Accessing the Switch

CHAPTERS

This guide applies to:

T1500G-10PS v2 or above, T1500G-8T v2 or above, T1500G-10MPS v2 or above, T1500-28PCT v3 or above, T1600G-18TS v2 or above, T1600G-28PS v3 or above, T1600G-28TS v3 or above, T1600G-52TS v3 or above, T1600G-52PS v3 or above, T1700X-16TS v3 or above, T1700G-28TQ v3 or above, T2500G-10TS v2 or above, T2600G-18TS v2 or above, T2600G-28TS v3 or above, T2600G-28MPS v3 or above, T2600G-28SQ v1 or above, T2600G-52TS v3 or above.

1 Overview

You can access and manage the switch using the GUI (Graphical User Interface, also called web interface in this text) or using the CLI (Command Line Interface). There are equivalent functions in the web interface and the command line interface, while web configuration is easier and more visual than the CLI configuration. You can choose the method according to their available applications and preference.

2 Web Interface Access

You can access the switch's web interface through the web-based authentication. The switch uses two built-in web servers, HTTP server and HTTPS server, for user authentication.

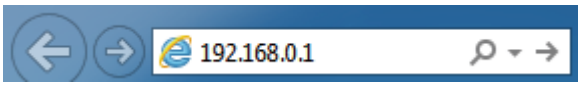
The following example shows how to login via the HTTP server.

2.1 Login

To manage your switch through a web browser in the host PC:

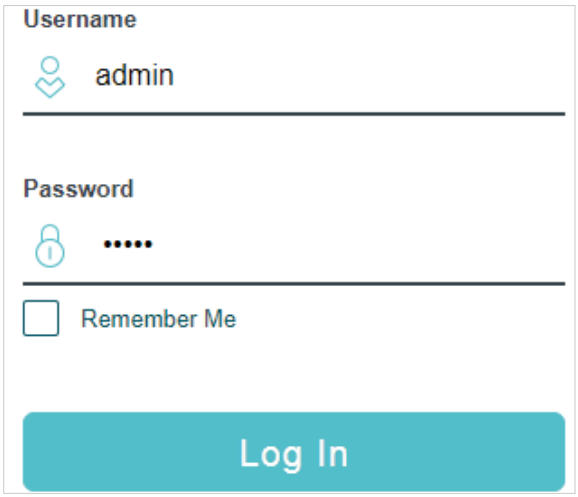
1) Make sure that the route between the host PC and the switch is available.
2) Launch a web browser. The supported web browsers include, but are not limited to, the following types:
   - IE 8.0, 9.0, 10.0, 11.0
   - Firefox 26.0, 27.0
   - Chrome 32.0, 33.0
3) Enter the switch's IP address in the web browser's address bar. The switch's default IP address is 192.168.0.1.

   Figure 2-1 Enter the Switch's IP Address in the Browser



4) Enter the username and password (both **admin** by default) in the pop-up login window.

   Figure 2-2 Login Authentication

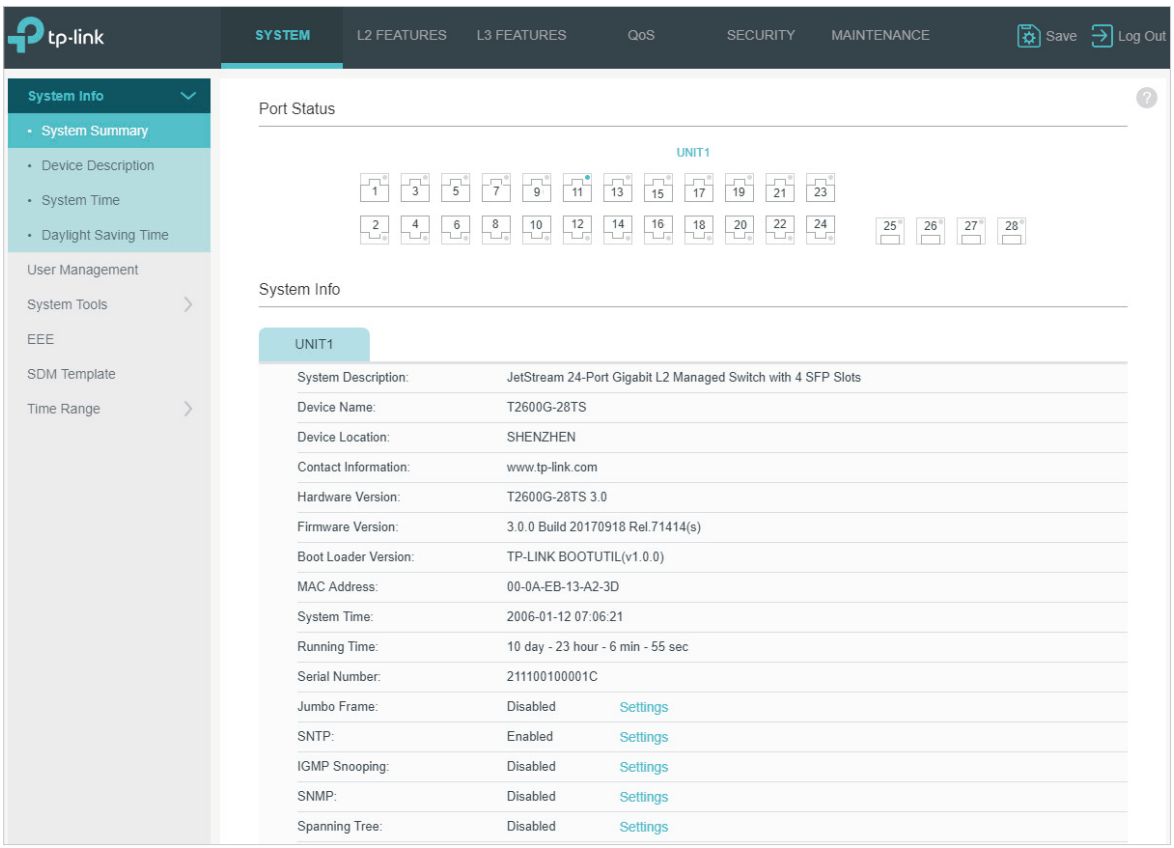


Note:

The first time you log in, change the password to better protect your network and devices.

