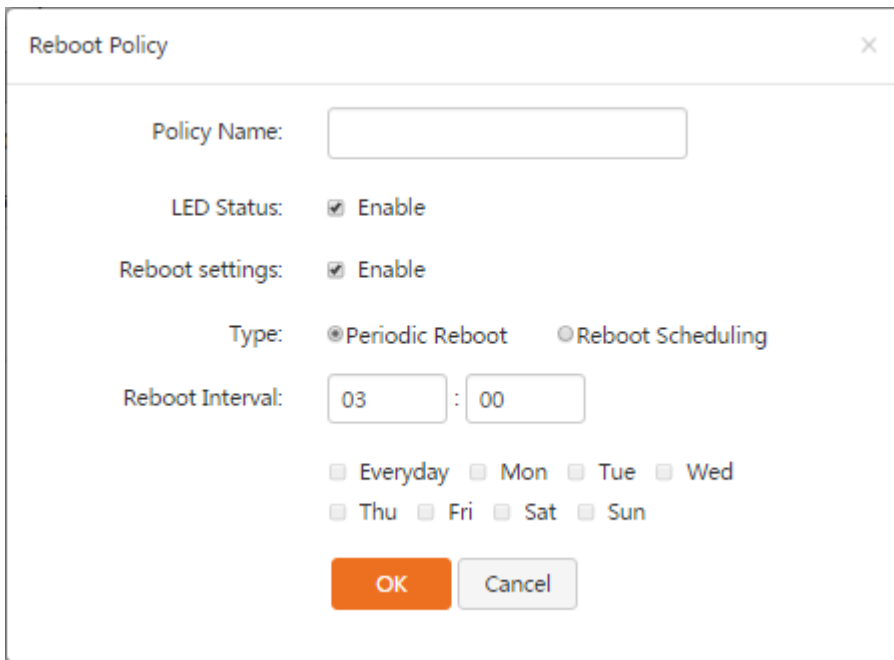
For the descriptions of button and parameters, click  on the upper right page.

To add a reboot policy:

1. Log in to the device’s web UI.
2. Go to **AC Management > Advanced Policy**.
3. Click **Reboot Policy**.



4. On the pop-up window, set up the parameters and click **OK**. You can enable or disable LED status. If you enable reboot settings, you can select *Periodic* or *Reboot Scheduling* to set up the parameters.



To add an alarm policy:

1. Log in to the device’s web UI.
2. Go to **AC Management > Advanced Policy**.
3. Click **Alarm Policy**.

4. On the pop-up window, set up the parameters and click **OK**.
 - If you enable and set up all the parameters, the alarm of AP traffic and AP accessing will be sent to the specified email and IP address.
 - If you enable *Alarm from Desktop*, you must install an alarm program on the computer. To get the program, contact our technical support engineer.

4.7.4 AP Management

On this page, you can reboot, upgrade a firmware or reset the selected APs.

For the descriptions of button and parameters, click  on the upper right page.

- Network
- Filter Management
- Bandwidth Control
- VPN
- Security
- AC Management
 - Discover AP
 - Wireless Policy
 - Advanced Policy
 - AP Management

AP Management

Reboot Upgrade Reset Delete Refresh


Model, MAC, SSID Search

Online device number:0

Model	MAC Address	Terminal/Limit	SSID	Channel	Firmware Version	State	Action
No data!							

4.7.5 Issue Policy

On this page, you can deliver the added policies to the selected APs.

For the descriptions of button and parameters, click  on the upper right page.

- Network
- Filter Management
- Bandwidth Control
- VPN
- Security
- AC Management
 - Discover AP
 - Wireless Policy
 - Advanced Policy
 - AP Management
 - Issue Policy

Issue Policy

Wireless Settings Advanced Settings Default Delete


Model/MAC/SSID Search

Online device numbers:0

Model	MAC Address	SSID	LED Status	Reboot Status	Alarm Status	Status
No data!						

4.7.6 AP DHCP

On this page, you can set up the DHCP server for the managed APs. Note that the DHCP server and the device's LAN IP address must be on the same IP segment.

For the descriptions of button and parameters, click  on the upper right page.

4.7.7 User Status

On this page, you can see or export the information of online users that connect to the managed online APs.

For the descriptions of button and parameters, click  on the upper right page.

4.8 Captive Portal

Captive Portal includes the following contents:

[Basic Setup](#): Set information about captive portal. This router supports captive portal and PPPoE authentication. Only one of them can be selected when the authentication function is enabled.

[User Management](#): Add username and password of captive portal.

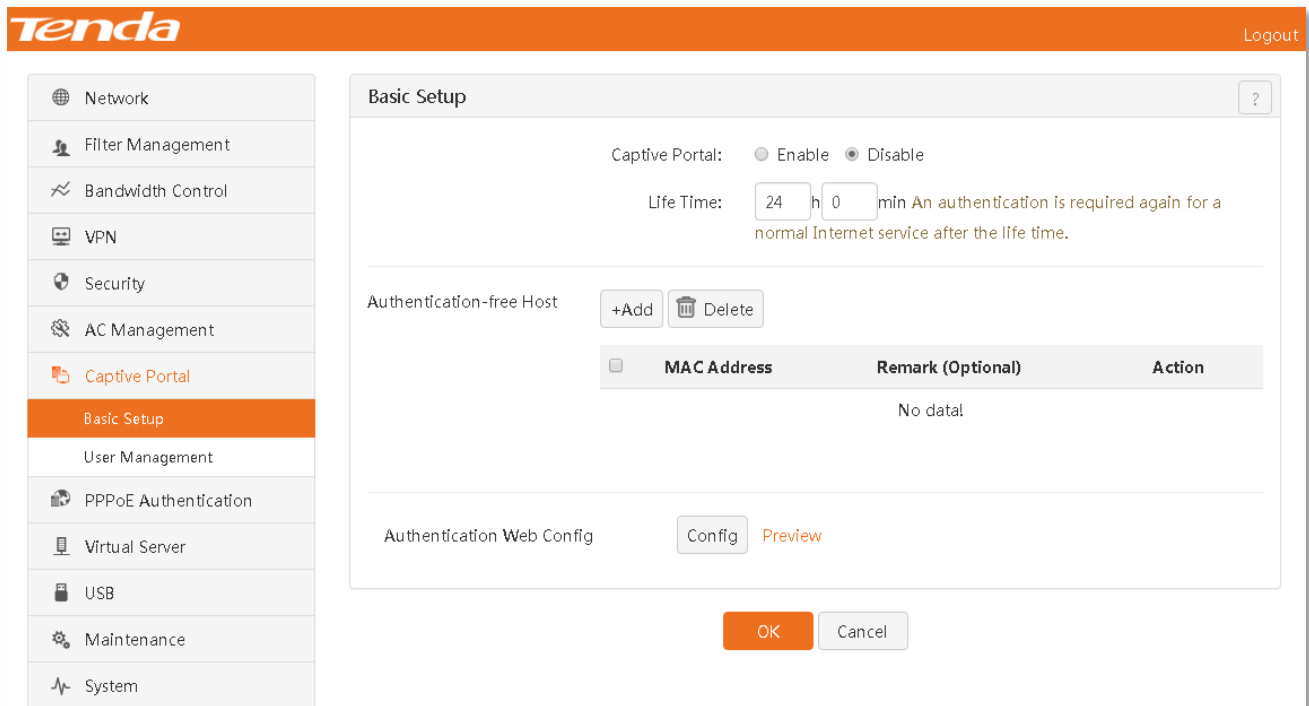
[Example of Captive Portal](#): Explain captive portal application through the example that the user performs captive portal to access the Internet.

4.8.1 Basic Setup

Overview

By default, a client connected to the router can access the Internet after the router is connected to the Internet. After the captive portal function is enabled, any client under the router must be authenticated before accessing the Internet.

Click 『Captive Portal』 to go to the Basic Setup page.


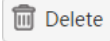



The screenshot shows the Tenda router's web interface. The top navigation bar is orange with the Tenda logo on the left and a 'Logout' link on the right. A left sidebar contains a list of menu items: Network, Filter Management, Bandwidth Control, VPN, Security, AC Management, Captive Portal (highlighted in orange), Basic Setup (highlighted in orange), User Management, PPPoE Authentication, Virtual Server, USB, Maintenance, and System. The main content area is titled 'Basic Setup' and contains the following configuration options:

- Captive Portal:** Radio buttons for 'Enable' and 'Disable'. 'Disable' is selected.
- Life Time:** Input fields for '24' hours and '0' minutes. A note states: 'An authentication is required again for a normal Internet service after the life time.'
- Authentication-free Host:** '+Add' and 'Delete' buttons.
- Table:** A table with columns 'MAC Address', 'Remark (Optional)', and 'Action'. The table is currently empty, showing 'No data!'.
- Authentication Web Config:** 'Config' and 'Preview' buttons.

At the bottom of the configuration area are 'OK' and 'Cancel' buttons.

Parameter description in the page:

Parameter	Description
Captive Portal	Enable/Disable the captive portal function.
Life Time	After the client passes the authentication and successfully accesses the Internet, Once the life time is over, an authentication is required again for normal Internet service.
Authentication-free Host	 Click this button to add a client that can access the Internet without any authentication.
	 Click this button to delete a selected authentication-free host.
Authentication-free Host (continued)	Mac Address Display a MAC address of a client that can access the Internet without any authentication.
	Remark Description of a client that can access the Internet without any authentication. No description is displayed if it is not filled during setting.
	Action Perform the reedit or delete action on a corresponding rule.
Authentication Web Config	 Click this button to configure a page that appears during client authentication.
	Preview Click to preview a set "Configuration Web".

Enable captive portal

Select Enable in the Captive Portal option and click **OK** to enable captive portal. If necessary, you can configure Authentication-free Host and Authentication Web Config.

Basic Setup
?

Captive Portal: Enable Disable

Life Time: h min An authentication is required again for a normal Internet service after the life time.

Authentication-free Host +Add

<input type="checkbox"/>	MAC Address	Remark (Optional)	Action
No data!			

Authentication Web Config Preview

4.8.2 User Management

Overview

This section describes how to add a username and password to be entered during captive portal of a client. Click 『Captive Portal』 > 『User Management』 to go to the configuration page.

Tenda
Logout

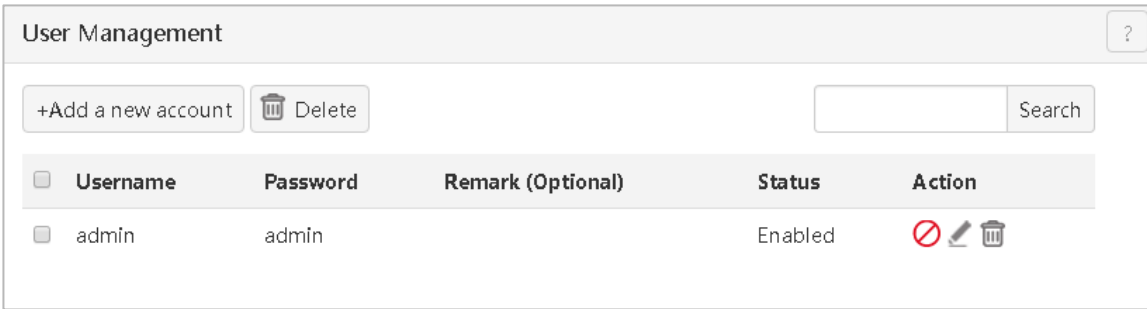
- Network
- Filter Management
- Bandwidth Control
- VPN
- Security
- AC Management
- Captive Portal
- Basic Setup
- User Management
- PPPoE Authentication
- Virtual Server
- USB
- Maintenance

User Management
?

+Add a new account

<input type="checkbox"/>	Username	Password	Remark (Optional)	Status	Action
No data!					

After an account is successfully added, the page is shown in the figure.



Parameter description in the page:

Parameter	Description
	Click this button to add an account for captive portal.
	Click this button to delete a selected captive portal account.
Username/Password	Username/Password to be entered during captive portal of a client.
Remark	Display the description of a corresponding account. No description is displayed if it is not filled during setting.
Status	User's current status including enabled and disabled.
Action	Perform the enable/disable, edit, and delete actions on a rule.

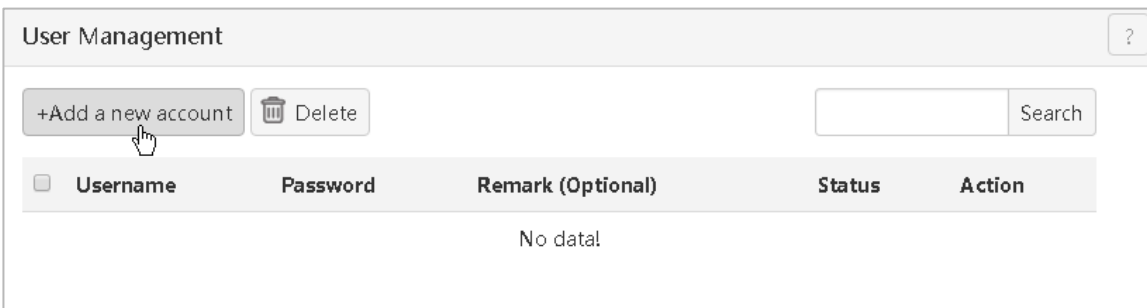


Tip

One account (username and password) shall not be subject to multiple user authentications at the same time.

Steps for adding a captive portal account

- 1) Go to the User Management page and click .



- 2) Set user information in the window that appears.

Add a new account
✕

Username	Passwork	Remark (Optional)	Action
<input type="text" value="admin"/>	<input type="text" value="admin"/>	<input type="text"/>	<input type="button" value="+"/> <input type="button" value="-"/>

After a captive portal account is successfully added, the page is shown in the figure below.

User Management
?

<input type="checkbox"/>	Username	Password	Remark (Optional)	Status	Action
<input type="checkbox"/>	admin	admin		Enabled	<input type="button" value="⊘"/> <input type="button" value="✎"/> <input type="button" value="🗑"/>

4.8.3 Example of Captive Portal Configuration

■ **Example:** An enterprise uses a G3 enterprise router to establish a network. The company specifies that an authentication is required when employees access the Internet in office hours. However, the network administrator needs no authentication. This can be achieved through the captive portal function. The MAC address of the network administrator's computer is CC:3A:61:71:1B:6E.

Configuration steps:

Step 1: Perform basic settings of captive portal.

1) Click **Enable** and **OK** to enable the captive portal function.

Basic Setup
?

Captive Portal: **Enable** Disable

Life Time: h min An authentication is required again for a normal Internet service after the life time.

Authentication-free Host

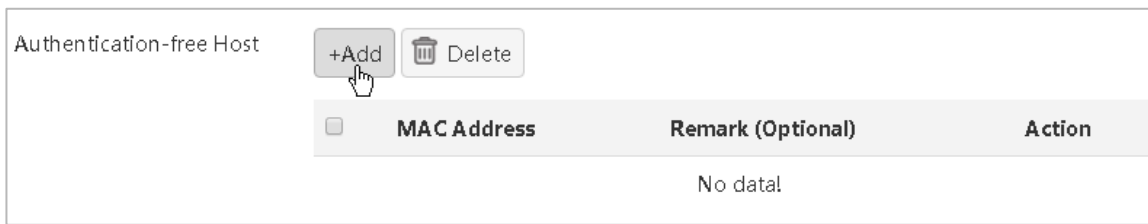
<input type="checkbox"/>	MAC Address	Remark (Optional)	Action
No data!			

Authentication Web Config

Preview

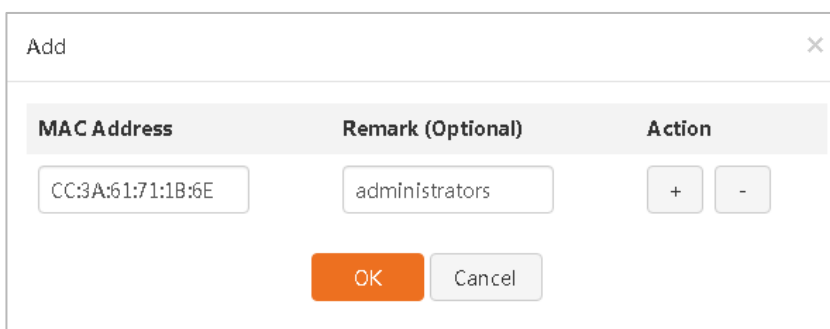
2) Add an authentication-free host.

Click .



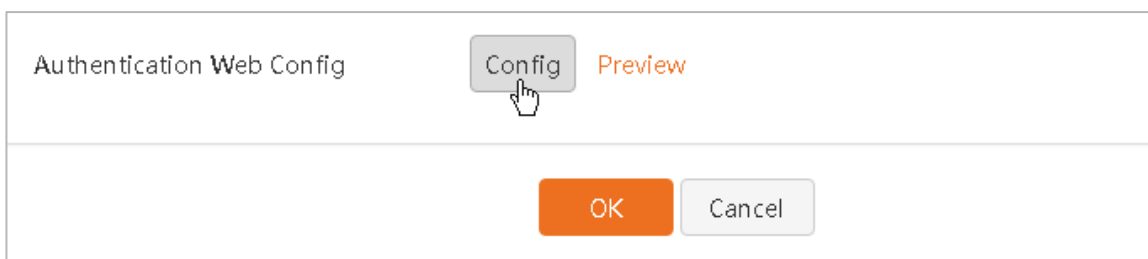
Set host contents in the window that appears.

- **MAC Address:** Enter a MAC address of a client that can access the Internet without any authentication.
- **Remark:** Enter remark about this client (Optional).
- Click **OK**.



3) Set authentication page information.

Click .



Set relevant information in the window that appears.

- **Web Title:** Modify the title of the captive portal page.
- **Web Content:** Set announcement contents such as Shenzhen Tenda Technology Co., Ltd.
- Click **OK**.

Authentication Web Config

Web Title: Welcome to Tenda network work

Web Content: Shenzhen Tenda Technology Co., Ltd. 35/256

OK Cancel

After settings are finished, the page is shown in the figure below.

Basic Setup

Captive Portal: Enable Disable

Life Time: 24 h 0 min An authentication is required again for a normal Internet service after the life time.

Authentication-free Host

+Add Delete

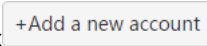
<input type="checkbox"/>	MAC Address	Remark (Optional)	Action
<input type="checkbox"/>	CC:3A:61:71:1B:6E	administrators	

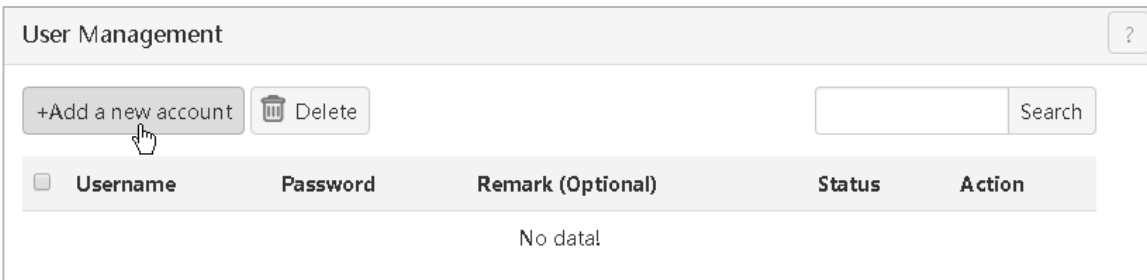
Authenticatoin Web Config

Config Preview

OK Cancel

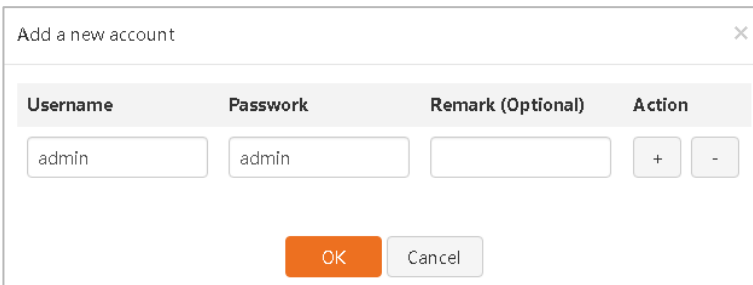
Step 2: Add a captive portal account.

Go to the User Management page and click .

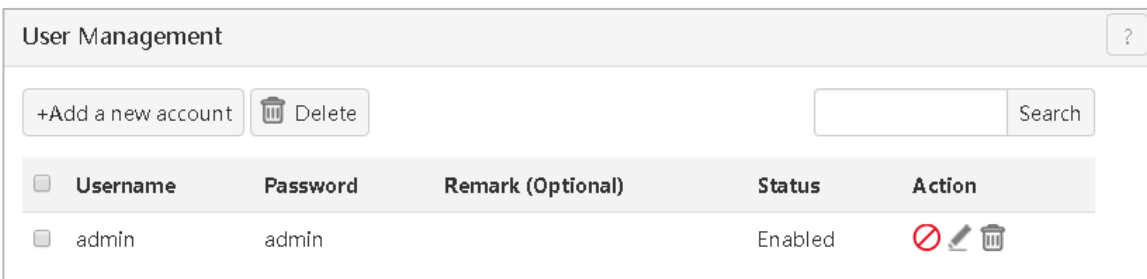


Set user information in the window that appears.

- **Username, Password:** Set a user name and password for captive portal.
- **Remark:** Enter the description of this user (optional).
- Click **OK** to finish settings.

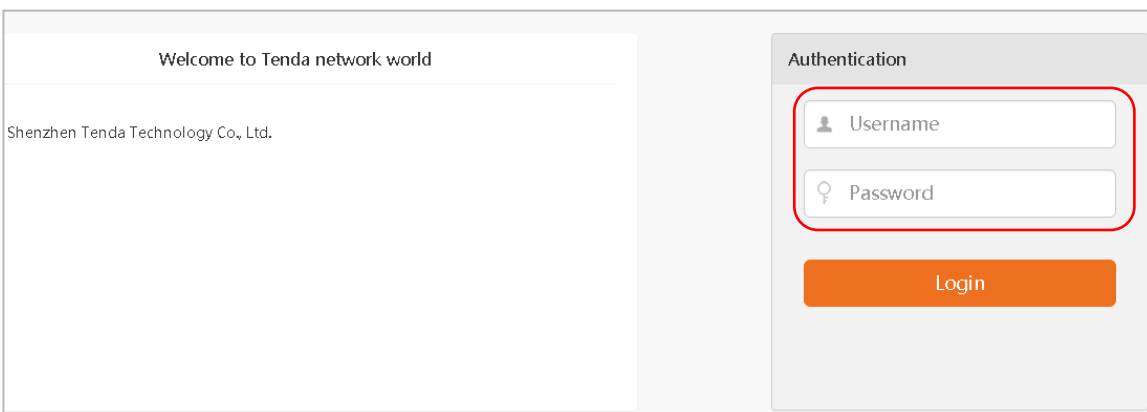


After a captive portal account is successfully added, the page is shown in the figure below.



The page below will appear when the client accesses the Internet or Intranet after settings are finished.

At this point, enter the added captive portal account and click **Login**.



4.9 PPPoE Authentication

PPPoE Authentication includes the following contents:

[Basic Setup](#): Set information about PPPoE authentication. This router supports captive portal and PPPoE authentication. Only one of them can be selected when the authentication function is enabled.

[Account Management](#): Add a user name and password for PPPoE authentication.

[Example of PPPoE Authentication](#): Explain PPPoE authentication application through the example that a user in the community performs dial-up networking.

4.9.1 Basic Setup

Overview

By default, a client connected to the router can access the Internet after the router is connected to the Internet. After the PPPoE authentication is enabled, any client under the router must perform PPPoE authentication before accessing the Internet. After PPPoE authentication is enabled, captive portal functions will be disabled.




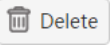
Click 『[PPPoE Authentication](#)』 to go to the Basic Setup page. Drag the scroll bar to view more information.


The screenshot shows the Tenda router's web interface. The left sidebar contains navigation options: Network, Filter Management, Bandwidth Control, VPN, Security, AC Management, Captive Portal, PPPoE Authentication (highlighted), Basic Setup (highlighted), Account Management, Virtual Server, USB, Maintenance, and System. The main content area is titled 'Basic Setup' and contains the following configuration options:

- PPPoE Server**: PPPoE Authentication: Enable Disable
- Server IP:
- Start IP of PPPoE user:
- End IP of PPPoE user:
- Preferred DNS:
- Alternate DNS: (Optional)
- Expiry Alert: Alert me ahead of:
- Alert Page for Account Due: [Preview](#)
- Alert Page for Account Expiry: [Preview](#)

At the bottom, there is an 'Authentication-free' section with '+Add' and 'Delete' buttons. Below this is a table header with columns: MAC Address, Remark (Optional), and Action.

Parameter description in the page:

Parameter		Description
PPPoE Server	PPPoE Authentication	Enable/Disable the PPPoE authentication function.
	Server IP	PPPoE server IP address.
	Start/End IP of PPPoE user	IP address range assigned to the client by the PPPoE server after the client performs PPPoE authentication.
	Preferred/Alternate DNS	Preferred/Alternate DNS address assigned to the client by the PPPoE server after the client performs PPPoE authentication.
Expiry Alert	Alert time before expiry.	Set alert time before the expiry of the account. The default is 7 days .
	Alert Page for Account Due	Set alert page information before the expiry of the account. Click  to configure alert page information. Click Preview to view effects.
	Alert Page for Account Expiry	Set alert page information after the expiry of the account. Click  to configure alert page information. Click Preview to view effects.
Authentication-free		Click this button to add a client that can access the Internet without any authentication.
		Click this button to delete a selected authentication-free host.
	Mac Address	Display a MAC address of a client that can access the Internet without any authentication.
	Remark	Description of a client that can access the Internet without any authentication. No description is displayed if it is not filled during setting.
	Action	Perform the reedit or delete action on a corresponding rule.

