IP-COM

User Guide

Gigabit Multi-business Router

Copyright Statement

Disclaimer

Pictures, images and product specifications herein are for references only. To improve internal design, operational function, and/or reliability, IP-COM reserves the right to make changes to the products described in this document without obligation to notify any person or organization of such revisions or changes. IP-COM does not assume any liability that may occur due to the use or application of the product or circuit layout(s) 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 purchasing this **IP-COM** product! Reading this User Guide will be helpful for configuring, managing and maintaining this product.

Intended Readers

This User Guide is intended for those who have basic technical knowledge related to the Internet and network terminology.

Conventions

This User Guide applies to SE3100v1.0. If not specifically indicated, “the device”, or “this product” mentioned in this User Guide stands for this Gigabit multi-business router.

Symbols in this User Guide:

Item	Meaning
NOTE	This format is used to highlight information of importance or special interest. Ignoring this may result in ineffective configurations, loss of data or damage to the device.
TIP	This format is used to highlight a procedure that will save time or resources.

Structure of this User Guide

Contents of all chapters in this User Guide are arranged as below:

Chapter	Content
Chapter 1 Product Overview	Introduces device appearance, package and main features.
Chapter 2 Device Installation	Introduces the device installation, installation notes, etc.
Chapter 3 Login	Introduces device login and logout.
Chapter 4 More Functions	Introduces how to set up the device’s advanced functions.
Appendix	Introduces FAQs, Technical Specifications, and Regulatory Compliance Information.

Data Download

Go to our IP-COM website ***www.ip-com.com.cn*** to download the latest data and manual.

Technical Support

Website: www.ip-com.com.cn

Tel: (86 755) 2765 3089

Email: info@ip-com.com.cn

Contents

Chapter 1 Product Overview

Overview

IP-COM SE3100 is a Gigabit business-class router that has integrated multi-WAN capability, load balance, bandwidth control, portal authentication, and VPN settings. There are three LAN/WAN multiplexing ports which can be configured as LAN ports, or WAN ports to suit your needs.

Features

- Supports load balance and DHCP server.
- Supports bandwidth control, static routing and portal authentication.
- Supports DDNS and remote device management.
- Supports VPN settings.

Package Contents

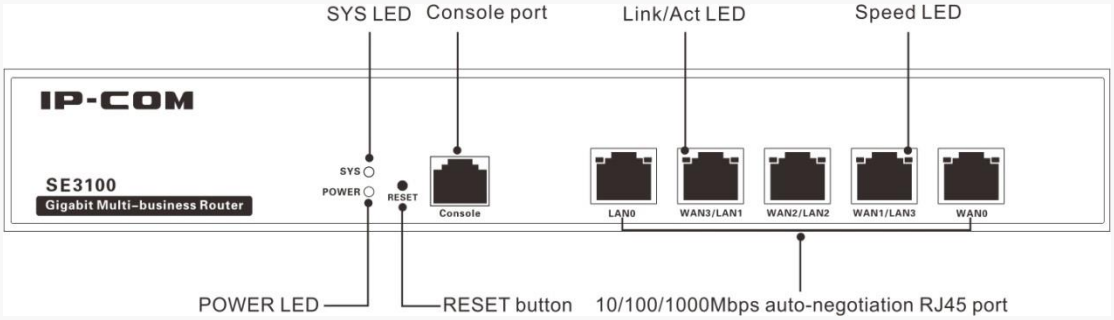
Open the box and verify the following package contents:

- SE3100 *1
- Power cord *1
- Ethernet cable *1
- Screw *6
- L-shaped bracket *2
- Rubber footpad sticker *4
- Install Guide *1

If any of the items are missing or damaged, please contact your dealer for replacement as soon as possible.

Appearance

Front Panel



↘ LED

LED	Color	Status	Description
POWER	Green	Solid	The device is receiving electrical power.
		Off	The device is malfunctioning or not connected to the power supply.
SYS	Green	Flashing	Slow flashing: Device system is working properly. Fast flashing: The system is starting up or erased internal storage (NAND-flash).
		Solid	Device system is working improperly.
		Off	The device is not yet ready.
Link/Act	Orange	Solid	The corresponding port is connected.
		Flashing	The corresponding port is transmitting data.
		Off	The corresponding port is connected improperly or not connected.
Speed	Green	Solid	The connectivity speed of corresponding port is up to 1000Mbps.
		Off	The corresponding port is disconnected or connectivity speed is up to 10/100Mbps.

↘ RESET (button)

Press this button to restore the device to factory default or to erase internal storage (NAND-flash).

When the device stays on standby:

- Press this button for five~fifteen seconds and release it; in approximately one minute, the device will reboot and restore to its factory defaults.
- Press this button for at least sixteen seconds and release it; in approximately one minute, the device will reboot and clear its internal storage.

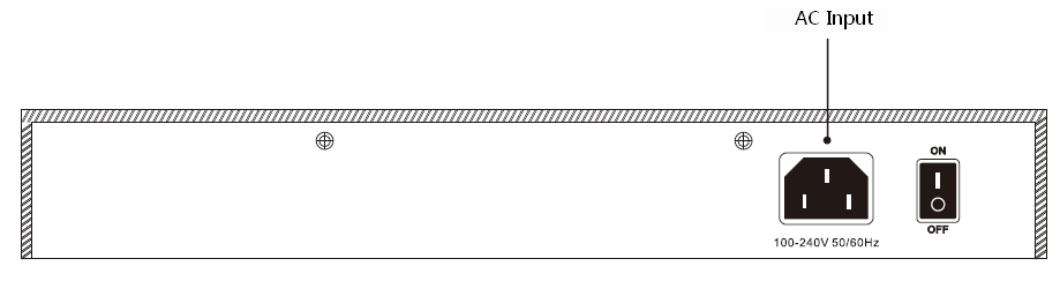
TIP

Erasing internal storage (NAND-flash) will not restore the device to factory defaults.

↘ Interface

- This device provides five 10/100/1000Mbps auto-negotiating **RJ45** ports, three of which are LAN/WAN multiplexing ports.
- **Console port**, is specially designed for developers or testers to maintain the connected clients or debug the device.

Back Panel



↘ AC Input

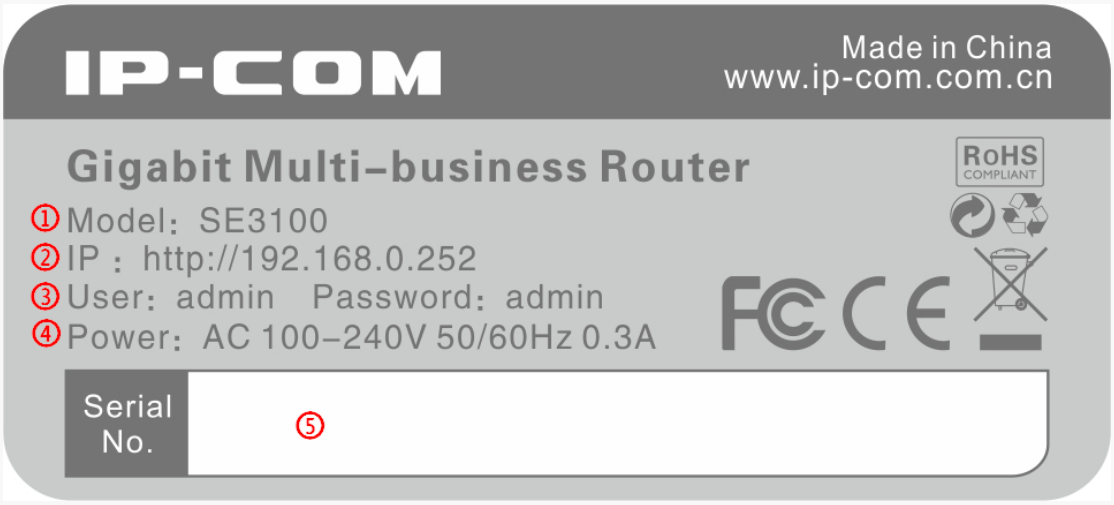
Power input port

Please use the included power cord to connect the device to the power supply.

↘ ON/OFF (button)

Power button; turn the device on/off.

Label



① Model No. of the device

② LAN IP of the device, used to access the device's Web management interface

③ Username and password to log in to the device.

④ AC input requirement

⑤ Serial number (SN) of the device. This is required if the device is sent back for maintenance.

Chapter 2 Device Installation

Installation Notes

To ensure service of this product, and for your own personal safety, please follow the note below.

Safety Alert

Install the device following static electricity precautions.

- Wear anti-static gloves while installing, and connect the device to power after finishing other installation.
- Use the included power cord to power the device.
- Make sure the input voltage matches the value which is marked on the device's label.
- Place the device in a well-ventilated and dry environment.
- Do not open the device case.
- Cut off the power connection if you want to clean the device. Do not clean the device with any liquid cleaner.
- Position the device away from a strong electrical current.

NOTE

There is an IP-COM seal on one of the cover screws. The seal must remain unbroken. The user should not break the seal as this will void the warranty.

Environmental Requests

➘ Temperature/Humidity

Item	Temperature	Humidity
Operation Environment	-10℃ ~ 45℃	10% ~ 90% RH (non-condensing)
Storage Environment	-40℃ ~ 70℃	5% ~ 90% RH (non-condensing)

➘ Anti-static Precautions

To protect the device from static electricity harm,

- Keep the device in a clean and clear environment.
- Clean the device regularly.
- Properly ground the device to efficiently dissipate static electricity.

➘ Lightning Protection

To protect the device from a lightning strike or power surge,

- Properly ground the device, rack and workbench.
- Properly cable the device, and if you need to cable outdoors, incorporate lightning arresters into the setup.

➘ Mounting Standards

Regardless of rack-mounting or desktop-mounting, confirm the following.

- Hardware which supports the device is stable.
- Position the device in a well-ventilated environment, and keep it at least 10cm free on all sides for cooling.
- Do not place any heavy objects on the device.
- Keep a vertical distance of at least 1.5cm between components for rack-mount installations.

Installation Tools

Things you'll need.

Installation

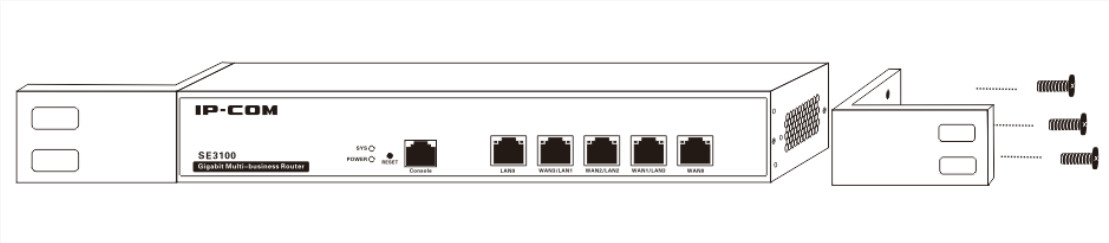
The device can be installed either in a rack or a flat surface (desktop/workbench).

A. Rack-mounting

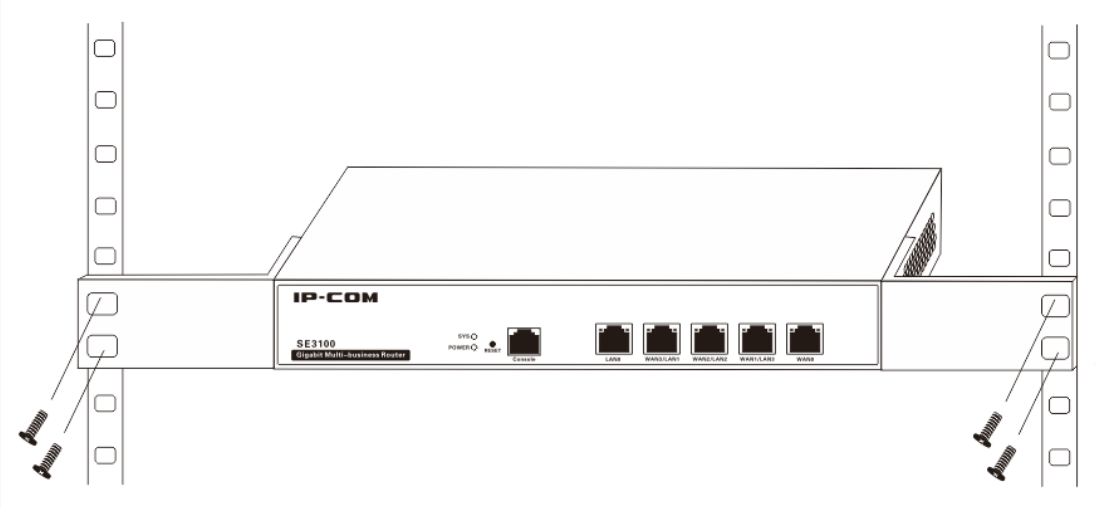
You can install the device in a standard 19-inch rack with the accessories (L-shaped brackets and screws) that come in the box.

1. Install the rack, in a location ensuring it is both stable and level.

2. Install the L-shaped brackets to the device with screws (as shown in the figure below).



3. Prepare four screws to install the device into the rack (as shown in the figure below).

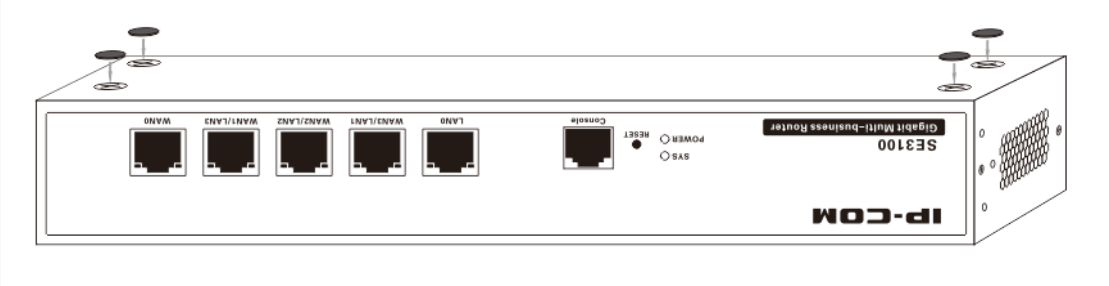


B. Desktop-mounting

You can install the device on a desktop if the rack is not available.

1. Place the device bottom up on a stable and flat desktop.

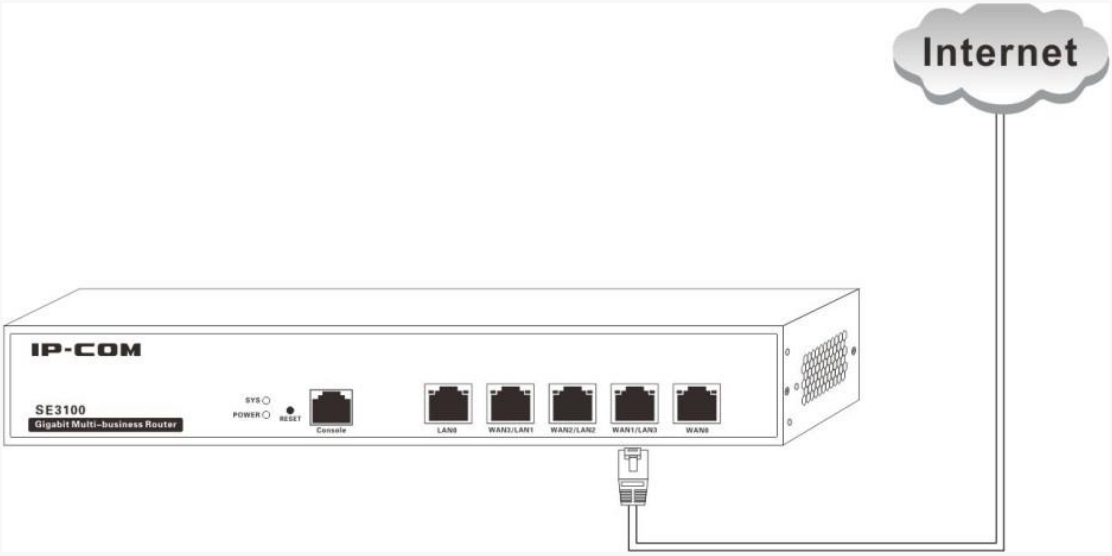
2. Attach the four rubber footpad stickers to the corresponding four corners of the bottom.



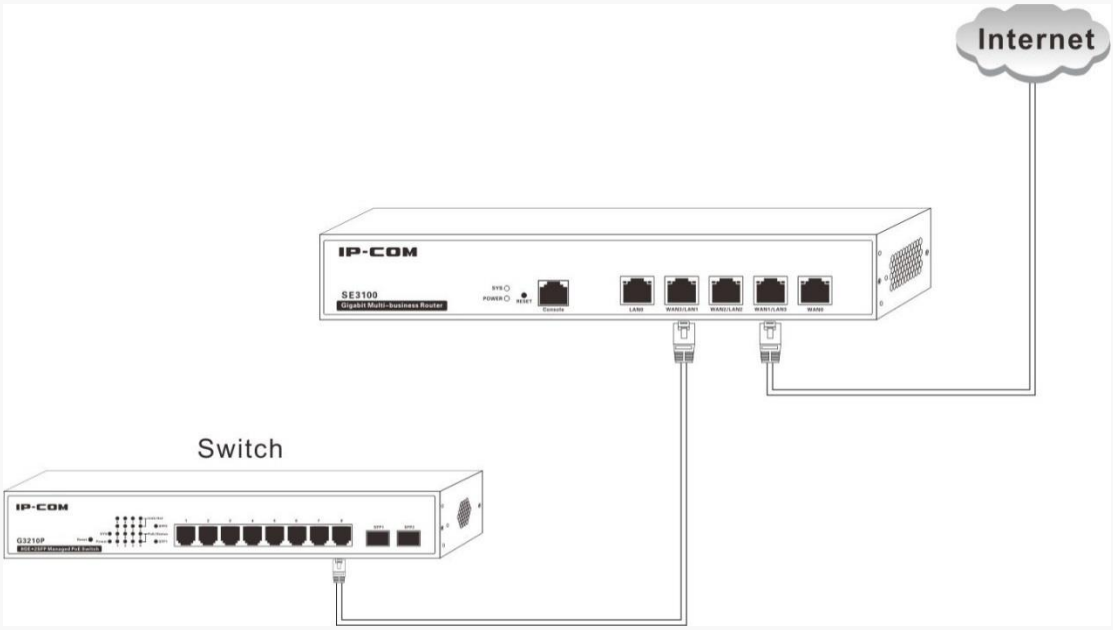
3 Gently place the device upright on the desktop.

Physical Connection

1 Plug the Internet access cable from your ISP into the WAN port on the device.

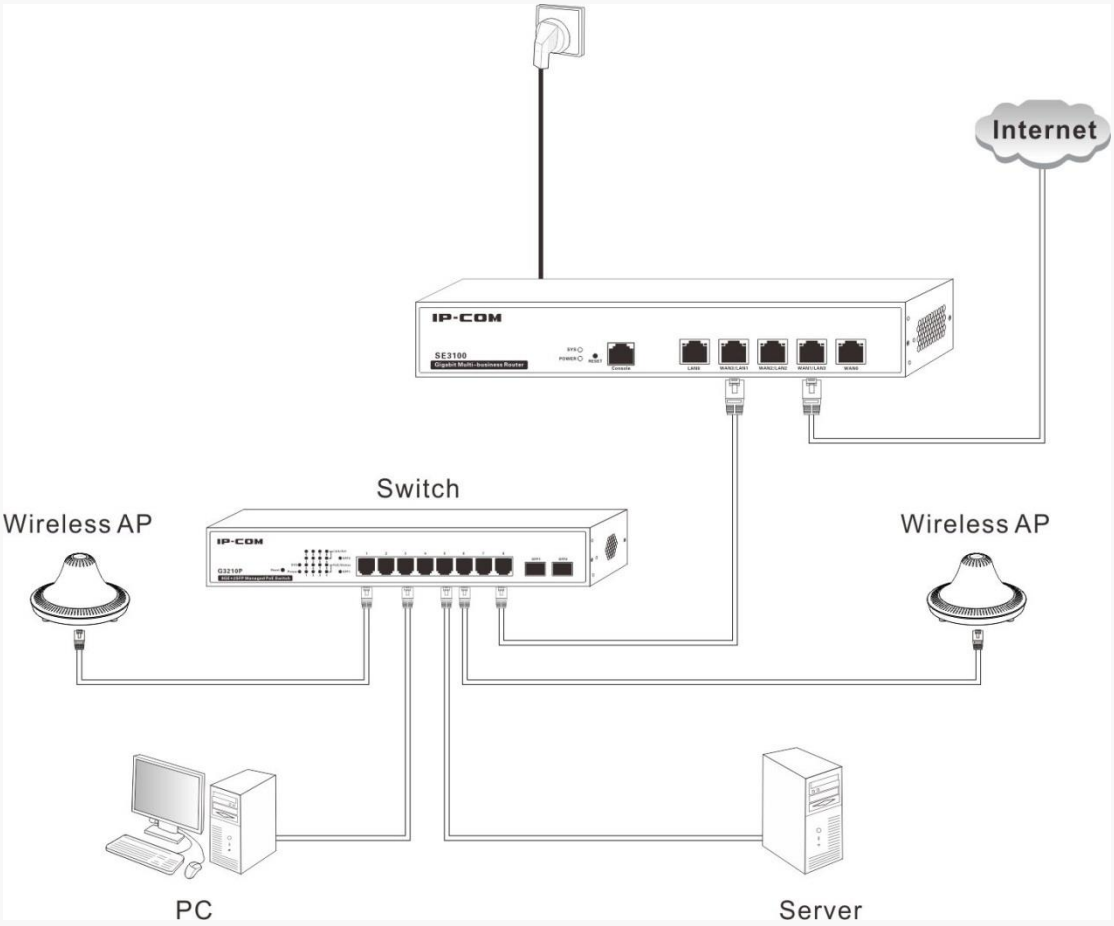


2 Connect the device to a switch via LAN port using an Ethernet cable.



❸ Connect other devices such as APs, servers or PCs, to the switch.

❹ Inspect your cabling, referring to the connection topology below. Connect the device to the power supply with the included power cord.



5 After the device is rebooted, the device will initialize its default settings. Check LEDs status, which should be displayed successively as the following:

- All LEDs (POWER, Link/Act and Speed LEDs) except "SYS" LED will light up and the system will start a self-test.
- POWER LED will remain solid; other LEDs will turn off.
- After initialization completes, the POWER LED remains solid, SYS blinks, and the Link/Act and Speed LEDs will display their working status respectively.

