DGCOM3000 Gateway & Switch All-in-One
Operation Manual

Publication Date: May. 2017

Version: V1.0

KYLAND

Disclaimer:

Kyland Technology Co., Ltd. tries to keep the content in this manual as accurate and as up-to-date as possible. This document is not guaranteed to be error-free, and we reserve the right to amend it without notice.

All rights reserved

Website: http://www.kyland.com
FAX: +86-10-88796678
Email: services@kyland.com.cn

Contents

1. Product Introduction

1.1 Overview

DGCOM3000 is an all-in-one switch gateway designed for system integration and application, to implement the communication gateway (application-layer) function on a switch. It can be deployed as a distribut ed intelligent communication node in any automation system to collect various types of data through the RS485, RS232, and RS422 serial ports and Ethernet ports. It uses a dedicated configuration tool to import predefined IEC 61850 templates (.icd/.cid files) and perform mapping configuration of internally collected data. The DGCOM3000 can serve as an IEC 61850-compliant Intelligent Electronic Device (IED) agent (node) to communicate with the master station, thereby simplifying the communication of automation systems. It accommodates 2 x 1000M SFP ports and 6 x 100M electrical ports and provides the robust network management function. The network management system (NMS) supports the CLI-, Telnet-, Web, and SNMP-based NMS software as well as OPC NMS software.

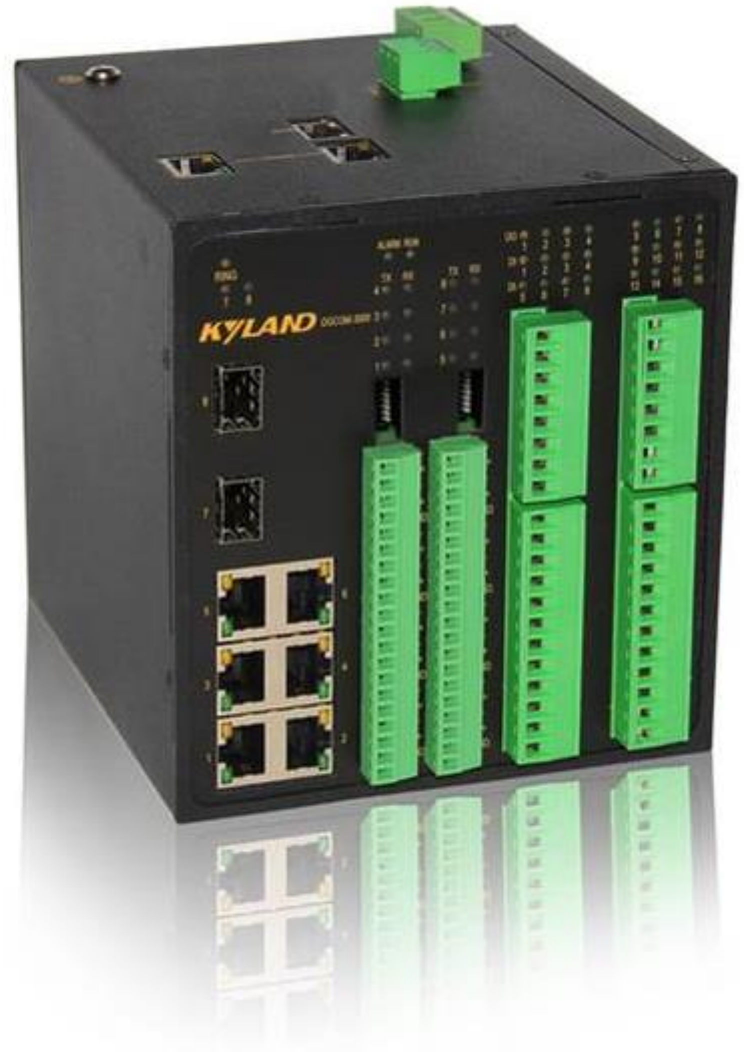


Figure 1 DGCOM3000 Illustration

2. Product Applications

2.1.Communication Protocol Conversion

The DGCOM3000 is applicable to scenarios in which various types of automation systems are integrated. It completes data collection and communication protocol conversion. It makes data communication with the relay protector, fault recorder, watt hour meter, direct current panel, and other devices through any serial ports or Ethernet ports. After internal processing, it makes data communication with a third-party system as per the specified communication standard through relevant network or serial ports. The DGCOM3000 can be widely applied in various automation systems as well as distributed data collection and protocol conversion scenarios. Figure 2 shows the typical application topology.

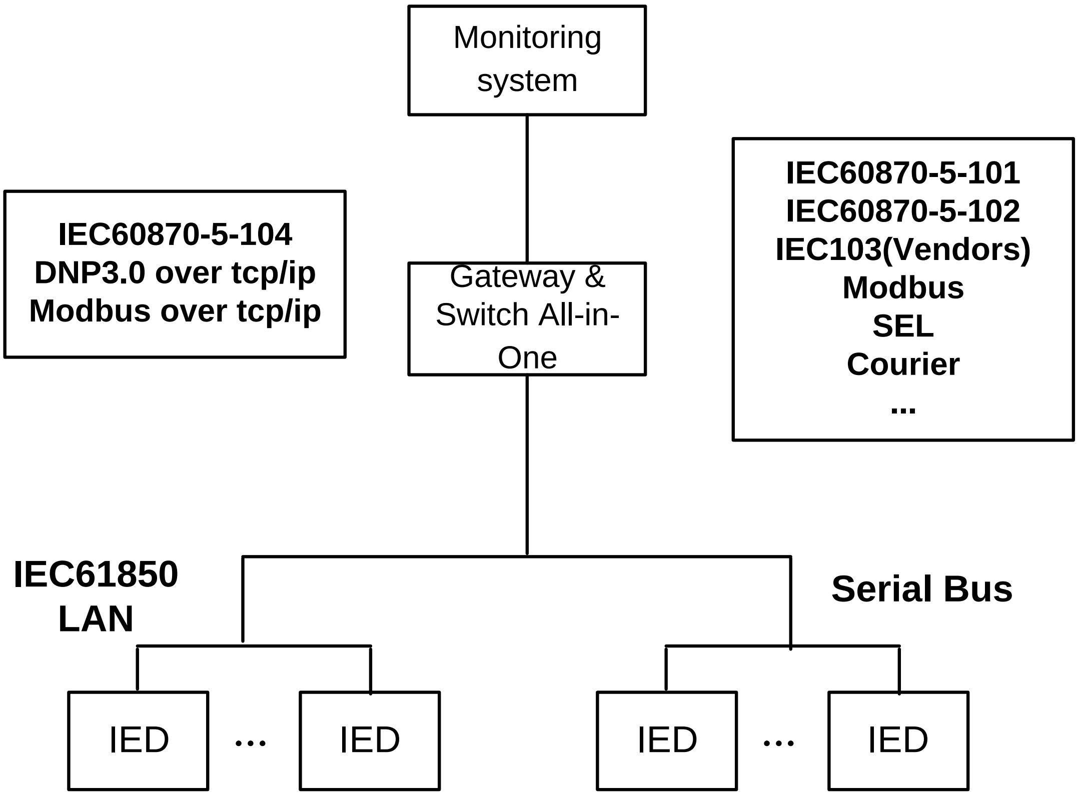


Figure 2 Application of the DGCOM3000 in communication protocol conversion

2.2.Integrated Automation of Power Stations

- Data collection and storage

Any communication port of the DGCOM3000 can be flexibly configured to support relevant data collection protocols. It collects various types of communication data of protection devices, measurement and control devices, instruments and meters, fault recorders, and intelligent sensors, and synchronously forwards collected real-time data in online mode while storing the data into the local real-time database, thereby greatly simplifying the communication topology structure of automation systems.

- Control and operation

The DGCOM3000 can forward control commands from the master station over different communication links, to control different devices on site. It supports batch control, ordered control, conditional control, and other functions by means of logic programming.

- Accurate real-time online monitoring

The DGCOM3000 relies on the clock server to provide high-precision time serving function. It synchronizes time via the Network Time Protocol (NTP), Simple Network Time Protocol (SNTP), and other protocols, to ensure time accuracy in the unit and implements transmission of local events and data with time tags, thereby providing convenience for subsequent data analysis and fault processing. See Figure 3.

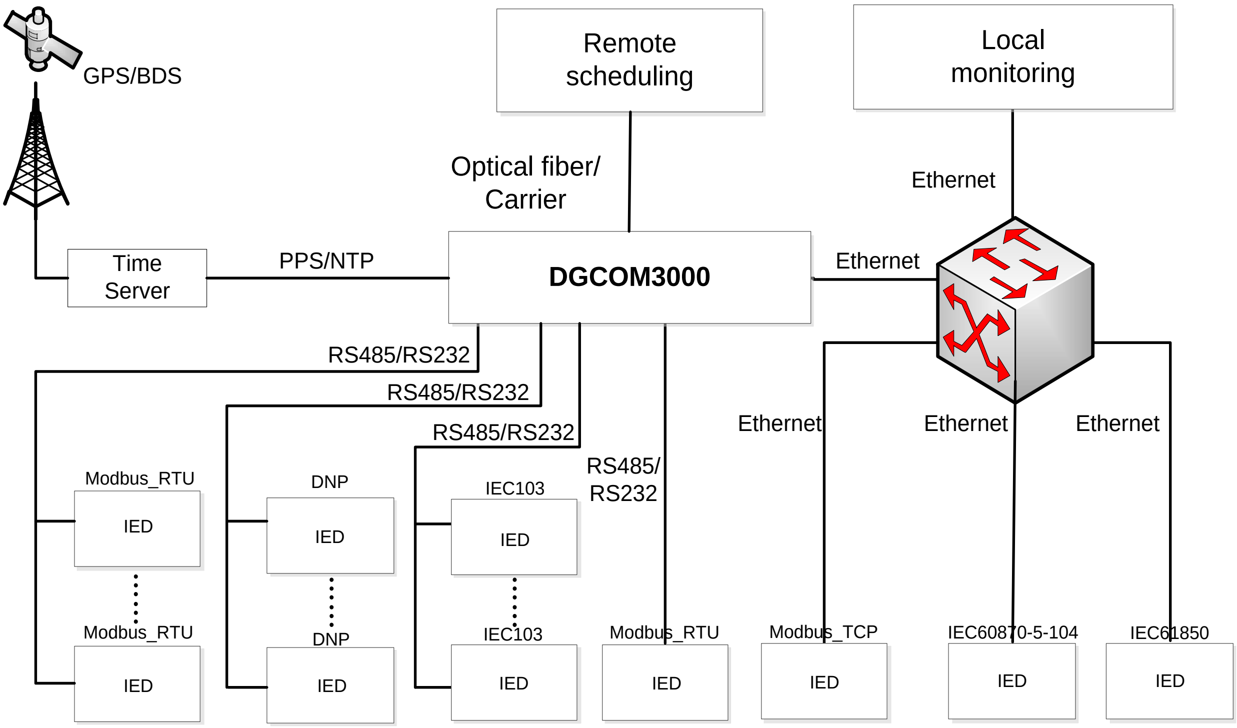


Figure 3 Application of the DGCOM3000 in integrated automation of power stations

2.3.Virtual Port Connection

The DGCOM3000 can be also configured to support the link-layer service of a virtual connection (STA server) on any serial port. It is capable of converting serial port data into TCP/IP network data, to implement bidirectional transparent transmission of serial data and TCP/IP network interface data. In this way, the serial port device can directly make data communication with TCP/IP-based network application software, to provide convenience for long-distance communication of considerable devices with serial ports.

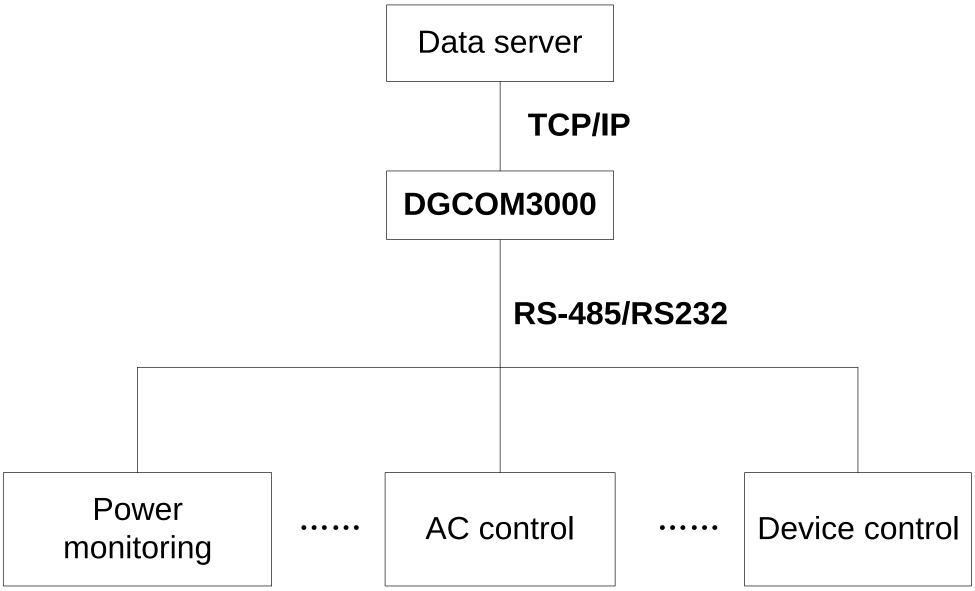


Figure 4 Application of the DGCOM3000 in virtual port connection

2.4.IEC61850 Client/Server Service

The DGCOM3000 supports IEC61850-compliant data collection and forwarding. It supports the import of any SCL (.icd/.cid) model files, and can be configured to provide the IEC61850 data server service for conventional IEDs as an abstract virtual IEC61850-compliant communication agent (VMD). In addition, it can serve as an IEC 61850 client to collect the data of IEC 61850 IEDs and convert the data into conventional protocol data. This feature provides a flexible, convenient, economical, and efficient solution for IEC 61850 communication of conventional devices and data exchange between IEC 61850 IEDs and conventional data collectors. Figure 5 shows the typical application.

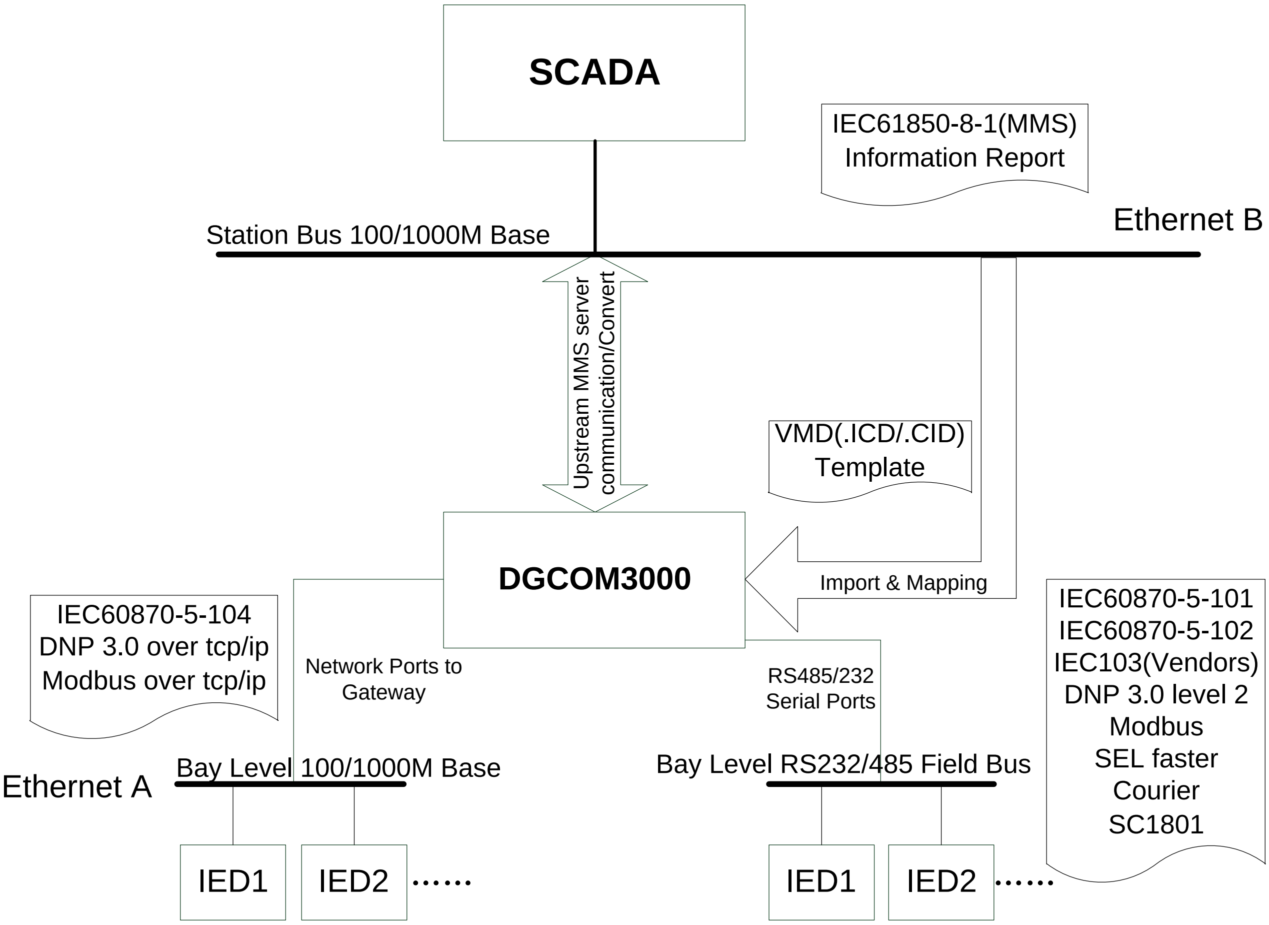


Figure 5 Application of the DGCOM3000 in IEC 61850 server service

2.5.SoftPLC Application

The embedded simple and easy-to-understand type-C script programming language enables the DGCOM3000 to meet different engineering application requirements, including online calculation, logic judgment, and arithmetical operation. The softPLC function is widely applied in information point combination calculation, data amount accumulation, batch processing control, closed loop control, timed execution, conditional blocking. The frequency of logic operation detection scanning can be as high as milliseconds.

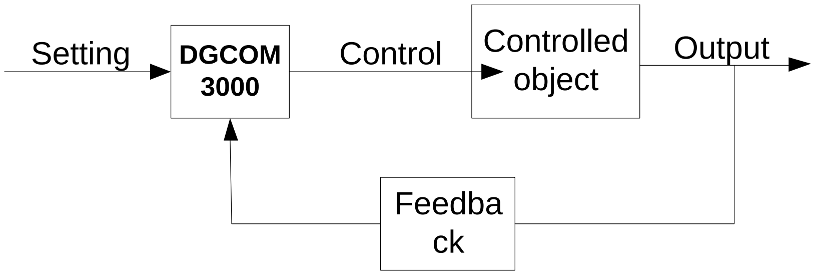


Figure 6 Application of the DGCOM3000 in advanced applications

3. Exchange function WEB configuration

3.1 Switch Access

You can access the switch by:

- **Console port**
- **Telnet/SSH**
- **Web browser**
- **Kyvision management software**

Kyvision network management software is designed by Kyland. For details, refer to its user manual.

3.1.1 View Types

When logging into the Command Line Interface (CLI) by the console port or Telnet, you can enter different views or switch between views by using the following commands.

Table 1 View Types

View Prompt	View Type	View Function	Command for View Switching
SWITCH #	Privileged mode	View recently used commands. View software version. View response information for ping operation. Upload/Download configuration file. Restore default configuration. Reboot switch. **Save current configuration.** Display current configuration. Update software.	Input “**configure terminal**” to switch from privileged mode to configuration mode. Input “**exit**” to return to the general mode.
SWITCH（config）#	Configuration mode	Configure all switch functions.	Input "**exit**" or "**end**" to return to the Privileged mode.

When the switch is configured through the CLI, "?" can be used to get command help. In the help information, there are different parameter description formats. For example, <1, 255> means a number range; <xx:xx:xx:xx:xx:xx> means a MAC address; <word31> means the string range is 1~31. In addition, ↑ and ↓ can be used to scroll through recently used commands.

3.1.2 Switch Access by Console Port

You can access a switch by its console port and the hyper terminal of Windows OS or other software that supports serial port connection, such as HTT3.3. The following example shows how to use Hyper Terminal to access switch by console port.

1. Connect the serial communication port of a PC and the console port of the switch with the DB9-RJ45 cable.

2. Run the Hyper Terminal in Windows desktop. Click [Start] → [All Programs] → [Accessories] → [Communications] → [Hyper Terminal], as shown in Figure 7.

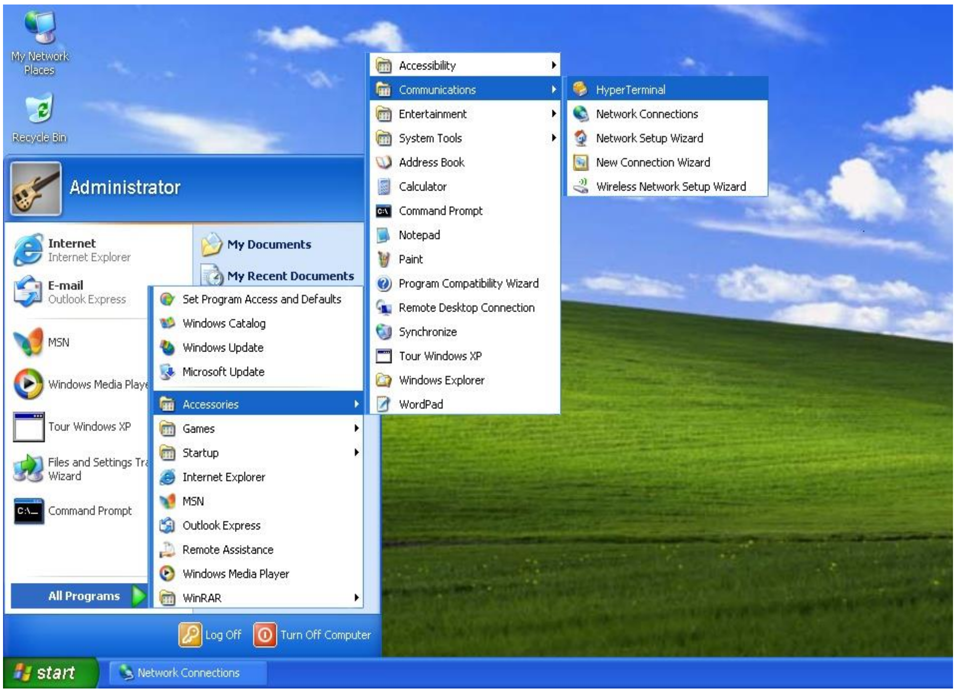
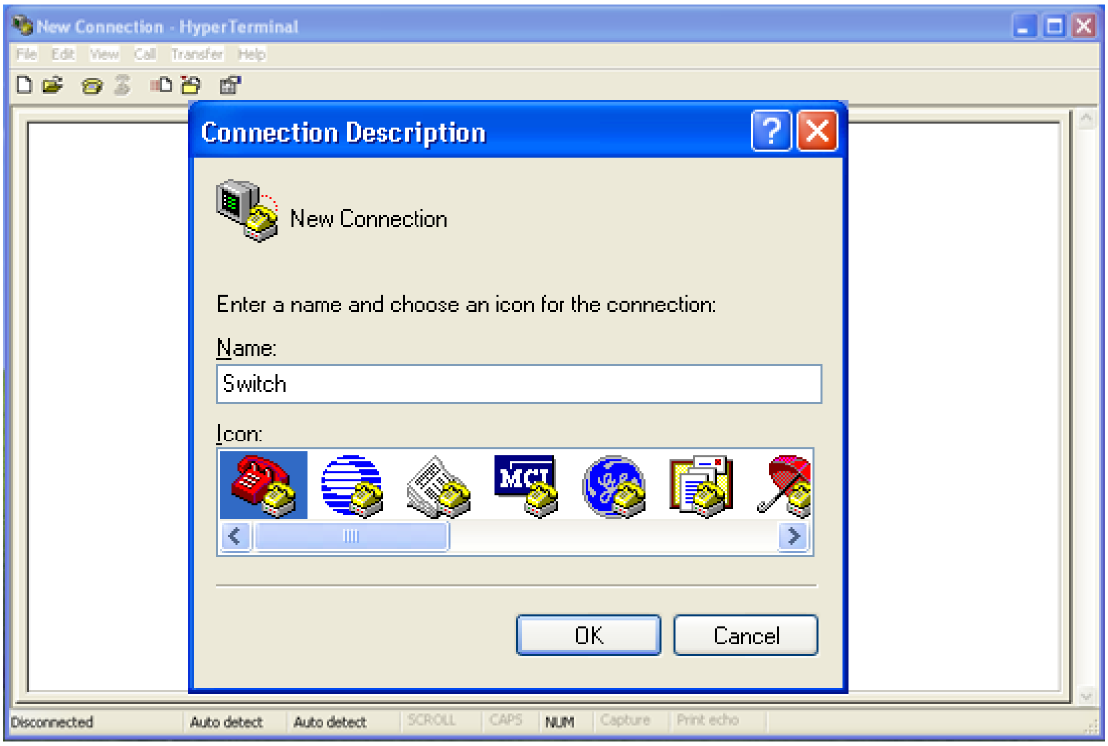


Figure 7 Starting the Hyper Terminal

3. Create a new connection "Switch", as shown in Figure 8.


New Connection - HyperTerminal
File Edit View Call Transfer Help
Connection Description
New Connection

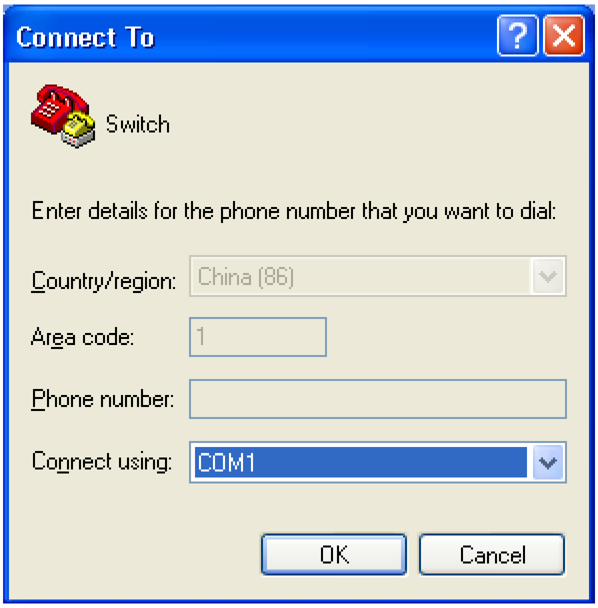
Enter a name and choose an icon for the connection:

Name: Switch

Icon:
OK
Cancel
Disconnected Auto detect Auto detect SCROLL CAPS NUM Capture Print echo

Figure 8 Creating a New Connection

4. Connect the communication port in use, as shown in Figure 9.



Enter details for the phone number that you want to dial:

Country/region: China (86)

Area code: 1

Phone number:

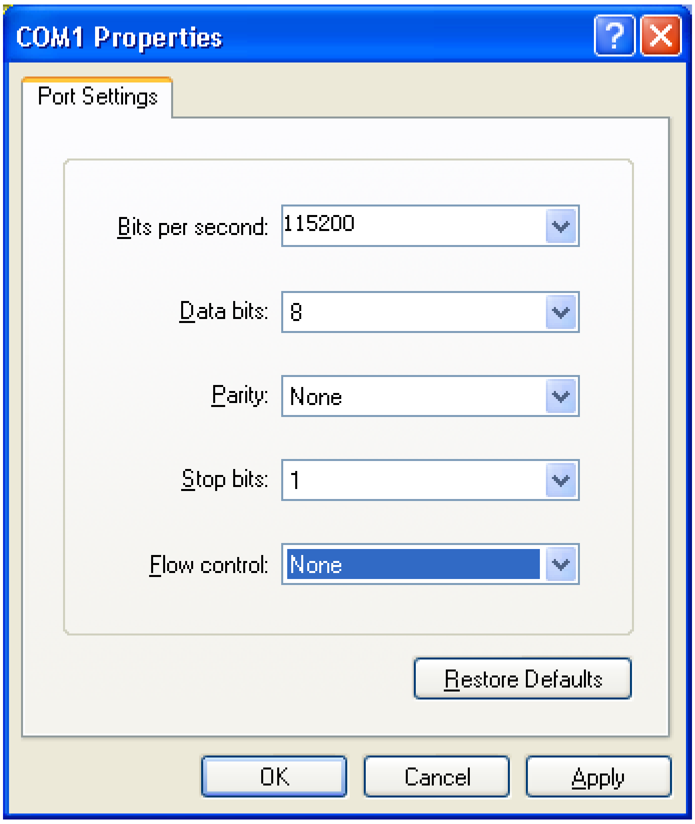
Connect using: COM1

Figure 9 Selecting the Communication Port

Note:

To confirm the communication port in use, right-click [My Computer] and click [Property] → [Hardware] → [Device Manager] → [Port].

5. Set port parameters (Bits per second: 115200, Data bits: 8, Parity: None, Stop bits: 1, and Flow control: None), as shown in Figure 10.


COM1 Properties

Port Settings

Bits per second: 115200

Data bits: 8

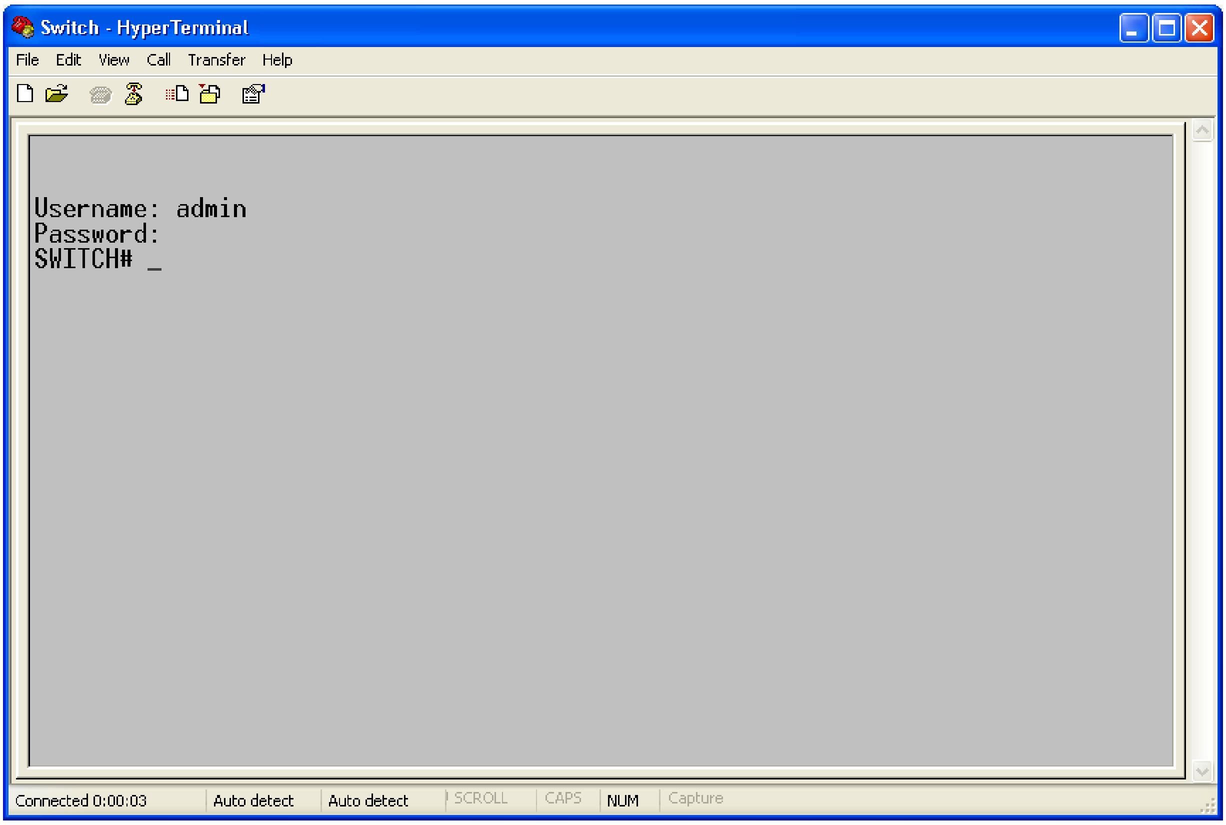
Parity: None

Stop bits: 1

Flow control: None

Figure 10 Setting Port Parameters

6. Click <OK> button to enter the switch CLI. Input default user "admin”, and password”123” to enter the privileged mode. You can also input other created users and password, as shown in Figure 11.


Switch - HyperTerminal
File Edit View Call Transfer Help
Connected 0:00:03 Auto detect Auto detect SCROLL CAPS NUM Capture

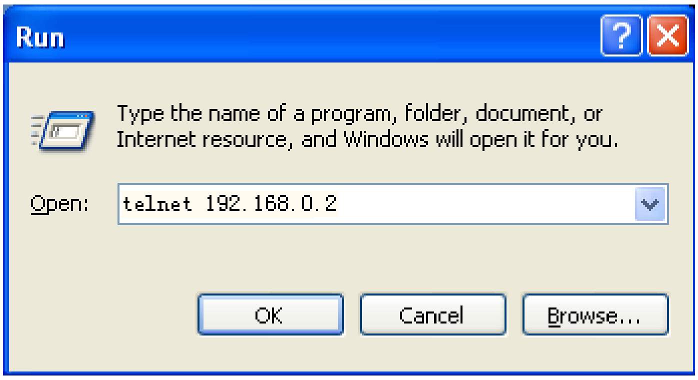
```
Username: admin
Password:
SWITCH# _
```

Figure 11 CLI

3.1.3 Switch Access by Telnet

The precondition for accessing a switch by Telnet is the normal communication between the PC and the switch.

1. Enter "**telnet** *IP address*" in the Run dialog box, as shown in Figure 12. The default IP address of a Kyland switch is 192.168.0.2.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

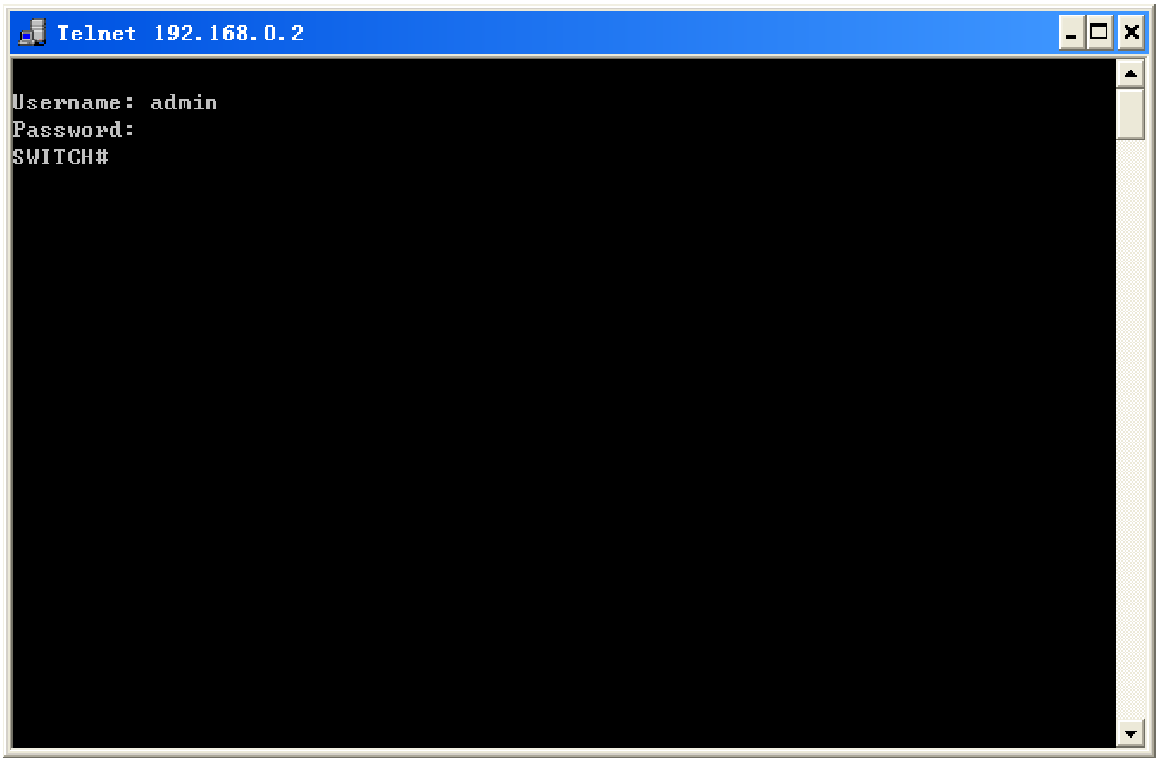
Open: telnet 192.168.0.2

Figure 12 Telnet Access

Note:

To confirm the switch IP address, please refer to “3.4 IP Configuration” to learn how to obtain IP address.

2. In the Telnet interface, input user "admin", and password "123" to log in to the switch. You can also input other created users and password, as shown in Figure 13.



```
Username: admin
Password:
SWITCH#
```

Figure 13 Telnet Interface

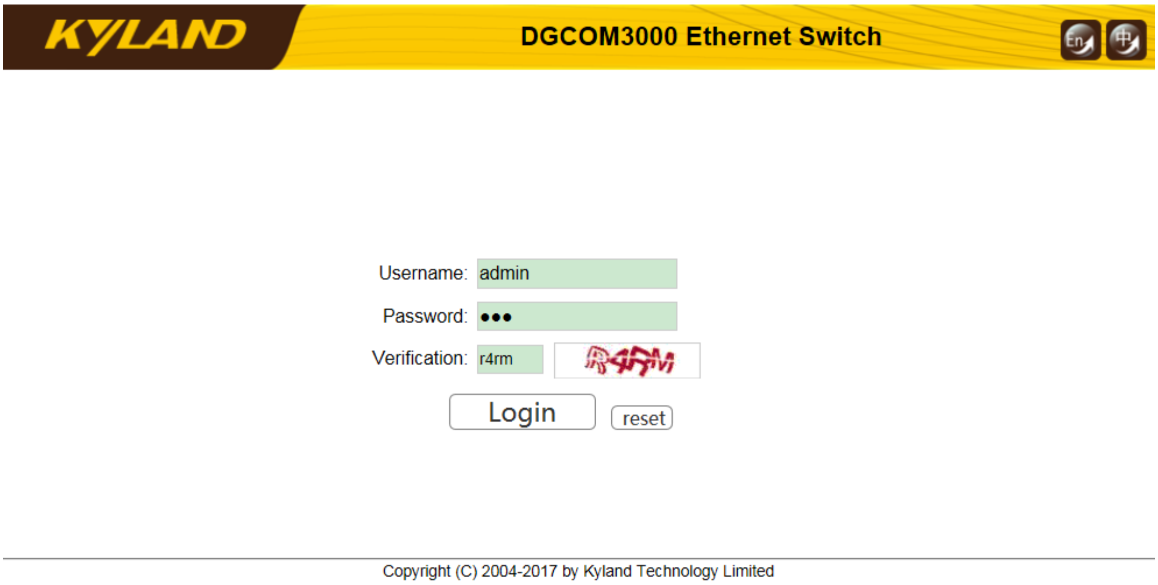
3.1.4 Switch Access by Web

The precondition for accessing a switch by Web is the normal communication between the PC and the switch.

Note:

IE8.0 or a later version is recommended for the best Web display results.