5) The typical web interface displays below. You can view the switch's running status and configure the switch on this interface.

Figure 2-3 Web Interface



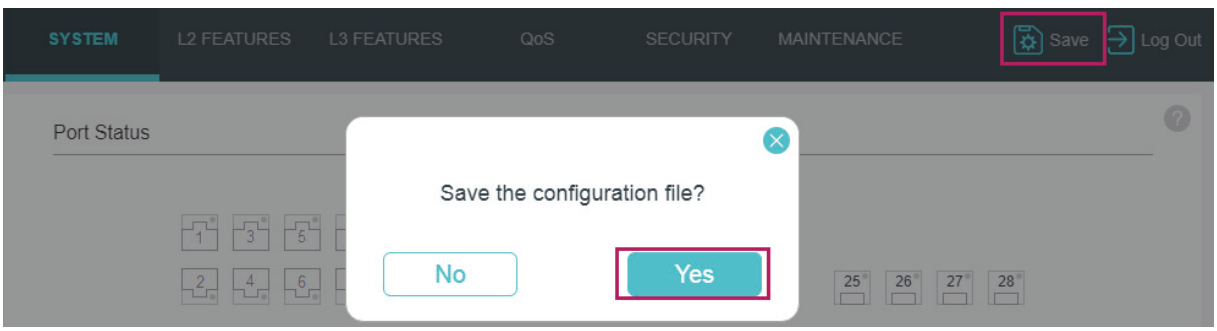
2.2 Save the Configuration File

The switch's configuration files fall into two types: the running configuration file and the start-up configuration file.

After you perform configurations on the sub-interfaces and click **Apply**, the modifications will be saved in the running configuration file. The configurations will be lost when the switch reboots.

If you need to keep the configurations after the switch reboots, please click Save on the main interface to save the configurations in the start-up configuration file.

Figure 2-4 Save the Configuration

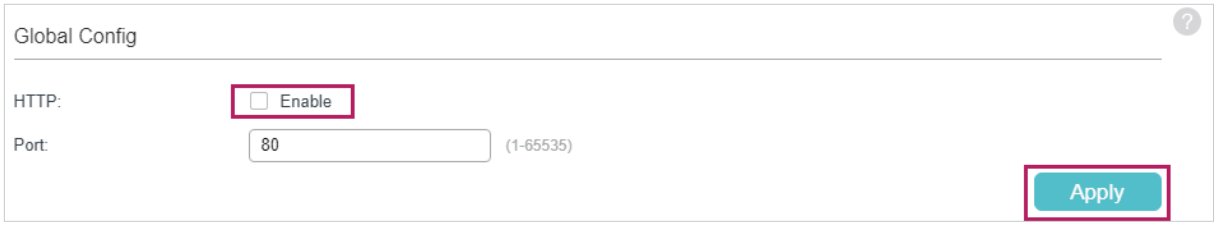


2.3 Disable the Web Server

You can shut down the HTTP server and HTTPS server to block any access to the web interface.

Go to **SECURITY > Access Security > HTTP Config**, disable the HTTP server and click **Apply**.

Figure 2-5 Shut Down HTTP Server



Go to **SECURITY > Access Security > HTTPS Config**, disable the HTTPS server and click **Apply**.

Figure 2-6 Disbale the HTTPS Server

2.4 Configure the Switch's IP Address and Default Gateway

If you want to access the switch via a specified port (hereafter referred to as the access port), you can configure the port as a routed port and specify its IP address, or configure the IP address of the VLAN which the access port belongs to.