Chapter 3 Login

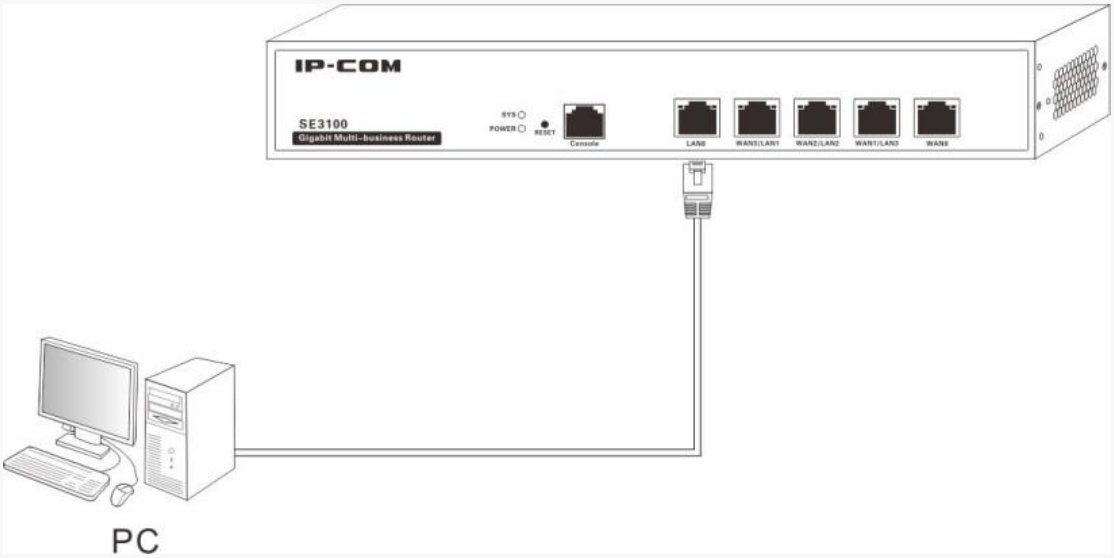
Log in to the Device

If you are setting up the device for the first time, the default parameters are needed for you to log in to the device's Web manager. The default parameters are:

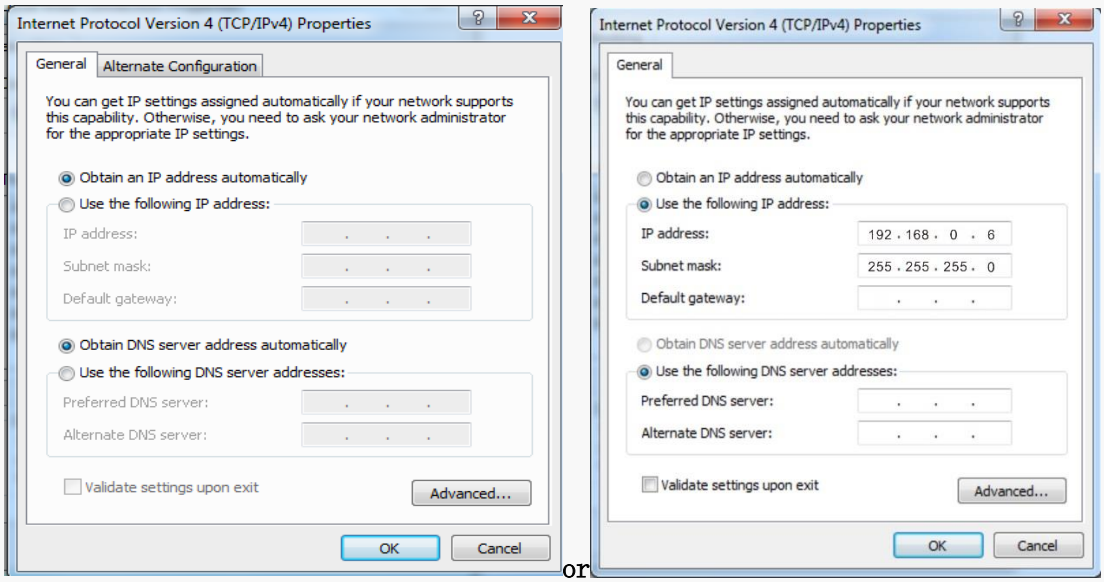
Item	Details
LAN IP Address	192.168.0.252
Username	admin
Password	admin

To log in to the device's Web manager:

1. Connect your PC to a LAN port on the device using an Ethernet cable.



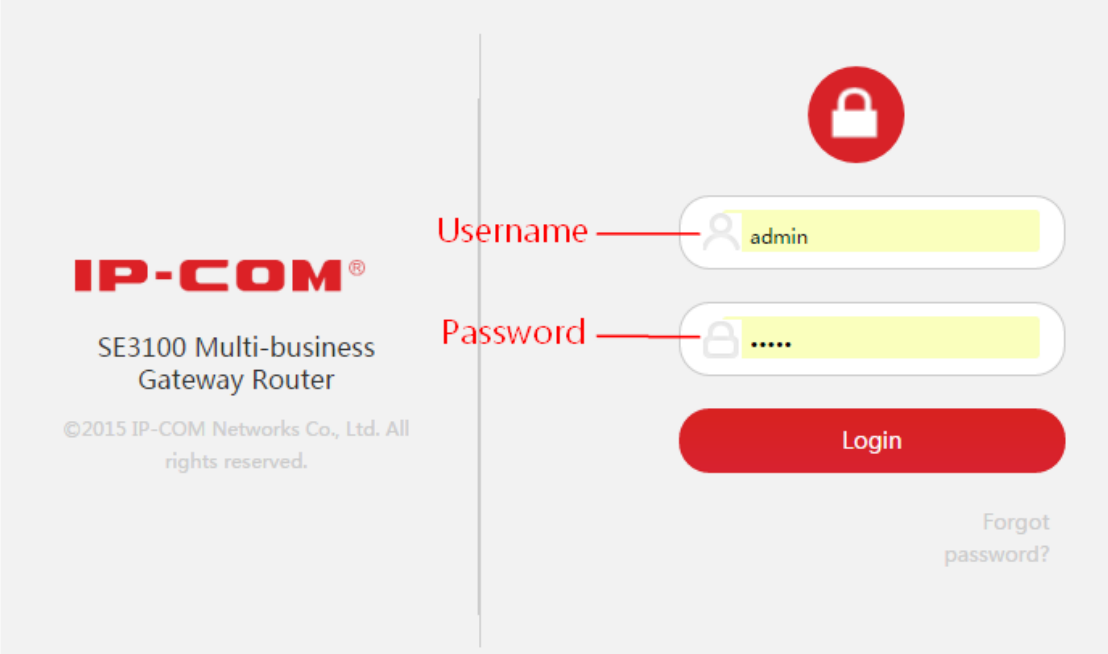
2. Set your PC as "Obtain an IP address automatically" and "Obtain DNS server address automatically". Or, configure your local PC IP address as 192.168.0.x ("x" can be any number between 2~254, excluding 252), subnet mask as 255.255.255.0.



or

❸ Launch your Web browser (Google Chrome is recommended); type 192.168.0.252 in the address bar and hit **Enter**.

❹ This will direct you to the device login page, prompting you to enter the username (default: admin) and password (default: admin), and hit **Enter**.



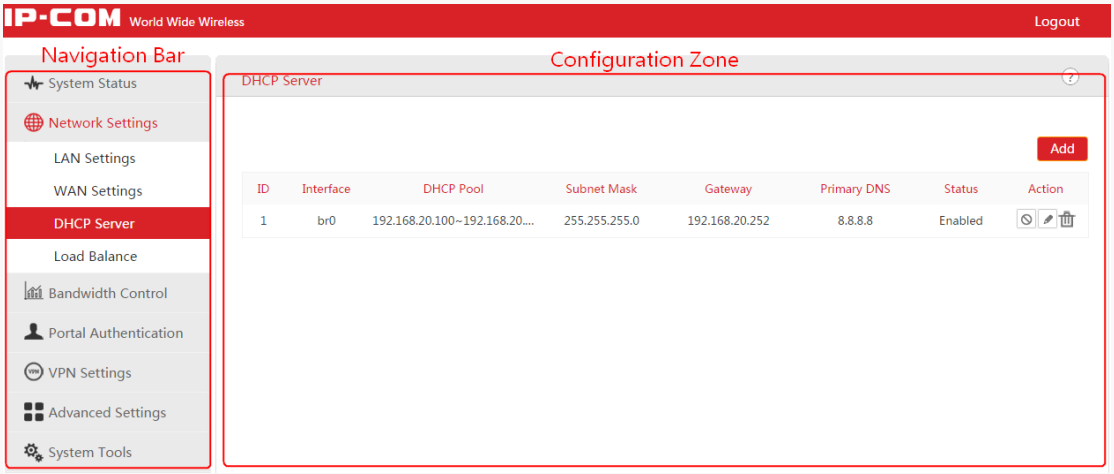
NOTE

Different Internet browsers may show different screen details. Input the correct username and password in their proper fields.

❺ When you see the configuration screen, set up or modify your configuration settings as desired.

For more functions, see Chapter 4 More Functions.

Web Management



Item	Description
Navigation Bar	Here you can select function menus. The results will be displayed on configuration zone.
Configuration Zone	Here you can set the device and view the configuration.

NOTE

Grey sections on the page cannot be modified in their current status, or they're unavailable.

Logout

Close the current screen or click Logout on the top right corner. Follow the onscreen instructions to log off.

NOTE

Closing the current device Web tab will not force current user to log off.

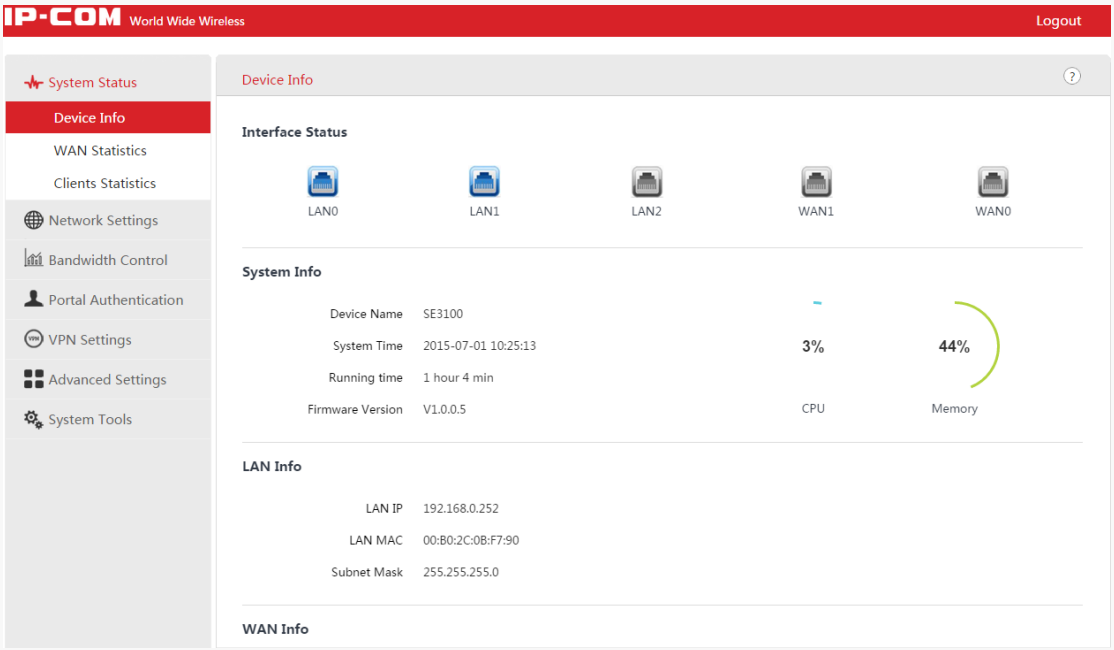
Chapter 4 More Functions

System Status

This section can help you get to know more about device info, WAN statistics and client statistics.

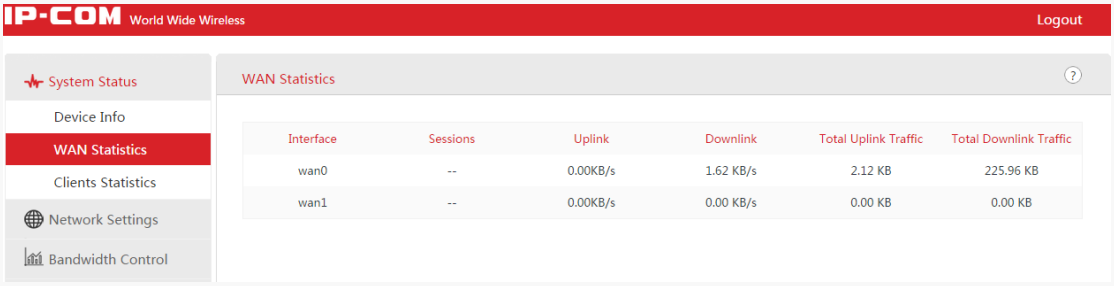
Device Info

Click **System Status > Device Info** to enter page below where you can view the device info, including interface status, system status, LAN info and WAN info.



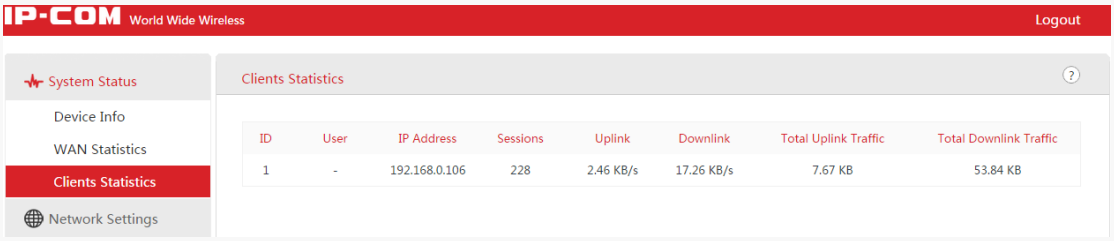
WAN Statistics

Click **System Status > WAN Statistics** to enter page below where you can view traffic statistics on WAN port (s).



Clients Statistics

Click **System Status > Clients Statistics** to enter page below where you can view real-time traffic statistics of connected hosts.

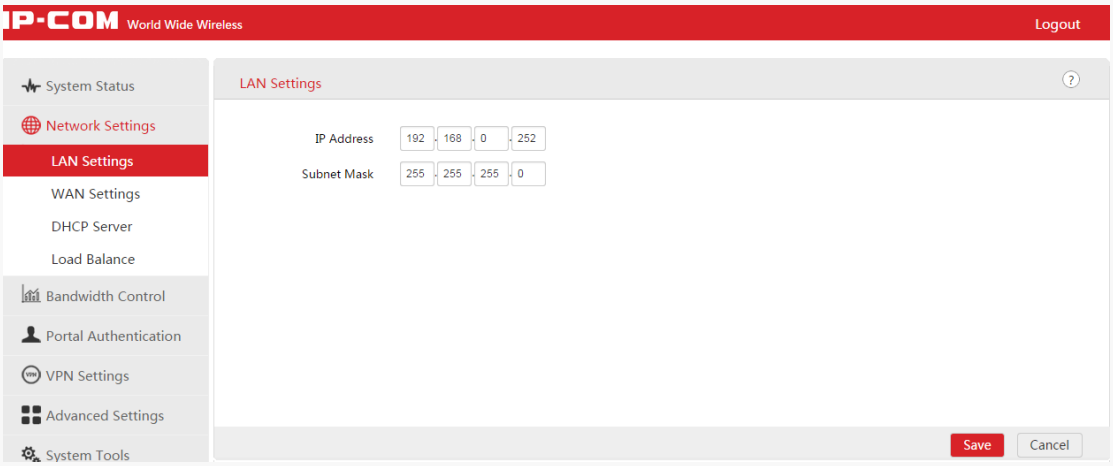


Network Settings

This section instructs you on setting up your device to the Internet.

LAN Settings

To configure the LAN IP address for the device, click **Network Settings > LAN Settings** to enter page below:



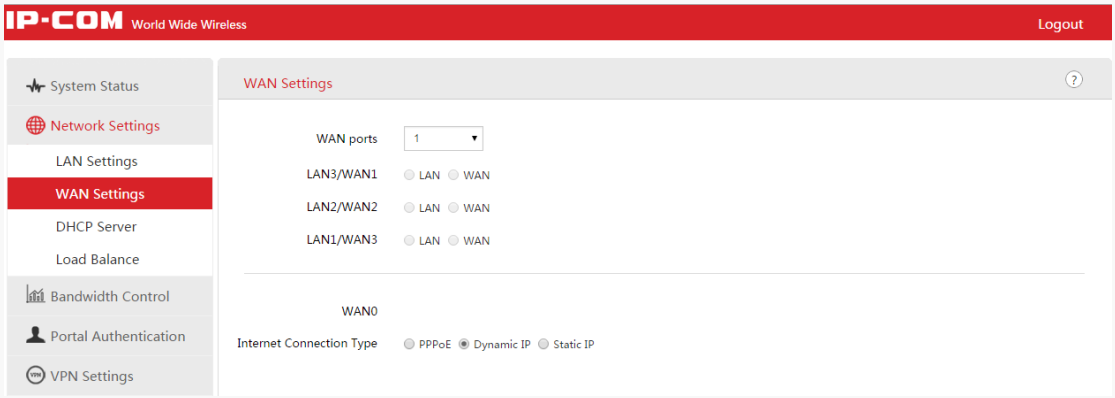
NOTE

1. To ensure a normal communication between the host and the Internet, the default Gateway of the host should be set to the LAN IP address of this device.

2. If the LAN IP address is changed, please use the new IP address to login the device.

WAN Settings

This page allows you to select the total number of WAN ports you prefer to use and configure the WAN Network for the device. By default, only **WAN 0** is the WAN port (Note that WAN1/LAN3, WAN2/LAN2, WAN3/LAN1 are LAN/WAN multiplexing ports). You can select the number of WAN ports from the **WAN ports** drop-down menu. Up to 4 WAN ports are supported on this device. Click **Network Settings > WAN Settings** to enter page below:

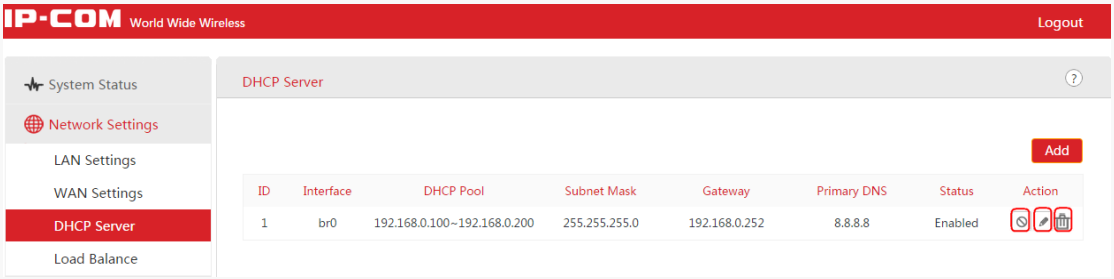


Three Internet connection types are available for the WAN port (s): PPPoE, Dynamic IP and Static IP.

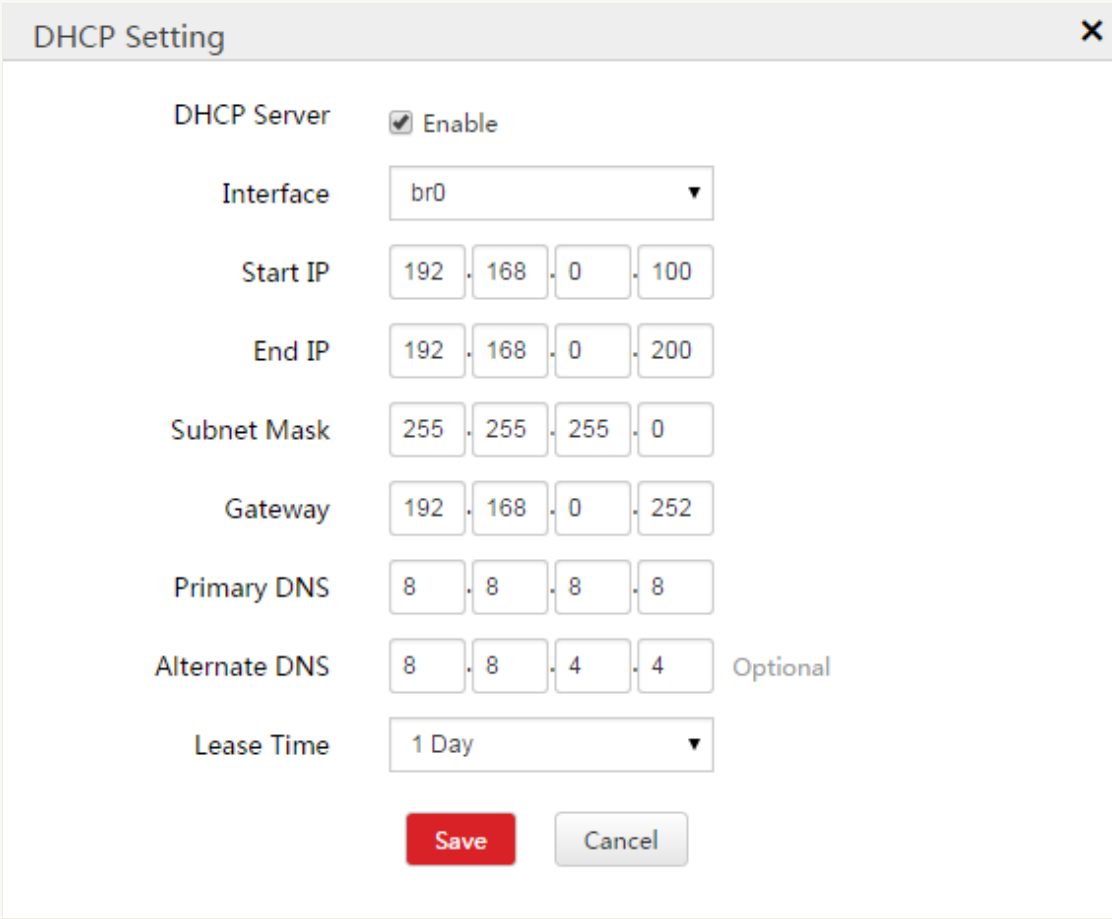
- **PPPoE:** Select **PPPoE**, if you've been provided the ISP user name and password.
- **Dynamic IP:** Select **Dynamic IP**, if you need neither account info nor additional settings for Internet access.
- **Static IP:** Select **Static IP**, if you've been provided by your ISP with static IP info, like IP address, subnet mask, default gateway, etc. for Internet access.

DHCP Server

This page allows you to modify the DHCP server parameters. Click **Network Settings > DHCP Server** to enter page below:



To disable the DHCP server, click the icon directly; to delete the DHCP parameters you've created, click the icon ; if you have deleted the DHCP parameters, click **Add** to add the only one rule for its DHCP server; to edit the DHCP parameters, click the icon to enter page below:

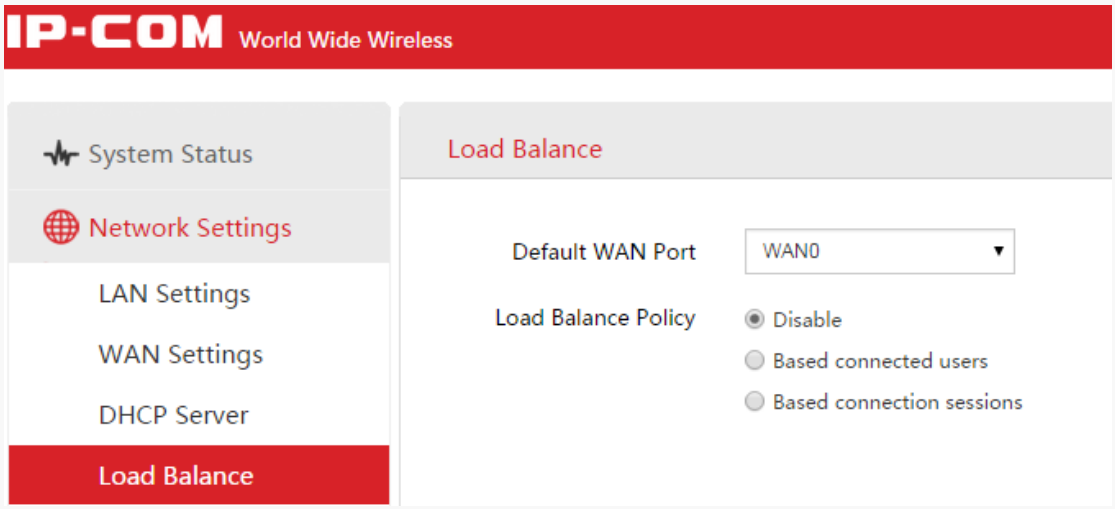


- **DHCP Server:** Check/Uncheck the Enable box to enable/disable the DHCP server on your device.
- **Start IP:** Enter the start IP address to make a range for the DHCP server to assign dynamic IPs.

- **End IP:** Enter the end IP address to make a range for the DHCP server to assign dynamic IPs.
- **Subnet Mask:** Enter the Subnet Mask. The default subnet mask is 255.255.255.0.
- **Gateway:** It is recommended to enter the IP address of the LAN port of the device.
- **Primary/Alternate DNS:** Enter the DNS server address provided by your ISP. If you are not clear, please consult your ISP.
- **Lease time:** It's the length of time for the IP address lease. After the IP address has expired, the client will be automatically assigned a new one.

Load Balance

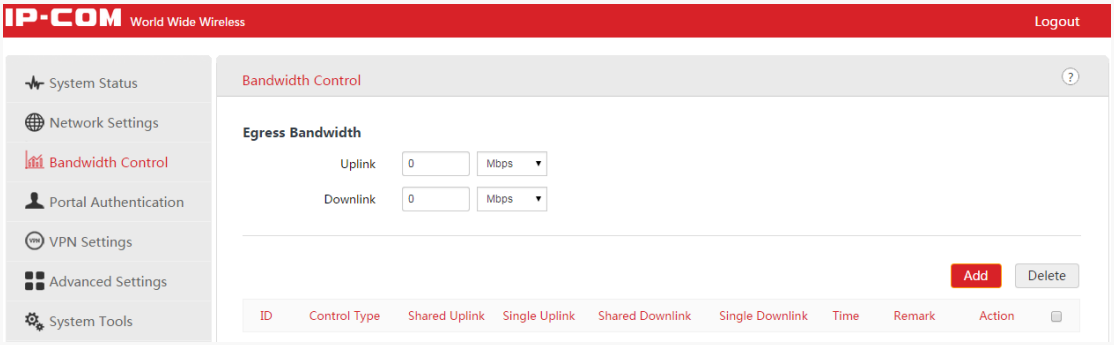
This page allows you to configure the sharing traffic statistics of the WAN ports to optimize resource utilization. When Load Balance is enabled, the device will use sessions or users automatically allocate connections to achieve load balance for corresponding WAN connections. Click **Network Settings > Load Balance** to enter page below:



- **Based connected users:** If 'Based connected users' is selected, the WAN bandwidth will automatically allocate connections based on users to achieve network load balance.
- **Based connection sessions:** If 'Based Connection Sessions' is selected, the WAN bandwidth will automatically allocate connections based on session numbers to achieve network load balance.