Parameter		Description
Flow Control Config	Policy Name	Flow policy name. It cannot be modified. After the PPPoE authentication function is enabled, the original "Bandwidth Control" function of the router will be replaced with PPPoE "Flow Control Config".
	Uplink/Downlink	Uplink/Downlink rate of corresponding policies. These policies will be associated with a PPPoE account. The maximum uplink/downlink rate of the user who uses this account to perform authentication is this rate.
	Action	Click  to modify an uplink/downlink rate. The default is 1,024KB/s. 1Mbps=128KB/s=1,024kb/s, 1B=8b

Enable PPPoE authentication

Select **Enable** in the **PPPoE Authentication** option and click **OK** at the bottom of the page to enable PPPoE authentication. If necessary, you can configure **Expiry Alert** and **Authentication-free**.

Basic Setup

?

PPPoE Server

PPPoE Authentication: Enable Disable

Server IP:

Start IP of PPPoE user:

End IP of PPPoE user:

Preferred DNS:

Alternate DNS:
(Optional)

Expiry Alert

Alert me ahead of: ▼

Alert Page for Account Due: [Preview](#)

Alert Page for Account Expiry: [Preview](#)

Authentication-free

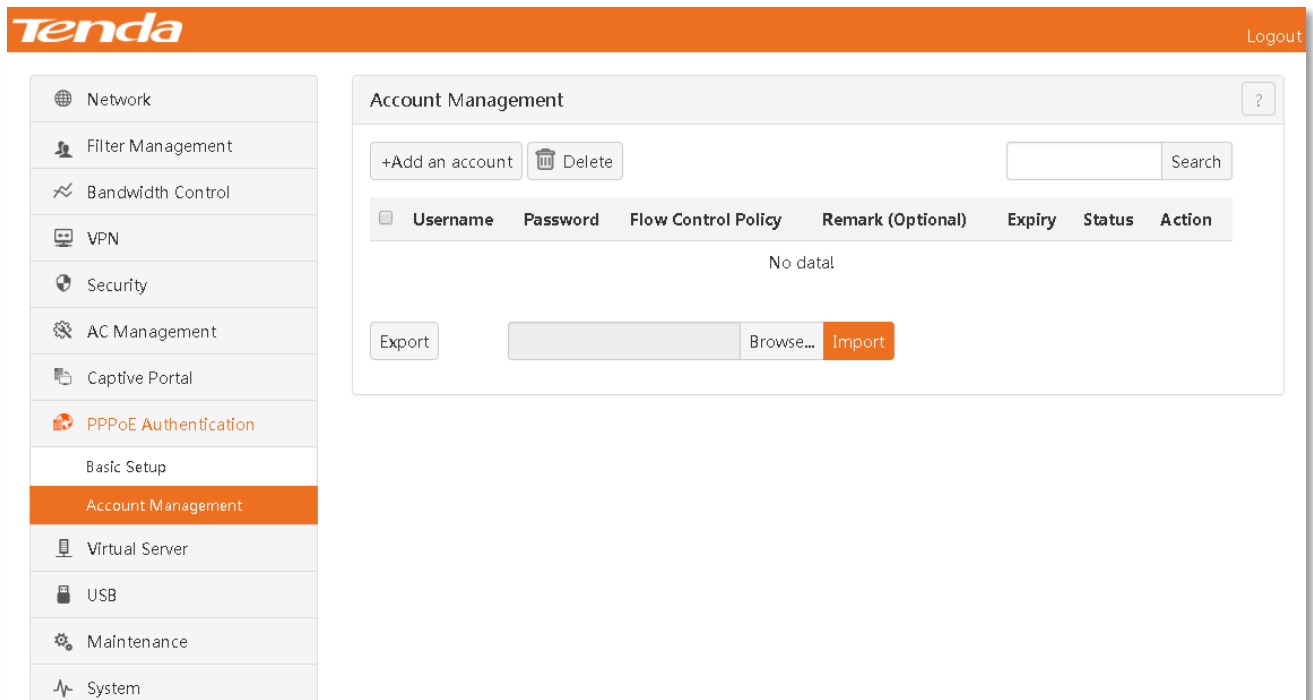
<input type="checkbox"/>	MAC Address	Remark (Optional)	Action
No data!			

4.9.2 Account Management

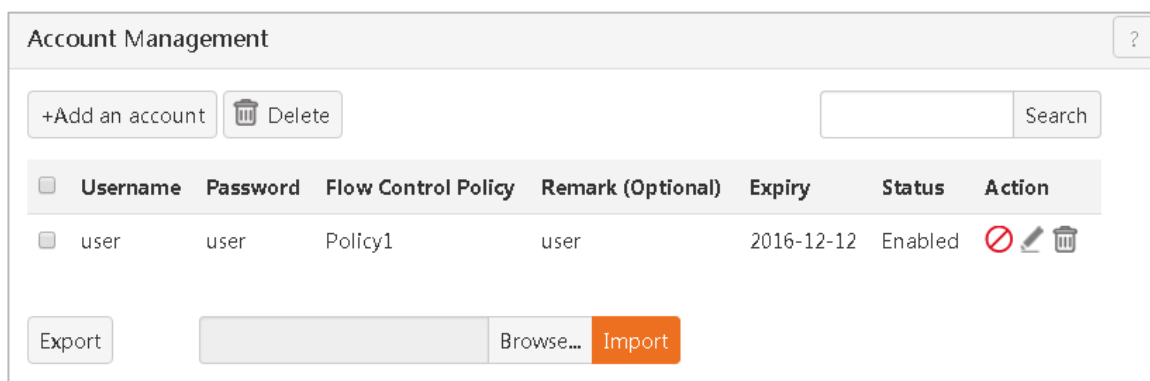
Overview

This section describes how to add a user name and password to be entered when a client performs PPPoE authentication.

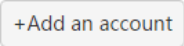
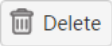



Click 『PPPoE Authentication』 > 『Account Management』 to go to the configuration page.



After an account is successfully added, the page is shown in the figure below:



Parameter description in the page:


Parameter	Description
	Click this button to add an account for PPPoE Authentication.
	Click this button to delete a selected PPPoE Authentication account.
Username/Password	Username/Password to be entered during PPPoE Authentication of a client.
Flow Control Policy	Flow control policy corresponding to this account.
Remark	Display the description of a corresponding account. No description is displayed if it is not filled during setting.
Expiry	Account expiry date.
Status	User's current status including enabled and disabled.
Action	Perform the enable/disable, edit, and delete actions on a rule.
	Click this button to export PPPoE user configuration files with cfg suffix. After an account is added, it is recommended to export this data to ensure that there is data to import without re-adding it when PPPoE user data is lost.
	Click to load exported PPPoE user data.
	Import loaded PPPoE user data into the device.

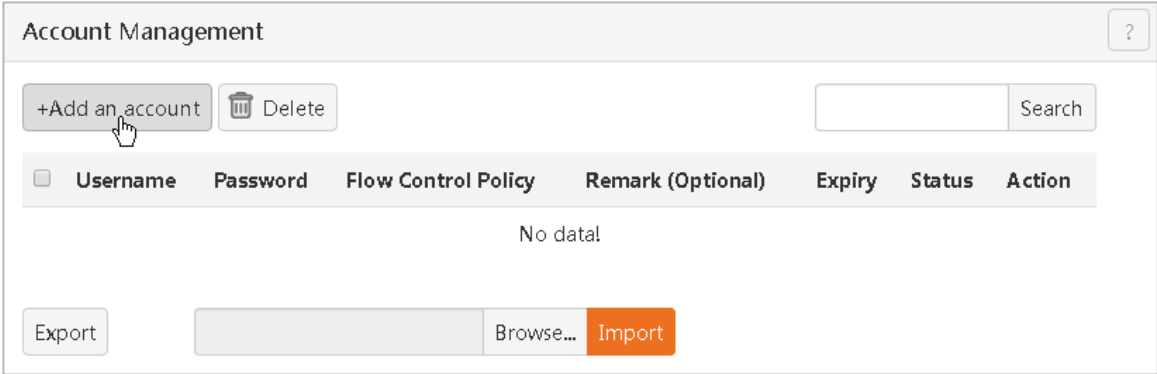


Tip

One account (username and password) shall not be subject to multiple user authentications at the same time.

Steps for adding a PPPoE account

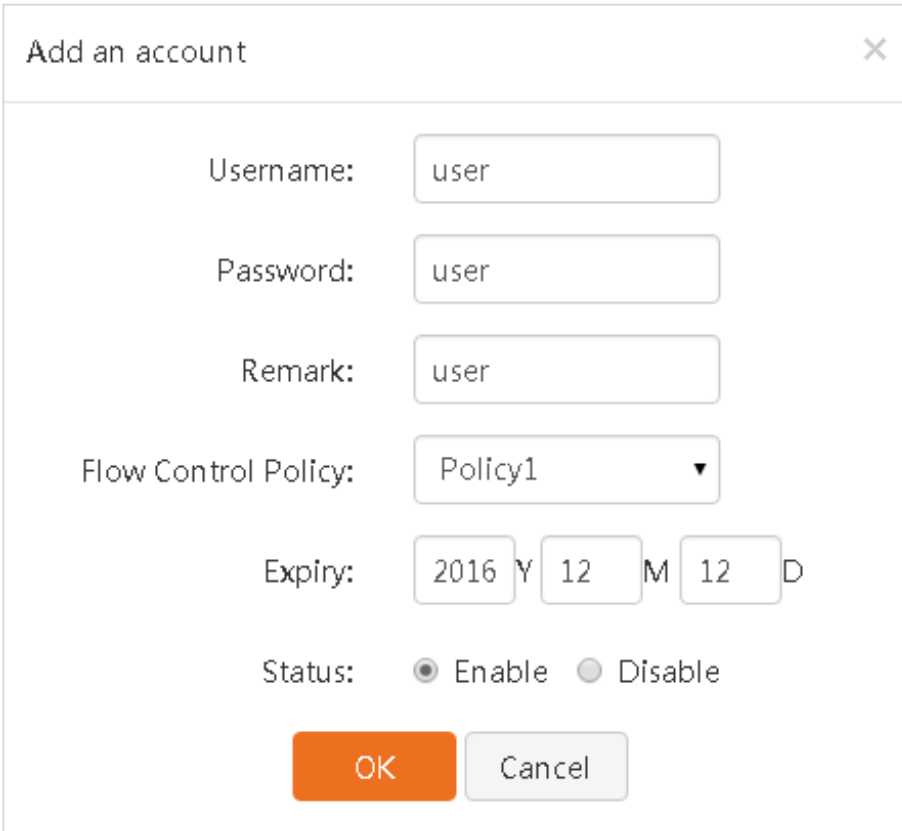
1) Click .



The screenshot shows the 'Account Management' window. At the top left, there is a '+Add an account' button with a mouse cursor over it, and a 'Delete' button with a trash icon. To the right is a search box with the text 'Search'. Below these is a table header with columns: Username, Password, Flow Control Policy, Remark (Optional), Expiry, Status, and Action. The table body is empty, displaying 'No data!'. At the bottom, there is an 'Export' button, a 'Browse...' button, and an 'Import' button.

2) Set an account and password in the window that appears.

- **Username**、**Password**: Set a username and password for PPPoE authentication.
- **Remark**: Set the description of this account (Optional).
- **Flow Control Policy**: Select a flow control policy for this account.
- **Expiry**: Set an expiry date for this account.
- Click **OK**.



The screenshot shows the 'Add an account' dialog box. It contains the following fields and controls:

- Username:
- Password:
- Remark:
- Flow Control Policy: ▼
- Expiry: Y M D
- Status: Enable Disable
- Buttons:

4.9.3 Example of PPPoE Authentication Configuration

- Networking Requirements:** A community uses a G3 enterprise router to establish a network. This network has successfully accessed the Internet. The community administrator does not allow renters to establish a network. The administrator wants to assign an Internet account and password to every renter. The Internet can be accessed by automatically obtaining an IP address without entering an account and password.
- Requirement Analysis:** The community administrator can enable the PPPoE server through the PPPoE authentication function of G3, add accounts and passwords (assigned to renters), and set his own computer to **Authentication-free**.

Configuration steps:

Step 1: Set basic setup for PPPoE authentication.

1) Click **Enable** and **OK** at the bottom of the page to enable the PPPoE authentication function.

Basic Setup ?

PPPoE Server

PPPoE Authentication: **Enable** Disable

Server IP:

Start IP of PPPoE user:

End IP of PPPoE user:

Preferred DNS:

Alternate DNS:

(Optional)

2) Set account expiry alert information that the client will receive.

Click Config.

Expiry Alert

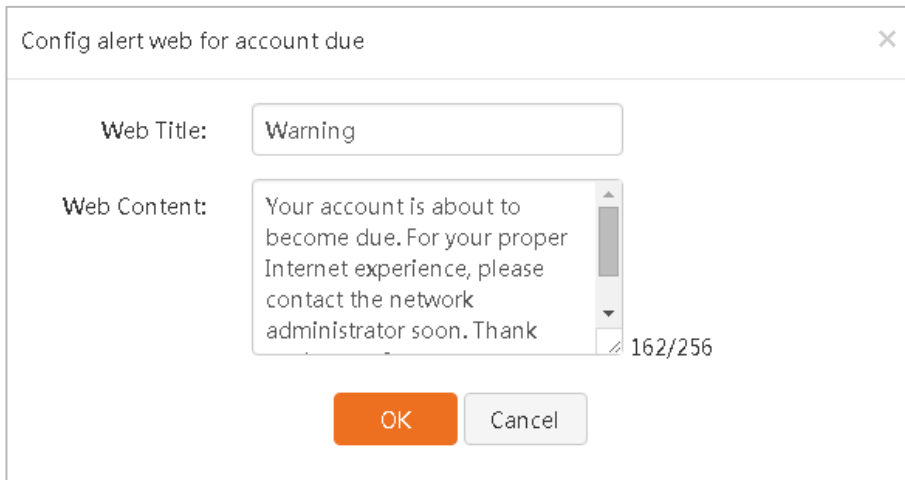
Alert me ahead of:

Alert Page for Account Due: Config Preview

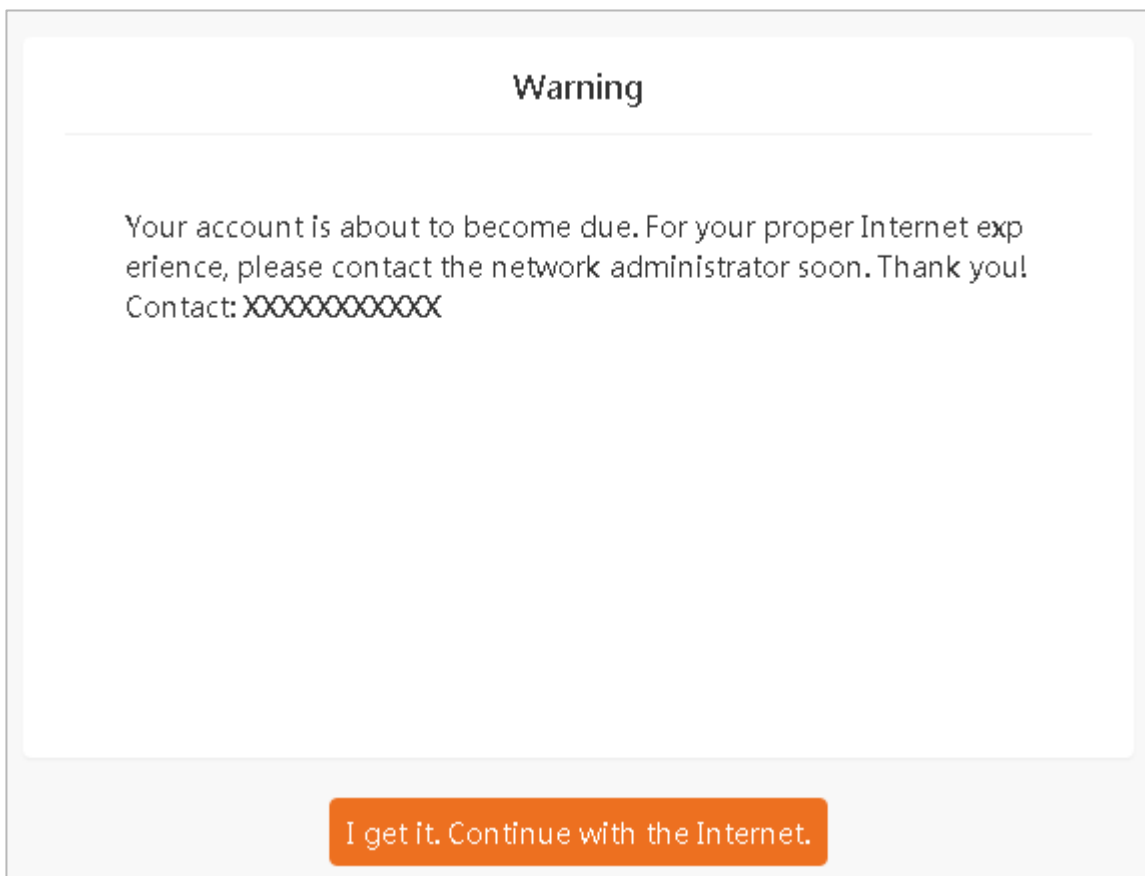
Alert Page for Account Expiry: Config Preview

Set alert contents in the window that appears.

- **Web Title:** You can modify title contents.
- **Web Content:** You can modify announcement contents.
- Click **OK**.



After settings are finished, go back to the Basic Setup page. At this point, click **Preview** to view setting effects, as shown in the figure below.



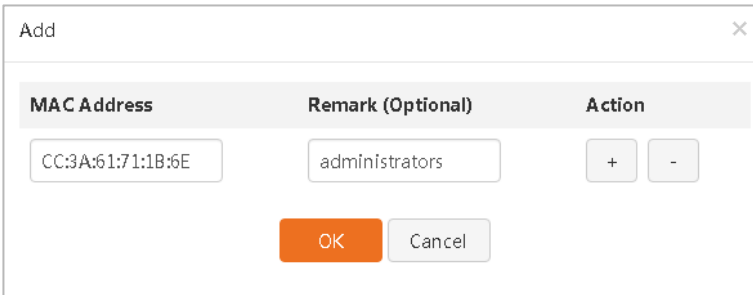
3) Add an authentication-free host. In this example, this host is the community administrator's computer. Assume that its MAC address is CC:3A:61:71:1B:6E.

Click .

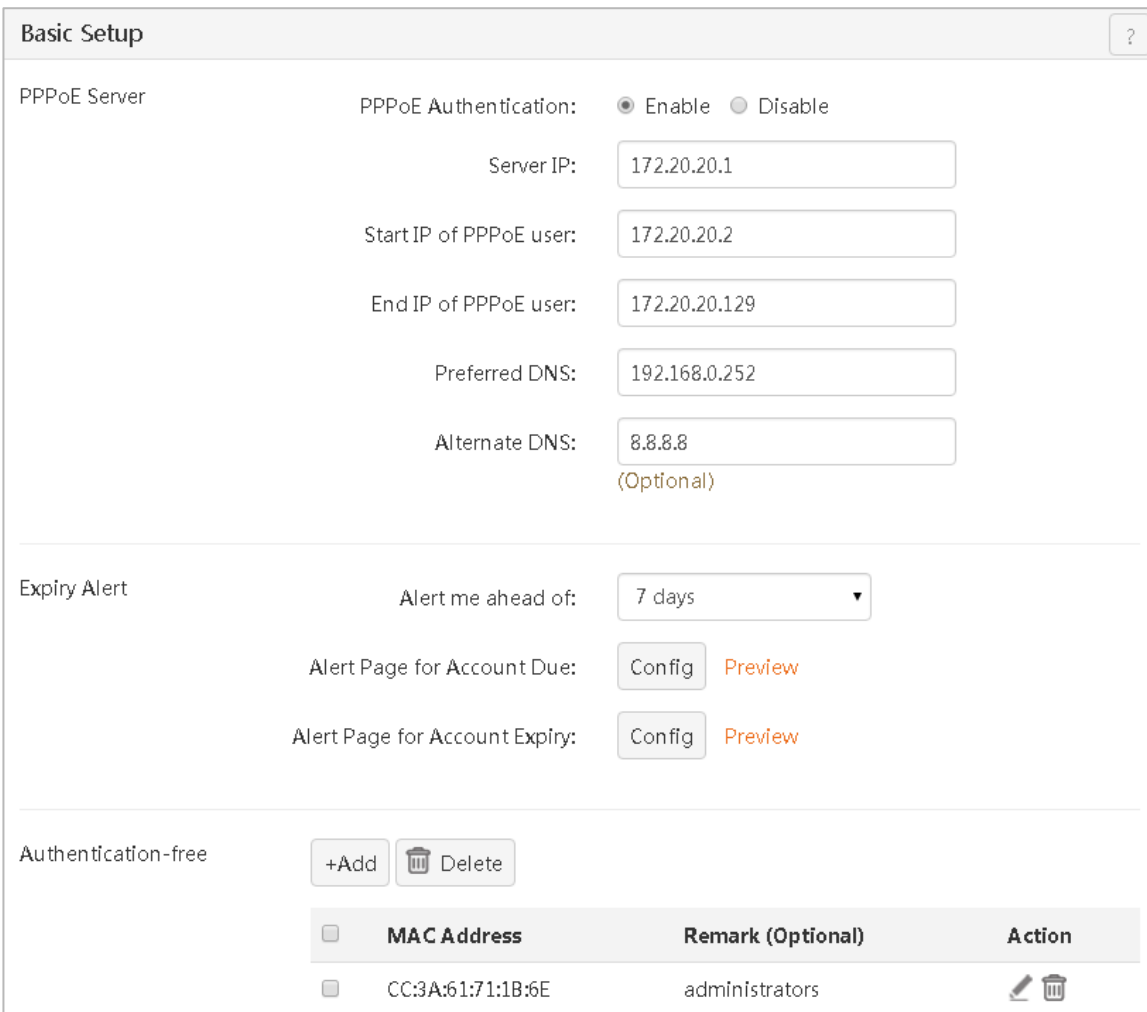


Set host contents in the window that appears.

- **MAC Address:** Enter a MAC address of a client that can access the Internet without any authentication.
- **Remark:** Enter remark about this client (Optional).
- Click **OK**.



After settings are finished, the page is shown in the figure below.



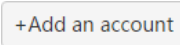
Step 2: Add a PPPoE user IP range (PPPoE user address IP to end IP) in the IP group. The default is 172.20.20.2 to 172.20.20.129. For detailed configuration steps, refer to [Steps for adding an IP group](#).



Tip

If you don't enable the IP Group functions of the router, skip this step.

Step 3: Add a PPPoE authentication account.

Go to the Account Management page and click .

Set user information in the window that appears.

1 — Set a username and password for PPPoE authentication.

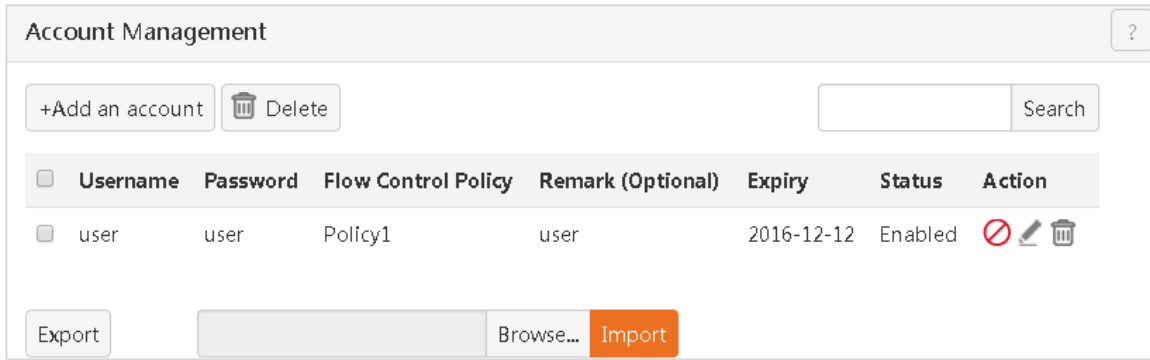
2 — Set the description of this account (Optional).

3 — Select a flow control policy for this account.

4 — Set an expiry date for this account.