1. Input "*IP address*" in the browser address bar. The login interface is displayed, as shown in Figure 14. Input the default user name "admin", password "123", and the Verification. Click <Login>. You can also input other created users and password.


KYLAND
DGCOM3000 Ethernet Switch
Login
reset
Copyright (C) 2004-2017 by Kyland Technology Limited

Username: admin

Password: ●●●

Verification: r4rm

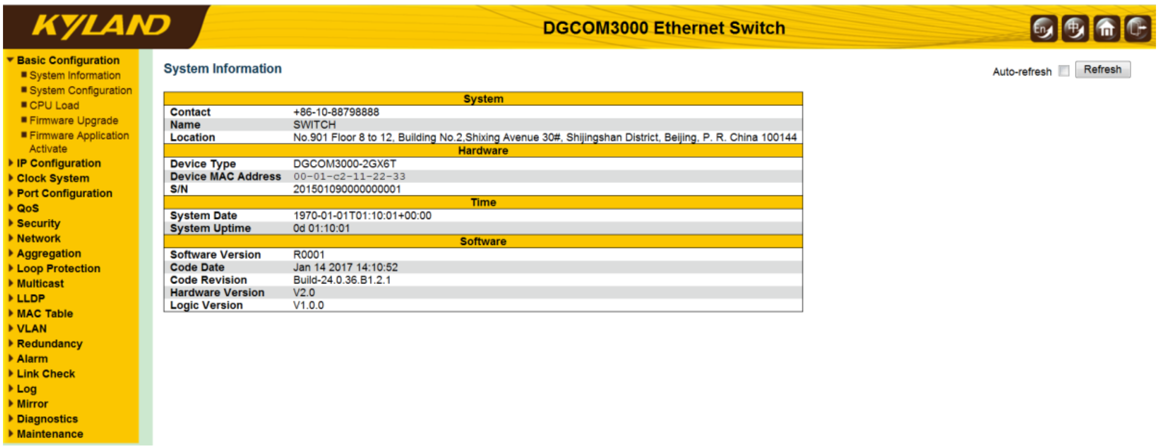
Figure 14 Web Login

you can click En or 中 to switch to the English or Chinese interface. The English login interface is displayed by default.

Note:

To confirm the switch IP address, please refer to "3.4 IP Configuration" to learn how to obtain IP address.

2. After you log in successfully, there is a navigation tree on the left of the interface, as shown in Figure 15.

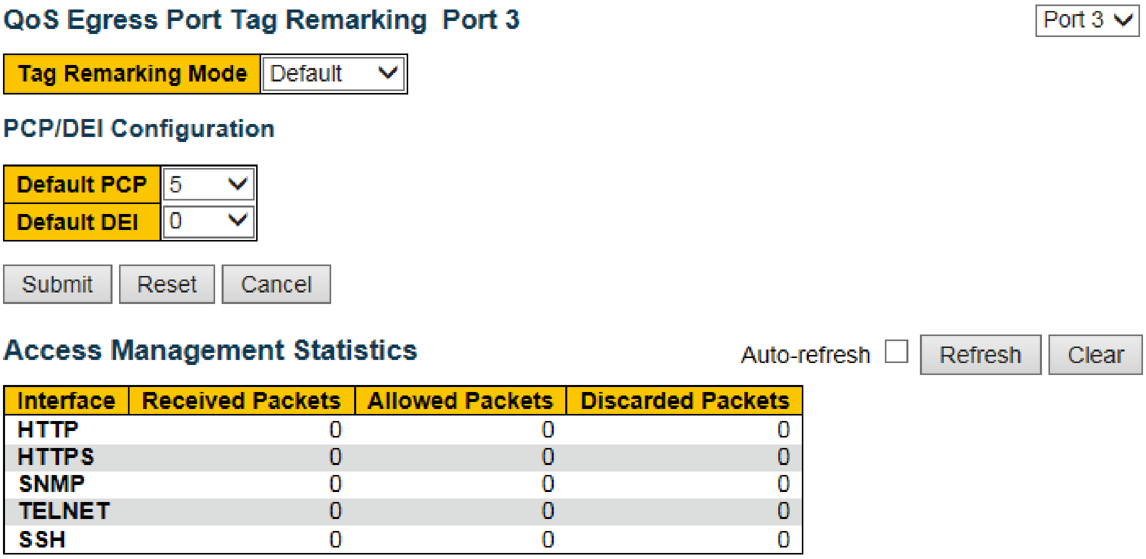


System	
Contact	+86-10-88798888
Name	SWITCH
Location	No.901 Floor 8 to 12, Building No.2,Shixing Avenue 30#, Shijingshan District, Beijing, P. R. China 100144
Hardware	
Device Type	DGCOM3000-2GX6T
Device MAC Address	00-01-c2-11-22-33
S/N	201501090000000001
Time	
System Date	1970-01-01T01:10:01+00:00
System Uptime	0d 01:10:01
Software	
Software Version	R0001
Code Date	Jan 14 2017 14:10:52
Code Revision	Build-24.0.36.B1.2.1
Hardware Version	V2.0
Logic Version	V1.0.0

Figure 15 Web Interface

You can expand or collapse the navigation tree by clicking menu on the navigation tree. You can click 🏠 to link to Figure 15, and click ⇥ to exit the Web interface.

As shown in Figure 16, the configuration/view page of each module provides multiple operation buttons and you can click a button to perform a relevant operation on the page. For example, you can click <Submit> to make the current configuration take effect, click <Reset> to cancel the current configuration and use the configuration that has taken effect, click <Cancel> to close the configuration page and return to the previous configuration page, or click <Refresh> to update information on the current page. You can also select "Auto-refresh" so that the information is automatically updated, at an interval of 3s, or click <Clear> to clear the current statistics and restart statistics.



QoS Egress Port Tag Remarking Port 3

Port 3

Tag Remarking Mode	Default

PCP/DEI Configuration

Default PCP	5
Default DEI	0

Access Management Statistics

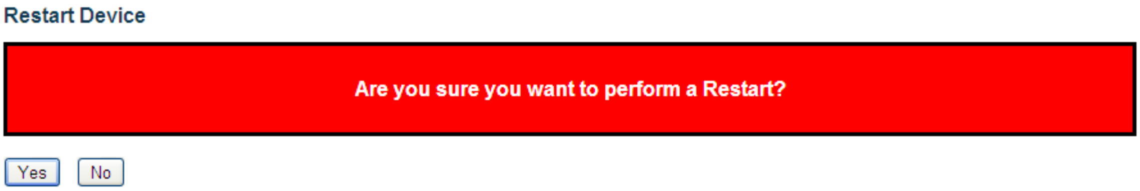
Auto-refresh □

Interface	Received Packets	Allowed Packets	Discarded Packets
HTTP	0	0	0
HTTPS	0	0	0
SNMP	0	0	0
TELNET	0	0	0
SSH	0	0	0

Figure 16 Configuration/Statistics Interface

3.2 Maintenance

1. Reboot the device, as shown in Figure 17.



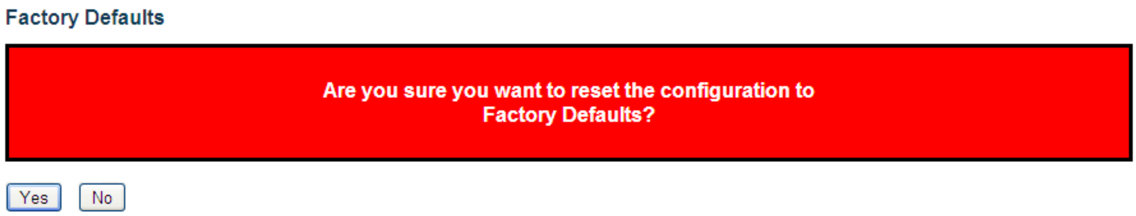
Restart Device

Are you sure you want to perform a Restart?

Figure 17 Reboot

Before rebooting, please confirm whether to save current configuration. If you select "Yes", the switch runs the current configuration after reboot. If you select "No", the switch runs the previous saved configuration. If no configuration has been saved, the switch will restore the default configuration after reboot.

2. Restore the default configuration, as shown in Figure 18.



Factory Defaults

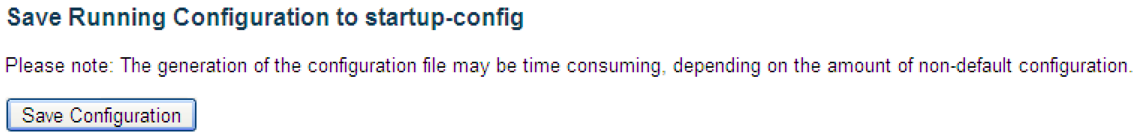
Are you sure you want to reset the configuration to Factory Defaults?

Figure 18 Restoring Default Configuration

Caution:

After you have restored the default settings, you need to restart the device to make settings take effect.

3. Save current running-config, as shown in Figure 19.

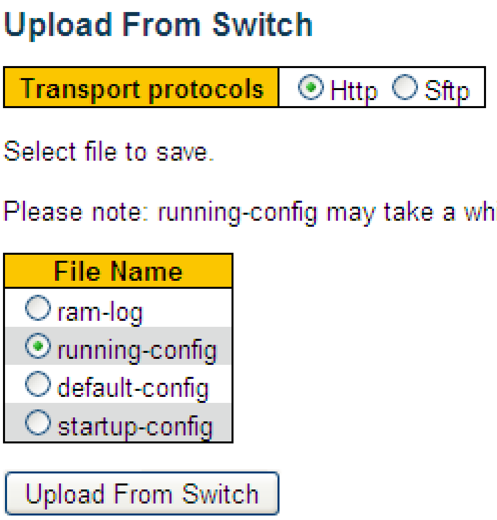


Save Running Configuration to startup-config

Please note: The generation of the configuration file may be time consuming, depending on the amount of non-default configuration.

Figure 19 Save Current Configuration

4. Upload the file from the switch to local /server, as shown in Figure 20, Figure 21.



Upload From Switch

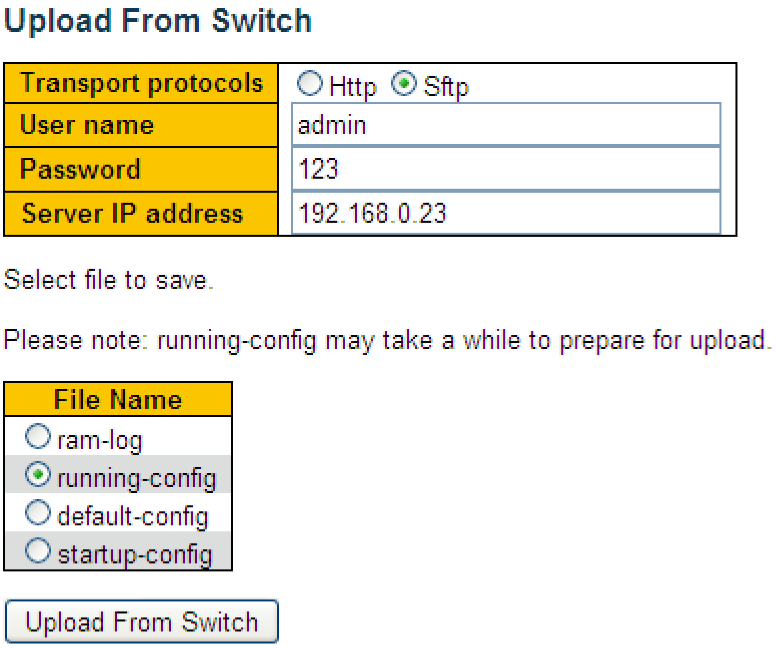
Transport protocols ● Http ○ Sftp

Select file to save.

Please note: running-config may take a while to prepare for upload.

File Name
○ ram-log
● running-config
○ default-config
○ startup-config

Figure 20 Upload File -HTTP



Upload From Switch

Transport protocols	○ Http ● Sftp
User name	admin
Password	123
Server IP address	192.168.0.23

Select file to save.

Please note: running-config may take a while to prepare for upload.

File Name
○ ram-log
● running-config
○ default-config
○ startup-config

Figure 21 Upload File -SFTP

{User name, Password }

Range: {1~63 characters, 1~63 characters}

Description: Input the user name and password created on SFTP server.

Server IP address

Format: A.B.C.D

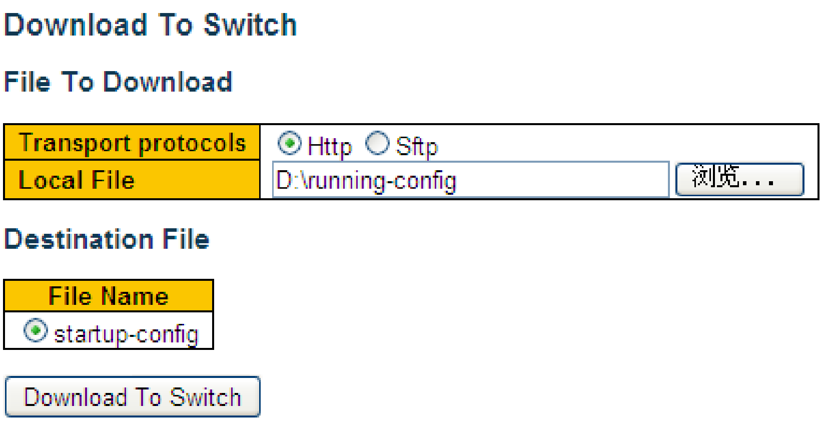
Description: Configure the IP address of the SFTP server.

Caution:

- Transmission file by SFTP, you need to configure SFTP user name, password, and SFTP server IP address.
- In the file transmission process, keeps the SFTP server running.

You can save a file in the switch to the local /server. **ram-log** file records the log information, **running-config** is the current running configuration file of the switch, **default-config** is the default configuration file, and **startup-config** is the switch startup file. Select a file and click <Upload From Switch> to save the file to the local/server.

5. Download the configuration file from local /server to switch as a new startup file for the switch, as shown in Figure 22, Figure 23.



Download To Switch

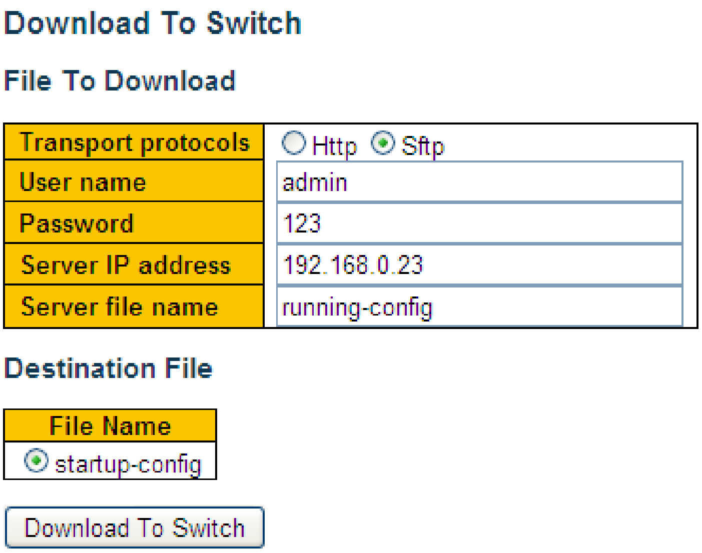
File To Download

Transport protocols	● Http ○ Sftp
Local File	D:\running-config 浏览...

Destination File

File Name
● startup-config

Figure 22 Download Configuration File -HTTP



Download To Switch

File To Download

Transport protocols	○ Http ● Sftp
User name	admin
Password	123
Server IP address	192.168.0.23
Server file name	running-config

Destination File

File Name
● startup-config

Figure 23 Download Configuration File –SFTP

Local File

Function: Select the configuration file stored in local.

{ User name, Password }

Range: { 1~63 characters, 1~63 characters }

Description: Input the user name and password created on SFTP server.

Server IP address

Format: A.B.C.D

Description: Configure the IP address of the SFTP server.

Server file name

Range: 1~63 characters

Description: Configure the configuration file name stored on SFTP server.

Caution:

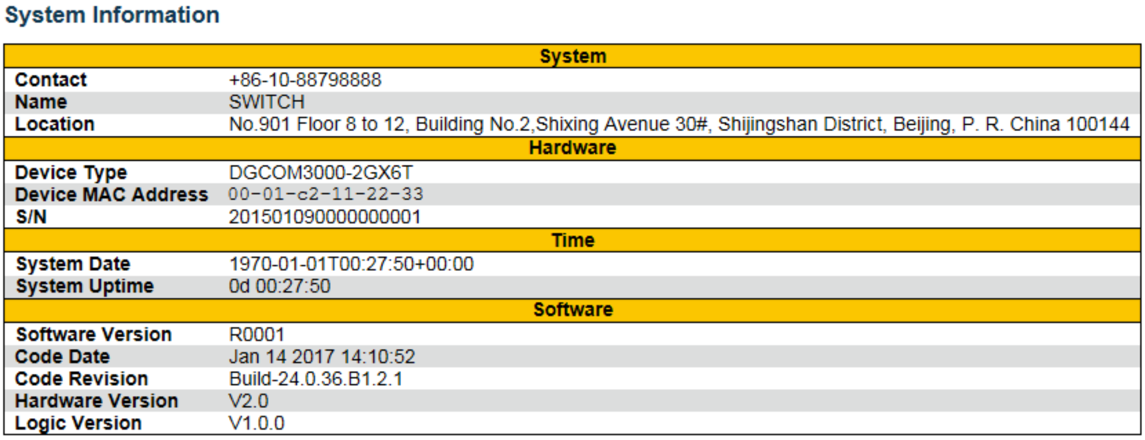
- Transmission file by SFTP, you need to configure SFTP user name, password, and SFTP server IP address.
- In the file transmission process, keeps the SFTP server running.

You can download the configuration file from local /server to switch as a new startup file for the switch. The new startup file will replace the original **startup-config** file. Click <Download To Switch> to download the configuration file from local /server to switch.

3.3 Basic Configuration

3.3.1 System Information

System information includes contact, system name, device type, MAC address, S/N, system time, and version information, as shown in Figure 24.



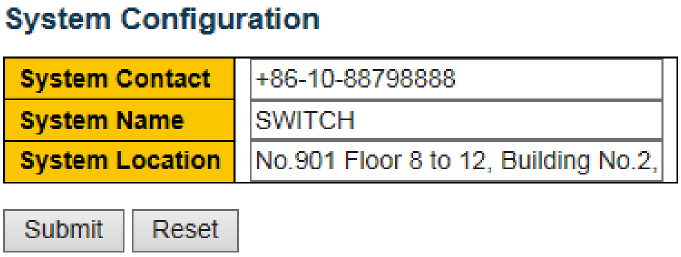
System Information

System	
Contact	+86-10-88798888
Name	SWITCH
Location	No.901 Floor 8 to 12, Building No.2,Shixing Avenue 30#, Shijingshan District, Beijing, P. R. China 100144
Hardware	
Device Type	DGCOM3000-2GX6T
Device MAC Address	00-01-c2-11-22-33
S/N	201501090000000001
Time	
System Date	1970-01-01T00:27:50+00:00
System Uptime	0d 00:27:50
Software	
Software Version	R0001
Code Date	Jan 14 2017 14:10:52
Code Revision	Build-24.0.36.B1.2.1
Hardware Version	V2.0
Logic Version	V1.0.0

Figure 24 System Information

3.3.2 System Configuration

System configuration includes contact, system name, and location configuration, as shown in Figure 25.



System Configuration

System Contact	+86-10-88798888
System Name	SWITCH
System Location	No.901 Floor 8 to 12, Building No.2,

Figure 25 System Configuration

System Contact

Range: 0~255 characters (ASCII characters from 32 to 126)

System Name

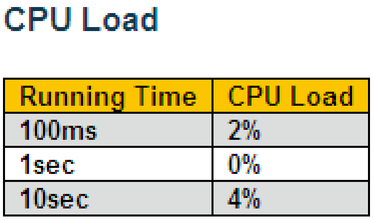
Range: 0~255 characters (alphabet A~Z / a~z, digits 0~9, minus sign -. The first character must be an alpha character, and the first or last character must not be a minus sign.

System Location

Range: 0~255 characters (ASCII characters from 32 to 126)

3.3.3 CPU Load

The load is measured as averaged over the last 100ms, 1sec and 10 seconds intervals, as shown in Figure 26.



CPU Load

Running Time	CPU Load
100ms	2%
1sec	0%
10sec	4%

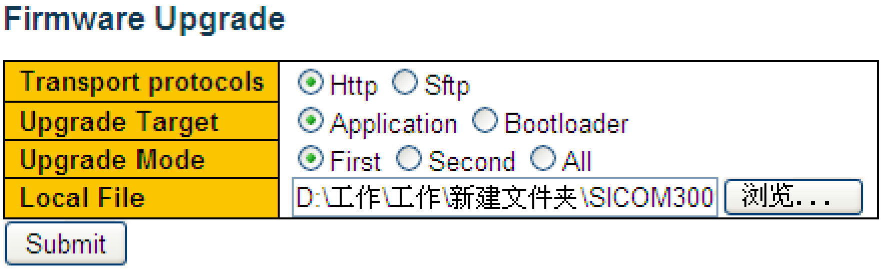
Figure 26 CPU Load

3.3.4 Firmware Upgrade

Firmware upgrade may help the switch to improve its performance. For this series switches, Firmware upgrade includes Boot version update and system software version update. The Boot version should be updated before the system software version. If the Boot version does not change, you can update only the system software version. Firmware upgrade needs the assistance of HTTP/SFTP.

3.3.4.1 Firmware Upgrade by HTTP

1. Upgrade firmware, as shown in Figure 27.



Firmware Upgrade

Transport protocols	● Http ○ Sftp
Upgrade Target	● Application ○ Bootloader
Upgrade Mode	● First ○ Second ○ All
Local File	D:\工作\工作\新建文件夹\SICOM300 浏览...

Figure 27 Upgrade Firmware-HTTP

Upgrade Target

Options: Application/Bootloader

Function: Select the upgrade target.

Upgrade Mode

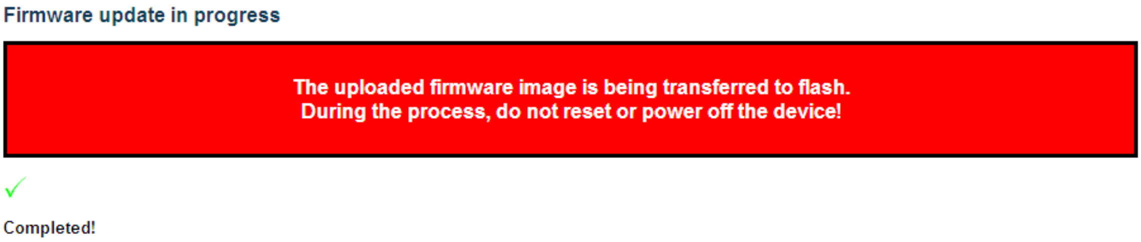
Options: First/Second/All

Description: Two firmware versions can be downloaded to the switch, and they can be the same or different. All indicates version 1 and version 2.

Local File

Function: Select the firmware update file stored in local.

2. When the update is completed as shown in Figure 28, please activate the software version and reboot the device, open the System Information page to check whether the update succeeded and the new version is active.



Firmware update in progress

The uploaded firmware image is being transferred to flash.
During the process, do not reset or power off the device!

✓

Completed!

Figure 28 Upgrade Successfully

Warning:

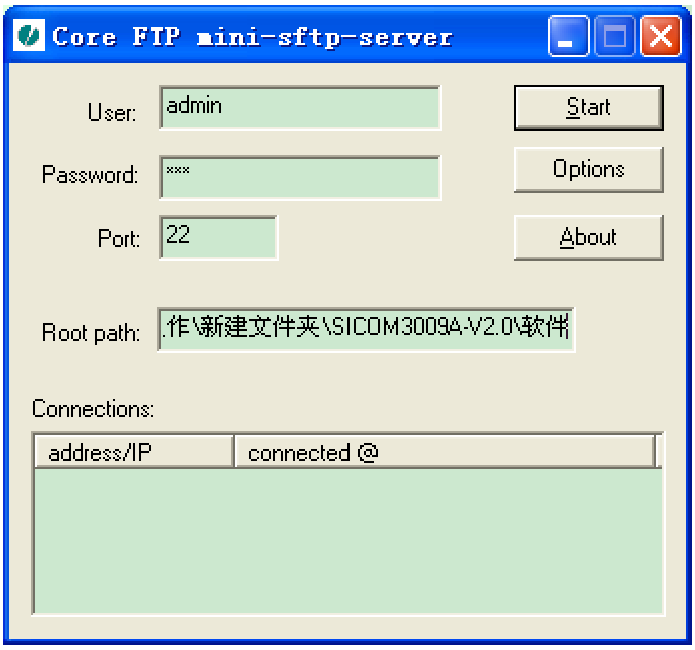
- When update completes, activate the software version and reboot the device to make the new version take effect.
- If update fails, do not reboot the device to avoid the loss of software file and startup anomaly.

3.3.4.2 Firmware Upgrade by SFTP

The Secure File Transfer Protocol (SFTP) is an SSH-based file transfer protocol. It provides encrypted file transfer to ensure security.

The following example uses MSFTP to describe the configuration of the SFTP server and the firmware upgrade process.

1. Add an SFTP user, as shown in Figure 29. Enter the user and password, for example, admin and 123. Set the port number to 22. Enter the path for saving the firmware version file in Root path.



Core FTP mini-sftp-server

User: admin

Password: ***

Port: 22

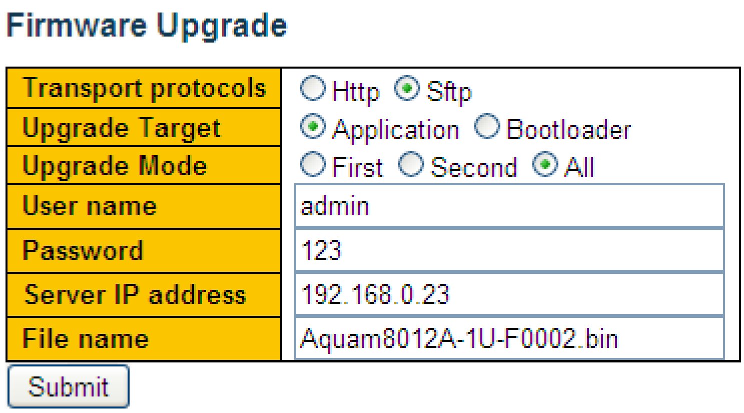
Root path: .作\新建文件夹\SICOM3009A-V2.0\软件

Connections:

address/IP	connected @

Figure 29 Adding an SFTP User

2. Upgrade firmware, as shown in Figure 30.



Firmware Upgrade

Transport protocols	○ Http ● Sftp
Upgrade Target	● Application ○ Bootloader
Upgrade Mode	○ First ○ Second ● All
User name	admin
Password	123
Server IP address	192.168.0.23
File name	Aquam8012A-1U-F0002.bin

Figure 30 Upgrade Firmware- SFTP

Upgrade Target

Options: Application/Bootloader

Function: Select the upgrade target.

Upgrade Mode

Options: First/Second/All

Description: Two firmware versions can be downloaded to the switch, and they can be the same or different. All indicates version 1 and version 2.

{ User name, Password }

Range: { 1~63 characters, 1~63 characters }

Description: Input the user name and password created on SFTP server.

Server IP address

Format: A.B.C.D

Description: Configure the IP address of the SFTP server.

File name

Range: 1~63 characters

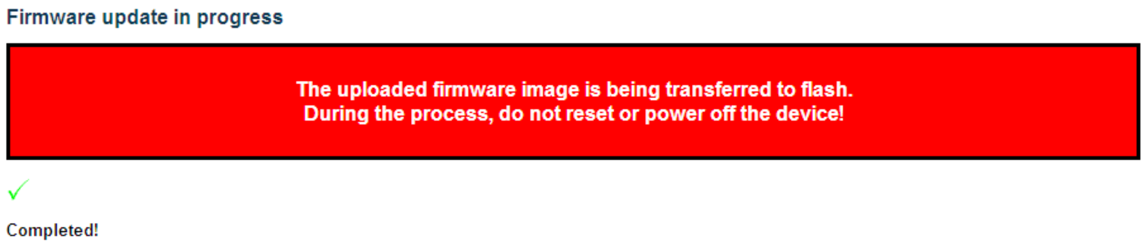
Description: Configure the firmware update file name stored on SFTP server.

Warning:

The file name must contain an extension. Otherwise, the upgrade may fail.

3. When the update is completed as shown in Figure 31, please activate the software version and reboot the device, open the System Information page to check whether the

update succeeded and the new version is active.



Firmware update in progress

The uploaded firmware image is being transferred to flash.
During the process, do not reset or power off the device!

✓

Completed!

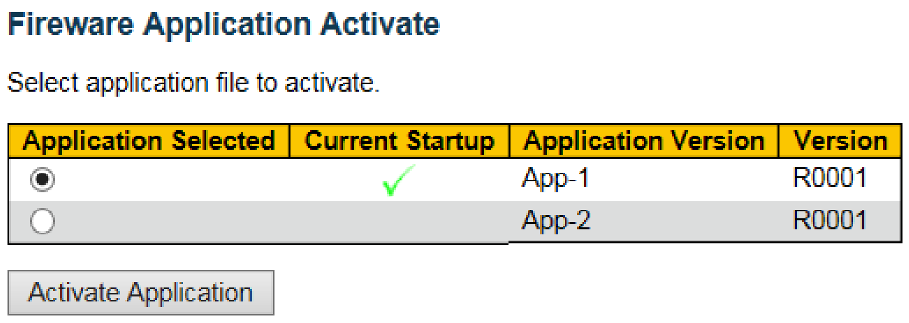
Figure 31 Upgrade Successfully

Warning:

- ➢ In the firmare upgrade process, keeps the SFTP server running.
- ➢ When update completes, reboot the device to activate the new version.
- ➢ If update fails, do not reboot the device to avoid the loss of software file and startup anomaly.

3.3.5 Firmware Application Activate

Activate the firmware application, as shown in Figure 32.



Fireware Application Activate

Select application file to activate.

Application Selected	Current Startup	Application Version	Version
●	✓	App-1	R0001
○		App-2	R0001

Figure 32 Activate the Firmware Application

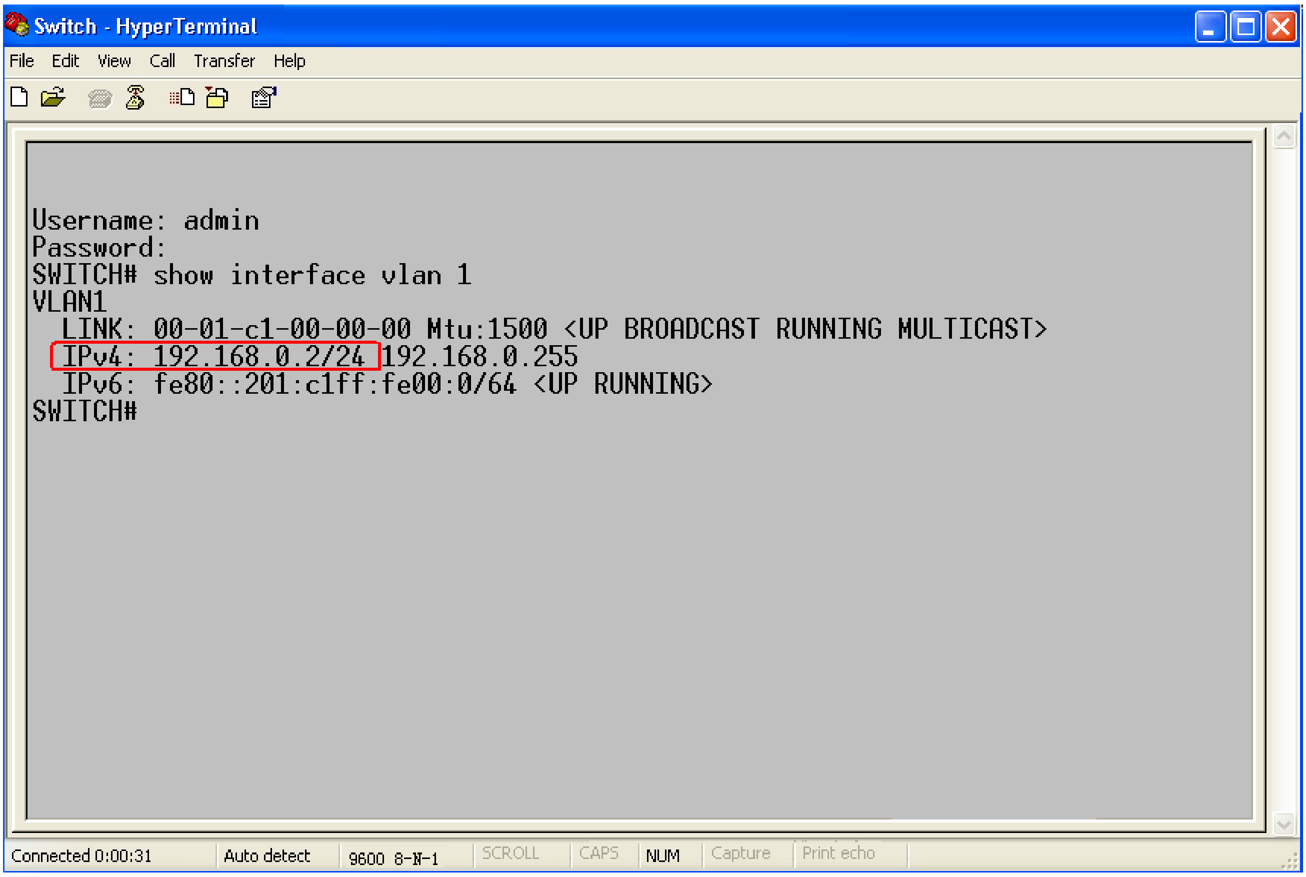
Select one version and click <Activate Application> button, configuring the version to be active version that is the next startup version. Only one can be active version at a time. Current Startup indicates the version is current running version.

3.4 IP Configuration

3.4.1 IP Address Configuration

1. View the switch IP address by using the console port.

Log in to the switch CLI through the console port. Run the "**show interface vlan 1**" command in the Privileged mode to view the switch IP address, as shown in the red circle of Figure 33.



```
Username: admin
Password:
SWITCH# show interface vlan 1
VLAN1
  LINK: 00-01-c1-00-00-00 Mtu:1500 <UP BROADCAST RUNNING MULTICAST>
  IPv4: 192.168.0.2/24 192.168.0.255
  IPv6: fe80::201:c1ff:fe00:0/64 <UP RUNNING>
SWITCH#
```

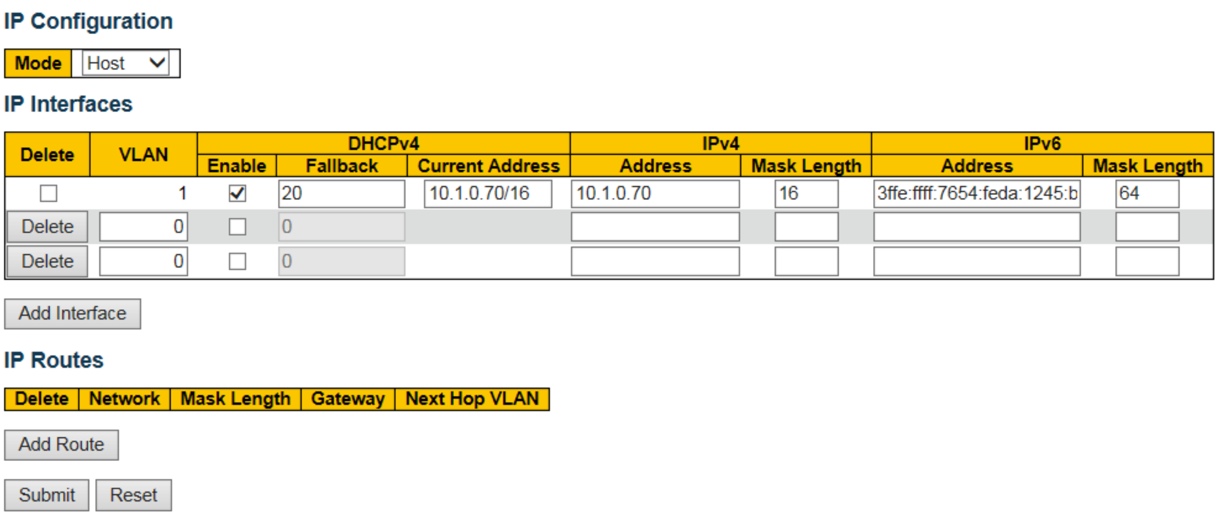
Figure 33 Displaying IP Address

2. Create IP interface.

Hosts in different VLANs cannot communicate with each other. Their communication packets need to be forwarded by a router or Layer 3 switch through a IP interface. This series switches support IP interfaces, which are virtual Layer 3 interfaces used for inter-VLAN communication. You can create one IP interface for each VLAN. The interface is used for forwarding Layer 3 packets of the ports in the VLAN.

3. Configure IP address

Switch IP address can be manually configured or automatically obtained, as shown in Figure 34.



IP Configuration

Mode	Host

IP Interfaces

Delete	VLAN	DHCPv4			IPv4		IPv6	
		Enable	Fallback	Current Address	Address	Mask Length	Address	Mask Length
□	1	☑	20	10.1.0.70/16	10.1.0.70	16	3ffe:ffff:7654:feda:1245:b	64
Delete	0	□	0					
Delete	0	□	0					

IP Routes

Delete	Network	Mask Length	Gateway	Next Hop VLAN

Figure 34 Configure IP Address

Delete

Function: Select the IP interface to be deleted.

VLAN

Function: Configure VLAN attribute of the IP interface, only ports in this VLAN will be able to access the IP interface.

DHCPv4-Enable

Options: Enable/Disable

Function: Disable DHCPv4, configure IP address and mask manually; enable DHCPv4, switch (as DHCP client) automatically obtains an IP address through DHCP. There should be a DHCP server in the network to assign IP addresses and mask to clients.

DHCPv4-Fallback

Range: 0~4294967295s

Function: If the value is not zero, the switch obtains the IP address attempt time over the Dynamic Host Configuration Protocol (DHCP). In this case, the IP address needs to be configured manually. After the attempt time expires, the IP address that is manually configured takes effect. If the value is **0**, the switch repeatedly tries to acquire an IP address till it obtains an IP address over DHCP. In this case, the IP address does not need to be manually configured.

DHCPv4-Current Address

Function: Display the IP address and mask length that is automatically acquired from the

DHCP server. If the switch fails to acquire an IP address over DHCP during the attempt time, the IP address and mask length that are manually configured are displayed in **Current Address**.

IPv4-Address

Format: A.B.C.D

Function: Manually configure IP address .