Bandwidth Control

This section will assist in prioritizing your network bandwidth usage, to assure a smooth streaming experience for surfing the Internet and online gaming. Click **Bandwidth Control** to enter page below:



◆ Total Egress Bandwidth Config

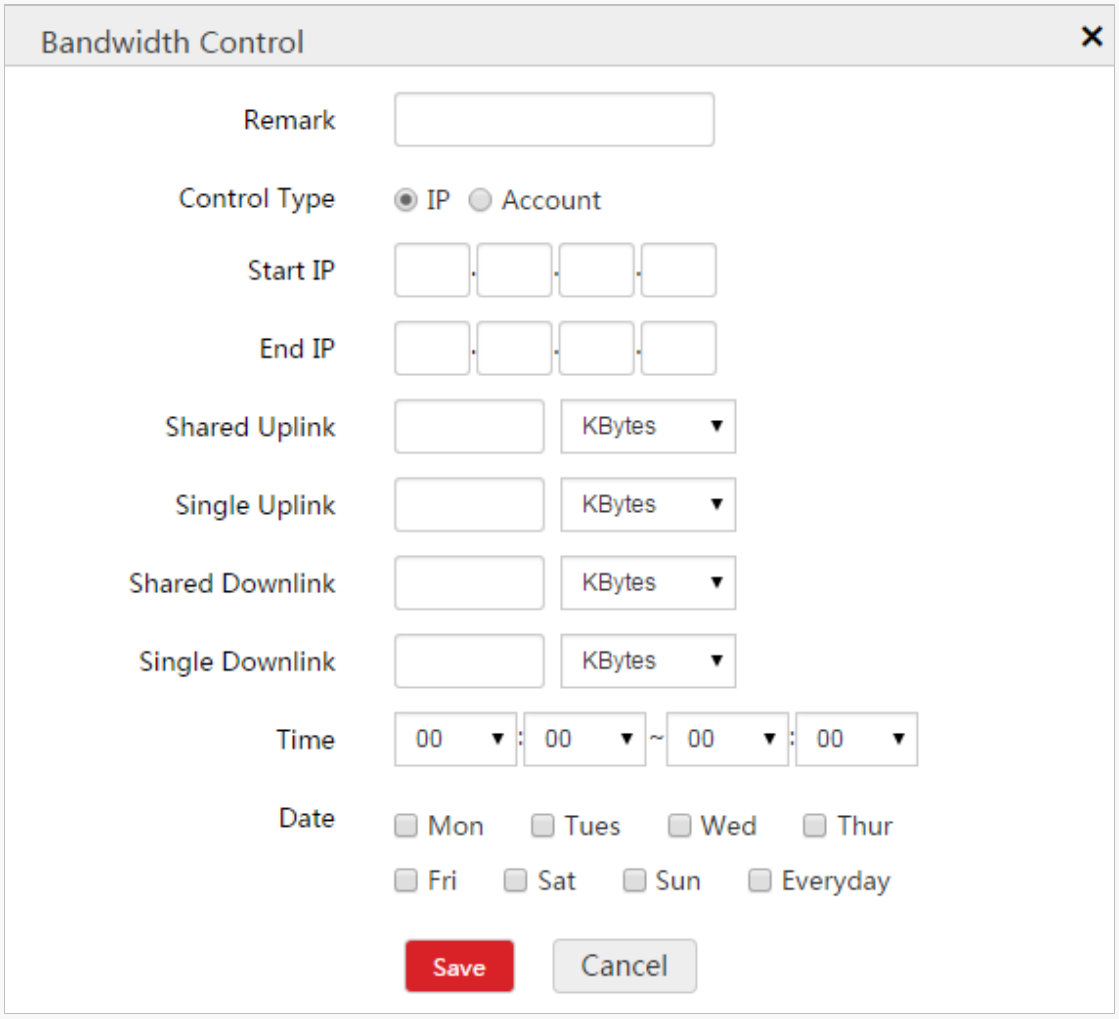
Total egress bandwidth is the bandwidth you have introduced. It is used as the basis of bandwidth division when there is no flow policy.

For instance, you've been provided with 12M ADSL broadband service. Set the total egress downlink to 12Mbps; and the total egress uplink to 1Mbps.

(**Tip**: 1Mbps=1024Kbps=128KByte/s)

◆ Bandwidth Control Config

For a better and reasonable network bandwidth experience, here you can configure the bandwidth to limit the speed of users with different IPs or accounts. Click **Add** to enter page below:



- **Remark:** Description of the group of IPs or accounts.
- **Control Type:** The device support bandwidth control based on IP range and accounts. When IP is selected, you need to specify the IP range (start IP and end IP). When Account is selected, you have to enable portal authentication.
- **Shared Uplink:** The total upload bandwidth shared by all selected accounts or IPs within the designated IP range.
- **Single Uplink:** The upload bandwidth that each account or each IP within the IP range can get to.
- **Shared Downlink:** The total download bandwidth shared by all selected accounts or IPs within the designated IP range.
- **Single Downlink:** The download bandwidth that each account or each IP within the IP range

can get to.

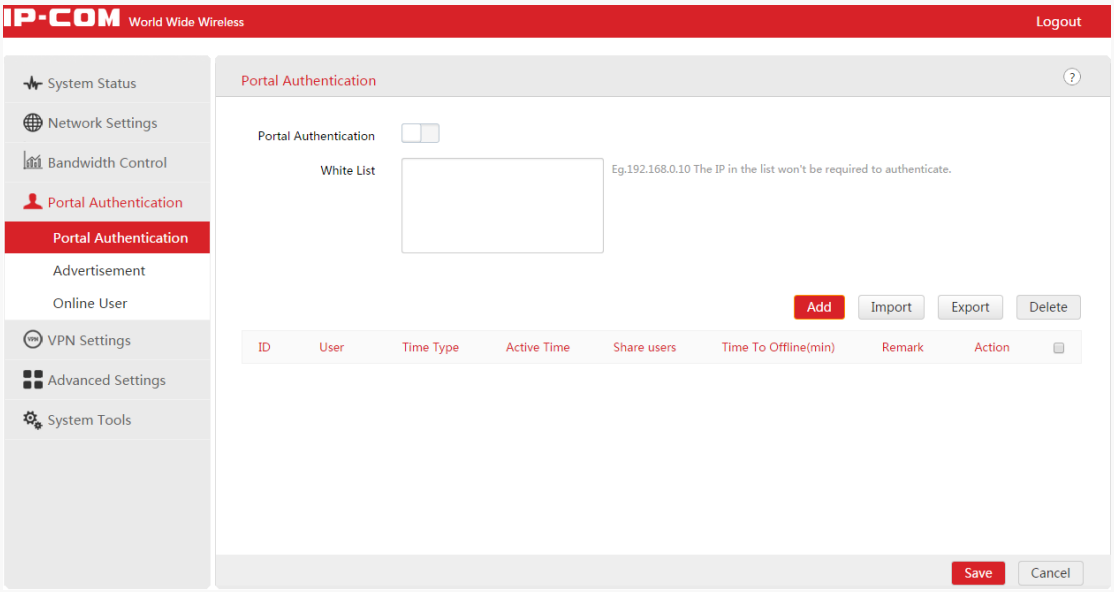
- **Time & Date:** Enter the effective time and date of the policy.

Portal Authentication

In this section, you can configure portal authentication settings for your device.

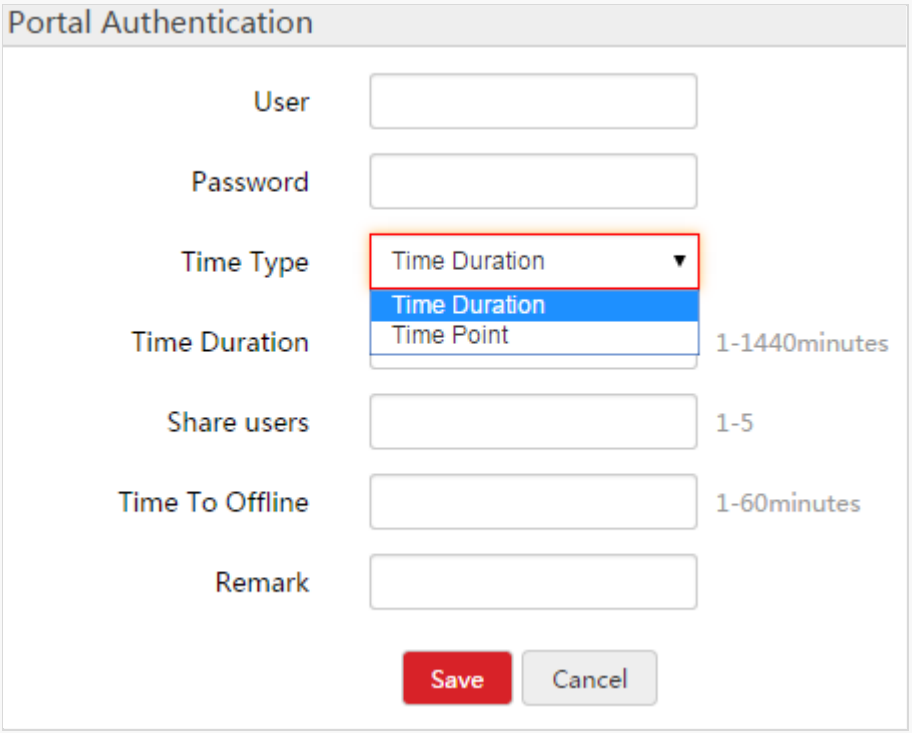
Portal Authentication

This page allows you to enable the portal authentication function and create the accounts for portal authentication. Once this function is enabled, when clients want to connect to the network via this device, clients have to be authenticated first.



- **Portal Authentication:** Enable or disable the portal authentication for the device.
- **White List:** Add IP addresses that won't be required to authenticate when portal authentication is enabled.
- **Add:** Click it to add accounts for portal authentication.
- **Export:** Click it to export the accounts information.
- **Import:** Click it to import the accounts information, it will re-write the accounts information.

To add an account for portal authentication, click **Add:**



❶ **User:** Create the login user account here.

❷ **Password:** Set the login password for the user account you've created.

❸ **Time Type:** Select the time type for your account. When you select Time Point, please enter a time point such as 2016-10-10 18:00 in the field below. When the account is authenticated, the account will expire at 2016-10-10 18:00. When you select Time Duration, please enter the time duration, such as 60 minutes, in the field below. When the account is authenticated, the account will expire after 60 minutes.

❹ **Share Users:** Specify the number of users to login with this account.

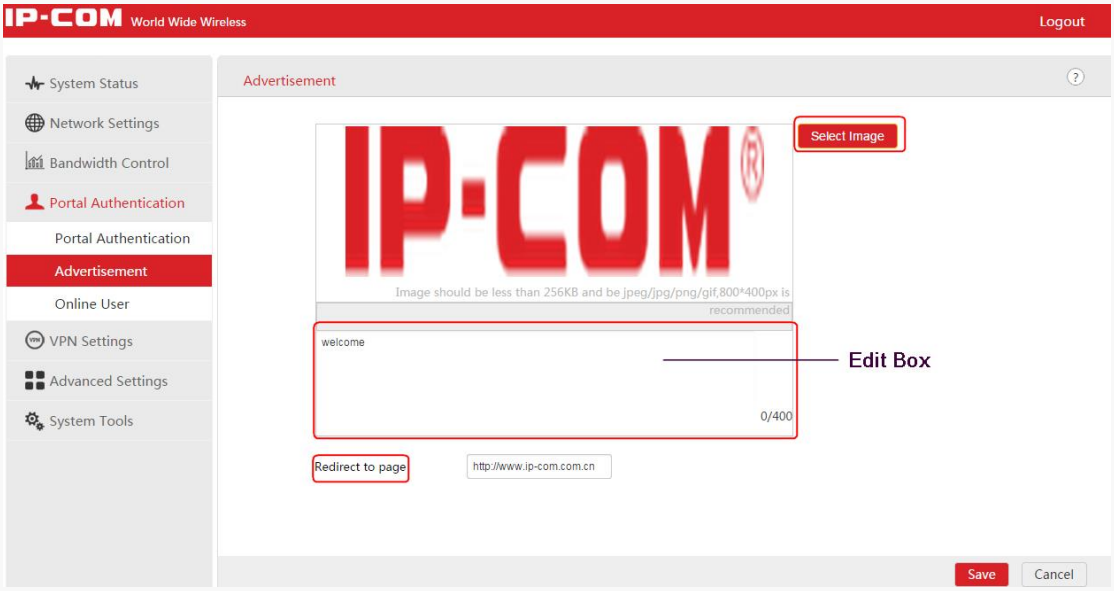
❺ **Time to Offline:** Enter the time duration, if no traffic statistics is generated during this time duration, the account will require to be authenticated again.

❻ Give some additional descriptions for the account (optional).

❼ Click **Save** to apply your settings.

Advertisement

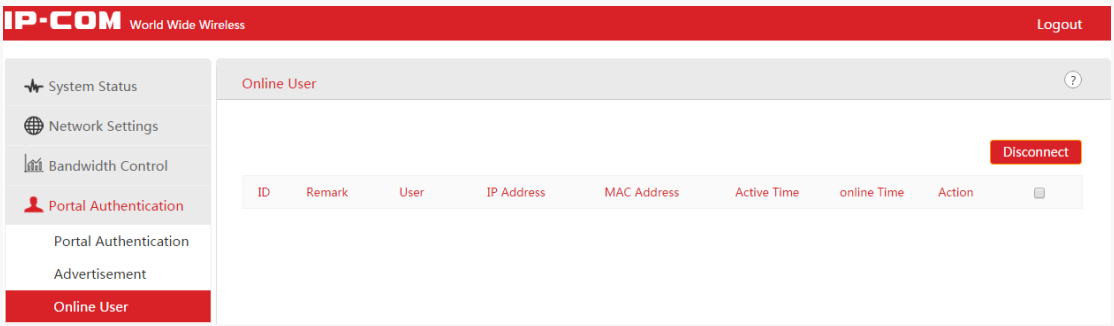
This page is used to customize the advertisement push page.



- **Select Image:** Select image to import to the device for the redirect page. The image should be less than 256KB and 800*400px jpeg/jpg/png/gif is recommended
- **Edit Box:** Here you can write the message that appears when users log in to the redirect page successfully. Up to 400 characters can be input here.
- **Redirect to page:** Enter the URL you want to redirect to when the User has been successfully authenticated.

Online User

This page allows you to view the account information when you enable portal authentication. Click **Disconnect** to disconnect the connected users. Then the user will be required to authenticate again.

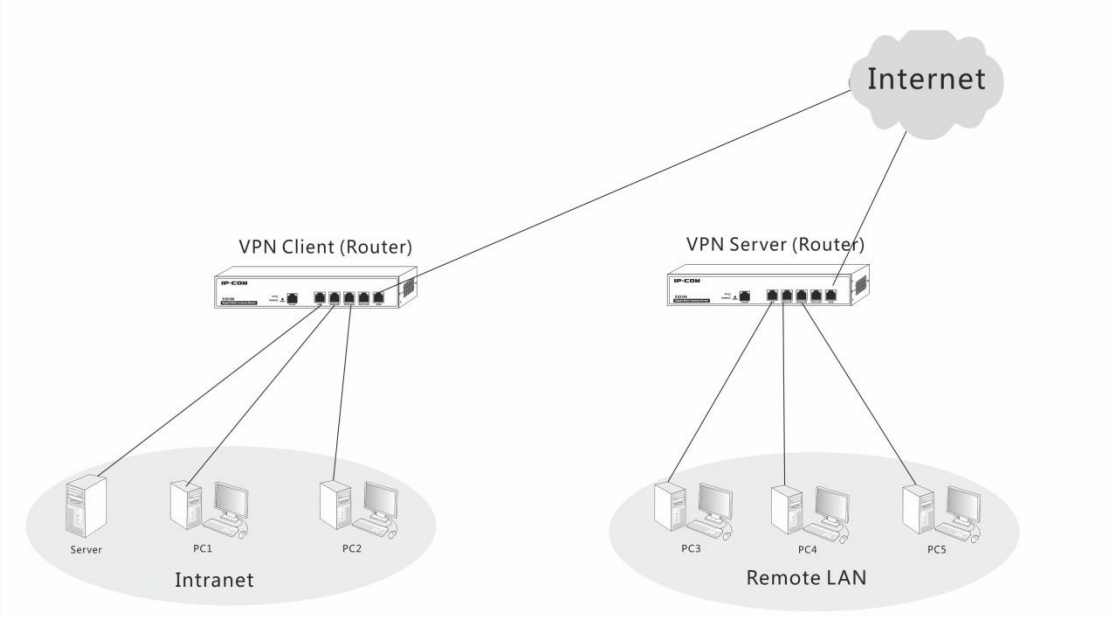


VPN Settings

VPN (Virtual Private Network) is a private network established via the public network, generally via the Internet. However, the private network is a logical network without any physical links, so it is called Virtual Private Network. VPN, a technology which will not expose the private data to all users on the Internet, allows employees to securely access their company's intranet while traveling outside the office.

VPN adopts the tunneling technology to establish a private connection between two endpoints. It is a connection secured by encrypting the data and using point-to-point authentication. Tunneling protocols, including L2TP, PPTP and IPsec, are supported on this router.

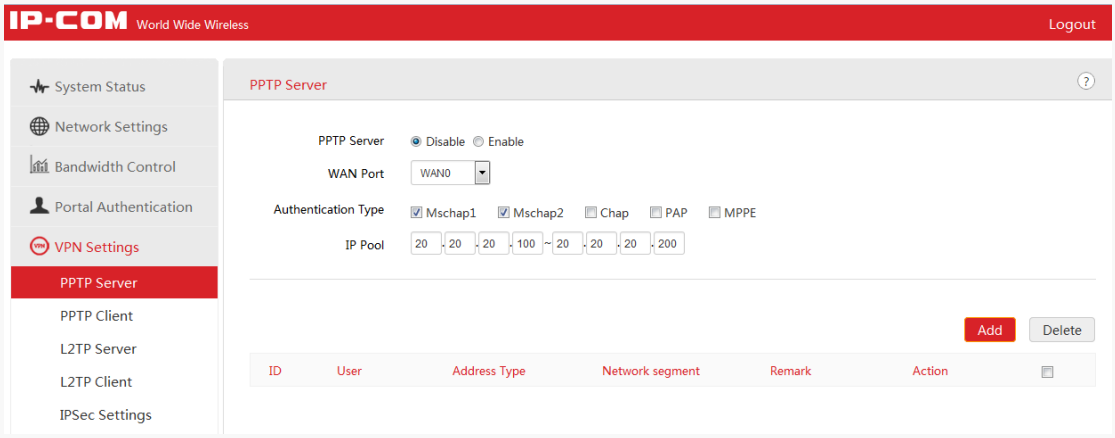
The following diagram is a typical VPN topology.



PPTP Server

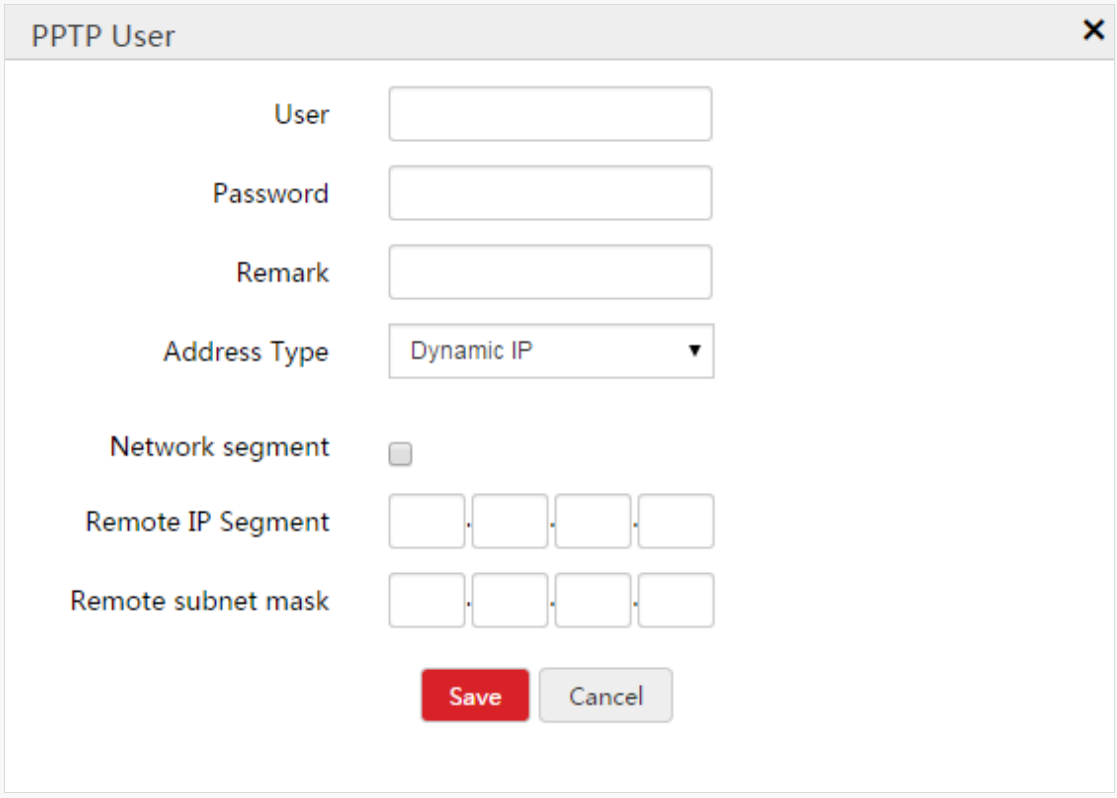
The Point-to-Point Tunneling Protocol (PPTP) is a layer 2 VPN tunneling protocol to encapsulate packets and add extra header to packets.

Click **VPN Settings > PPTP Server** to enter page below:



- **PPTP Server:** Check **Enable** to enable the PPTP server.
- **WAN Port:** Select the WAN port on which to enable the PPTP server. This port's IP address is the PPTP server address of the PPTP client.
- **Authentication Type:** Specify the encryption type for PPTP tunnel.
- **IP Pool:** Specify the IP Pool for PPTP clients.

To set a PPTP user, click **Add** to enter page below:

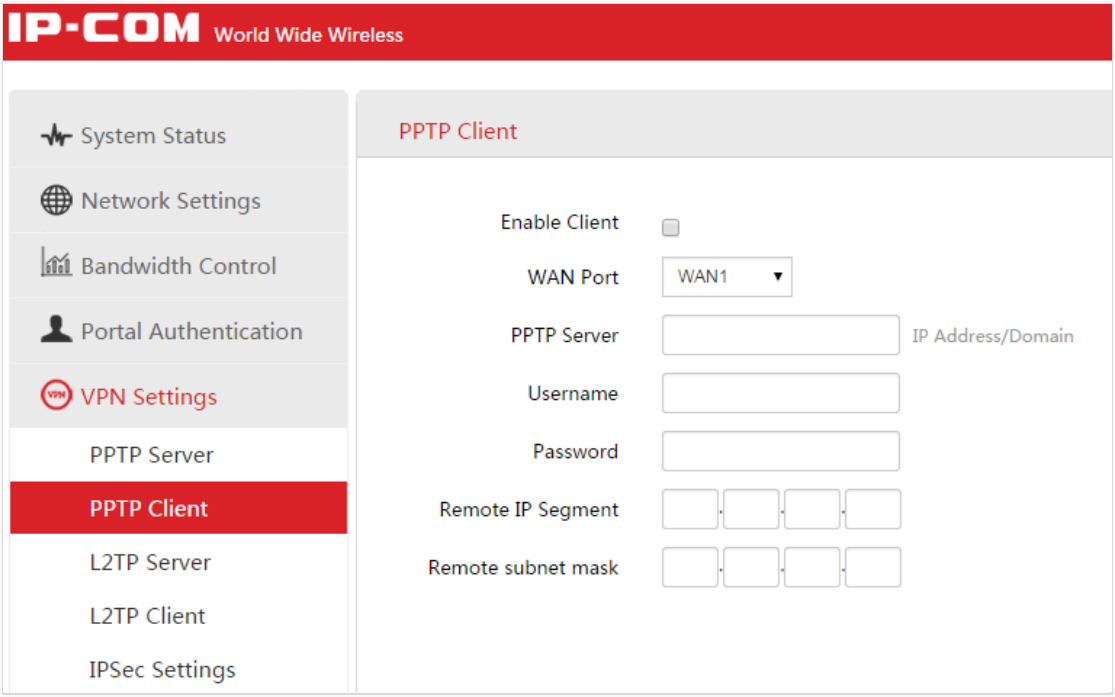


- **User:** Set the account name of PPTP tunnel.
- **Password:** Set the password of PPTP tunnel.
- **Remark:** Descriptions of the PPTP user (optional).

- **Address Type:** Do not change the default setting (Dynamic IP) unless necessary. When Dynamic IP is selected, the PPTP client will obtain an IP address automatically from the PPTP server. When Manual is selected, you need to specify an IP address manually for the PPTP client.
- **Network Segment:** If the PPTP client is a network, check this option. Otherwise, do not check it.
- **Remote IP Segment:** Set the internal IP segment for the PPTP client. When the PPTP client is a network, this is a required option.
- **Remote Subnet Mask:** Set the internal subnet mask for the PPTP client. When the PPTP client is a network, this is a required option.

PPTP Client

When there is a PPTP server in your network, you can connect your router to the PPTP server by configuring the PPTP client function. Click **VPN Settings > PPTP Client** to enter page below:



- **Enable Client:** Check it to enable the PPTP client function.
- **WAN Port:** Select the WAN port on which to enable the PPTP Client.
- **PPTP Server:** Configure the PPTP server's IP address, which is the WAN IP address of the remote router whose PPTP server function is enabled.

- **Username:** Enter the user name you've configured on the PPTP server.
- **Password:** Enter the password you've configured on the PPTP server.
- **Remote IP Segment:** Set the internal IP segment of the remote PPTP server.
- **Remote Subnet Mask:** Set the internal subnet mask of the remote PPTP server.

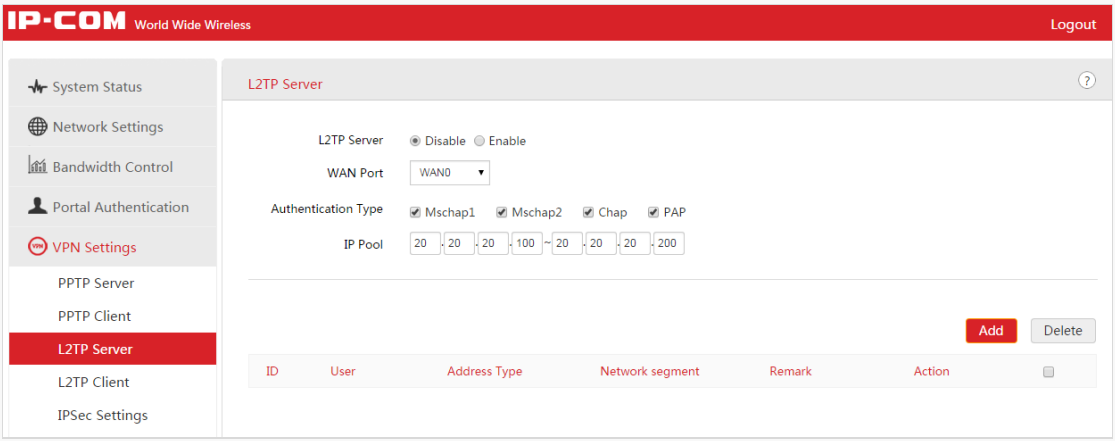
NOTE

MPPE is not supported for the PPTP Client function of this router. If this router works as the PPTP client, please disable MPPE on the PPTP server.