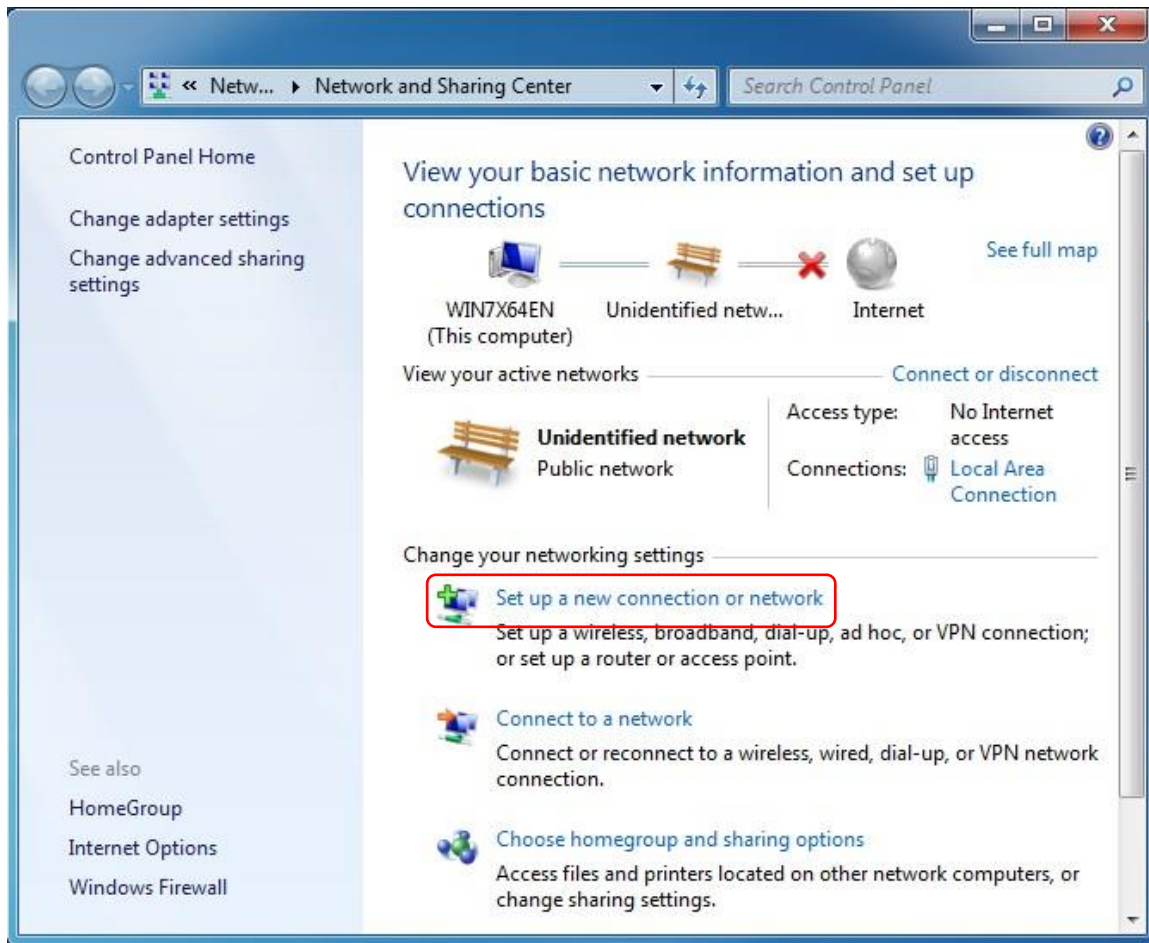
5 — Click **OK**.

After the account is successfully added, the page is shown in the figure below.

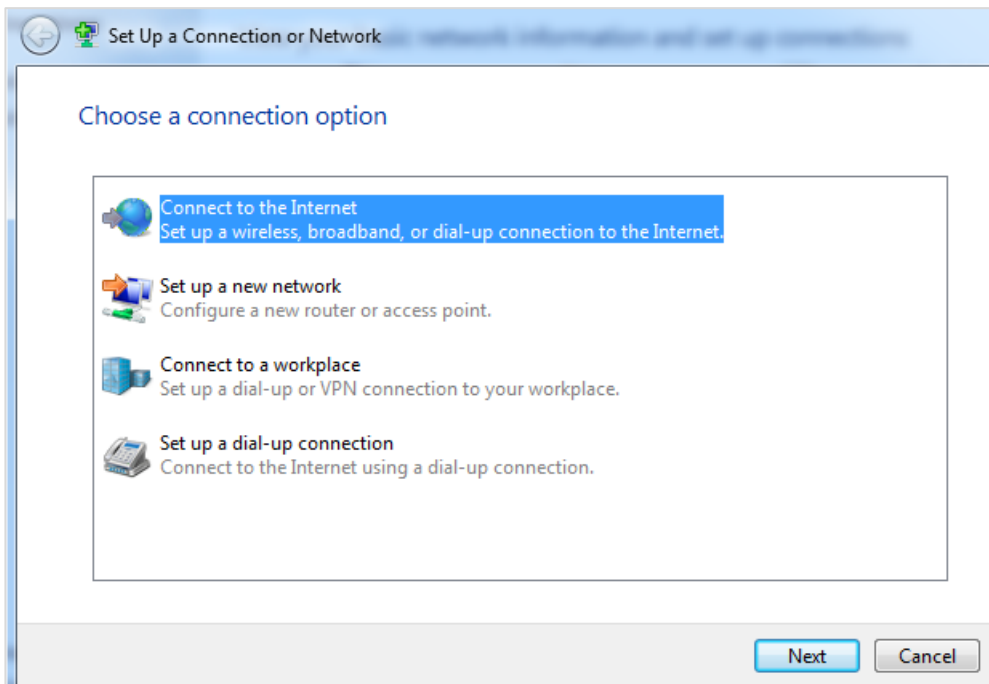


Step 4: The client performs dial-up networking (Take Windows 7 as an example).

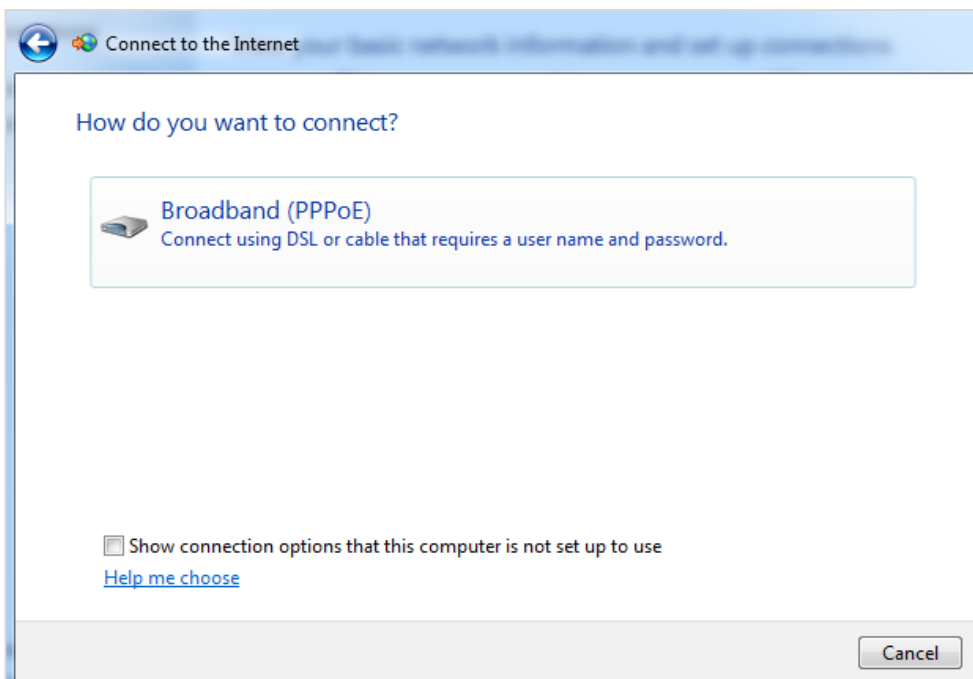
- 1 Click the start icon at the bottom left of the desktop.
- 2 Click **Control Panel > Network and Internet > Network and Sharing Center > Set up a new connection or network**.



3 Select Connect to **Internet** and click **Next**.



4 Click **Broadband**.



- 5 Fill in a **Username and Password** for PPPoE authentication (In this example, zhangsan for both), check Remember this password **(R)**, and click **Connect**.

Wait a moment, and the dial-up is successful. If you want to go to the broadband connection interface, after startup, find and click the network icon at the bottom right and then click Broadband Connection to normal access the Internet.

4.10 Virtual Server

Virtual Server includes the following contents:

[Port Forwarding](#): Allow Internet users to access Intranet resources.

[UPnP](#): Automatically realize forwarding between WAN and LAN ports. It is recommended to keep default settings.

[DMZ Host](#): Allows a computer in the Intranet to realize two-way unlimited communication with the Internet.

[DDNS](#): Allow a changing WAN IP address of the router to establish a forwarding relation with a fixed domain name. When performing remote access, the user needs only to access this domain name.

4.10.1 Port Forwarding

Overview

By default, the host in the WAN cannot actively access the host in the LAN. Port forwarding enables users in the WAN to access the host in the LAN and protects the interior of the LAN against invasion. Port forwarding defines a service port and uses an IP address to specify its corresponding LAN server. The router locates to this server the service request on this port from the WAN.

Click 『Virtual Server』 to go to the Port Forwarding page.

After a rule is successfully added, the page is shown in the figure below.

Parameter description in the page:

Parameter	Description
	Click this button to add a port forwarding rule.
	Click this button to delete a selected port forwarding rule.
Intranet Host IP	IP address of the Intranet server computer.
Intranet Port	Service port of the Intranet server.
Extranet Port	Router port open to Internet users to access.
Protocol	Protocol type of a corresponding service. If you are uncertain of service protocol types during settings, you are recommended to select All .
Line	WAN port for Intranet service forwarding, i.e. WAN port used when the Extranet accesses the Intranet server.
Status	Status of this rule, including Enabled and Disabled .
Action	Perform the enable/disable, edit, and delete actions on a rule.

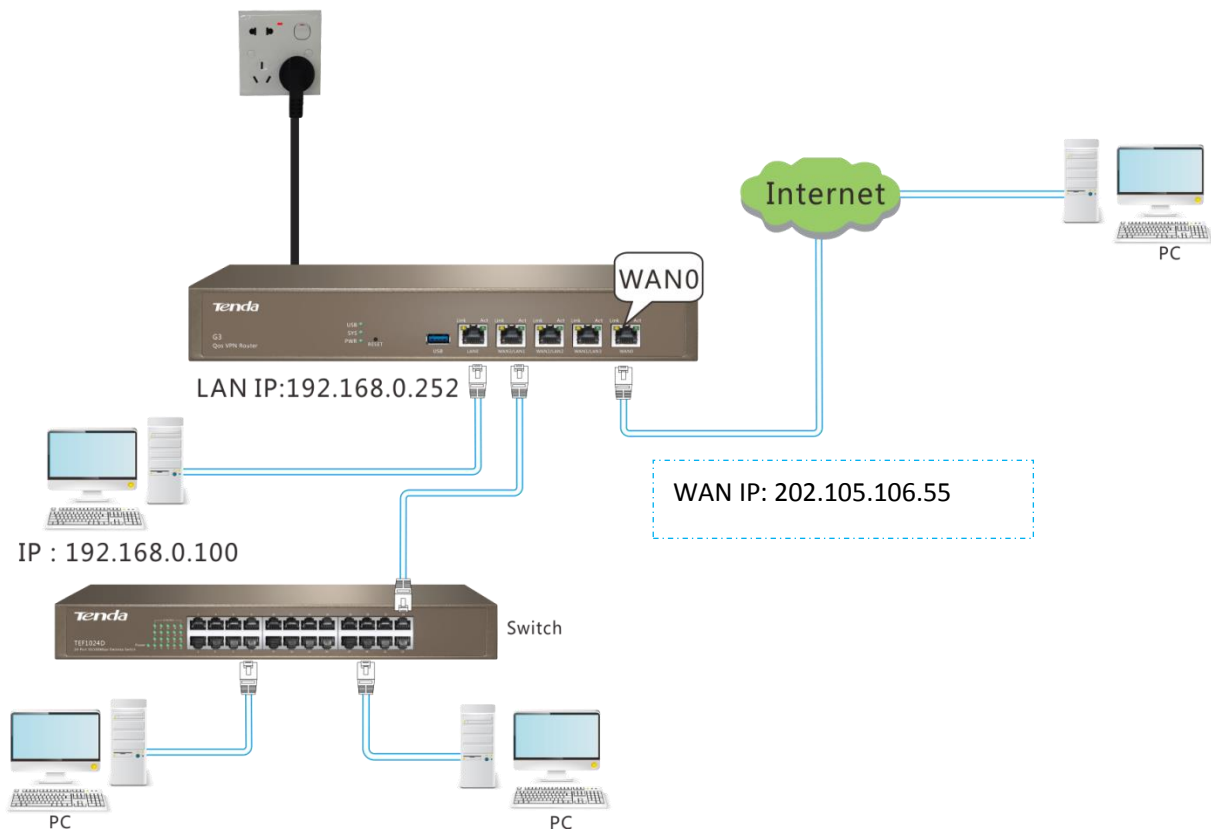
Example of port forwarding

- Example:** An enterprise uses a G3 enterprise router to establish a network. A business trip employee needs to access his own resources on the company computer. This can be achieved through the port forwarding function. Establish an FTP server on the company computer, store resources to be accessed on the server, and set the port forwarding function on the router.

Assume that basic information about the FTP server is as follows:

Item	Particular Content
IP Address	192.168.0.100
Username and Password	admin
Port	21

The reference topological graph is as follows:





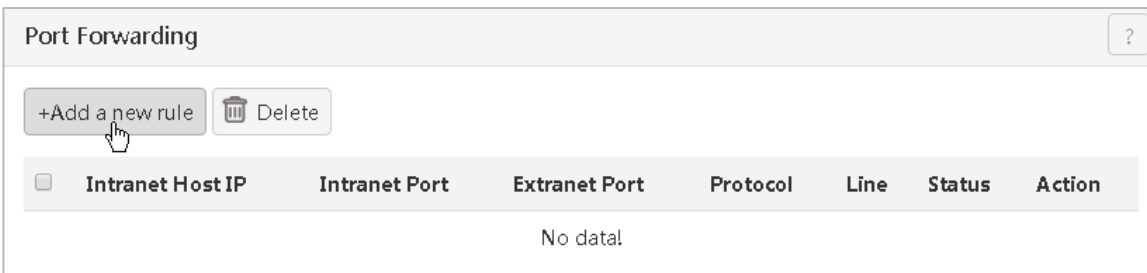
Tip

- Ensure that addresses obtained by the WAN port can access the Internet.
- An intranet computer IP address must be manually configured to avoid service interruption due to automatic change of IP address.
- System firewall, some pieces of antivirus software, and security software may prevent other computers from accessing the server on the computer. You are recommended to disable them temporarily when using this function.

Setup steps:

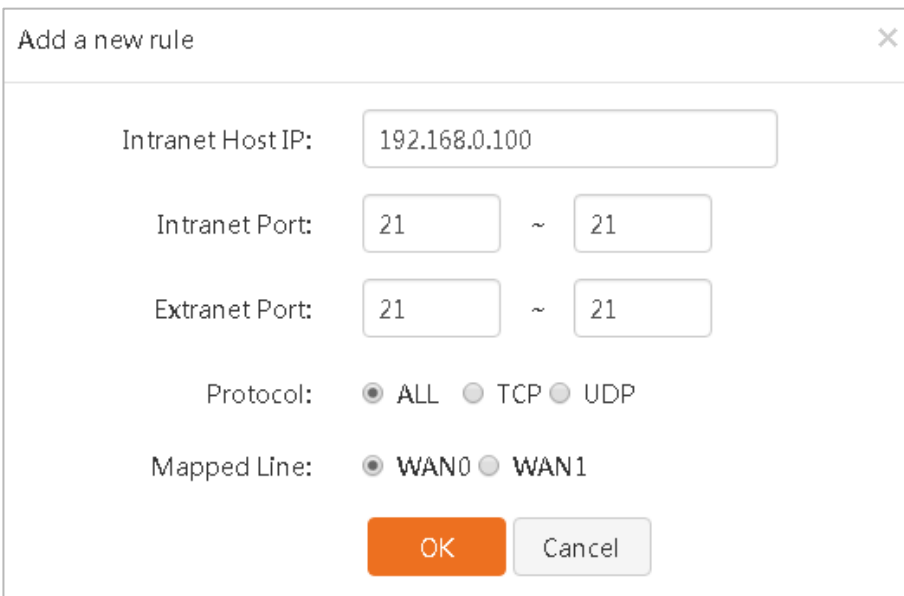
Step 1: Set port forwarding.

Click +Add a new rule.



Set rule contents in the window that appears.

- Intranet Host IP: Enter an IP address of the Internet server.
- Intranet Port: Enter a port used by the server.
- Extranet Port: Enter a router port open to the Extranet.
- Protocol: Select service protocols. It is recommended to select **all**.
- Mapped Line: Select a WAN port for Intranet service forwarding.
- Click **OK** to finish settings.



After a port forwarding rule is successfully added, the page is shown in the figure below.

Port Forwarding							?
+Add a new rule		Delete					
<input type="checkbox"/>	Intranet Host IP	Intranet Port	Extranet Port	Protocol	Line	Status	Action
<input type="checkbox"/>	192.168.0.100	21-21	21-21	ALL	WAN0	Enabled	

Step 2: Internet users access the intranet.

When extranet users access Intranet resources, they need only to access ftp://202.105.106.55 on the computers connected to the Internet.

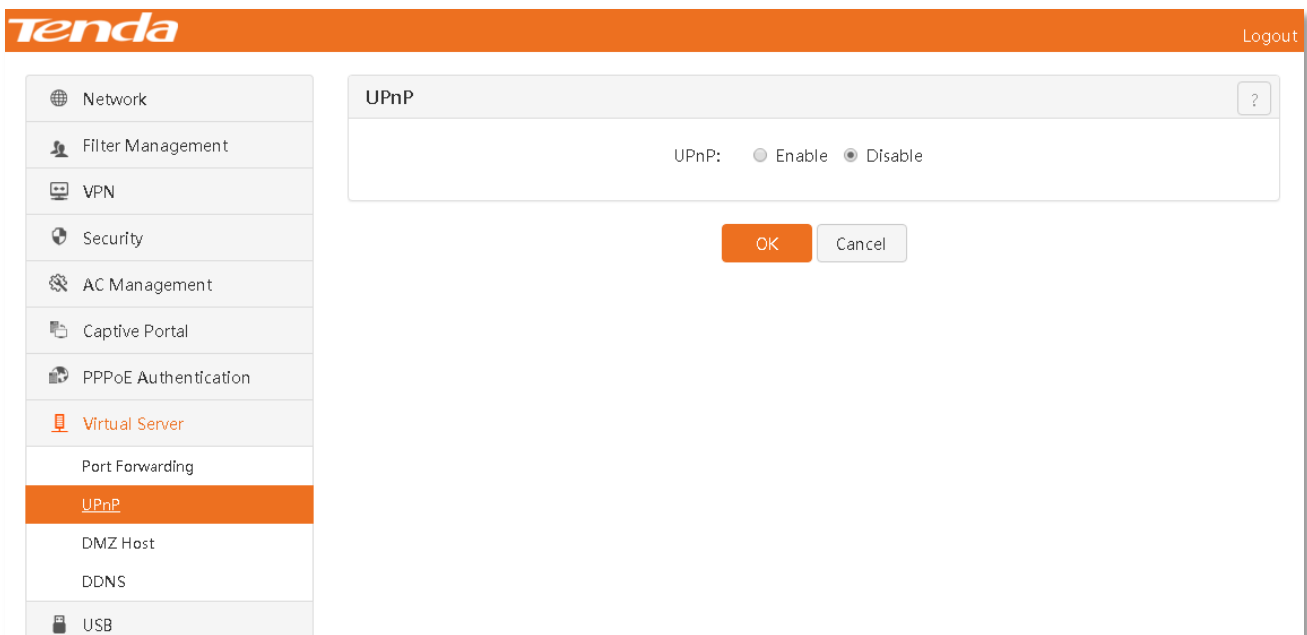
Note

- "Extranet Port" of the port forwarding rule shall not be same as "Port" of remote web management, otherwise a conflict will occur, causing port forwarding failure.
- After a rule is set, Internet users can access a corresponding server erected in the LAN in the form of "Protocol name://Current WAN IP address: Extranet port".

4.10.2 UPnP

UPnP (Universal Plug and Play) can achieve the automatic port forwarding function. The UPnP protocol can automatically identify user devices and automatically open a port for some programs. This function can be valid provided that the operating system supports UPnP or UPnP application software is installed.

Click 『Virtual Server』 > 『UPnP』 to go to the configuration page. Unless otherwise specially required, it is recommended to keep default settings.



- After the device enables the UPnP function, when programs supporting UPnP (e.g. Thunder)run in the LAN, you can see port translation information in the UPnP page, as shown in the figure below. Port translation information is provided when applications send a request.

UPnP
?

UPnP: Enable Disable

Remote Host	External Port	Internal Host	Internal Port	Protocol	Description
anywhere	12260	192.168.0.159	9202	UDP	Thunder5
anywhere	12260	192.168.0.159	12260	TCP	Thunder5

Refresh

OK
Cancel

- After the device enables the UPnP function, if a LAN computer supports UPnP, enter "Network" (for Windows 7) or "My Network Places" (for Windows XP) and you will see the network icon of the device. You can log in to the device web page through this icon.

4.10.3 DMZ Host

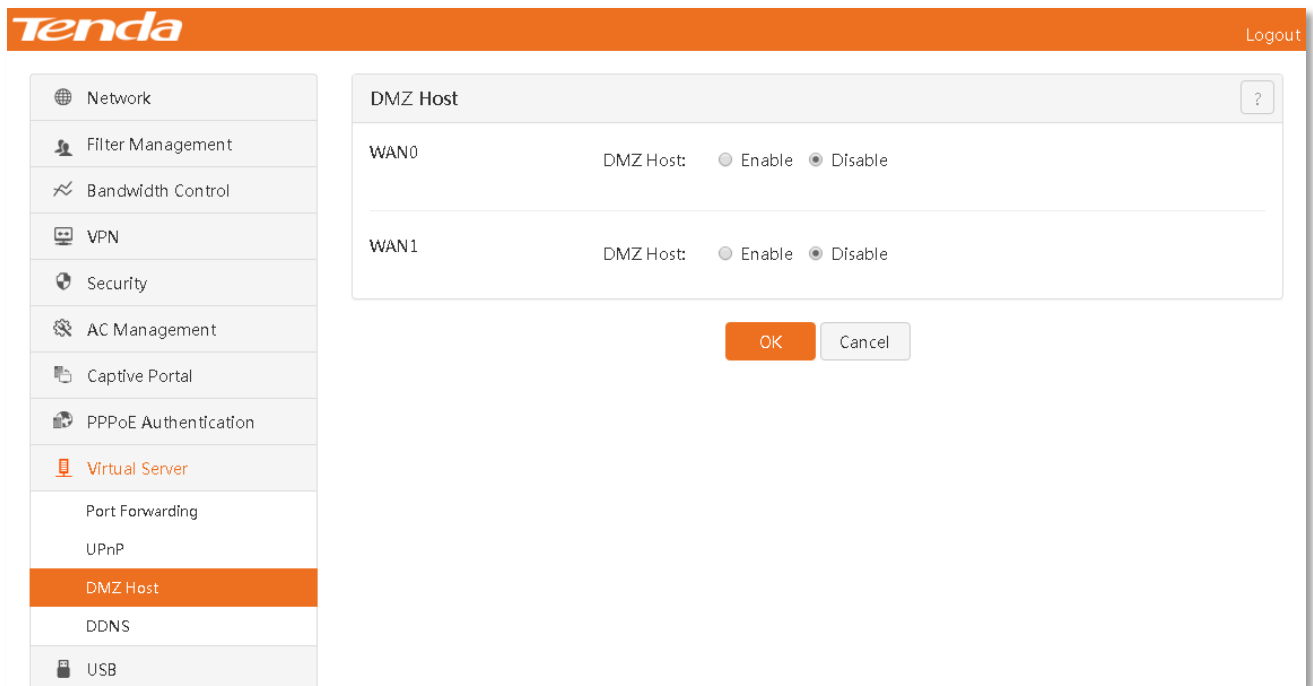
Overview

After a LAN computer is set to a DMZ host, this computer is not restricted when it communicates with the Internet. For example, for some video conferences and online games, you can set computers under these applications to DMZ hosts so that the video conferences and online games function more smoothly.

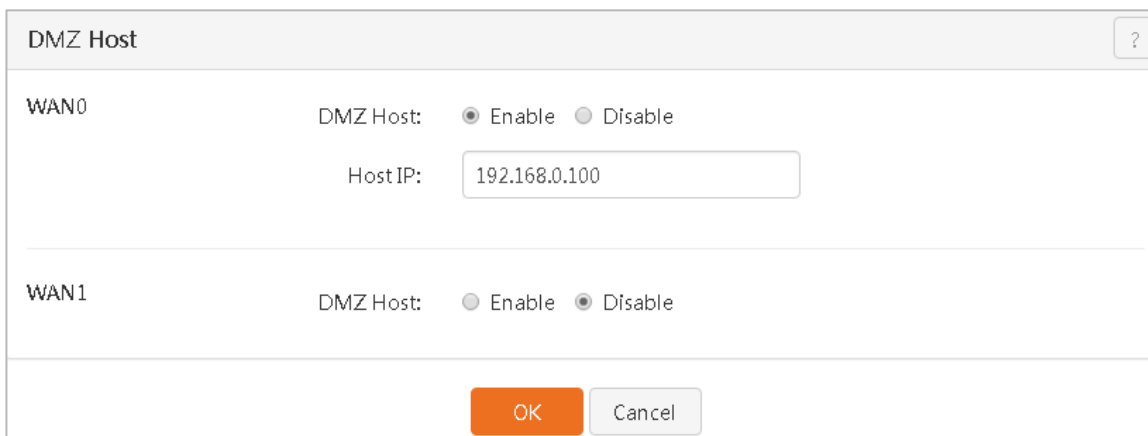
Click 『Virtual Server』 > 『DMZ Host』 to go to the configuration page.

Note

- When a computer is set to a DMZ host, this computer is fully exposed to the extranet and the router firewall does not act on this host any more. Hackers may use the DMZ host to attack the local network. Do not use the DMZ host function carelessly.
- It is necessary to manually set the IP address of the Intranet computer as the DMZ host to a static IP address to avoid failure of the DMZ function due to dynamic acquisition.
- Security software, antivirus software, and system firewall may affect the DMZ host function. Disable them temporarily when using this function. When you do not use the DMZ host function, you are recommended to cancel DMZ settings and enable firewall, security software, and antivirus software.



Steps for enabling a DMZ host



Setup steps:

- 1 Click **Enable** on a corresponding WAN port.
- 2 **Host IP:** Enter an IP address of a computer as a DMZ host.
- 3 Click **OK**.

4.10.4 DDNS

Overview

DDNS (Dynamic Domain Name Service) is to forward the router's dynamic WAN IP address (public network IP address) to a fixed domain name. When the service runs, the DDNS client sends this host's current WAN IP address to the DDNS server through information transmission. The server updates the forwarding relation between the domain name and the IP address in the database to achieve dynamic domain name resolution.