IPv4-Mask Length

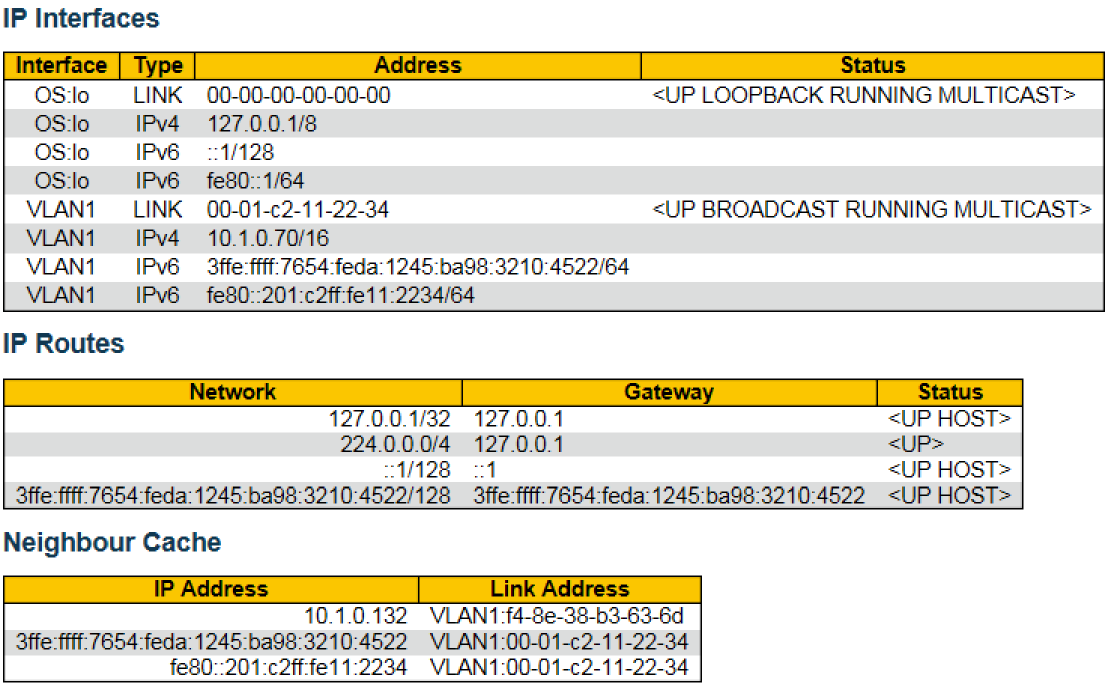
Function: The subnet mask is a number with a length of 32 bits and consists of a string of 1 and a string of 0. "1" corresponds to network number fields and subnet number fields, while "0" corresponds to host number fields. Mask length is the number of “1” in subnet mask.

Click <Add Interface> to add a new IP interface, a maximum of 8 interfaces is supported.

Caution:

- Each IP interface supports one IP address.
- IP addresses of different network segments should be configured for different IP interfaces.

4. View IP interfaces, as shown in Figure 35.



IP Interfaces

Interface	Type	Address	Status
OS:lo	LINK	00-00-00-00-00-00	<UP LOOPBACK RUNNING MULTICAST>
OS:lo	IPv4	127.0.0.1/8	
OS:lo	IPv6	::1/128	
OS:lo	IPv6	fe80::1/64	
VLAN1	LINK	00-01-c2-11-22-34	<UP BROADCAST RUNNING MULTICAST>
VLAN1	IPv4	10.1.0.70/16	
VLAN1	IPv6	3ffe:ffff:7654:feda:1245:ba98:3210:4522/64	
VLAN1	IPv6	fe80::201:c2ff:fe11:2234/64	

IP Routes

Network	Gateway	Status
127.0.0.1/32	127.0.0.1	<UP HOST>
224.0.0.0/4	127.0.0.1	<UP>
::1/128	::1	<UP HOST>
3ffe:ffff:7654:feda:1245:ba98:3210:4522/128	3ffe:ffff:7654:feda:1245:ba98:3210:4522	<UP HOST>

Neighbour Cache

IP Address	Link Address
10.1.0.132	VLAN1:f4-8e-38-b3-63-6d
3ffe:ffff:7654:feda:1245:ba98:3210:4522	VLAN1:00-01-c2-11-22-34
fe80::201:c2ff:fe11:2234	VLAN1:00-01-c2-11-22-34

Figure 35 View IP Interfaces

3.4.2 ARP

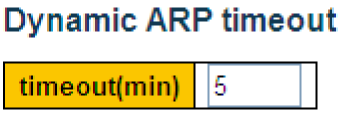
3.4.2.1 Introduction

The Address Resolution Protocol (ARP) resolves the mapping between IP addresses and MAC addresses by the address request and response mechanism. The switch can learn the mapping between IP addresses and MAC addresses of other hosts on the same network segment. It also supports static ARP entries for specifying mapping between IP addresses and MAC addresses. Dynamic ARP entries periodically age out, ensuring consistency between ARP entries and actual applications.

This series switches provide not only Layer 2 switching function, but also the ARP function for resolving the IP addresses of other hosts on the same network segment, enabling the communication between the NMS and managed hosts.

3.4.2.2 Web Configuration

1. Configure ARP aging time, as shown in Figure 36.



Dynamic ARP timeout

timeout(min) 5

Figure 36 Configuring Aging Time

timeout

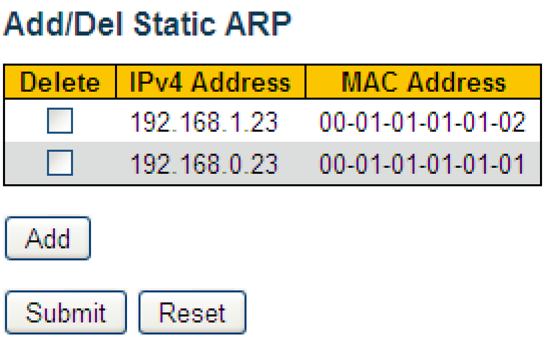
Range: 0 ~ 60min

Default: 5min

Function: Configure ARP aging time, when aging time is set to 0, aging is prohibited.

Description: ARP aging time is the duration from when a dynamic ARP entry is added to the table to when the entry is deleted from the table.

2. Add static ARP entry, as shown in Figure 37.



Add/Del Static ARP

Delete	IPv4 Address	MAC Address
□	192.168.1.23	00-01-01-01-01-02
□	192.168.0.23	00-01-01-01-01-01

Figure 37 Adding Static ARP Entry

ARP

Portfolio: {IP address, MAC address}

Format: {A.B.C.D, HH-HH-HH-HH-HH-HH} (H is a hexadecimal number.)

Function: Configure static ARP entry.

Caution:

In general, the switch automatically learns ARP entries. Manual configuration is not required.

Click <Add> to add a new static ARP entry, a maximum of 128 static ARP entries is supported.

3.4.3 DHCP Configuration

With the continuous expansion of network scale and the growing of network complexity, under the conditions of the frequent movement of computers (such as laptops or wireless network) and the computers outnumbering the allocable IP addresses, the BootP protocol that is specially for the static host configuration has become increasingly unable to meet actual needs. For fast access and exit network and improving the utilization ratio of IP address resources, we do need to develop an automatic mechanism based on BootP to assign IP addresses. DHCP (Dynamic Host Configuration Protocol) was introduced to solve these problems.

DHCP employs a client-server communication model. The client sends a configuration request to the server, and then the server replies configuration parameters such as an IP address to the client, achieving the dynamic configuration of IP addresses. The structure of a DHCP typical application is shown in Figure 38.

无法显示链接的图像。该文件可能已被移动、重命名或删除。请验证该链接是否指向正确的文件和位置。

Figure 38 DHCP Typical Application

Caution:

In the process of dynamic obtainment of IP addresses, the messages are transmitted in the way of broadcast, so it is required that the DHCP client and the DHCP server are in a same segment. If they are in the different segments, the client can communicate with the server via a DHCP relay to get IP addresses and other configuration parameters.

DHCP supports two types of IP address allocation mechanisms.

Static allocation: the network administrator statically binds fixed IP addresses to few specific clients such as a WWW server and sends the binding IP addresses to clients by DHCP. The tenancy term for static allocation is permanent.

Dynamic allocation: DHCP server dynamically allocates an IP address to a client. This allocation mechanism can allocate a permanent IP address or an IP address with a limited lease period to a client. When the lease expires, the client needs to reapply an IP address.

The network administrator can choose a DHCP allocation mechanism for each client.

3.4.3.1 DHCP Server Configuration

3.4.3.1.1 Introduction

DHCP server is a provider of DHCP services. It uses DHCP messages to communicate with DHCP client to allocate a suitable IP address to the client and assign other network parameters to the client as required. In the following conditions, the DHCP server generally is used to allocate IP addresses.

- Large network scale. The workload of manual configuration is heavy and it is hard to manage the entire network.
- The hosts outnumber the assignable IP addresses, and it is unable to allocate a fixed IP address to each host.
- Only a few hosts in the network need fixed IP addresses.

3.4.3.1.2 DHCP Address Pool

The DHCP server selects an IP address from an address pool and allocates it together with other parameters to the client. The IP address allocation sequence is as follows:

1. The IP address statically bound to the client MAC address.

2. The IP address that is recorded in the DHCP server that it was ever allocated to the client.

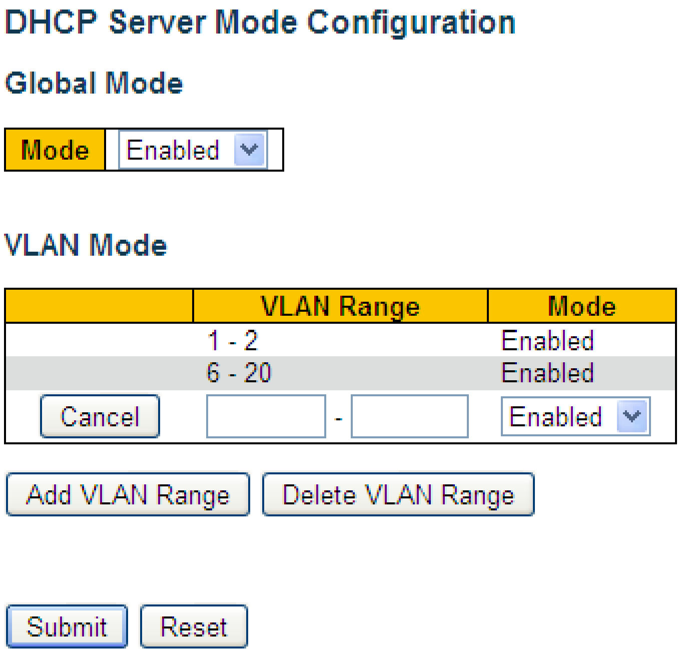
3. The IP address that is specified in the request message sent from the client.

4. The first allocable IP address found in an address pool.

5. If there is no available IP address, check the IP address whose lease expires and that had conflicts in order. If found, allocate the IP address. If not, no process.

3.4.3.1.3 Web Configuration

1. Enable DHCP server, as shown in Figure 39.



DHCP Server Mode Configuration

Global Mode

Mode	Enabled

VLAN Mode

	VLAN Range	Mode
	1 - 2	Enabled
	6 - 20	Enabled
Cancel	-	Enabled

Figure 39 Enable DHCP Server

Global Mode

Options: Disabled/Enabled

Default: Disabled

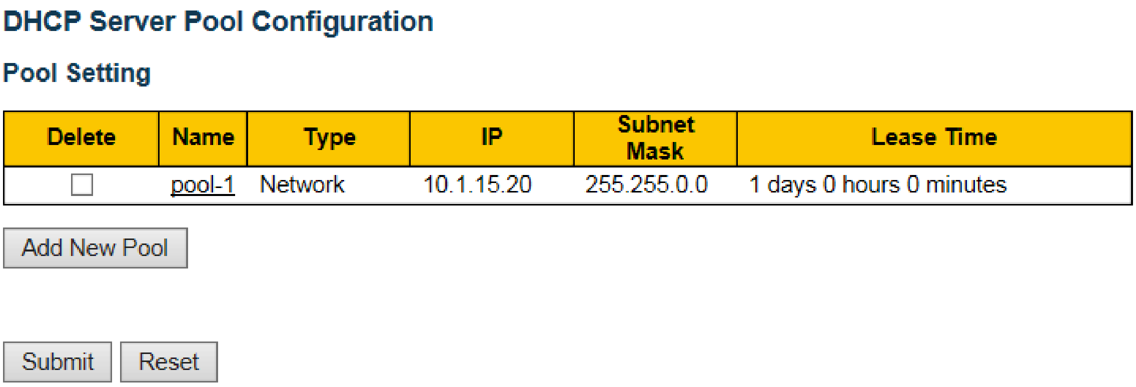
Function: Select the current switch to the DHCP server to allocate an IP address to a client or not.

{VLAN Range, Mode}

Range: {1~4095, Disabled/Enabled}

Function: If the VLAN of a client that applies for an IP address is set to Enabled, the DHCP server allocates an IP address to the client. Otherwise, the DHCP server does not allocate an IP address to the client.

2. Create DHCP address pool, as shown in Figure 40.



DHCP Server Pool Configuration

Pool Setting

Delete	Name	Type	IP	Subnet Mask	Lease Time
□	pool-1	Network	10.1.15.20	255.255.0.0	1 days 0 hours 0 minutes

Figure 40 Create DHCP Address Pool

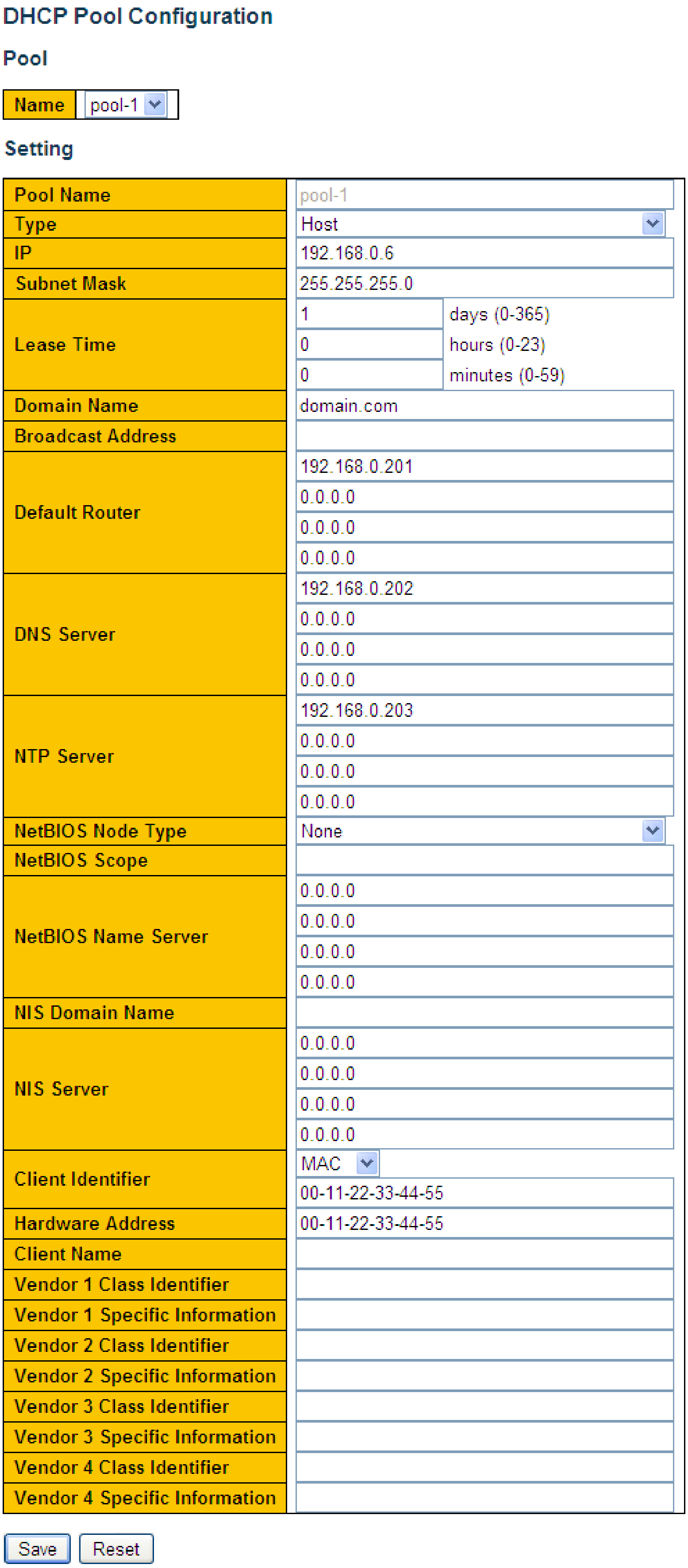
Name

Range: 1~32 characters

Function: configure the name of the IP address pool.

Click <Add New Pool> to create a new DHCP address pool.

3. Configure the DHCP address pool, click <Name> in Figure 40 to configure the DHCP address pool, as shown in Figure 41.



DHCP Pool Configuration

Pool

Name	pool-1

Setting

Pool Name	pool-1
Type	Host
IP	192.168.0.6
Subnet Mask	255.255.255.0
Lease Time	1 days (0-365) 0 hours (0-23) 0 minutes (0-59)
Domain Name	domain.com
Broadcast Address	
Default Router	192.168.0.201 0.0.0.0 0.0.0.0 0.0.0.0
DNS Server	192.168.0.202 0.0.0.0 0.0.0.0 0.0.0.0
NTP Server	192.168.0.203 0.0.0.0 0.0.0.0 0.0.0.0
NetBIOS Node Type	None
NetBIOS Scope	
NetBIOS Name Server	0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
NIS Domain Name	
NIS Server	0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
Client Identifier	MAC 00-11-22-33-44-55
Hardware Address	00-11-22-33-44-55
Client Name	
Vendor 1 Class Identifier	
Vendor 1 Specific Information	
Vendor 2 Class Identifier	
Vendor 2 Specific Information	
Vendor 3 Class Identifier	
Vendor 3 Specific Information	
Vendor 4 Class Identifier	
Vendor 4 Specific Information	

Figure 41 Configure IP Address Pool

Name

Function: select a created pool name.

Type

Options: None/Network/Host

Default: None

Function: Configure the address pool type. Network: the switch dynamically allocates IP addresses to multiple DHCP clients. Host: the switch supports static allocation of IP addresses to special DHCP clients.

{IP, Subnet Mask}

Function: Network indicates that you can configure the range of the IP address pool, and the address range is determined by the subnet mask. The subnet mask is a number with a length of 32 bits and consists of a string of 1 and a string of 0. "1" corresponds to network number fields and subnet number fields, while "0" corresponds to host number fields. It is generally configured to 255.255.255.0.

Host indicates that you can configure the IP address of the client statically bounded. Static IP address allocation is implemented by bounding the MAC address and IP address of the client. When the client with this MAC address requests for IP address, the DHCP server finds the IP address corresponding to the MAC address of the client and allocates the IP address to the client. The priority of this allocation mode is higher than that of dynamic IP address allocation, and the tenancy term is permanent.

Lease Time

Range: 0 day 0 hour 0 minute~365 days 23 hours 59 minutes

Default: 1 day 0 hour 0 minute

Description: Configure lease timeout of dynamic allocation. For different address pools, DHCP server can set different address lease time, but the addresses in the same DHCP address pool have the same lease time.

Domain Name

Range: 1~36 characters

Function: Configure the domain name of the IP address pool. When allocating an IP address to a client, send the domain name suffix to the client too.

Broadcast Address

Format: A.B.C.D

Function: Configure the client broadcast address allocated by DHCP server.

Default Router

Format: A.B.C.D

Function: Configure the client gateway address allocated by DHCP server.

Explanation: when the DHCP client visits the host that is in the different segment, the data must be forwarded via gateways. When the DHCP server allocates IP addresses to clients, it can specify gateway addresses at the same time. DHCP address pool can configure max 4 gateways.

DNS Server

Format: A.B.C.D

Function: Configure the client DNS server address allocated by DHCP server.

Explanation: When visiting the network host via a domain name, the domain name needs to be resolved to an IP address, which is realized by DNS (Domain Name System). In order to let a DHCP client visit a network host via a domain name, when the DHCP server allocates IP addresses to clients, it can specify IP addresses of domain name servers at the same time. DHCP address pool can configure max 4 DNS servers.

NTP Server

Format: A.B.C.D

Function: Configure the client NTP server address allocated by DHCP server.

NetBIOS Node Type

Options: None/B-node/P-node/M-node/H-node

Default: None

Function: Configure the client NetBIOS node type allocated by DHCP server. When the DHCP client uses the NetBIOS protocol for communication on the network, a mapping must be established between the host name and IP address. Different node types obtain the mapping in different modes.

Description: The B-node obtains the mapping in broadcast mode. The P-node obtains the mapping by sending a unicast packet to communicate with the WINS server. The M-node obtains the mapping by sending a broadcast packet the first time. If the M-node fails to obtain the mapping the first time, it obtains the mapping by sending a unicast packet to communicate with the WINS server the second time. The H-node obtains the mapping by sending a unicast packet to communicate with the WINS server the first time. If the H-node fails to obtain the mapping the first time, it obtains the mapping by sending a broadcast packet the second time.

NetBIOS Scope

Range: 1~36 characters

Function: Configure the NetBIOS name.

NetBIOS Name Server

Format: A.B.C.D

Function: Configure the client WINS server address allocated by the DHCP server.

Explanation: For the client running a Microsoft Windows operating system (OS), the Windows Internet Naming Service (WINS) server provides the service of resolving a host name into an IP address for the host that uses the NetBIOS protocol for communication. Therefore, most Windows OS-based clients require WINS configuration. To enable the DHCP client to resolve a host name into an IP address, specify the WINS server address when the DHCP server allocates an IP address to the client. DHCP address pool can configure max 4 WINS servers.

NIS Domain Name

Range: 1~36 characters

Function: Configure the client NIS domain name allocated by DHCP server.

NIS Server

Format: A.B.C.D

Function: Configure the client NIS server address allocated by DHCP server.

Client Identifier

Options: None/FQDN/MAC

Default: None

Function: When the pool type is host, specify client's unique identifier

Description: MAC, configure the static binding client MAC address; FQDN, configure the static binding client full name domain name, that is, the host name plus the full path.

Hardware Address

Format: HH-HH-HH-HH-HH-HH (H is a hexadecimal number)

Function: When the pool type is host, configure the MAC address of the client statically bounded.

Client Name

Range: 1~32 characters

Function: Configure client user name configure client user name.

Vendor i Class Identifier

Range: 1~64 characters

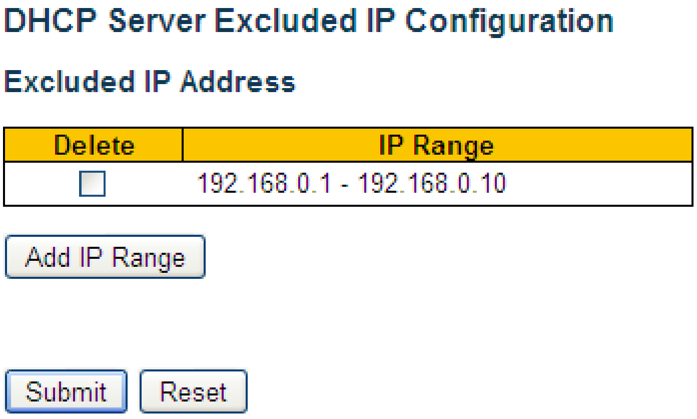
Function: Configure the client Vendor Class Identifier allocated by DHCP server.

Vendor i Specific Information

Range: 1~64 hexadecimal numbers

Function: Configure the client Vendor Specific Information allocated by DHCP server.

4. Configure excluded IP addresses(IP addresses are not allocated dynamically in the DHCP address pool), as shown in Figure 42.



DHCP Server Excluded IP Configuration

Excluded IP Address

Delete	IP Range
□	192.168.0.1 - 192.168.0.10

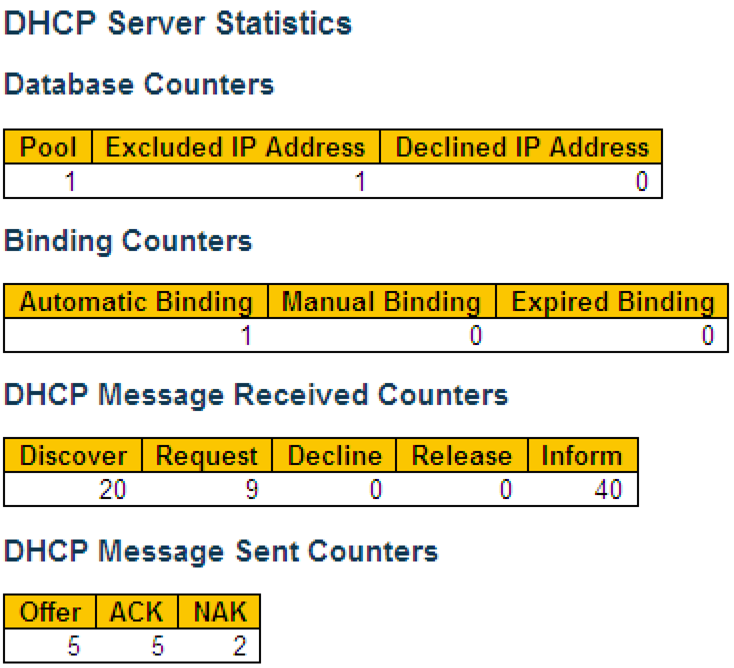
Figure 42 Configure Excluded IP Addresses

IP Range

Function: Configure the range of IP addresses are not allocated dynamically in the DHCP address pool. When allocating IP addresses, the DHCP server must eliminate the occupied IP address (for example, IP addresses of the gateway and DNS server). Otherwise, the same IP address may be allocated to two clients, causing IP address conflict.

Click <Add IP Range> to configure the range of IP addresses are not allocated dynamically.

5. View DHCP server statistics information, as shown in Figure 43.



DHCP Server Statistics

Database Counters

Pool	Excluded IP Address	Declined IP Address
1	1	0

Binding Counters

Automatic Binding	Manual Binding	Expired Binding
1	0	0

DHCP Message Received Counters

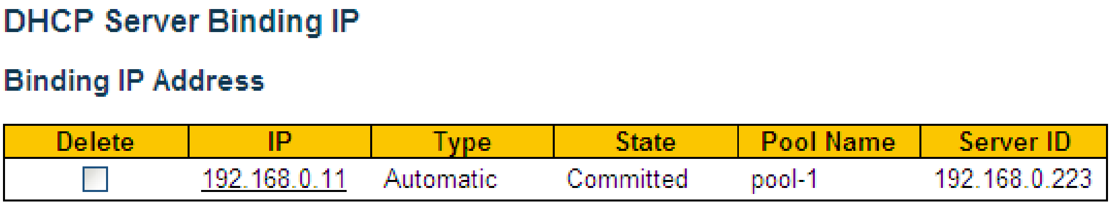
Discover	Request	Decline	Release	Inform
20	9	0	0	40

DHCP Message Sent Counters

Offer	ACK	NAK
5	5	2

Figure 43 View DHCP Server Statistics Information

6. View information about IP addresses allocated by the DHCP server, as shown in Figure 44.



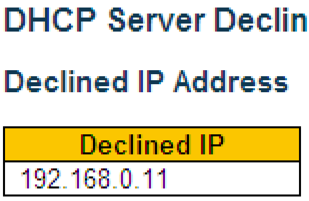
DHCP Server Binding IP

Binding IP Address

Delete	IP	Type	State	Pool Name	Server ID
□	192.168.0.11	Automatic	Committed	pool-1	192.168.0.223

Figure 44 View Information About IP Addresses Allocated by the DHCP Server

7. View the IP addresses declined by DHCP clients , as shown in Figure 45.



DHCP Server Declined IP

Declined IP Address

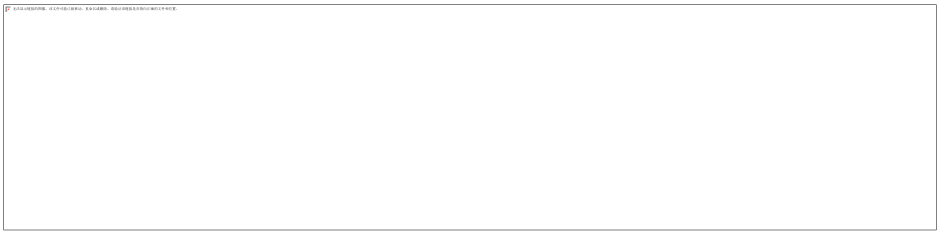
Declined IP
192.168.0.11

Figure 45 View the IP addresses Declined by DHCP Clients

When a client detects that an IP address allocated by the server conflicts with a static IP address in the same network segment, it sends a decline packet to the server to reject this IP address. The server records the IP address rejected by the client, and will not allocate this IP address to other clients within a certain period of time.

3.4.3.1.4 Typical Configuration Example

As Figure 46 shows, switch A works as a DHCP server and switch B works as a DHCP client. The port 3 of Switch A connects with the port 4 of Switch B. The client sends out IP address request messages and the server can allocate an IP address to the client in two ways. The excluded IP address range is 192.168.0.1~192.168.0.10 when DHCP server dynamically allocates IP address.



无法显示链接的图像。该文件可能已被移动、重命名或删除。请验证该链接是否指向正确的文件和位置。

Figure 46 DHCP Typical Configuration Example

Statically allocate IP address

➢ Switch A configuration:

1. Enable DHCP server status in correspond VLANs, as shown in Figure 39.

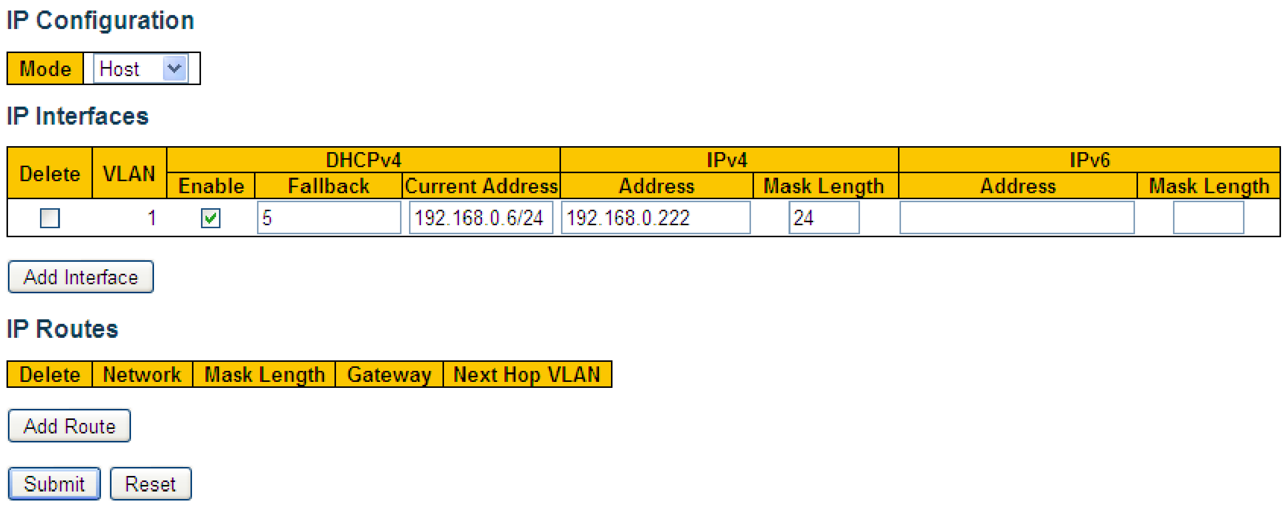
2. Create a DHCP IP pool: pool-1, as shown in Figure 40.

3. Set the pool type as Host; IP address as 192.168.0.6; mask as 255.255.255.0; Bind the MAC address of switch B: 00-11-22-33-44-55, as shown in Figure 41.

➢ Switch B configuration:

1. Set switch B automatically obtains an IP address through DHCP.

2. The switch B obtains the IP address of 192.168.0.6 and the subnet mask of 255.255.255.0 from the DHCP server, as shown in Figure 47.



IP Configuration

Mode	Host

IP Interfaces

Delete	VLAN	DHCPv4			IPv4		IPv6	
		Enable	Fallback	Current Address	Address	Mask Length	Address	Mask Length
☐	1	☑	5	192.168.0.6/24	192.168.0.222	24		

IP Routes

Delete	Network	Mask Length	Gateway	Next Hop VLAN

Figure 47 DHCP Client Obtain IP Address-1

Dynamically allocate IP address

➢ Switch A configuration:

1. Enable DHCP server status in correspond VLANs, as shown in Figure 39.

2. Create a DHCP IP pool: pool-1, as shown in Figure 40.

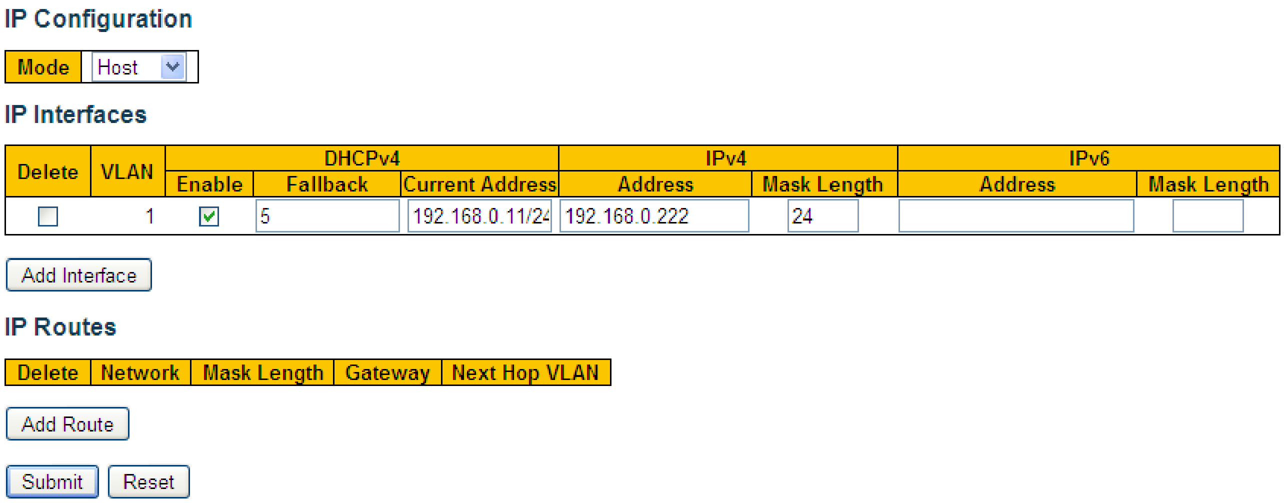
3. Set the pool type as Network; IP address as 192.168.0.6; mask as 255.255.255.0, as shown in Figure 41.

4. Configure excluded IP address range as 192.168.0.1~192.168.0.10, as shown in Figure 42.

➢ Switch B configuration:

1. Set switch B automatically obtains an IP address through DHCP.

2. DHCP server searches the assignable IP addresses in the address pool in order and allocates the first found assignable IP address and other network parameters to Switch B. The subnet mask is 255.255.255.0, as shown in Figure 48.



IP Configuration

Mode	Host

IP Interfaces

Delete	VLAN	DHCPv4			IPv4		IPv6	
		Enable	Fallback	Current Address	Address	Mask Length	Address	Mask Length
☐	1	☑	5	192.168.0.11/24	192.168.0.222	24		

IP Routes

Delete	Network	Mask Length	Gateway	Next Hop VLAN

Figure 48 DHCP Client Obtain IP Address-2

3.4.3.2 DHCP Snooping

3.4.3.2.1 Introduce

DHCP Snooping is a monitoring function of DHCP services on layer 2 and is a security feature of DHCP, ensuring the security of the client further. The DHCP Snooping security mechanism can control that only the trusted port can forward the request message of the DHCP client to the legal server, meanwhile, it can control the source of the response message of the DHCP server, ensuring the client to obtain an IP address from the valid server and preventing the fake or invalid DHCP server from allocating IP addresses or other configuration parameters to other hosts.

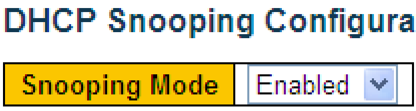
DHCP Snooping security mechanism divides port to trusted port and untrusted port.

Trusted port: it is the port that connects with the valid DHCP server directly or indirectly. Trusted port normally forwards the request messages of DHCP clients and the response messages of DHCP servers to guarantee that DHCP clients can obtain valid IP addresses.

Untrusted port: it is the port that connects with the invalid DHCP server. Untrusted port does not forward the request messages of DHCP clients and the response messages of DHCP servers to prevent DHCP clients from obtaining invalid IP addresses.

3.4.3.2.2 Web Configuration

1. Enable DHCP Snooping function, as shown in Figure 49.



DHCP Snooping Configuration

Snooping Mode	Enabled

Figure 49 DHCP Snooping State

DHCP Snooping Mode

Options: Enable/Disable

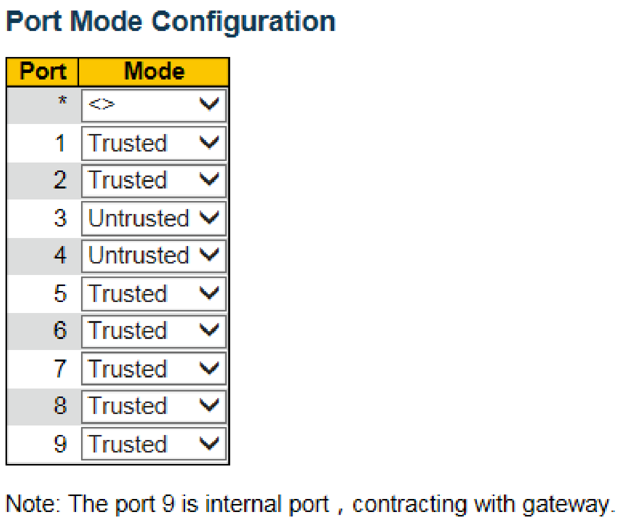
Default: Disable

Function: Enable/Disable switch DHCP Snooping function.

Caution:

The switch working as DHCP server and client cannot enable DHCP Snooping function.

2. Configure trusted ports, as shown in Figure 50.



Port Mode Configuration

Port	Mode
*	<>
1	Trusted
2	Trusted
3	Untrusted
4	Untrusted
5	Trusted
6	Trusted
7	Trusted
8	Trusted
9	Trusted

Note: The port 9 is internal port , contracting with gateway.

Figure 50 Configure Trust Port

Mode

Options: Trusted/Untrusted

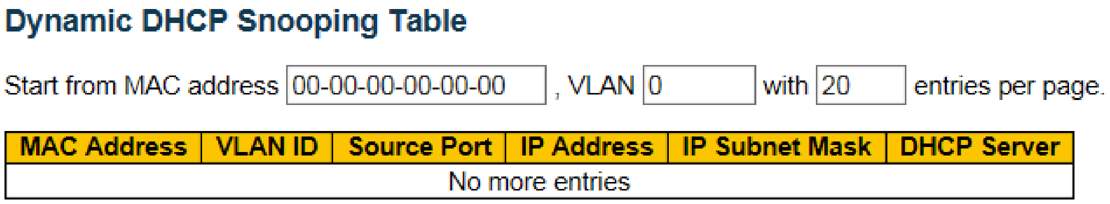
Default: Trusted

Function: set the port to a trusted port or an untrusted port. The ports that connect with valid DHCP servers directly or indirectly are trusted ports.

Caution:

The trusted port configuration and Port Trunk is mutually exclusive. The port joining in a trunk group cannot be set to a trusted port. The trusted port cannot join in a trunk group.

3. View the Dynamic DHCP Snooping Table, as shown in the following figure.



Dynamic DHCP Snooping Table

Start from MAC address 00-00-00-00-00-00 , VLAN 0 with 20 entries per page.