L2TP Server

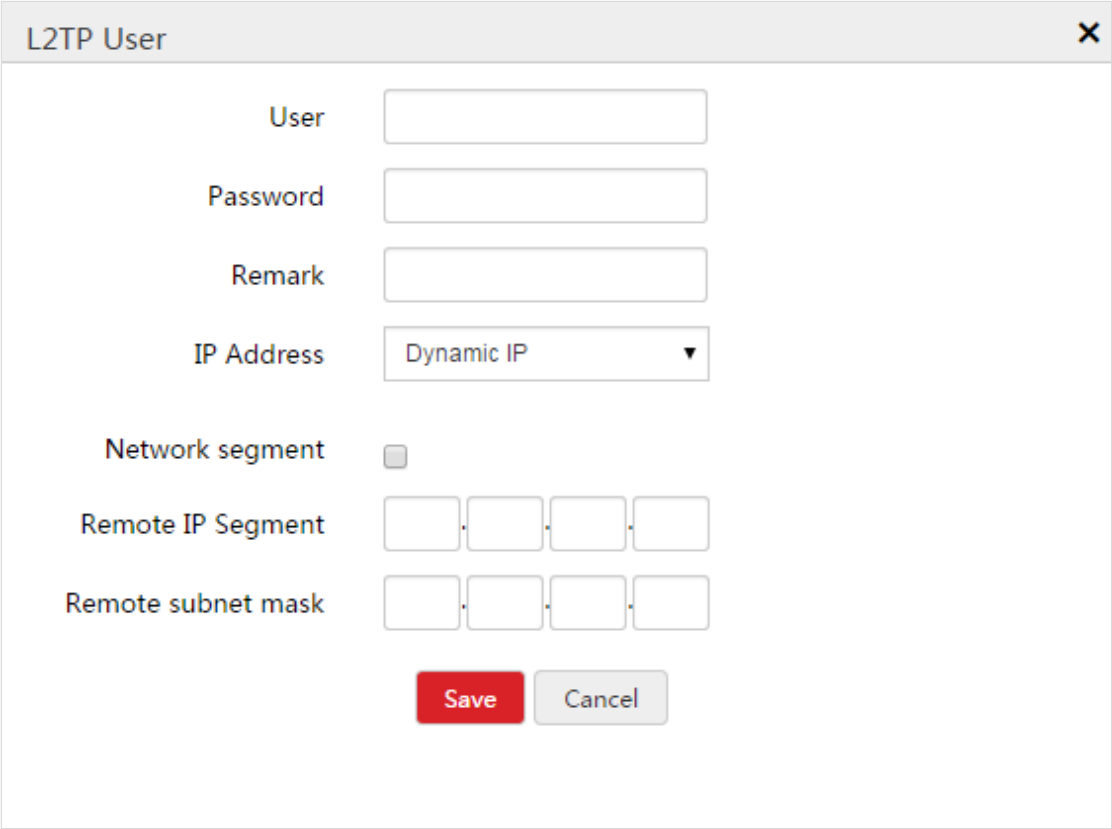
The Layer 2 Tunneling Protocol (L2TP) is a layer 2 VPN tunneling protocol to encapsulate packets and add extra header to packets by using PPP (Point to Point Protocol).

Click **VPN Settings > L2TP Server** to enter page below:



- **L2TP Server:** Check **Enable** to enable the L2TP server.
- **WAN Port:** Select the WAN port on which to enable the L2TP server. This port's IP address is the L2TP server address of the L2TP client.
- **Authentication Type:** Select the encryption type for the L2TP server.
- **IP Pool:** Set the IP pool for the L2TP server.

To set an L2TP user, click **Add** to enter page below:

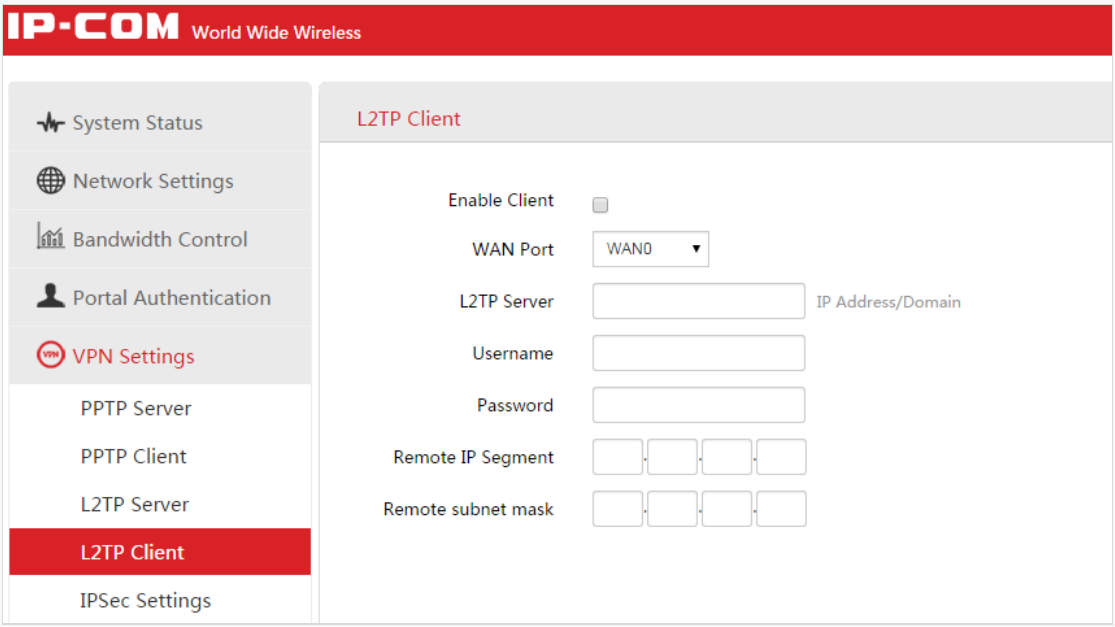


- **User:** Set the account name of L2TP tunnel.
- **Password:** Set the password of L2TP tunnel.
- **Remark:** Descriptions of the L2TP user (optional).
- **IP Address:** Do not change the default setting (Dynamic IP) unless necessary. When Dynamic IP is selected, the L2TP client will obtain an IP address automatically from the L2TP server. When Manual is selected, you need to specify an IP address manually for the L2TP client.
- **Network Segment:** If the L2TP client is a network, check this option. Otherwise, do not check it.
- **Remote IP Segment:** Set the internal IP segment for the L2TP client. When the L2TP client is a network, this is a required option.
- **Remote Subnet Mask:** Set the internal subnet mask for the L2TP client. When the L2TP client is a network, this is a required option.

L2TP Client

When there is a L2TP server in your network, you can connect your router to the L2TP server by

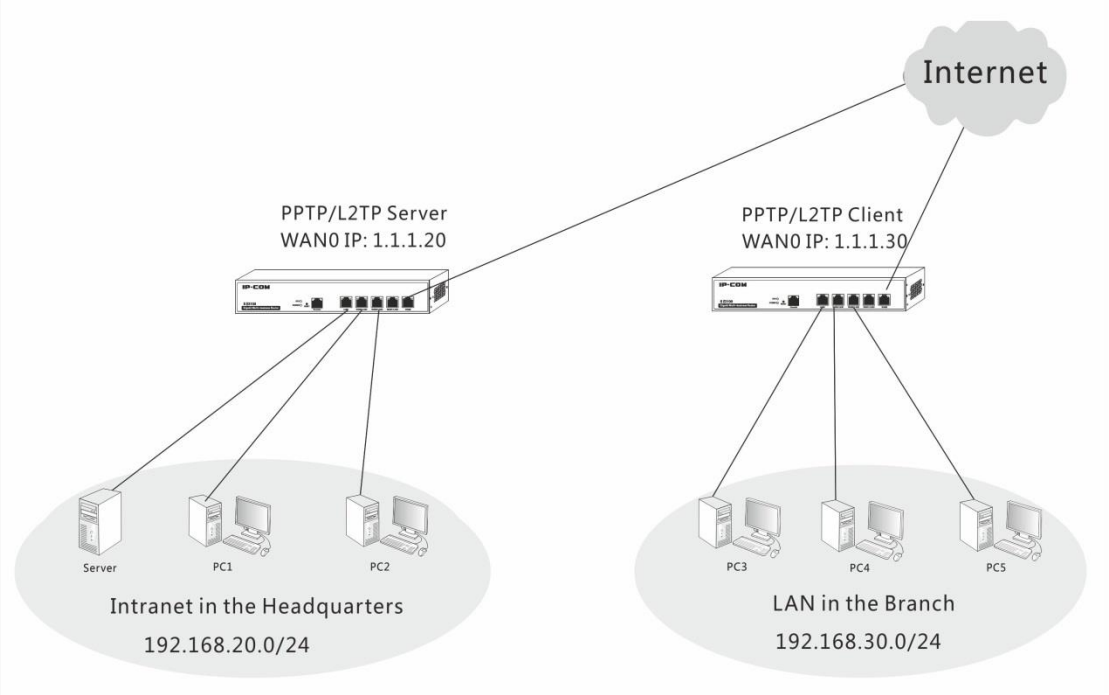
configuring the L2TP client function. Click **VPN Settings > L2TP Client** to enter page below:



- **Enable Client:** Check it to enable the L2TP client function.
- **WAN Port:** Select the WAN port on which to enable the L2TP Client.
- **L2TP Server:** Configure the L2TP server's IP address, which is the WAN IP address of the remote router whose L2TP server function is enabled.
- **Username:** Enter the user name you've configured on the L2TP server.
- **Password:** Enter the password you've configured on the L2TP server.
- **Remote IP Segment:** Set the internal IP segment of the remote L2TP server.
- **Remote Subnet Mask:** Set the internal subnet mask of the remote L2TP server.

Application Example of PPTP/L2TP

There is a company based in Place A, but has a branch office in Place B. Staffs both in the headquarters and its branch need to share their internal resources securely. Assume that the VPN routers in Place A and Place B are SE3100 and verify that the two SE3100 can access the Internet successfully.



Configurations on the SE3100 in the headquarters

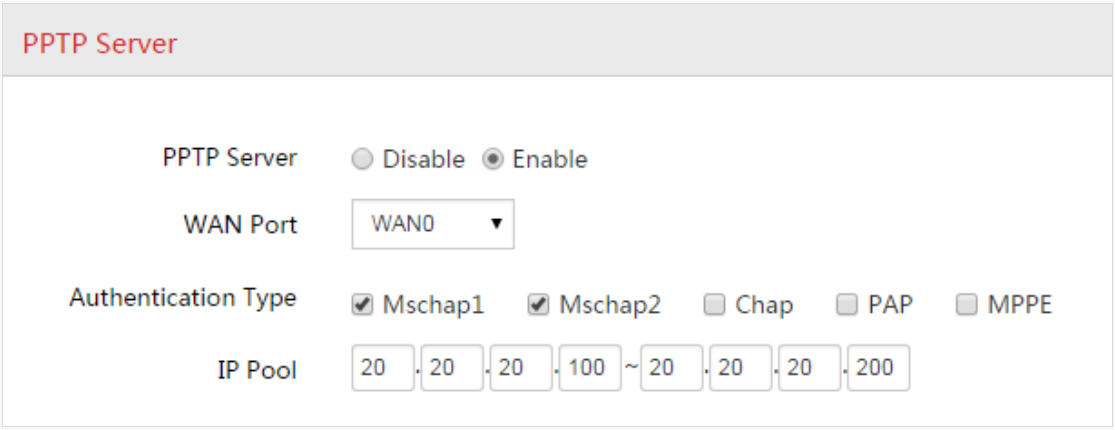
As configurations of L2TP and PPTP are similar, next we will take PPTP as an example.

Step 1: Click **VPN Settings > PPTP Server** to configure basic parameters:

1. Enable the PPTP server function.
2. Select **WAN0** as the port for PPTP server.
3. Select authentication type for the PPTP server.
4. Configure PPTP IP pool.
5. Click **Save** to save your settings.

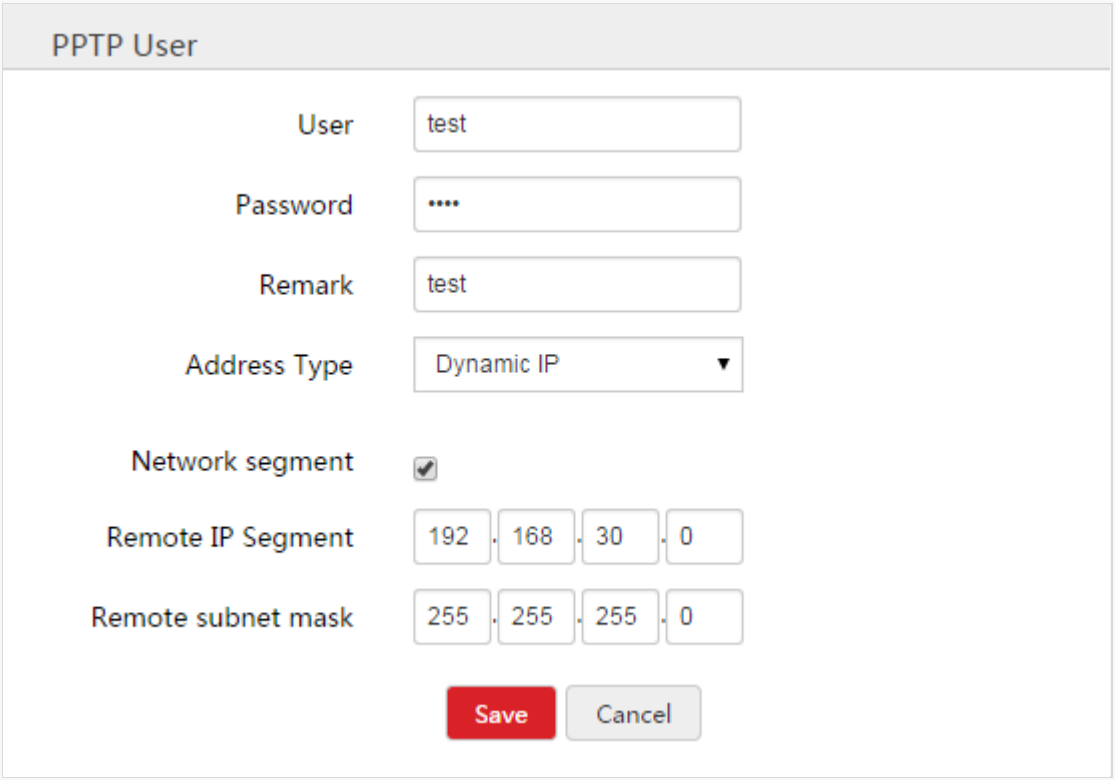
NOTE

1. In this example, SE3100, as the PPTP client, does not support MPPE. Thus, do not check the MPPE option. If a windows operation system is used as the PPTP client, you can check MPPE.
2. As L2TP does not support MPPE, you don't have to take MPPE into consideration.



Step 2: Click **Add** to add a PPTP user:

1. Set the PPTP user name, say test.
2. Set the PPTP password, say test.
3. Give a remark for the PPTP user.
4. Select the address type (Recommended: Dynamic IP).
5. Check **Network Segment**.
6. Set the Internal IP segment of the PPTP client, say 192.168.30.0.
7. Set the subnet mask of PPTP client, say 255.255.255.0.
8. Click **Save** to apply your changes.



◆ **Configurations on the SE3100 in the branch**

❶ On the web UI of SE3100 in the branch, click **VPN Settings > PPTP Client** to configure PPTP client settings.

❷ Check **Enable Client**.

❸ Select **WAN0** as the port for PPTP client.

❹ Enter the WAN IP address of the PPTP server, say 1.1.1.20.

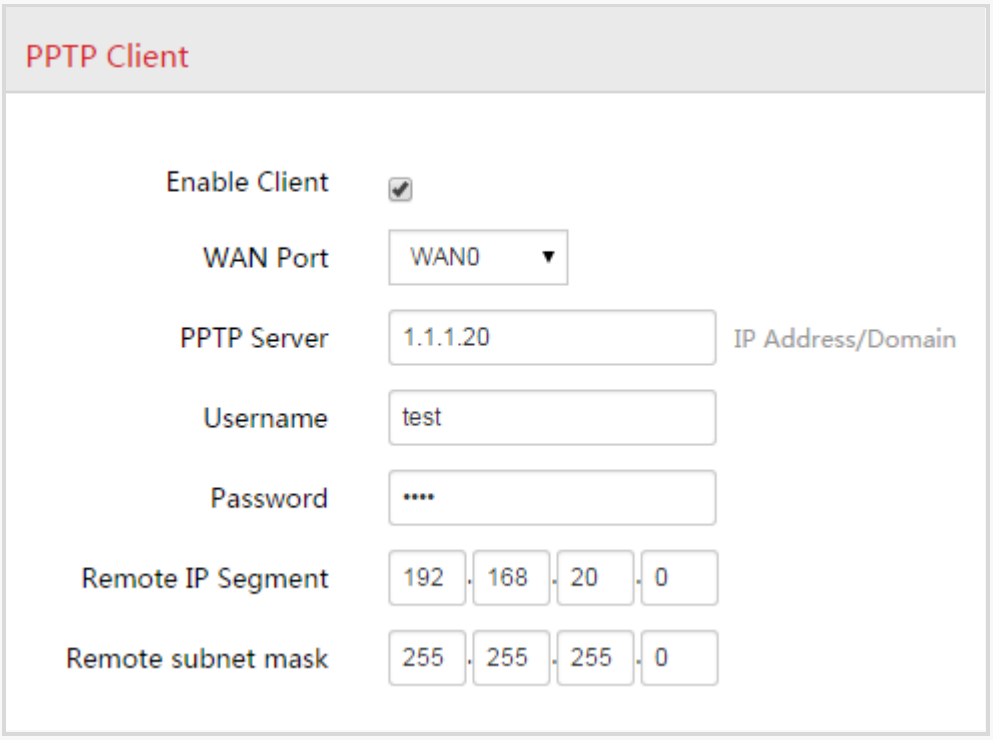
❺ Enter the PPTP user name, say test.

❻ Enter the PPTP password, say test.

❼ Enter the IP segment of the remote PPTP server, say 192.168.20.0.

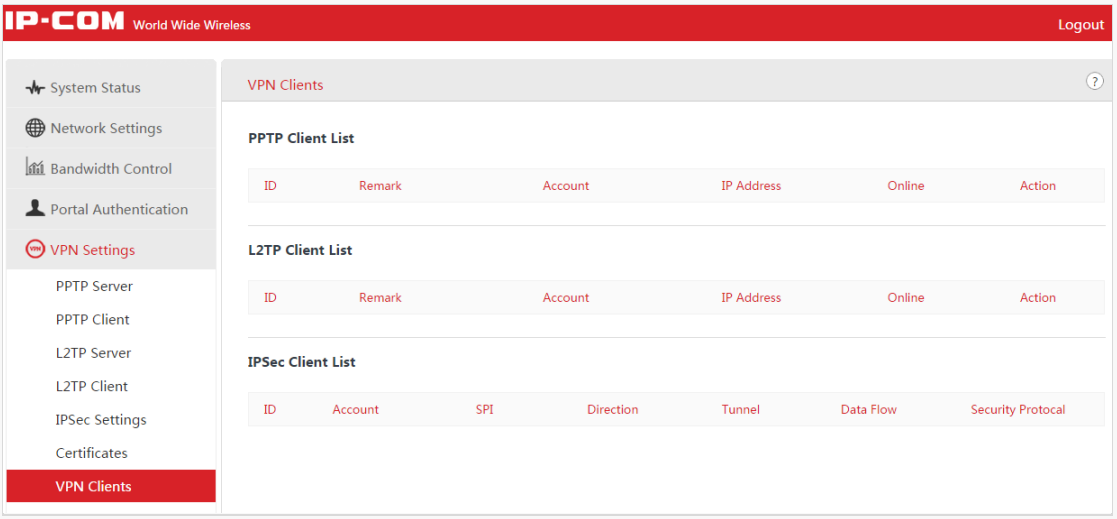
❽ Enter the subnet mask of the remote PPTP server, say 255.255.255.0.

❾ Click **Save** to apply your changes.



◆ Verification

Method 1: On the web UI of SE3100 in the headquarters, click **VPN Settings > VPN Clients** to view the PPTP Client List. If the PPTP client negotiates with the PPTP server successfully, PPTP client info will be displayed here.



Method 2: When staffs in the headquarters and the branch can PING each other's internal IPs successfully, or when they can visit each other's internal resources successfully, like FTP server, file server, etc., PPTP negotiation has been achieved successfully.

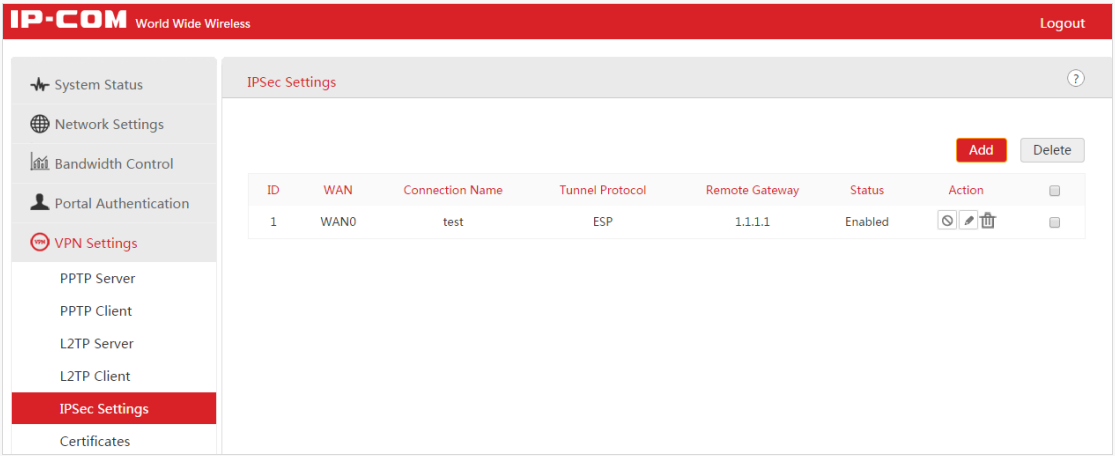
IPSec Settings

IPsec (IP Security) is a set of services and protocols defined by IETF (Internet Engineering Task Force) to provide high security for IP packets and prevent attacks.

To ensure a secured communication, the two IPsec peers use IPsec protocol to negotiate the data encryption algorithm and the security protocols for checking the integrity of the transmission data, and exchange the key to data de-encryption.

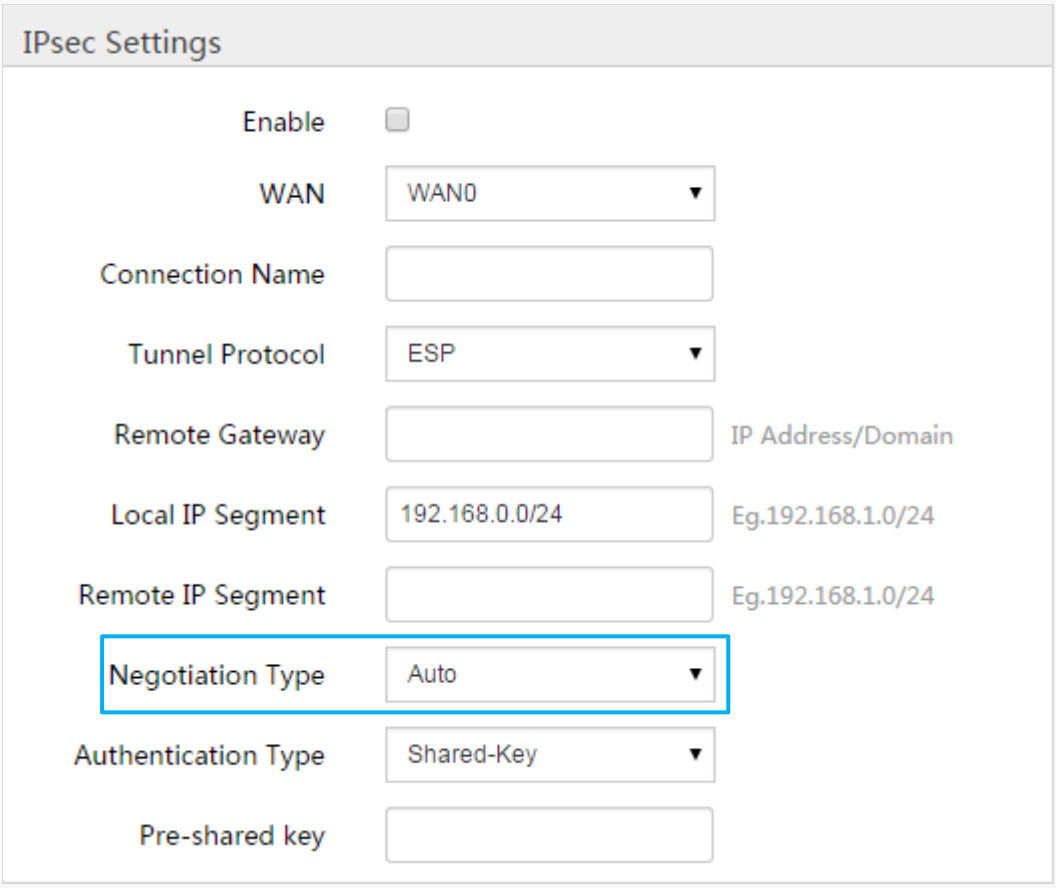
IPsec has two important security protocols: AH (Authentication Header) and ESP (Encapsulating Security Payload). AH is used to guarantee the data integrity. If the packet has been tampered during transmission, the receiver will drop this packet when validating the data integrity. ESP is used to check the data integrity and encrypt the packets. Even if the encrypted packet is intercepted, the third party still cannot get the actual information.

