Configuring Access Security

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 Access Security

1.1 Overview

Access Security provides different security measures for accessing the switch remotely so as to enhance the configuration management security.

1.2 Supported Features

Access Control

This function is used to control the users' access to the switch based on IP address, MAC address or port.

HTTP

This function is based on the HTTP protocol. It can allow or deny users to access the switch via a web browser.

HTTPS

This function is based on the SSL or TLS protocol working in transport layer. It supports a security access via a web browser.

SSH

This function is based on the SSH protocol, a security protocol established on application and transport layers. The function with SSH is similar to a telnet connection, but SSH can provide information security and powerful authentication.

Telnet

This function is based on the Telnet protocol subjected to TCP/IP protocol. Through Telnet, users can log on to the switch remotely.

Serial Port

You can configure the serial port parameters. Only T2600G series switches support Serial Port.

2 Access Security Configurations

With access security configurations, you can:

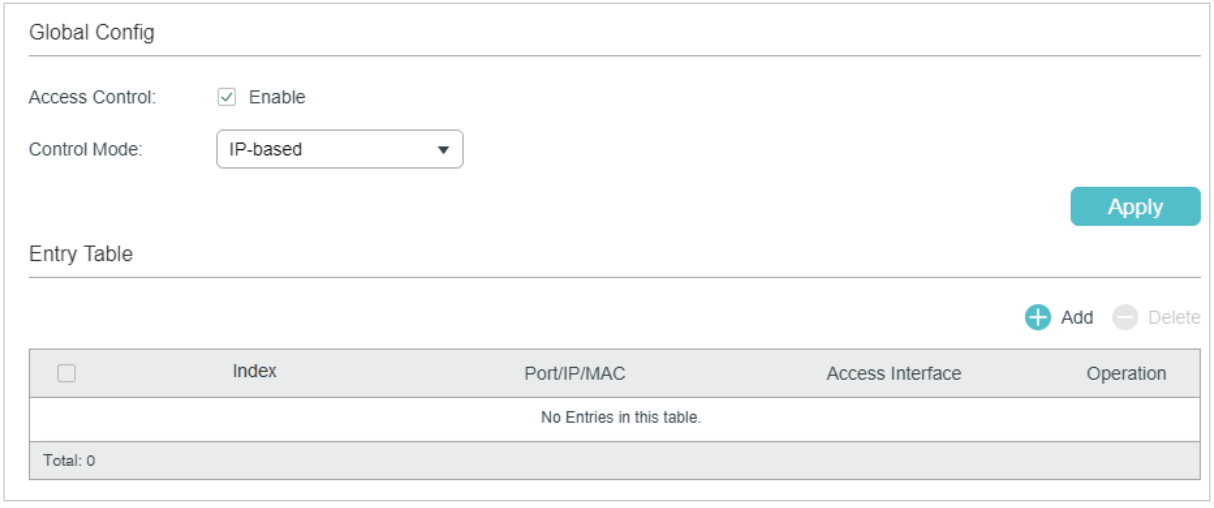
- Configure the Access Control feature
- Configure the HTTP feature
- Configure the HTTPS feature
- Configure the SSH feature
- Configure the Telnet function
- Configure the Serial Port parameters

2.1 Using the GUI

2.1.1 Configuring the Access Control Feature

Choose the menu **SECURITY** > **Access Security** > **Access Control** to load the following page.

Figure 2-1 Configuring the Access Control



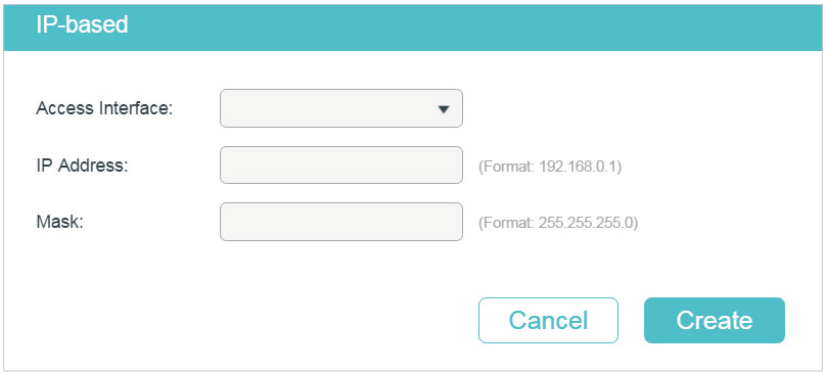
1) In the **Global Config** section, enable Access Control, select one control mode and click **Apply**.

Control Mode	Select the control mode for users to log in to the web management page. **IP-based**: Only the users within the IP-range you set here are allowed to access the switch. **MAC-based**: Only the users with the MAC address you set here are allowed to access the switch. **Port-based**: Only the users connecting to the ports you set here are allowed to access the switch.

2) In the **Entry Table** section, click Add to add an Access Control entry.

When the **IP-based** mode is selected, the following window will pop up.