Tip

The DDNS function is generally used with other functions such as port forwarding, remote web management, and DMZ.

Click 『Virtual Server』 > 『DDNS』 to go to the configuration page.

The screenshot shows the Tenda web management interface. The top navigation bar is orange with the 'Tenda' logo on the left and a 'Logout' link on the right. A sidebar menu on the left contains various system settings, with 'DDNS' highlighted in orange. The main content area displays the 'DDNS' configuration page. It features a table with two rows: 'WAN0' and 'WAN1'. Each row has a 'DDNS:' label followed by two radio buttons: 'Enable' and 'Disable'. The 'Disable' radio button is selected for both WAN0 and WAN1. Below the table, there are two buttons: 'OK' (orange) and 'Cancel' (grey).

After the rule is set successfully, the page is shown in the figure below.

DDNS
?

WAN0

DDNS: Enable Disable

DDNS Provider: Go to register

Provider link: [DDNS service upgrade](#)[DDNS service help](#)

Service Type: General service

Username:

Password:

Domain Name Info:

Status: authorized

WAN1

DDNS: Enable Disable

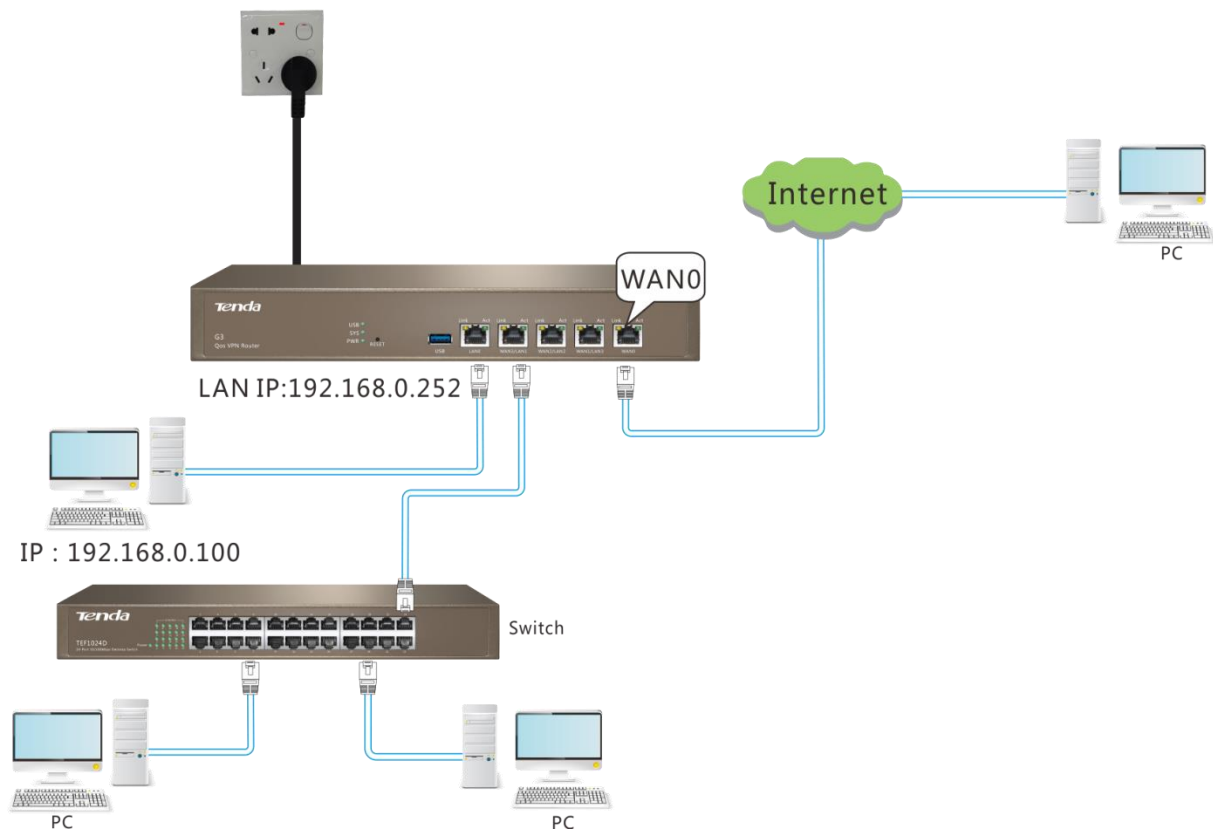
Description of some parameters in the page:

Parameter	Description
DDNS	Enable/Disable the DDNS function. The default is Disable.
DDNS Provider	Service provider who provides DDNS. This router supports 3322.org, 88ip.cn, oray.com, and gnway.com.
Provider link	Valid for oray.com only. Click this link to learn about more information about Oray DDNS.
Username	Username to log in to DDNS service, i.e. login user name registered on the DDNS Provider website.
Password	Password to log in to DDNS, i.e. password registered on the DDNS Provider website.
Domain Name Info	Domain name information obtained from the DDNS server. When setting DDNS providers except oray.com, you need to manually enter a domain name registered on their websites.
Status	Operating status of DDNS service.

Example of DDNS

- **Example:** An enterprise uses a G3 enterprise router to establish a network. The WAN IP address of the router is dynamically changed. A business trip employee needs to access his own resources on the company computer. This can be achieved through the DDNS function. Establish an FTP server on the company computer. Store resources to be accessed on the server. Set the DDNS and port forwarding function on the router.

The reference topological graph is as follows:



Configuration steps:

Step 1: Register a domain name.

- 1 Enter the DDNS configuration page, enable DDNS, select a DDNS provider such as oray.com, and click **Go to register**.

DDNS
?

WAN0

DDNS: Enable Disable

DDNS Provider: [Go to register](#)

Provider link: [DDNS service upgrade](#)[DDNS service help](#)

Service Type: General service

Username:

Password:

Domain Name Info:

Status: unauthorized

WAN1

DDNS: Enable Disable

2 Register a domain name by referring to prompt messages in the website.

Assume that registered basic information is as follows:

Item	Particular Content
Provider	oray.com
Username	Tom-Jerry
Passwords	tomjerry123456
Domain Name	tom-jerry.imwork.net

Step 2: Set a DDNS rule.

Reenter the DDNS configuration page and perform actions by referring to the following contents.

- 1 DDNS:** Click Enable.
- 2 DDNS Provider:** Select a corresponding provider (in this example, oray.com).
- 3 Username/Password:** Enter the user name and password registered in the DDNS Provider website.
- 4** Click **OK**

DDNS

WAN0

DDNS: Enable Disable

DDNS Provider: oray.com [Go to register](#)

Provider link: [DDNS service upgradeDDNS service help](#)

Service Type: General service

Username: Tom-Jerry

Password:

Domain Name Info:

Status: unauthorized

WAN1

DDNS: Enable Disable

OK Cancel

After finishing settings, refresh the page and wait a moment. The connection is successful when "Status" is displayed as authorized and "Domain Name Info" has obtained a domain name address. All domain names set in the DDNS Provider website will be displayed in "Domain Name Info" in this page. All of these domain names forward the WAN IP address of the router.

DDNS

WAN0

DDNS: Enable Disable

DDNS Provider: oray.com [Go to register](#)

Provider link: [DDNS service upgradeDDNS service help](#)

Service Type: General service

Username: Tom-Jerry

Password:

Domain Name Info: tom-jerry.imwork.net

Status: authorized

WAN1

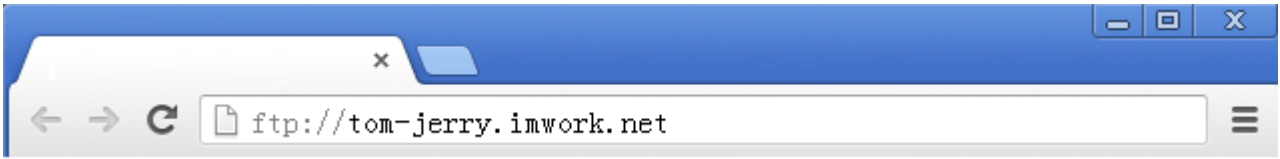
DDNS: Enable Disable

OK Cancel

Step 3: Set the port forwarding function. For detailed configuration steps, refer to [Port Forwarding](#).

Step 4: Remotely access the router.

When external users access Intranet resources, they need only to access ftp://tom-jerry.imwork.net on the computers connected to the Internet.



4.11 USB

[USB Sharing](#): Allow the LAN to share device resources stored on the router USB port.

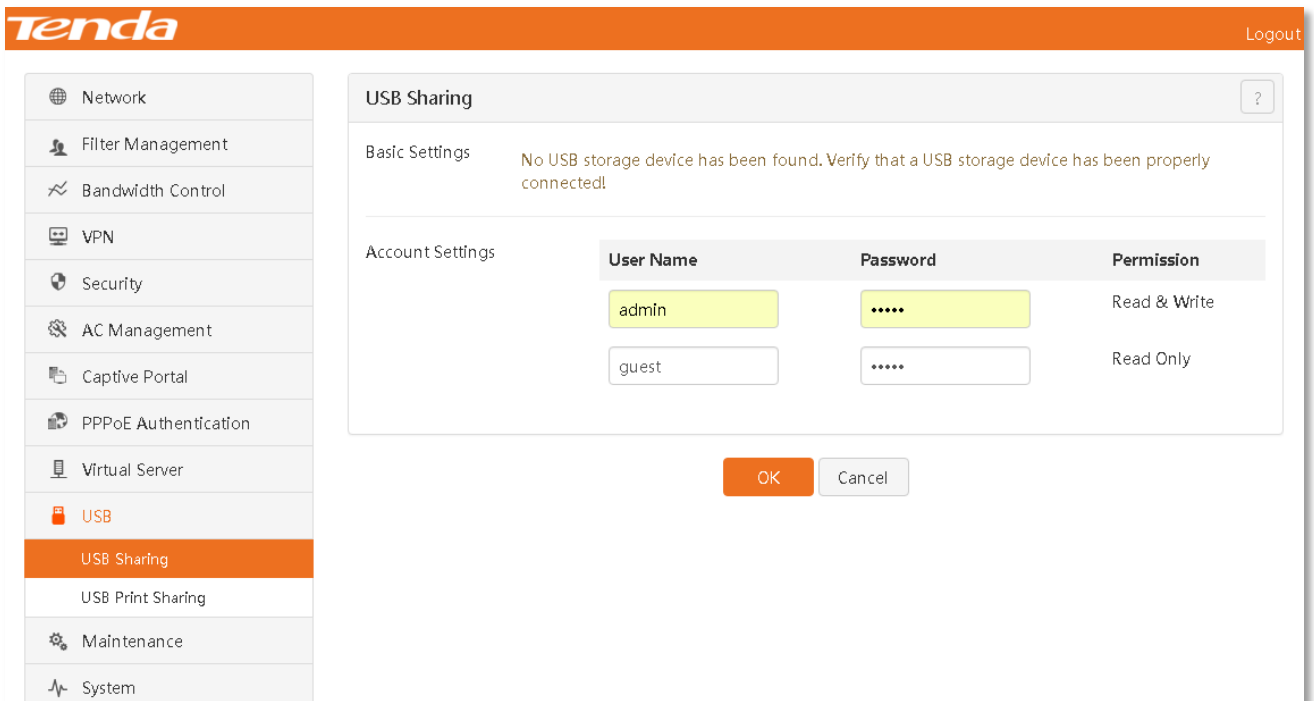
[USB Print Sharing](#): Allow the LAN to share printing service.

4.11.1 USB Sharing

Overview

This device can automatically identify a USB storage device plugged into its USB port, and displays information about the total and available disk space of this USB storage device in the configuration page. LAN users can access information in the USB storage device.

Click 『USB Sharing』 to go to the configuration page.



When a U-disk is plugged into the router, the router can automatically identify U-disk information, as shown in the figure below.

The screenshot shows the 'USB Sharing' configuration page. Under 'Basic Settings', the 'sda' field is set to '10%' and there is an 'Eject' button. The 'Access Locally' field shows 'ftp://192.168.0.252:21 or \\192.168.0.252'. The 'Allowed to Access From the Internet' option is set to 'Disable'.


User Name	Password	Permission
admin	Read & Write
guest	Read Only

After the "Allowed to Access From the Internet" function is enabled, the page is shown in the figure below:

The screenshot shows the 'USB Sharing' configuration page with 'Allowed to Access From the Internet' set to 'Enable'. A red box highlights the 'Access From the Internet' field, which contains the URL 'ftp://192.168.3.146:21'.

User Name	Password	Permission
admin	Read & Write
guest	Read Only

Parameter description in the page:

Parameter		Description
Basic Settings	sda1	Displays a utilization rate of the USB storage device on the router.
		To avoid data loss of the USB storage device, click this button and remove this device.
	Access Locally	Address where clients under the router access resources of the USB storage device. The default parameters are as follows: <ul style="list-style-type: none"> • ftp:\\192.168.0.252:21: Directly click this link to access. • \\192.168.0.252: Copy this website to the "Start">"Run" menu of the computer before any access.
	Allowed to Access From the Internet	Enable/Disable Internet users to access resources in the USB storage device. The default is Disable.
	Access From the Internet	Internet users can access resources in the USB storage device through this address.
Account Settings	Username and Password	User name and password to be entered when users access the USB storage device. A user name and password can be modified according to actual situations.
	Permission	<ul style="list-style-type: none"> • Read & Write: Users can access and modify resources in the USB storage device. • Read Only: Users can access only resources in the USB storage device.

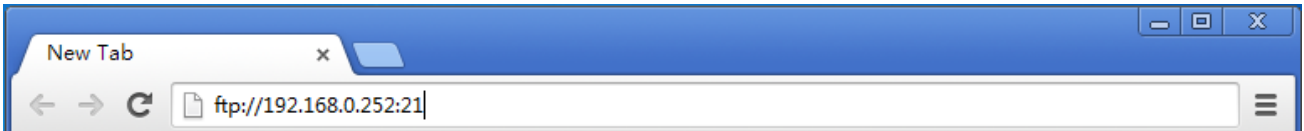
Example that the Intranet accesses resources in the USB device on the router

■ **Example:** An enterprise uses a G3 enterprise router to establish a network. One mobile storage device as a server is connected to the USB port of the router. When searching data, employees can log in to this server to download data. Assume that the network administrator informs employees of the following information about access to the server:

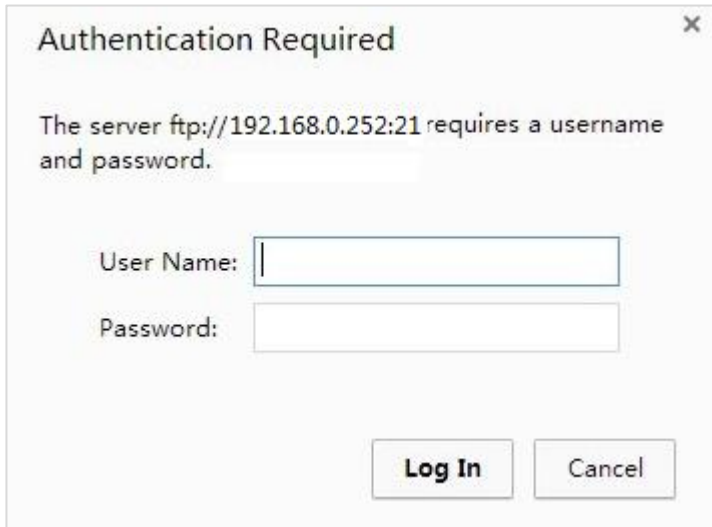
- Address used when employees access the server: \\192.168.0.252.
- Address used when business trip employees access the server: ftp://172.16.200.53:21
- Both the user name and password are guest.

User Access Steps (Take Windows 7 as an example):

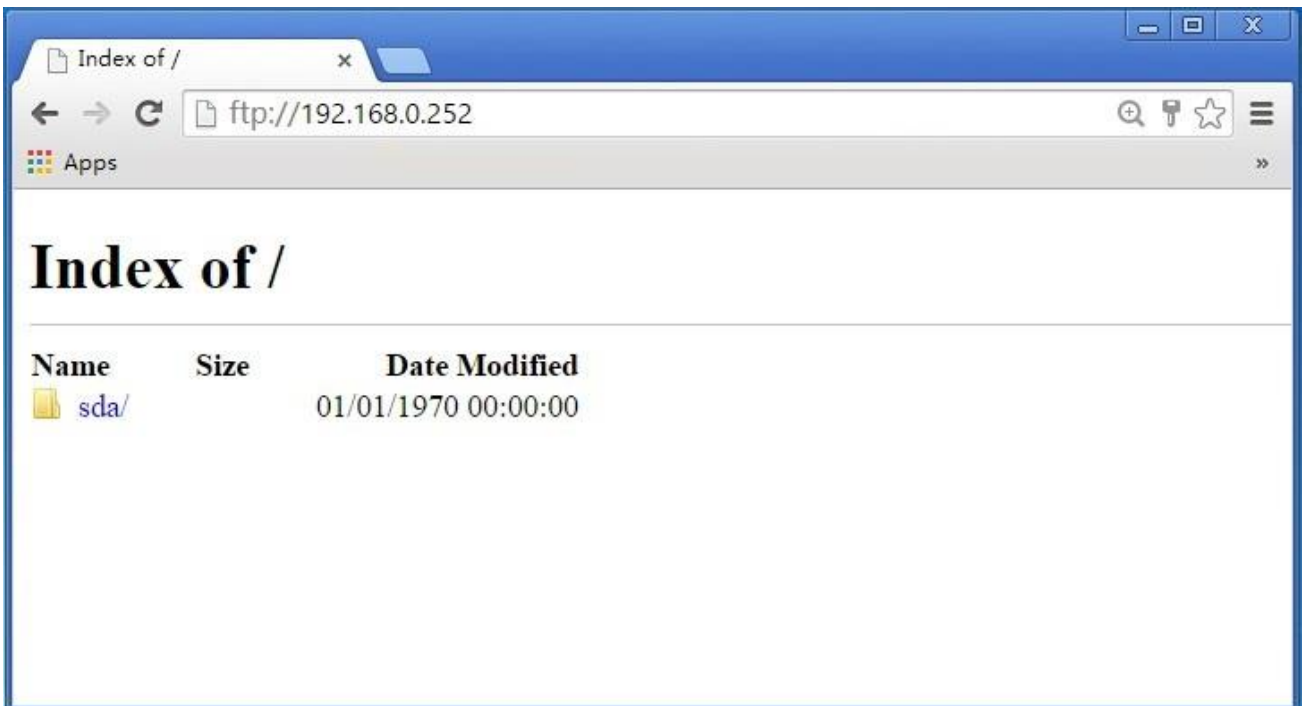
- 1 Type the address ftp://xxx.xxx.xxx.xxx:xx (ftp://192.168.0.1 here) in the address bar of a web browser. Tap **Enter** on the keyboard.



- 2 Type the User name and the Password to access the USB device and click **Log In**.



- 3 Then you can share the files on the USB storage drive.



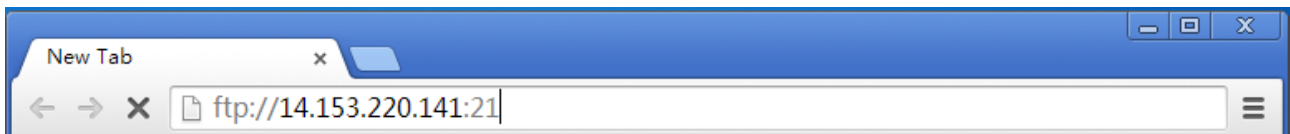
Example that the Internet accesses resources in the USB device on the router

■ **Example:** An enterprise uses a G3 enterprise router to establish a network. One mobile storage device as a server is connected to the USB port of the router. Business trip employees need to log in to this server to search data. This can be achieved by enabling the "Allowed to Access From the Internet" function of USB Sharing. Assume that the network administrator informs employees of the following information about access to the server:

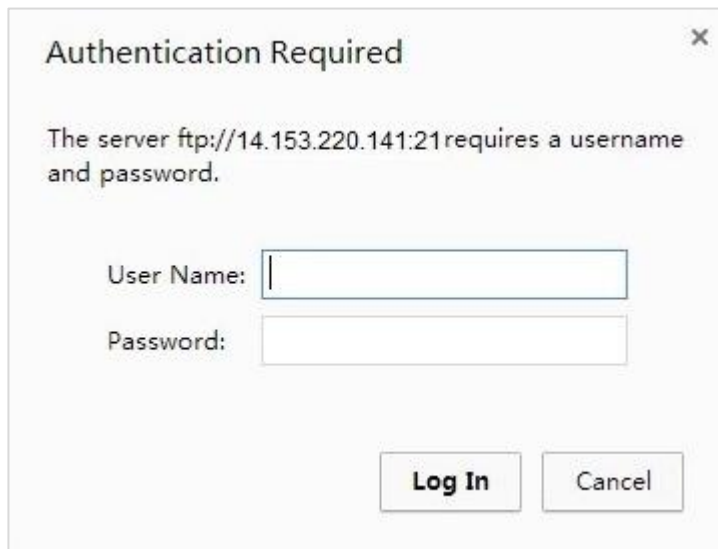
- Address used when employees access the server: \\192.168.0.252.
- Address used when business trip employees access the server: ftp://172.16.200.53:21
- Both the user name and password are guest.

User Access Steps (Take Windows 7 as an example):

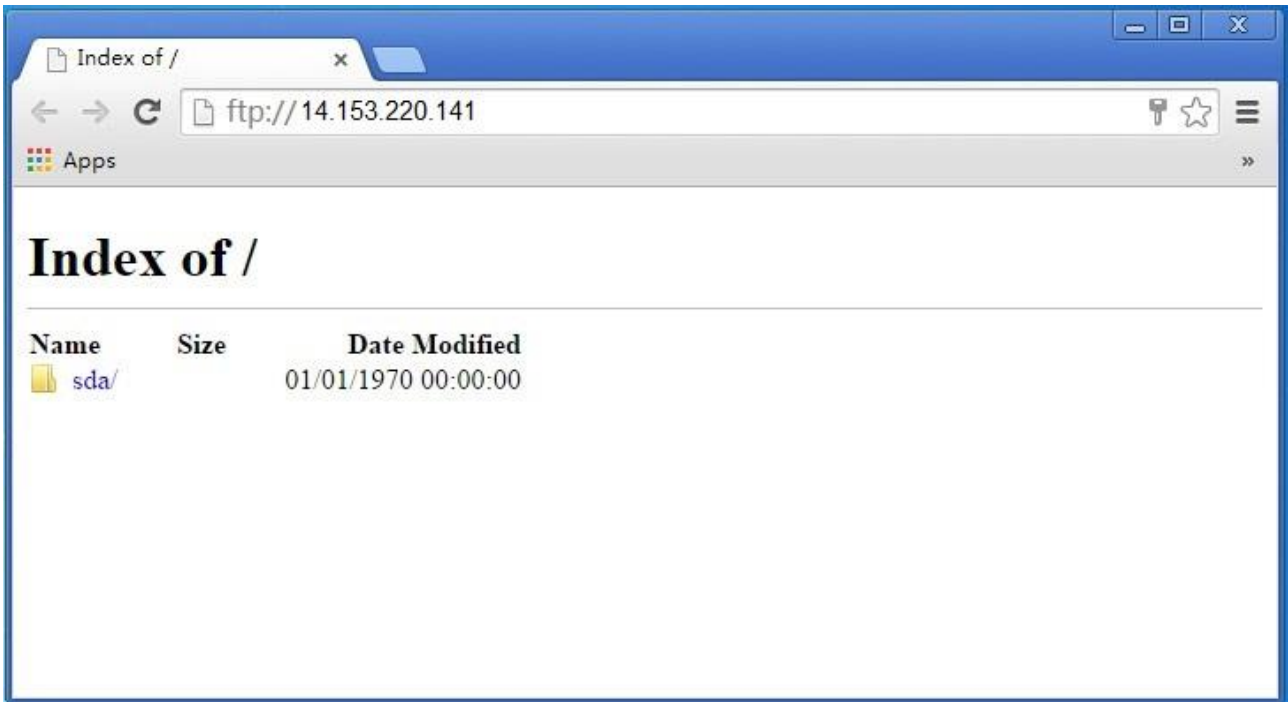
1 Type the address ftp://xxx.xxx.xxx.xxx:xx (xxx.xxx.xxx.xxx MUST be public IP address, ftp://**14.153.220.141:21** here) in the address bar of a web browser on a computer from the Internet. Tap **Enter** on the keyboard.



2 Type the default User name (Guest account) and the Password you just specified and click **Log In**.



- 3 Then you can share the files on the USB storage drive.