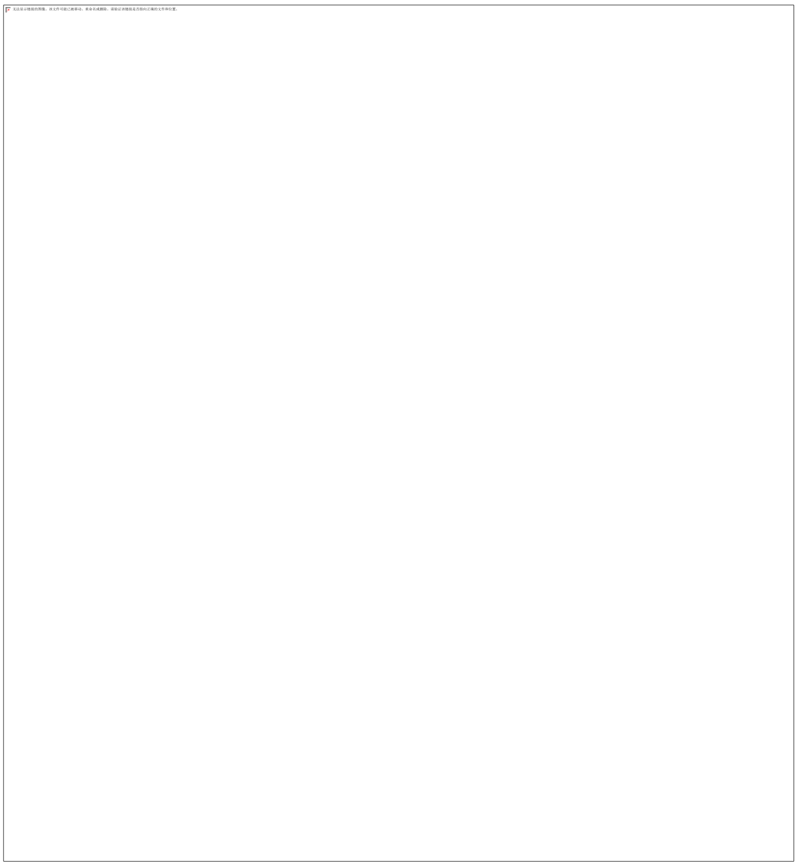
MAC Address	VLAN ID	Source Port	IP Address	IP Subnet Mask	DHCP Server
No more entries					

Figure 51 Dynamic DHCP Snooping Table

Statistics Displays the current number of DHCP servers to send and receive data.

3.4.3.2.3 Typical Configuration Example

As Figure 52 shows, the DHCP client requests an IP address from the DHCP server. An unauthorized DHCP server exists in the network. Set port 1 to a trusted port by DHCP Snooping to forward the request message of the DHCP client to the DHCP server and forward the response message of the DHCP server to the DHCP client. Set port 3 to an untrusted port that cannot forward the request message of the DHCP client and the response message of the unauthorized DHCP server, ensuring that the client can obtain a valid IP address from the valid DHCP server.



无法显示链接的图像。该文件可能已被移动、重命名或删除。请验证该链接是否指向正确的文件和位置。

Figure 52 DHCP Snooping Typical Configuration Example

Switch B configuration:

➢ Enable DHCP Snooping function, as shown in Figure 49.

➢ Set the port 1 of switch B to a trusted port and set the port 3 to an untrusted port, as shown in Figure 50.

3.4.3.3 Option 82 Configuration

Option 82 (Relay Agent Information Entry) records the client information. When the Option 82 supported DHCP Snooping receives the request message from the DHCP client, it add the corresponding Option 82 field into the messages and then forward the message to the DHCP server. The server supporting Option 82 can flexibly allocate addresses according to the Option 82 message.

Once Option 82 is enabled, the Option 82 field will be added into the message. The Option 82 field of this series switches contains two sub-options: sub-option 1 (Circuit ID) and sub-option 2 (Remote ID). The formats of two sub-options are shown below:

➢ Sub-option 1 contains the VLAN ID and number of the port that receives the request message from the DHCP client, as shown in Table 2.

Table 2 Sub-option 1 Field Format

Sub-option type（0x01）	Length（0x04）	VLAN ID	Port number
One byte	One byte	Two bytes	Two bytes

Sub-option type: the type of the sub-option 1 is 1.

Length: the number of bytes that VLAN ID and Port number occupy.

VLAN ID: On DHCP Snooping device, the VLAN ID of the port that receives the request message from the DHCP client.

Port number: On DHCP Snooping device, the number of the port that receives the request message from the DHCP client.

➢ The content of Sub-option 2 is the MAC address of the DHCP Snooping device that receives the request message from the DHCP client, as shown in Table 3.

Table 3 Sub-option 2 Field Format-MAC Address

Sub-option type（0x02）	Length（0x06）	MAC 地址
One byte	One byte	6 bytes

Sub-option type: the type of the sub-option 2 is 2

Length: the number of bytes that sub-option2 content occupies. MAC address occupies 6 bytes and character string occupies 16 bytes.

MAC address: the content of sub-option2 is the MAC address of the DHCP Snooping device that receives the request message from the DHCP client.

3.4.3.3.1 DHCP Snooping Supports Option 82 Function

1 Introduction

If DHCP Snooping device supports Option 82 function, when the DHCP Snooping receives a DHCP request message, it will process the request message according to whether the message contains Option 82 and the client policy, and then forward the processed message to the DHCP server. The specific processing method is shown in Table 4.

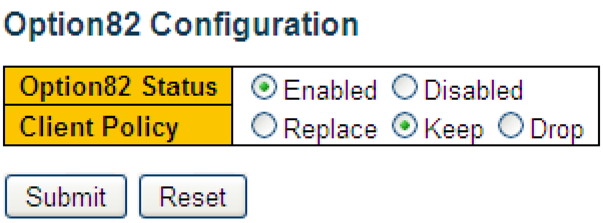
Table 4 Processing Modes for Request Messages (DHCP Snooping)

Receive the request message from the DHCP client	**Configuration policy**	**DHCP Snooping device processing the request message**
The request message contains Option 82	Drop	Drop the request message
	Keep	Keep the message format unchanged and forward the message
	Replace	Replace the Option 82 field in the message with the Option 82 field of the Snooping device and forward the new message
The request message does not contain Option 82	Drop/Keep/Replace	Add the Option 82 field of the Snooping device into the message and forward it

When the DHCP Snooping device receives the response message from the DHCP server, if the message contains Option 82 field, remove the Option 82 field and forward the message to the client

2 Web Configuration

DHCP Snooping Option 82 configuration is shown in Figure 53.



Option82 Configuration

Option82 Status	● Enabled ○ Disabled
Client Policy	○ Replace ● Keep ○ Drop

Figure 53 DHCP Snooping Option82 Configuration

Option82 Status

Options: Enable/Disable

Default: Disable

Function: Enable/Disable Option82 function on DHCP Snooping device.

Client Policy

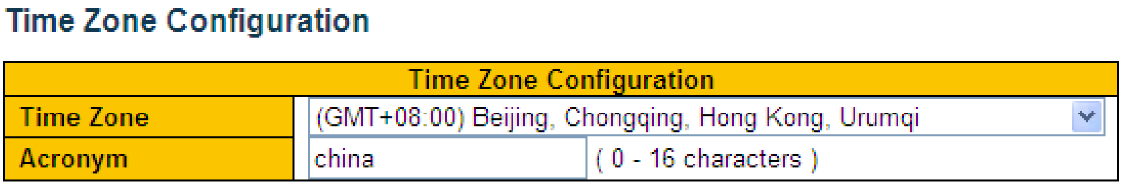
Options: Drop/Replace/Keep

Default: Replace

Function: Configure client policy. The DHCP Snooping device processes the request message sent from the Client according to Client Policy, as shown in Table 4.

3.5 Clock System

1. Configure the time zone, as shown in Figure 54.



Time Zone Configuration

Time Zone Configuration	
Time Zone	(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi
Acronym	china (0 - 16 characters)

Figure 54 Configure the Time Zone

Time Zone

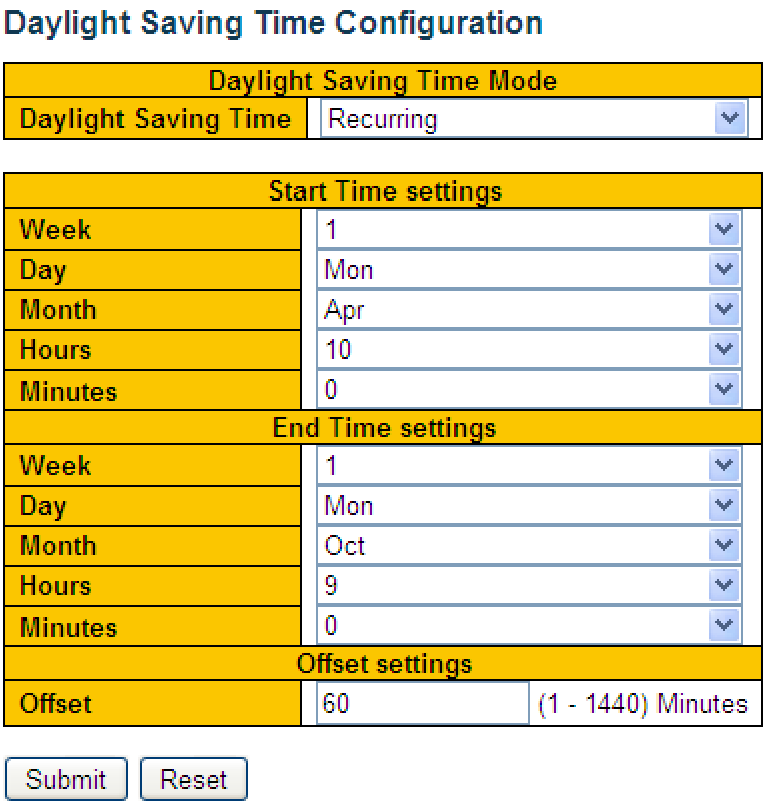
Function: Select the local timezone.

Acronym

Function: Description the time zone.

2. Configure daylight saving time, as shown in Figure 55 and Figure 56.

To make full use of time and save energy, Daylight Saving Time (DST) can be used in summer. To be specific, adjust clock forward some time in summer. DST configuration includes recurring and Non-recurring configuration.

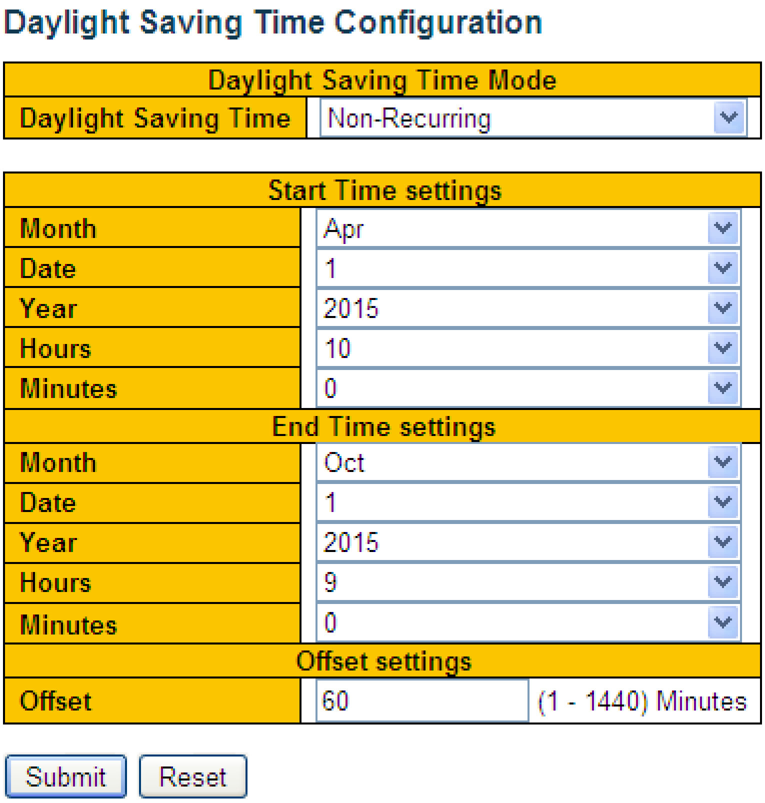


Daylight Saving Time Configuration

Daylight Saving Time Mode	
Daylight Saving Time	Recurring

Start Time settings	
Week	1
Day	Mon
Month	Apr
Hours	10
Minutes	0
End Time settings	
Week	1
Day	Mon
Month	Oct
Hours	9
Minutes	0
Offset settings	
Offset	60 (1 - 1440) Minutes

Figure 55 Configure Recurring DST



Daylight Saving Time Configuration

Daylight Saving Time Mode	
Daylight Saving Time	Non-Recurring

Start Time settings	
Month	Apr
Date	1
Year	2015
Hours	10
Minutes	0
End Time settings	
Month	Oct
Date	1
Year	2015
Hours	9
Minutes	0
Offset settings	
Offset	60 (1 - 1440) Minutes

Figure 56 Configure Non-Recurring DST

Daylight Saving Time

Options: Disabled/Recurring/Non-Recurring

Default: Disabled

Function: Enable or disable DST. After DST is enabled, clock will be adjusted forward some time in summer. Recurring means recurring time year by year.

Start Time setting /End Time setting

Function: After DST is enabled, Configure the time segment for DST. In non-Recurring mode, you need to configure year, month, date, hour, and minute to specify the time segment for DST. As shown in Figure 56 the DST is configured to be executed in the period from 10:00 a.m. April 1, 2015 to 9:00 a.m. October 1, 2015. You can set the month, week, day, hour, and minute in cycle mode to specify the DST execution time range every year. For example, you can configure the DST to be executed from 10:00 a.m. on the first Monday in April to 9:00 a.m. on the first Monday in October every year in Figure 55.

Offset

Range: 1~1440min

Default: 1min

Function: Set the DST clock offset, that is, the time length that the clock is brought forward for the DST execution.

CAUTION

Caution：

- Start time should be different from end time.
- Start time indicates non-DST time. End time indicates DST time.

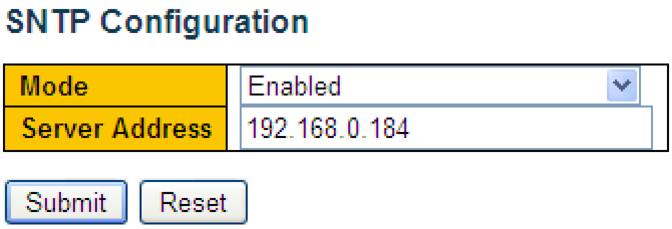
For example, run DST from 10:00:00 April 1st to 9:00:00 October 1st. The offset is 60 min. Non-DST time will run until 10:00:00 April 1st. Then the clock jumps to 11:00:00 to start DST. DST runs until 9:00:00 October 1st. Then the clock jumps back to 8:00:00 to run non-DST time.

3. Configure SNTP, as shown in Figure 57.

The Simple Network Time Protocol (SNTP) synchronizes time between server and client by means of requests and responses. As a client, the switch synchronizes time from the server according to packets of the server.

Caution:

- To synchronize time by SNTP, there must be an active SNTP server.
- All the time information carried in the SNTP protocol is standard time information of time zone 0.



SNTP Configuration

Mode	Enabled
Server Address	192.168.0.184

Figure 57 Enable SNTP

Mode

Options: Enabled/Disabled

Default: Disabled

Function: Enable/Disable SNTP.

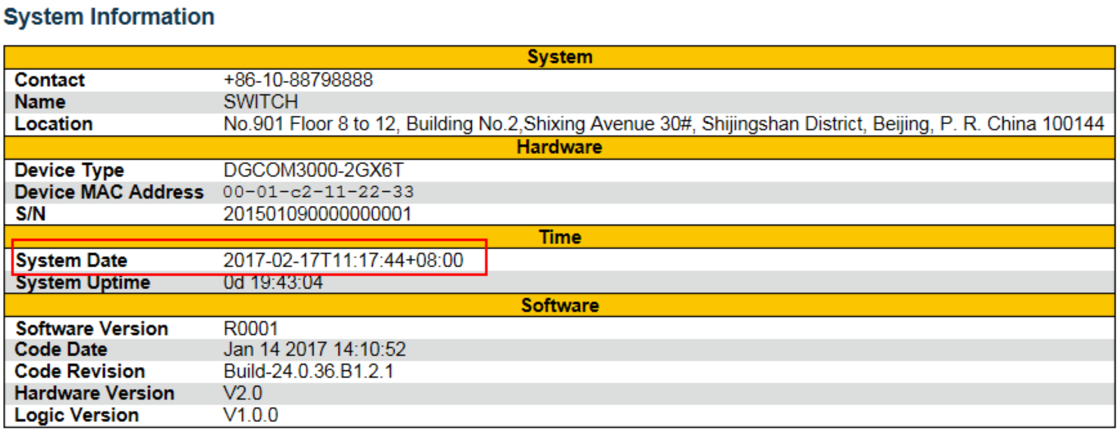
Server Address

Format: A.B.C.D

Function: Configure the IP address of the SNTP server. Clients will synchronize time according to server packets.

4. Check whether the clock is synchronized from the server.

Click [Basic Configuration]→[System Information] to view the clock information, as shown in Figure 58.



System Information

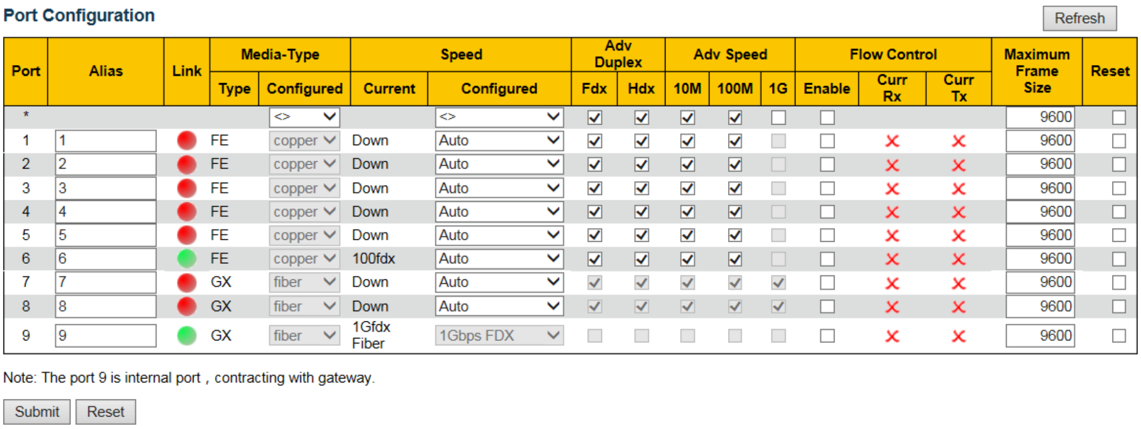
System	
Contact	+86-10-88798888
Name	SWITCH
Location	No.901 Floor 8 to 12, Building No.2,Shixing Avenue 30#, Shijingshan District, Beijing, P. R. China 100144
Hardware	
Device Type	DGCOM3000-2GX6T
Device MAC Address	00-01-c2-11-22-33
S/N	201501090000000001
Time	
System Date	2017-02-17T11:17:44+08:00
System Uptime	0d 19:43:04
Software	
Software Version	R0001
Code Date	Jan 14 2017 14:10:52
Code Revision	Build-24.0.36.B1.2.1
Hardware Version	V2.0
Logic Version	V1.0.0

Figure 58 View the Clock Information

You can view the switch time information based on the server time, in combination with the selected time zone and DST configuration.

3.6 Port Configuration

1. Configure port status, port speed, flow control, and other information, as shown in Figure 59.



Port Configuration

Port	Alias	Link	Media-Type		Speed		Adv Duplex		Adv Speed			Flow Control			Maximum Frame Size	Reset
			Type	Configured	Current	Configured	Fdx	Hdx	10M	100M	1G	Enable	Curr Rx	Curr Tx		
*				<>		<>	☑	☑	☑	☑	□	□			9600	□
1	1	🔴	FE	copper	Down	Auto	☑	☑	☑	☑	□	□	✗	✗	9600	□
2	2	🔴	FE	copper	Down	Auto	☑	☑	☑	☑	□	□	✗	✗	9600	□
3	3	🔴	FE	copper	Down	Auto	☑	☑	☑	☑	□	□	✗	✗	9600	□
4	4	🔴	FE	copper	Down	Auto	☑	☑	☑	☑	□	□	✗	✗	9600	□
5	5	🔴	FE	copper	Down	Auto	☑	☑	☑	☑	□	□	✗	✗	9600	□
6	6	🟢	FE	copper	100fdx	Auto	☑	☑	☑	☑	□	□	✗	✗	9600	□
7	7	🔴	GX	fiber	Down	Auto	☑	☑	☑	☑	☑	□	✗	✗	9600	□
8	8	🔴	GX	fiber	Down	Auto	☑	☑	☑	☑	☑	□	✗	✗	9600	□
9	9	🟢	GX	fiber	1Gfdx Fiber	1Gbps FDX	□	□	□	□	□	□	✗	✗	9600	□

Note: The port 9 is internal port , contracting with gateway.

Figure 59 Port Configuration

Link

Display the link status of ports.

Green: The port is in Linkup state and can communicate normally.

Red: The port is in Linkdown state and cannot communicate normally.

Speed-Current

Display the communication speed and duplex mode of ports.

Speed-Configured

Options: Disabled/Auto/10Mbps HDX/10Mbps FDX/100Mbps HDX/100Mbps FDX//1Gbps FDX

Default: Auto (10/100Base-TX port), 100Mbps FDX (100Base-FX port)

Function: Configure the speed and duplex mode of ports. Disabled indicates the port is disabled and disallows data transmission. This option directly affects the hardware status of the port and triggers port alarms.

Description: The speed and duplex mode of ports can be automatically negotiated or forcibly set. When Auto is set, the port speed and duplex mode will be automatically negotiated according to port connection status. You are advised to enable auto-negotiation for each port to avoid the connection problems caused by mismatched port configuration. If you want to force port speed/duplex mode, please make sure the same speed/duplex mode configuration in the connected ports at both ends.

Caution:

- The 10/100Base-TX port can be set to Auto, 10Mbps HDX/10Mbps FDX/100Mbps HDX/100Mbps FDX.
- The 10/100/1000Base-TX port can be set to Auto, 10Mbps HDX/10Mbps FDX/100Mbps HDX/100Mbps FDX/1Gbps FDX.

Adv Duplex

Options: Fdx/Hdx

Function: Configure the auto-negotiation duplex mode of ports.

Description: Fdx indicates the port can receive and transmit data at the same time; Hdx indicates the port only receives or transmits data at the same time. When the port mode is set to Auto, the duplex mode of the port is determined by means of negotiation with the peer by default. The negotiated duplex mode can be either Fdx or Hdx. The parameter can be configured for a port to negotiate only one duplex mode, thereby controlling the negotiation of the duplex mode.

Adv Speed

Options: 10M/100M/1G

Function: Configure the auto-negotiation speed of ports.

Description: When the port mode is set to **Auto**, the port speed is determined by means of negotiation with the peer by default. The negotiated speed can be any rate within the port rate capability range. The parameter can be configured for a port to negotiate only some rates, thereby controlling the speed negotiation.

Caution:

The Adv Duplex configuration and Adv Speed configuration take effect only in auto mode.

Flow Control

Options: Enabled/Disabled

Default: Disabled

Function: Enable/Disable flow control function on the designated port.

Description: Once the flow control function is enabled, the port will inform the sender to slow the transmitting speed to avoid packet loss by algorithm or protocol when the port-received flow is bigger than the size of port cache. If the devices work in different duplex modes (half/full), their flow control is realized in different ways. If the devices work in full duplex mode, the receiving end will send a special frame (Pause frame) to inform the sending end to stop sending packets. When the sender receives the Pause frame, it will stop sending packets for a period of "wait time" carried in the Pause frame and continue sending packets once the "wait time" ends. If the devices work in half duplex mode, they support back pressure flow control. The receiving end creates a conflict or a carrier signal. When the sender detects the conflict or the carrier wave, it will take backoff to postpone the data transmission.

Curr Rx/Curr Tx

Function: Display the flow control status of ports.

Maximum Frame Size

Range: 1518~9600 bytes

Default: 9600 bytes

Function: Set the maximum size of a packet that is received by a port. Packets with the size larger than the value are discarded.

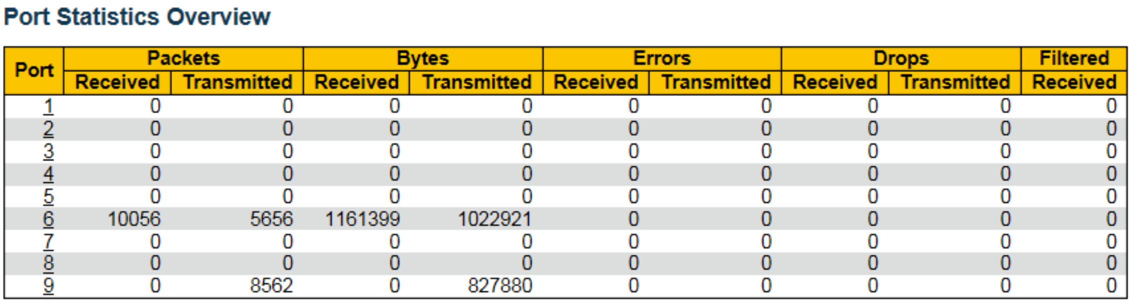
Reset

Options: Enabled/Disabled

Default: Disabled

Function: Reset the port or not.

2. View the port statistics, as shown in Figure 60.



Port Statistics Overview

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	10056	5656	1161399	1022921	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	0	8562	0	827880	0	0	0	0	0

Figure 60 Port Statistics

Port

Click <port> to enter the “detailed port statistics” page.

Packets

Display the number of packets that each port sends/receives.

Bytes

Display the number of bytes that each port sends/receives.

Errors

Display the number of error packets that each port sends/receives.

Drops

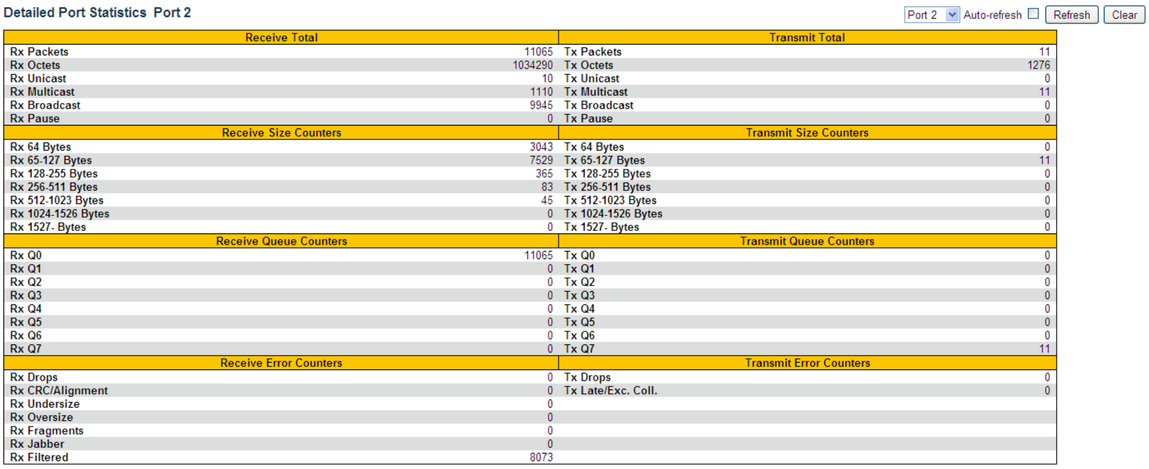
Display the number of packets that are discarded due to transmission/receiving conflicts.

Filtered Received

Display the number of packets that are filtered out by the receive end.

Click <port> to enter the “detailed port statistics” page.

3. View detailed port statistics, as shown in Figure 61.



Detailed Port Statistics Port 2

Receive Total		Transmit Total	
Rx Packets	11065	Tx Packets	11
Rx Octets	1034290	Tx Octets	1276
Rx Unicast	10	Tx Unicast	0
Rx Multicast	1110	Tx Multicast	11
Rx Broadcast	9945	Tx Broadcast	0
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	3043	Tx 64 Bytes	0
Rx 65-127 Bytes	7529	Tx 65-127 Bytes	11
Rx 128-255 Bytes	365	Tx 128-255 Bytes	0
Rx 256-511 Bytes	83	Tx 256-511 Bytes	0
Rx 512-1023 Bytes	45	Tx 512-1023 Bytes	0
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	0
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Q0	11065	Tx Q0	0
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	11
Receive Error Counters		**Transmit Error Counters**	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	8073		

Figure 61 Detailed Port Statistics

Select a port, and view the designated port detailed statistics.

3.7 QoS Configuration

3.7.1 Introduction

Quality of Service (QoS) enables differentiated services based on different requirements under limited bandwidths by means of traffic control and resource allocation on IP networks. QoS tries to satisfy the transmission of different services to reduce network congestion and minimize congestion's impact on the services of high priority.

Traffic classification, traffic policing, traffic shaping, congestion management, and congestion avoidance are the main concepts of QoS deployment. They mainly complete the following functions:

Traffic classification: identifies an object based on certain matching rules. It is the basis and prerequisite of QoS.

Traffic policing: supervises the traffic rate of packets that are transmitted to a device. When the traffic rate exceeds the specified traffic rate, the device adopts restriction or penalty measures to protect network resources against damage. Traffic policing is classified into port-based traffic policing and queue-based traffic policing.

Traffic shaping: proactively adjusts traffic output rate. It aims at adapting traffic to available network resources of a downstream device to prevent unnecessary packet discarding and congestion. Traffic shaping is classified into port-based traffic shaping and queue-based traffic shaping.

Congestion management: This is mandatory for solving resource competition. Congestion management caches packets in queues and determines the sequence of packet forwarding based on a certain scheduling algorithm, achieving preferential forwarding for key services.

Congestion avoidance: Excessive congestion may result in damage on network resources. Congestion avoidance monitors the use of network resources. When detecting increasing congestion, the function adopts proactive packet discarding and tunes traffic volume to solve the overload.

Traffic policing, traffic shaping, congestion management, and congestion avoidance control the network traffic and allocated resources from different aspects. They are the specific embodiment of QoS. For example, the switch supervises packets that are transmitted to a network based on the committed rate. It conducts shaping on the packets before the packets leave the switch. It conducts queue scheduling management in the case of congestion, and adopts congestion avoidance measures when the congestion is intensifying.

3.7.2 Principle

Each port of this series switches supports 8 cache queues, from 0 to 7 in priority ascending order.

When a frame reaches the port, the switch determines the queue for the frame according to the frame information and port. This series switches support traffic classification in the following queue mapping modes: port, 802.1Q header information, differentiated services code point (DSCP), and QoS control list (QCL), with the priority in ascending order.

When forwarding data, a port uses a scheduling mode to schedule the data in 8 queues and the bandwidth of each queue. This series switches support two scheduling modes: 6 Queues Weighted and SP（Strict Priority）.

WRR (Weighted Round Robin) schedules data flows based on weight ratio. Queues obtain their bandwidths based on their weight ratio. WRR prioritizes high-weight ratio queues. More bandwidths are allocated to queues with higher weight ratio.

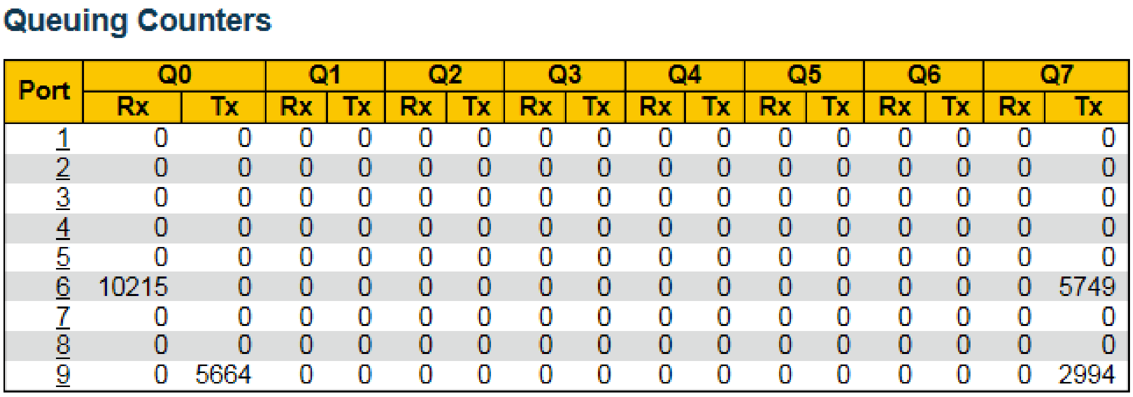
SP mode forwards high-priority packets preferentially. It is mainly used for transmitting sensitive signals. If a frame enters the high-priority queue, the switch stops scheduling the low-priority queues and starts to process the data of the high-priority queue. When the high-priority queue contains no data, the switch starts to process the data of the queue with lower priority.

6 Queues Weighted indicates that queue 6 and queue 7 use the Strict Priority scheduling mode, and queue 0 ~ queue 5 use the WRR scheduling mode. Data in queue 7 is processed prior to data in queue 6. When both queue 7 and queue 6 are empty, data in queue 0 ~ queue 5 is scheduled based on the weight ratio.

3.7.3 Web Configuration

3.7.3.1 Qos Statistics

1.View queue counters, as shown in Figure 62.



Queuing Counters

Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	10215	0	0	0	0	0	0	0	0	0	0	0	0	0	0	5749
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	5664	0	0	0	0	0	0	0	0	0	0	0	0	0	2994

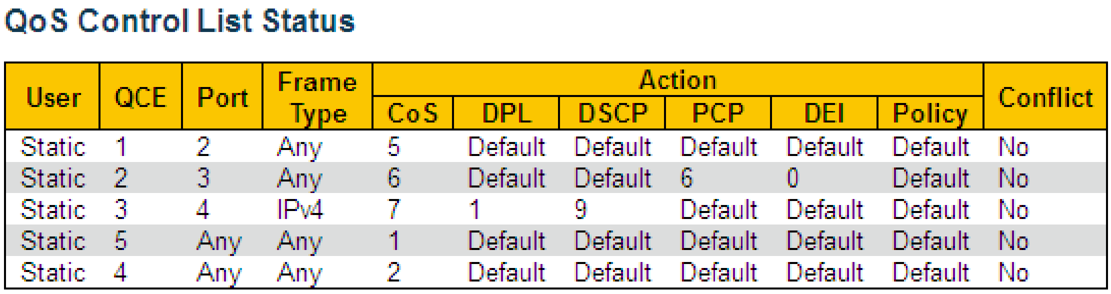
Figure 62 View Queue Counters

Display the number of packets that each queue sends/receives.

Click <port> to enter the “detailed port statistics” page, as shown in Figure 61.

3.7.3.2 QCL Status

1.View QCL entries, as shown in Figure 63.



QoS Control List Status

User	QCE	Port	Frame Type	Action						Conflict
				CoS	DPL	DSCP	PCP	DEI	Policy	
Static	1	2	Any	5	Default	Default	Default	Default	Default	No
Static	2	3	Any	6	Default	Default	6	0	Default	No
Static	3	4	IPv4	7	1	9	Default	Default	Default	No
Static	5	Any	Any	1	Default	Default	Default	Default	Default	No
Static	4	Any	Any	2	Default	Default	Default	Default	Default	No

Figure 63 View QCL Entries

Conflict

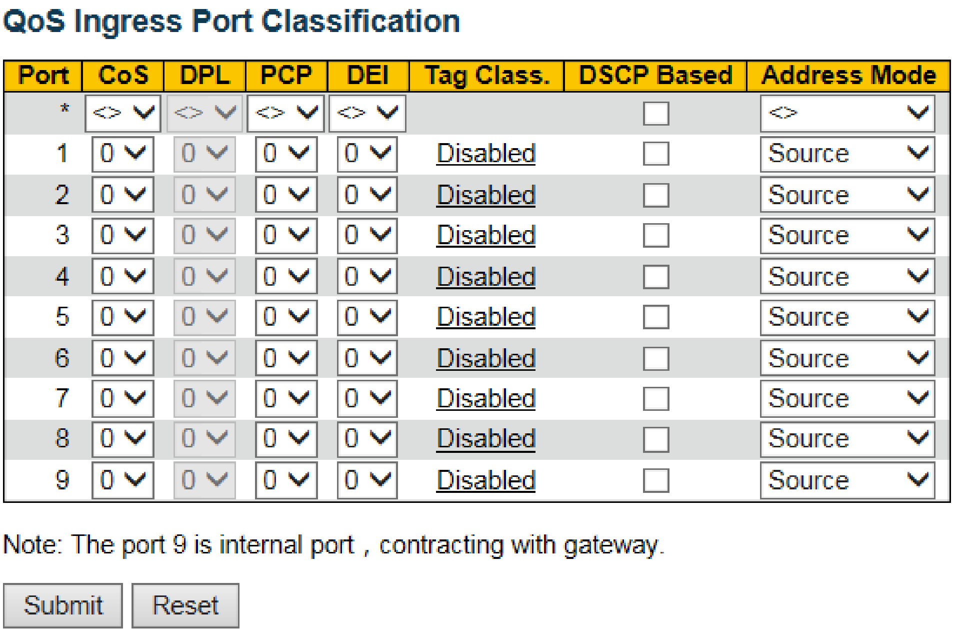
Options: No/Yes

Function: Displays the conflict status of a QCL entry. If resources for creating a QCL entry are insufficient, **Conflict** is set to **Yes** for this entry. Otherwise, **Conflict** is set to **No** for this entry.

Click <Resolve Confilct> to release resources required for a conflicting QCL entry so that the resource conflict is solved.

3.7.3.3 Port Classification

1.Configure port-based Port Classification mode, as shown in Figure 64.



QoS Ingress Port Classification

Port	CoS	DPL	PCP	DEI	Tag Class.	DSCP Based	Address Mode
*	<>	<>	<>	<>		□	<>
1	0	0	0	0	Disabled	□	Source
2	0	0	0	0	Disabled	□	Source
3	0	0	0	0	Disabled	□	Source
4	0	0	0	0	Disabled	□	Source
5	0	0	0	0	Disabled	□	Source
6	0	0	0	0	Disabled	□	Source
7	0	0	0	0	Disabled	□	Source
8	0	0	0	0	Disabled	□	Source
9	0	0	0	0	Disabled	□	Source

Note: The port 9 is internal port，contracting with gateway.

Figure 64 Configure Port-based Port Classification Mode

CoS

Range: 0~7

Default: 0

Function: Configure port default CoS value.

Description: The CoS value determines the queue for storing packets. The CoS value ranges from 0 to 7, which respectively corresponds to queue 0 to queue 7. After a packet is transmitted to the switch, the switch allocates the CoS value to the packet. If the received packet is tag type and the tag classification is disabled, or the received packet is untag type, the CoS value in the packet is the default CoS value of the port that receives the packet.

PCP

Range: 0~7

Default: 0

Function: Configure the default PCP（Priority Code Point）value of the port.

Explanation: When a packet is untagged, the priority in the tag added to the packet is the default PCP value of the port.