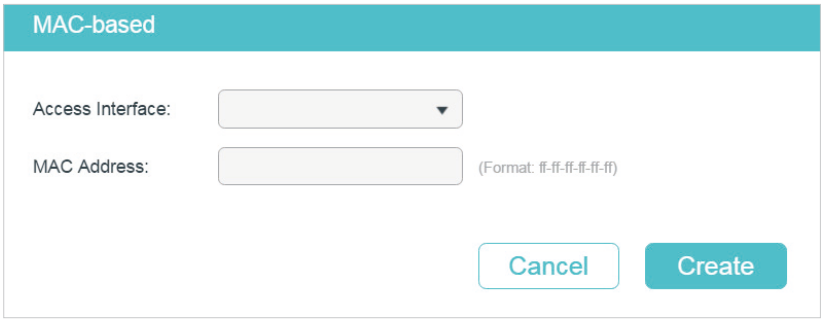
Figure 2-2 Configuring Access Control Entry-IP Based



Access Interface	Select the interface to control the methods for users' accessing. **SNMP**: A function to manage the network devices via NMS. **Telnet**: A connection type for users to remote login. **SSH**: A connection type based on SSH protocol. **HTTP**: A connection type based on HTTP protocol. **HTTPS**: A connection type based on SSL protocol. **Ping**: A communication protocol to test the connection of the network.
IP Address/ Mask	Enter the IP address and mask to specify an IP range. Only the users within this IP range can access the switch.

When the **MAC-based** mode is selected, the following window will pop up.

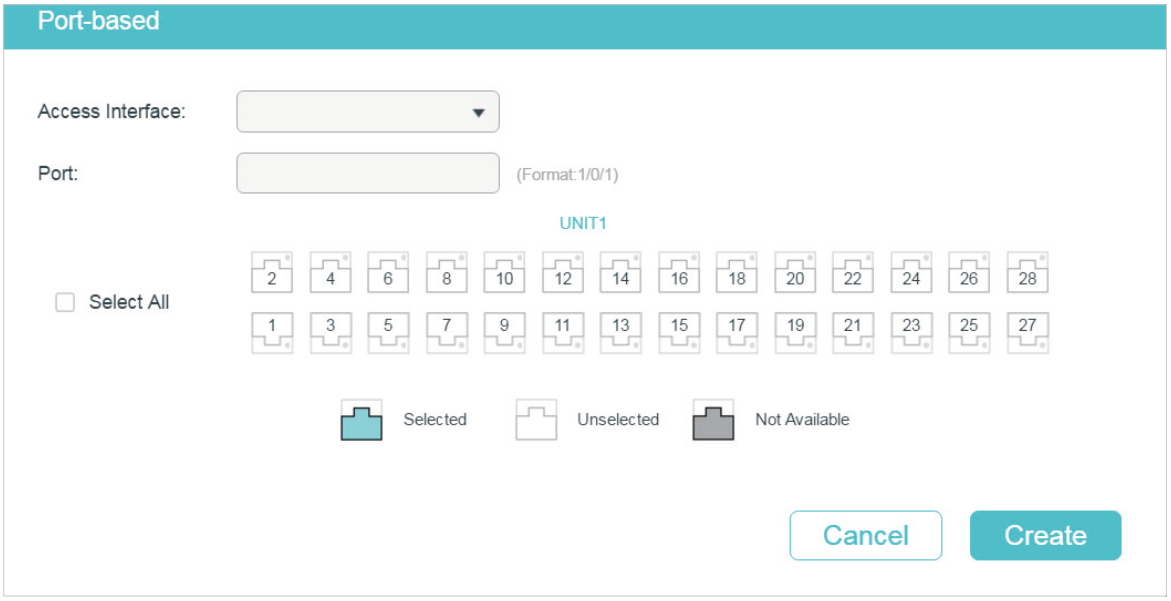
Figure 2-3 Configuring Access Control Entry-MAC Based



Access Interface	Select the interface to control the methods for users' accessing. **SNMP**: A function to manage the network devices via NMS. **Telnet**: A connection type for users to remote login. **SSH**: A connection type based on SSH protocol. **HTTP**: A connection type based on HTTP protocol. **HTTPS**: A connection type based on SSL protocol. **Ping**: A communication protocol to test the connection of the network.
MAC Address	Specify the MAC address. Only the users with the correct MAC address can access the switch.

When the **Port-based** mode is selected, the following window will pop up.

Figure 2-4 Configuring Access Control Entry-Port Based



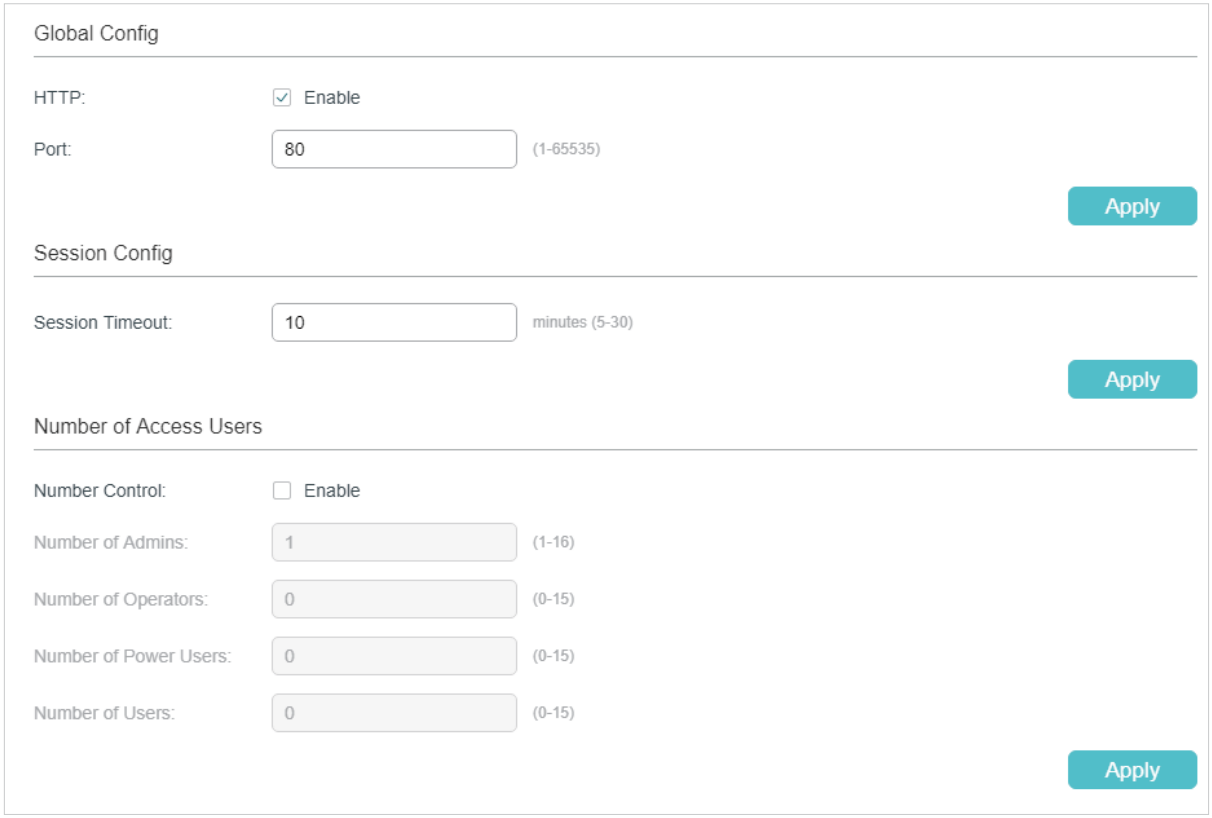
Access Interface	Select the interface to control the methods for users' accessing. **SNMP**: A function to manage the network devices via NMS. **Telnet**: A connection type for users to remote login. **SSH**: A connection type based on SSH protocol. **HTTP**: A connection type based on HTTP protocol. **HTTPS**: A connection type based on SSL protocol. **Ping**: A communication protocol to test the connection of the network.
Port	Select one or more ports to configure. Only the users connected to these ports are allowed to access the switch.