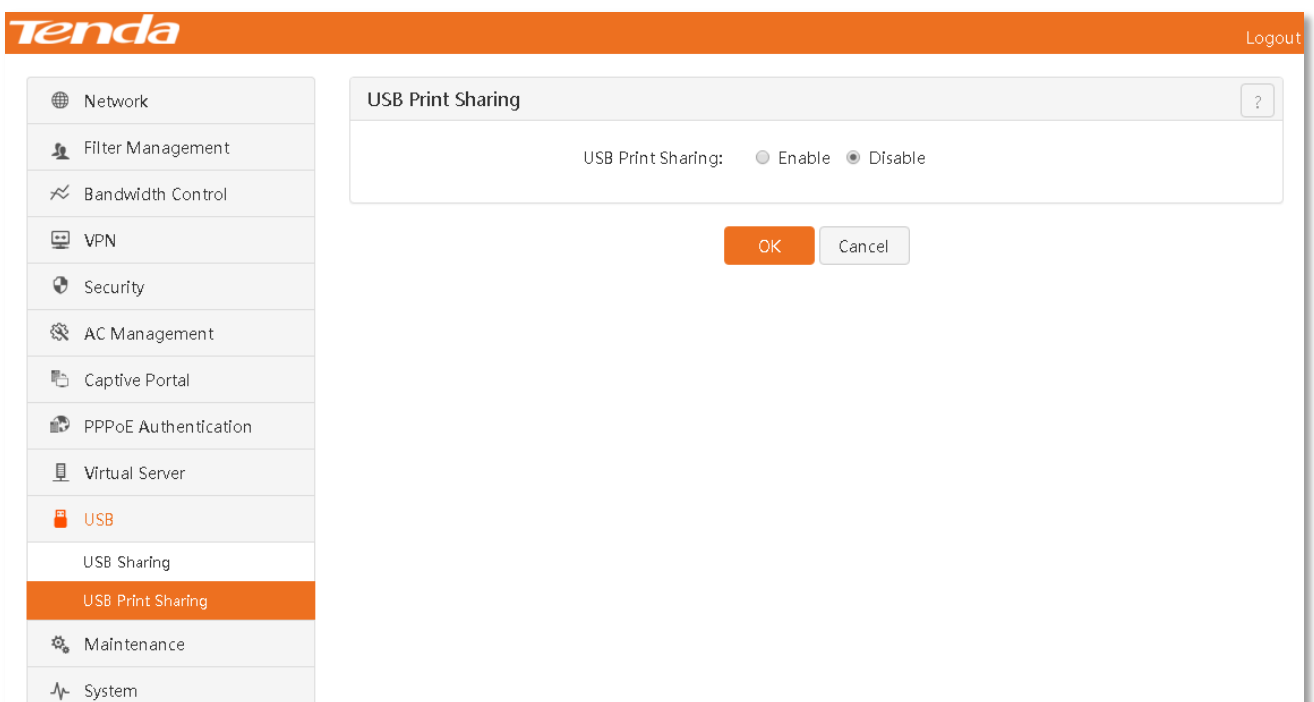


4.11.2 USB Print Sharing

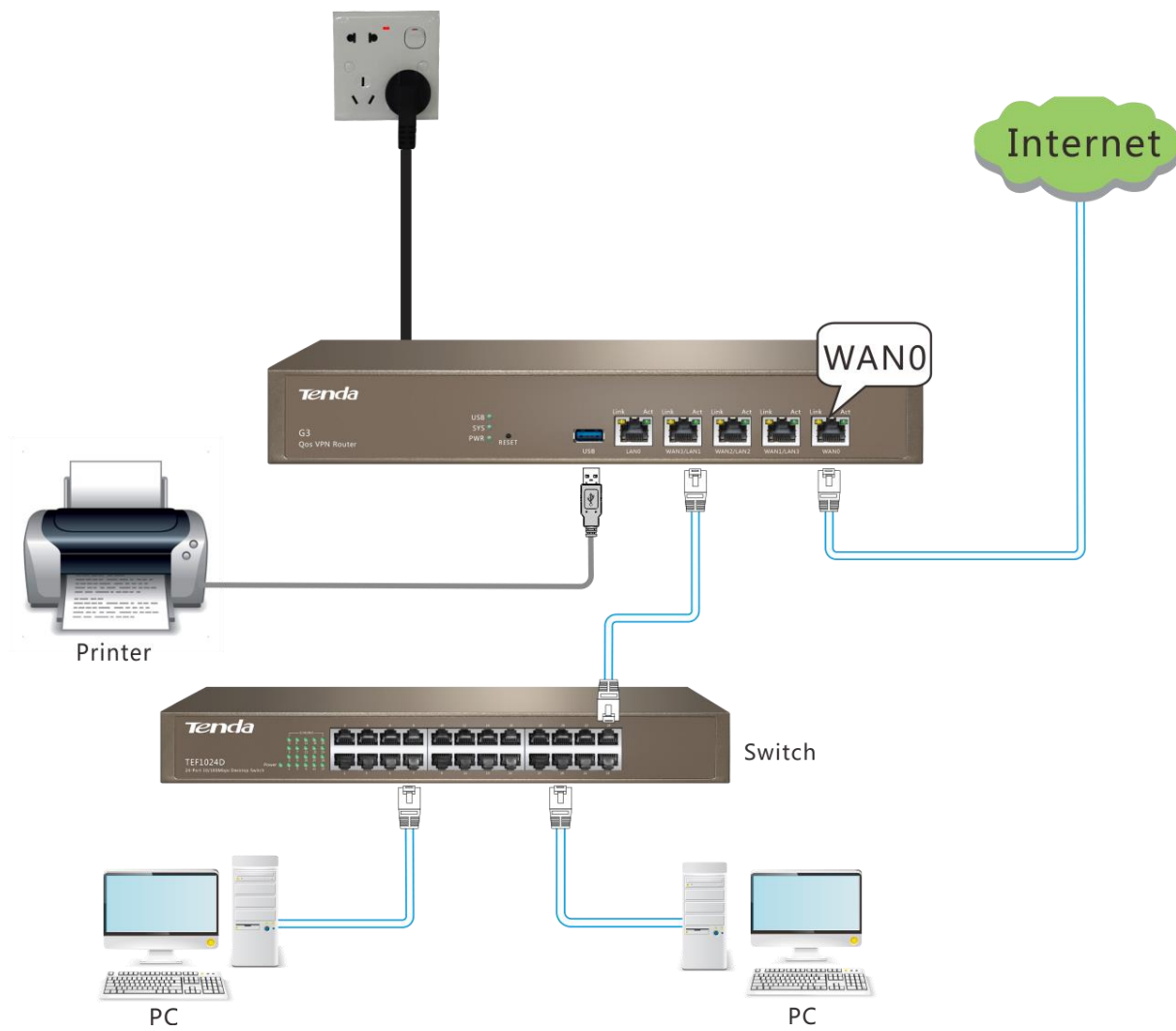
Overview

This router supports the USB printing service and allows computers in the LAN to share a USB printer connected to the device USB port.

Click 『Virtual Server』>『USB Print Sharing』 to go to the configuration page. The print sharing function is disabled by default.



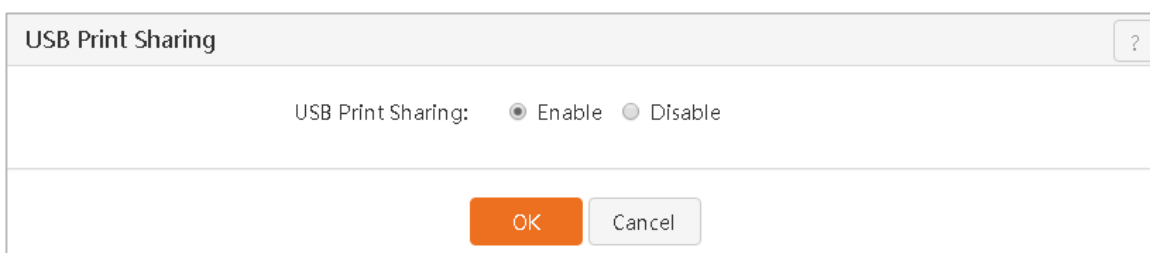
The reference topological graph is as follows:




Operating steps for USB printing (Take HP LaserJet 1020 as an example)

Step 1: Connect the USB printer to the USB port of the router.

Step 2: Enable the USB printing function of the router.

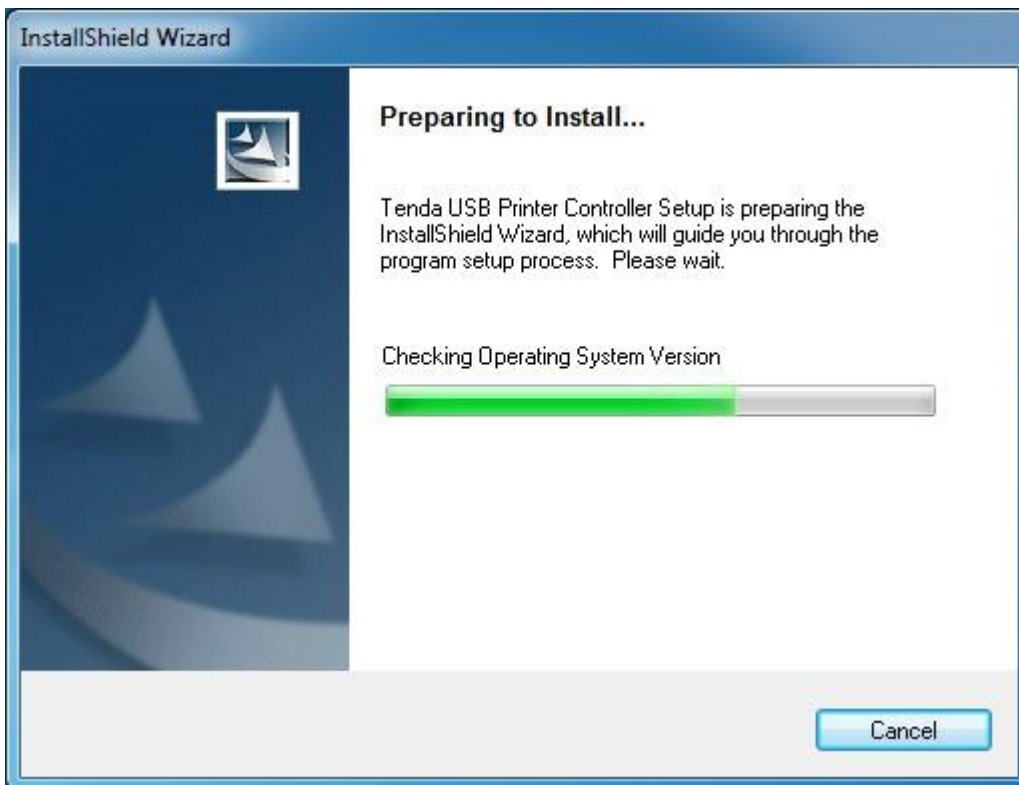


Step 3: Install the Tenda printer controller on the LAN computer (Take Windows 7 as an example).

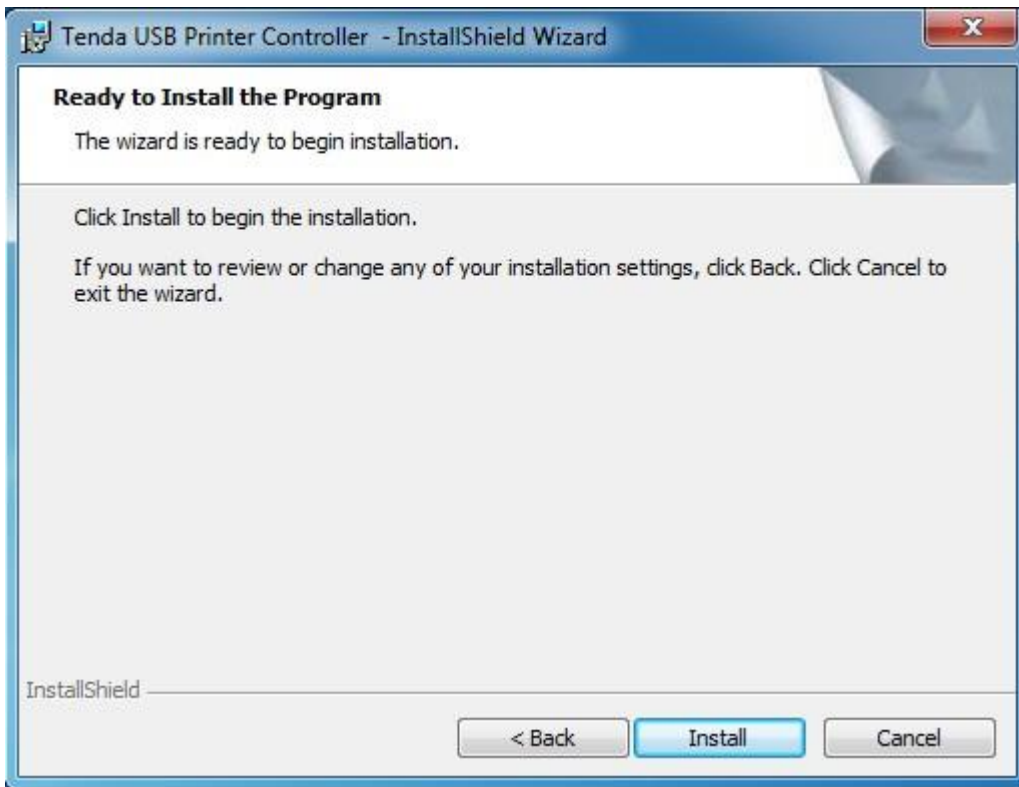
- 1 Download and decompress the printer controller at tenda website (<http://www.tendacn.com>) .
- 2 Double-click the installation program  setup .
- 3 Select **English** and click **OK**.



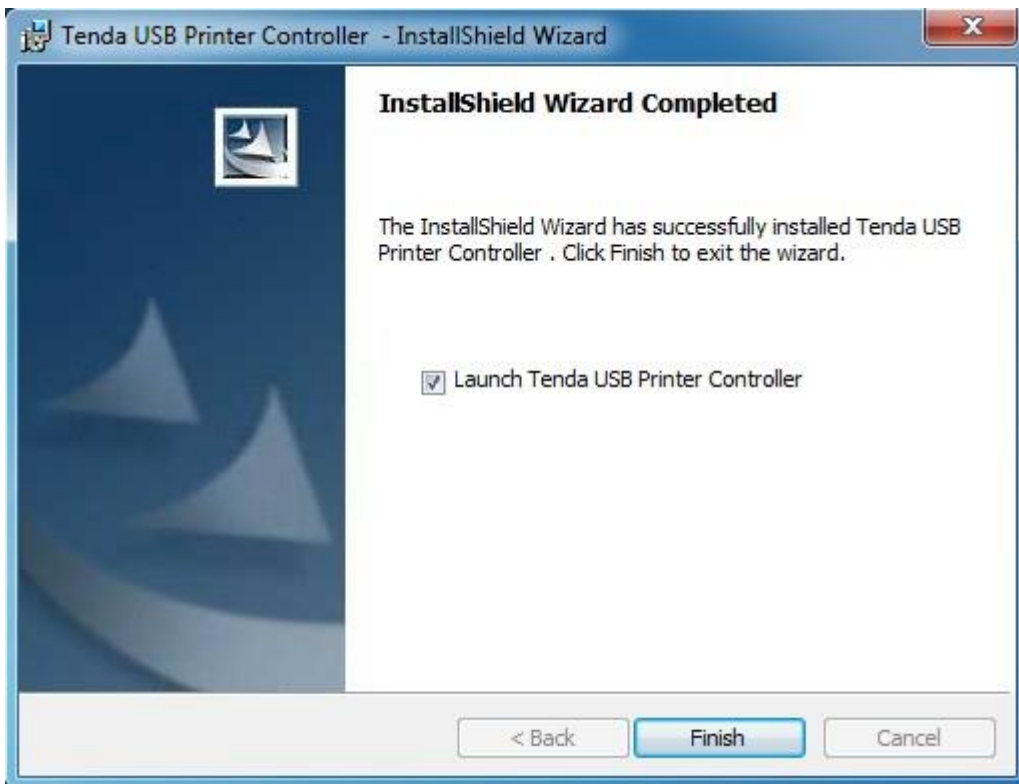
- 4 Then the USB Printer Controller will start installing.



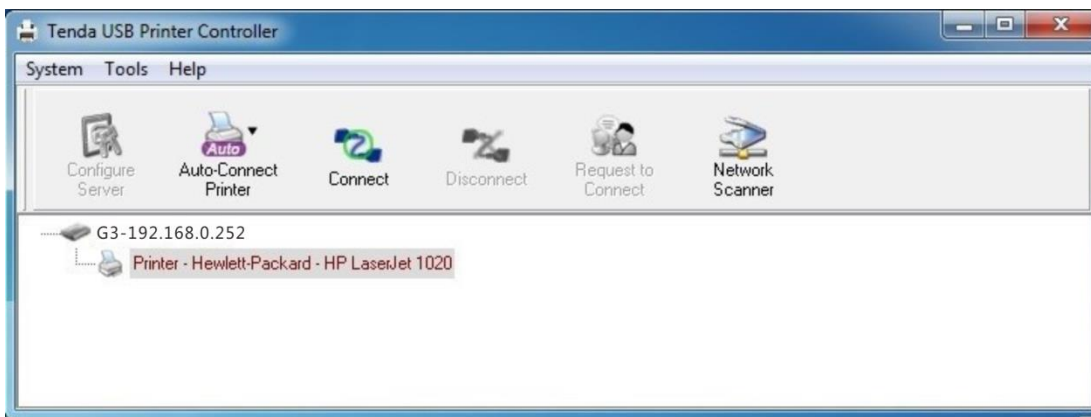
- 5 Keep click next until the following page appears, then click **Install**.



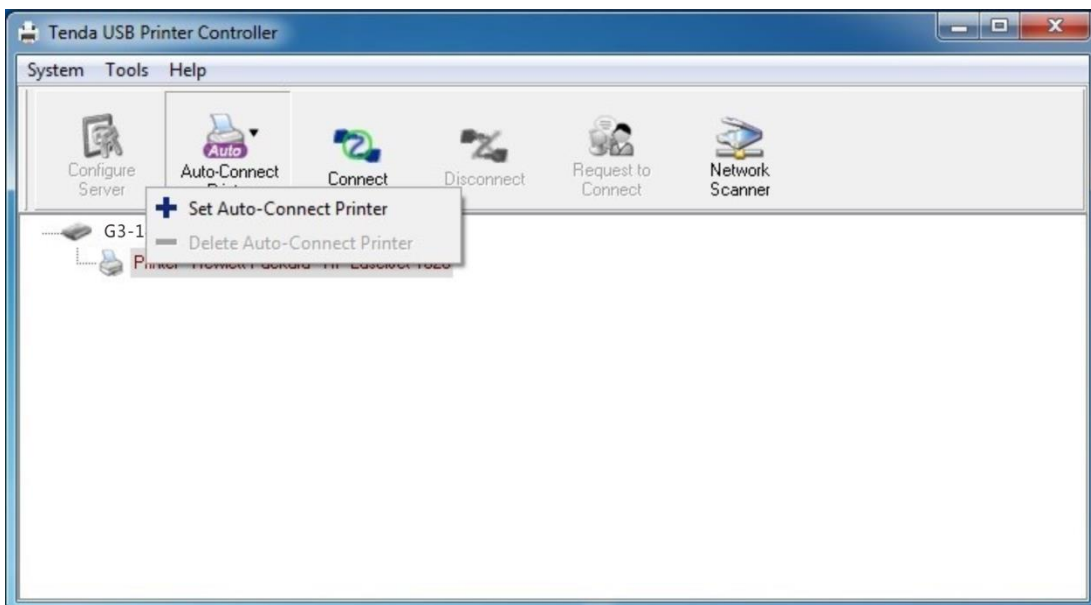
- 6 Click **Finish** when the following page appears.



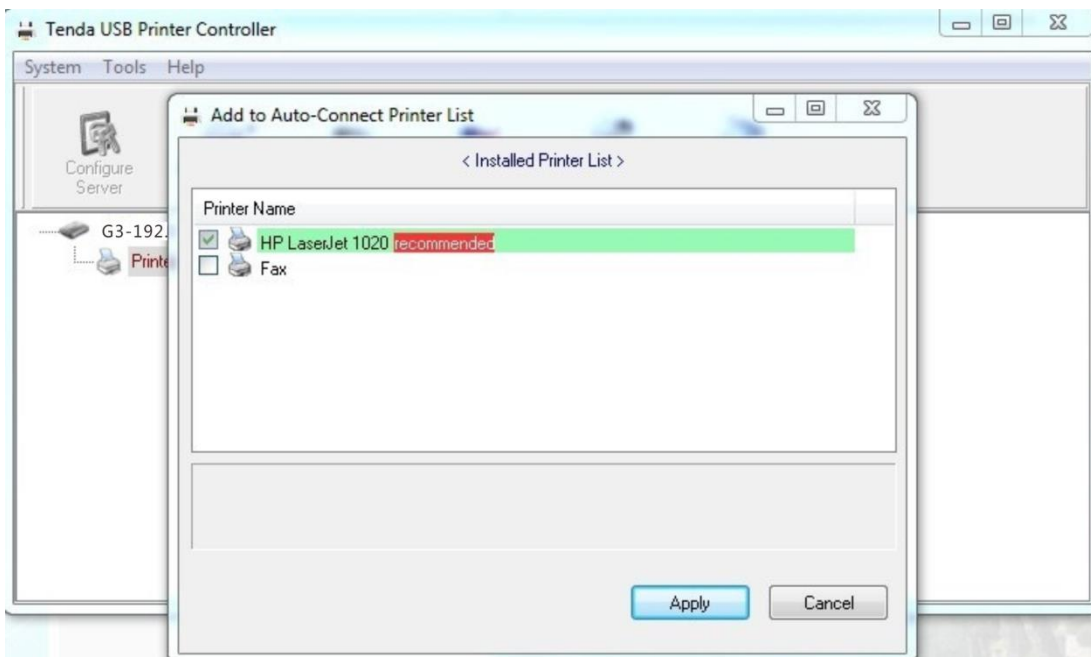
Wait a moment, and the printer under the router will be automatically identified.



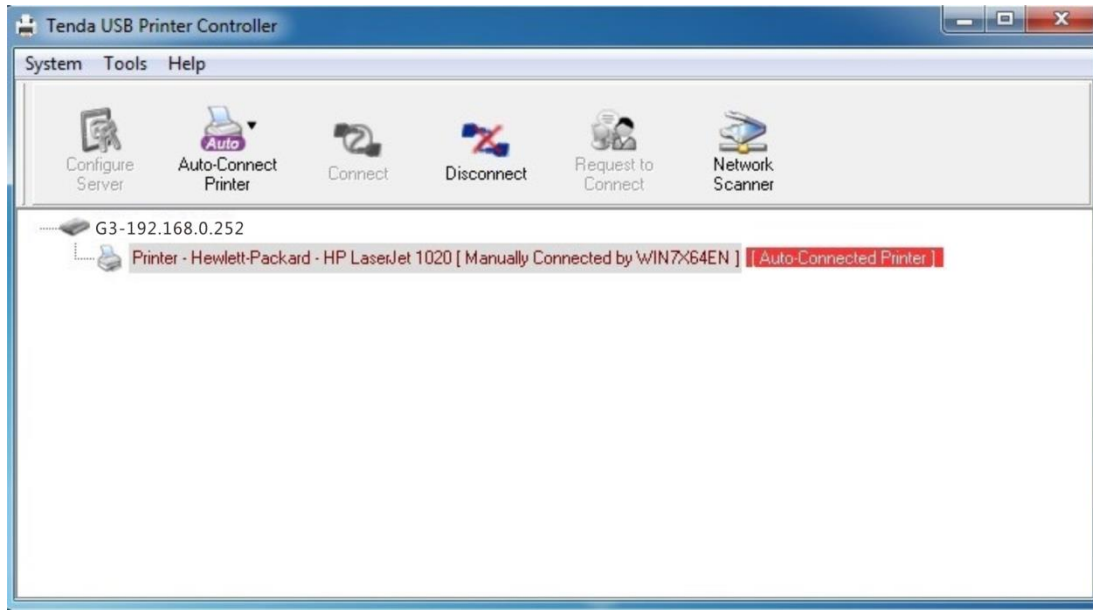
7 Click the **Printer**, and then **Auto-Connect Printer > Set Auto-Connect Printer**.



8 Select your printer and click **Apply**.



When the page below appears, it indicates that the USB printer is connected to the Router successfully.



Then you can print the files!



After installation is successful, the shortcut of the printer will be generated on the desktop of the computer.



Tip

- The USB Printer Controller is compatible with most printers on the market, but if your printer cannot be detected by the USB Printer Controller, you can contact our technical support for help.
 - When you select **Auto-Connect Printer**, the USB printer can be used by several computers simultaneously. but when **Connect** is selected, the USB printer can only be used by a computer at one time.
-

Step 4: Install a printer driver on the LAN computer.

After installation is successful, the printer will print a test page.



Tip

If there is no printer driver, you can let the computer perform automatic detection and download and install a printer driver from the Internet.

4.12 Maintenance

Maintenance includes the following contents:

[Username & Password](#): Modify a user name and password to log in to the router.

[Reboot](#): Reboot the router when any set parameters cannot be valid or the router cannot operate normally.

[Back & Restore](#): Back up or restore router configuration information.

[Firmware Upgrade](#): Enable the router to obtain more stable performance and new value-added functions.

[Reset to Factory Defaults](#): Reset the device to factory defaults during abnormal operation of the router or in case of emergency.

[Time & Date](#): Set time & date of the router.

[Remote WEB Management](#): Set Internet users' authority of access to the Internet.

4.12.1 Username & Password


Overview

Click 『Maintenance』 to go to the Username & Password page. You can modify a user name and password in the router login management page. This router supports "admin" and "guest" login.


The screenshot shows the Tenda router web interface. The top navigation bar is orange with the 'Tenda' logo on the left and a 'Logout' link on the right. A left sidebar contains a menu of system functions, with 'Maintenance' highlighted in orange. Under 'Maintenance', 'Username & Password' is selected. The main content area displays the 'Username & Password' configuration page, which includes a table with the following data:

Type	Username	Action
admin	admin	
guest	guest	

Parameter description in the page:

Parameter	Description
Type	<ul style="list-style-type: none"> admin: Router configurations can be viewed and modified. guest: Router configuration information can be viewed only and the router cannot be set.
Username	User name of a corresponding account.
Action	Click  to modify a user name and password of a corresponding account.

Configuration steps for modifying a login user name and password

- 1 Click  after a corresponding account.