DEI

Range: 0~1

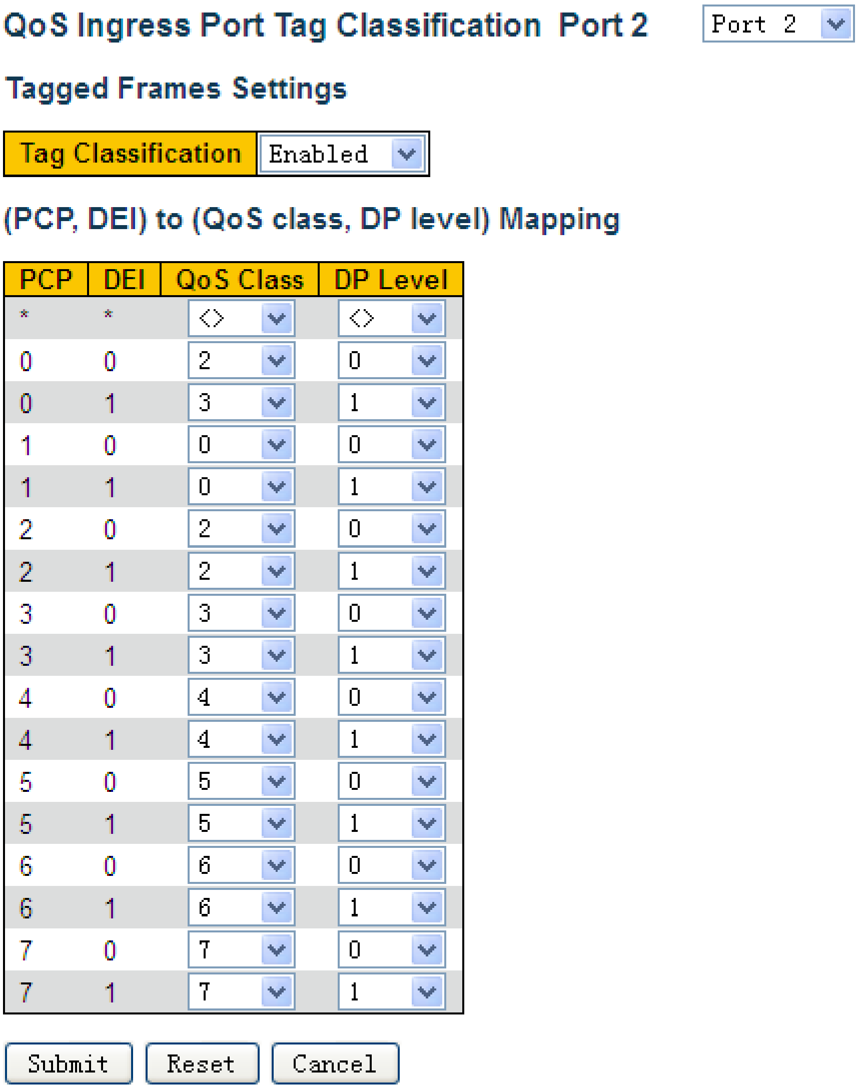
Default: 0

Function: Configure the default DEI（Drop Eligible Indicator）value of the port.

Explanation: When a packet is untagged, the CFI in the tag added to the packet is the default DEI value of the port.

2. Configure 802.1Q frame header-based queue mapping mode

Click <Tag Class.> in Figure 64 to enter 802.1Q frame header queue mapping mode configuration page, as shown in Figure 65.



QoS Ingress Port Tag Classification Port 2 Port 2

Tagged Frames Settings

Tag Classification: Enabled

(PCP, DEI) to (QoS class, DP level) Mapping

PCP	DEI	QoS Class	DP Level
*	*	<>	<>
0	0	2	0
0	1	3	1
1	0	0	0
1	1	0	1
2	0	2	0
2	1	2	1
3	0	3	0
3	1	3	1
4	0	4	0
4	1	4	1
5	0	5	0
5	1	5	1
6	0	6	0
6	1	6	1
7	0	7	0
7	1	7	1

Figure 65 Configure 802.1Q Frame Header Queue Mapping Mode

Tag Classification

Options: Enabled/Disabled

Default: Disabled

Function: Whether to enable the 802.1Q header information-based queue mapping mode. This queue mapping mode has a higher priority over the port-based queue mapping mode.

Caution:

The 802.1Q header information-based queue mapping mode is applicable only to tagged packets received by a port.

(PCP, DEI) to (QoS class, DP level) Mapping

Range: 0~7 (QoS class) 0~1 (DP Level)

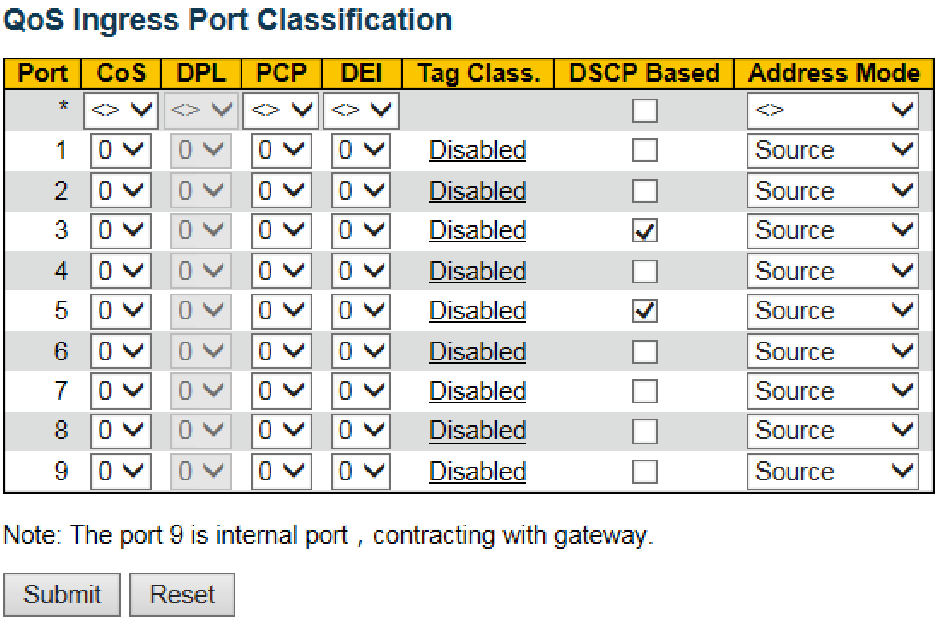
Default: The PCP value range is 0, 1, 2, 3, 4, 5, 6, and 7, which are respectively mapped to the QoS classes 1, 0, 2, 3, 4, 5, 6, and 7. The DEI value range is 0 and 1, which are respectively mapped to the DP levels 0 and 1.

Function: Set the mapping from (PCP, DEI) to (CoS, DPL) based on PCP and DEI values in packets.

Description: The QoS class is equivalent to the CoS value. The CoS value determines the queue for storing packets, and the CoS values 0-7 respectively correspond to queues 0-7. After a packet is transmitted to the switch, the switch allocates the CoS value and DPL value to the packet. The CoS value and DPL value of the packet are (CoS, DPL) mapped from (PCP, DEI) if the received packet is tag type, and the tag classification is enabled.

You can select a port to configure the 802.1Q header information-based queue mapping mode in the upper right corner of the page.

3. Enable DSCP-based queue mapping mode, as shown in Figure 66.



QoS Ingress Port Classification

Port	CoS	DPL	PCP	DEI	Tag Class.	DSCP Based	Address Mode
*	<>	<>	<>	<>		□	<>
1	0	0	0	0	Disabled	□	Source
2	0	0	0	0	Disabled	□	Source
3	0	0	0	0	Disabled	☑	Source
4	0	0	0	0	Disabled	□	Source
5	0	0	0	0	Disabled	☑	Source
6	0	0	0	0	Disabled	□	Source
7	0	0	0	0	Disabled	□	Source
8	0	0	0	0	Disabled	□	Source
9	0	0	0	0	Disabled	□	Source

Note: The port 9 is internal port , contracting with gateway.

Figure 66 Enable DSCP-based Queue Mapping Mode

DSCP Based

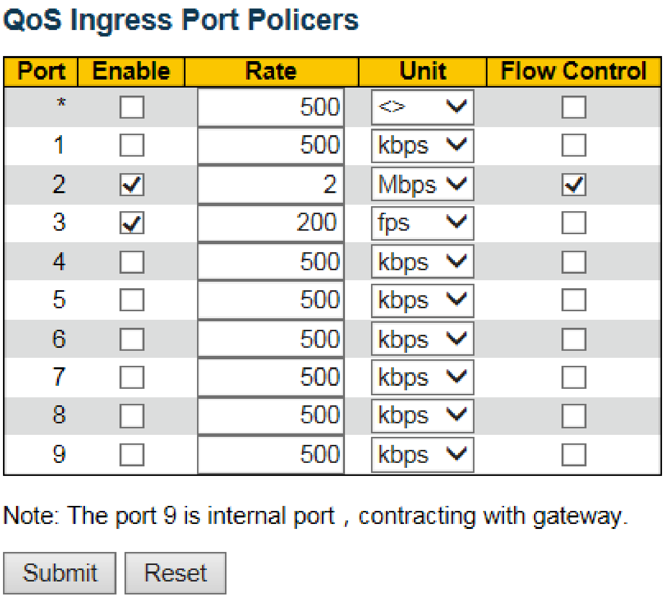
Options: Enabled/Disabled

Default: Disabled

Function: Whether to enable the DSCP-based queue mapping mode. This queue mapping mode has a higher priority over the 802.1Q header information-based queue mapping mode.

3.7.3.4 Port Policing

1.Configure ingress port policers, as shown in Figure 67.



QoS Ingress Port Policers

Port	Enable	Rate	Unit	Flow Control
*	□	500	<>	□
1	□	500	kbps	□
2	☑	2	Mbps	☑
3	☑	200	fps	□
4	□	500	kbps	□
5	□	500	kbps	□
6	□	500	kbps	□
7	□	500	kbps	□
8	□	500	kbps	□
9	□	500	kbps	□

Note: The port 9 is internal port，contracting with gateway.

Figure 67 Configure Ingress Port Policers

Enable

Options: Enabled/Disabled

Default: Disabled

Function: Enable or disable ingress port policers. The traffic policing of a port is implemented by port rate limit or port flow control.

Rate, Unit

Range: 100~3276700kbps/ 1~3276Mbps/ 100~3276700fps/ 1~3276Kfps

Default: 500kbps

Function: Limit the rate of packets received by a port. Packets with the rate exceeding the value are discarded.

Flow Control

Options: Enabled/Disabled

Default: Disabled

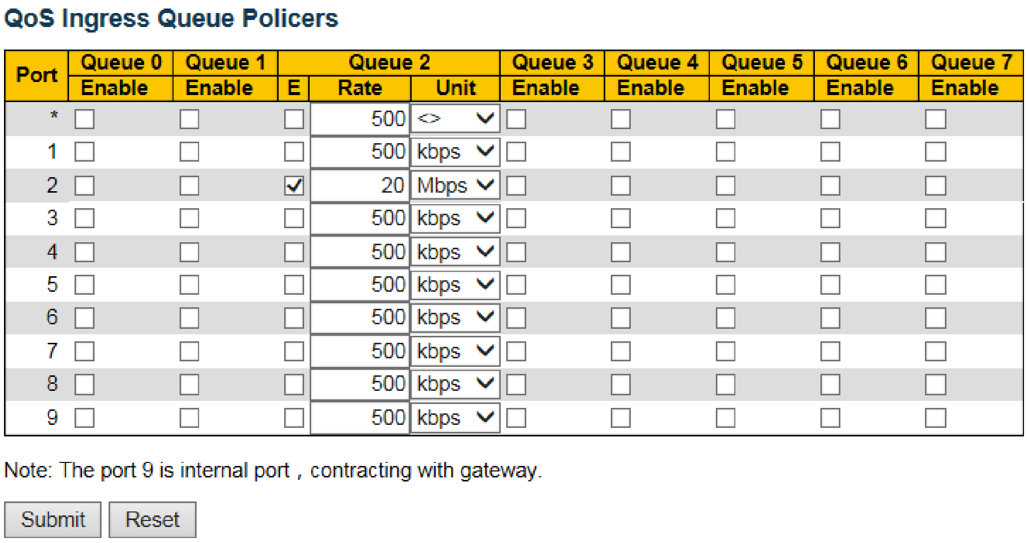
Function: Whether to enable port flow control. After flow control is enabled for a port, when the traffic received by the port is larger than the limit value, the sender is instructed to slow down the transmission to prevent packet loss by means of algorithms or protocols.

Note:

The precondition for the flow control function taking effect is to enable the port flow control in Port Configuration page (Figure 59).

3.7.3.5 Queue Policing

1. Configure ingress queue policers, as shown in Figure 68.



QoS Ingress Queue Policers

Port	Queue 0	Queue 1	Queue 2			Queue 3	Queue 4	Queue 5	Queue 6	Queue 7
	Enable	Enable	E	Rate	Unit	Enable	Enable	Enable	Enable	Enable
*	□	□	□	500	<>	□	□	□	□	□
1	□	□	□	500	kbps	□	□	□	□	□
2	□	□	☑	20	Mbps	□	□	□	□	□
3	□	□	□	500	kbps	□	□	□	□	□
4	□	□	□	500	kbps	□	□	□	□	□
5	□	□	□	500	kbps	□	□	□	□	□
6	□	□	□	500	kbps	□	□	□	□	□
7	□	□	□	500	kbps	□	□	□	□	□
8	□	□	□	500	kbps	□	□	□	□	□
9	□	□	□	500	kbps	□	□	□	□	□

Note: The port 9 is internal port , contracting with gateway.

Figure 68 Configure Ingress Queue Policers

E

Options: Enabled/Disabled

Default: Disabled

Function: Enable or disable ingress queue policers. You need to set the rate and unit after traffic policing is enabled for a queue.

Rate, Unit

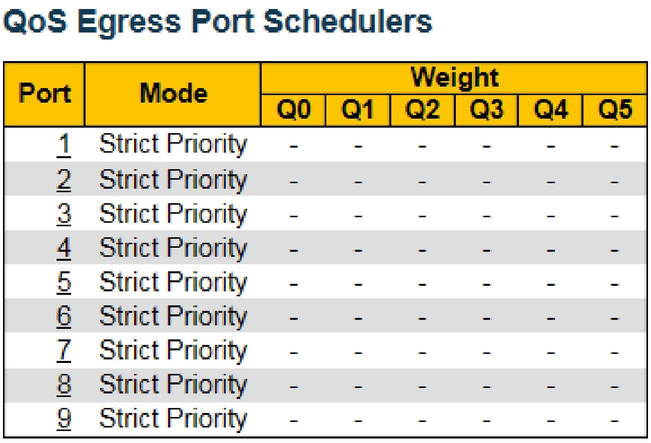
Range: 100~3276700kbps/ 1~3276Mbps

Default: 500kbps

Function: Limit the rate of packets received by a queue of a port. Packets with the rate exceeding the value are discarded.

3.7.3.6 Port Scheduler

1.Configure port queue scheduling mode, as the figure shows below.

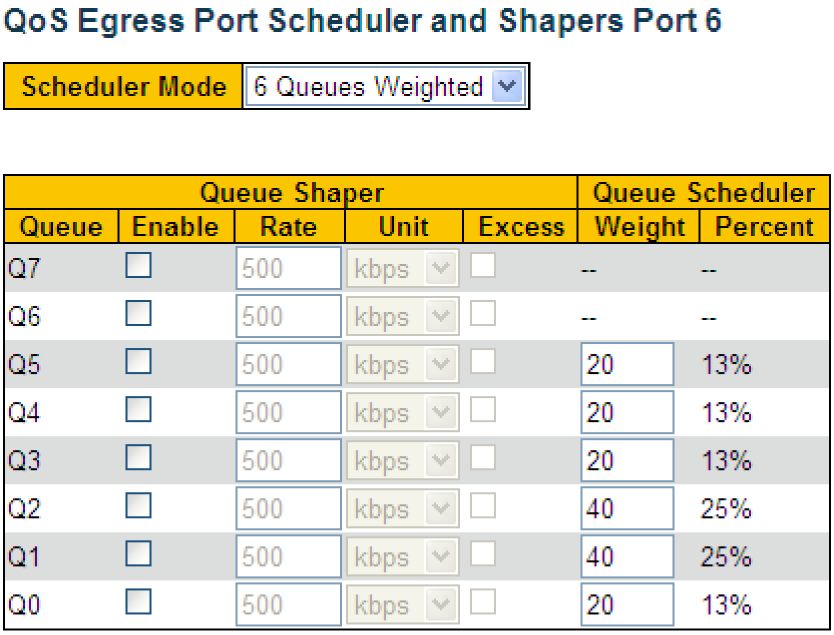


QoS Egress Port Schedulers

Port	Mode	Weight					
		Q0	Q1	Q2	Q3	Q4	Q5
1	Strict Priority	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-
7	Strict Priority	-	-	-	-	-	-
8	Strict Priority	-	-	-	-	-	-
9	Strict Priority	-	-	-	-	-	-

Figure 69 View Port Queue Scheduling Mode

Click <Port> to enter the “port queue scheduling mode” configuration page.



QoS Egress Port Scheduler and Shapers Port 6

Scheduler Mode	6 Queues Weighted

Queue Shaper					Queue Scheduler	
Queue	Enable	Rate	Unit	Excess	Weight	Percent
Q7	□	500	kbps	□	--	--
Q6	□	500	kbps	□	--	--
Q5	□	500	kbps	□	20	13%
Q4	□	500	kbps	□	20	13%
Q3	□	500	kbps	□	20	13%
Q2	□	500	kbps	□	40	25%
Q1	□	500	kbps	□	40	25%
Q0	□	500	kbps	□	20	13%

Figure 70 Configre Port Queue Scheduling Mode

Scheduler Mode

Options: Strict Priority/6 Queues Weighted

Default: Strict Priority

Function: Configure the egress-queue mode of the selected port.

Queue Weight

Range: 1~100

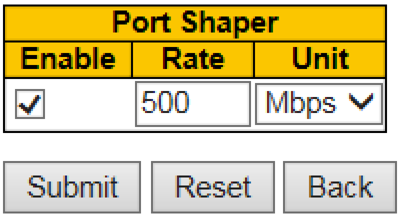
Default: 17

Function: Configure weight values of the queue.

You can select a port to configure the queue scheduling mode in the upper right corner of the page.

3.7.3.7 Port Shaping

1. Configure Port Shaper as shown in Figure 71.



Port Shaper		
Enable	Rate	Unit
☑	500	Mbps

Figure 71 Configure Port Shaper

Enable

Options: Enabled/Disabled

Default: Disabled

Function: Enable or disable egress port shapers. Traffic shaping of a port is implemented by port rate limit.

Rate, Unit

Range: 100~3281943kbps/ 1~3281Mbps

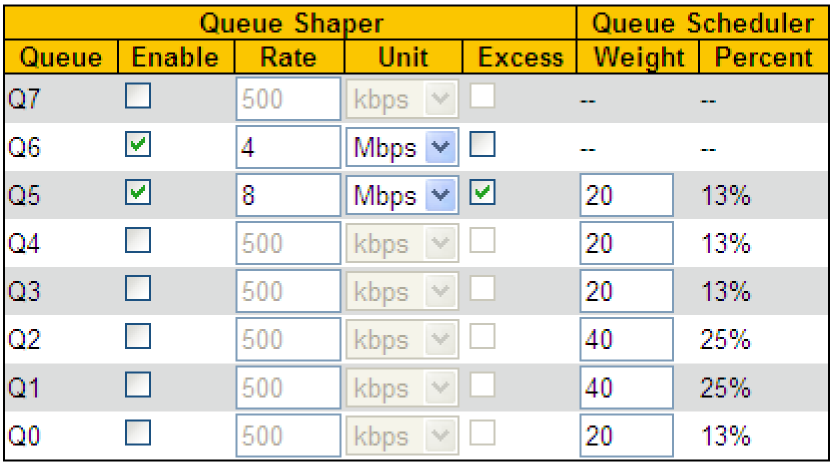
Default: 500kbps

Function: Limit the rate of packets transmitted by a port. Packets with the rate exceeding the value are discarded.

Click <Back> to close the current configuration page and return to the previous configuration page.

You can select a port to configure traffic shaping in the upper right corner of the page.

2. Configure the queue shapers, as shown in Figure 71.



Queue Shaper					Queue Scheduler	
Queue	Enable	Rate	Unit	Excess	Weight	Percent
Q7	☐	500	kbps	☐	--	--
Q6	☑	4	Mbps	☐	--	--
Q5	☑	8	Mbps	☑	20	13%
Q4	☐	500	kbps	☐	20	13%
Q3	☐	500	kbps	☐	20	13%
Q2	☐	500	kbps	☐	40	25%
Q1	☐	500	kbps	☐	40	25%
Q0	☐	500	kbps	☐	20	13%

Figure 72 Configure the Queue Shapers

Enable

Options: Enabled/Disabled

Default: Disabled

Function: Enable or disable the queue shapers.

Rate, Unit

Range: 100~3281943kbps/ 1~3281Mbps

Default: 500kbps

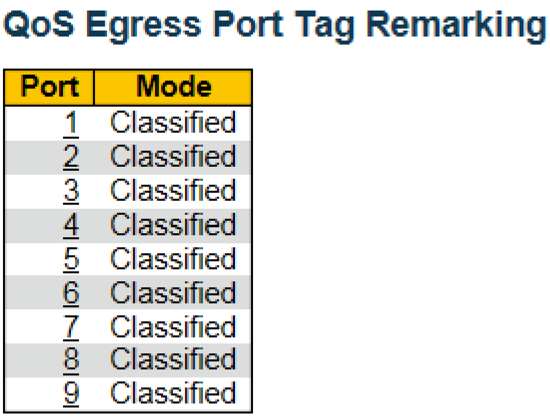
Function: Limit the rate of packets transmitted by a queue of a port. Packets with the rate exceeding the value are discarded.

Click <Back> to close the current configuration page and return to the previous configuration page.

You can select a port to configure traffic shaping in the upper right corner of the page.

3.7.3.8 Port Tag Remarking

1.Configure 802.1p remarking, as shown in Figure 73.



QoS Egress Port Tag Remarking

Port	Mode
1	Classified
2	Classified
3	Classified
4	Classified
5	Classified
6	Classified
7	Classified
8	Classified
9	Classified

Figure 73 Configure 802.1p Remarking

Mode

Option: Classified/Mapped/Default

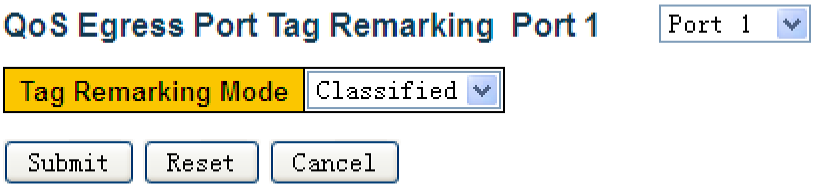
Function: Displays the 802.1p retagging mode when an egress port forwards packets. 802.1p retagging is used to update the PCP value and DEI value in packets when an egress port forwards packets.

Caution:

If packets forwarded by an egress port are untagged, the 802.1p retagging function is unavailable.

Click <Port> to enter 802.1p remarking configuration page.

➢ Configre 802.1p remarking mode to Classified, as shown in Figure 74.



QoS Egress Port Tag Remarking Port 1 Port 1

Tag Remarking Mode: Classified

Figure 74 Configre 802.1p Remarking Mode to Classified

Tag Remarking Mode

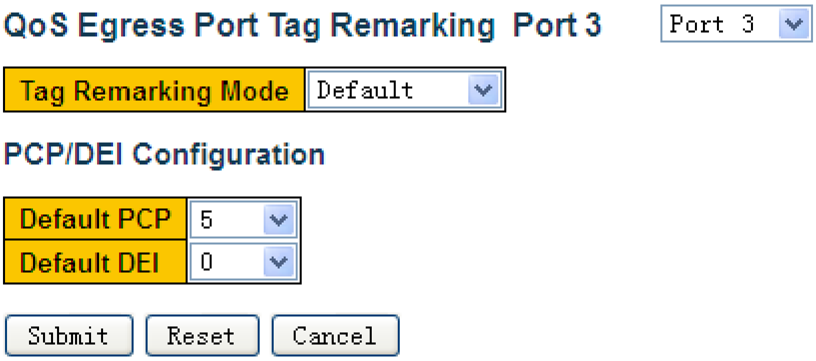
Options: Classified/Mapped/Default

Default: Classified

Function: Configre 802.1p remarking mode. Classified: The PCP value and DEI value in packets are not updated when an egress port forwards the packets.

You can select a port to configure the 802.1p retagging mode in the upper right corner of the page.

➢ Configre 802.1p remarking mode to Default, as shown in Figure 75.



QoS Egress Port Tag Remarking Port 3 Port 3

Tag Remarking Mode: Default

PCP/DEI Configuration

Default PCP: 5

Default DEI: 0

Figure 75 Configre 802.1p Remarking Mode to Default

Tag Remarking Mode

Options: Classified/Mapped/Default

Default: Classified

Function: Configre 802.1p remarking mode. Default: The PCP value and DEI value in packets are updated to the default values (set in the lower part of the page) of an egress port when the egress port forwards the packets.

Default PCP

Range: 0~7

Default: 0

Function: Set the default PCP value of an egress port.

Default DEI

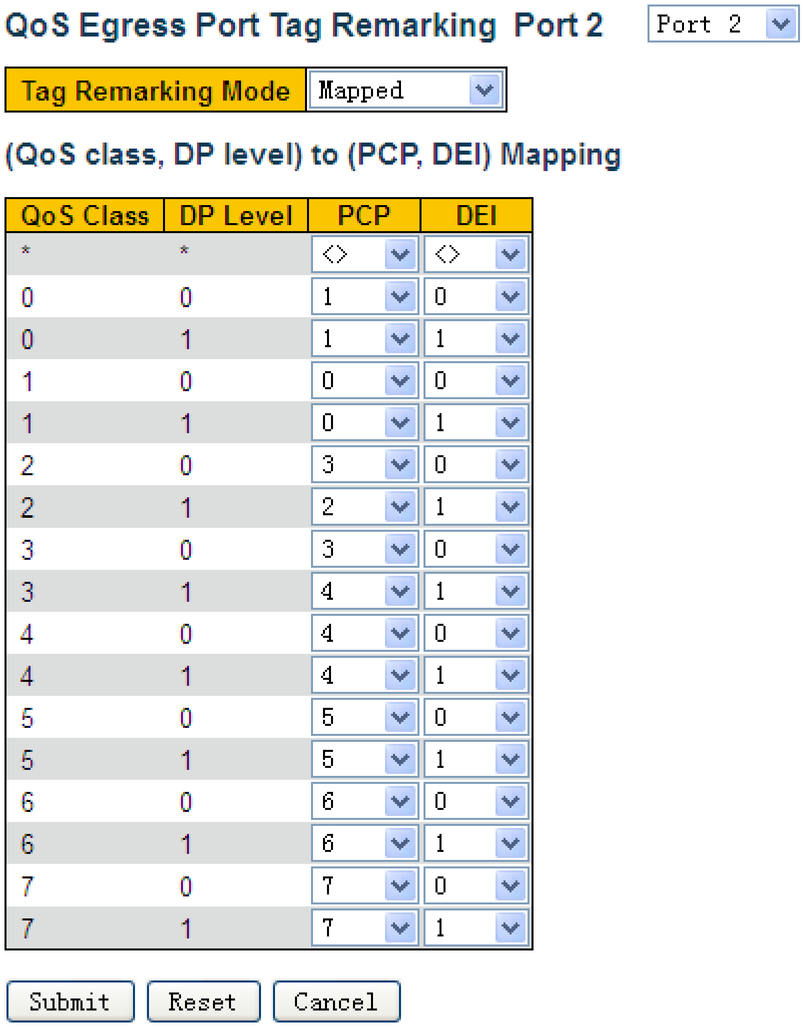
Range: 0~1

Default: 0

Function: Set the default DEI value of an egress port.

You can select a port to configure the 802.1p retagging mode in the upper right corner of the page.

➢ Configre 802.1p remarking mode to Mapped, as shown in Figure 76.



QoS Egress Port Tag Remarking Port 2 Port 2

Tag Remarking Mode	Mapped

(QoS class, DP level) to (PCP, DEI) Mapping

QoS Class	DP Level	PCP	DEI
*	*	<>	<>
0	0	1	0
0	1	1	1
1	0	0	0
1	1	0	1
2	0	3	0
2	1	2	1
3	0	3	0
3	1	4	1
4	0	4	0
4	1	4	1
5	0	5	0
5	1	5	1
6	0	6	0
6	1	6	1
7	0	7	0
7	1	7	1

Figure 76 Configre 802.1p Remarking Mode to Mapped

Tag Remarking Mode

Options: Classified/Mapped/Default

Default: Classified

Function: Configre 802.1p remarking mode. Mapped: The PCP value and DEI value in packets are updated to the (PCP, DEI) mapped from (CoS, DPL) when an egress port forwards the packets. The mapping is configured in the lower part of the page.

(QoS class, DP level) to (PCP, DEI) Mapping

Range: 0~7 (PCP) 0~1 (DEI)

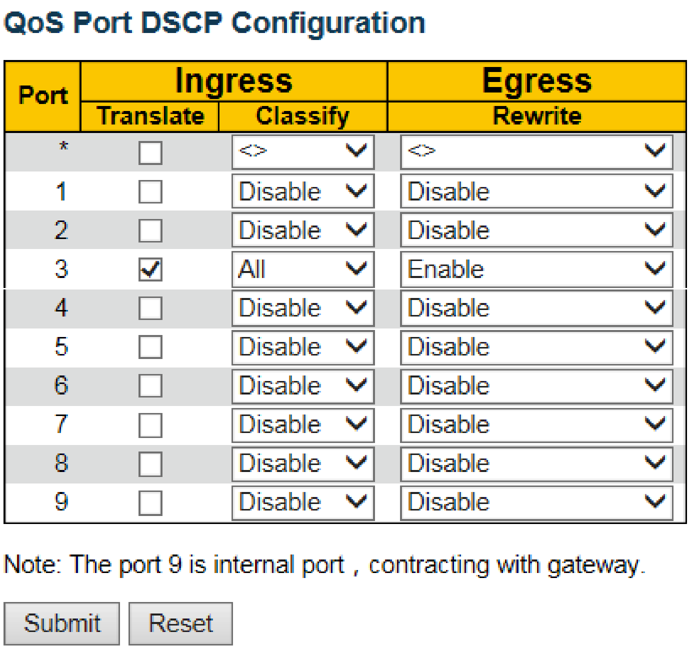
Default: The QoS class range is 0, 1, 2, 3, 4, 5, 6, and 7, which are respectively mapped to the PCP values 1, 0, 2, 3, 4, 5, 6, and 7. The DP level value range is 0 and 1, which are respectively mapped to the DEI values 0 and 1.

Function: Configure the mapping from (CoS, DPL) to (PCP, DEI) based on the CoS and DPL values in packets.

You can select a port to configure the 802.1p retagging mode in the upper right corner of the page.

3.7.3.9 Port DSCP

1.Enable the DSCP translation of an ingress port and the DSCP rewriting function of an egress port, as shown in Figure 77.



QoS Port DSCP Configuration

Port	Ingress		Egress
	Translate	Classify	Rewrite
*	□	<>	<>
1	□	Disable	Disable
2	□	Disable	Disable
3	☑	All	Enable
4	□	Disable	Disable
5	□	Disable	Disable
6	□	Disable	Disable
7	□	Disable	Disable
8	□	Disable	Disable
9	□	Disable	Disable

Note: The port 9 is internal port , contracting with gateway.

Figure 77 Configure Port DSCP Function

Translate

Options: Enabled/Disabled

Default: Disabled

Function: Whether to translate the DSCP value in a packet received by an ingress port. If it is set to Enable, the DSCP value is translated according to the DSCP translation table (“Translate” column in Figure 79).

Classify

Options: Disable/DSCP=0/Selected/All

Default: Disable

Function: Selects the rewritten DSCP value of an egress port when Rewrite is set to Enable.

Disable: The DSCP value in packets is not rewritten when an egress port forwards the packets.

DSCP=0: When an egress port forwards packets, if the DSCP values in the packets are 0, the DSCP values in the packets are rewritten according to the classification in Figure 80.

Selected: When an egress port forwards packets, if the DSCP values in the packets are a selected value (“Classify” column in Figure 79), the DSCP values in the packets are rewritten according to the classification in Figure 80.

All: When an egress forwards packets, the DSCP values in the packets are written according to the classification in Figure 80.

Rewrite

Options: Disable/Enable/Remap DP Unaware/Remap DP Aware

Default: Disable

Function: Set the rewriting mode of the DSCP value in packets when an egress port forwards the packets.

Disable: The DSCP values in packets are not rewritten when an egress port forwards the packets.

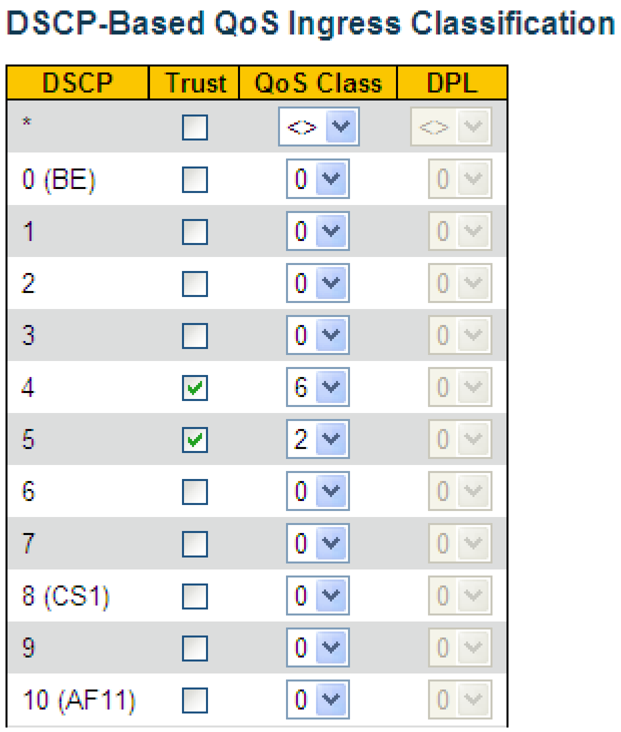
Enable: Whether the DSCP values in packets are rewritten is determined based on the classify configuration when an egress port forwards the packets.

Remap DP Unaware: The DSCP values in packets are rewritten based on the mapping (“Remap DP0” column in Figure 79) from (DSCP, DPL=0) to DSCP when an egress forwards the packets.

Remap DP Aware: The DSCP values in packets are rewritten based on the mapping (“Remap DP0” and “Remap DP1” columns in Figure 79) from (DSCP, DPL) to DSCP when an egress forwards the packets.

3.7.3.10 DSCP-Based QoS

1.Configure DSCP-based queue mapping mode, as shown in Figure 78.



DSCP-Based QoS Ingress Classification

DSCP	Trust	QoS Class	DPL
*	☐	<>	<>
0 (BE)	☐	0	0
1	☐	0	0
2	☐	0	0
3	☐	0	0
4	☑	6	0
5	☑	2	0
6	☐	0	0
7	☐	0	0
8 (CS1)	☐	0	0
9	☐	0	0
10 (AF11)	☐	0	0

Figure 78 Configure DSCP-based Queue Mapping Mode

Trust

Options: Enabled/Disabled

Default: Disabled

Function: Whether to trust the DSCP value.

Caution:

The DSCP-based queue mapping mode is applicable only to the DSCP values in packets received by a port are trusted

QoS Class

Range: 0~7

Default: 0

Function: Set the mapping from DSCP to CoS.

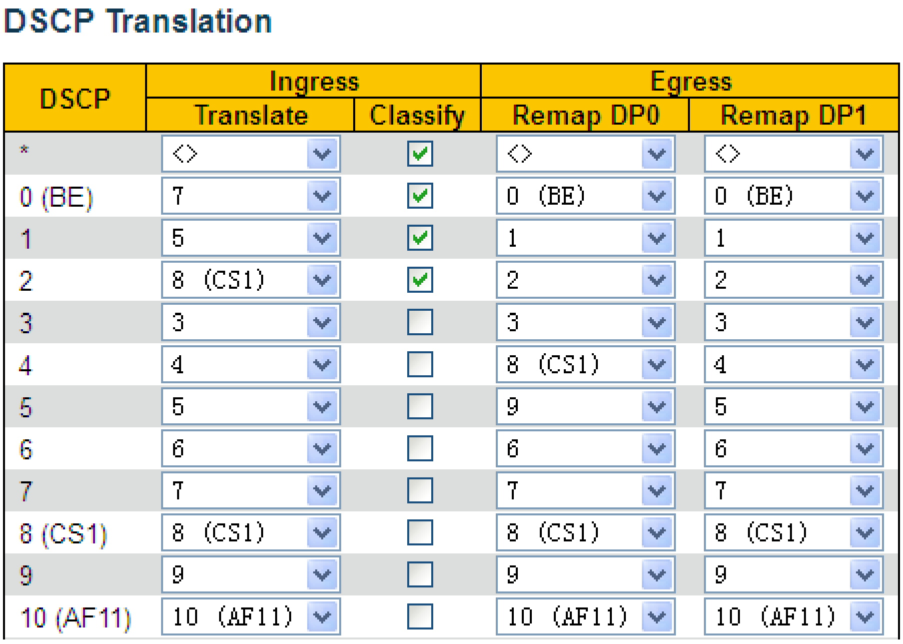
Description: The QoS class is equivalent to the CoS value. The CoS value determines the queue for storing packets, and the CoS values 0~7 respectively correspond to queues 0~7. After a packet with the DSCP value being a trusted value is transmitted to the switch, the switch allocates the CoS value to the packet according to the mapping from DSCP to CoS.

Caution:

If translate is enabled for an ingress port, the switch allocates the CoS value based on the translated DSCP value. Otherwise, the switch allocates the CoS value based on the original DSCP value in packets.

3.7.3.11 DSCP Translation

1.Configuring DSCP translation and rewriting, as shown in Figure 79.



DSCP Translation

DSCP	Ingress		Egress	
	Translate	Classify	Remap DP0	Remap DP1
*	<>	☑	<>	<>
0 (BE)	7	☑	0 (BE)	0 (BE)
1	5	☑	1	1
2	8 (CS1)	☑	2	2
3	3	□	3	3
4	4	□	8 (CS1)	4
5	5	□	9	5
6	6	□	6	6
7	7	□	7	7
8 (CS1)	8 (CS1)	□	8 (CS1)	8 (CS1)
9	9	□	9	9
10 (AF11)	10 (AF11)	□	10 (AF11)	10 (AF11)

Figure 79 Configuring DSCP Translation and Rewriting

Translate

Range: 0~63

function: Set the translation table of DSCP values.

Classify

Options: Enabled/Disabled

Default: Disabled

Function: When Classify is set to Selected in Figure 77, this parameter is used to set the selected DSCP value.

Caution:

When translate is enabled for an ingress port, the selected DSCP value is the DSCP value after translation. Otherwise, the selected DSCP value is the original DSCP value in packets.

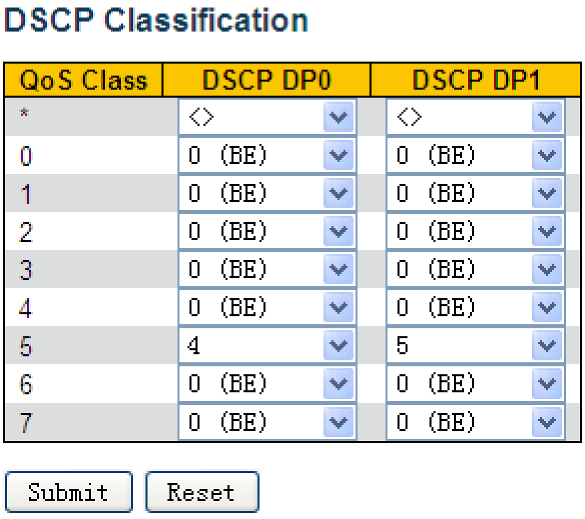
Remap DP0/ Remap DP1

Range: 0~63

Function: Set the mapping from (DSCP, DPL) to DSCP values.

3.7.3.12 DSCP Classification

1.Configure DSCP classification, as shown in Figure 80.