3) Click **Create**. Then you can view the created entries in the **Entry Table**.

2.1.2 Configuring the HTTP Function

Choose the menu **SECURITY** > **Access Security** > **HTTP Config** to load the following page.

Figure 2-5 Configuring the HTTP Function



1) In the **Global Control** section, enable HTTP function, specify the port using for HTTP, and click **Apply** to enable the HTTP function.

HTTP	HTTP function is based on the HTTP protocol. It allows users to manage the switch through a web browser.

Port	Specify the port number for HTTP service.

2) In the **Session Config** section, specify the Session Timeout and click **Apply**.

Session Timeout	The system will log out automatically if users do nothing within the Session Timeout time.

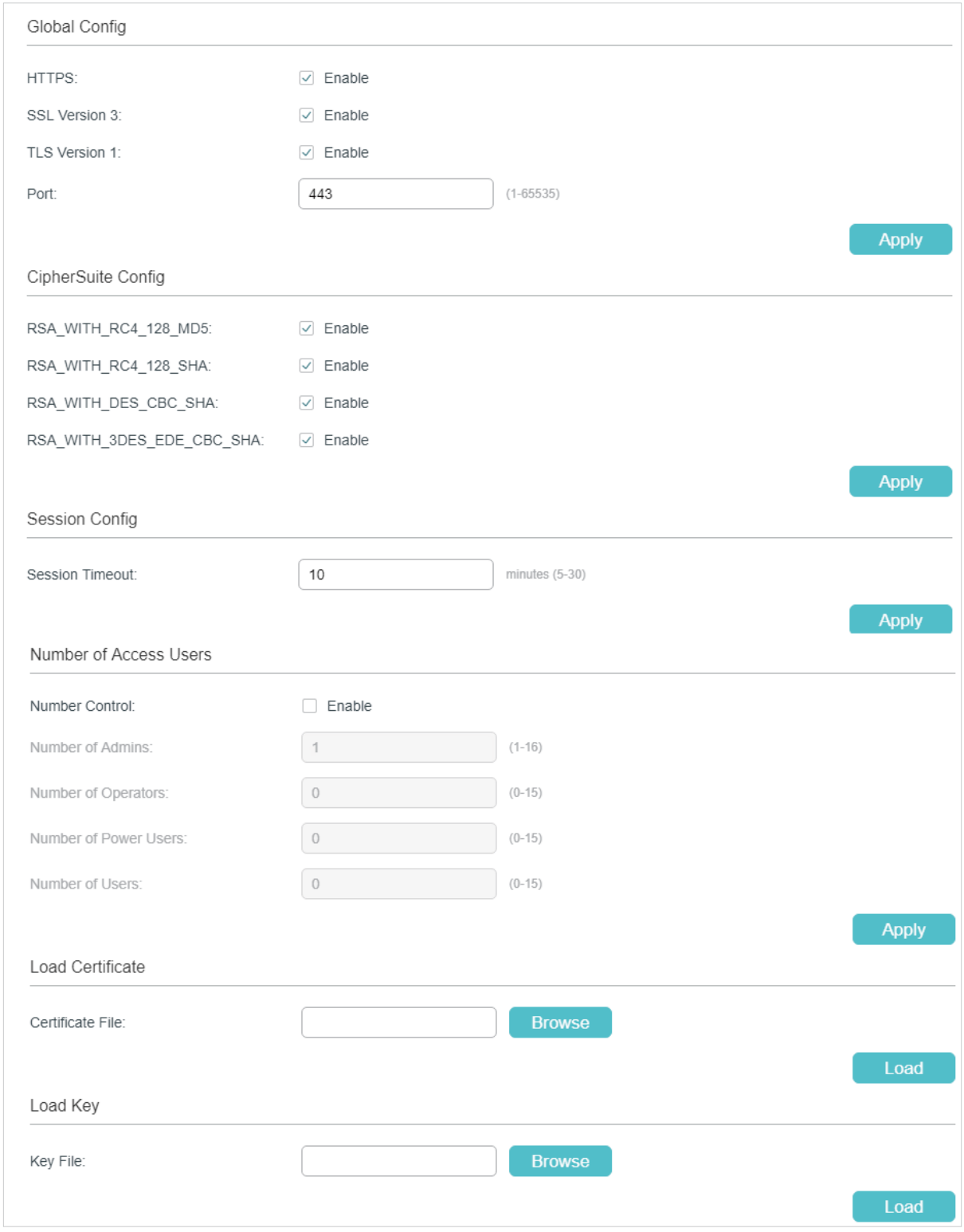
3) In the **Number of Access Users** section, enable Number Control function, specify the following parameters and click **Apply**.