Username & Password		
Type	Username	Action
admin	admin	
guest	guest	

- 2 In the dialog box that appears, enter the current login password, set a new login user name and password, and click **OK**.

admin ×

Old Username:

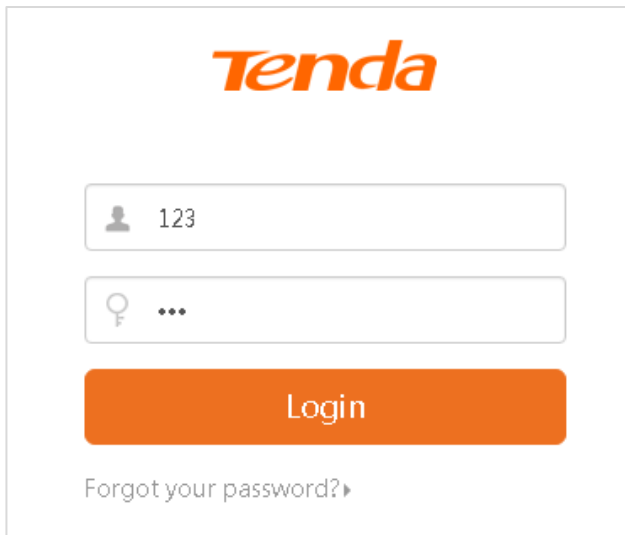
Old Password:

New Username:

New Password:

Confirm the password:

The page will go to the login page. At this point, enter the set user name and password and click **Login** to the management page of the router.

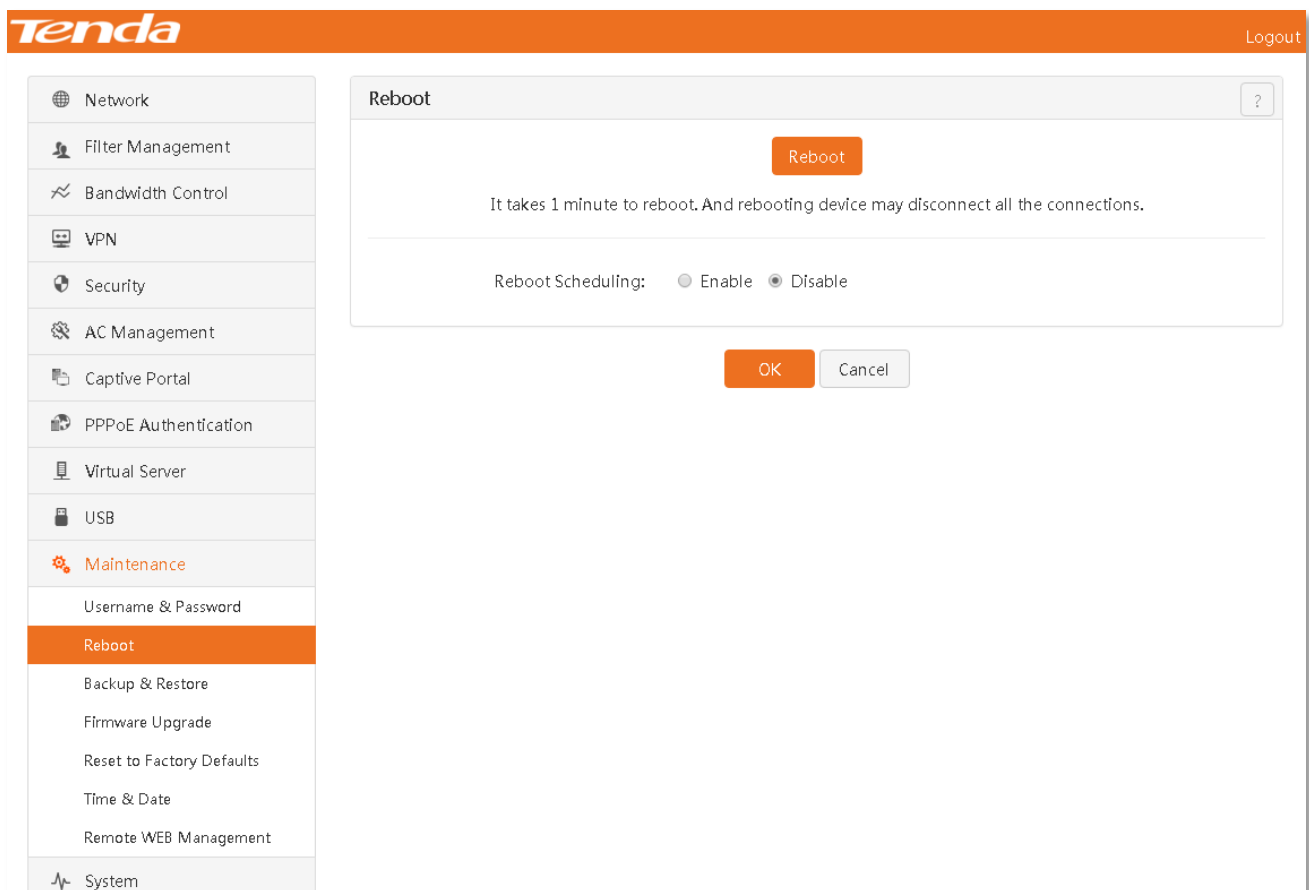


The image shows the Tenda login page. At the top is the Tenda logo in orange. Below it is a username input field containing '123' with a person icon on the left. Underneath is a password input field with a key icon and three dots on the left. A large orange 'Login' button is centered below the fields. At the bottom, there is a link that says 'Forgot your password?' with a right-pointing arrow.

4.12.2 Reboot

Overview

Reboot the router when a set parameter cannot be valid or the router cannot operate normally. This router supports "Manual Reboot" and "Reboot Scheduling". Click 『Maintenance』>『Reboot』 to go to the configuration page.



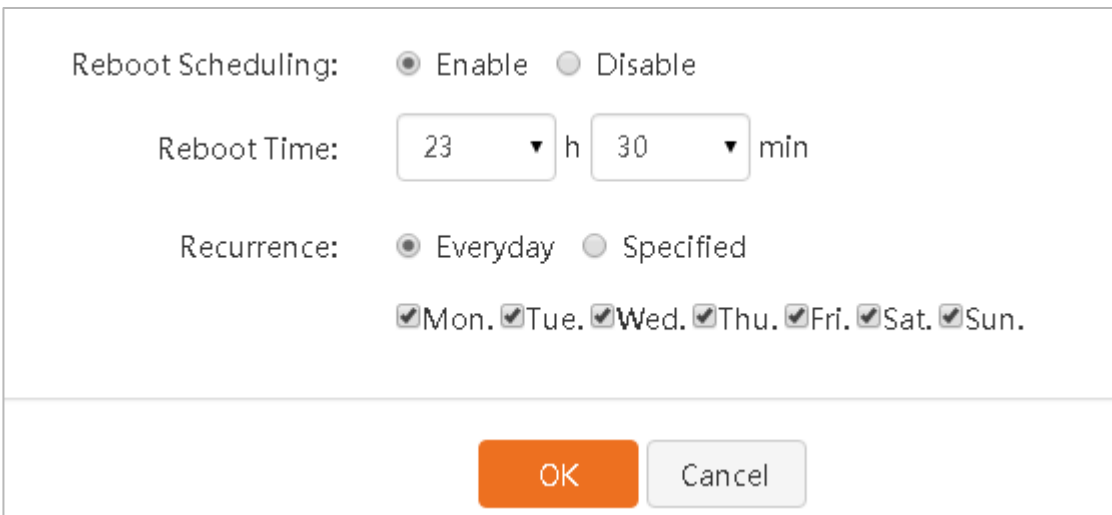
The image shows the Tenda web management interface. The top header is orange with the Tenda logo on the left and a 'Logout' link on the right. A left sidebar contains a menu with items: Network, Filter Management, Bandwidth Control, VPN, Security, AC Management, Captive Portal, PPPoE Authentication, Virtual Server, USB, Maintenance (highlighted in orange), Username & Password, Reboot (highlighted in orange), Backup & Restore, Firmware Upgrade, Reset to Factory Defaults, Time & Date, Remote WEB Management, and System. The main content area is titled 'Reboot' and features a 'Reboot' button. Below the button, a message states: 'It takes 1 minute to reboot. And rebooting device may disconnect all the connections.' Underneath this message is a 'Reboot Scheduling' section with two radio buttons: 'Enable' and 'Disable', where 'Disable' is selected. At the bottom of the configuration area are 'OK' and 'Cancel' buttons.

Steps for setting manual reboot

After going to the configuration page, click **Reboot**, perform operations according to prompts in the page, and wait for the router to be rebooted.

Steps for setting reboot scheduling

- 1 **Reboot Scheduling:** Click Enable.
- 2 **Reboot Time:** Click the dropdown list and select automatic reboot time of the router such as 23:30.
- 3 **Recurrence:** Set an automatic reboot date of the router such as everyday.
- 4 Click **OK**.



The screenshot shows a configuration dialog box for 'Reboot Scheduling'. It has two sections: 'Reboot Scheduling' and 'Recurrence'. In the 'Reboot Scheduling' section, the 'Enable' radio button is selected. In the 'Recurrence' section, the 'Everyday' radio button is selected, and all days of the week (Mon., Tue., Wed., Thu., Fri., Sat., Sun.) are checked. At the bottom, there are 'OK' and 'Cancel' buttons.

Reboot Scheduling: Enable Disable

Reboot Time: 23 h 30 min

Recurrence: Everyday Specified

Mon. Tue. Wed. Thu. Fri. Sat. Sun.

OK Cancel

After the settings of the above-mentioned rule are finished, the router will be automatically rebooted at 23:30 every day.

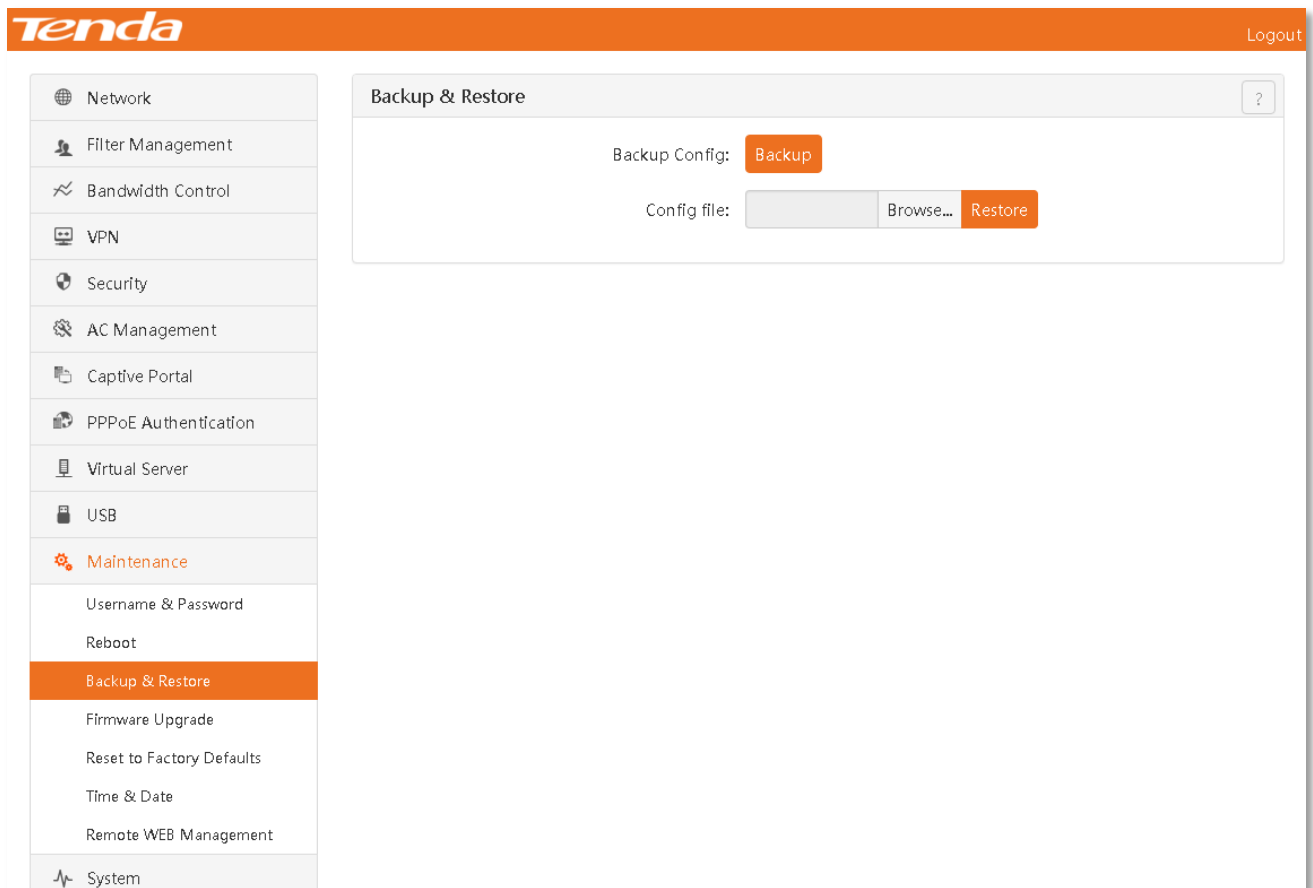
4.12.3 Backup & Restore

Overview

The existing configuration information of the router can be backed up to prevent loss of configuration information when the router is reset to factory defaults after it fails. The system will export a configuration file after backup. If the device is reset to factory defaults, the previous configurations can be restored by importing the configuration file.

- Backup: Back up the existing configuration information of the router.
- Restore: Restore previous configurations by importing a backup file of the router.

Click 『Maintenance』 > 『Backup & Restore』 to go to the configuration page.



Steps for setting backup

- 1 Click **Backup**.
- 2 Select a storage path for a backup file by referring to the prompts on the computer..

Steps for setting restoration

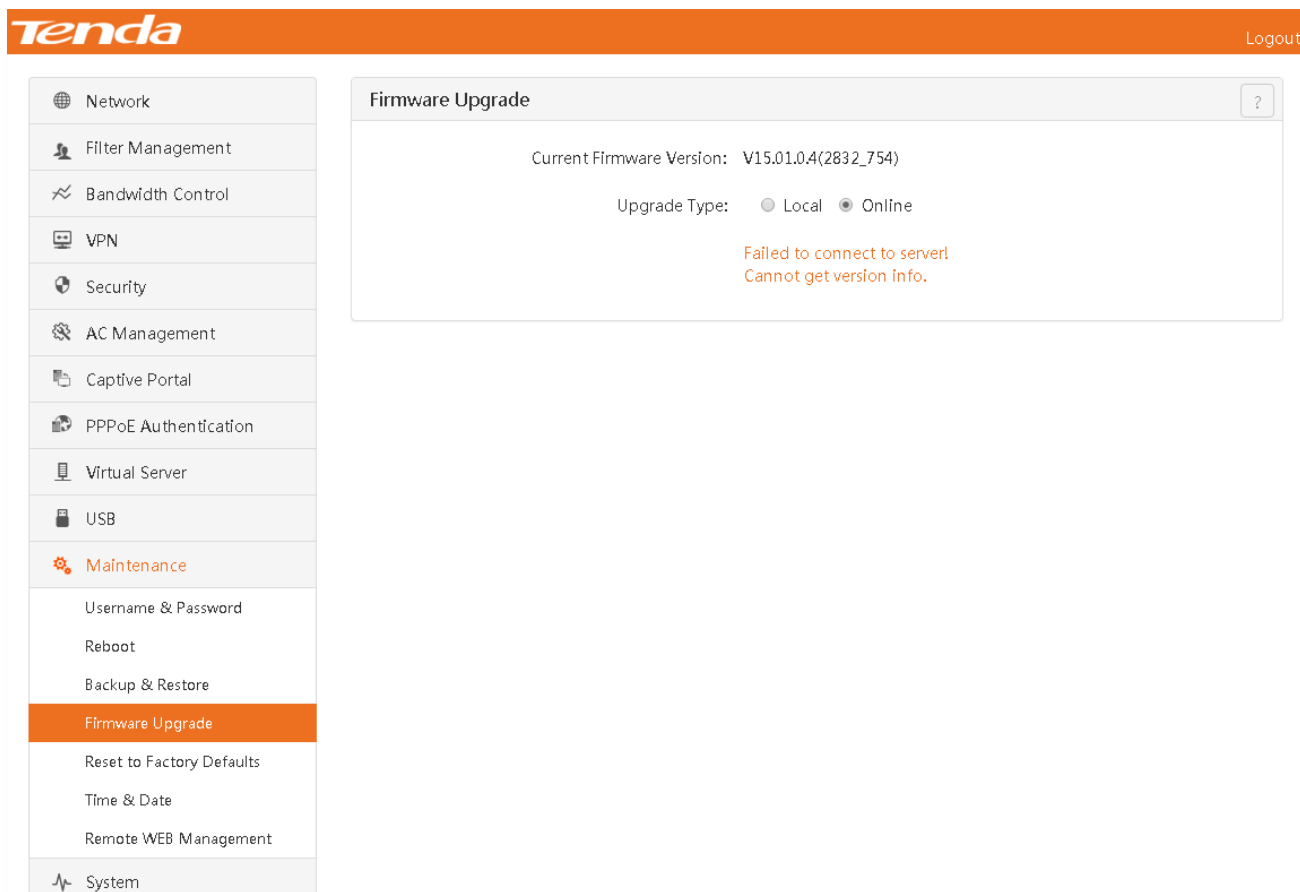
- 1 Click **Browse...** , select and load a router backup file.
- 2 Click **Restore** and until the progress bar is over.

4.12.4 Firmware Upgrade

Overview

This router supports Local and Online. The default is Online, i.e. the system automatically detects whether there is a new upgrade program, and displays any detected information about firmware upgrade.

Firmware upgrade allows you to obtain more stable firmware versions or newly added functions and to upgrade router firmware. Click 『Maintenance』 > 『Firmware Upgrade』 to go to the configuration page.



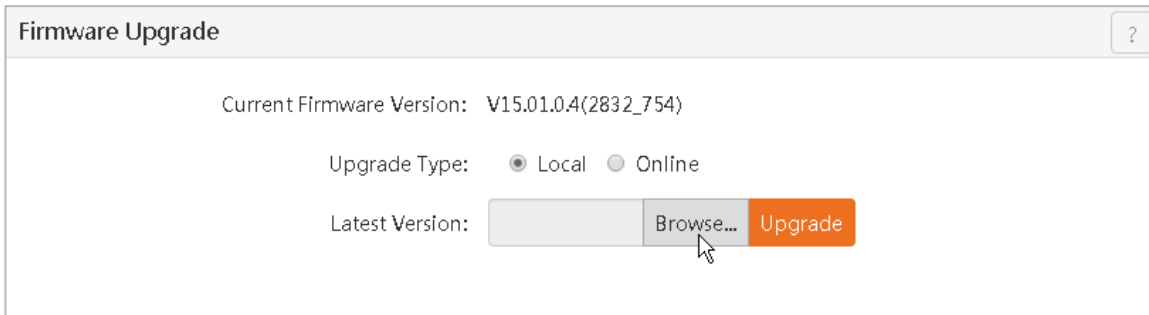
The screenshot displays the Tenda router's web interface. The top navigation bar is orange with the 'Tenda' logo on the left and a 'Logout' link on the right. A left sidebar menu lists various system settings, with 'Maintenance' expanded to show 'Firmware Upgrade' as the active selection. The main content area is titled 'Firmware Upgrade' and shows the current firmware version as 'V15.01.04(2832_754)'. Below this, the 'Upgrade Type' is set to 'Online' (indicated by a selected radio button). A red error message is displayed: 'Failed to connect to server! Cannot get version info.'

Steps for local upgrade

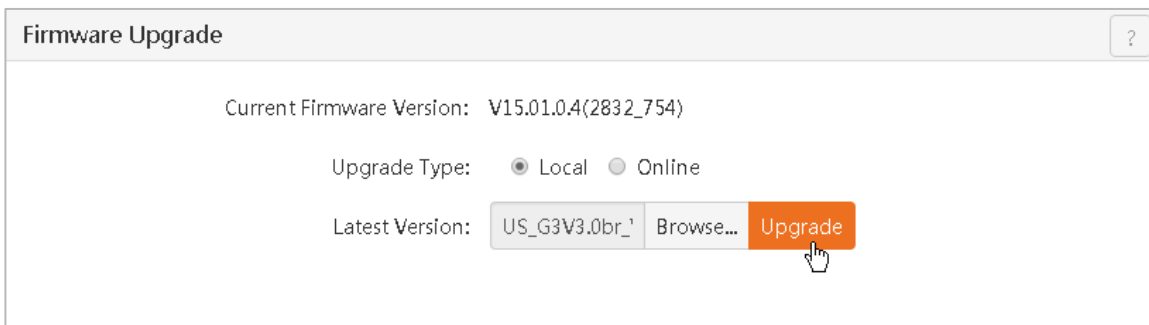
Note

- Before upgrade, check the correctness of the software. Incorrect upgrade will damage the router.
- It is recommended to connect a computer to the router with a network cable and ensure normal power supply in the upgrade process.
- After the upgrade of the router is finished, reset the router to factory defaults and reset Internet access parameters to experience the stability and value-added functions of the higher version of the firmware better.

- 1 Log in to Tenda website at <http://www.tendacn.com>, download and store the latest upgrade firmware of the router in a corresponding directory of the computer.
- 2 Click **Browse...** , find and load the upgrade firmware in the corresponding directory.



- 3 Click **Upgrade**.



A progress bar will appear. Wait until the progress bar is over.

After the the progress bar is over, the page will go to the login page. At this point, go to the system management page to reset the router to factory defaults and reset Internet access parameters.

4.12.5 Reset to Factory Defaults

Overview

You can reset the router to factory defaults when you cannot access the Internet, but fail to identify problems or when you need to log in to the management page of the router, but forget a login password.

The router supports "Reset Firmware to Factory Defaults" and "Reset Hardware to Factory Defaults" methods. The default login IP address of the router is 192.168.0.252.

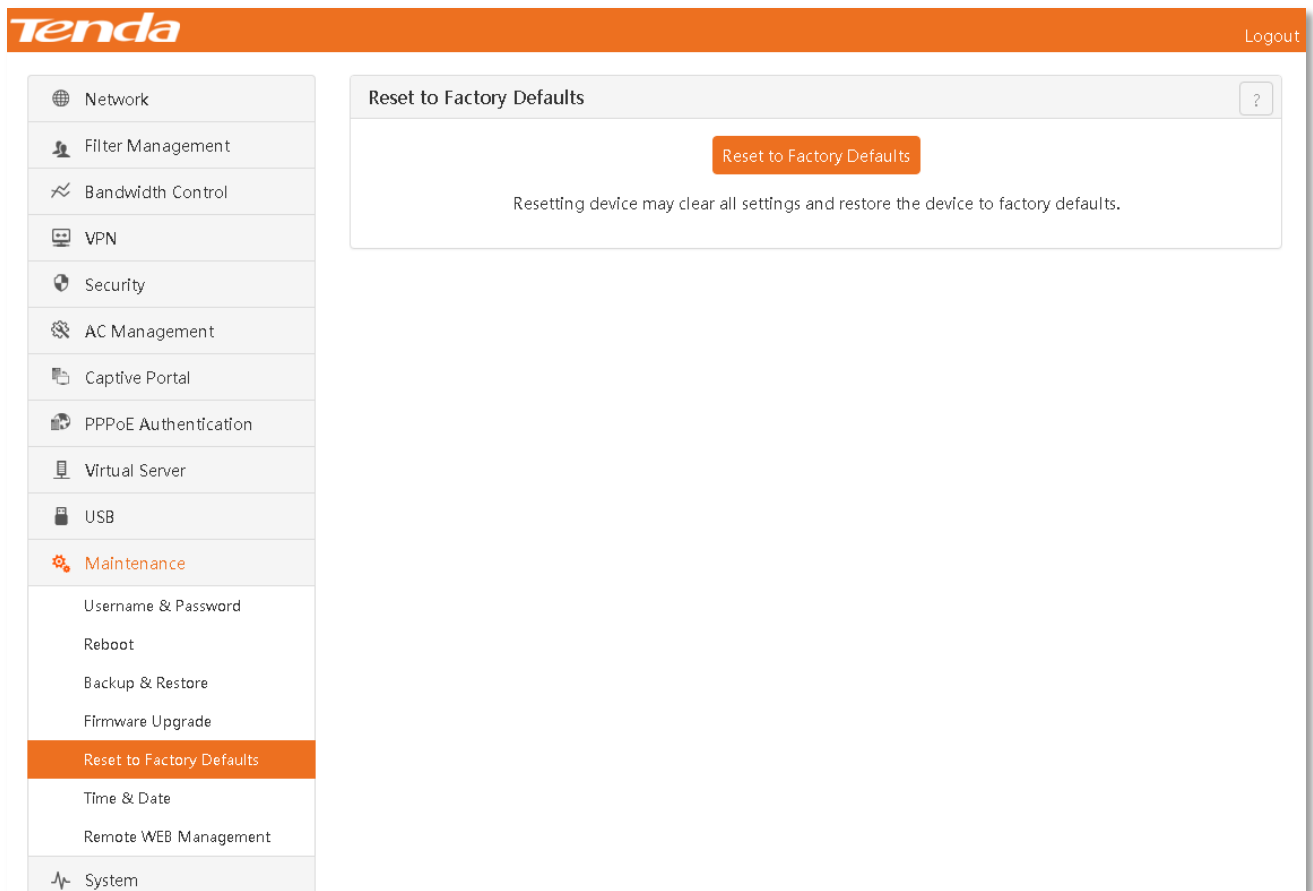
Note

- Reset to factory defaults means that all settings of the router will be lost and that the router must be reset before accessing the Internet.
- Ensure that the power supply of the router is normal in the process of reset to factory defaults.

Reset to factory defaults from the web management page

Click 『Maintenance』 > 『Reset to Factory Defaults』 to go to the configuration page.