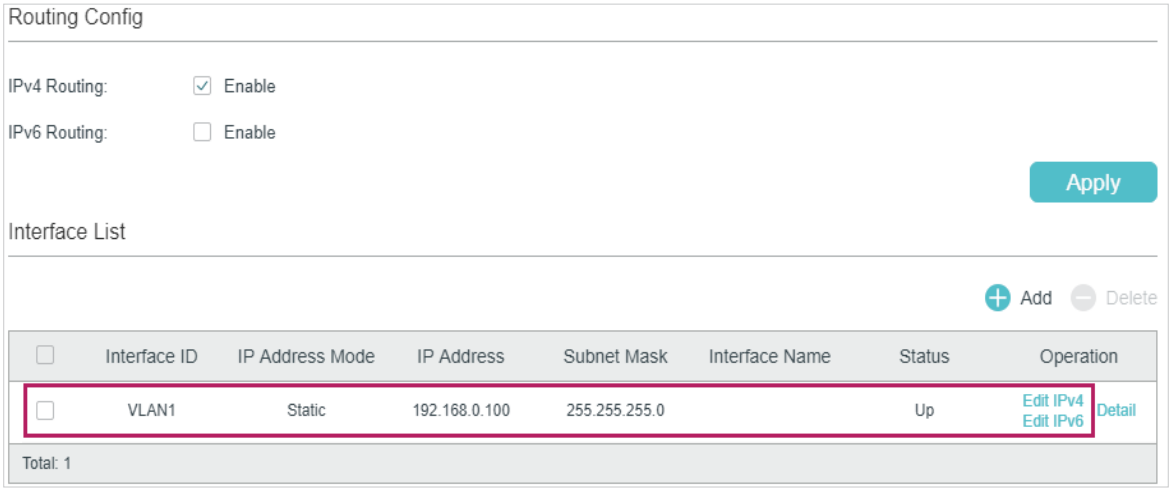
- Change the IP Address

By default, all the ports belong to VLAN 1 with the VLAN interface IP 192.168.0.1.

The following example shows how to change the switch's default access IP address 192.168.0.1.

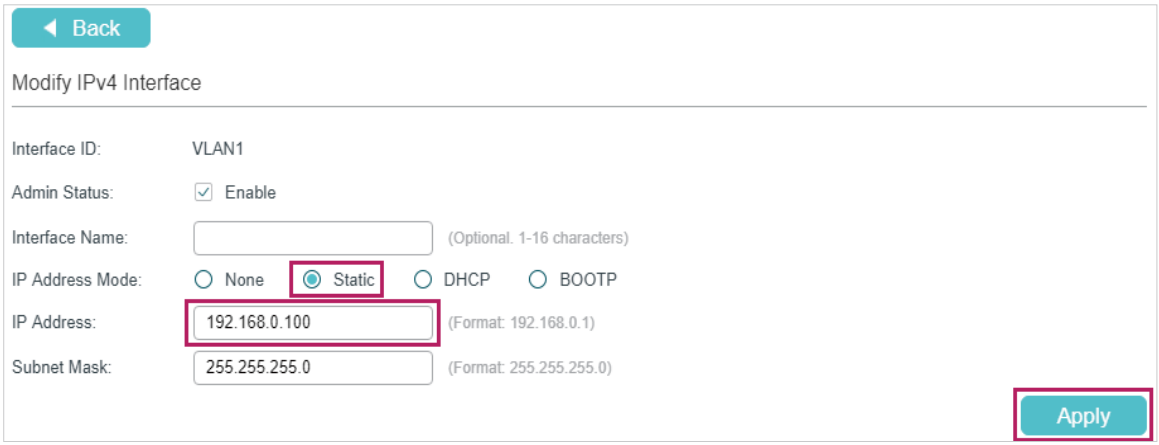
1) Go to **L3 FEATURES > Interface**. The default access IP address in VLAN 1 in the Interface List. Click **Edit IPv4** to modify VLAN1's IP address.

Figure 2-7 Change VLAN1's IP Address



2) Choose the **IP Address Mode** as **Static**. Enter the new access address in the **IP Address** field and click **Apply**. Make sure that the route between the host PC and the switch's new IP address is available.

Figure 2-8 Specify the IP Address



3) Enter the new IP address in the web browser to access the switch.

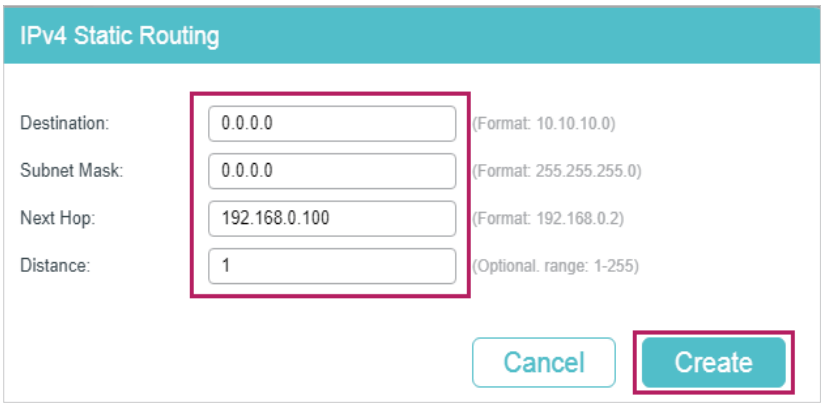
4) Click Save to save the settings.

■ Configure the Default Gateway

The following example shows how to configure the switch's gateway. By default, the switch has no default gateway.

1) Go to page **L3 FEATURES > Static Routing > IPv4 Static Routing Config**. Click Add to load the following page and configure the parameters related to the switch's gateway. Then click **Create**.

Figure 2-9 Configure the Default Gateway

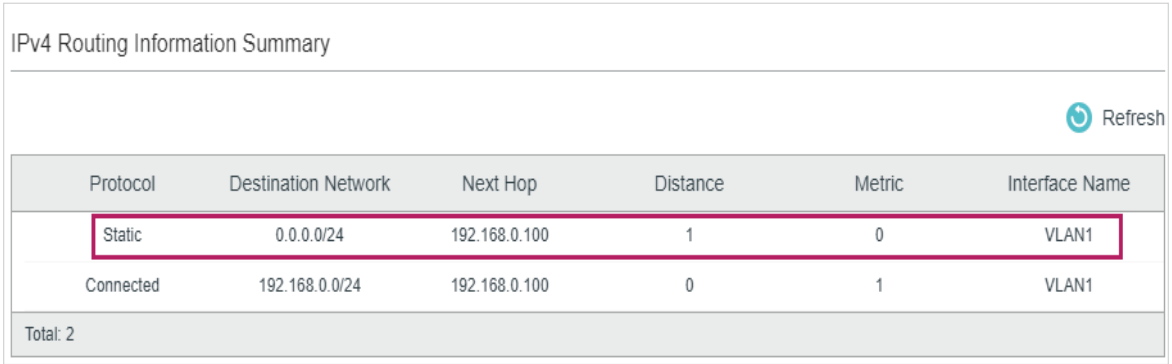


Destination	Specify the destination as 0.0.0.0.
Subnet Mask	Specify the subnet mask as 0.0.0.0.
Next Hop	Configure your desired default gateway as the next hop's IP address.
Distance	Specify the distance as 1.