DSCP Classification

QoS Class	DSCP DP0	DSCP DP1
*	<>	<>
0	0 (BE)	0 (BE)
1	0 (BE)	0 (BE)
2	0 (BE)	0 (BE)
3	0 (BE)	0 (BE)
4	0 (BE)	0 (BE)
5	4	5
6	0 (BE)	0 (BE)
7	0 (BE)	0 (BE)

Figure 80 Configure DSCP Classification

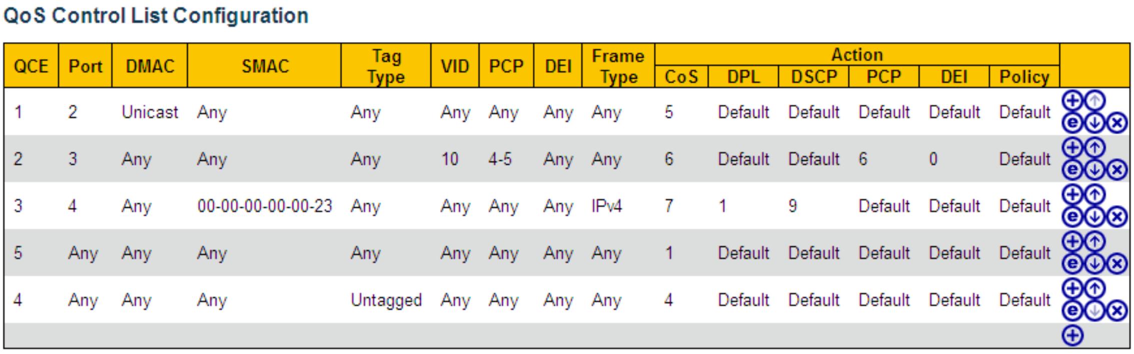
DSCP DP0/DSCP DP1

Range: 0~63

Function: Set the mapping from (CoS, DPL) to DSCP values. The QoS class is equivalent to the CoS value. The CoS value determines the queue for storing packets, and the CoS values 0-7 respectively correspond to queues 0-7.

3.7.3.13 QoS Control List

1.Configure QCL entry, as shown in Figure 81.



QoS Control List Configuration

QCE	Port	DMAC	SMAC	Tag Type	VID	PCP	DEI	Frame Type	Action						
									CoS	DPL	DSCP	PCP	DEI	Policy	
1	2	Unicast	Any	Any	Any	Any	Any	Any	5	Default	Default	Default	Default	Default	⊕ ⓔ ⊗
2	3	Any	Any	Any	10	4-5	Any	Any	6	Default	Default	6	0	Default	⊕ ⓔ ⊗
3	4	Any	00-00-00-00-00-23	Any	Any	Any	Any	IPv4	7	1	9	Default	Default	Default	⊕ ⓔ ⊗
5	Any	Any	Any	Any	Any	Any	Any	Any	1	Default	Default	Default	Default	Default	⊕ ⓔ ⊗
4	Any	Any	Any	Untagged	Any	Any	Any	Any	4	Default	Default	Default	Default	Default	⊕ ⓔ ⊗
															⊕

Figure 81 Configure QCL Entry

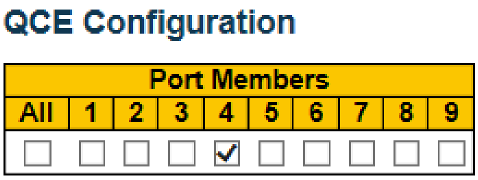
The queue mapping of packets is implemented by matching QCL entries. Each entry consists of several conditions in the logical AND relationship. It is considered that a packet received by a member port matches a QCL entry only when the packet meets all the conditions. QCL entries are independent of each other.

When there are multiple QCL entries, the device compares a packet with the QCL entries one by one (from top to bottom). Once a match is found, the action is taken and no further comparison is conducted. Click <⊕> to add a new QCL entry; click <ⓔ> to edit the QCL entry; click <⊗> to delete the QCL entry, click <⦶> to move up the current entry; click <⦶> to move down the current entry.

QCE is the ID of a QCL entry, which is numbered based on the entry creation time sequence.

2. Configure QCL entry parameters

- ➢ Select a port on which the current QCL entry takes effect, as shown in Figure 82.



QCE Configuration

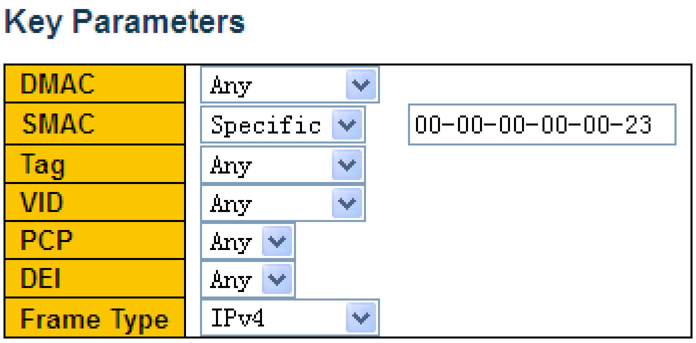
Port Members									
All	1	2	3	4	5	6	7	8	9
□	□	□	□	☑	□	□	□	□	□

Figure 82 Select Port Member

Port members

Function: Select a port on which the current QCL entry takes effect. All ports are member ports by default.

- ➢ Configure QCL entry parameters, as shown in Figure 83.



Key Parameters

DMAC	Any	
SMAC	Specific	00-00-00-00-00-23
Tag	Any	
VID	Any	
PCP	Any	
DEI	Any	
Frame Type	IPv4	

Figure 83 Configure QCL Entry Parameters

DMAC

Options: Any/ Unicast/ Multicast / Broadcast

Default: Any

Function: Set a condition--destination MAC address. When the destination MAC address in a packet received by a member port meets settings of this parameter, the condition is matched successfully.

SMAC

Options: Any/ Specific

Default: Any

Function: Set a condition--source MAC address. When it is set to Specific, a MAC address needs to be set. When the source MAC address in a packet received by a member port meets settings of this parameter, the condition is matched successfully.

Tag

Options: Any/ Untagged/ Tagged

Default: Any

Function: Set a condition--tag. When a packet received by a member port meets settings of this parameter, the condition is matched successfully.

VID

Options: Any/ Specific（1~4095）/ Range（1~4095）

Default: Any

Function: Set a condition--VID. When it is set to Specific, the VID value needs to be set. When it is set to Range, the VID range needs to be set. When the VID in a packet received by a member port meets settings of this parameter, the condition is matched successfully.

This parameter is unavailable when Tag is set to Untagged.

PCP

Options: Any/0/1/2/3/4/5/6/7/0-1/2-3/4-5/6-7/0-3/4-7

Default: Any

Function: Set a condition--PCP. When the PCP value in a packet received by a member port meets settings of this parameter, the condition is matched successfully. This parameter is unavailable when Tag is set to Untagged.

DEI

Options: Any/0/1

Default: Any

Function: Set a condition--DEI. When the DEI value in a packet received by a member port meets settings of this parameter, the condition is matched successfully. This parameter is unavailable when Tag is set to Untagged.

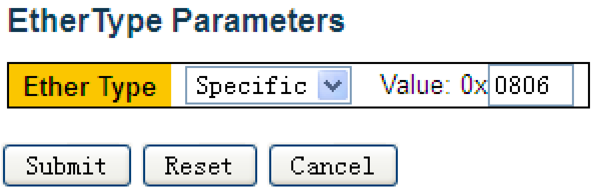
Frame Type

Options: Any/ EtherType/ LLC/ SNAP/ IPv4/ IPv6

Default: Any

Function: Select frame type.

➢ Configure the EtherType frame parameters, as shown in Figure 84.



EtherType Parameters

Ether Type: Specific; Value: 0x 0806

Figure 84 Configure the EtherType Frame Parameters

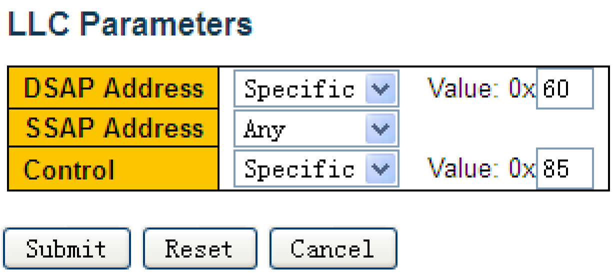
Ether Type

Options: Any/ Specific（0x0600~0xFFFF）

Default: Any

Function: Set a condition--Ethernet type. When it is set to Specific, an Ethernet type needs to set. When an Ethernet packet received by a member port meets settings of this parameter, the condition is matched successfully.

➢ Configure the LLC frame parameters, as shown in Figure 85.



LLC Parameters

DSAP Address	Specific	Value: 0x 60
SSAP Address	Any	
Control	Specific	Value: 0x 85

Figure 85 Configure the LLC Frame Parameters

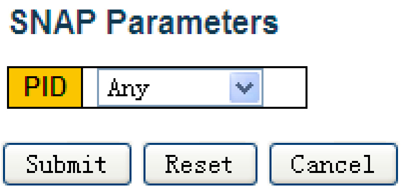
DSAP Address/SSAP Address/Control

Options: Any/Specific（0x00~0xFF）

Default: Any

Function: Set a condition--LLC packet parameters. When DSAP Address, SSAP Address, or Control is set to Specific, a specific value needs to be entered. When an LLC packet received by a member port meets settings of the parameters, the condition is matched successfully.

➢ Configure the SNAP frame parameters, as shown in Figure 86.



SNAP Parameters

PID	Any

Figure 86 Configure the SNAP Frame Parameters

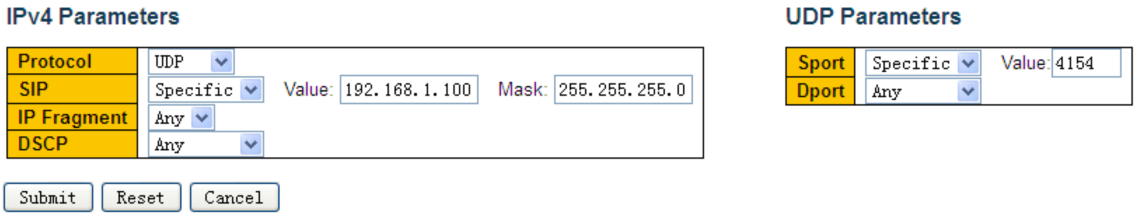
PID

Options: Any/ Specific（0x0000~0xFFFF）

Default: Any

Function: Set a condition--SNAP packet parameter. When it is set to Specific, a PID value needs to be entered. When the PID in an SNAP packet received by a member port meets settings of this parameter, the condition is matched successfully.

➢ Configure the IPv4/ IPv6 frame parameters, as shown in Figure 87.



IPv4 Parameters

Protocol	UDP
SIP	Specific Value: 192.168.1.100 Mask: 255.255.255.0
IP Fragment	Any
DSCP	Any

UDP Parameters

Sport	Specific Value: 4154
Dport	Any

Figure 87 Configure the IPv4 Frame Parameters

Protocol

Options: Any/ UDP/ TCP/ Other（0~255）

Default: Any

Function: Set a condition--IPv4 packet protocol type. When it is set to UDP or TCP, a source port ID and a destination port ID need to be set. When it is set to Other, a protocol ID needs to be set. When the protocol type in a packet received by a member port meets settings of this parameter, the condition is matched successfully.

Sport/ Dport

Options: Any/ Specific（0~65535）/ Range（0~65535）

Default: Any

Function: Set a condition--TCP/UDP source port ID and destination port ID. When they are set to Specific, a port ID needs to be set. When they are set to Range, a port ID range needs to be set. When the port IDs in an IP packet received by a member port meets settings of this parameter, the condition is matched successfully.

SIP

Options: Any/ Specific

Default: Any

Function: Set a condition--source IP address and source IP address mask. When it is set to Specific, an IP address and IP address mask need to be set. When the SIP in an IP packet received by a member port meets settings of this parameter, the condition is matched successfully.

IP Fragment

Options: Any/ Yes/ No

Default: Any

Function: Set a condition--IP fragment packet. When the fragment in an IPv4 packet received by a member port meets settings of this parameter, the condition is matched successfully.

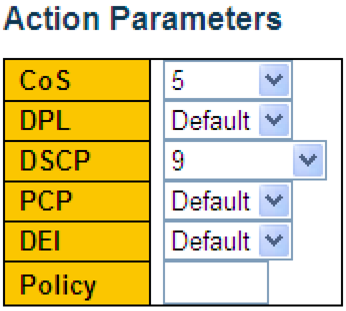
DSCP

Options: Any/ Specific（0~63）/ Range（0~63）

Default: Any

Function: Set a condition--DSCP value. When it is set to Specific, a DSCP value needs to be entered. When it is set to Range, the DSCP range needs to be set. When the DSCP in an IP packet received by a member port meets settings of this parameter, the condition is matched successfully.

➢ Configure the QCL action, as shown in Figure 88.



Action Parameters

CoS	5
DPL	Default
DSCP	9
PCP	Default
DEI	Default
Policy	

Figure 88 Configure the QCL Action

CoS

Options: 0~7/ Default

Default: 0

Function: The CoS value determines the queue for storing packets. The CoS value ranges from 0 to 7, which corresponds to queue 0 to queue 7. The value Default indicates that the CoS value is 0. When a packet received by a member port matches the QCL entry, the switch allocates a CoS value to the packet.

DPL

Options: Default/ 0/ 1

Default: Default

Function: Change the DPL value in a packet received by a member port to the value of this parameter when the packet matches the QCL entry. The value **Default** indicates that the DPL value in a packet is not changed.

DSCP

Options: Default/ 0~63

Default: Default

Function: Change the DSCP value in a packet received by a member port to the value of this parameter when the packet matches the QCL entry. The value Default indicates that the DSCP value in a packet is not changed.

PCP

Options: Default/ 0~7

Default: Default

Function: Change the PCP value in a packet received by a member port to the value of this parameter when the packet matches the QCL entry. The value Default indicates that the PCP value in a packet is not changed.

DEI

Options: Default/ 0/ 1

Default: Default

Function: Change the DEI value in a packet received by a member port to the value of this parameter when the packet matches the QCL entry. The value Default indicates that the DEI value in a packet is not changed.

Policy

options: 0-255

Default: none

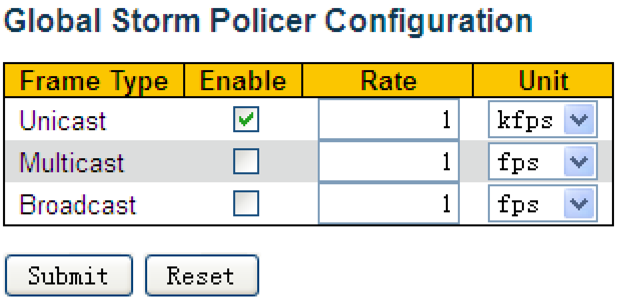
Function: Configure the port policy value to be used with the ACL function.

Caution:

The PCP value and DEI value in a packet cannot be changed separately. That is, the PCP value and DEI value must be changed simultaneously or retain their original values.

3.7.3.14 Storm Policing

1.Configure port storm control, as shown in Figure 89.



Global Storm Policer Configuration

Frame Type	Enable	Rate	Unit
Unicast	☑	1	kfps
Multicast	□	1	fps
Broadcast	□	1	fps

Figure 89 Configure Port Storm Control

Port storm control is to limit the port-received broadcast/unknown multicast/unknown unicast packets. When the rate of broadcast/unknown multicast/unknown unicast packets received on the port exceeds the configured threshold, the system will discard excess broadcast/unknown multicast/unknown unicast packets to keep the broadcast/unknown multicast/unknown unicast traffic within the allowable range, ensuring normal network operation.

Enable

Options: Enabled/Disabled

Default: Disabled

Function: Enable or disable port storm control.

Rate, Unit

Range: 1~1024000fps/ 1~1024kfps

Default: 1fps

Function: Configure the threshold for port rate limiting and the packets that exceed the threshold will be dropped.

3.7.4 Typical Configuration Example

As shown in Figure 90, port1~port5 forward packet to port 6. Among them,

The packets received by port1 are Untag, and the packets entering port 1 are mapped to queue 2.

The PCP value of port 2 received packet is 0, DEI value is 1, and the packets entering port 2 are mapped to queue 3.

The DSCP value of port 3 received packet is 4, and the packets entering port 3 are mapped to queue 6.

Port 4 maps all received packets with the source MAC address of 00-00-00-00-00-23 to queue 5 and changes the DSCP value in these packets to 9 for forwarding.

The DSCP value of port 5 received packet is 5, and the packets entering port 5 are mapped to queue 2.

Port 6 adopts SP+WRR scheduling mode.

Configuration process:

1. Set the CoS value of port 1 is 2, as shown in Figure 64.

2. Enable Tag Class of port 2, and map (PCP=0, DEI=1) to CoS=3, as shown in Figure 65.

3. Enable DSCP Based of port 3 and port 5, as shown in Figure 66.

4. Trust DSCP value 4 and 5, and map DSCP value 4 to queue 6 and DSCP value 5 to queue 2, as shown in Figure 78.

5. Congiure a QCL entry for port 4, as shown in Figure 82.

6. Configure the QCL entry parameters: set SMAC to 00-00-00-00-00-23, and frame type to IPv4, as shown in Figure 83.

7. Configure the QCL entry action parameters: set CoS value to 5 and DSCP value to 9, as shown in Figure 88.

8. Configure port 6 queue scheduling mode to 6 Queues Weighted, queue weight of Q0~Q5 to 20, 40, 40, 20, 20, 20, as shown in Figure 70.

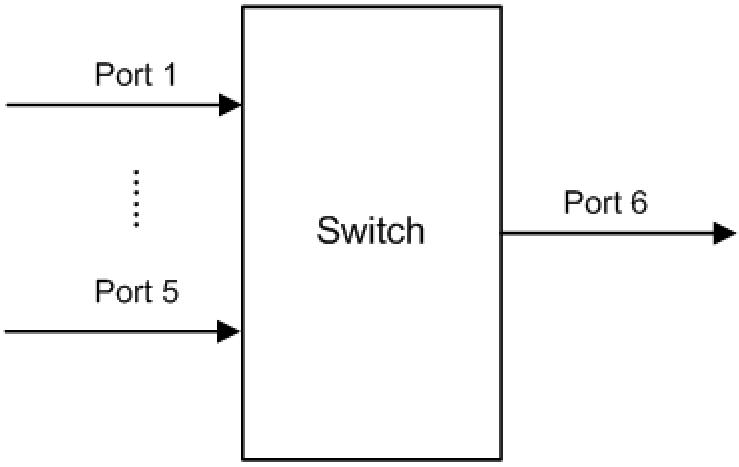


Figure 90 QoS Configuration Example

Port1 and port5 packets enter queue 2, port2 packets enter queue 3, port3 packets enter queue 6, port4 packets enter queue 5.

Queue 6 and queue 7 use the strict priority scheduling mode, and queues 0 through 5 uses the WRR scheduling mode. Data in queue 6 is processed first. When queue 6 is empty, data in queues 0 through 5 is scheduled by weight ratio.

The queue weight are 20, 40, 40, 20, 20, 20. So the bandwidth proportion allocated to the packets in ingress queue 2 is 40/（20+40+40+20+20+20）=25%, that allocated to the packets in ingress queue 3 is 20/（20+40+40+20+20+20）=13%, and that allocated to the packets in ingress queue 5 is 20/（20+40+40+20+20+20）=13%. Among them, port 1 and port 5 packets both enter queue 2, so they are forwarded according to the rule of First In, First out (FIFO), but the total bandwidth proportion of port 1 and port 5 must be 25%.

3.8 Security

3.8.1 User Management

3.8.1.1 Introduction

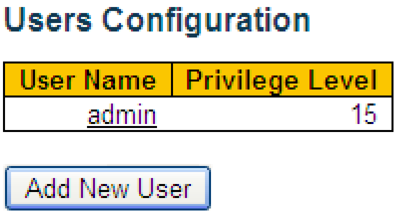
To avoid security problems caused by illegitimate users, the series switches provide hierarchical user management. The switch provides different operation rights based on user levels, satisfying diversified access control requirements. Three user levels are available, as shown in Table 5.

Table 5 User Level

User Level	Privilege Level	Description
Guest	5~9	The lowest level, guest users can only view switch configuration.
System	10~14	Medium level, system users have certain access and configuration rights. System users cannot access the following functions: user management, software update, reboot, load default, and file transmission.
Admin	15	Highest level, admin users have the rights to perform all functions.

3.8.1.2 Web Configuration

1. Create new users, as shown in Figure 91.



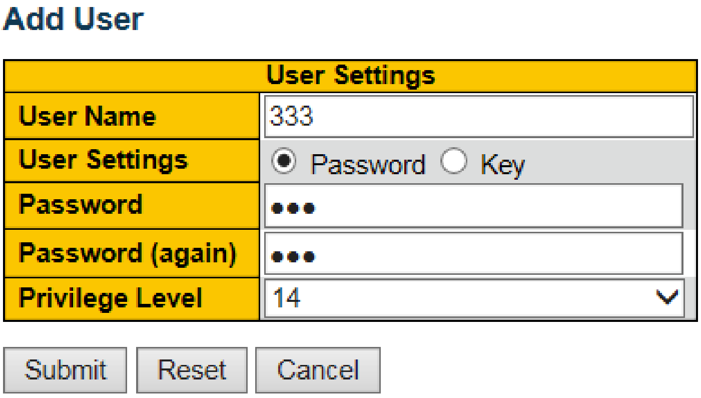
Users Configuration

User Name	Privilege Level
admin	15

Figure 91 Create New Users

Click <Add New User> to configure different level user, the switch supports a maximum of 20 users.

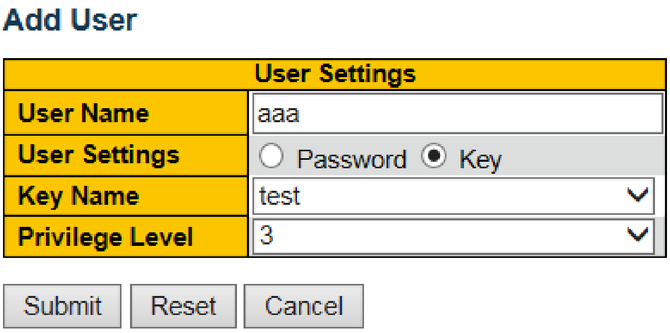
2. Configure different level user, as shown in the following figure.



Add User

User Settings	
User Name	333
User Settings	● Password ○ Key
Password	●●●
Password (again)	●●●
Privilege Level	14

Figure 92 Configure User rating password



Add User

User Settings	
User Name	aaa
User Settings	○ Password ● Key
Key Name	test
Privilege Level	3

Figure 93 Configure User rating key

User Name

Range: 1~31 characters

Function: Configure the user name.

User Settings

Options: Password / Key

Function: Configure the user login authentication mode

Password

Range: 0~31 characters

Function: Configure the password to be used when the current user accesses the switch.

Password (again)

Range: 0~31 characters

Function: Confirm the access password.

Key name

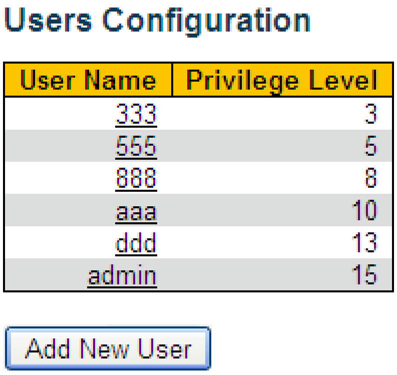
Function: Configure the user login key.

Privilege Level

Range: 0~15

Function: Configure user level, users of different levels have different operation rights.

3. View the users list, as shown in Figure 94.



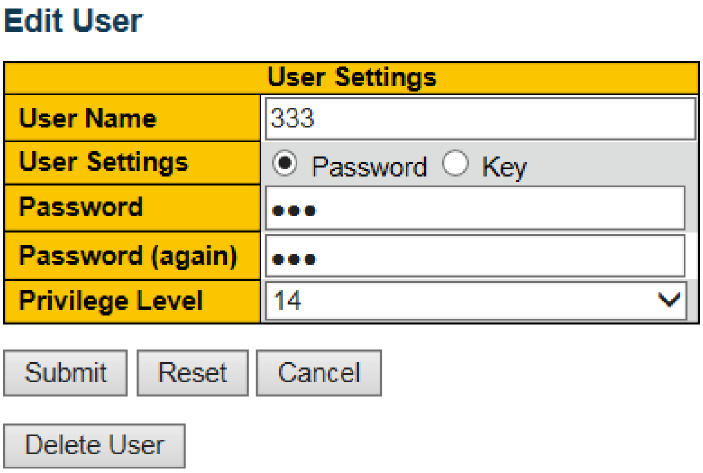
Users Configuration

User Name	Privilege Level
333	3
555	5
888	8
aaa	10
ddd	13
admin	15

Figure 94 Users List

Click <User Name> to modify current user configuration.

4. Modify the user configuration, as shown in Figure 95.



Edit User

User Settings	
User Name	333
User Settings	● Password ○ Key
Password	●●●
Password (again)	●●●
Privilege Level	14

Figure 95 Modify the User Configuration

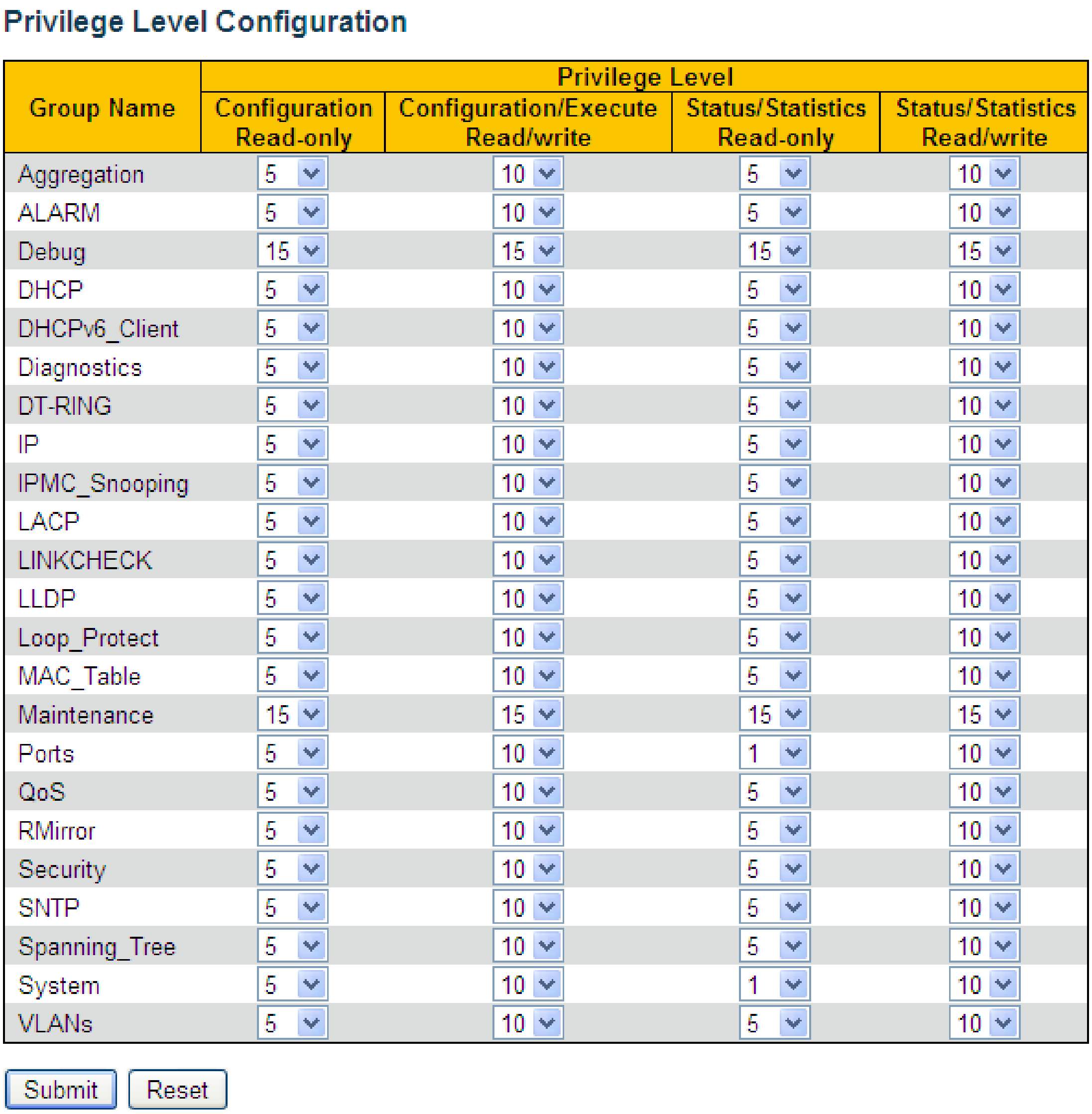
You can modify user password and privilege level.

Click <Delete User> to delete current user.

Note:

- Default user admin cannot be deleted.
- The privilege level of default user is 15, cannot be modified; but the default password (123) can be modified.

5. Configure groups privilege level, as shown in Figure 96.



Privilege Level Configuration

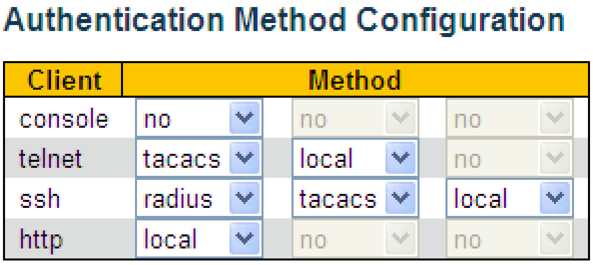
Group Name	Privilege Level			
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
Aggregation	5	10	5	10
ALARM	5	10	5	10
Debug	15	15	15	15
DHCP	5	10	5	10
DHCPv6_Client	5	10	5	10
Diagnostics	5	10	5	10
DT-RING	5	10	5	10
IP	5	10	5	10
IPMC_Snooping	5	10	5	10
LACP	5	10	5	10
LINKCHECK	5	10	5	10
LLDP	5	10	5	10
Loop_Protect	5	10	5	10
MAC_Table	5	10	5	10
Maintenance	15	15	15	15
Ports	5	10	1	10
QoS	5	10	5	10
RMirror	5	10	5	10
Security	5	10	5	10
SNTP	5	10	5	10
Spanning_Tree	5	10	5	10
System	5	10	1	10
VLANs	5	10	5	10

Figure 96 Configure groups privilege level

When the user privilege level is same or greater than a group privilege level, the user can access or configure the group. The access or configure right is based on the user privilege level.

3.8.2 Authentication login configuration

Configure access mode to switch, authentication mode and authentication order, as shown in Figure 97.



Authentication Method Configuration

Client	Method		
console	no	no	no
telnet	tacacs	local	no
ssh	radius	tacacs	local
http	local	no	no

Figure 97 Authentication Login Configuration

Client

Options: console/telnet/ssh/http

Function: Select access mode to switch.

Method 1/Method 2/Method 3

Options: no/local/tacacs/radius

Default: local

Function: The methods from left to right are method 1, method 2, and method 3. Select the order of authentication. Authentication method 1 is first performed. If the authentication fails, authentication method 2 is conducted. If both authentications method 1 and authentication method 2 fail, authentication method 3 is conducted.

Description: **no** means authentication is disabled and login is not possible. **local** means using username and password set in local to perform authentication. **tacacs** means using the username and password set in TACACS+ server for authentication. **radius** means using the username and password set in RADIUS server for authentication.

Caution:

If tacacs/radius is selected for method 1 and method 2, it is recommended to configure method 3 as local. This will enable the management client to login switch vis the local user if none of the configured remote authentication servers are alive.

3.8.3 SSH Configuration

3.8.3.1 Introduction

SSH (Secure Shell) is a network protocol for secure remote login. It encrypts all transmitted data to prevent information disclosure. When data is encrypted by SSH, users can only use command lines to configure switches.

The switch supports the SSH server function and allows the connection of multiple SSH users that log in to the switch remotely through SSH.

3.8.3.2 Key

Unencrypted information is called plain text, and encrypted information is called ciphertext, and encryption and decryption are carried out under key control. A key is a set of specific strings that are the only parameter that controls the exchange of plaintext and ciphertext and acts as a "key". The encryption operation can turn the plaintext into a ciphertext, and the decryption operation can restore the ciphertext to plaintext.

Key-based security authentication requires a key, that is, there is a pair of keys at each end of the communication, that is, a private key and a public key. You can use the public key to encrypt the message, and then use the private key to use the private key to decrypt the data, so as to ensure the confidentiality of the data.

3.8.3.3 Implementation

In order to realize the SSH secure connection in the communication process, the server and the client experience the following five stages:

Version negotiation stage: currently, SSH consists of two versions: SSH1 and SSH2. The two parties negotiate a version to use.

Key and algorithm negotiation stage: SSH supports multiple types of encryption algorithms. The two parties negotiate an algorithm to use.

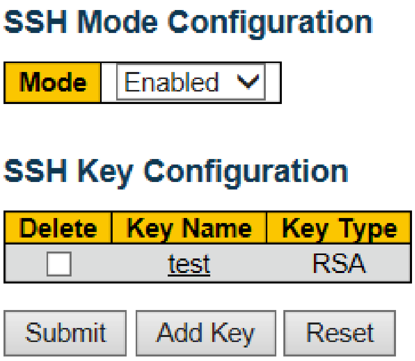
Authentication state: the SSH client sends an authentication request to the server and the server authenticates the client.

Session request stage: the client sends a session request to the server after passing the authentication.

Session stage: the client and the server start communication after passing the session request.

3.8.3.4 Web Configuration

1. Enable SSH protocol, as shown in Figure 98.



SSH Mode Configuration

Mode	Enabled

SSH Key Configuration

Delete	Key Name	Key Type
□	test	RSA

Figure 98 Enable SSH Protocol

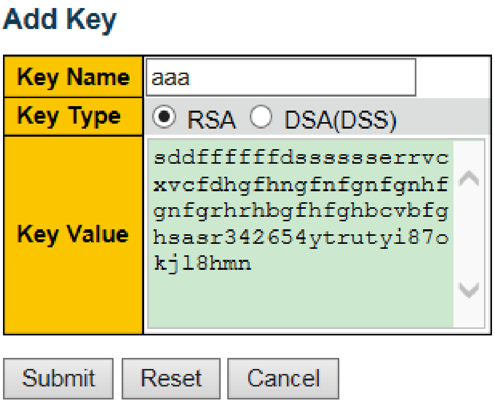
Mode

Options: Enabled/Disabled

Default: Enabled

Function: Enable/Disable SSH protocol. If it is enabled, the switch works as the SSH server.

2.click "Add Key" to enter the Add Key interface, as shown in the following figure.



Add Key

Key Name	aaa
Key Type	● RSA ○ DSA(DSS)
Key Value	sddffffffdsssssserrvc xvcfdhgfhngfnfgnfgnhf gnfgrhrhbgfhfghbcvbfg hsasr342654ytrutyi87o kjl8hmn

Figure 99 Add Key

Key name

Range: 3-20 characters**Key type**

Options: RSA / DSA

Default configuration: RSA

Key Value

Format: {public key}

Algorithm name: ssh-rsa | ssh-dsa

Public key: based on 64-bit code, less than 2048 bytes in length

Key information: More information about the key

Function: Configure the public key of the client, usually generated by the Puttygen software and copied to the server's key value, the private key stored in the client.

3.8.3.5 Typical Configuration Example

The Host works as the SSH client to establish a local connection with switch, as shown in Figure 100.

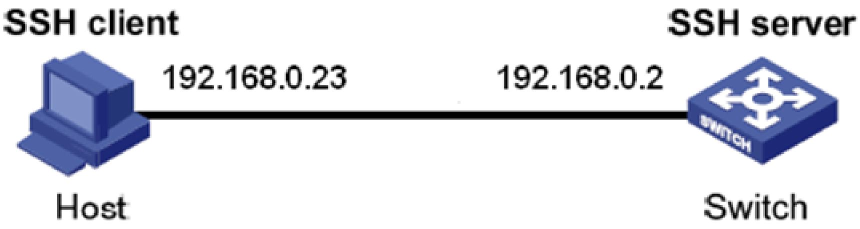
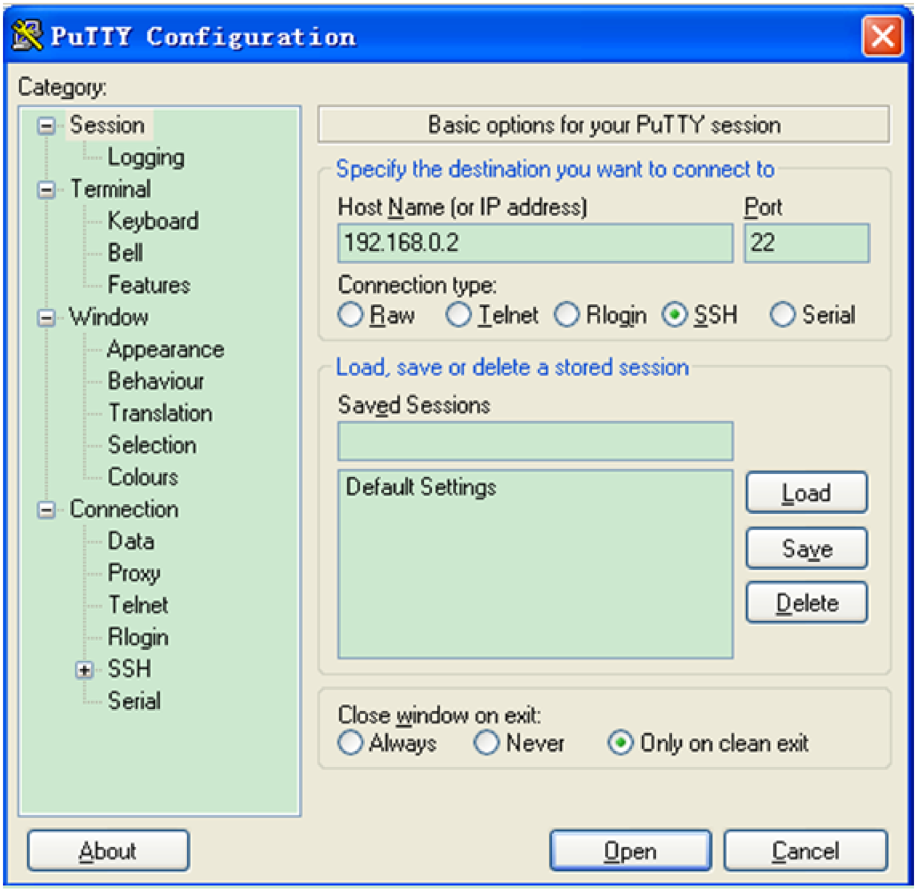


Figure 100 SSH Configuration Example

- SSH users use password authentication.

1. Configure user name: 333, authentication type: password, password: 123, as shown in Figure 92.

2. Establish the connection with the SSH server. First, run the PuTTY.exe software, as shown in Figure 101; input the IP address of the SSH server "192. 168.0.2" in the space of Host Name (or IP address).