Click **VPN Settings > IPSec Settings** to enter page below and click **Add** to configure IPsec settings:



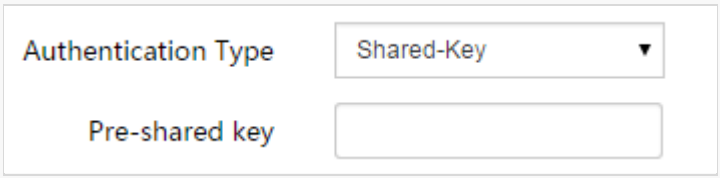
Two negotiation types are available here for IPsec settings: Auto and Manual. When Auto is selected, the SPI value is obtained via auto-negotiation. When Manual is selected, you need to specify a value manually.

Negotiation Type --- Auto

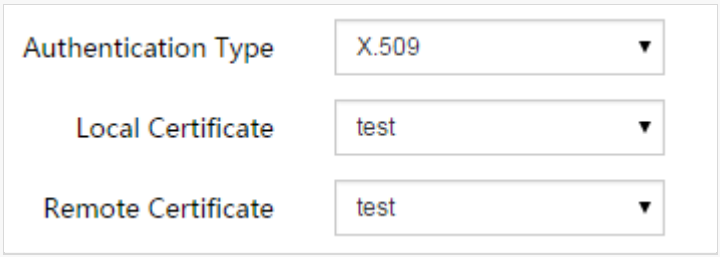


- **Enable:** check it to enable the IPsec function.
- **WAN:** Specify the local WAN port for this Policy. The "Remote Gateway" of the remote router should be set to the IP address of this WAN port.
- **Connection Name:** Set a name for IPsec connection for identification.
- **Tunnel Protocol:** Select the corresponding tunnel protocol: ESP, AH or ESP+AP.
- **Remote Gateway:** IP address or domain name of the remote router.
- **Local IP Segment:** Internal IP segment of the local router.
- **Remote IP Segment:** Internal IP segment of the remote router.
- **Negotiation Type:** Select Auto. If Manual is selected, see Negotiation Type --- Manual.
- **Authentication Type:** Select the authentication type: Shared Key or X.509.

  When Shared-Key is selected, please set a key for mutual authentication. Pre-shared keys of the local router and the remote router must be the same.

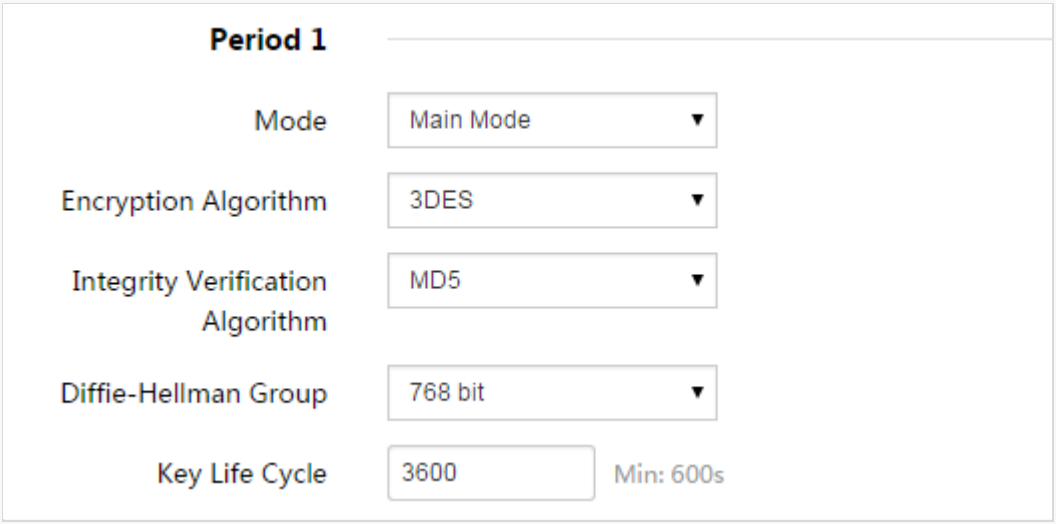


When X.509 is selected, please ensure that certificates of the local router and the remote router are the same. For settings of the certificate, see Certificates.



When the Negotiation Type is Auto, the entire negotiation process will be divided into 2 periods: In Period 1, the two sides will negotiate to exchange security proposals, like integrity verification algorithm and encryption algorithm, and establish an ISAKMP (Internet Security Association and Key Management Protocol) SA (Security Association) so that more info in Period 2 can be exchanged securely. In Period 2, it will establish IPsec SA by using ISAKMP SA created in Period 1 to protect communication data between two sides.

Period 1:



- **Mode:** Set the exchange mode for the negotiation in Period 1. The exchange mode must be identical with its remote one. Two modes are available here. In Main mode, the two sides exchange packets a lot. As this mode provides identification protection, it is suitable for higher identification protection. In Aggressive mode (also called Active mode), the two sides exchange just a few packets and negotiate quickly. It does not provide identification protection.
- **Encryption Algorithm:** Select the encryption algorithm for IPsec session. The following encryption algorithms are supported on this router.

  DES: DES (Data Encryption Standard) encrypts a 64-bit (the last 8-bit of 64-bit is used for parity check) block of plain text with a 56-bit key.

  3DES: Triple DES, encrypts a plain text with 168-bit key.

  AES-128: Use the AES (Advanced Encryption Standard) algorithm and 128-bit key for encryption.

  AES-192: Use the AES (Advanced Encryption Standard) algorithm and 192-bit key for encryption.

  AES-256: Use the AES (Advanced Encryption Standard) algorithm and 256-bit key for encryption.

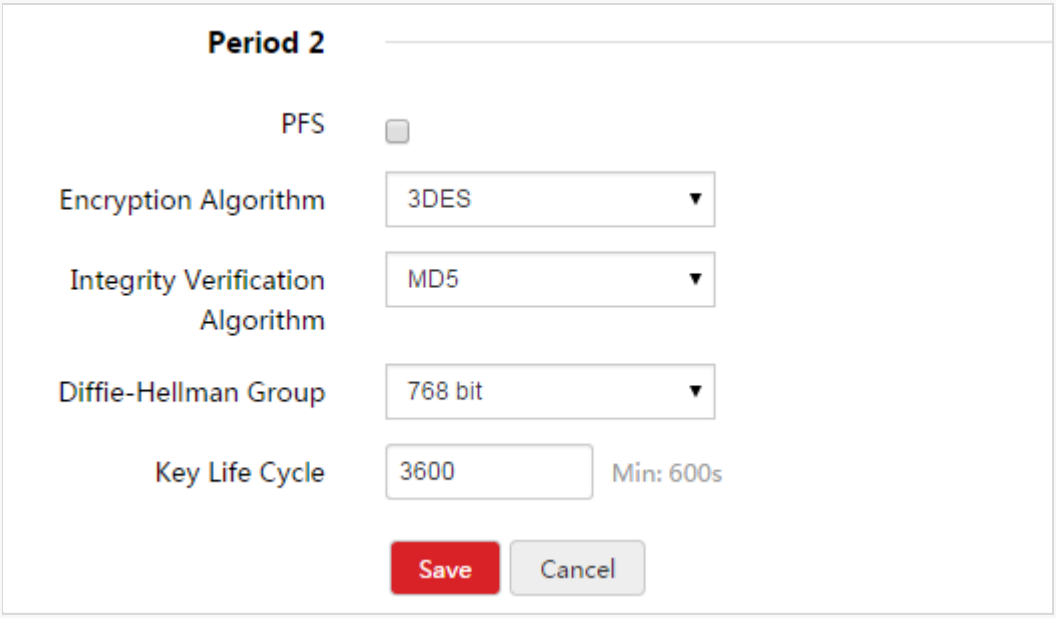
- **Integrity Verification Algorithm:** Select the verification algorithm for IPsec session. The following verification algorithms are supported on this router.

  MD5: MD5 (Message Digest Algorithm) generates a 128-bit message digest and prevents the message from being tampered.

  SHA1: SHA1 (Secure Hash Algorithm) generates a 160-bit message digest and it is more difficult to be cracked than MD5.

- **Diffie-Hellman Group:** Select the DH (Diffie-Hellman) group to be used in generating session key of IPsec tunnel.
- **Key Life Cycle:** Set the living time of IPsec SA.

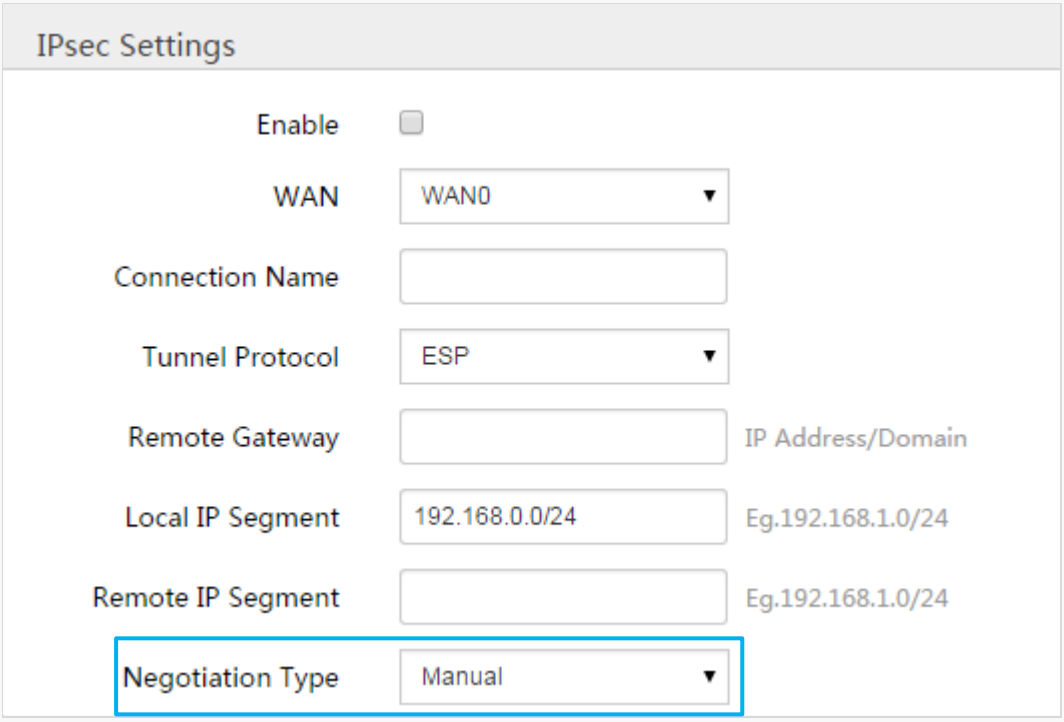
Period 2



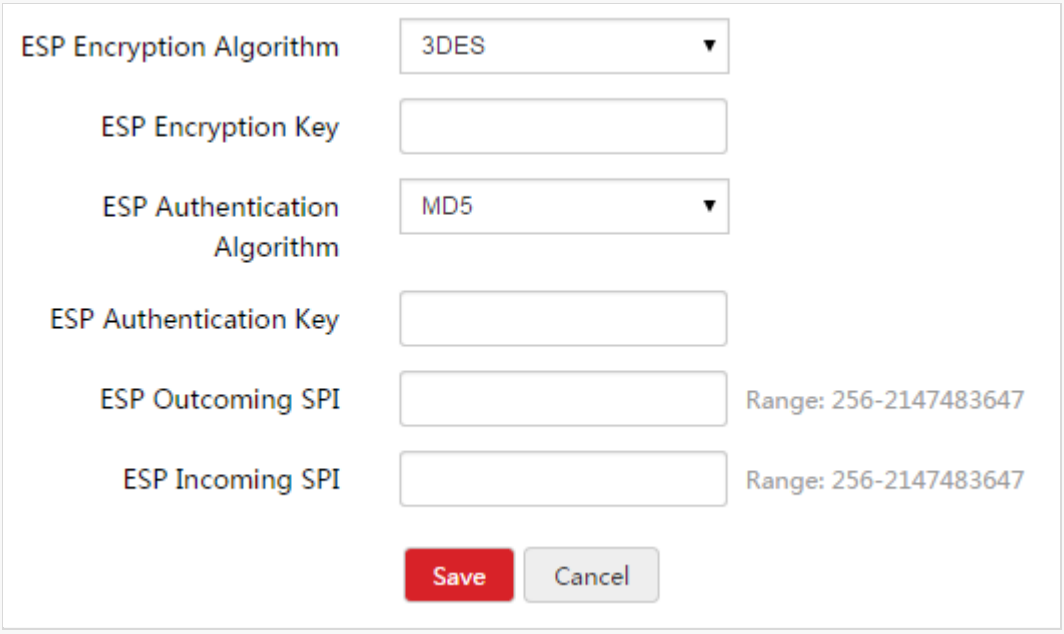
- **PFS:** Select the PFS (Perfect Forward Security) to enhance security. PFS configurations on both sides should be identical. With PFS function, IPsec Server and Client negotiate to create a new key in Period 2. As it is independent of the key created in Period 1, this key can be secure even when the key in Period 1 is de-encrypted. Without PFS, the key in Period 2 is created based on the key in Period 1 and thus once the key in Period 1 is de-encrypted, the key in Period 2 is easy to be de-encrypted, in this case, the communication security is threatened.

As for descriptions of other parameters, see Period 1.

Negotiation Type --- Manual



As for descriptions of parameters on the page above, see Negotiation Type --- Auto.



- **ESP Encryption Algorithm:** Select ESP encryption algorithm for ESP security protocol. The following encryption algorithms are supported on this router.

  DES: DES (Data Encryption Standard) encrypts a 64-bit (the last 8-bit of 64-bit is used for parity check) block of plain text with a 56-bit key.

  3DES: Triple DES, encrypts a plain text with 168-bit key.

AES-128: Use the AES (Advanced Encryption Standard) algorithm and 128-bit key for encryption.

AES-192: Use the AES (Advanced Encryption Standard) algorithm and 192-bit key for encryption.

AES-256: Use the AES (Advanced Encryption Standard) algorithm and 256-bit key for encryption.

- **ESP Encryption Key:** Set the ESP encryption key. Keys on both sides should be identical.
- **ESP/AH Authentication Algorithm:** When ESP is selected, set ESP authentication algorithm. When AH is selected, set AH authentication algorithm. The following authentication algorithms are supported on this router.

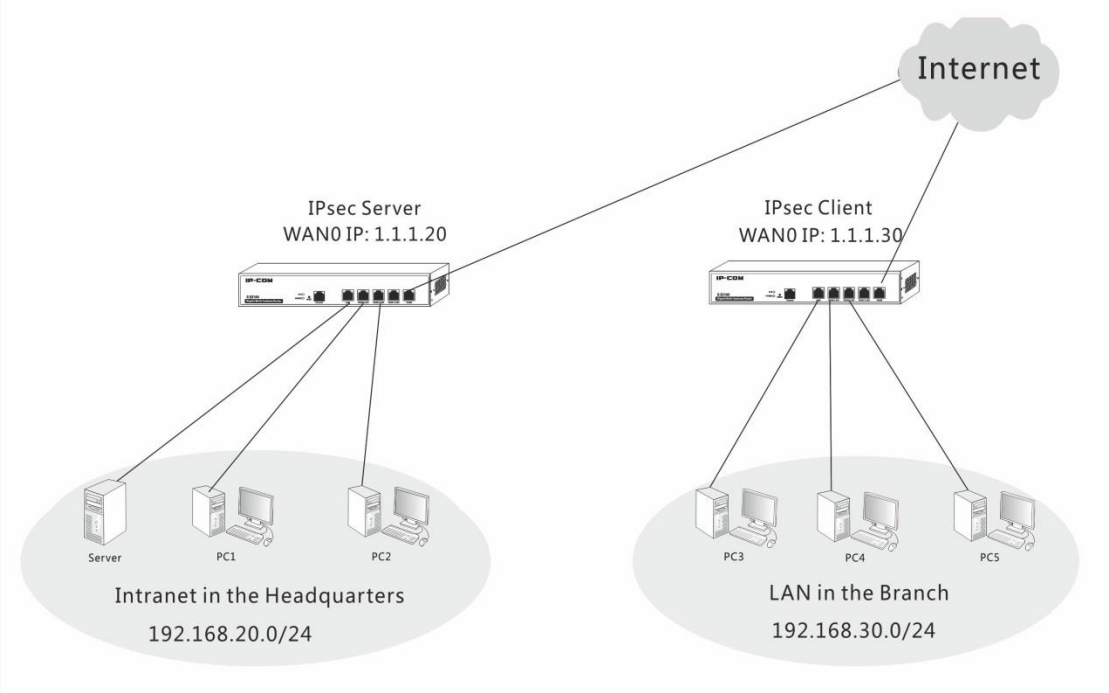
  MD5: MD5 (Message Digest Algorithm) generates a 128-bit message digest and prevents the message from being tampered.

  SHA1: SHA1 (Secure Hash Algorithm) generates a 160-bit message digest and it is more difficult to be cracked than MD5.

- **ESP/AH Authentication Key:** Set the ESP/AH authentication key. Keys on both sides should be identical.
- **ESP/AH Outcoming SPI:** Specify the Outcoming SPI (Security Parameter Index) manually. SPI, remote gateway and tunnel protocol identify an IPsec alliance. The Outgoing SPI here must match the Incoming SPI value at the other end of the tunnel.
- **ESP/AH Incoming SPI:** Specify the Incoming SPI (Security Parameter Index) manually. SPI, remote gateway and tunnel protocol identify an IPsec alliance. The Incoming SPI here must match the Outgoing SPI value at the other end of the tunnel.

Application Example of IPsec

There is a company based in Place A, but has a branch office in Place B. Staff both in the headquarters and its branch need to share their internal resources securely. Assume that the VPN routers in Place A and Place B are SE3100 and verify that the two SE3100 can access the Internet successfully.



Configurations on the SE3100 in the headquarters

1. Click **VPN Settings > IPsec Settings** and click **Add** to configure IPsec parameters (Assume that the negotiation type is Auto and the authentication type is Shared-Key).

2. Check **Enable** and select **WAN0** as the WAN port on which to enable the IPsec server.

3. Set a connection name, say Server.

4. Specify the remote gateway, say 1.1.1.30.

5. Specify the remote IP segment, say 192.168.30.0/24. And the Local IP Segment will be displayed as 192.168.20.0/24 automatically.

6. Set a pre-shared key, say 12345678.

7. Check **PFS**.

8. Verify that other parameters on both the IPsec server and IPsec client are identical.

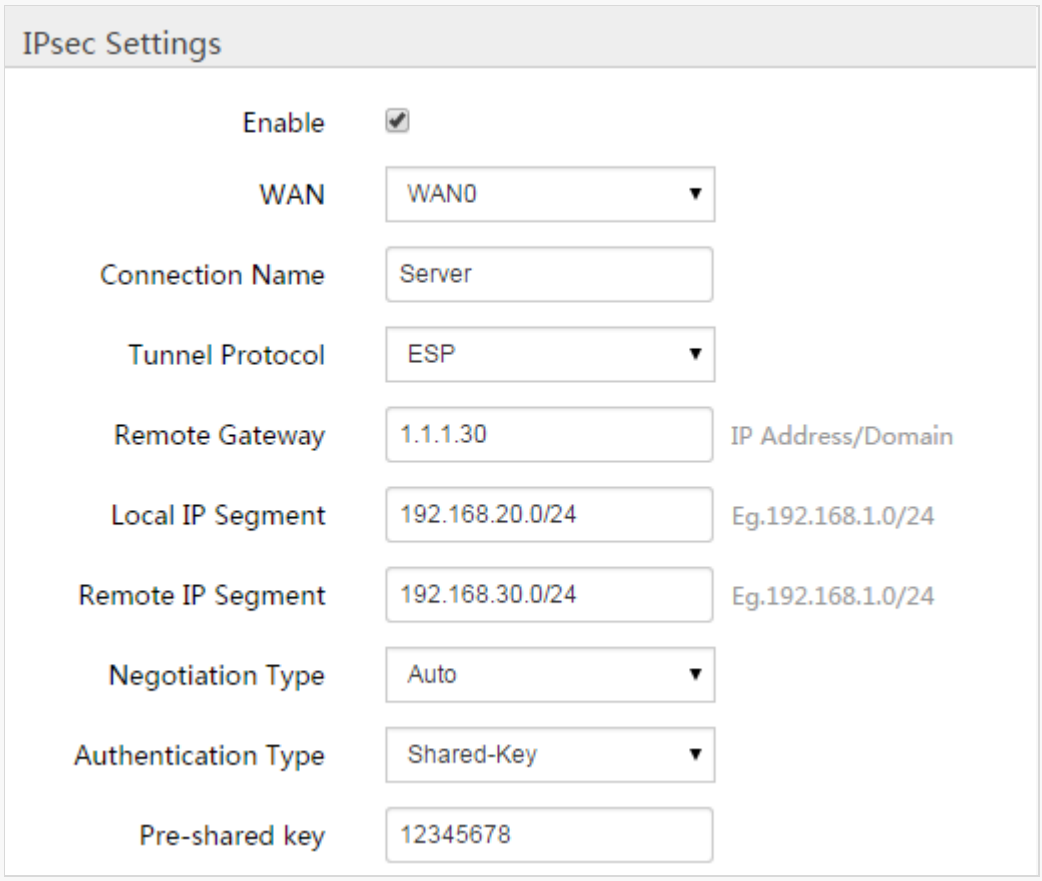
9. Click **Save** to apply your changes.

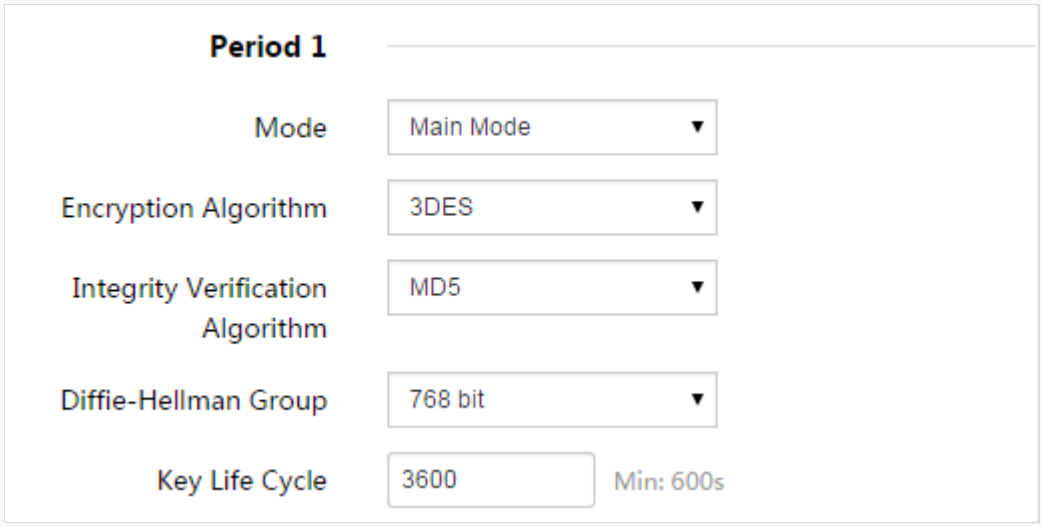
TIP

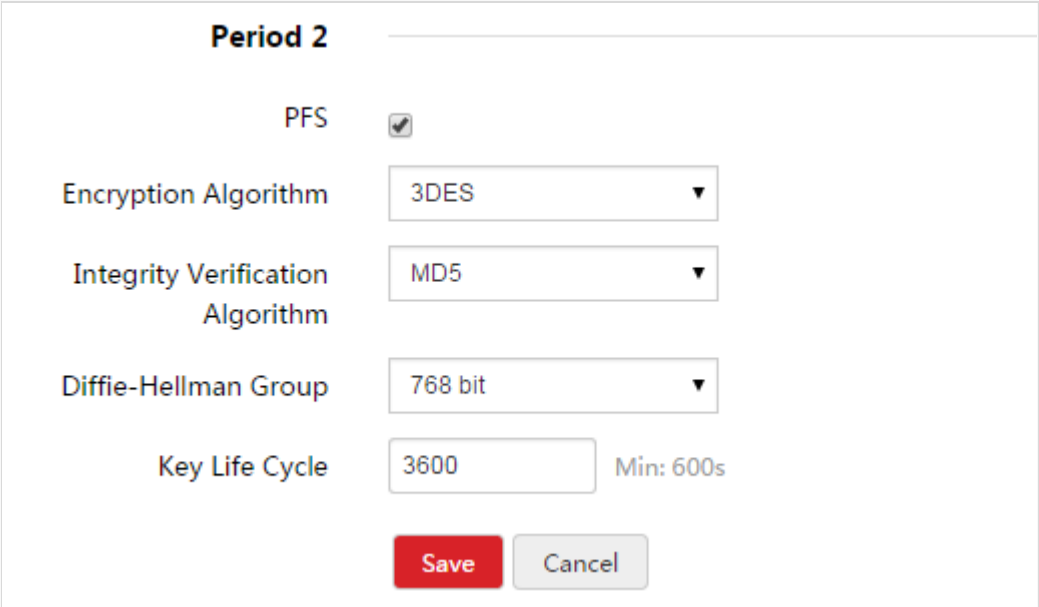
1. **When the negotiation type is Auto, and the authentication type is X.509,** set corresponding Local Certificate and Remote Certificate, and keep other parameters the same as

shown above. For settings of certificates, see Certificates.