2) Click Save to save the settings.

3) Check the routing table to verify the default gateway you configured. The entry marked in red box displays the valid default gateway.

Figure 2-10 View the Default Gateway



3 Command Line Interface Access

Users can access the switch's command line interface through the console (only for switch with console port), Telnet or SSH connection, and manage the switch with the command lines.

Console connection requires the host PC connecting to the switch's console port directly, while Telnet and SSH connection support both local and remote access.

The following table shows the typical applications used in the CLI access.

Table 3-1 Method list

Method	Using Port	Typical Applications
Console	Console port (connected directly)	Hyper Terminal
Telnet	RJ-45 port	CMD
SSH	RJ-45 port	Putty

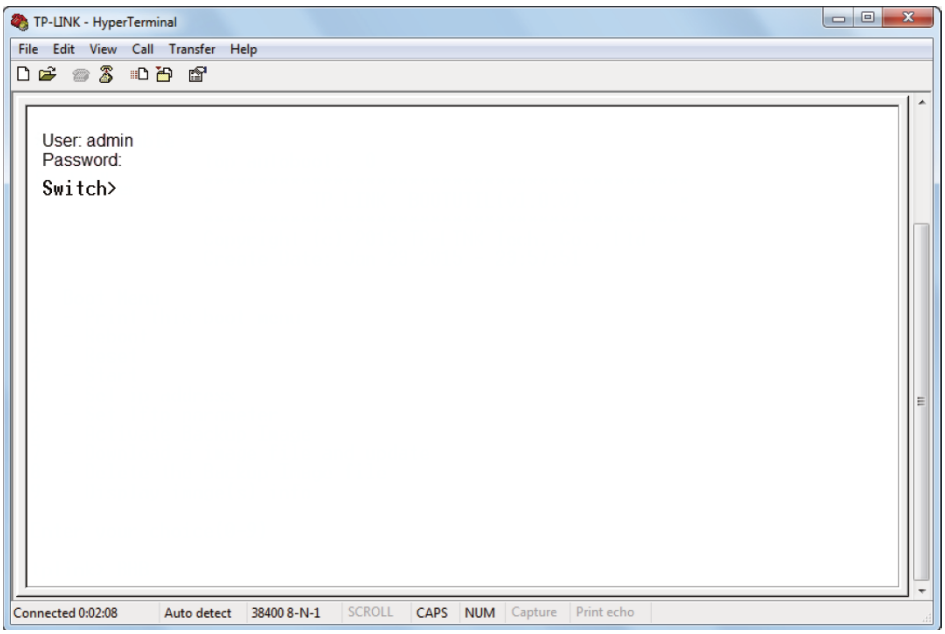
3.1 Console Login (only for switch with console port)

Follow these steps to log in to the switch via the Console port:

1) Connect the PC or terminal to the Console port on the switch with the serial cable.
2) Start the terminal emulation program (such as the Hyper Terminal) on the PC and configure the terminal emulation program as follows:
   - Baud Rate: 38400bps
   - Data Bits: 8
   - Parity: None
   - Stop Bits: 1
   - Flow Control: None
3) Type the User name and Password in the Hyper Terminal window. The default value for both of them is **admin**. Press **Enter** in the main window and **Switch>** will appear, which

indicates that you have successfully logged in to the switch and you can use the CLI now.

Figure 3-1 CLI Main Window

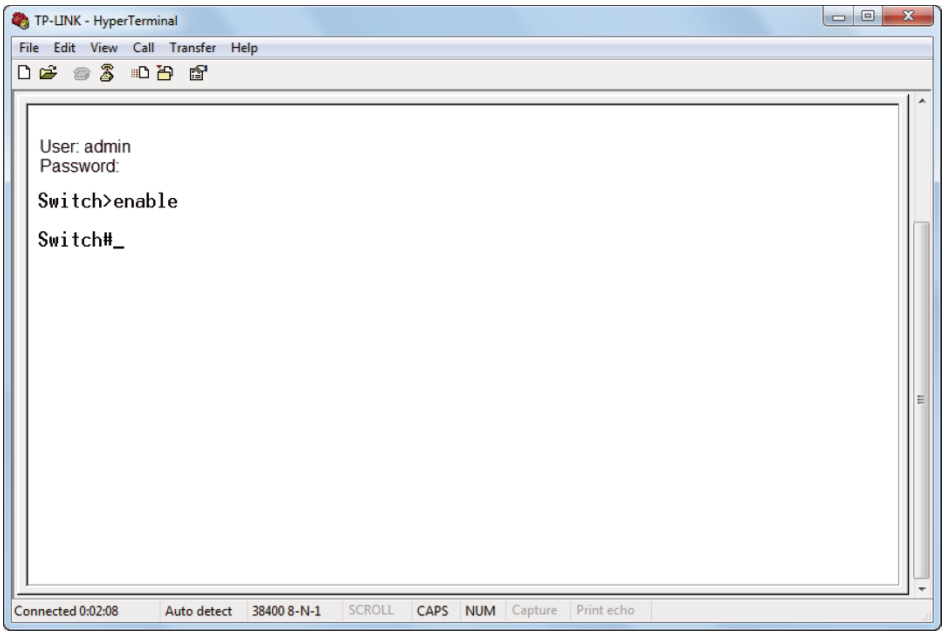


Note:

The first time you log in, change the password to better protect your network and devices.