Number Control	Enable or disable Number Control. With this option enabled, you can control the number of the users logging on to the web management page at the same time. The total number of users should be no more than 16.
Number of Admins	Specify the maximum number of users whose access level is Admin.
Number of Operators	Specify the maximum number of users whose access level is Operator.
Number of Power Users	Specify the maximum number of users whose access level is Power User.
Number of Users	Specify the maximum number of users whose access level is User.

2.1.3 Configuring the HTTPS Function

Choose the menu **SECURITY** > **Access Security** > **HTTPS Config** to load the following page.

Figure 2-6 Configuring the HTTPS Function



1) In the **Global Config** section, enable HTTPS function, select the protocol the switch supports and specify the port using for HTTPS. Click **Apply**.

HTTPS	Enable or disable the HTTPS function. HTTPS function is based on the SSL or TLS protocol. It provides a secure connection between the client and the switch.
SSL Version 3	Enable or disable SSL Version 3 protocolon the switch. SSL is a transport protocol. It can provide server authentication, encryption and message integrity to allow secure HTTP connection.
TLS Version 1	Enable or disable TLS Version 1 protocol on the switch. TLS is a transport protocol upgraded from SSL. It supports a different encryption algorithm from SSL, so TLS and SSL are not compatible. TLS can support a more secure connection.

2) In the **CipherSuite Config** section, select the algorithm to be enabled and click **Apply**.

RSA_WITH_ RC4_128_MD5	Key exchange with RC4 128-bit encryption and MD5 for message digest.
RSA_WITH_ RC4_128_SHA	Key exchange with RC4 128-bit encryption and SHA for message digest.
RSA_WITH_ DES_CBC_SHA	Key exchange with DES-CBC for message encryption and SHA for message digest.
RSA_ WITH_3DES_ EDE_CBC_SHA	Key exchange with 3DES and DES-EDE3-CBC for message encryption and SHA for message digest.

3) In the **Session Config** section, specify the Session Timeout and click **Apply**.

Session Timeout	The system will log out automatically if users do nothing within the Session Timeout time.

4) In the **Number of Access Users** section, enable Number Control function, specify the following parameters and click **Apply**.

Number Control	Enable or disable Number Control. With this option enabled, you can control the number of the users logging on to the web management page at the same time. The total number of users should be no more than 16.
Number of Admins	Specify the maximum number of users whose access level is Admin.
Number of Operators	Specify the maximum number of users whose access level is Operator.
Number of Power Users	Specify the maximum number of users whose access level is Power User.

Number of Users	Specify the maximum number of users whose access level is User.

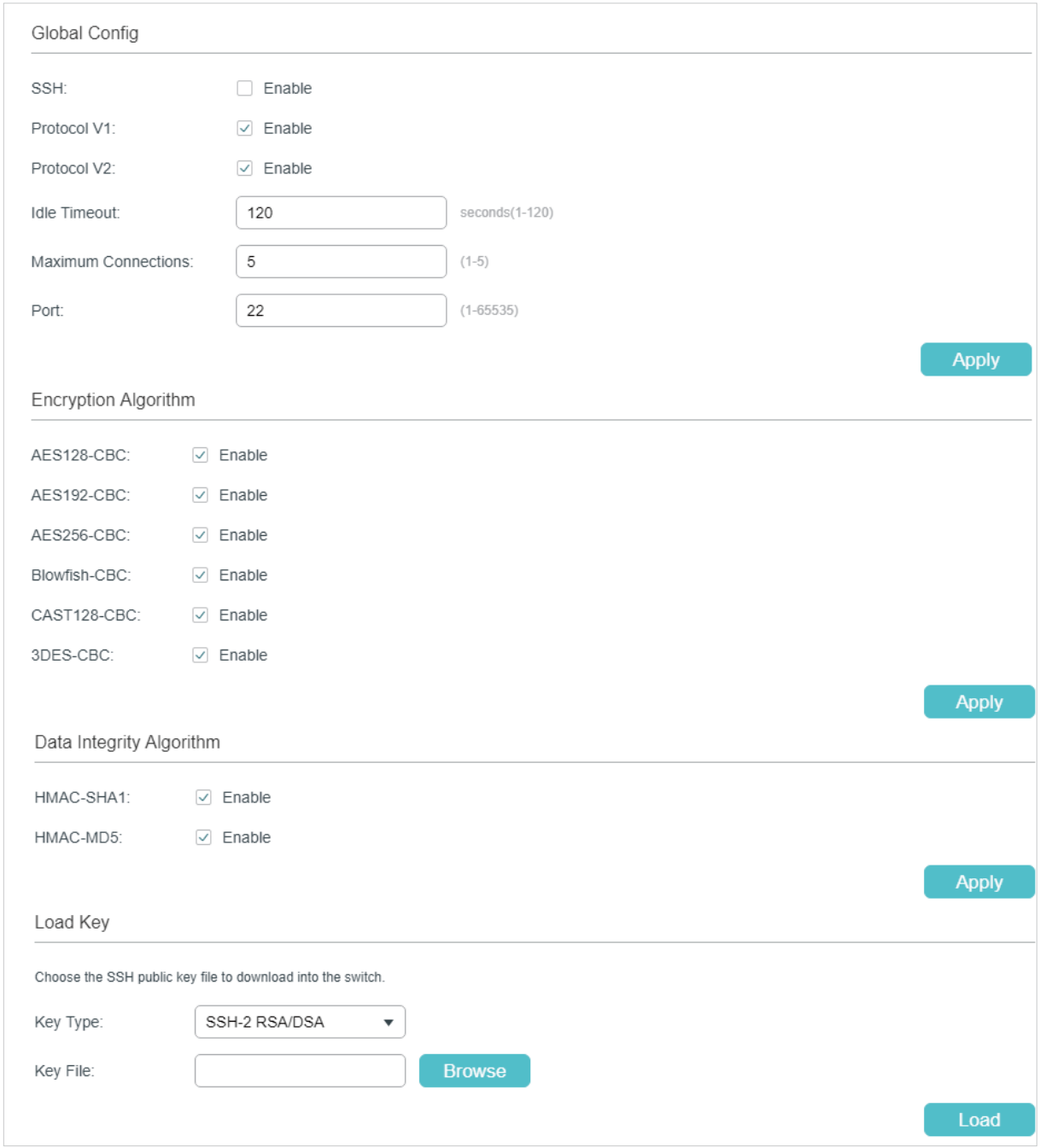
5) In the **Load Certificate** and **Load Key** section, download the certificate and key.