Click **Reset to Factory Defaults** to restore the router to factory state.



Reset to factory defaults using the RESET button

In power-on state, press and hold the RESET button on the front panel with a spike for 8s and release it. Wait approximately 45s.

4.12.6 Time & Date

Overview

This section describes how to set time & date of the router. Functions such as filter management of the router may involve time settings. Therefore, time & date of the router must be correct to ensure that the rule is valid. Click 『Maintenance』 > 『Time & Date』 to go to the configuration page.

This router supports Sync with the Internet and Custom setting methods.

The screenshot displays the Tenda router's web interface. On the left is a sidebar menu with the following items: Network, Filter Management, Bandwidth Control, VPN, Security, AC Management, Captive Portal, PPPoE Authentication, Virtual Server, USB, Maintenance (highlighted in orange), Username & Password, Reboot, Backup & Restore, Firmware Upgrade, Reset to Factory Defaults, Time & Date (highlighted in orange), Remote WEB Management, and System. The main content area is titled 'Time & Date' and contains the following settings:

- Time & Date:** Sync with the Internet, Custom
- Sync Interval:** 0.5h (dropdown menu)
- Time Zone:** (GMT + 08: 00) Beijing, Chongqing, Hong Kong, Urumqi (dropdown menu)

At the bottom of the configuration area are two buttons: 'OK' (orange) and 'Cancel' (grey).

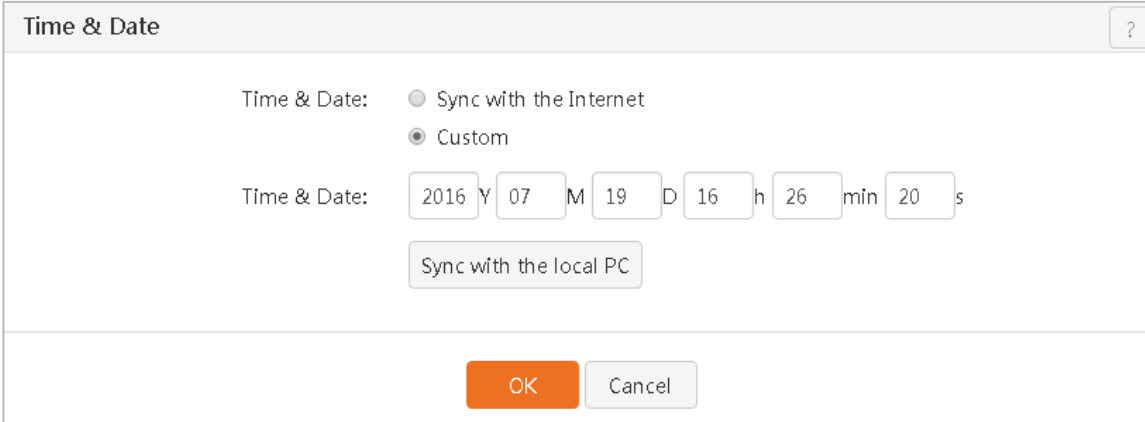


Tip

- The default method for obtaining time & date of the router is Sync with the Internet. After router networking is successful, the router will automatically synchronize time for a time zone according to a time calibration cycle.
- After the router is shut down, time information will disappear. After the router is turned on and connected to the Internet next time, the router will automatically obtain time for a time zone so that all settings about time become valid.

Steps for manually setting time & date

- 1 **Time & Date:** Click Custom
- 2 **Time & Date:** Click **Sync with the local PC.**
- 3 Click **OK.**

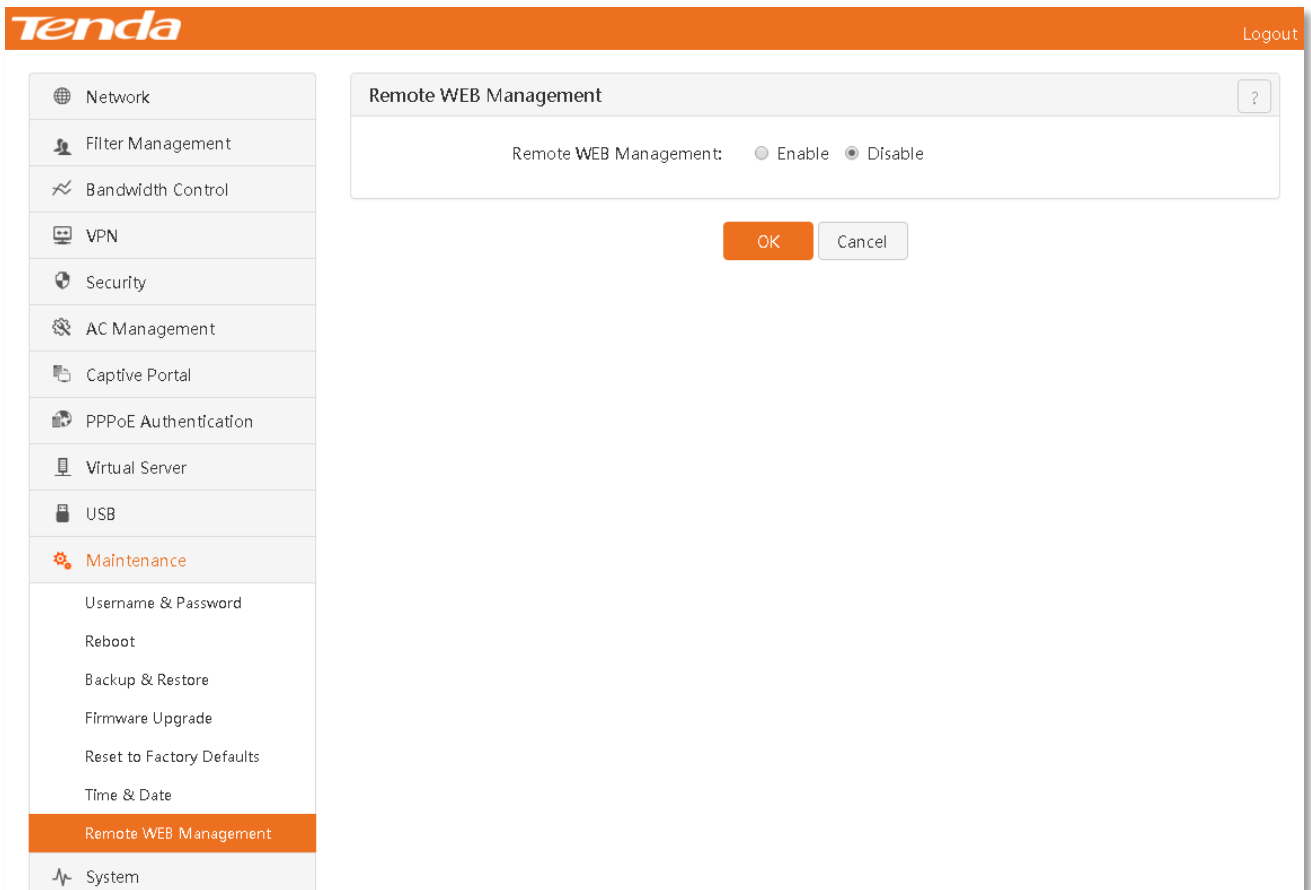


The screenshot shows a dialog box titled "Time & Date" with a help icon (?) in the top right corner. Inside the dialog, there are two radio button options: "Sync with the Internet" (unselected) and "Custom" (selected). Below these options, the current time and date are displayed as "2016 Y 07 M 19 D 16 h 26 min 20 s". A button labeled "Sync with the local PC" is positioned below the time display. At the bottom of the dialog, there are two buttons: "OK" (highlighted in orange) and "Cancel".

4.12.7 Remote WEB Management

Overview

In general, only the clients connected to the router with a network cable can log in to the web management page of the device. If necessary, you can remotely access the WEB UI of the device via the WAN interface. Click 『Maintenance』 > 『Remote WEB Management』 to go to the configuration page.



After a rule is enabled, the page is shown in the figure below.

Remote WEB Management
?

Remote WEB Management: Enable Disable


WAN: WAN0 WAN1

Allowed Internet User(s):

Port:

Parameter description in the page:

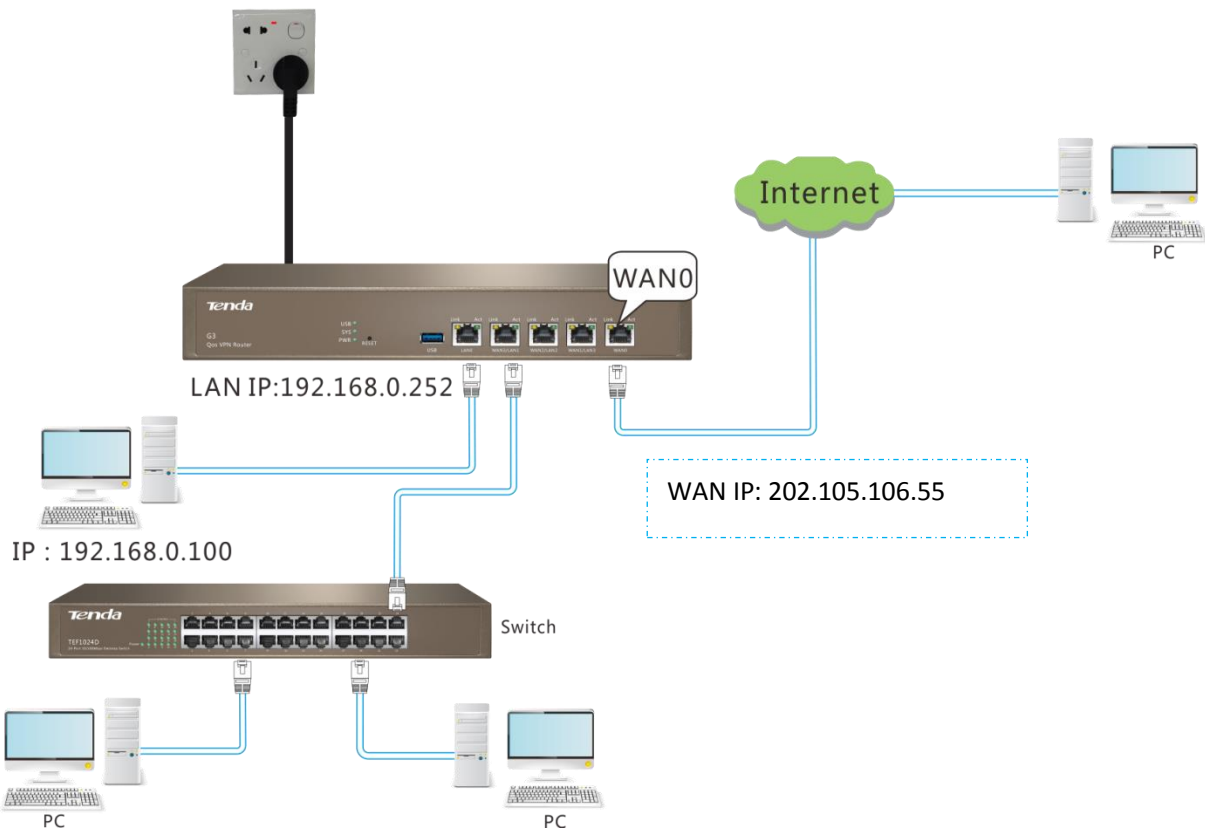
Parameter	Description
Remote WEB Management	Enable/Disable the remote web management function. The default is Disable .
WAN	Router WAN port, i.e. WAN port used to remotely access the router.
Allowed Internet User(s)	Authority to remotely access the router. <ul style="list-style-type: none"> Anyone: All computers on the Internet can log in to the router web page. It

	<p>is not recommended to select this item for network security.</p> <ul style="list-style-type: none">• Someone: Only the computers with specified IP addresses can log in to the router web page.
Port Number	<p>Port number used during remote management on the device. The default is 8088 and can be modified as needed.</p> <p> Tip</p> <p>Ports 1-1,024 have been occupied by known services. To avoid port conflict, it is strongly recommended to modify these ports to Ports 1,025-65,535.</p>

Example of WEB management

- **Example:** An enterprise uses a G3 enterprise router to establish a network. The IP address of the router WAN0 is 202.105.106.55. The network administrator on business trip may need to maintain the network and must remotely log in to the router management page. This can be achieved through remote WEB management.

The reference topological graph is as follows:



Configuration steps:

Step 1: Enable the remote WEB management.

- 1 **Remote WEB Management:** Click Enable.
- 2 **WAN:** Select an enabled WAN for remote management (In this example, WAN0).
- 3 Click **OK**.

Remote WEB Management ?

Remote WEB Management: Enable Disable

WAN: WAN0 WAN1

Allowed Internet User(s):

Port:

Step 2: Remotely access the router.

Log in to and manage the router by accessing <http://202.105.106.55:8088> on the browser of the remote computer (that has been connected to the Internet and has obtained a Public network IP address).

4.13 System status

System includes the following contents:

[System Info](#): View basic information about the router.

[Live Users](#): Display a list of users connected to the router.

[Traffic Statistics](#): View traffic statistics information of the current client of the router.

[Defense Logs](#): View attacks on the LAN.

[Syslogs](#): View log information of the router.

4.13.1 System Info

Click 『System』 to go to the System Info page. You can view information about the ports, system, LAN port, and WAN port of the router. Drag the scroll bar to view more information.

The screenshot shows the Tenda web interface with the 'System Info' page selected in the left sidebar. The main content area is titled 'System Info' and contains the following information:

Port Overview

LAN0 LAN1 LAN2 WAN1 WAN0

System Info

Device Name:	Multi-WAN VPN router
Time & Date:	2016-07-19 16:29:32
Uptime:	5h47min15s
Firmware Version:	V15.01.0.4(2832_754)
CPU Usage:	2%
Storage Usage:	14%

LAN

LAN MAC Address:	C8:3A:35:07:A0:50
LAN IP:	192.168.0.252

WAN

WAN0:	Plugged	WAN1:	Unplugged
Connection Type:	Dynamic IP	Connection Type:	Dynamic IP

Parameter description in the page:

Parameter	Description
Port Overview	View the connection status and role (WAN or LAN port) of the RJ45 ports of the device.
System Info	Basic information about the router, including device name, time & date, uptime, firmware version, etc.
LAN	Information about the LAN port MAC address and login IP address.
WAN	Internet access information of the router WAN port, including connection type, IP address information, connection status, etc.

4.13.2 Live Users

Click 『System』>『Live Users』 to go to the configuration page. You can view the quantity of DHCP user, VPN user, PPPoE user, captive portal, and IPSec connected to the router.

The screenshot shows the Tenda router's web interface. The top navigation bar includes the Tenda logo and a 'Logout' button. A sidebar menu on the left lists various system settings, with 'System' highlighted in orange and 'Live Users' selected. The main content area is titled 'Live Users' and features a summary dashboard with five categories: DHCP User (1), VPN User (0), PPPoE User (0), Captive Portal (0), and IPSec (0). Below the dashboard is a table listing active users:

Item	IP Address	MAC Address	Uptime	Remaining
1	192.168.0.159	C8:3A:35:D5:75:A6	0d5h3min56s	29min

Parameter description in the page:

Parameter	Description
DHCP User	Quantity of clients that obtain IP addresses from the DHCP server of the router.
VPN User	Display the quantity of VPN clients connected to the VPN server of the router after the VPN server function is enabled.
PPPoE User	Display the quantity of clients that perform PPPoE authentication after PPPoE authentication is enabled.
Captive Portal	Display the current quantity of clients that perform captive portal after captive portal is enabled.
IPSec	Display the quantity of IPSec tunnels that have been successfully set after IPSec is enabled.

4.13.3 Traffic Statistics

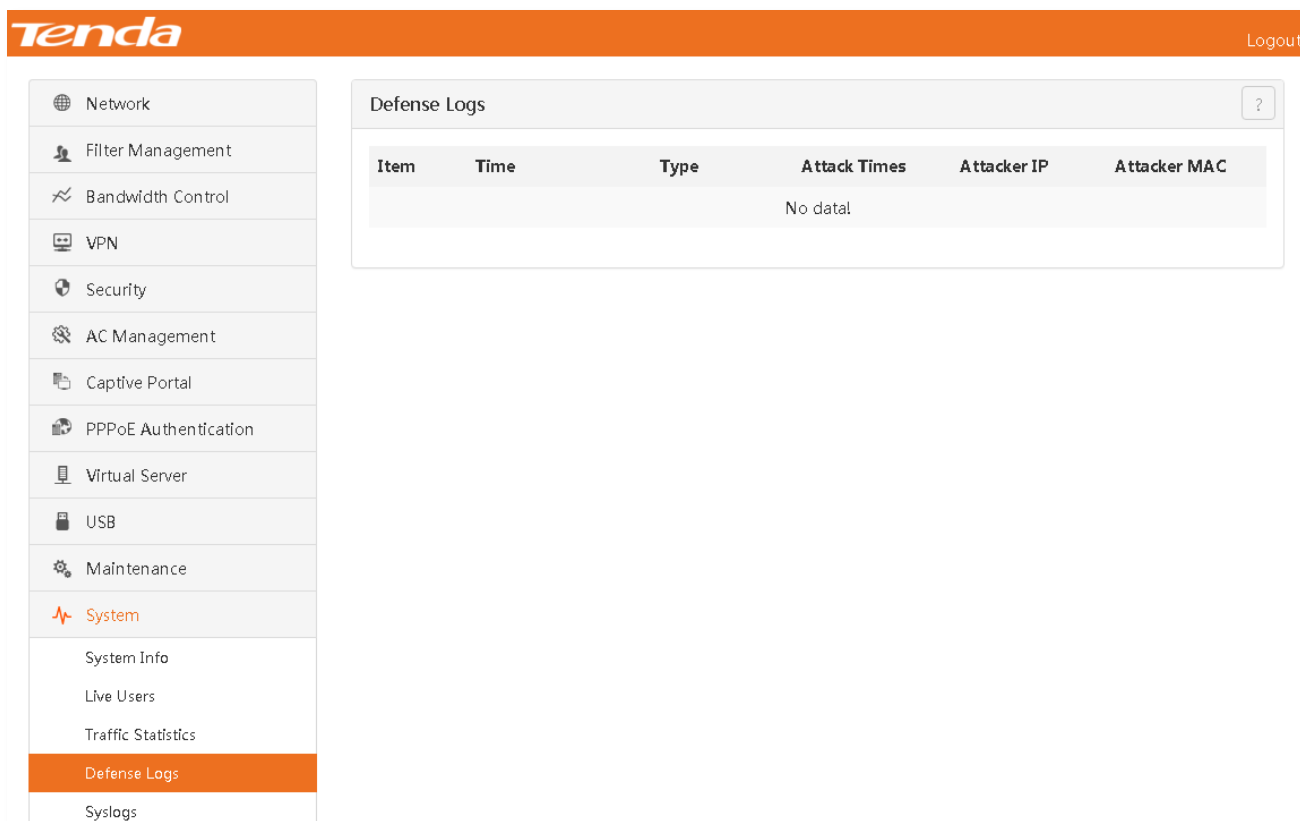
Click 『System』 > 『Traffic Statistics』 to go to the configuration page. You can view current traffic statistics information of router clients.

The screenshot shows the Tenda web interface. The top navigation bar includes the Tenda logo and a 'Logout' button. The left sidebar menu has 'System' highlighted in orange. The main content area is titled 'Traffic Statistics' and features a line chart showing upstream and downstream traffic. Below the chart is a table with the following data:

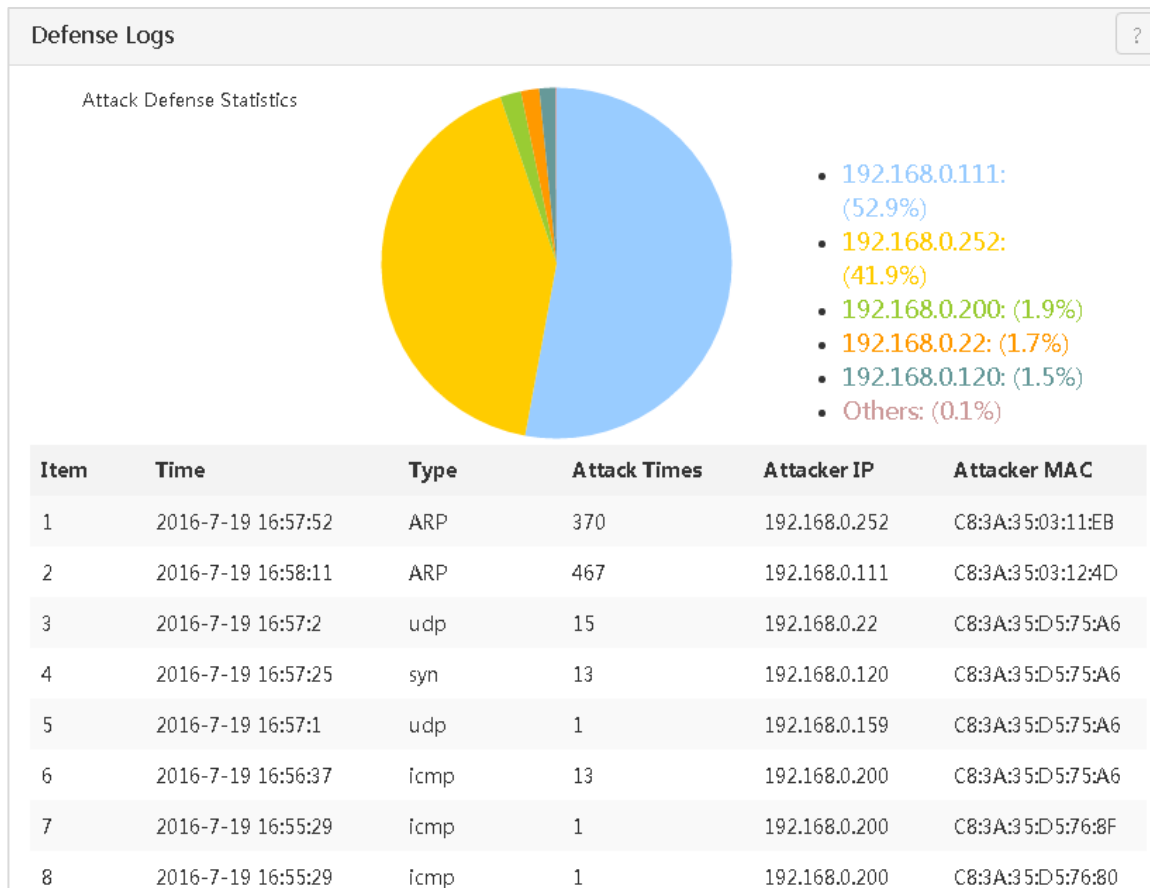
Item	IP Address	Session	Upstream Speed	Downstream Speed
1	192.168.0.159	29	0KB/s	0KB/s
2	192.168.0.205	1	0KB/s	0KB/s

4.13.4 Defense Logs

Click 『System』 > 『Defense Logs』 to go to the configuration page. You can view router defense log information.

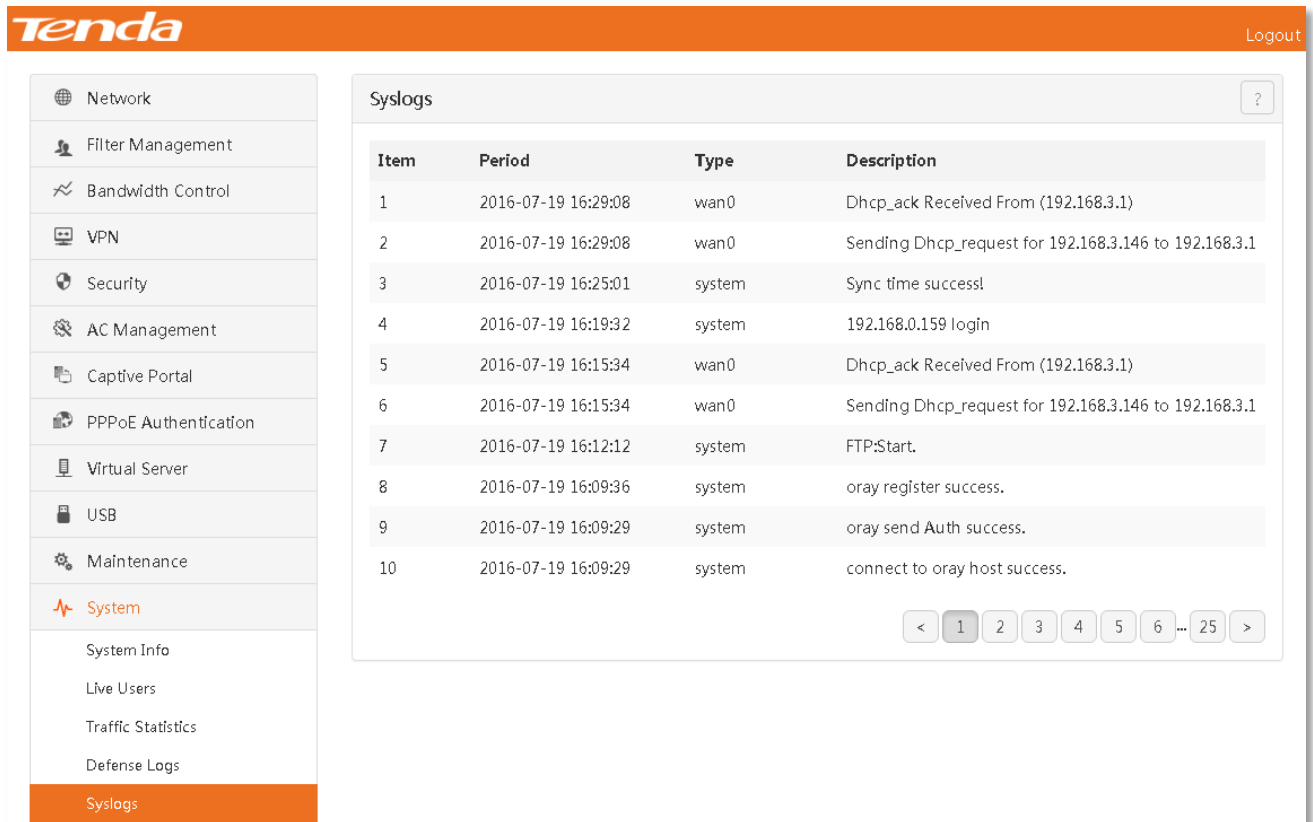


When the router is attacked, you can view relevant information, as shown in the figure below:



4.13.5 Syslogs

Click 『System』>『Syslogs』 to go to the configuration page. You can view router log information. When the router fails, you can view log information for troubleshooting.