4) Enter **enable** to enter the User EXEC Mode to further configure the switch.

Figure 3-2 User EXEC Mode



Note:

In Windows XP, go to **Start > All Programs > Accessories > Communications > Hyper Terminal** to open the Hyper Terminal and configure the above settings to log in to the switch.

3.2 Telnet Login

The switch supports Login Local Mode for authentication by default.

Login Local Mode: Username and password are required, which are both admin by default.

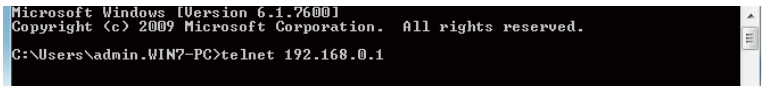
The following steps show how to manage the switch via the Login Local Mode:

1) Make sure the switch and the PC are in the same LAN (Local Area Network). Click **Start** and type in **cmd** in the Search bar and press **Enter**.

Figure 3-3 Open the CMD Window

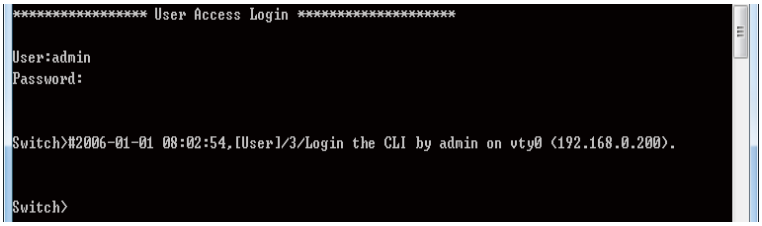
2) Type in **telnet 192.168.0.1** in the CMD window and press **Enter**.

Figure 3-4 Log In to the Switch



3) Type in the login username and password (both **admin** by default). Press **Enter** and you will enter User EXEC Mode.

Figure 3-5 Enter User EXEC Mode

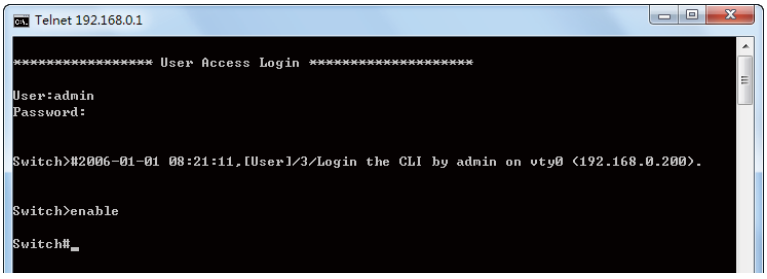


Note:

The first time you log in, change the password to better protect your network and devices.

4) Type in **enable** command and you will enter Privileged EXEC Mode. By default no password is needed. Later you can set a password for users who want to access the Privileged EXEC Mode.

Figure 3-6 Enter Privileged EXEC Mode



Now you can manage your switch with CLI commands through Telnet connection.

3.3 SSH Login

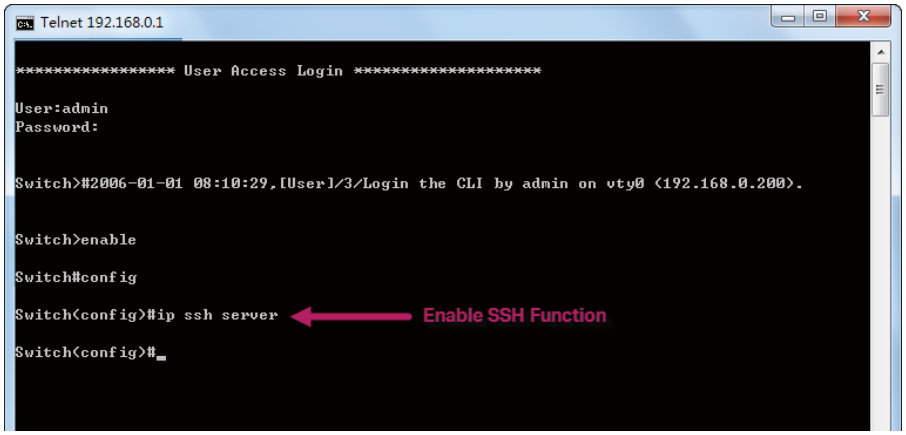
SSH login supports the following two modes: Password Authentication Mode and Key Authentication Mode. You can choose one according to your needs:

- Password Authentication Mode: Username and password are required, which are both **admin** by default.

- Key Authentication Mode (Recommended): A public key for the switch and a private key for the client software (PuTTY) are required. You can generate the public key and the private key through the PuTTY Key Generator.