Certificate File	Select the desired certificate to download to the switch. The certificate must be BASE64 encoded. The SSL certificate and key downloaded must match each other, otherwise the HTTPS connection will not work.
Key File	Select the desired Key to download to the switch. The key must be BASE64 encoded. The SSL certificate and key downloaded must match each other, otherwise the HTTPS connection will not work.

2.1.4 Configuring the SSH Feature

Choose the menu **SECURITY** > **Access Security** > **SSH Config** to load the following page.

Figure 2-7 Configuring the SSH Feature



1) In the **Global Config** section, select **Enable** to enable SSH function and specify following parameters.

SSH	Select **Enable** to enable the SSH function. SSH is a protocol working in application layer and transport layer. It can provide a secure, remote connection to a device. It is more secure than Telnet protocol as it provides strong encryption.

Protocol V1	Select **Enable** to enable SSH version 1.
Protocol V2	Select **Enable** to enable SSH version 2.
Idle Timeout	Specify the idle timeout time. The system will automatically release the connection when the time is up.
Maximum Connections	Specify the maximum number of the connections to the SSH server. New connection will not be established when the number of the connections reaches the maximum number you set.
Port	Specify the port using for SSH.

2) In the **Encryption Algorithm** section, enable the encryption algorithm you want the switch to support and click **Apply**.

3) In **Data Integrity Algorithm** section, enable the integrity algorithm you want the switch to support and click **Apply**.

4) In **Import Key File** section, select key type from the drop-down list and click **Browse** to download the desired key file.

Key Type	Select the key type. The algorithm of the corresponding type is used for both key generation and authentication.
Key File	Select the desired public key to download to the switch. The key length of the downloaded file ranges of 512 to 3072 bits.

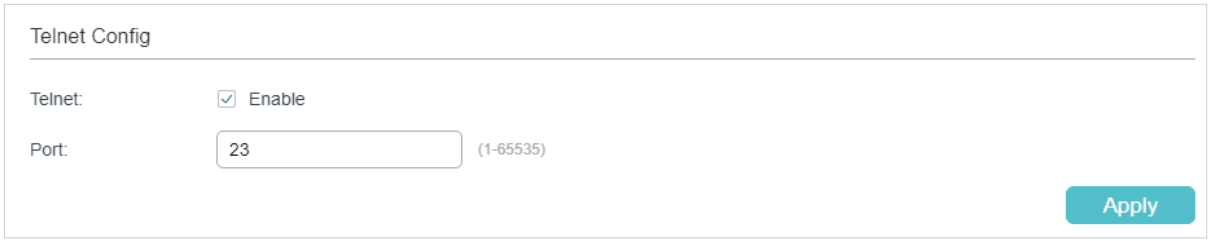
Note:

It will take a long time to download the key file. Please wait without any operation.

2.1.5 Configuring the Telnet Function

Choose the menu **SECURITY** > **Access Security** > **Telnet Config** to load the following page.

Figure 2-8 Configuring the Telnet Function



Enable Telnet and click **Apply**.

Telnet	Select **Enable** to make the Telnet function effective. Telnet function is based on the Telnet protocol subjected to TCP/IP protocol. It allows users to log on to the switch remotely.
Port	Specify the port using for Telnet.

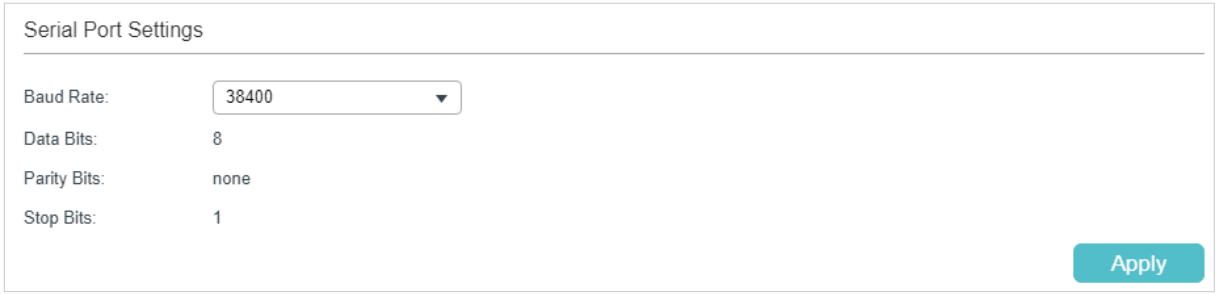
2.1.6 Configuring the Serial Port Parameters

Note:

Only T2600G series switches support Serial Port.