2. **When the negotiation type is Manual,** please verify that encryption key and authentication keys on both the IPsec server and IPsec client are identical, and outcoming SPIs and incoming SPIs are opposite.





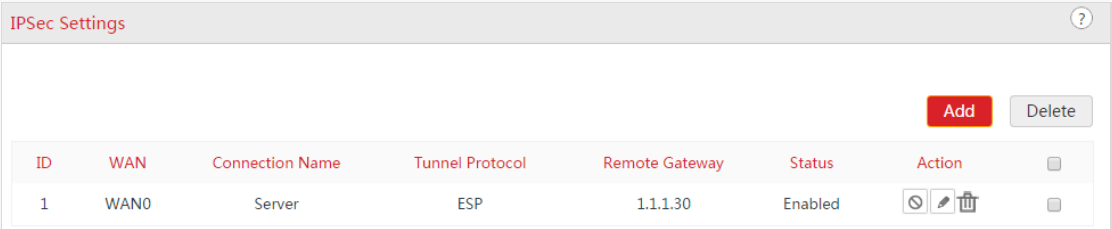


When configurations are completed, the following actions are allowed:

- Click the button to disable IPsec settings, and click the button to enable IPsec settings.
- Click the button to edit IPsec settings.
- Click the button to delete IPsec settings.

NOTE

When IPsec negotiation completes, you cannot directly edit IPsec settings. If necessary, click the button to disable IPsec settings first, and then edit it.



◆ Configurations on the SE3100 in the branch

❶ Click **VPN Settings > IPsec Settings** and click **Add** to configure IPsec parameters (Assume that the negotiation type is Auto and the authentication type is Shared-Key).

❷ Check **Enable** and select **WAN0** as the WAN port on which to enable the IPsec server.

❸ Set a connection name, say Client.

❹ Specify the remote gateway, say 1.1.1.20.

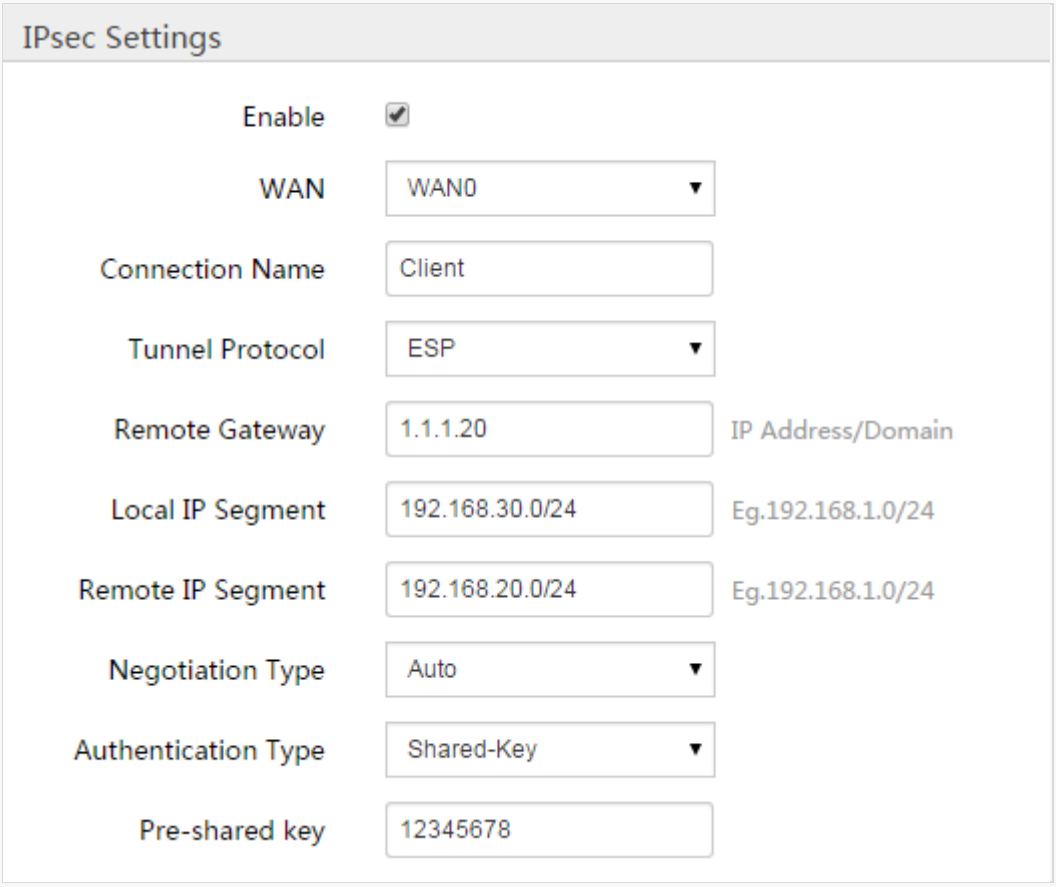
❺ Specify the remote IP segment, say 192.168.20.0/24. And the Local IP Segment will be displayed as 192.168.30.0/24 automatically.

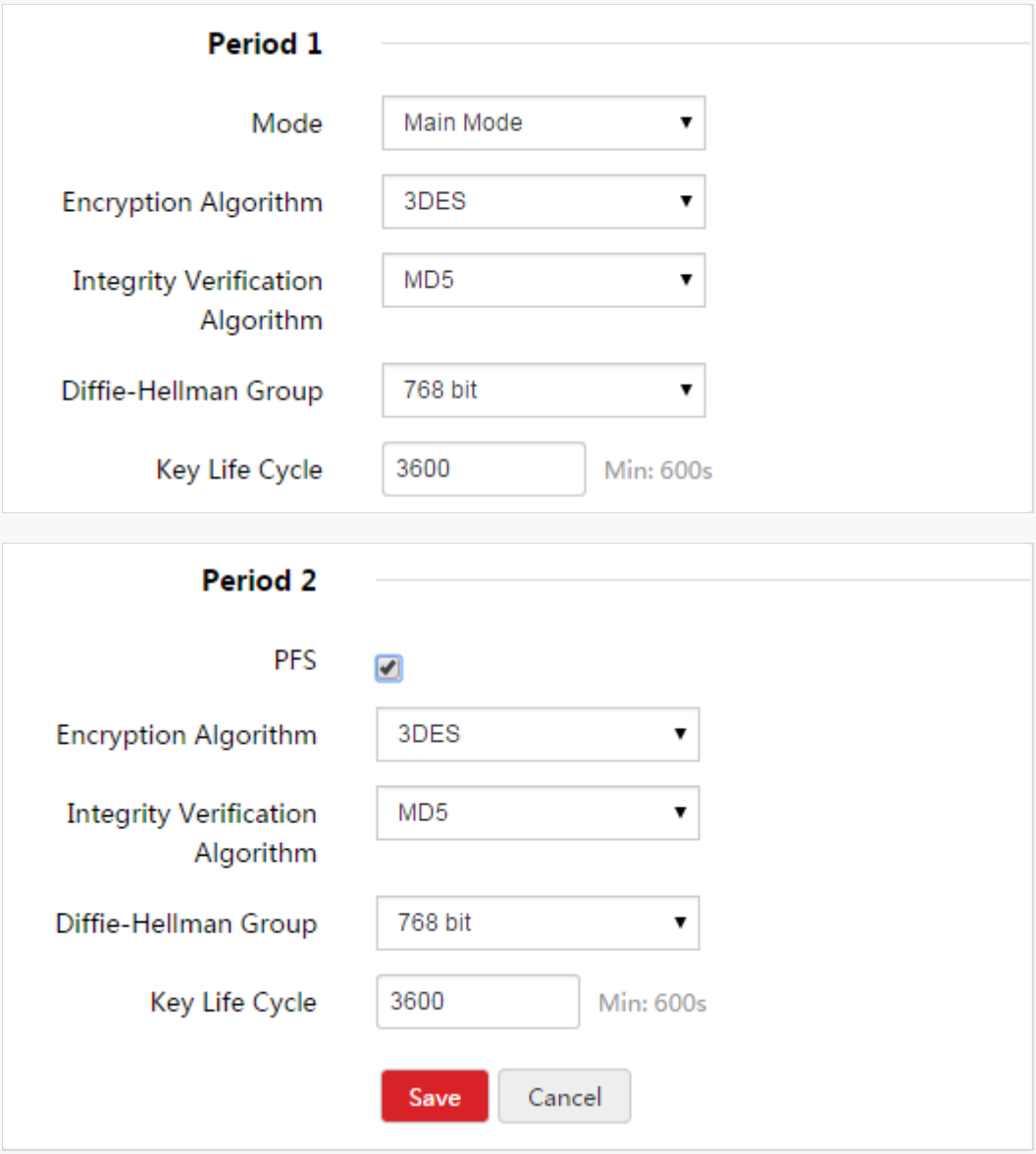
❻ Set a pre-shared key, say 12345678.

❼ Check **PFS**.

❽ Verify that other parameters on both the IPsec server and IPsec client are identical.

❾ Click **Save** to apply your changes.



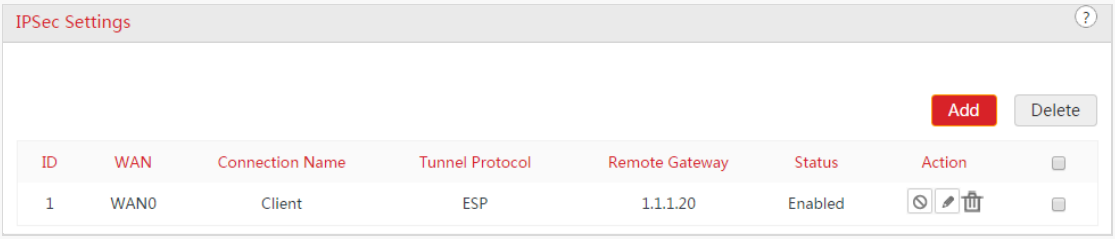


When configurations are completed, the following actions are allowed:

- Click the button  to disable IPsec settings, and click the button  to enable IPsec settings.
- Click the button  to edit IPsec settings.
- Click the button  to delete IPsec settings.

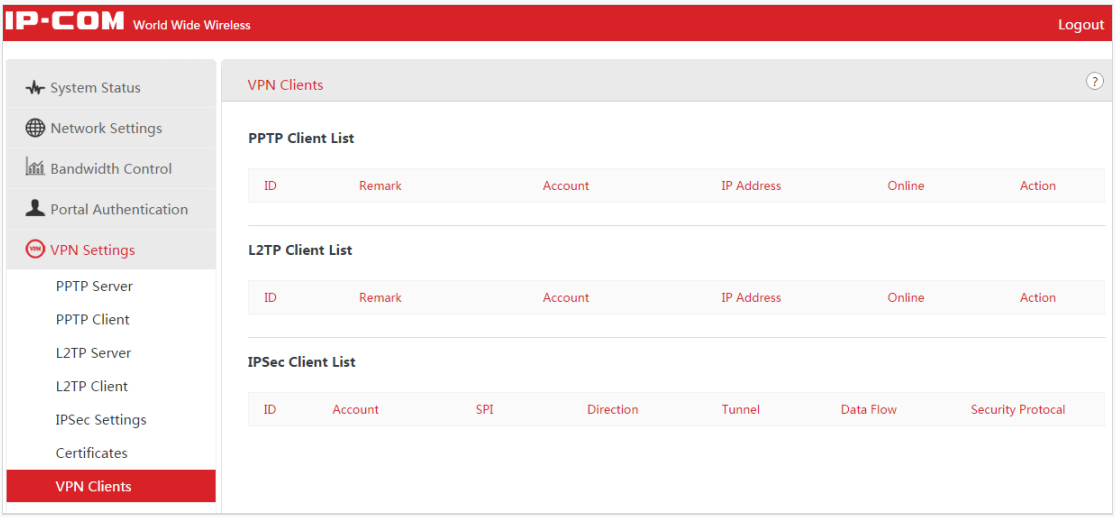
NOTE

When IPsec negotiation completes, you cannot directly edit IPsec settings. If necessary, click the button  to disable IPsec settings first, and then edit it.



◆ Verification

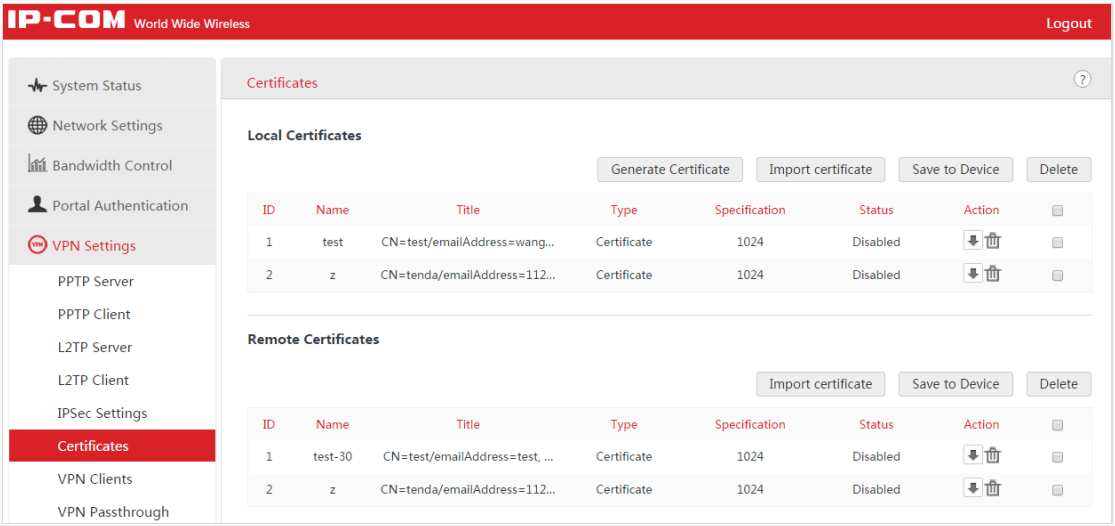
Method 1: On the web UI of SE3100 in the headquarters, click **VPN Settings > VPN Clients** to view the IPsec Client List. If the IPsec client negotiates with the IPsec server successfully, IPsec client info will be displayed here.



Method 2: When staffs in the headquarters and the branch can PING each other's internal IPs successfully, or when they can visit each other's internal resources successfully, like FTP server, file server, etc., IPsec negotiation has been achieved successfully.

Certificates

The function of Certificates should be used together with the IPsec function. When the authentication type of IPsec is X.509, corresponding certificates configurations will be needed. Click **VPN Settings > Certificates** to configure certificates settings:



1 On the local router, generate a local certificate, click **Save to Device** and click  to download the certificate. Meanwhile, import the certificate to “Remote Certificates” of the remote router and click **Save to Device**.

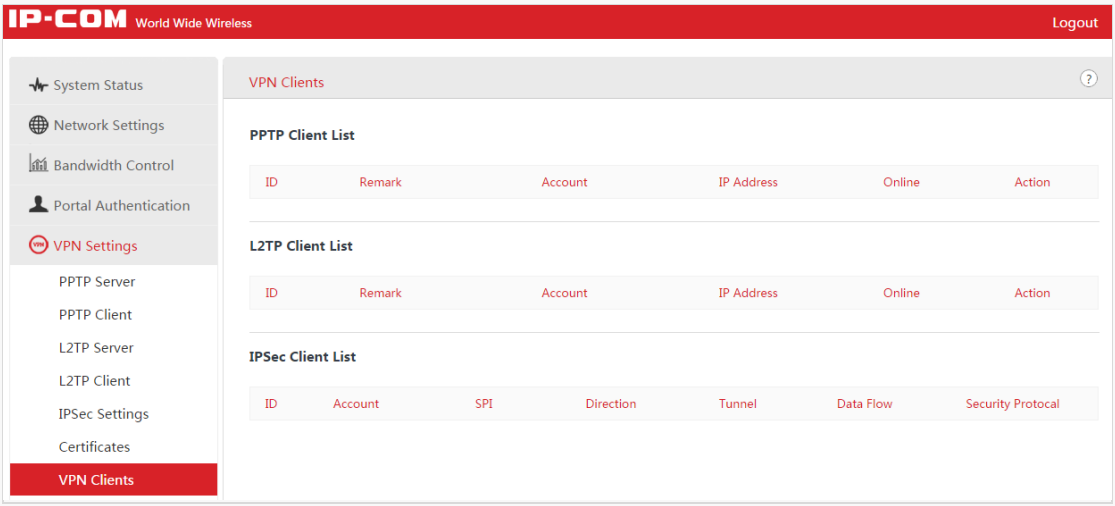
2 On the remote router, generate a local certificate and click **Save to Device** and click  to download the certificate. Meanwhile, import the certificate to “Remote Certificates” of the local router and click **Save to Device**.

TIP

How to generate a local certificate: you can click **Generate Certificate** to generate one, or you can click **Import Certificate** to import the certificate and key generated in other ways.

VPN Clients

When you configure a PPTP/L2TP server or IPsec settings on the local router and its corresponding client has been negotiated successfully, the corresponding client info will be displayed on the VPN Client page.



PPTP Client List/L2TP Client List:

- **ID:** Sequence number of the PPTP/L2TP client.
- **Remark:** User identification of the connected PPTP/L2TP client.
- **Account:** User name of the connected PPTP/L2TP client.
- **IP Address:** The IP address that the connected PPTP/L2TP client has obtained.
- **Online:** Online duration of the PPTP/L2TP client.
- **Action:** Click **Disconnect** will disconnect the corresponding client's connection and the client will connect to it actively.

IPsec Client List

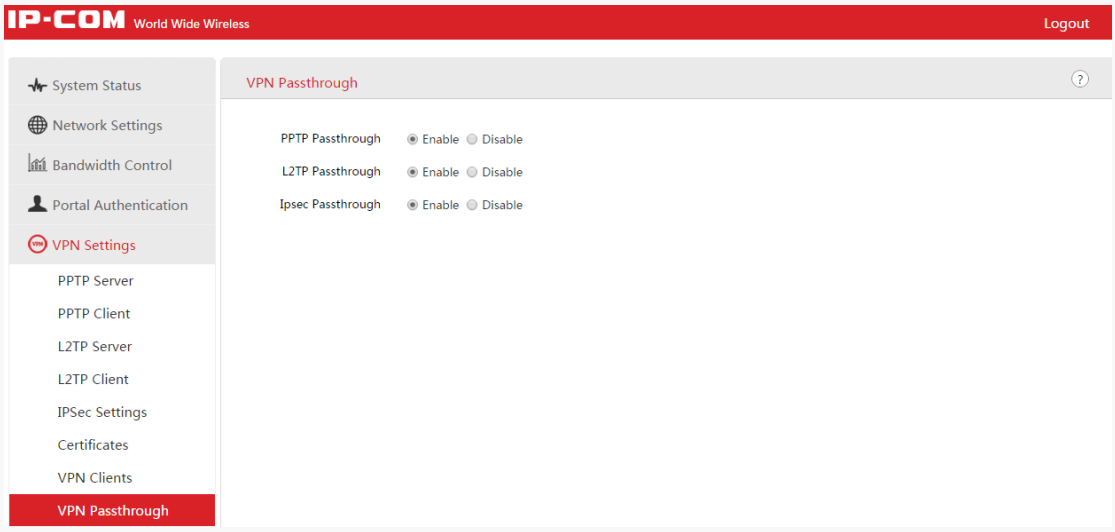
- **ID:** Sequence number of the IPsec client.
- **Account:** Connection name of the IPsec client.
- **SPI:** The SPI value is obtained via manual setup or auto-negotiation. SPI, remote gateway and tunnel protocol identify an IPsec alliance.
- **Direction:** In or Out. In: remote router to local router. Out: local router to remote router.
- **Tunnel:** If the direction is In, the tunnel will be displayed as "the WAN IP address of the remote router" first and then "the WAN IP address of the local router". If the direction is Out, the tunnel will be displayed as "the WAN IP address of the local router" first and then "the WAN IP address of the remote router".
- **Data Flow:** The direction of data flow. If it is In, the data flow will be from the internal network of the remote router to the internal network of the local router. If it is Out, it is the opposite.

- Security Protocol: Display the tunnel security protocols after the IPsec negotiation: ESP, AH or ESP+AH.

VPN Passthrough

In actual VPN application, NAT gateway may exist on its physical link. When packets pass by the NAT gateway, its IP address or port number will change. Thus, after the remote VPN tunnel has received packets, authentication failure occurs and packets will be dropped directly. VPN Passthrough can avoid this problem by adding new IP header and UDP header to packets of ESP protocol. Then format of the packet will be "New IP/UDP Header/ESP Header/IP Header/Data. As the NAT gateway will only change the IP header of the outermost layer, and the IP header is not included in ESP verification. In this way, IPsec communication will not be affected. However, NAT passthrough only applies to ESP. As the IP header is included in AH verification, AH and NAT cannot co-exist.

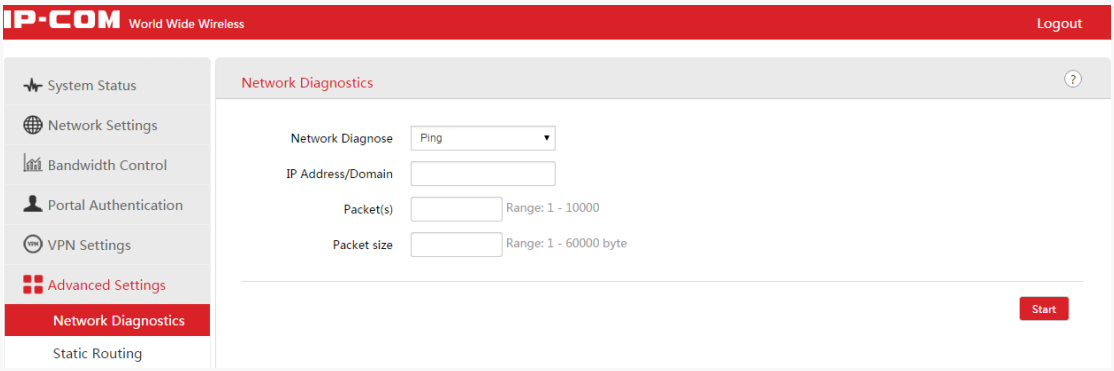
Click **VPN Settings > VPN Passthrough** to configure VPN Passthrough settings.



Advanced Settings

Network Diagnostics

This page allows you to test your network connection. If your network is malfunctioning, click **Advanced Settings > Network Diagnostics** to use the ping or Traceroute utility to test your network and find out where the problem is.



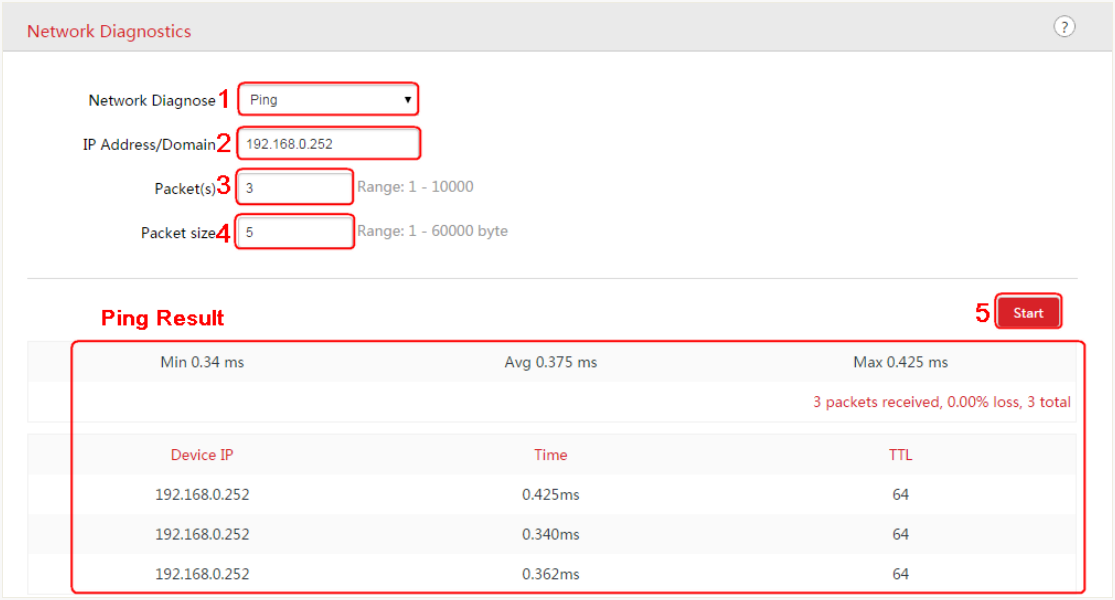
Ping

Ping, a computer network administration utility, is used to test the reachability of a host on an Internet Protocol (IP) network and to measure the round-trip time for messages sent from the original host to a destination computer.