Specify the destination you want to connect to

Host Name (or IP address): 192.168.0.2

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

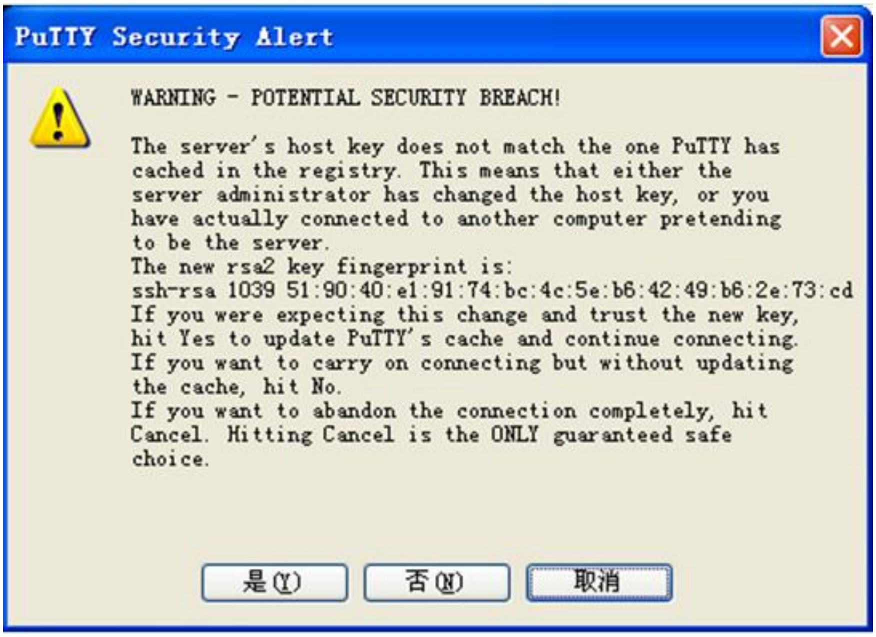
Saved Sessions

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

Figure 101 SSH Client Configuration

3. Click <Open> button and following warning message appears shown in Figure 102, click the <是(Y)> button.

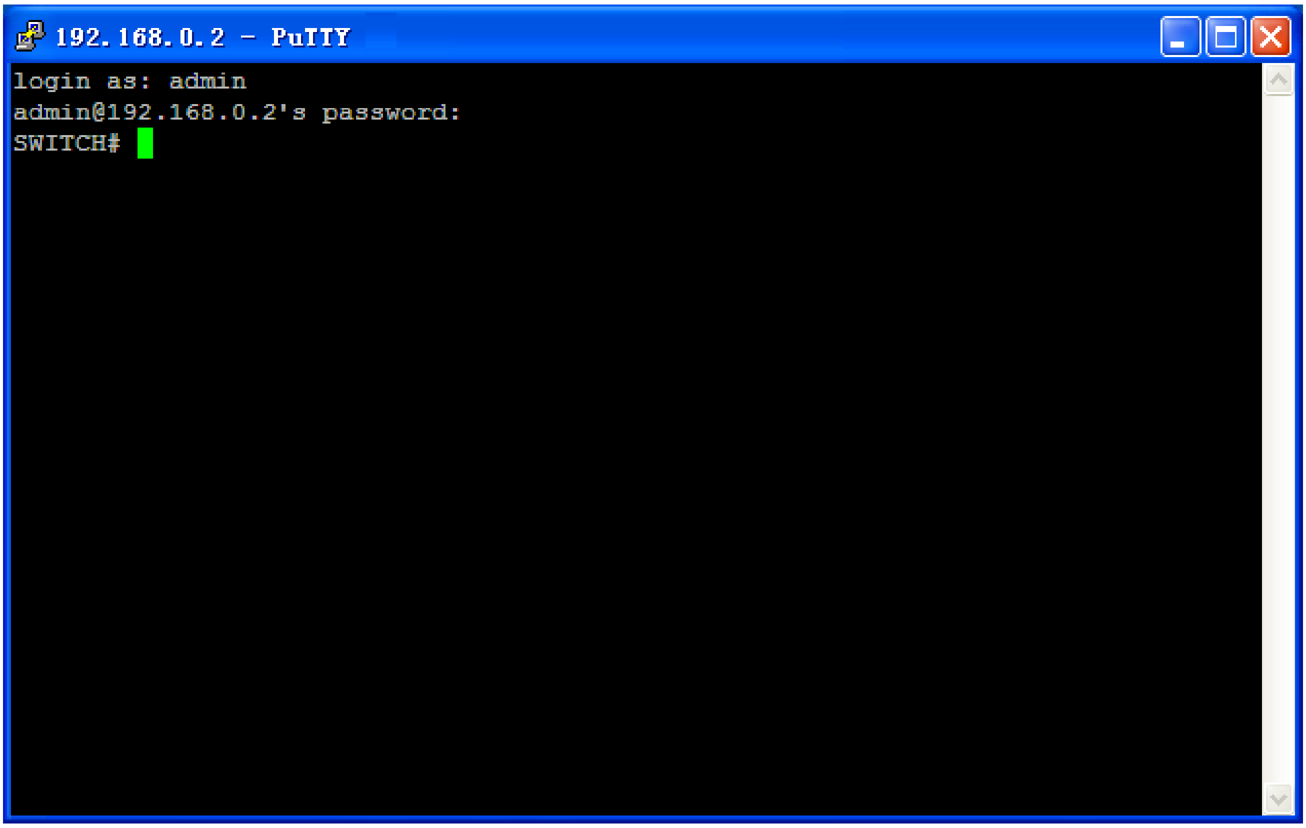


WARNING - POTENTIAL SECURITY BREACH!

The server's host key does not match the one PuTTY has cached in the registry. This means that either the server administrator has changed the host key, or you have actually connected to another computer pretending to be the server.
The new rsa2 key fingerprint is:
ssh-rsa 1039 51:90:40:e1:91:74:bc:4c:5e:b6:42:49:b6:2e:73:cd
If you were expecting this change and trust the new key, hit Yes to update PuTTY's cache and continue connecting.
If you want to carry on connecting but without updating the cache, hit No.
If you want to abandon the connection completely, hit Cancel. Hitting Cancel is the ONLY guaranteed safe choice.

Figure 102 Warning Message

4. Input the user name "admin" and the password "123" to enter the switch configuration interface, as shown in Figure 103.

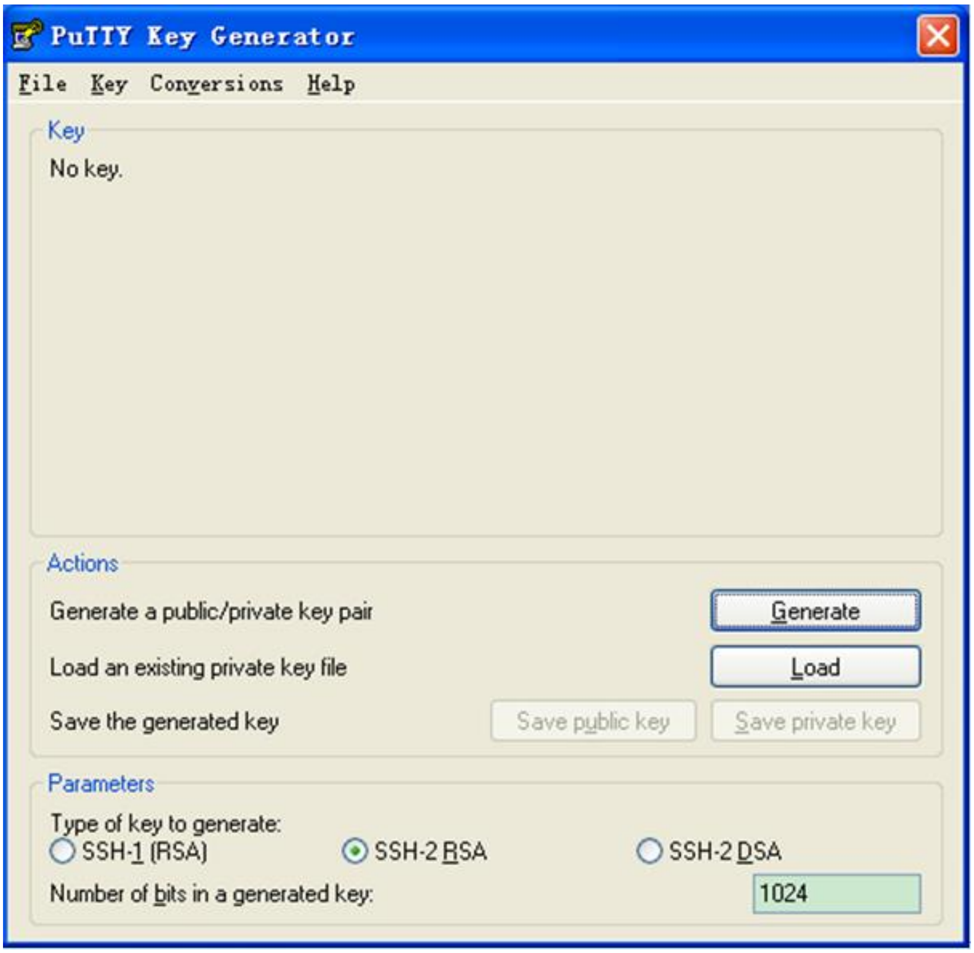


```
login as: admin
admin@192.168.0.2's password:
SWITCH#
```

Figure 103 Login Interface of the SSH Authentication

➢ SSH users use key authentication.

1. configure the SSH client, as shown in Figure 93.run the PuTTY.exe software, click the <Generate> button to generate the client key pair, as shown in Figure 104.



No key.

Generate a public/private key pair

Load an existing private key file

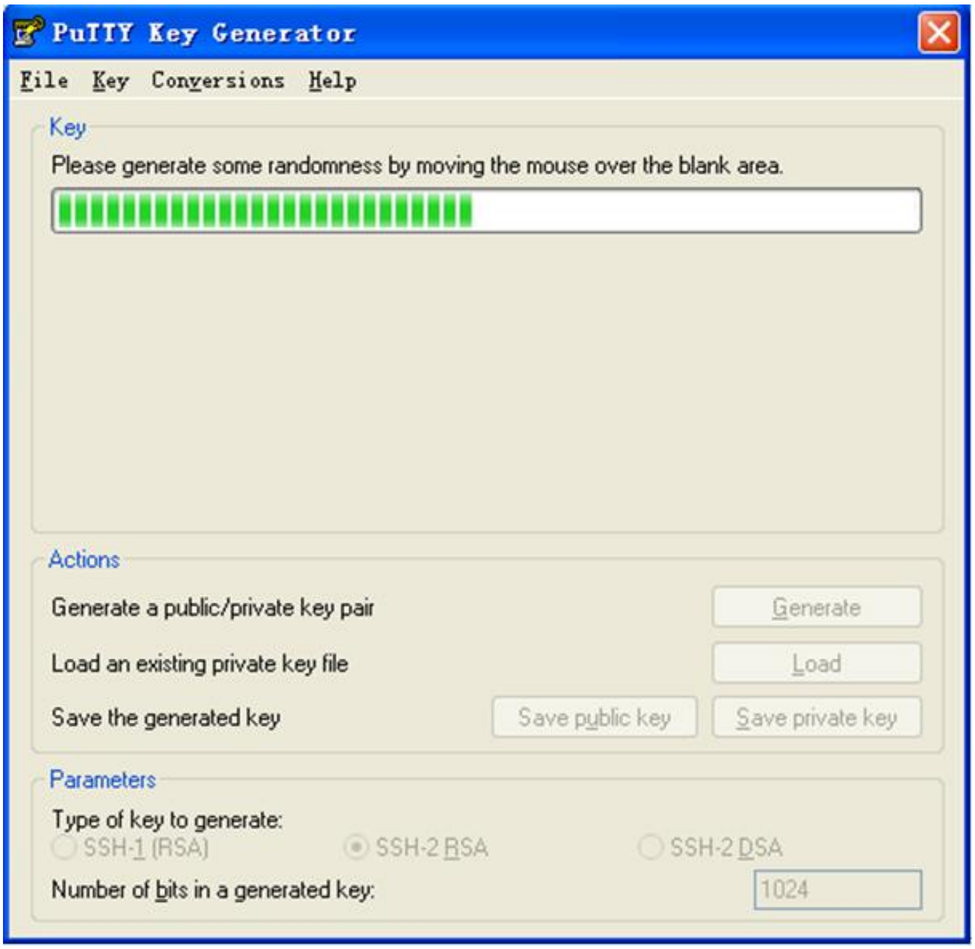
Save the generated key

Type of key to generate:
○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 1024

Figure 104 Generate the client key

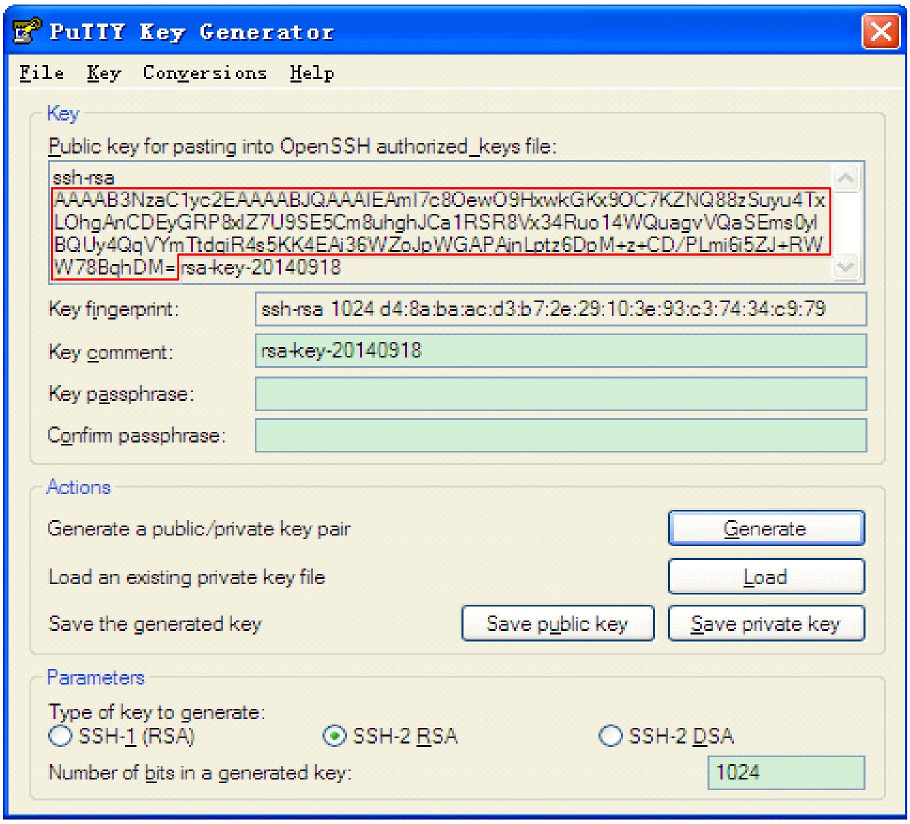
2. generate the client key pair in the process of moving the mouse in the window, otherwise the process does not move, the key to stop generating, as shown in Figure 105.



PuTTY Key Generator
File Key Conversions Help
Key
Please generate some randomness by moving the mouse over the blank area.
Actions
Generate a public/private key pair
Generate
Load an existing private key file
Load
Save the generated key
Save public key
Save private key
Parameters
Type of key to generate:
○ SSH-1 (RSA)
● SSH-2 RSA
○ SSH-2 DSA
Number of bits in a generated key:
1024

Figure 105 Key generation process

3. Figure 106 shows the key, click the <Save private key> button to store the private key 444.ppk file, and copy the public key to the SSH key configuration key value and enter the key name 444, as shown in Figure 99.



Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAIEAmI7c8OewO9HxwkGKx9OC7KZNQ88zSuyu4Tx
LOhgAnCDEyGRP8xlZ7U9SE5Cm8uhghJCa1RSR8Vx34Ruo14WQuagvVQaSEms0yl
BQUy4QqVYmTtdqiR4s5KK4EAi36WZoJpWGAPAjnLptz6DpM+z+CD/PLmi6i5ZJ+RW
W78BqhDM= rsa-key-20140918
```

Key fingerprint: ssh-rsa 1024 d4:8a:ba:ac:d3:b7:2e:29:10:3e:93:c3:74:34:c9:79

Key comment: rsa-key-20140918

Key passphrase:

Confirm passphrase:

Generate a public/private key pair

Load an existing private key file

Save the generated key

Type of key to generate:
○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 1024

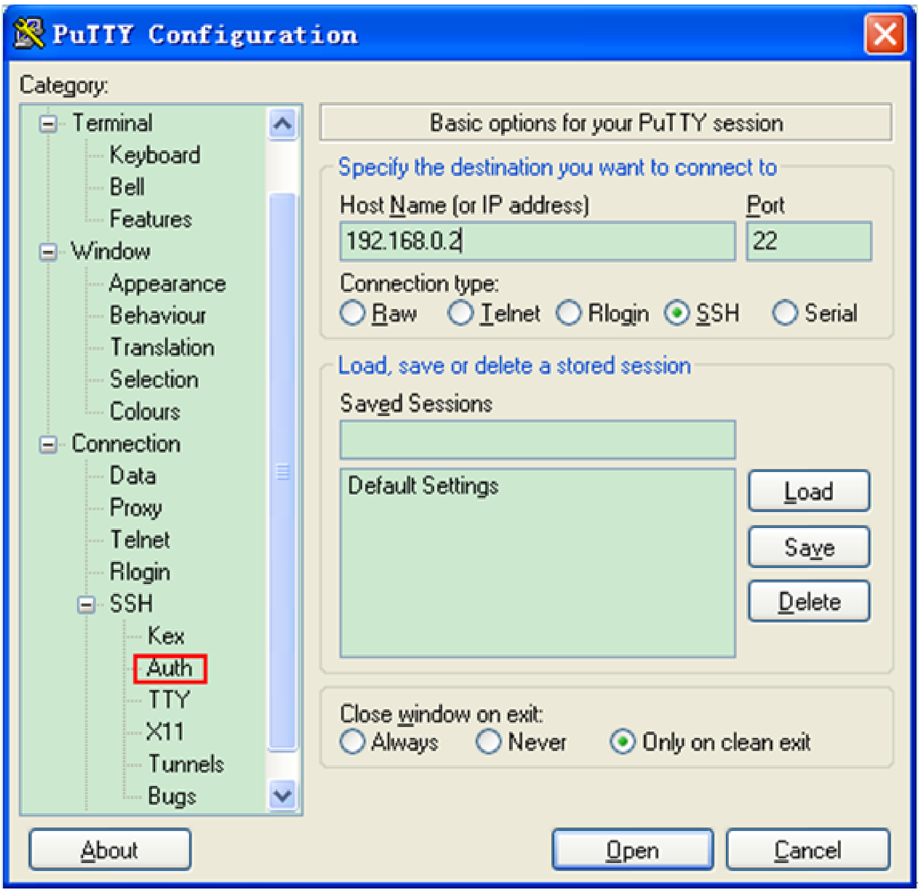
Figure 106 Generates a key value

Note:

Copy the public key to the WEB page SSH configuration, just copy the red part of the content, otherwise it will pop up an error message "key value contains illegal characters, please use the alphanumeric slash and equal sign."

4. Configure SSH user name: 444, authentication type: key, key: 444, as shown in Figure 93.

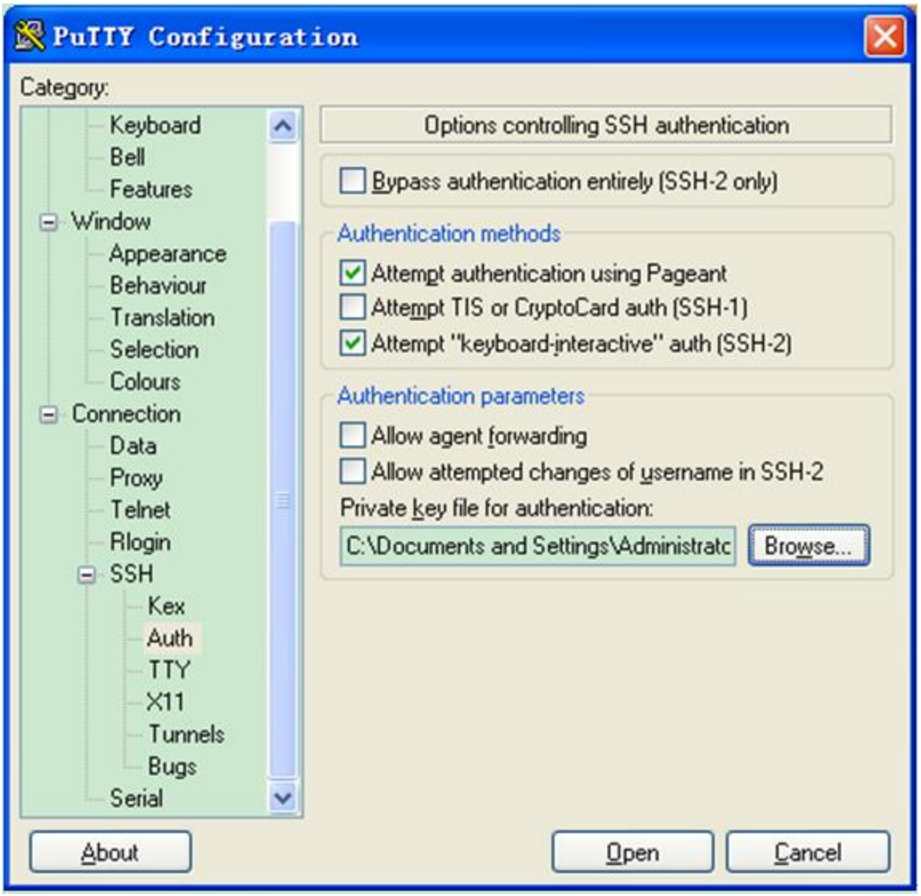
5. Establish the connection with the SSH server. First, run the PuTTY.exe software, as shown in Figure 107; input the IP address of the SSH server "192. 168.0.2" in the space of Host Name (or IP address).



Host Name (or IP address): 192.168.0.2
Port: 22
Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial
Close window on exit: ○ Always ○ Never ● Only on clean exit

Figure 107 SSH Client Configuration

6. Click on the left side of Figure 107 [SSH] → [Auth], shown in Figure 108 appears, click the <Browse> button, select the private key file stored in step 4.



Options controlling SSH authentication

□ Bypass authentication entirely (SSH-2 only)

Authentication methods

☑ Attempt authentication using Pageant

□ Attempt TIS or CryptoCard auth (SSH-1)

☑ Attempt "keyboard-interactive" auth (SSH-2)

Authentication parameters

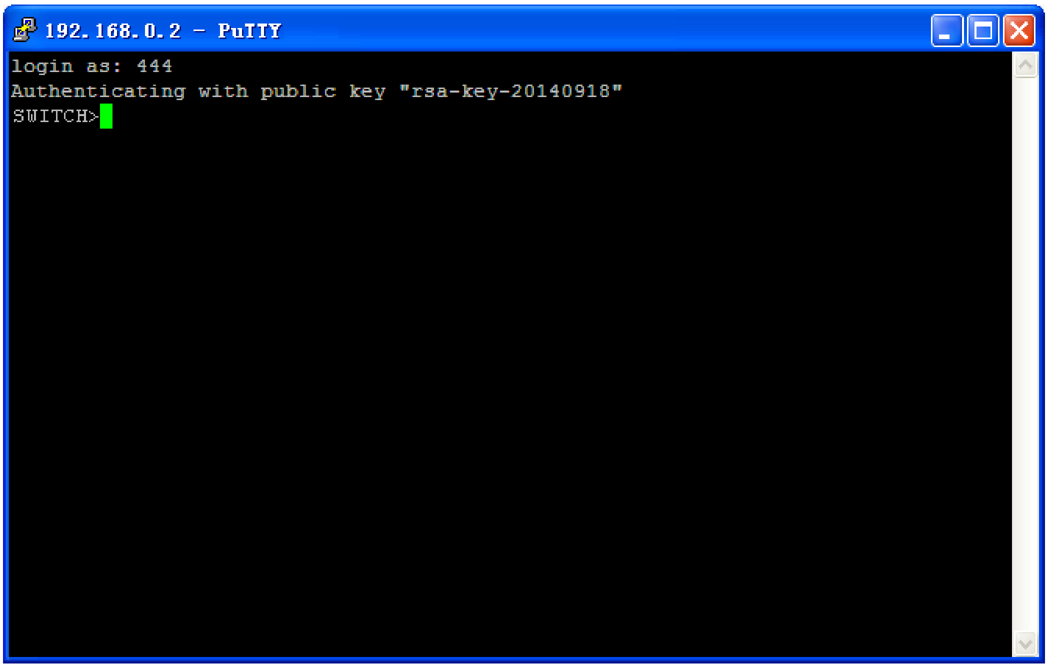
□ Allow agent forwarding

□ Allow attempted changes of username in SSH-2

Private key file for authentication: C:\Documents and Settings\Administratc

Figure 108 Select the key file

7. Click the <Open> button, follow the prompts to enter the user name, you can enter the switch configuration interface, as shown in Figure 109.