Choose the menu **SECURITY** > **Access Security** > **Serial Port Config** to load the following page.

Figure 2-9 Configuring the Serial Port Parameters



Configure the Baud Rate and click **Apply**.

Baud Rate	Configure the baud rate of the console connection. The default value is 38400 bps.
Data Bits	Displays the data bits.
Parity Bits	Displays the parity bits.
Stop Bits	Displays the stop bits.

2.2 Using the CLI

2.2.1 Configuring the Access Control

Follow these steps to configure the access control:

Step 1	**configure** Enter global configuration mode.

Step 2 Use the following command to control the users' access by limiting the IP address:

user access-control ip-based enable

Configure the control mode as IP-based.

user access-control ip-based { *ip-addr ip-mask* **} [** snmp **] [** telnet **] [** ssh **] [** http **] [** https **] [** ping **] [** all **]**

Only the users within the IP-range you set here are allowed to access the switch.

ip-addr: Specify the IP address of the user.

ip-mask: Specify the subnet mask of the user.

[snmp **] [** telnet **] [** ssh **] [** http **] [** https **] [** ping **] [** all **]**: Select to control the types for users' accessing. By default, these types are all enabled.

Use the following command to control the users' access by limiting the MAC address:

user access-control mac-based enable

Configure the control mode as MAC-based.

user access-control mac-based { *mac-addr* **} [** snmp **] [** telnet **] [** ssh **] [** http **] [** https **] [** ping **] [** all **]**

Only the users with the MAC address you set here are allowed to access the switch.

mac-addr: Specify the MAC address of the user.

[snmp **] [** telnet **] [** ssh **] [** http **] [** https **] [** ping **] [** all **]**: Select to control the types for users' accessing. By default, these types are all enabled.

Use the following command to control the users' access by limiting the ports connected to the users:

user access-control port-based enable

Configure the control mode as Port-based.

user access-control port-based interface { fastEthernet *port-list* **| gigabitEthernet** *port-list* **| ten-gigabitEthernet** *port-list* **} [** snmp **] [** telnet **] [** ssh **] [** http **] [** https **] [** ping **] [** all **]**

Only the users connecting to the ports you set here are allowed to access the switch.

port-list: Specify the list of Ethernet port, in the format of 1/0/1-4. You can appoint 5 ports at most.

[snmp **] [** telnet **] [** ssh **] [** http **] [** https **] [** ping **] [** all **]**: Select to control the types for users' accessing. By default, these types are all enabled.

Step 3 **show user configuration**

Verify the security configuration information of the user authentication information and the access interface.

Step 4 **end**

Return to privileged EXEC mode.

Step 5	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to set the type of access control as IP-based. Set the IP address as 192.168.0.100, set the subnet mask as 255.255.255.255 and make the switch support snmp, telnet, http and https.

Switch#configure

Switch(config)#user access-control ip-based enable

Switch(config)#user access-control ip-based 192.168.0.100 255.255.255.255 snmp telnet http https

Switch(config)#show user configuration

User authentication mode: IP based

Index	IP Address	Access Interface
-----	----------	----------
1	192.168.0.100/32	SNMP Telnet HTTP HTTPS

Switch(config)#end

Switch#copy running-config startup-config

2.2.2 Configuring the HTTP Function

Follow these steps to configure the HTTP function:

Step 1	**configure** Enter global configuration mode.
Step 2	**ip http server** Enable the HTTP function. By default, it is enabled.
Step 3	**ip http session timeout** *minutes* Specify the Session Timeout time. The system will log out automatically if users do nothing within the Session Timeout time. *minutes*: Specify the timeout time, which ranges from 5 to 30 minutes. The default value is 10.

Step 4	**ip http max-users** *admin-num operator-num poweruser-num user-num* Specify the maximum number of users that are allowed to connect to the HTTP server. The total number of users should be no more than 16. *admin-num*: Enter the maximum number of users whose access level is Admin. The valid values are from 1 to 16. *operator-num*: Enter the maximum number of users whose access level is Operator. The valid values are from 0 to 15. *poweruser-num*: Enter the maximum number of users whose access level is Power User. The valid values are from 0 to 15. *user-num*: Enter the maximum number of users whose access level is User. The valid values are from 0 to 15.
Step 5	**show ip http configuration** Verify the configuration information of the HTTP server, including status, session timeout, access-control, max-user number and the idle-timeout, etc.
Step 6	**end** Return to privileged EXEC mode.
Step 7	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to set the session timeout as 9, set the maximum admin number as 6, and set the maximum operator number as 2, the maximum power user number as 2, the maximum user number as 2.