Before logging in via SSH, follow the steps below to enable SSH on the terminal emulation program:

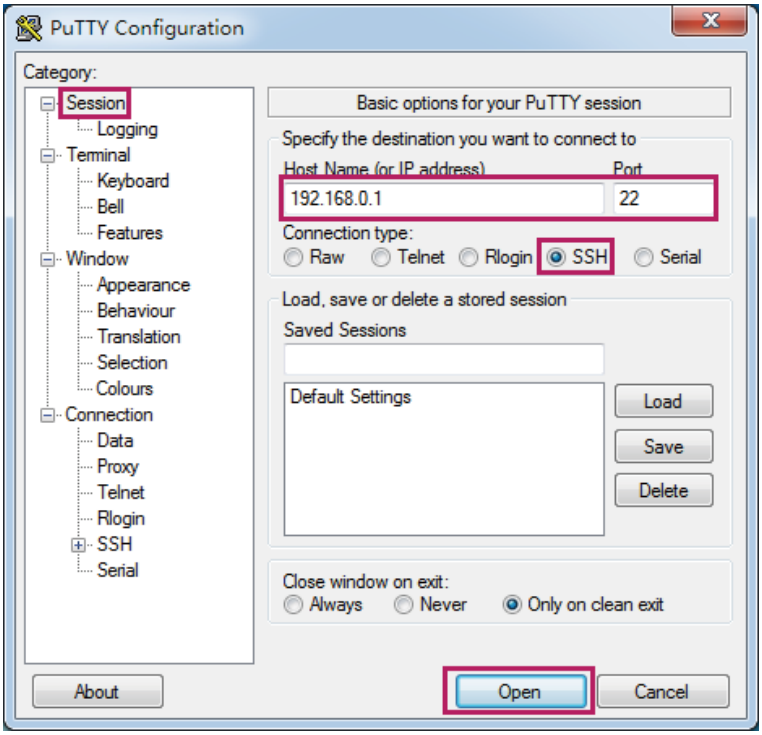
Figure 3-7 Enable SSH



Password Authentication Mode

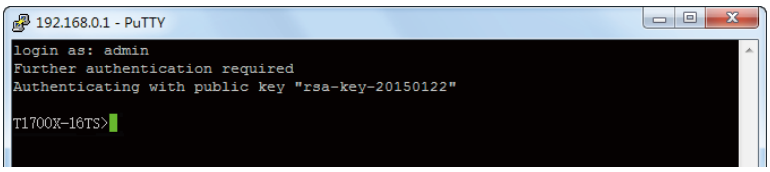
1) Open PuTTY and go to the Session page. Enter the IP address of the switch in the **Host Name** field and keep the default value 22 in the **Port** field; select **SSH** as the Connection type. Click **Open**.

Figure 3-8 Configurations in PuTTY



2) Enter the login username and password to log in to the switch, and you can continue to configure the switch.

Figure 3-9 Log In to the Switch



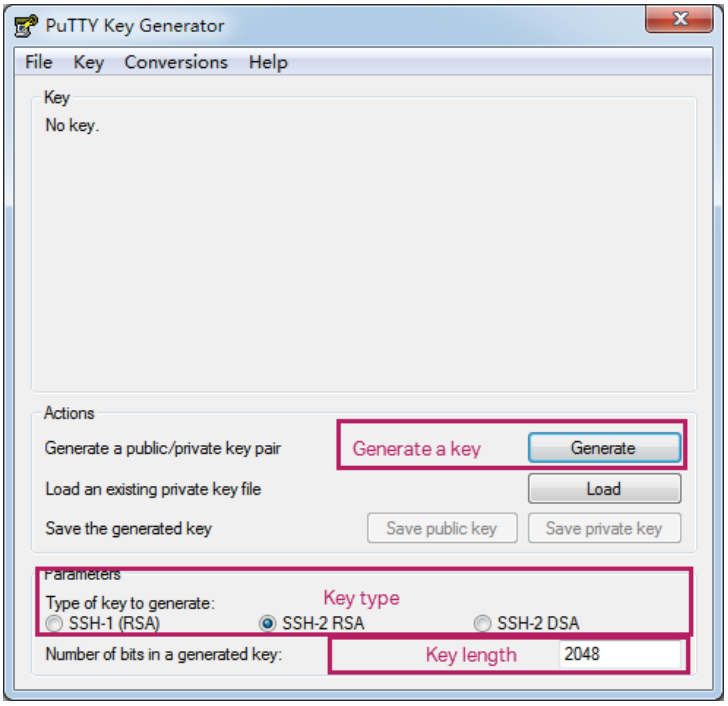
Note:

The first time you log in, change the password to better protect your network and devices.

Key Authentication Mode

1) Open the PuTTY Key Generator. In the Parameters section, select the key type and enter the key length. In the **Actions** section, click **Generate** to generate a public/private key pair. In the following figure, an SSH-2 RSA key pair is generated, and the length of each key is 1024 bits.