Tenda Logout

- Network
- Filter Management
- Bandwidth Control
- VPN
- Security
- AC Management
- Captive Portal
- PPPoE Authentication
- Virtual Server
- USB
- Maintenance
- System**
 - System Info
 - Live Users
 - Traffic Statistics
 - Defense Logs
 - Syslogs**

Syslogs

Item	Period	Type	Description
1	2016-07-19 16:29:08	wan0	Dhcp_ack Received From (192.168.3.1)
2	2016-07-19 16:29:08	wan0	Sending Dhcp_request for 192.168.3.146 to 192.168.3.1
3	2016-07-19 16:25:01	system	Sync time success!
4	2016-07-19 16:19:32	system	192.168.0.159 login
5	2016-07-19 16:15:34	wan0	Dhcp_ack Received From (192.168.3.1)
6	2016-07-19 16:15:34	wan0	Sending Dhcp_request for 192.168.3.146 to 192.168.3.1
7	2016-07-19 16:12:12	system	FTP:Start.
8	2016-07-19 16:09:36	system	oray register success.
9	2016-07-19 16:09:29	system	oray send Auth success.
10	2016-07-19 16:09:29	system	connect to oray host success.

< 1 2 3 4 5 6 ... 25 >



5

Appendix

Manually set IP address

Product specification


FAQs

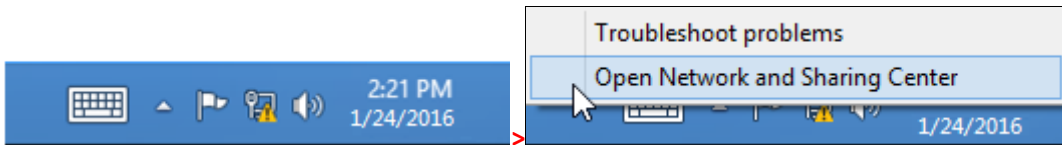
Safety and emission statement

1 Configure your computer

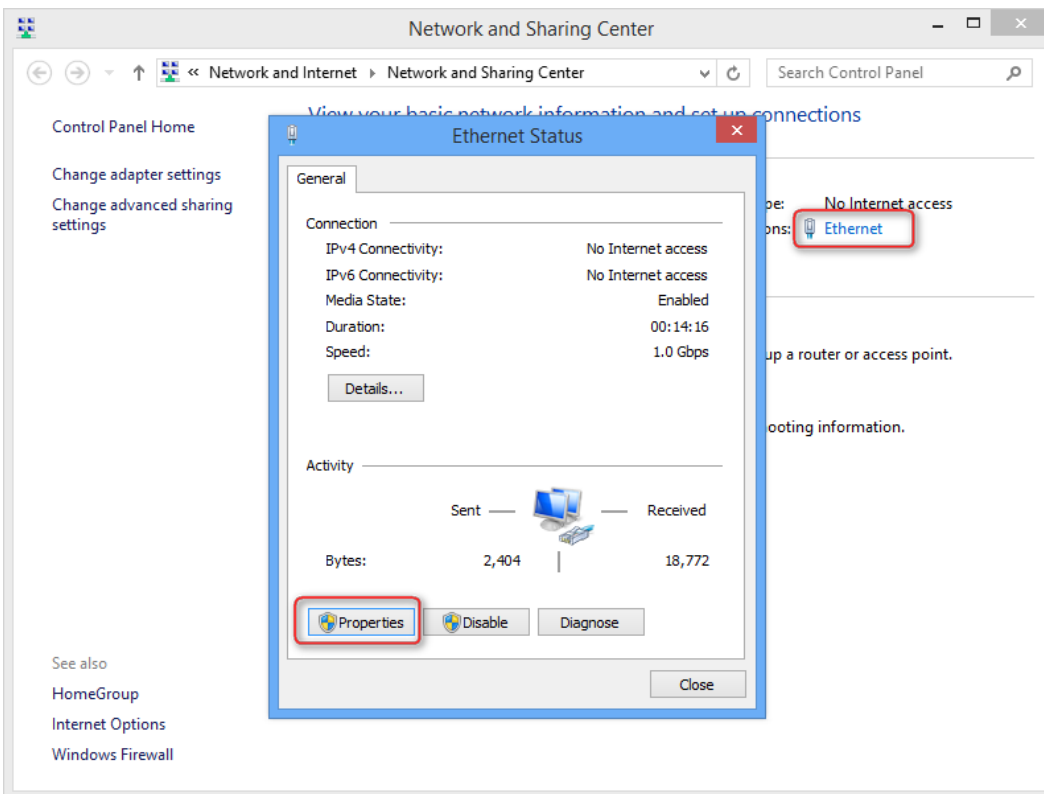
Refer to corresponding settings according to a computer operating system: [Windows 8](#), [Windows 7](#), and [Windows XP](#).

Windows 8

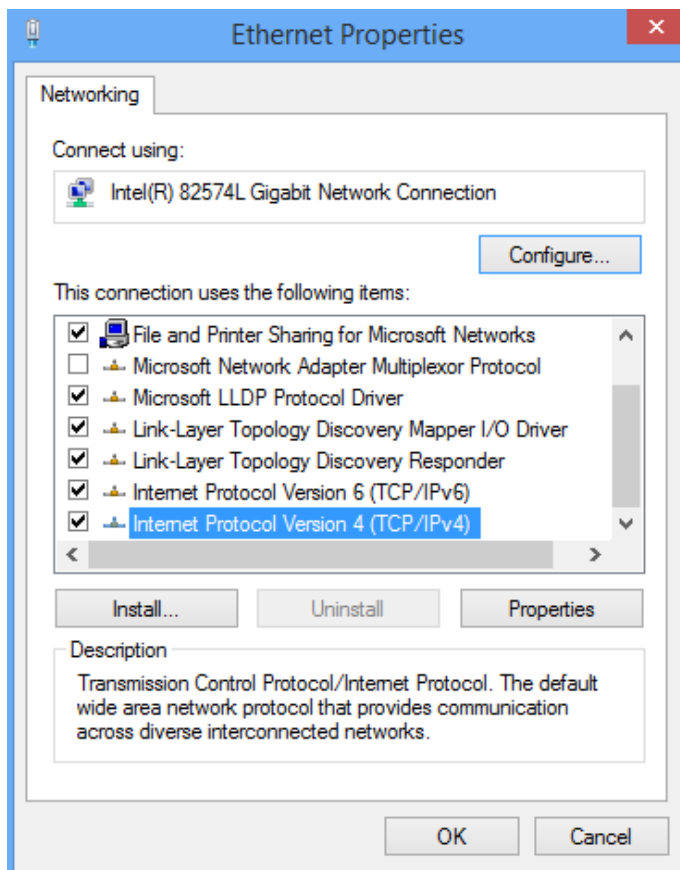
- 1 Right click the icon  on the bottom right corner of your desktop. Click Open Network and Sharing Center.



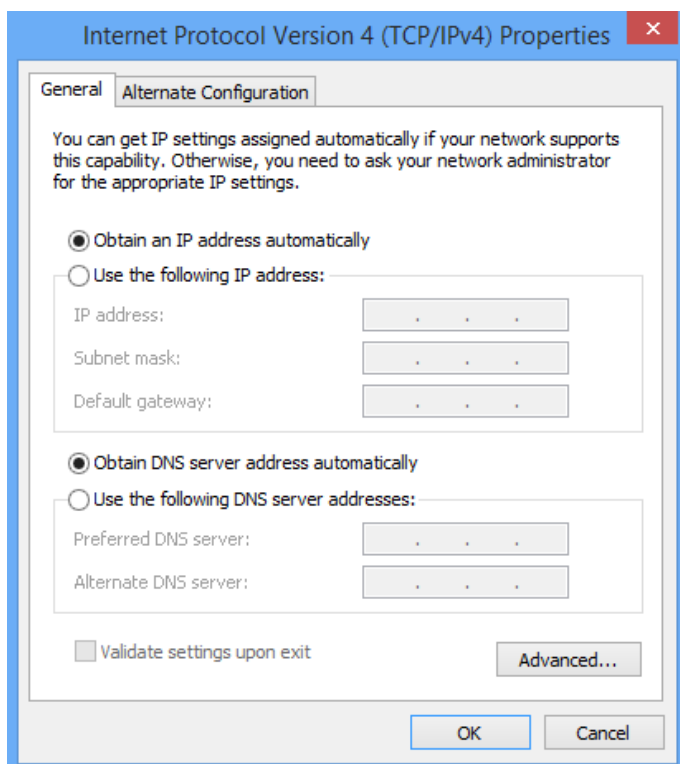
- 2 Click **Ethernet** , click **Properties**.




- 3 Find and double click **Internet Protocol Version 4(TCP/IPv4)**.

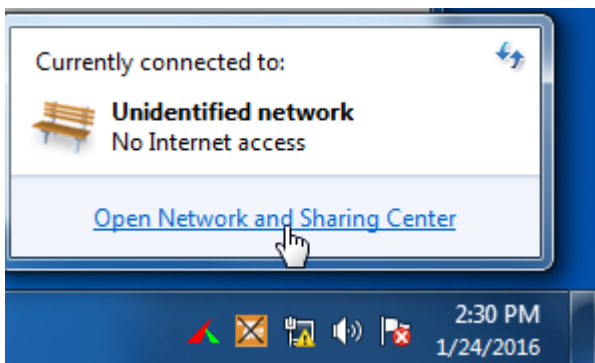


- 4 Select Obtain an IP address automatically and Obtain DNS server address automatically and click **OK**. Click **OK** again on the Ethernet Properties window.

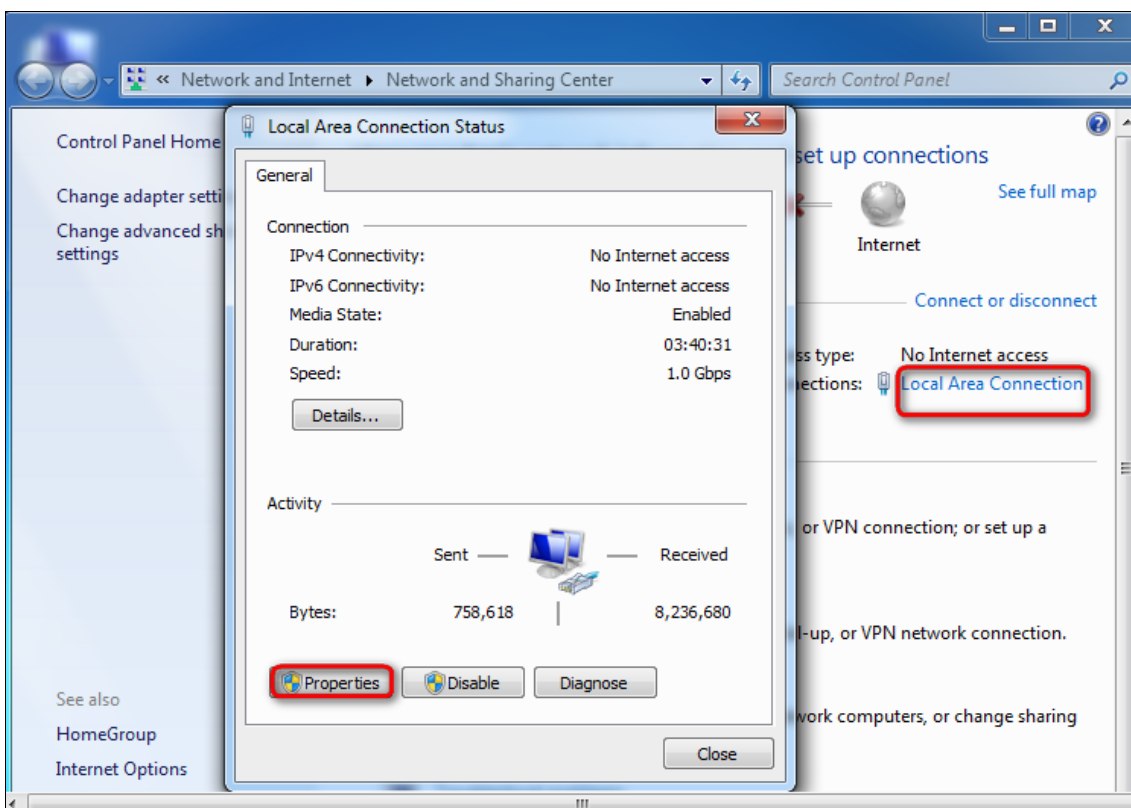


Windows 7

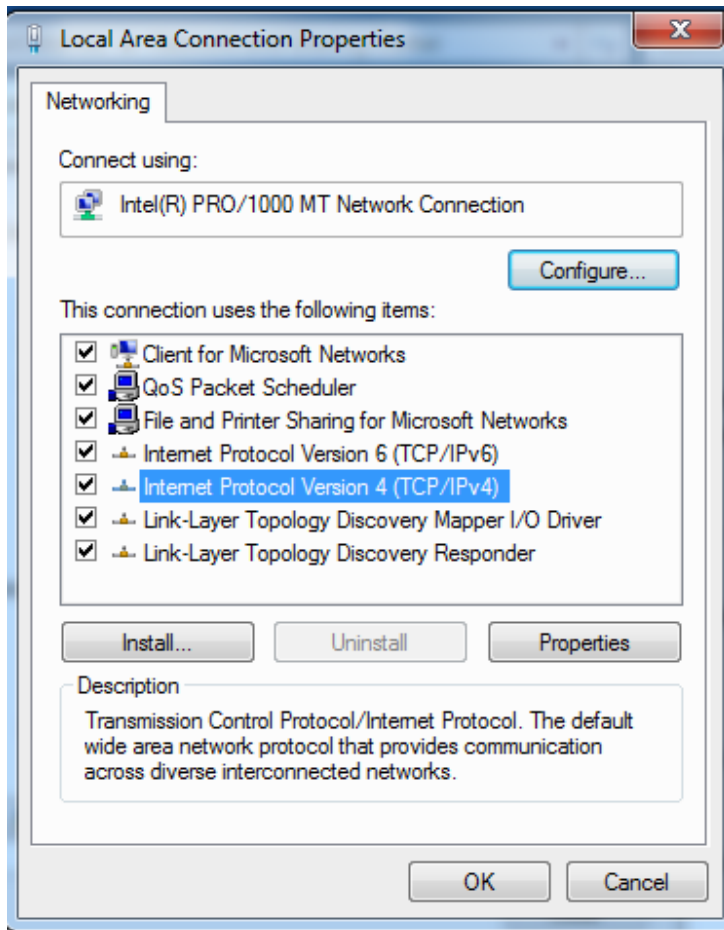
- 1 Click the icon  on the bottom right corner of your desktop. Click Open Network and Sharing Center.



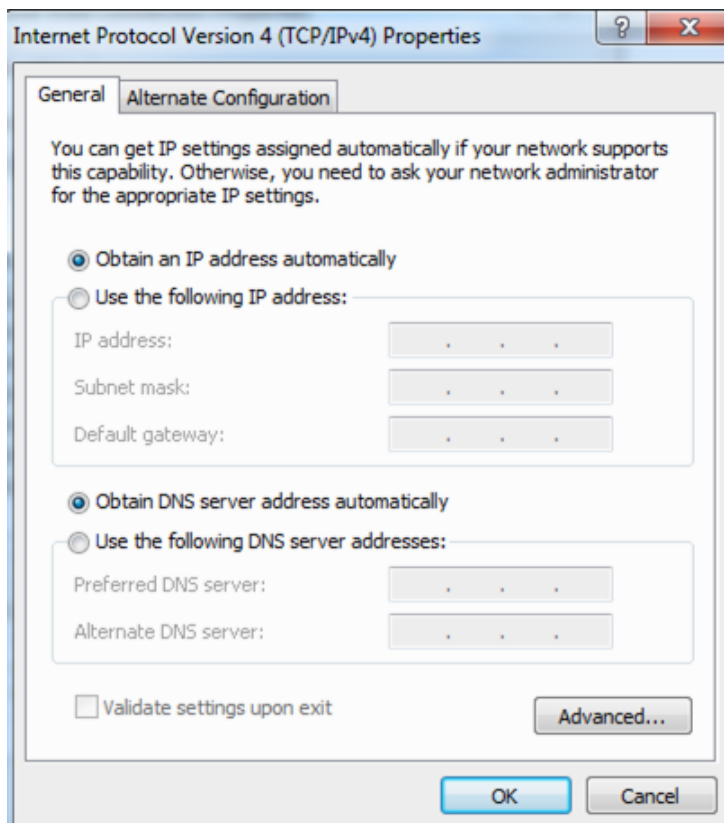
- 2 Click **Local Area Connection**, click **Properties**.



- 3 Double click **Internet Protocol Version 4 (TCP/IPv4)**.

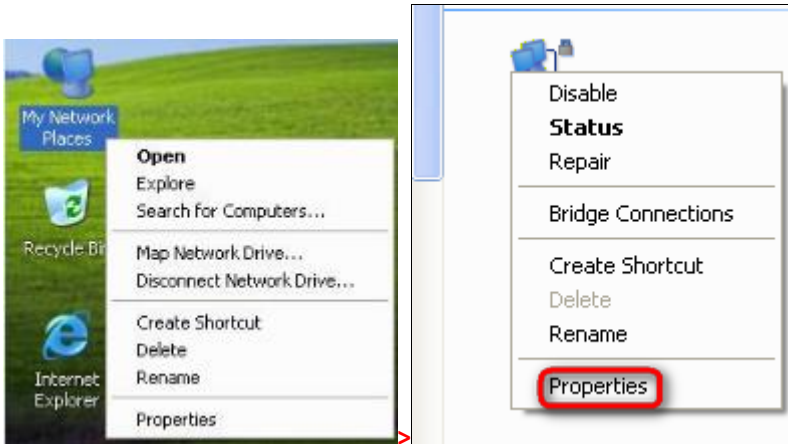


- 4 Select Obtain an IP address automatically and Obtain DNS server address automatically and click **OK**. Click **OK** on the Local Area Connection Properties window.

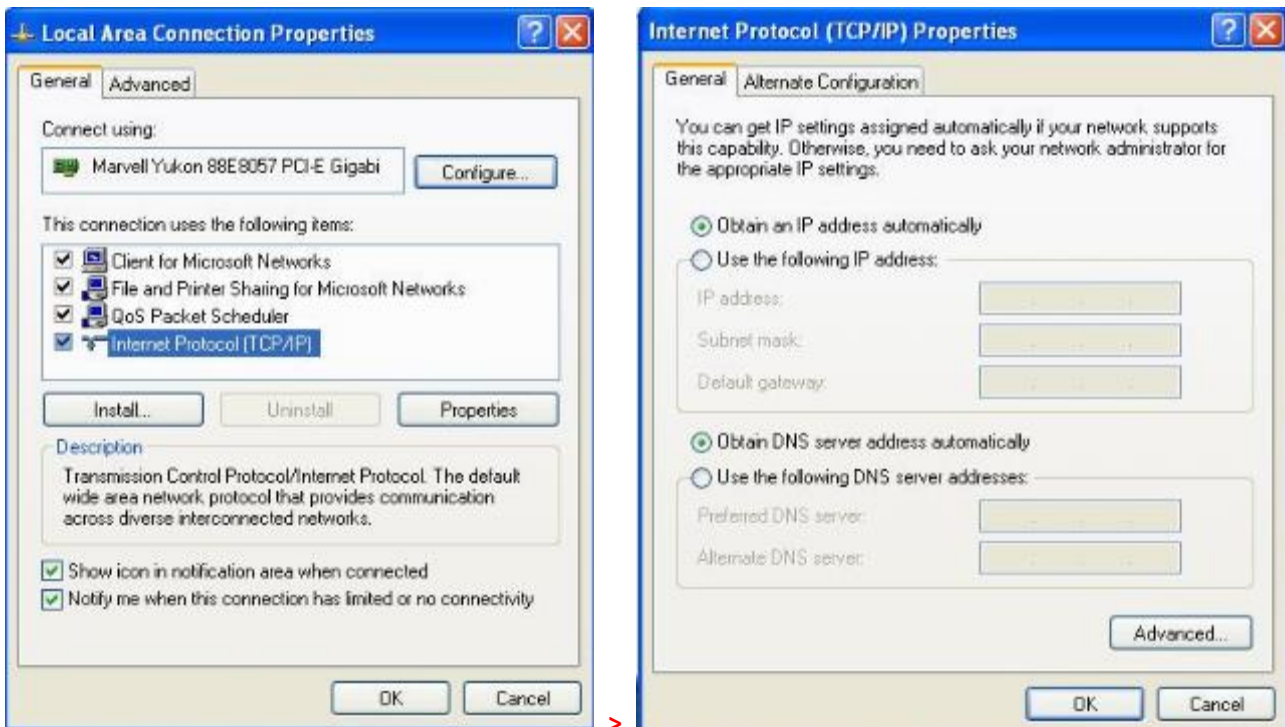


Windows XP

- 1 Right click **My Network Places** on your desktop and select **Properties**. Right click **Local Area Connection** and select **Properties**.



- 2 Scroll down to find and double click **Internet Protocol (TCP/IP)**. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically** and click **OK**.



- 3 Click **OK** on the **Local Area Connection Properties** window (see 2 for the screenshot).

2 Product Specification

Item	Specification
Device capacity	200
Memory	512MB
FLASH	128MB
Maximum concurrent connections	60000
Network port	Five 10/100/1000 Mbps self-adaption RJ45 ports of which two are WAN ports and three are LAN ports by default
Other ports	1 USB3.0 interface
Indicators	One PWR indicator, one SYS indicator, one USB indicator. every RJ45 port provided with one Link indicator and one Act indicator.
Button	One RESET button
Operating Storage temperature	0°C to 40°C -40°C to 70°C
Operating Storage humidity	10% to 90% RH (Non-condensing) 5% to 90% RH (Non-condensing)
Power input	100-240V AC, 50/60Hz
Power consumption	≤ 12W
Dimensions	294mm*178mm*44mm

3 FAQs


Question 1: What to do in case of failure to go to the router management page after entering 192.168.0.252?

Answer: Please check the following aspects:

- Ensure that the network cable is correctly connected and is not loose.
- Confirm that the computer IP address is 192.168.0.X (X is 2-254 except 252).
- Clear the browser cache or use other browsers to try.
- Close the firewall or use other computers to try.
- Confirm that no other devices in the LAN have an IP address of 192.168.0.252.
- If login still fails after the above-mentioned operations, reset the device to factory defaults and log in again.

Question 2: How to select a connection method?

Answer:

Connection Type	Typical Broadband Service Method	Applicable Internet Access Characteristics
ADSL	Telephone wire/Network cable	1. There is a username and password 2. Click broadband connection () to dial up
Dynamic IP	Wired TV/Network cable	1. Connect a cable from the last router to access the Internet 2. Users who access the Internet by connecting a wired TV (The Pearl River Broadband, Wired Communication, and Topway)
Static IP	Network cable/Optical fiber	There is a fixed IP address, subnet mask, default gateway, and DNS server

Question 3: How to reset the router to factory defaults in case of failure to log in to the router management page?

Answer:

Press and hold the RESET button of the router with a spike for 8s and release it. Wait approximately 1 minute. Reset parameters after the device are reset to factory defaults. The default login address of the router is 192.168.0.252. Log in again.

Question 4: How to do if a prompt message of "IP address conflicts with other systems in the network" appears on the computer after the computer is connected to the router?

Answer:

- 1 Ensure that there are no other DHCP servers or that other DHCP servers have been shut down.

- 2 Ensure that no computers in the LAN occupy the LAN IP address of the router. LAN IP is 192.168.0.252 by default.
- 3 Ensure that no IP address statically set for a computer in the LAN is used by other computers.

For more questions, visit <http://www.tendacn.com>.

4 Safety and emission statement



CE Mark Warning

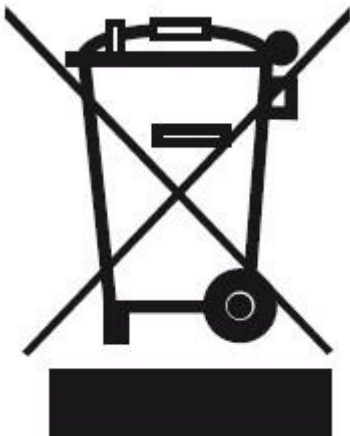
This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

For Pluggable Equipment, the socket-outlet shall be installed near the equipment and shall be easily accessible.

WARNING: The mains plug is used as disconnect device, the disconnect device shall remain readily operable.

The Product is designed for IT Power Distribution System.

NOTE: (1) The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. (2) To avoid unnecessary radiation interference, it is recommended to use a shielded RJ45 cable.



RECYCLING

This product bears the selective sorting symbol for Waste electrical and electronic equipment (WEEE). This means that this product must be handled pursuant to European directive 2012/19/EU in order to be recycled or dismantled to minimize its impact on the environment.

User has the choice to give his product to a competent recycling organization or to the retailer when he buys an new electrical or electronic equipment.



FCC Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

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, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Caution!

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

NOTE: (1) The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. (2) To avoid unnecessary radiation interference, it is recommended to use a shielded RJ45 cable.