Switch#configure

Switch(config)#ip http server

Switch(config)#ip http session timeout 9

Switch(config)#ip http max-user 6 2 2 2

Switch(config)#show ip http configuration

HTTP Status:	Enabled
HTTP Port:	80
HTTP Session Timeout:	9
HTTP User Limitation:	Enabled
HTTP Max Users as Admin:	6
HTTP Max Users as Operator:	2
HTTP Max Users as Power User:	2
HTTP Max Users as User:	2

Switch(config)#end

Switch#copy running-config startup-config

2.2.3 Configuring the HTTPS Function

Follow these steps to configure the HTTPS function:

Step 1	**configure** Enter global configuration mode.
Step 2	**ip http secure-server** Enable the HTTPS function. By default, it is enabled.
Step 3	**ip http secure-protocol { [** ssl3 **] [** tls1 **] }** Configure to make the switch support the corresponding protocol. By default, the switch supports SSLv3 and TLSv1. ssl3: Enable the SSL version 3 protocol. SSL is a transport protocol. It can provide server authentication, encryption and message integrity to allow secure HTTP connection. tls1: Enable the TLS version 1 protocol. TLS is s transport protocol upgraded from SSL. It supports different encryption algorithm from SSL, so TLS and SSL are not compatible. TLS can support a more secure connection.
Step 4	**ip http secure-ciphersuite { [3des-ede-cbc-sha] [rc4-128-md5] [rc4-128-sha] [des-cbc-sha] }** Enable the corresponding ciphersuite. By default, these types are all enabled. **3des-ede-cbc-sha**: Key exchange with 3DES and DES-EDE3-CBC for message encryption and SHA for message digest. **rc4-128-md5**: Key exchange with RC4 128-bit encryption and MD5 for message digest. **rc4-128-sha**: Key exchange with RC4 128-bit encryption and SHA for message digest. **des-cbc-sha**: Key exchange with DES-CBC for message encryption and SHA for message digest.
Step 5	**ip http secure-session timeout** *minutes* Specify the Session Timeout time. The system will log out automatically if users do nothing within the Session Timeout time. *minutes*: Specify the timeout time, which ranges from 5 to 30 minutes. The default value is 10.

Step 6	**ip http secure-max-users** *admin-num operator-num poweruser-num user-num* Specify the maximum number of users that are allowed to connect to the HTTPS server. The total number of users should be no more than 16. *admin-num*: Enter the maximum number of users whose access level is Admin. The valid values are from 1 to 16. *operator-num*: Enter the maximum number of users whose access level is Operator. The valid values are from 0 to 15. *poweruser-num*: Enter the maximum number of users whose access level is Power User. The valid values are from 0 to 15. *user-num*: Enter the maximum number of users whose access level is User. The valid values are from 0 to 15.
Step 7	**ip http secure-server download certificate** *ssl-cert* **ip-address** *ip-addr* Download the desired certificate to the switch from TFTP server. *ssl-cert*: Specify the name of the SSL certificate, which ranges from 1 to 25 characters. The certificate must be BASE64 encoded. The SSL certificate and key downloaded must match each other. *ip-addr*: Specify the IP address of the TFTP server. Both IPv4 and IPv6 addresses are supported.
Step 8	**ip http secure-server download key** *ssl-key* **ip-address** *ip-addr* Download the desired key to the switch from TFTP server. *ssl-key*: Specify the name of the key file saved in TFTP server. The key must be BASE64 encoded. *ip-addr*: Specify the IP address of the TFTP server. Both IPv4 and IPv6 addresses are supported.
Step 9	**show ip http secure-server** Verify the global configuration of HTTPS.
Step 10	**end** Return to privileged EXEC mode.
Step 11	**copy running-config startup-config** Save the settings in the configuration file.

The following example shows how to configure the HTTPS function. Enable SSL3 and TLS1 protocol. Enable the ciphersuite of 3des-ede-cbc-sha. Set the session timeout time as 15, the maximum admin number as 2, the maximum operator number as 2, the maximum power user number as 2, the maximum user number as 2. Download the certificate named ca.crt and the key named ca.key from the TFTP server with the IP address 192.168.0.100.

Switch#configure

Switch(config)#ip http secure-server

Switch(config)#ip http secure-protocol ssl3 tls1

Switch(config)#ip http secure-ciphersuite 3des-ede-cbc-sha

Switch(config)#ip http secure-session timeout 15

Switch(config)#ip http secure-max-users 2 2 2 2

Switch(config)#ip http secure-server download certificate ca.crt **ip-address** 192.168.0.100

Start to download SSL certificate.....

Download SSL certificate OK.

Switch(config)#ip http secure-server download key ca.key **ip-address** 192.168.0.100

Start to download SSL key.....

Download SSL key OK.

Switch(config)#show ip http secure-server

HTTPS Status:	Enabled
HTTPS Port:	443
SSL Protocol Level(s):	ssl3 tls1
SSL CipherSuite:	3des-ede-cbc-sha
HTTPS Session Timeout:	15
HTTPS User Limitation:	Enabled
HTTPS Max Users as Admin:	2
HTTPS Max Users as Operator:	2
HTTPS Max Users as Power User:	2
HTTPS Max Users as User:	2

Switch(config)#end

Switch#copy running-config startup-config

2.2.4 Configuring the SSH Feature

Follow these steps to configure the SSH function:

Step 1	**configure** Enter global configuration mode.
Step 2	**ip ssh server** Enable the SSH function. By default, it is disabled.