Figure 3-10 Generate a Public/Private Key Pair

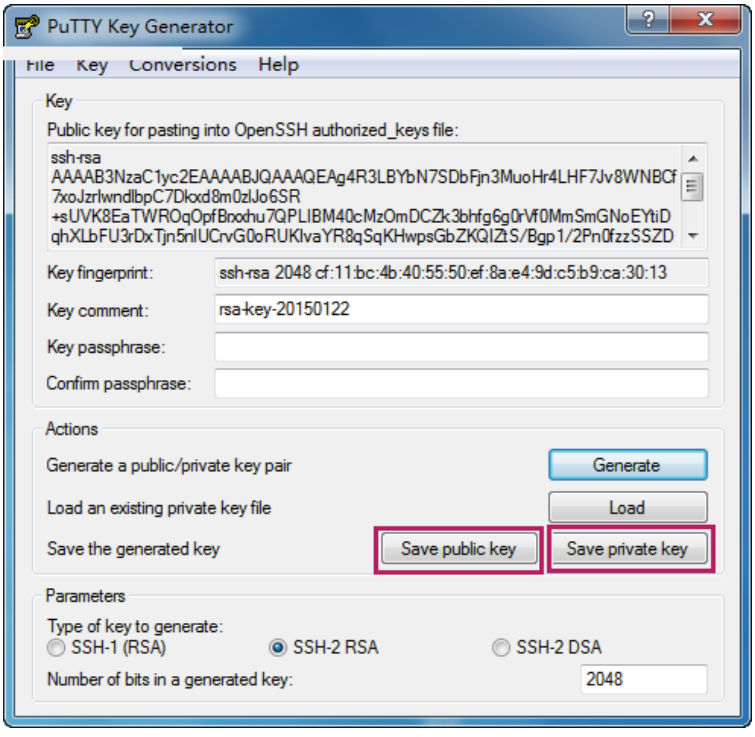


Note:

- The key length should be between 512 and 3072 bits.
- You can accelerate the key generation process by moving the mouse quickly and randomly in the Key section.

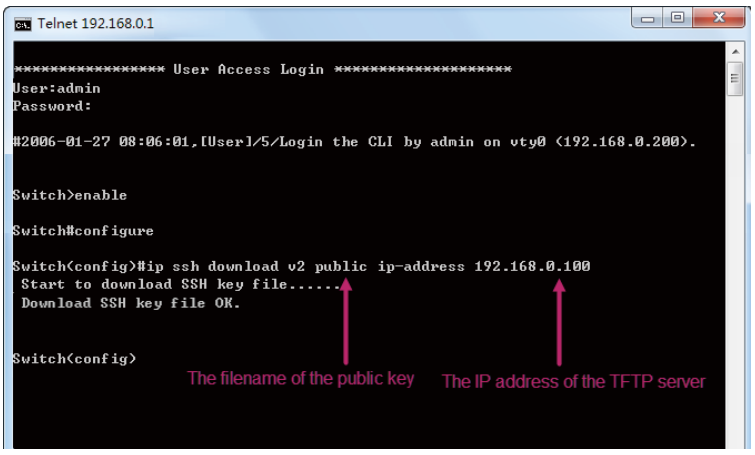
2) After the keys are successfully generated, click **Save public key** to save the public key to a TFTP server; click **Save private key** to save the private key to the host PC.

Figure 3-11 Save the Generated Keys



3) On Hyper Terminal, download the public key file from the TFTP server to the switch as shown in the following figure:

Figure 3-12 Download the Public Key to the Switch

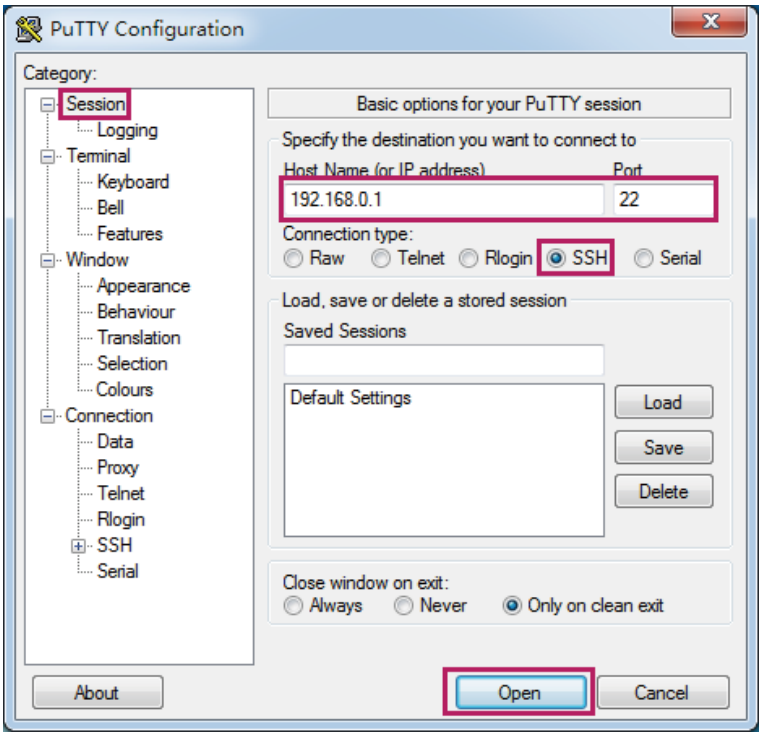


Note:

- The key type should accord with the type of the key file. In the above CLI, v1 corresponds to SSH-1 (RSA), and v2 corresponds to SSH-2 RSA and SSH-2 DSA.
- The key downloading process cannot be interrupted.