To implement **Ping** action, click **Advanced Settings > Network Diagnostics** and finish settings as shown below:

1. **Network Diagnose:** Select **Ping** from the drop-down menu.
2. **IP Address/Domain:** Specify an IP address or domain name you wish to diagnose.
3. **Packet(s):** Set the number of Ping packets within the range from 1 to 10000.
4. **Packet Size:** Set the packet size within the range from 1 to 60000 bytes.
5. Click **Start** to Ping the network.

Then you can view the Ping info in the ping result box below:



Traceroute

Traceroute is a computer network diagnostic tool for displaying the route (path) and measuring whether network connection is available or not. When malfunctions occur to the network, you can locate trouble spot of the network with this traceroute test.

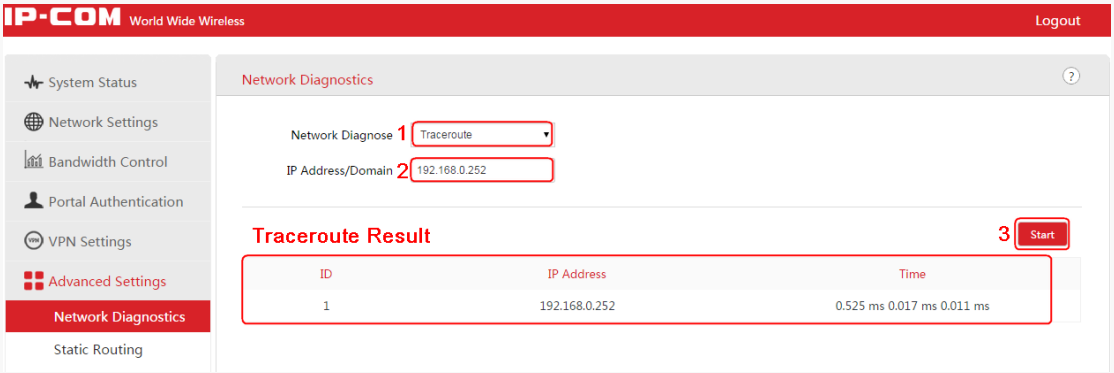
To implement Traceroute action, click **Advanced Settings > Network Diagnostics** and finish settings as shown below:

1 **Network Diagnose:** Select **Traceroute** from the drop-down menu.

2 Enter the destination IP or domain name of the destination host.

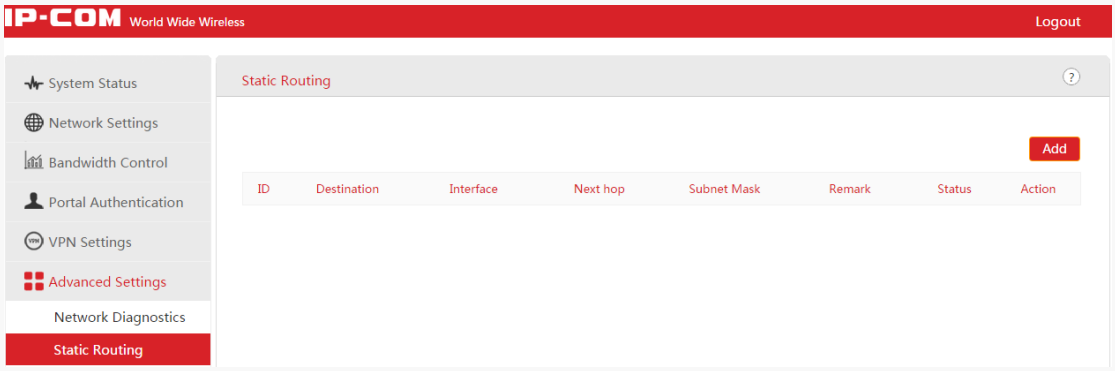
3 Click **Start** to traceroute the network.

Then you can view the traceroute info in the traceroute box below:



Static Routing

Static routing provides additional routing information to your router. Typically, you do not need to add static routes. However, when there are several routers in the network, you may want to set up static routing. Static routing determines the path of the data in your network. You can use this feature to allow users on different IP segments to access the Internet via this device. It is not recommended to use this setting unless you are familiar with static routing.

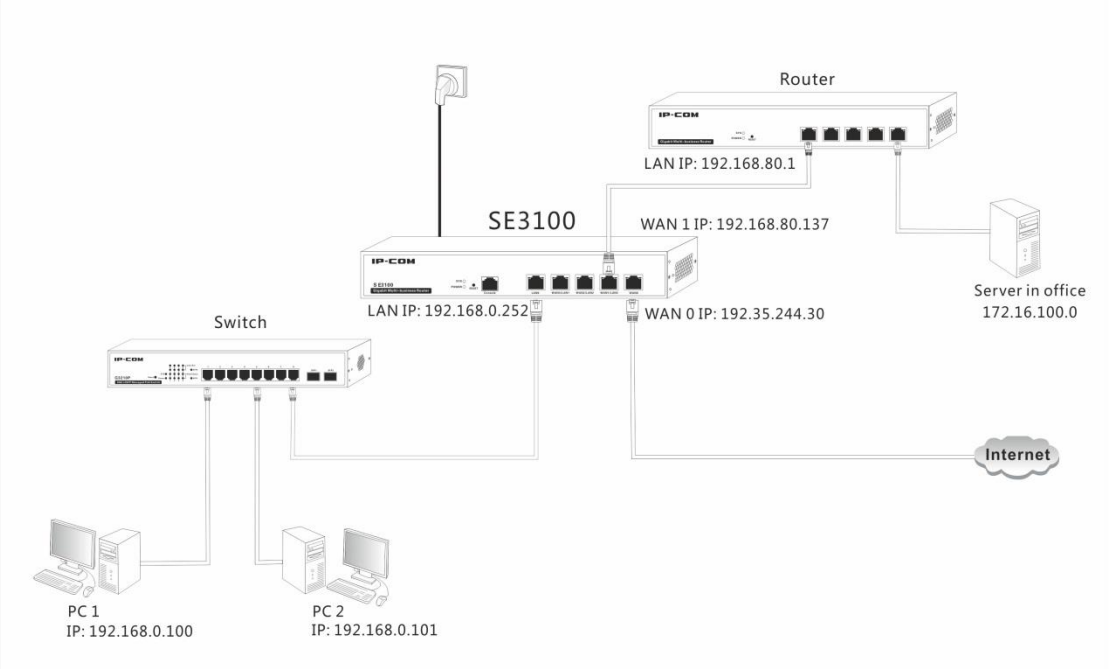


- **Destination:** The destination network segment.
- **Interface:** Select the port you wish to configure the static routing rule.
- **Next Hop:** Enter the gateway to which the packet should be sent next.
- **Subnet Mask:** Enter the Subnet Mask used on the destination network.
- **Remark:** Give a brief description for the rule.
- **Add:** Click it to create a static routing rule.

TIP

1. Gateway must be on the same IP segment as WAN or LAN segment of the router.

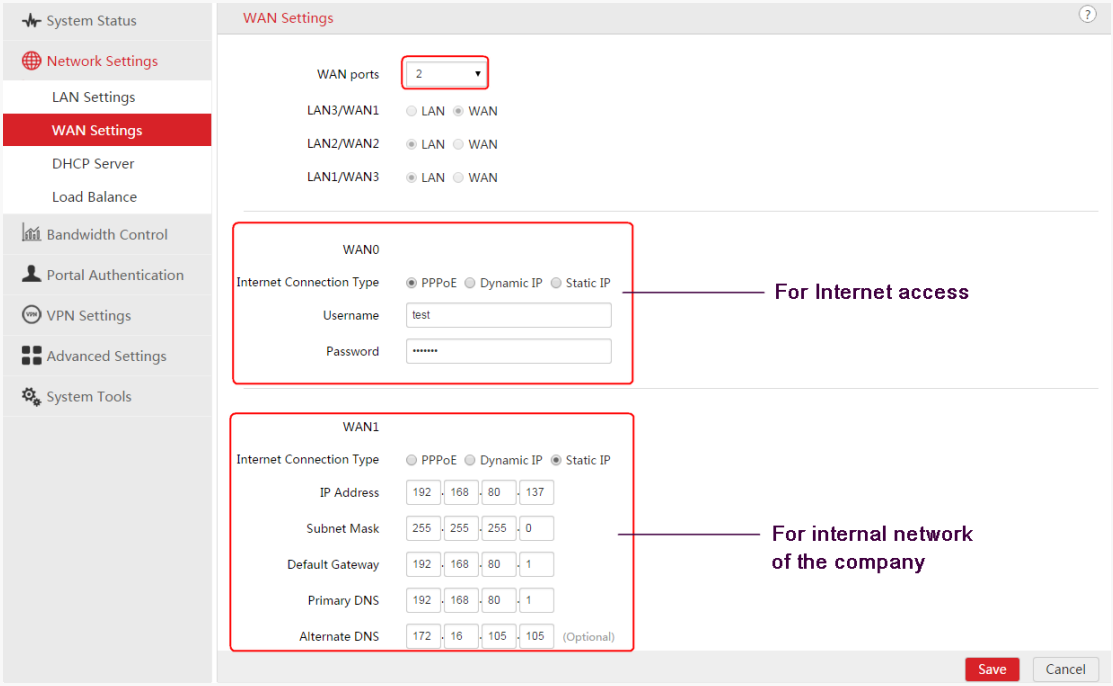
2. Subnet Mask must be entered 255.255.255.255 if destination IP address is a single host.



For example, your company's internal network and Internet are on different IP net segments and you want PCs on your LAN to access the Internet and your company internal network via this device. You can simply configuring static routes on this Router. The figure above depicts this application scenario.

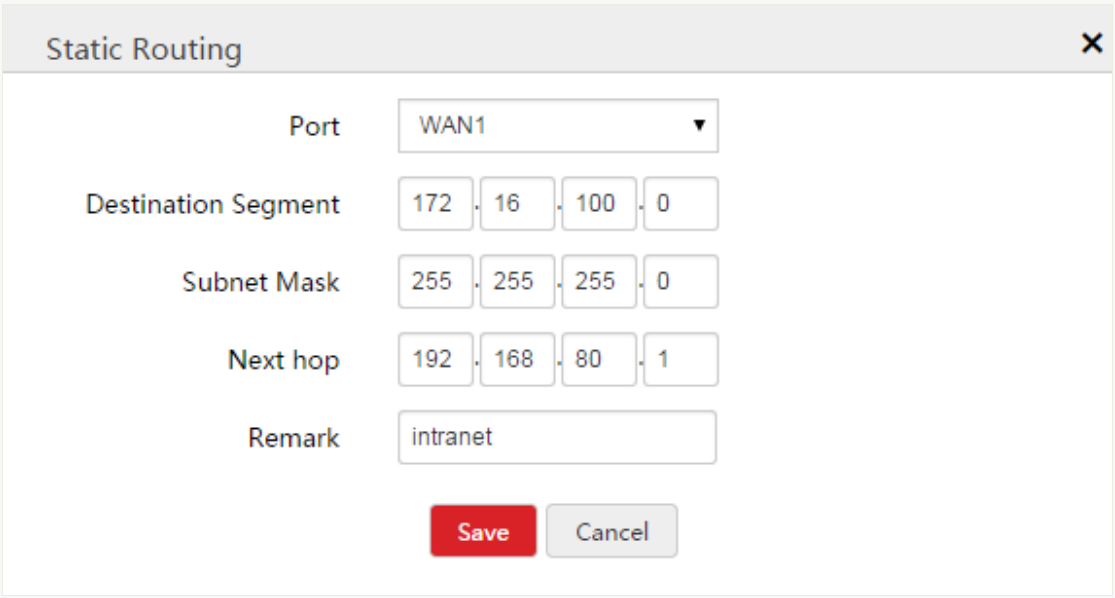
Configuration Steps:

Step 1: Click **Network Settings > WAN Settings** to set 2 WAN ports and configure corresponding WAN settings for this device. For specific steps, see WAN Settings.



Step 2: Add a static route to WAN 1 (As the default WAN port is WAN 0, in this example, you only have to add a staic route to WAN 1).

❶ Click **Advanced Settings > Static Routing** and click **Add** to create a static routing rule.



❷ **Port:** Select WAN 1 from the drop-down menu.

❸ **Destination Segment:** Enter the destination segment here. In this example, it is 172.16.100.0.

❹ **Subnet Mask:** In this example, enter 255.255.255.0.

❺ **Next Hop:** Enter the gateway of WAN 1 here. In this example, it is 192.168.80.1.

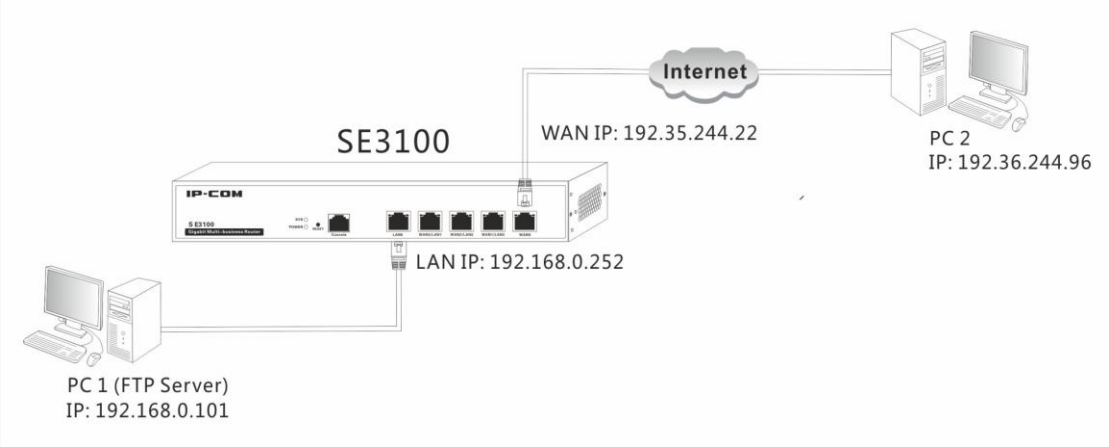
❻ **Remark:** Give a description for this rule.

❼ Click **Save** to apply your settings.

Then your PCs in the LAN can access both the internal network of your company and the Internet.

Port Forwarding

Port forwarding is useful for web servers, ftp servers, e-mail servers, gaming, and other specialized Internet applications. When you enable Port Forwarding, the communication requests from the Internet to your router's WAN port will be forwarded to the specified IP address.



Application Example:

As shown in the diagram above, your PC (PC1: 192.168.0.101) connects to the router and runs an FTP server on port number 21. Your friend (PC2: 192.36.244.96) wants to access the FTP server on your PC.

TIP

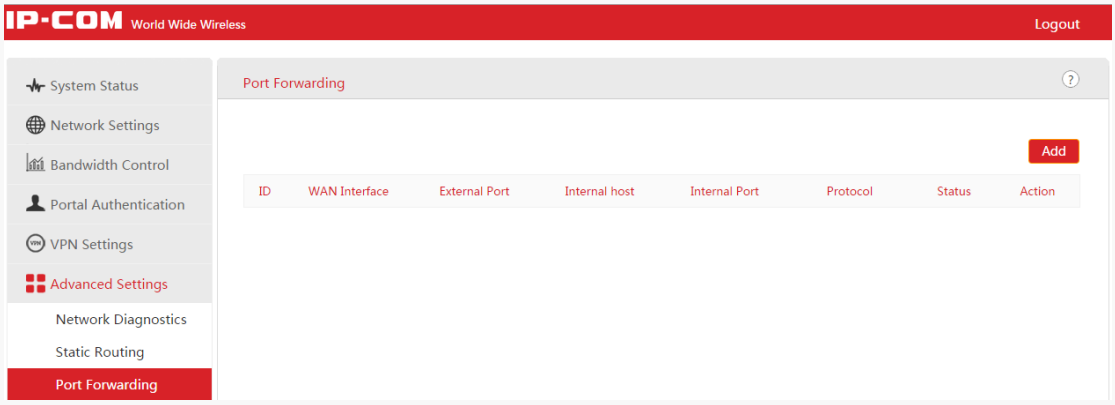
1. Make sure your WAN IP address (Internet IP address) is a public IP address. Private IP addresses are not routed on the Internet.

2. Make sure that the service port number you entered on the router and the service port number you configured on the PC are identical.

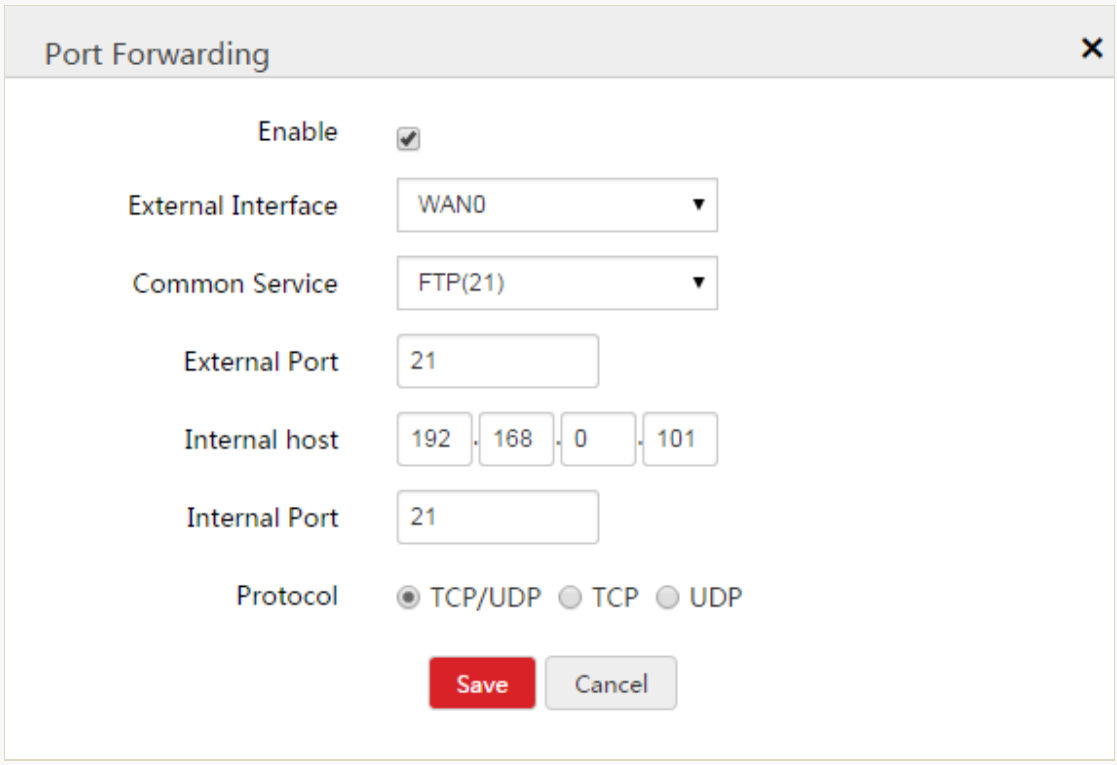
3. To ensure that your server computer always has the same IP address, assign a static IP address

to your PC.

4. Operating System built-in firewall and some anti-virus programs may block other PCs from accessing resources on your PC. So it is advisable to disable them before using this feature.



1 Click **Advanced Settings > Port Forwarding** to enter the page as shown above and click **Add**.



2 Check the **Enable** box to enable the port forwarding function.

3 **External Interface:** Specify the WAN port you want to configure port forwarding settings.

4 **External /Internal Port:** Specify the external port and internal port (Generally, the port

number in both External and Internal port fields are the same, say, 21 for FTP). Contact the corresponding service provider or google it if you don't know the port number of the service to use.

❺ **Internal host:** Specify the internal host's IP address. In this example, enter 192.168.0.101.

❻ **Protocol:** Specify the protocol required for the service utilizing the port(s). Select TCP/UDP if you are not sure.

❼ Click **Save** to apply your changes.

Now, your friends only need to enter **ftp://xxx.xxx.xxx.xxx:21** in their browsers to access your FTP server. xxx.xxx.xxx.xxx is the router's WAN IP address. In this example, it is 192.35.244.22, and then your friends need to enter **ftp:// 192.35.244.22:21** in their browsers.

NOTE

If you use the port number 80 here, you must set the port number for remote WAN (Click **Advanced Settings > Remote WAN**) to any port number excluding 80 to avoid conflicts. Otherwise the port forwarding feature may not be effective.

Remote WAN

The Remote WAN allows the device to be configured and managed remotely from the Internet via a web browser. Click **Advanced Settings > Remote WAN** to enter the configuration page.

TIP

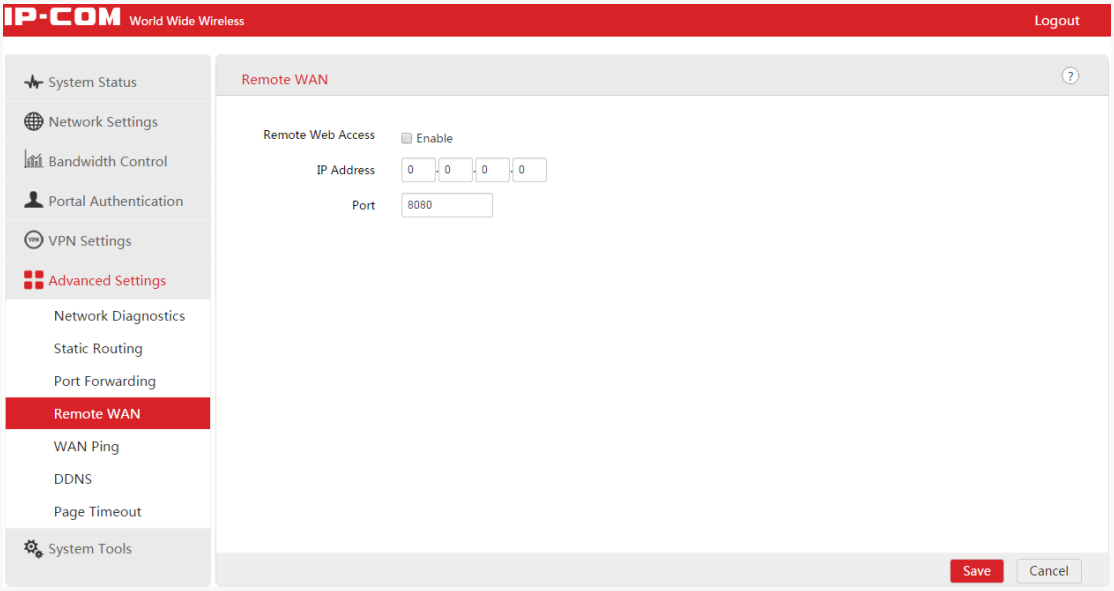
1. For better security, customize a port number between 1024 and 65535 for the remote WAN interface. Do not use the number of any common service port (1-1024) in case of conflicts.

2. Make sure your WAN IP address (Internet IP address) is a public IP address. Private IP addresses are not routed on the Internet.

3. It is unsafe to make your router remotely accessible to all PCs on external network. For better security, we suggest that only enter the IP address of the PC for remote management.

To access your router (WAN IP address: 102.33.66.88) at your home from the PC

(218.88.93.33) at your office via the port number 8080:



❶ Check the **Enable** box to enable the Remote Web Access function.

❷ **IP Address:** Specify the IP address for remote management (When it is set to 0.0.0.0, the device becomes remotely accessible to all the PCs on Internet or other external networks. It is not safe). In this example, enter 218.88.93.33.

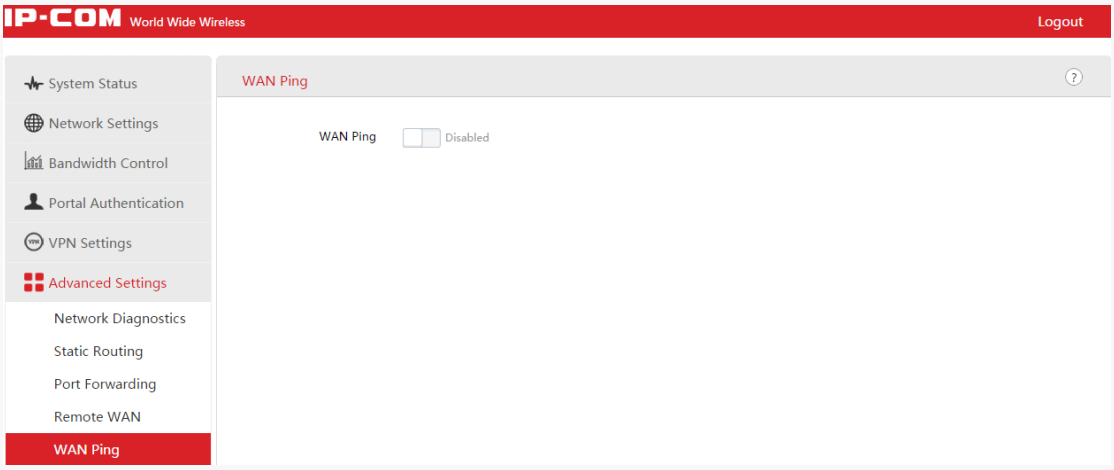
❸ **Port:** Specify the management port to be open to outside access. The default setting is 8080. This can be changed.

❹ Click **Save** to apply your changes.

Type **http://102.33.66.88:8080** into your browser's address or location field and you can access the router at your home remotely.

WAN Ping

This page is used to enable ping response from WAN port. Click **WAN Ping** to enable the ping response from WAN port. Then when remote host ping the IP of WAN port, the device will response.