Step 3	**ip ssh version {** v1 | v2 **}** Configure to make the switch support the corresponding protocol. By default, the switch supports SSHv1 and SSHv3. v1 | v2: Select to enable the corresponding protocol.
Step 4	**ip ssh timeout** *value* Specify the idle timeout time. The system will automatically release the connection when the time is up. *value*: Enter the value of the timeout time, which ranges from 1 to 120 seconds. The default value is 120 seconds.
Step 5	**ip ssh max-client** *num* Specify the maximum number of the connections to the SSH server. New connection will not be established when the number of the connections reaches the maximum number you set. *num*: Enter the number of the connections, which ranges from 1 to 5. The default value is 5.
Step 6	**ip ssh algorithm {** AES128-CBC | AES192-CBC | AES256-CBC | Blowfish-CBC | Cast128-CBC | 3DES-CBC | HMAC-SHA1 | HMAC-MD5 **}** Enable the corresponding algorithm. By default, these types are all enabled. AES128-CBC | AES192-CBC | AES256-CBC | Blowfish-CBC | Cast128-CBC | 3DES-CBC: Specify the encryption algorithm you want the switch supports. HMAC-SHA1 | HMAC-MD5: Specify the data integrity algorithm you want the switch supports.
Step 7	**ip ssh download {** v1 | v2 **}** *key-file* **ip-address** *ip-addr* Select the type of the key file and download the desired file to the switch from TFTP server. v1 | v2: Select the key type. The algorithm of the corresponding type is used for both key generation and authentication. *key-file*: Specify the name of the key file saved in TFTP server. Ensure the key length of the downloaded file is in the range of 512 to 3072 bits. *ip-addr*: Specify the IP address of the TFTP server. Both IPv4 and IPv6 addresses are supported.
Step 8	**show ip ssh** Verify the global configuration of SSH.
Step 9	**end** Return to privileged EXEC mode.
Step 10	**copy running-config startup-config** Save the settings in the configuration file.

Note:

It will take a long time to download the key file. Please wait without any operation.

The following example shows how to configure the SSH function. Set the version as SSH V1 and SSH V2. Enable the AES128-CBC and Cast128-CBC encryption algorithm. Enable the HMAC-MD5 data integrity algorithm. Choose the key type as SSH-2 RSA/DSA.

Switch(config)#ip ssh server

Switch(config)#ip ssh version v1

Switch(config)#ip ssh version v2

Switch(config)#ip ssh timeout 100

Switch(config)#ip ssh max-client 4

Switch(config)#ip ssh algorithm AES128-CBC

Switch(config)#ip ssh algorithm Cast128-CBC

Switch(config)#ip ssh algorithm HMAC-MD5

Switch(config)#ip ssh download v2 publickey **ip-address** 192.168.0.100

Start to download SSH key file.....

Download SSH key file OK.

Switch(config)#show ip ssh

Global Config:

SSH Server: Enabled

Protocol V1: Enabled

Protocol V2: Enabled

Idle Timeout: 100

MAX Clients: 4

Port: 22

Encryption Algorithm:

AES128-CBC: Enabled

AES192-CBC: Disabled

AES256-CBC: Disabled

Blowfish-CBC: Disabled

Cast128-CBC: Enabled

3DES-CBC: Disabled

Data Integrity Algorithm:

HMAC-SHA1: Disabled

HMAC-MD5: Enabled

Key Type: SSH-2 RSA/DSA

Key File:

---- BEGIN SSH2 PUBLIC KEY ----

Comment: “dsa-key-20160711”

Switch(config)#end

Switch#copy running-config startup-config

2.2.5 Configuring the Telnet Function

Follow these steps enable the Telnet function:

Step 1	**configure** Enter global configuration mode.
Step 2	**telnet enable** Enable the telnet function. By default, it is enabled.
Step 3	**telnet port** *port* Specify the port using for Telnet. It ranges from 1 to 65535.
Step 4	**end** Return to privileged EXEC mode.
Step 5	**copy running-config startup-config** Save the settings in the configuration file.

2.2.6 Configuring the Serial Port Parameters

Note:

Only T2600G series switches support Serial Port.

Follow these steps enable the serial port parameters:

Step 1	**configure** Enter global configuration mode.
Step 2	**serial_port baud_rate {** 9600 | 19200 | 38400 | 57600 | 115200 **}** Specify the baud rate of the console connection. 9600 | 19200 | 38400 | 57600 | 115200: Specify the communication baud rate on the console port. The default value is 38400 bps.

Step 3	**end** Return to privileged EXEC mode.
Step 4	**copy running-config startup-config** Save the settings in the configuration file.

3 Appendix: Default Parameters

Default settings of Access Security are listed in the following tables.

Table 3-1 Default Settings of Access Control Configuration

Parameter	Default Setting
Access Control	Disabled

Table 3-2 Default Settings of HTTP Configuration

Parameter	Default Setting
HTTP	Enabled
Port	80
Session Timeout	10 minutes
Number Control	Disabled

Table 3-3 Default Settings of HTTPS Configuration

Parameter	Default Setting
HTTPS	Enabled
SSL Version 3	Enabled
TLS Version 1	Enabled
Port	443
RSA_WITH_RC4_128_MD5	Enabled
RSA_WITH_RC4_128_SHA	Enabled
RSA_WITH_DES_CBC_SHA	Enabled
RSA_WITH_3DES_EDE_CBC_SHA	Enabled
Session Timeout	10 minutes
Number Control	Disabled

Table 3-4 Default Settings of SSH Configuration

Parameter	Default Setting
SSH	Disabled
Protocol V1	Enabled
Protocol V2	Enabled
Idle Timeout	120 seconds
Maximum Connections	5

Parameter	Default Setting
Port	22
AES128-CBC	Enabled
AES192-CBC	Enabled
AES256-CBC	Enabled
Blowfish-CBC	Enabled
Cast128-CBC	Enabled
3DES-CBC	Enabled
HMAC-SHA1	Enabled
HMAC-MD5	Enabled
Key Type:	SSH-2 RSA/DSA

Table 3-5 Default Settings of Telnet Configuration

Parameter	Default Setting
Telnet	Enabled
Port	23

Table 3-6 Default Settings of Serial Port

Parameter	Default Setting
Baud Rate	38400 bps