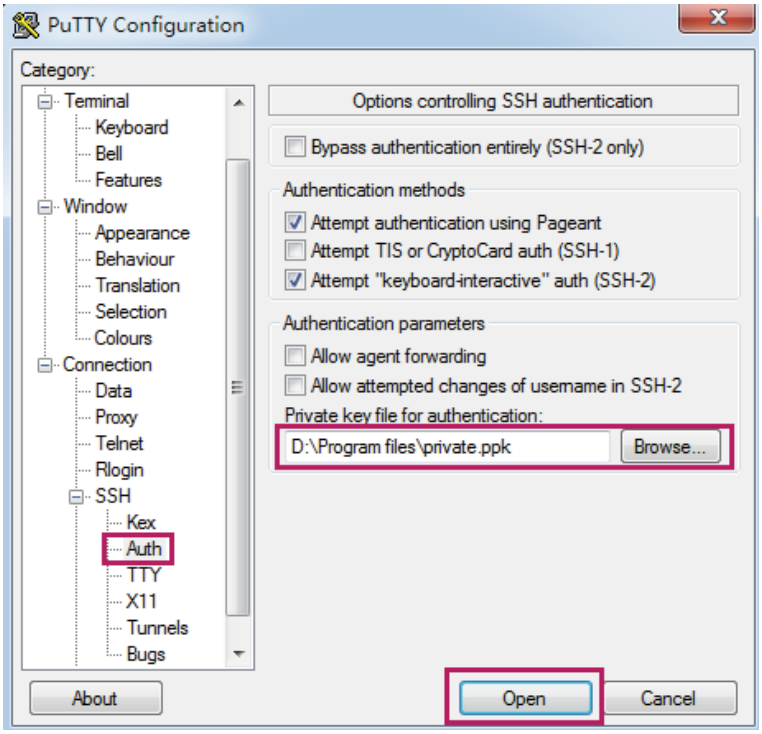
4) After the public key is downloaded, open PuTTY and go to the **Session** page. Enter the IP address of the switch and select **SSH** as the Connection type (keep the default value in the Port field).

Figure 3-13 Configure the Host Name and Connection Type



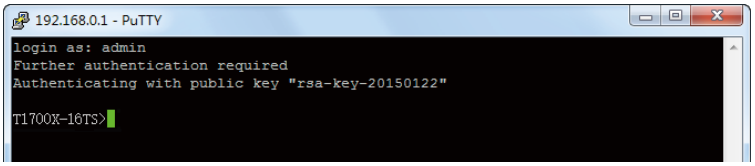
5) Go to **Connection > SSH > Auth**. Click **Browse** to download the private key file to PuTTY. Click **Open** to start the connection and negotiation.

Figure 3-14 Download the Private Key to PuTTY



6) After negotiation is completed, enter the username to log in. If you can log in without entering the password, the key authentication completed successfully.

Figure 3-15 Log In to the Switch



Note:

The first time you log in, change the password to better protect your network and devices.

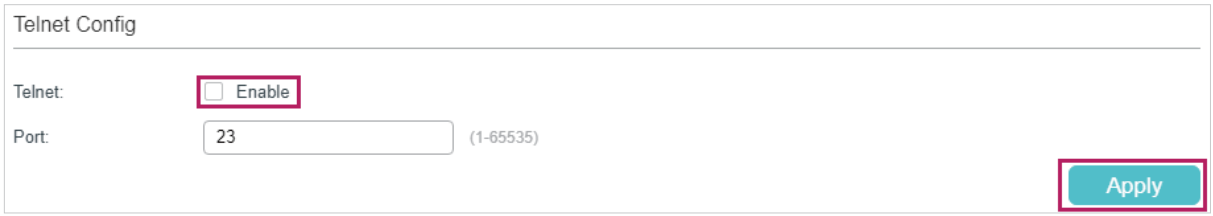
3.4 Disable Telnet login

You can shut down the Telnet function to block any Telnet access to the CLI interface.

- Using the GUI:

Go to **SECURITY > Access Security > Telnet Config, disable the Telnet function and click Apply.**

Figure 3-16 Disable Telnet login



- Using the CLI:

Switch#configure

Switch(config)#telnet disable

3.5 Disable SSH login

You can shut down the SSH server to block any SSH access to the CLI interface.

- Using the GUI:

Go to **SECURITY > Access Security > SSH Config, disable the SSH server and click Apply.**

Figure 3-17 Shut down SSH server

- Using the CLI:

Switch#configure

Switch(config)#no ip ssh server

3.6 Copy running-config startup-config

The switch's configuration files fall into two types: the running configuration file and the start-up configuration file.

After you enter each command line, the modifications will be saved in the running configuration file. The configurations will be lost when the switch reboots.

If you need to keep the configurations after the switch reboots, please user the command **copy running-config startup-config** to save the configurations in the start-up configuration file.

Switch(config)#end

Switch#copy running-config startup-config

3.7 Change the Switch's IP Address and Default Gateway

If you want to access the switch via a specified port (hereafter referred to as the access port), you can configure the port as a routed port and specify its IP address, or configure the IP address of the VLAN which the access port belongs to.

- Change the IP Address

By default, all the ports belong to VLAN 1 with the VLAN interface IP 192.168.0.1/24. In the following example, we will show how to replace the switch's default access IP address 192.168.0.1/24 with 192.168.0.10/24.

Switch#configure

Switch(config)#interface vlan 1

Switch(config-if)#ip address 192.168.0.10 255.255.255.0

The connection will be interrupted and you should telnet to the switch's new IP address 192.168.0.10.

C:\Users\Administrator>telnet 192.168.0.10

User:admin

Password:tplink

Switch>enable

Switch#copy running-config startup-config

- Configure the Default Gateway

In the following example, we will show how to configure the switch's gateway as 192.168.0.100. By default, the switch has no default gateway.

Switch#configure

Switch(config)#ip route 0.0.0.0 0.0.0.0 192.168.0.100 1

Switch(config)#end

Switch#copy running-config startup-config