DDNS

Dynamic DNS or DDNS is a term used for the updating in real time of Internet Domain Name System (DNS) name servers. We use a numeric IP address allocated by Internet Service Provider (ISP) to connect to Internet; the address may either be stable ("static"), or may change from one session on the Internet to the next ("dynamic"). However, a numeric address is inconvenient to remember; an address which changes unpredictably makes connection impossible. The DDNS provider allocates a static host name to the user; whenever the user is allocated a new IP address this is communicated to the DDNS provider by software running on a computer or network device at that address; the provider distributes the association between the host name and the address to the Internet's DNS servers so that they may resolve DNS queries. Thus, uninterrupted access to devices and services whose numeric IP address may change is maintained.

Click **Advanced Settings > DDNS** to enter the DDNS page.

TIP

1. To use the DDNS feature, you need to have an account with one of the domain service providers in the drop-down menu first.

2. This router supports 4 DDNS service providers: 88ip.cn, 3322.org, dyndns and no-ip.com.

Application Example:

If your ISP gave you a dynamic (changing) public IP address, you want to access your router remotely but you cannot predict what your router's WAN IP address will be, and the address can

change frequently. In this case, you can use a commercial Dynamic DNS service. It lets you register your domain to their IP address and forwards traffic directed at your domain to your frequently changing IP address.

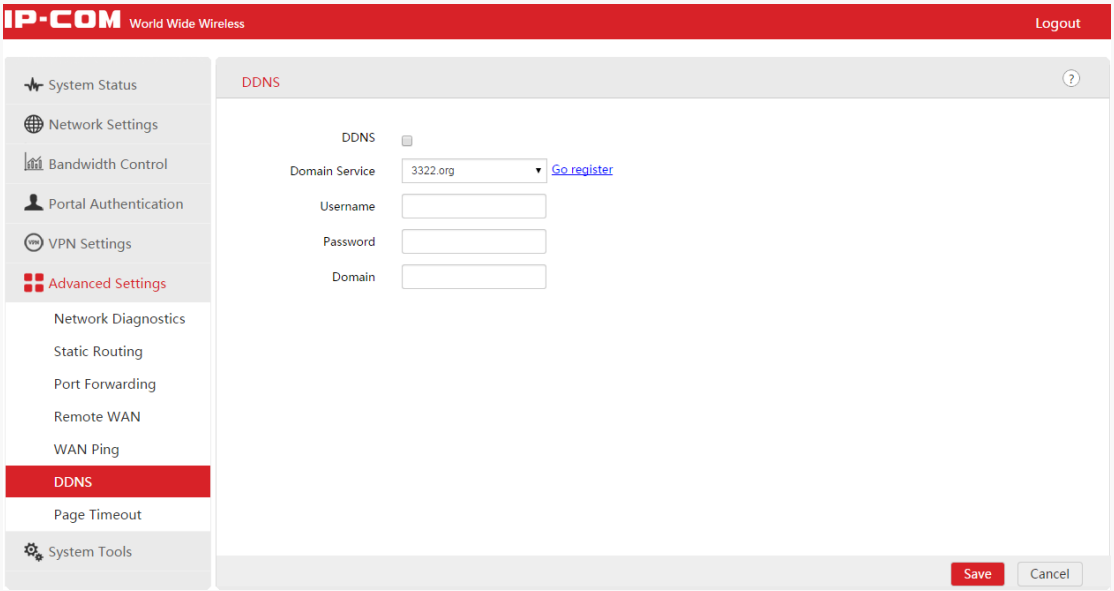
Assume that you obtain the following account from your dyndns.org service provider:

User Name: ip-com

Password: 123456

Domain Name: ipcom.dyndns.org.

And you want to use the PC at 218.88.93.33 to remotely access this router on port number 8090.



❶ **DDNS:** Check the DDNS box to enable this function.

❷ **Domain Service:** Select your DDNS service provider from the drop-down menu. Here in this example, select **dyndns.org**.

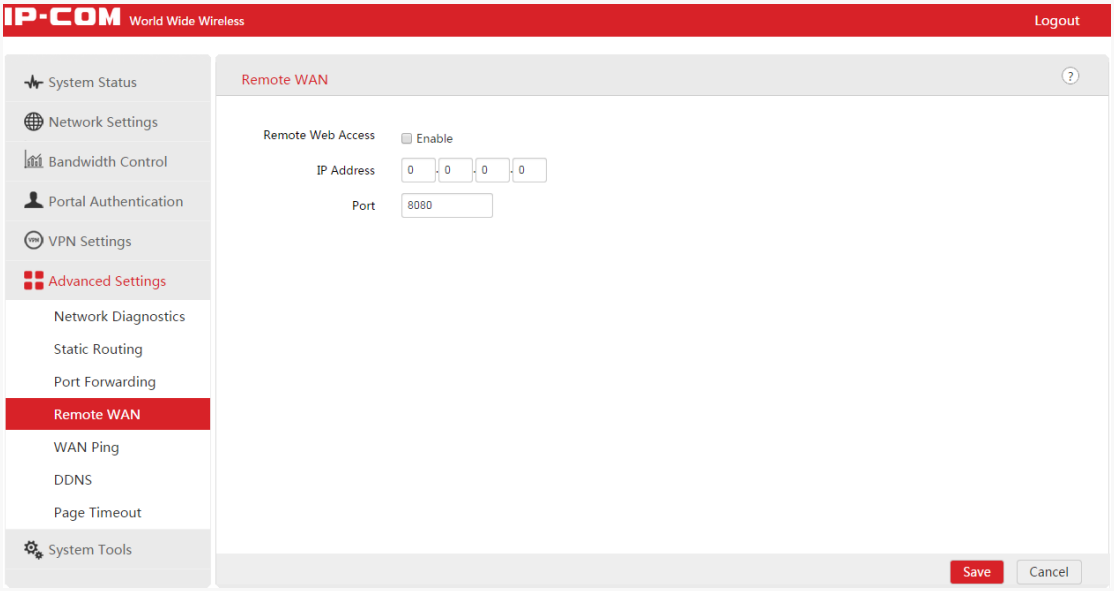
❸ **Username:** Enter the DDNS user name registered with your DDNS service provider. Here in this example, enter ip-com.

❹ **Password:** Enter the DDNS Password registered with your DDNS service provider. Here in this example, enter 123456.

❺ **Domain:** Enter the DDNS domain name with your DDNS service provider. Here in this example, enter ipcom.dyndns.org.

❻ Click **Save** to save your settings.

❼ Click **Advanced Settings > Remote WAN** to enable the Remote WAN function, enter 218.88.93.33 in the IP Address field, and 8090 in the Port field , then click **Save** to save your settings.



Now you can access the router from the Internet by entering **http://ipcom.dyndns.org:8090** in your browser.

Page Timeout

You are automatically logged out of the web manager after a period of inactivity. You can set the length of the inactive period. To change the page idle timeout, click **Advanced Settings > Page Timeout** to set the page timeout you wish to and click **Save**. The default is 5 minutes.

System Tools

This section helps you to better monitor and maintain your device.

Date & Time

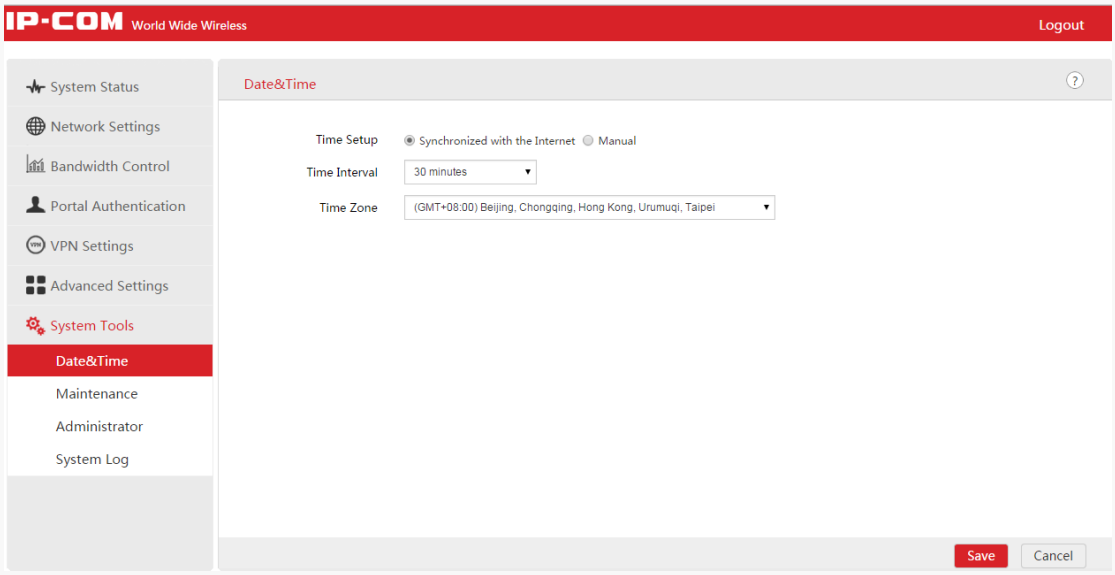
This page assists you in setting the device's current time; you can select to either set the time and date manually or obtain the GMT time from the Internet automatically. System time can be configured using the following 2 methods:

Synchronized with the Internet: If enabled, system automatically connects to NTP server on the Internet to synchronize the time.

Manual: Specify the time and date manually or click **Synchronized with local time** to automatically copy your current PC's time to the device.

Method 1: To synchronize with the Internet:

1. Click **System Tools > Date & Time**.
2. **Time Setup:** Select **Synchronized with the Internet**.
3. **Time Interval:** Select a time interval from the drop-down list.
4. **Time Zone:** Select your time zone.
5. Click **Save** to apply your changes.



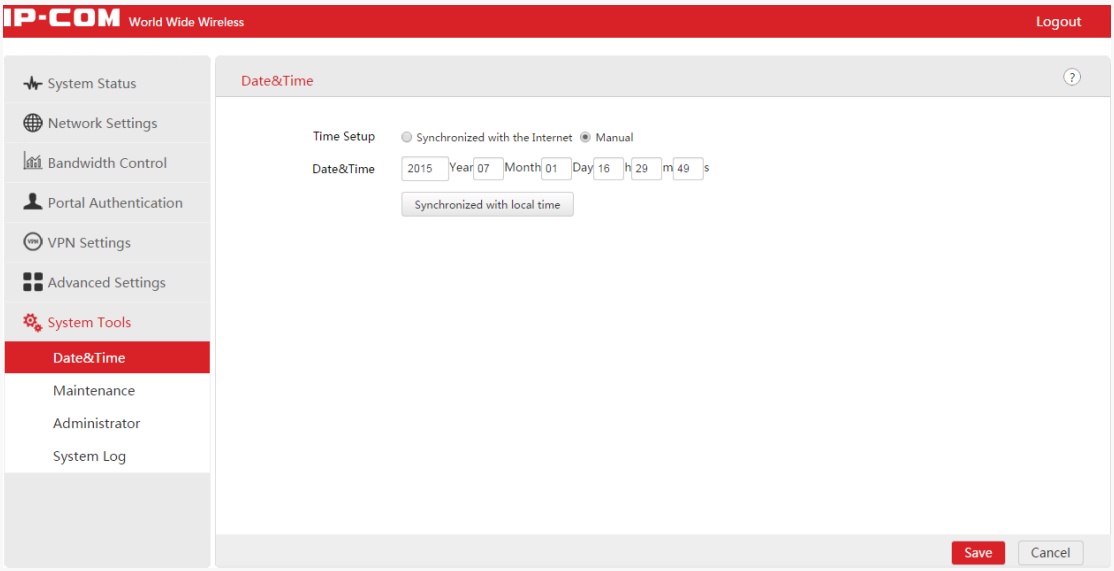
Method 2: To set date and time manually:

1. Click **System Tools > Date & Time**.

❷ **Time Setup:** Select **Manual**.

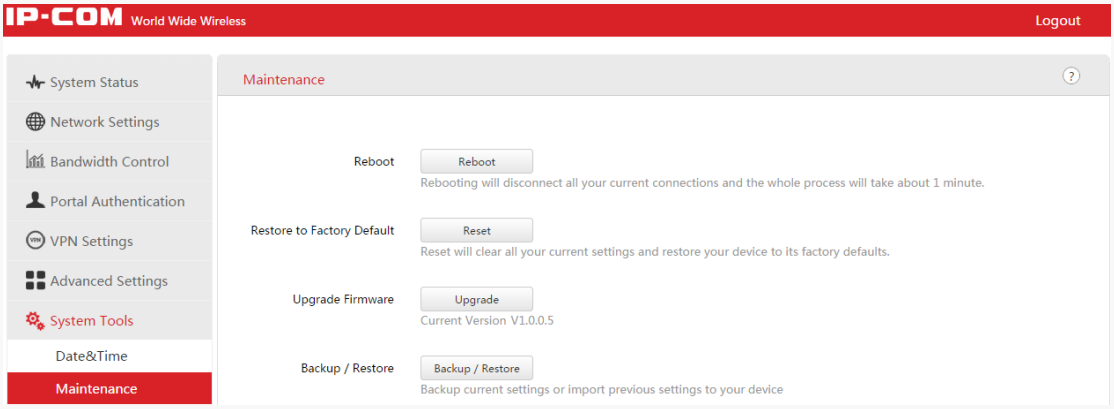
❸ Specify the time and date manually or click **Synchronized with local time** to automatically copy your PC's time to the device.

❹ Click **Save** to apply your changes.



Maintenance

Here you can reboot, reset, upgrade your device, and backup/restore settings for your device. click **System Tools > Maintenance** to enter page below:



Reboot

When some settings you have configured cannot be activated or your device is functioning improperly, you can reboot your device. Locate the Reboot section and click **Reboot** to reboot the device. All the connections will be disconnected when rebooting.

Reset

If the device or client connected to the device fails to access the Internet due to incorrect configurations and you cannot solve the problem, you can reset the device. Once you reset your device, all your current settings will be lost and you need to reconfigure it.

To reset your device, two methods are available:

Method 1: Via Web UI

Click **System Tools** > **Maintenance**, locate the Restore to Factory Default section and click **Reset**.

Method 2: Via the hardware RESET button

Pressing the RESET button for 5~15 seconds restores this device to its factory defaults.

Factory Default Settings:

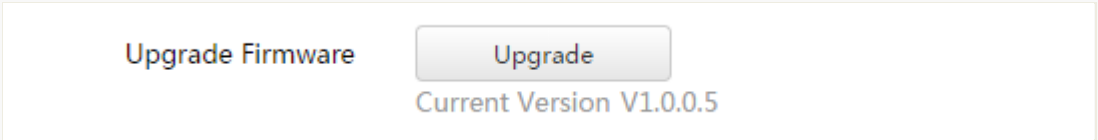
- User Name: admin
- Password: admin
- IP Address: 192.168.0. 252

Upgrade

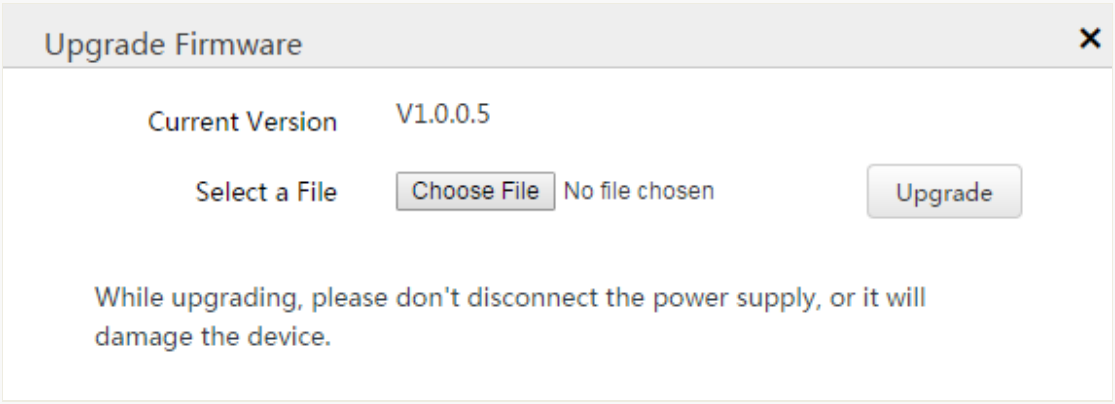
If your device is in normal operation, it is not advisable to upgrade your device. If you want to acquire the latest software version or better value-added functions for your device, you can access our official website www.ip-com.com.cn to download the latest software for upgrading.

To upgrade your device:

1. Launch a web browser and go to www.ip-com.com.cn to download the latest firmware.
2. Unzip the compressed upgrade file in the corresponding directory.
3. Click **System Tools** > **Maintenance**, locate the Upgrade Firmware section and click **Upgrade**.



❹ Click **Choose File** (in Google browser) to locate and select the upgrade file in the corresponding directory on your hard disk.



❺ Click **Upgrade**.

NOTE

1. While upgrading, please verify that your PC is connected to the device with an Ethernet cable and power is delivered on this device. And the upgrading process will take several minutes, please be patient.

2. When the upgrading is completed, your device will be restored to factory default settings automatically and you need to reconfigure your device.

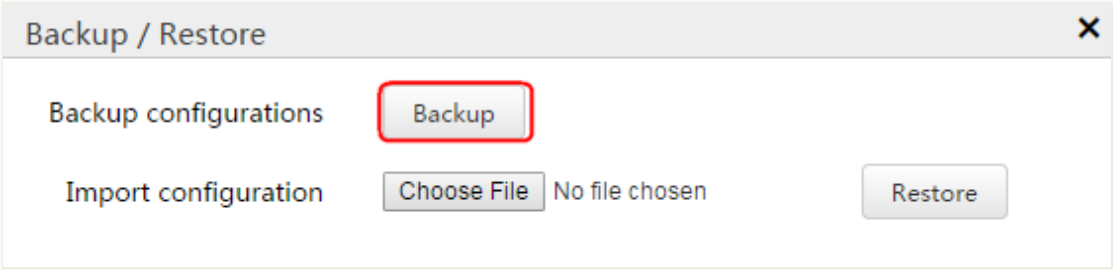
Backup/Restore

If you configure many settings on this device, which will make this device work in good status and suitable environment, it's suggested to backup settings for this device, which will be convenient for troubleshooting and saving time for next time's configuration.

To backup your configurations:

❶ Click **System Tools** > **Maintenance**, locate the Backup/Restore section and click **Backup/Restore**.

❷ Click **Backup** on the pop-out window and follow on screen instructions to save your configurations in a directory on your hard disk.

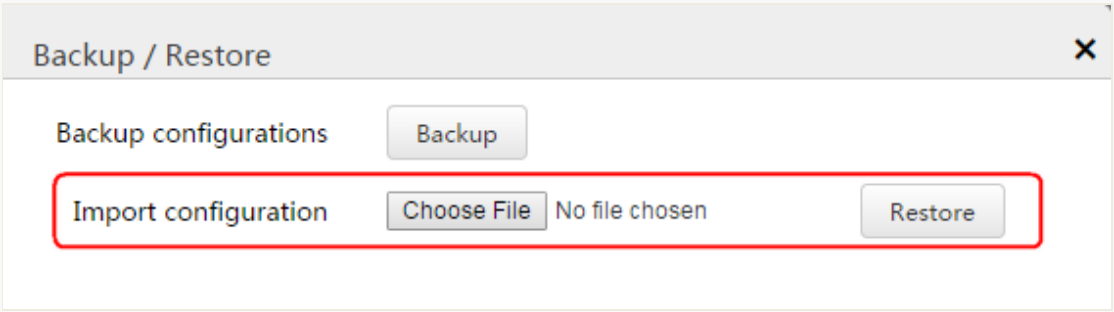


To restore your configurations:

❶ Click **System Tools > Maintenance**, locate the Backup/Restore section and click **Backup/Restore**.

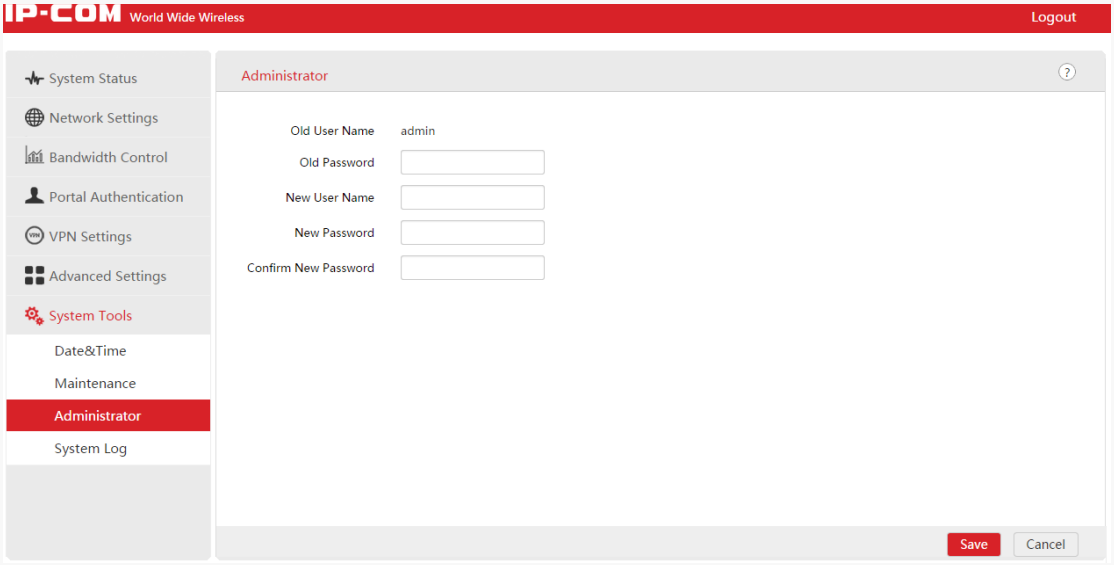
❷ Click **Choose File** (in Google browser) to load configuration files which you have stored on your hardware disk previously.

❸ Click **Restore**.



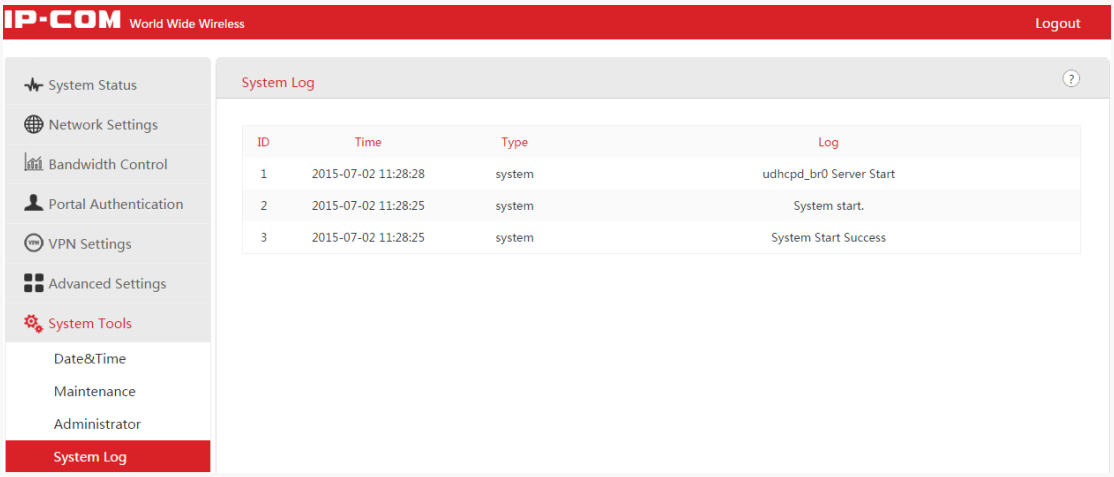
Administrator

This page allows you to change the login username and password of the administrator. Click **System Tools > Administrator** to enter page below:



System Log

Here you can view the history of the device's actions. After 300 entries, the previous logs will be cleared automatically.



Appendix

1 FAQs

Q1: I cannot log in to the device configuration screen with 192.168.0.252 during the initial login. What should I do?

A1: ❶ Verify that all cables are connected correctly and well.

❷ Confirm the TCP/IP settings on your PC, verify it is 192.168.0.x（"x" can be any number between 2~254, excluding 252) and retry.

❸ Clear the Web browser cache or try another browser.

❹ Try another computer to access the configuration screen.

❺ Restore the device to factory defaults and retry.

❻ Confirm there is no device in the same LAN whose IP is 192.168.0.252, and retry.

Q2: I forgot my login username and password. What should I do?

A2: Try the default settings first (Default LAN IP: **192.168.0.252**, Login username: **admin**; password: **admin**). If it does not work, restore the device to factory defaults and retry with the default settings.

Q3: How do I restore the device to factory defaults if I cannot access the device configuration screen?

A3: Power up the device and press the RESET button on the front panel for 5~15 seconds. In about one minute, the device should restore to its factory defaults.

NOTE

Restoring factory defaults will delete all the configured settings. You must reconfigure them.

2 Technical Specifications

Item	Specification
Max Connections	120
CPU	Dual-core ARM 800MHz processor
DDR3	256MB
FLASH	128MB
Max concurrent session	60000
Throughput (two-way)	100Mbps
Interface	5 10/100/1000Mbps auto-negotiating RJ45 ports (Default: 2 WAN, 3 LAN; Max: 4 WAN, 1 LAN) 1 Console port
LEDs	1 POWER LED 1 SYS LED 5 Link/Act LEDs 5 Speed LEDs
Button	1 RESET button 1 ON/OFF button
Operation/Storage temperature	-10℃~45℃ / -40℃~70℃
Operation/Storage humidity	10%~90% RH (non-condensing) / 5%~90% RH (non-condensing)
AC input	100~240V AC, 50/60Hz
Power consumption	≤ 24W
Dimension	294mm*178mm*44mm

3 Regulatory Compliance Information

CE Mark Warning

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

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.

FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to 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.

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

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. The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this 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.