```
login as: 444
Authenticating with public key "rsa-key-20140918"
SWITCH>
```

Figure 109 Login Interface of the key authentication

3.8.4 SSL Configuration

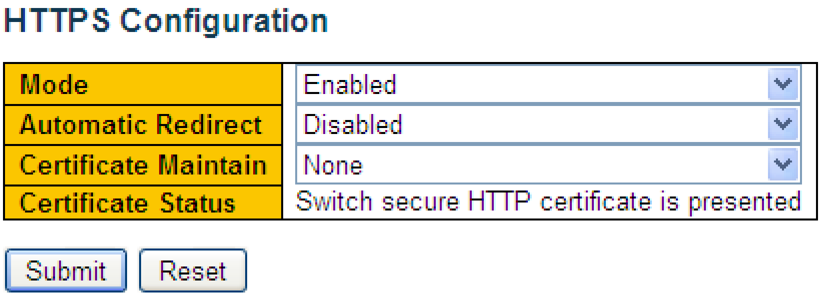
3.8.4.1 Introduce

SSL (Secure Socket Layer) is a security protocol and provides the security link for the TCP-based application layer protocol, such as HTTPS. SSL encrypts the network connection at the transport layer and uses the symmetric encryption algorithm to guarantee the data security, and uses the secret key authentication code to ensure the information reliability. This protocol is widely used in Web browser, receiving and sending emails, network fax, real time communication, and so on, providing an encryption protocol for the security transmission in the network.

Once a switch enables SSL, users must use the secure link https, such as https://192.168.0.2, to access the switch.

3.8.4.2 Web Configuration

1. Enable HTTPS protocol, as shown in Figure 110.



HTTPS Configuration

Mode	Enabled
Automatic Redirect	Disabled
Certificate Maintain	None
Certificate Status	Switch secure HTTP certificate is presented

Figure 110 Enable HTTPS Protocol

Mode

Options: Enabled/Disabled

Default: Disabled

Function: Enable or disable the HTTPS protocol. After enabling HTTPS, users can use http://*ip address* and the secure link https://*ip address* to access the switch.

Automatic Redirect

Options: Enabled/ Disabled

Default: Disabled

Function: Enabled means users must use the secure link https://*ip address* to access the switch. Disabled means users can use http://*ip address* and the secure link https://*ip address* to access the switch. The parameter “Automatic Redirect” can be configured only if the “Mode” is enabled.

Certificate Maintain

Options: None/Delete/Upload/Generate

Default: None

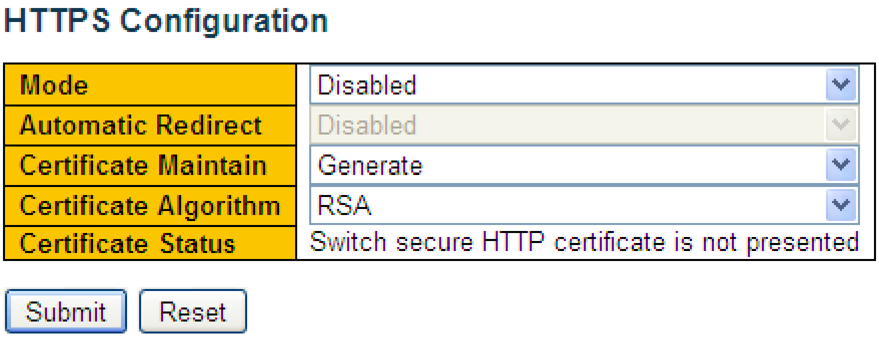
Function: Maintain the HTTPS certificate. The parameter “Certificate Maintain” can be configured only if the “Mode” is disabled. **Delete** is used to delete an existing HTTPS certificate from the switch. **Upload** is used to upload a correct HTTPS certificate to the switch by using the web browser or URL. **Generate** indicates that the switch automatically generates a correct HTTPS certificate.

Certificate Status

Options: Switch secure HTTP certificate is presented/Switch secure HTTP certificate is not presented/Switch secure HTTP certificate is generating

Function: Displays the HTTPS certificate status in the switch. **Switch secure HTTP certificate is presented** indicates that a certificate is available in the switch. In this case, you can log in to the Web Page of the switch over HTTPS. **Switch secure HTTP certificate is not presented** indicates that no certificate is available in the switch. In this case, you cannot log in to the Web page over HTTPS. **Switch secure HTTP certificate is generating** indicates that an HTTPS certificates is being generated.

2. Gnerate HTTPS certificate, as shown in Figure 111.



HTTPS Configuration

Mode	Disabled
Automatic Redirect	Disabled
Certificate Maintain	Generate
Certificate Algorithm	RSA
Certificate Status	Switch secure HTTP certificate is not presented

Figure 111 Generate Certificate

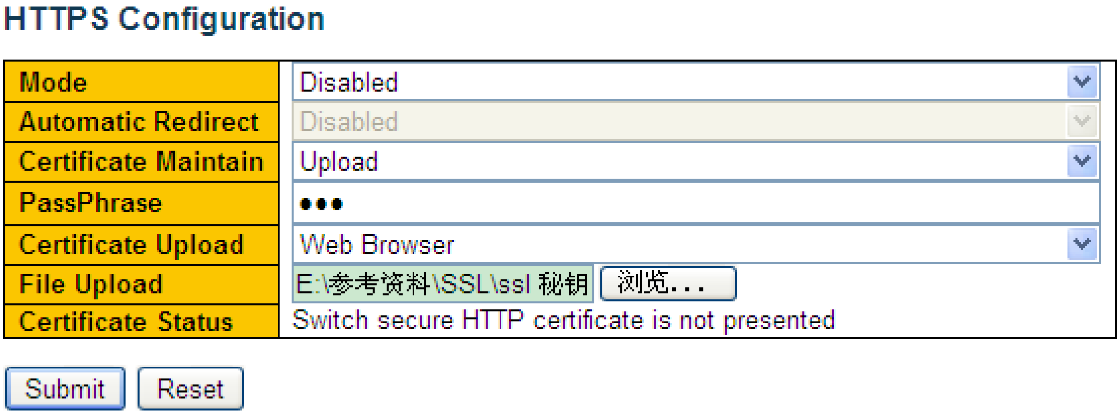
Certificate Algorithm

Options: RSA/DSA

Default: RSA

Function: Select the algorithm for generating HTTPS certificate.

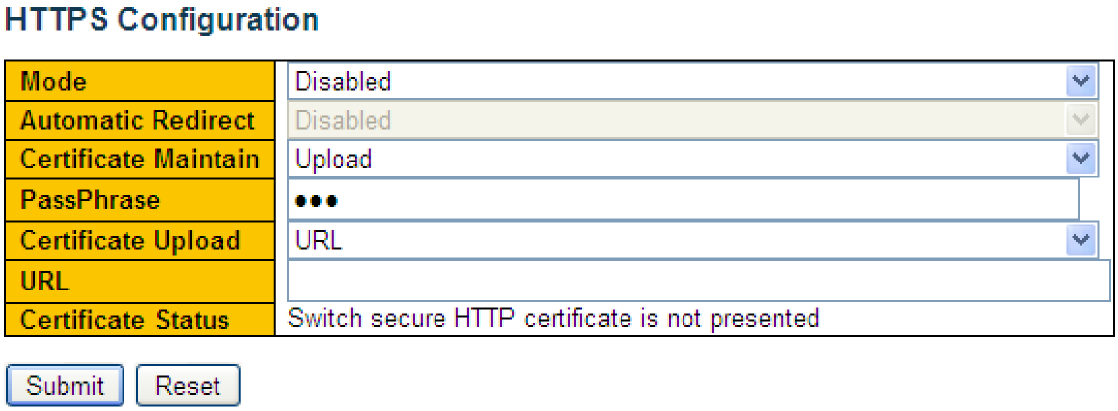
3. Upload HTTPS certificate, as shown in Figure 112, Figure 113.



HTTPS Configuration

Mode	Disabled
Automatic Redirect	Disabled
Certificate Maintain	Upload
PassPhrase	•••
Certificate Upload	Web Browser
File Upload	E:\参考资料\SSL\ssl 秘钥 浏览...
Certificate Status	Switch secure HTTP certificate is not presented

Figure 112 Upload Certificate -Web Browser



HTTPS Configuration

Mode	Disabled
Automatic Redirect	Disabled
Certificate Maintain	Upload
PassPhrase	•••
Certificate Upload	URL
URL	
Certificate Status	Switch secure HTTP certificate is not presented

Figure 113 Upload Certificate -URL

PassPhrase

Function: It is used for encrypting the certification.

Certificate Upload

Options: Web Browser/URL

Default: Web Browser

Function: Select the certificate upload method.

File Upload

Function: Select the HTTPS certificate file stored in local.

URL

Function: Configure the storage path of the HTTPS certificate file. The supported protocols are HTTP, HTTPS, TFTP, and FTP, the configuration format is as follows: http://10.10.10.10:80/new_image_path/new_image.dat or FTP://username:password@10.10.10.10/new_image_path/new_image.dat.

4. When the HTTPS certificate is presented in switch, input the username and password to successfully log into switch through HTTPS.

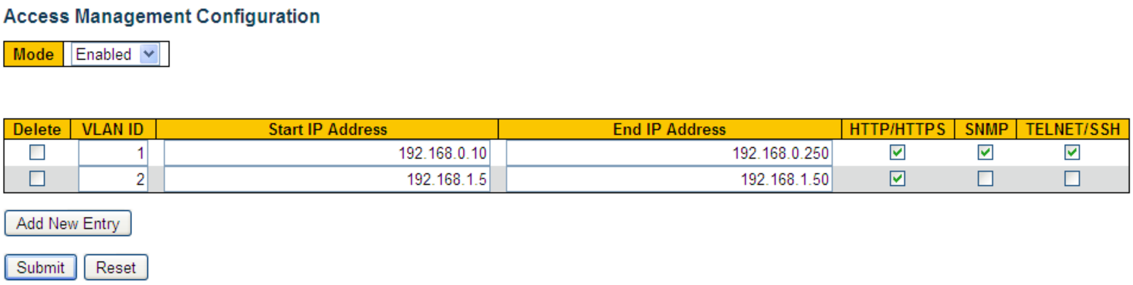
3.8.5 Access Management

3.8.5.1 Introduction

Access entries can be configured to manage access to the switch, so as to restrict the hosts that can access the switch as well as the access mode. A maximum of 16 access entries can be configured. A host that matches any of the access entries can successfully access the switch.

3.8.5.2 Web Configuration

1. Configure access management entry, as shown in Figure 114.



Access Management Configuration

Mode: Enabled

Delete	VLAN ID	Start IP Address	End IP Address	HTTP/HTTPS	SNMP	TELNET/SSH
□	1	192.168.0.10	192.168.0.250	☑	☑	☑
□	2	192.168.1.5	192.168.1.50	☑	□	□

Figure 114 Configure Access Management Entry

Mode

Options: Enabled/Disabled

Default: Disabled

Function: Enable or disable the switch access management. Disable: the access to the switch is not restricted.

VLAN ID

Range: 1~4094

Function: Configure the VLAN ID of access management entry.

Start IP Address/End IP Address

Function: Configure the IP address range of access management entry.

HTTP/HTTPS

Function: When HTTP/HTTPS is selected, a host that matches the VLAN ID and IP address in an access entry can access the switch over HTTP/HTTPS.

SNMP

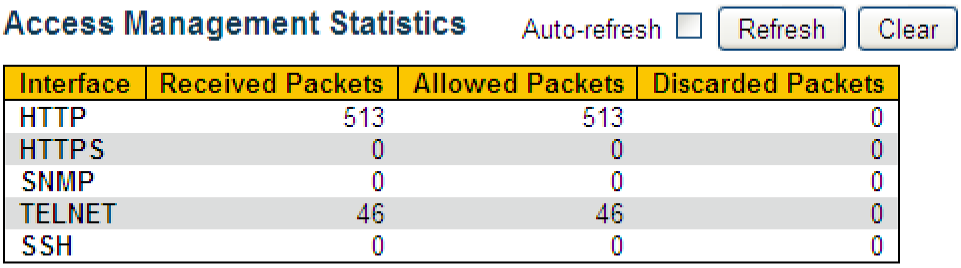
Function: When SNMP is selected, a host that matches the VLAN ID and IP address in an access entry can access the switch over SNMP.

TELNET/SSH

Function: When TELNET/SSH is selected, a host that matches the VLAN ID and IP address in an access entry can access the switch over TELNET/SSH.

Click <Add New Entry> to configure the access manegement entry, the switch supports a maximum of 16 access manegement entries.

2. View access management statistics, as shown in Figure 115.



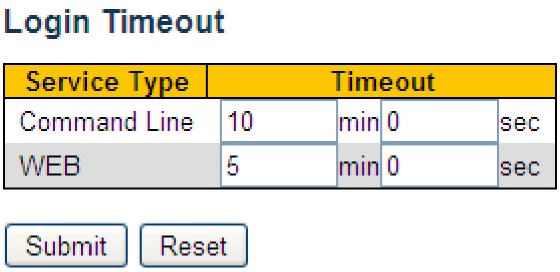
Access Management Statistics

Auto-refresh □ Refresh Clear

Interface	Received Packets	Allowed Packets	Discarded Packets
HTTP	513	513	0
HTTPS	0	0	0
SNMP	0	0	0
TELNET	46	46	0
SSH	0	0	0

Figure 115 View Access Management Statistics

3. Configure timeouts for switch access modes, as shown in Figure 116.



Login Timeout

Service Type	Timeout
Command Line	10 min 0 sec
WEB	5 min 0 sec

Submit Reset

Figure 116 Configure Timeouts for Switch Access Modes

Timeout

Range: (0~1440) min (0~3600) s

Default: 10 min for Command Line, 5 min for web

Function: Configure the login user timeout and disconnection time. The time starts counting when a user finishes all configurations, and the system will automatically exit the access mode when the time ends. When the time is set to 0, the user timeout and disconnection function is disabled. In this case, the server will not judge whether the user login times out and therefore the user will not exit the current login mode.

3.8.6 SNMP v1/SNMP v2c

3.8.6.1 Introduction

The Simple Network Management Protocol (SNMP) is a framework using TCP/IP to manage network devices. With the SNMP function, the administrator can query device information, modify parameter settings, monitor device status, and discover network faults.

3.8.6.2 Implementation

SNMP adopts the management station/agent mode. Therefore, SNMP involves two types of NEs: NMS and agent.

The Network Management Station (NMS) is a station running SNMP-enabled network management software client. It is the core for the network management of an SNMP network.

Agent is a process in the managed network devices. It receives and processes request packets from the NMS. When an alarm occurs, the agent proactively reports it to the NMS.

The NMS is the manager of an SNMP network, while agent is the managed device of the SNMP network. The NMS and agents exchange management packets through SNMP.

SNMP involves the following basic operations:

Get-Request

Get-Response

Get-Next-Request

Set-Request

Trap

The NMS sends Get-Request, Get-Next-Request, and Set-Request packets to agents to query, configure, and manage variables. After receiving these requests, agents reply with Get-Response packets. When an alarm occurs, an agent proactively reports it to the NMS with a trap packet.

3.8.6.3 Explanation

This series switches support SNMP v2c. SNMP v2c is compatible with SNMPv1.

SNMP v1 uses community name for authentication. A community name acts as a password, limiting NMS's access to agents. If the community name carried by an SNMP packet is not acknowledged by the switch, the request fails and an error message is returned.

SNMP v2c also uses community name for authentication. It is compatible with SNMP v1, and extends the functions of SNMP v1.

To enable the communication between the NMS and agent, their SNMP versions must match. Different SNMP version can be configured on an agent, so that it can use different versions to communicate with different NMSs.

3.8.6.4 MIB Introduction

Any managed resource is called managed object. The Management Information Base (MIB) stores managed objects. It defines the hierarchical relationships of managed objects and attributes of objects, such as names, access permissions, and data types. Each agent has its own MIB. The NMS can read/write MIBs based on permissions. Figure 117 shows the relationships among the NMS, agent, and MIB.

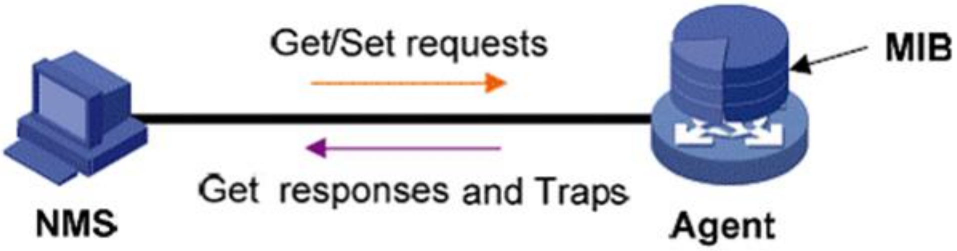


Figure 117 Relationship among NMS, Agent, and MIB

MIB defines a tree structure. The tree nodes are managed objects. Each node has a unique

Object Identifier (OID), which indicates the location of the node in the MIB structure. As shown in Figure 118, the OID of object A is 1.2.1.1.

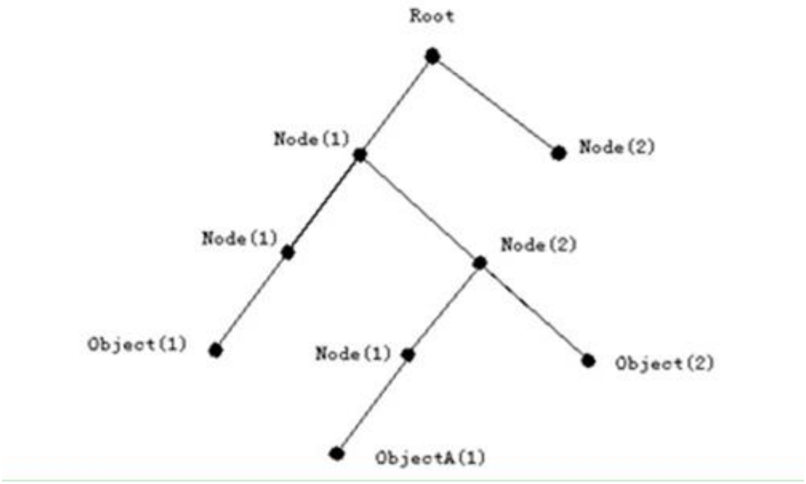
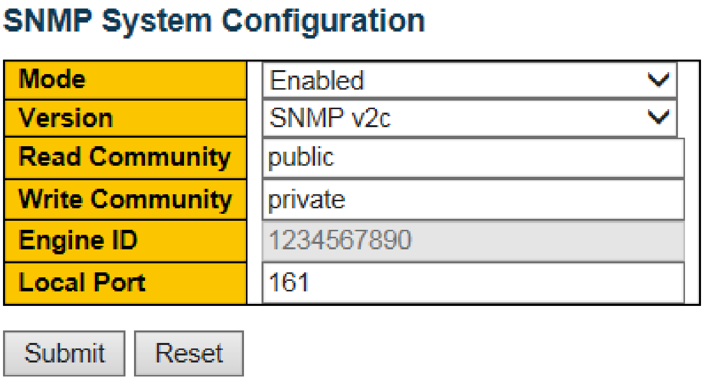


Figure 118 MIB Structure

3.8.6.5 Web Configuration

1. Enable SNMP protocol and select SNMP version, as shown in Figure 119.



SNMP System Configuration

Mode	Enabled
Version	SNMP v2c
Read Community	public
Write Community	private
Engine ID	1234567890
Local Port	161

Figure 119 Enable SNMP Protocol and Select SNMP Version

Mode

Options: Enabled/Disabled

Default: Enabled

Function: Enable/Disable SNMP.

Version

Options: SNMP v1/SNMP v2c/SNMP v3

Default: SNMP v2c

Function: Choose a SNMP version. SNMP v2c is compatible with SNMP v1; SNMP v3 is compatible with SNMP v1 and SNMP v2c.

Read Community

Range: 0~255 characters

Default: public

Function: Configure the name of read-only community.

Description: The MIB information of the switch can be read only if the community name carried by an SNMP packet is identical with that configured on the switch.

Read Community

Range: 0~255 characters

Default: private

Function: Configure the name of read-write community.

Description: The MIB information of the switch can be read and written only if the community name carried by an SNMP packet is identical with that configured on the switch.

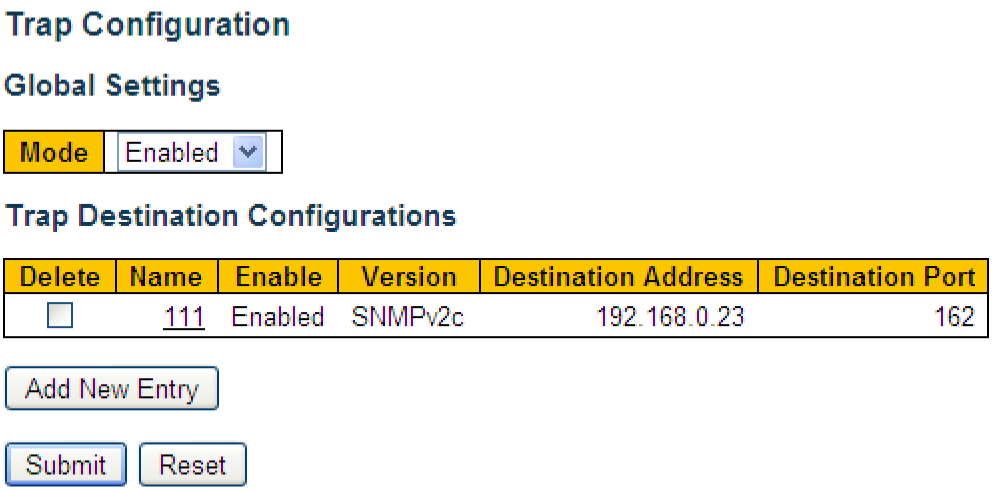
Local port

Range: 1 ~ 65535

Default: 161

Function: Configure the port number to receive SNMP requests.

2. Configure global trap mode, as shown in Figure 120.



Trap Configuration

Global Settings

Mode	Enabled

Trap Destination Configurations

Delete	Name	Enable	Version	Destination Address	Destination Port
□	111	Enabled	SNMPv2c	192.168.0.23	162

Figure 120 Configure Global Trap Mode

Mode

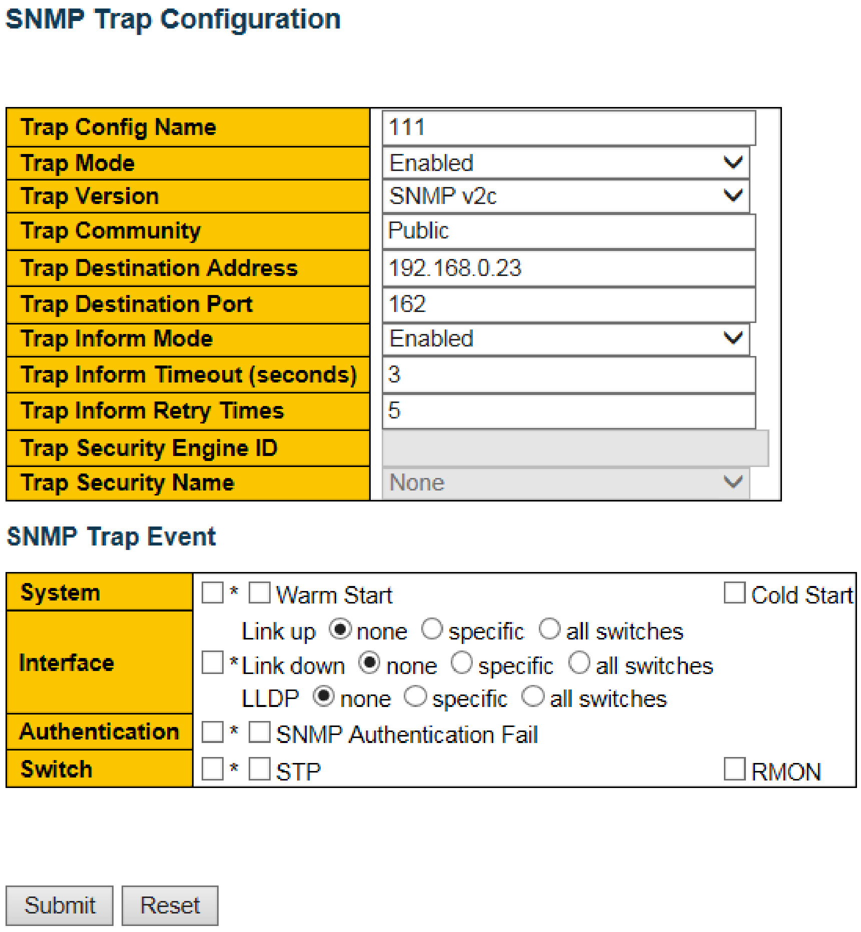
Options: Enabled/Disabled

Default: Disabled

Function: Enable/Disable global trap mode.

Cilck <Add New Entry> to configure trap entry, the switch supports a maximum of 4 trap entries. Click <Name> to modify the trap entry.

3. Configure trap entry, as shown in Figure 121.



SNMP Trap Configuration

Trap Config Name	111
Trap Mode	Enabled
Trap Version	SNMP v2c
Trap Community	Public
Trap Destination Address	192.168.0.23
Trap Destination Port	162
Trap Inform Mode	Enabled
Trap Inform Timeout (seconds)	3
Trap Inform Retry Times	5
Trap Security Engine ID	
Trap Security Name	None

SNMP Trap Event

System	□ * □ Warm Start □ Cold Start
Interface	Link up ● none ○ specific ○ all switches □ * Link down ● none ○ specific ○ all switches LLDP ● none ○ specific ○ all switches
Authentication	□ * □ SNMP Authentication Fail
Switch	□ * □ STP □ RMON

Figure 121 Configure Trap Entry

Trap Config Name

Range: 1~255 characters

Function: Configure trap entry name.

Trap Mode

Options: Enabled/Disabled

Default: Disabled

Function: Enable/Disable the trap entry. After enabling the trap mode, switch can send trap message to NMS.

Trap Version

Options: SNMP v1/SNMP v2c/SNMP v3

Default: SNMP v2c

Function: Set the version of trap packets sent from the switch to the server.

Trap Community

Range: 0~255 characters

Default: public

Function: Configure the community carried by trap message.

Trap Destination Address

Format: A.B.C.D

Function: Configure the address of the server for receiving trap messages.

Trap Destination Port

Range: 1~65535

Default: 162

Function: Configure the number of port for sending trap messages.

Trap Inform Mode

Options: Enabled/Disabled

Default: Disabled

Function: Whether to send a response to the switch after the server receives a trap packet.

Trap Inform Timeout

Range: 0~2147s

Default: 3s

Function: Set the timeout time for sending trap packets. After sending a trap packet to the server, the switch retransmits the trap packet if it does not receive a response from the server within this period.

Trap Inform Retry Times

Range: 0~255

Default: 5

Function: Set the number of timeout retransmission times of trap packets. If the accumulated number of transmission times exceeds the value of this parameter and the server does not respond yet, it is considered that transmitting the trap packet fails.

Trap Security Engine ID

Range: An engine ID is an even number of digits in hexadecimal notation, which cannot be all 0's or all F's. The range of the even number of digits is 10 to 64.

Function: Configure the Trap Security Engine ID carried by trap message.

Trap security name

Default: None

Function: SNMP v3 Trap security name, v1, v2c version is invalid.

Warm Start/ Cold Start

Options: Enabled/Disabled

Default: Disabled

Function: whether to send trap message or not when switch warm starting/cold starting.

Link up/ Link down

Options: none/specific/all switches

Default: none

Function: Whether to send a port up/down trap packet when the port status changes.

LLDP

Options: none/specific/all switches

Default: none

Function: Whether to send a Link Layer Discovery Protocol (LLDP) trap packet when the neighbor status changes.

SNMP Authentication Fail

Options: Enabled/Disabled

Default: Disabled

Function: whether to send trap message or not when SNMP Authentication Failure.

STP

Options: Enabled/Disabled

Default: Disabled

Function: whether to send trap message or not when STP status changing.

3.8.6.6 Typical Configuration Example

SNMP management server is connected to the switch through Ethernet. The IP address of the management server is 192.168.0.23, and that of the switch is 192.168.0.2. The NMS monitors and manages the Agent through SNMP v2c, and reads and writes the MIB node information of the Agent. When the Agent is faulty, it proactively sends trap packets to the NMS, as shown in Figure 122.

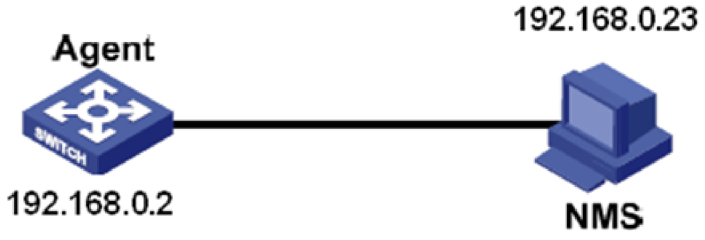


Figure 122 SNMP v2c Configuration Example

Configuration on Agent:

1. Enable SNMP and v2c state; configure access rights with Read only community "public" and Read and write community "private", as shown in Figure 119.

2. Configure global trap mode, as shown in Figure 120.

3. Create trap entry 111, enable trap mode; set the trap version to SNMP v2c, destination IP address to 192.168.0.23. Select system, interface, authentication, and switch all trap events, and adopt default settings for the other parameters, as shown in Figure 121.

If you want to monitor and manage Agent devices, run the corresponding management software in NMS, such as Kyvision developed by Kyland.

For details about operations of Kyvision, refer to the *Kyvision Operation Manual*.

3.8.7 SNMPv3

3.8.7.1 Introduce

SNMP v3 provides a User-Based Security Model (USM) authentication mechanism. You can configure authentication and encryption functions. Authentication is used for verifying the validity of packet sender, preventing illegitimate users' access. Encryption is used for encrypt packets transmitted between the NMS and the Agent, avoiding interception. The authentication and encryption functions can improve the security of communication between the SNMP NMS and the SNMP Agent.

To enable the communication between the NMS and agent, their SNMP versions must match. Different SNMP version can be configured on an agent, so that it can use different versions to communicate with different NMSs.

3.8.7.2 Implementation

SNMP v3 provides four configuration tables. Each table can contain 16 entries. These tables determine whether specific users can access MIB information.

You can create multiple users in the user table. Each user uses different security policies for authentication and encryption.

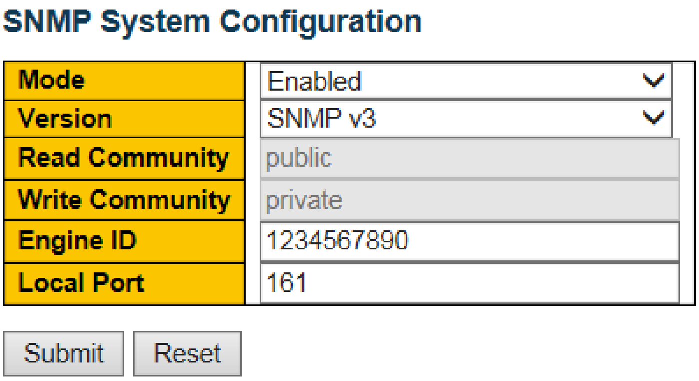
The group table is the collection of multiple users. In the group table, access rights are defined based on user groups. All the users of a group have the rights of the group.

The view table refers to the MIB view information, which specifies the MIB information that can be accessed by users. The MIB view may contain all nodes of a certain MIB subtree (that is, users are allowed to access all nodes of the MIB subtree) or contain none of the nodes of a certain MIB subtree (that is, users are not allowed to access any node of the MIB subtree).

You can define MIB access rights in the access table by group name, security model, and security level.

3.8.7.3 Web Configuration

1. Enable SNMP protocol and select SNMP version, as shown in Figure 123.



SNMP System Configuration

Mode	Enabled
Version	SNMP v3
Read Community	public
Write Community	private
Engine ID	1234567890
Local Port	161

Figure 123 Enable SNMP Protocol and Select SNMP Version

Mode

Options: Enabled/Disabled

Default: Enabled

Function: Enable/Disable SNMP.

Version

Options: SNMP v1/SNMP v2c/SNMP v3

Default: SNMP v2c

Function: Choose a SNMP version. SNMP v2c is compatible with SNMP v1; SNMP v3 is compatible with SNMP v1 and SNMP v2c.

Engine ID

Range: An engine ID is an even number of digits in hexadecimal notation, which cannot be all 0's or all F's. The range of the even number of digits is 10 to 64.

Function: Set the engine ID for the SNMP v3 system. When the engine ID is changed, users corresponding to device IDs in the user table are cleared.

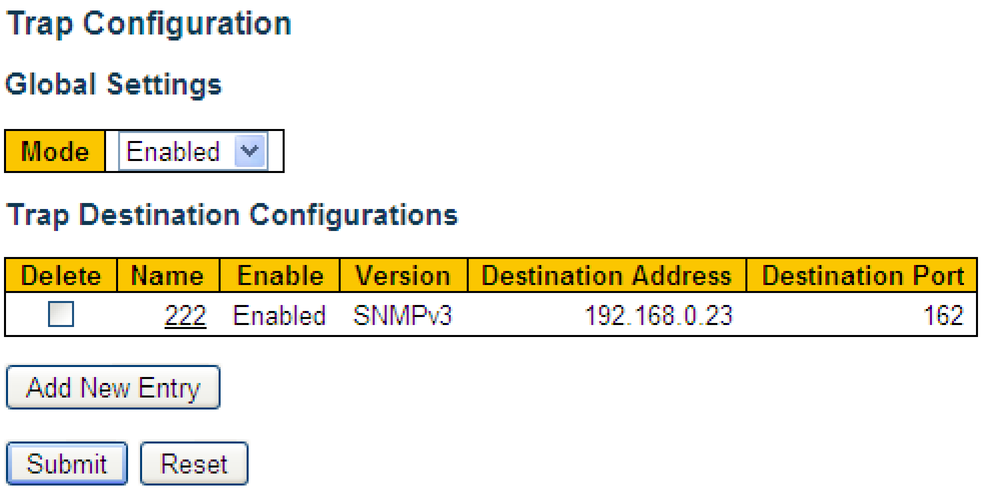
Local port

Range: 1 ~ 65535

Default: 161

Function: Configure the port number to receive SNMP requests.

2. Configure global trap mode, as shown in Figure 124.



Trap Configuration

Global Settings

Mode	Enabled

Trap Destination Configurations

Delete	Name	Enable	Version	Destination Address	Destination Port
□	222	Enabled	SNMPv3	192.168.0.23	162

Figure 124 Configure Global Trap Mode

Mode

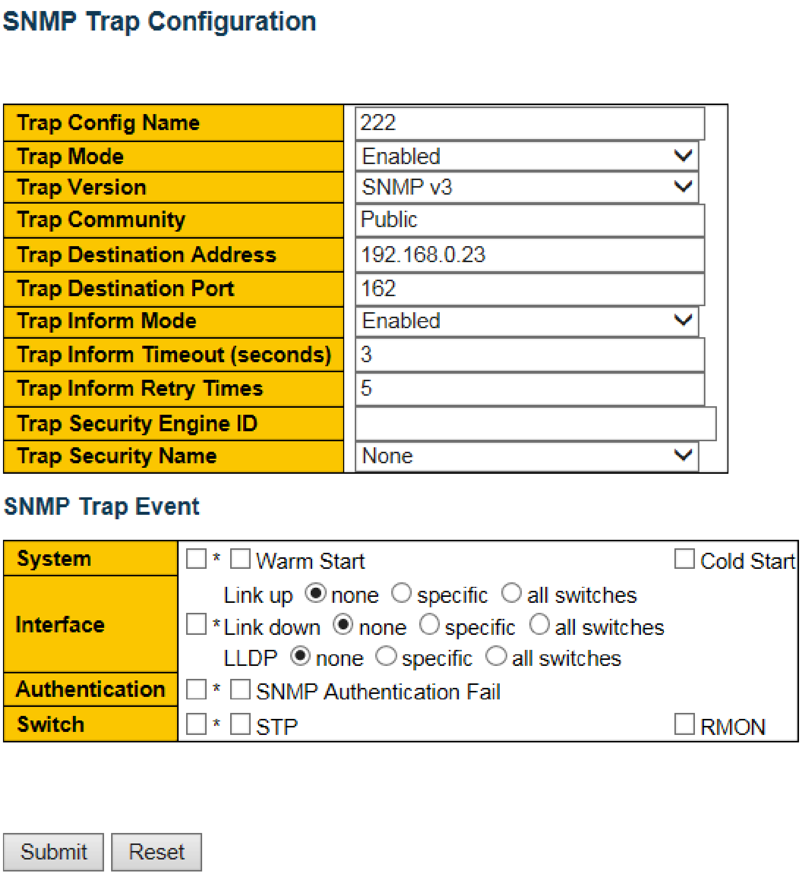
Options: Enabled/Disabled

Default: Disabled

Function: Enable/Disable global trap mode.

Cilck <Add New Entry> to configure trap entry, the switch supports a maximum of 4 trap entries. Click <Name> to modify the trap entry.

3. Configure trap entry, as shown in Figure 125.



SNMP Trap Configuration

Trap Config Name	222
Trap Mode	Enabled
Trap Version	SNMP v3
Trap Community	Public
Trap Destination Address	192.168.0.23
Trap Destination Port	162
Trap Inform Mode	Enabled
Trap Inform Timeout (seconds)	3
Trap Inform Retry Times	5
Trap Security Engine ID	
Trap Security Name	None

SNMP Trap Event

System	□ * □ Warm Start □ Cold Start
Interface	Link up ● none ○ specific ○ all switches □ * Link down ● none ○ specific ○ all switches LLDP ● none ○ specific ○ all switches
Authentication	□ * □ SNMP Authentication Fail
Switch	□ * □ STP □ RMON

Figure 125 Configure Trap Entry

Trap Config Name

Range: 1~255 characters

Function: Configure trap entry name.

Trap Mode

Options: Enabled/Disabled

Default: Disabled

Function: Enable/Disable the trap entry. After enabling the trap mode, switch can send trap message to NMS.

Trap Version

Options: SNMP v1/SNMP v2c/SNMP v3

Default: SNMP v2c

Function: Set the version of trap packets sent from the switch to the server.

Trap Community

Range: 0~255 characters

Default: public

Function: Configure the community carried by trap message.

Trap Destination Address

Format: A.B.C.D

Function: Configure the address of the server for receiving trap messages.

Trap Destination Port

Range: 1~65535

Default: 162

Function: Configure the number of port for sending trap messages.

Trap Inform Mode

Options: Enabled/Disabled

Default: Disabled

Function: Set whether to send a response to the switch after the server receives a trap packet.

Trap Inform Timeout

Range: 0~2147s

Default: 3s

Function: Set the timeout time for sending trap packets. After sending a trap packet to the server, the switch retransmits the trap packet if it does not receive a response from the server within this period.

Trap Inform Retry Times

Range: 0~255

Default: 5

Function: Set the number of timeout retransmission times of trap packets. If the accumulated number of transmission times exceeds the value of this parameter and the server does not respond yet, it is considered that transmitting the trap packet fails.

Trap Probe Security Engine ID

Options: Enabled/Disabled

Default: Enabled

Function: Set the security engine ID carried in SNMP v3 trap packets. When it is set to

Enabled, the switch automatically probes and acquires the security engine ID. When it is set to Disabled, the security engine ID is acquired from the value of Trap Security Engine ID.

Trap Security Engine ID

Range: An engine ID is an even number of digits in hexadecimal notation, which cannot be all 0's or all F's. The range of the even number of digits is 10 to 64.

Function: Configure the Trap Security Engine ID carried by trap message.

Trap security name

Default: None

Function: SNMP v3 Trap security name.

Warm Start/ Cold Start

Options: Enabled/Disabled

Default: Disabled

Function: whether to send trap message or not when switch warm starting/cold starting.

Link up/ Link down

Options: none/specific/all switches

Default: none

Function: Whether to send a port up/down trap packet when the port status changes.

LLDP

Options: none/specific/all switches

Default: none

Function: Whether to send an LLDP trap packet when the neighbor status changes.

SNMP Authentication Fail

Options: Enabled/Disabled

Default: Disabled

Function: whether to send trap message or not when SNMP Authentication Failure.

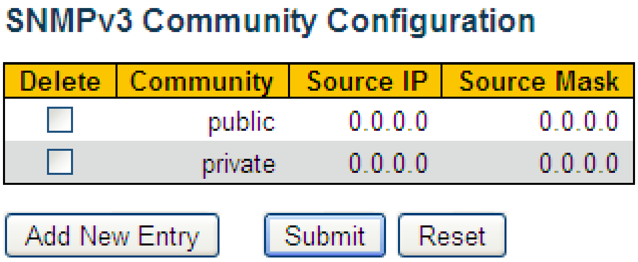
STP

Options: Enabled/Disabled

Default: Disabled

Function: whether to send trap message or not when STP status changing.

4. Configure community, as shown in Figure 126.



SNMPv3 Community Configuration

Delete	Community	Source IP	Source Mask
□	public	0.0.0.0	0.0.0.0
□	private	0.0.0.0	0.0.0.0

Figure 126 Configure Community

Community

Range: 1~32 characters

Function: Configure the community name .

When SNMP v3 is selected, a community name can be set to enable the network management system (NMS) to access the switch over SNMPv1 and SNMPv2. In this case, the community name on the NMS must be consistent with that on the switch. The access permissions of a community name depend on the configuration of the group table and access table.

Source IP

Format: A.B.C.D

Function: Configure the NMS IP address.

Source Mask

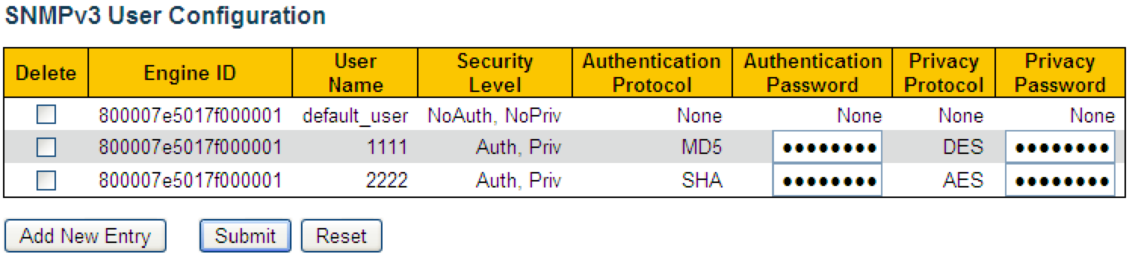
Function: Network indicates that you can configure the range of the IP address pool, and the address range is determined by the subnet mask. The subnet mask is a number with a length of 32 bits and consists of a string of 1 and a string of 0. "1" corresponds to network number fields and subnet number fields, while "0" corresponds to host number fields. The NMS IP address is determined by Source IP and Source Mask.

Click <Add New Entry> to configure community, the switch supports a maximum of 16 communities.

Note:

By default, the community names public and private exist on the switch. There is no IP address restriction on the NMS.

4. Configure the user table, as shown in Figure 127.



SNMPv3 User Configuration

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
□	800007e5017f000001	default_user	NoAuth, NoPriv	None	None	None	None
□	800007e5017f000001	1111	Auth, Priv	MD5	••••••••	DES	••••••••
□	800007e5017f000001	2222	Auth, Priv	SHA	••••••••	AES	••••••••

Figure 127 SNMP v3 User Table Configuration

Engine ID

Range: An engine ID is an even number of digits in hexadecimal notation, which cannot be all 0's or all F's. The range of the even number of digits is 10 to 64.

Function: Set the user engine ID. If the user engine ID is different from the SNMPv3 system engine ID, the user is ineffective currently.

User Name

Range: 1~32 characters

Function: Create the user name.

Security Level

Options: NoAuth,NoPriv/Auth,NoPriv/Auth,Priv

Function: Configure the security level of current user.

Description: NoAuth,NoPriv indicates that neither authentication nor encryption is required. Auth,NoPriv indicates that authentication is required but not encryption. Auth,Priv indicates that both authentication and encryption are required.

Authentication Protocol

Options: MD5/SHA

Function: Select an authentication algorithm. The authentication protocol and authentication password need to be set when Security Level is set to Auth, NoPriv or NoAuth, Priv.

Authentication Password

Range: 8~32 characters (MD5) 8~40 characters (SHA)

Function: Create the authentication password.

Privacy Protocol

Options: DES/AES

Function: Select a encryption protocol. The privacy protocol and privacy password need to be set when Security Level is set to Auth, Priv.

Privacy Password

Range: 8~32 characters

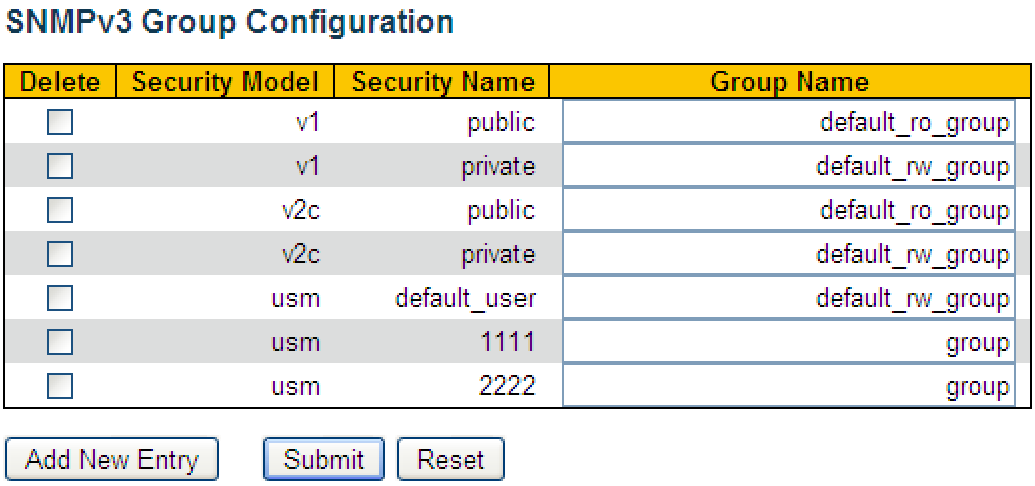
Function: Create the encryption password.

Click <Add New Entry> to configure user entry. A maximum of 16 users are supported.

Note:

By default, the user default_user exists in the switch and the security level is NoAuth, NoPriv.

5. Configure the group table, as shown in Figure 128.



SNMPv3 Group Configuration

Delete	Security Model	Security Name	Group Name
□	v1	public	default_ro_group
□	v1	private	default_rw_group
□	v2c	public	default_ro_group
□	v2c	private	default_rw_group
□	usm	default_user	default_rw_group
□	usm	1111	group
□	usm	2222	group

Figure 128 SNMP v3 Group Table Configuration

Security Model

Default: v1/v2/usm

Description: Select the security model of current group(SNMP version). SNMP v3 adopts User-based Security Model (USM) .

Security Name

Range: all existing communities/user names, 1~32 characters

Function: Configure the security name. When the security model is v1/v2, the security name must be identical with community. When the security model is usm, the security name must be identical with the user name in the user table.

Group Name

Range: 1~32 characters

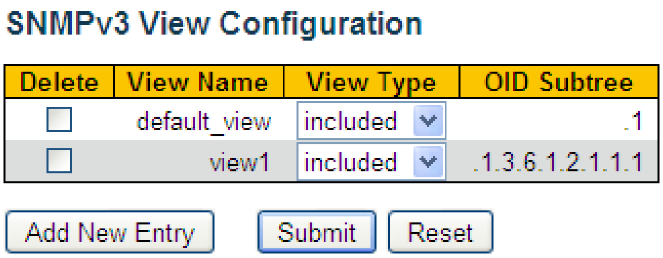
Function: Configure the name of the group table, users with same group name belong to one group.

Click <Add New Entry> to configure group table. A maximum of 16 groups are supported.

Note:

By default, the following group tables exist in the switch: {v1,public,default_ro_group}, {v1,private,default_rw_group}, {v2c,public,default_ro_group}, {v2c,private,default_rw_group}, and {usm,default_user,default_rw_group}.

6. Configure the view table, as shown in Figure 129.



SNMPv3 View Configuration

Delete	View Name	View Type	OID Subtree
□	default_view	included	.1
□	view1	included	.1.3.6.1.2.1.1.1

Figure 129 SNMP v3 View Table Configuration

View Name

Range: 1~32 characters

Function: Configure the view name.

View Type

Options: included/excluded

Default: included

Function: Included indicates that the current view includes all nodes of the MIB tree. Excluded indicates that the current view does not include any nodes of the MIB tree.

OID Subtree

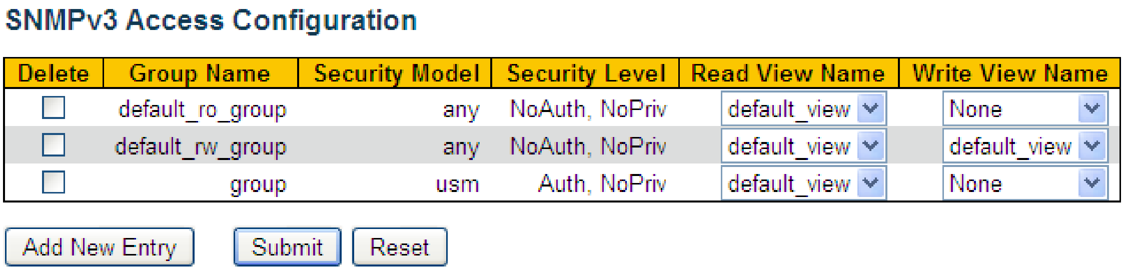
Function: MIB tree, indicated by the OID of the root node of the tree.

Click <Add New Entry> to configure view table. A maximum of 16 view entries are supported.

Note:

By default, the view default_view exists in the switch and this view covers all nodes in subtree 1.

7. Configure the access table, as shown in Figure 130.



SNMPv3 Access Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
□	default_ro_group	any	NoAuth, NoPriv	default_view	None
□	default_rw_group	any	NoAuth, NoPriv	default_view	default_view
□	group	usm	Auth, NoPriv	default_view	None

Figure 130 SNMP v3 Access Table Configuration

Group Name

Range: all existing group names, 1~32 characters

Function: Users in the group have the same access rights.

Security Model

Default: any/v1/v2/usm

Function: Set the security model (that is, SNMP version number) adopted when the current group accesses the switch. SNMPv3 adopts User-based Security Model (USM) and the value **any** indicates that any security model can be adopted. The group name and Security Model in access table should be identical with those in group table.

Security Level

Options: NoAuth,NoPriv/Auth,NoPriv/Auth,Priv

Function: Select the security level of current group.

Description: NoAuth,NoPriv indicates that neither authentication nor encryption is required. Auth,NoPriv indicates that authentication is required but not encryption. Auth,Priv indicates that both authentication and encryption are required. When authentication/encryption is required, the user can access specified MIB information only if the authentication/encryption protocol and authentication/encryption password are identical with those configured in the user table.

The security levels are NoAuth,NoPriv, Auth,NoPriv and Auth,Priv in ascending order. The content with a lower security level is allowed to be accessed with a higher security level. For example, if both authentication/encryption protocol and authentication/encryption password are correct, security level is configured as Auth,NoPriv can be successfully accessed with the Auth,NoPriv and Auth,Priv security level but cannot be accessed with the NoAuth,NoPriv security level.

Read View Name

Options: default_view/None/all existing view names

Function: Select the name of read-only view.

Write View Name

Options: default_view/None/all existing view names

Function: Select the name of write view.

Click <Add New Entry> to configure access table. A maximum of 16 access entries are supported.

Note:

By default, the following access tables exist in the switch: {default_ro_group, any, NoAuth,NoPriv, default_view, None} and {default_rw_group, any, NoAuth,NoPriv, default_view, default_view}.

3.8.7.4 Typical Configuration Example

SNMP management server is connected to the switch through Ethernet. The IP address of the management server is 192.168.0.23, and that of the switch is 192.168.0.2. User 1111 and user 2222 manage the Agent through SNMP v3. Security level is set to AuthNoPriv, and the switch can perform read-only operation on all node information of the Agent. When an alarm occurs, the Agent sends trap v3 messages to the NMS proactively, as shown in Figure 131.

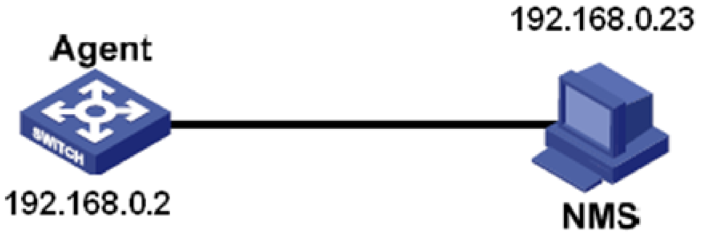


Figure 131 SNMP v3 Configuration Example

Configuration on the Agent:

1. Enable SNMP and v3 state, as shown in Figure 123.

2. Configure the SNMP v3 user table

Set a user name to 1111, security level to Auth,Priv, authentication protocol to MD5, authentication password to aaaaaaaa, privacy protocol to DES, and privacy password to xxxxxxxx.

Set another user name to 2222, security level to Auth,Priv, authentication protocol to SHA, authentication password to bbbbbbbb, privacy protocol to AES, and privacy password to yyyyyyyy, as shown in Figure 127.

3. Create group, set security model to usm, and add user 1111 and user 2222 to the group, as shown in Figure 128.

4. Configure the SNMP v3 access table

Set the group name to group, security model to usm, security level to Auth,NoPriv, read view to default_view, and write view to None, as shown in Figure 130.

5. Enable the global trap mode, as shown in Figure 124.

6. Create trap entry 222, enable trap mode; set the trap version to SNMP v3, destination IP address to 192.168.0.23. Select system, interface, authentication, and switch all trap events, and adopt default settings for the other parameters, as shown in Figure 125.

If you want to monitor and manage Agent devices, run the corresponding management software in NMS.

3.8.8 RMON

3.8.8.1 Introduce

Based on SNMP architecture, Remote Network Monitoring (RMON) allows network management devices to proactively monitor and manage the managed devices. An RMON network usually involves the Network Management Station and Agents. The NMS manages Agents and Agents can collect statistics on various types of traffic on these ports.

RMON mainly provides statistics and alarm functions. With the statistics function, Agents can periodically collect statistics on various types of traffic on these ports, such as the number of packets received from a certain network segment during a certain period. Alarm function is that Agents can monitor the values of specified MIB variables. When a value reaches the alarm threshold (such as the number of packets reaches the specified value), Agent can automatically record alarm events in RMON log, or send a Trap message to the management device.

3.8.8.2 RMON Groups

RMON (RFC2819) defines multiple RMON groups. The series devices support statistics group, history group, event group, and alarm group in public MIB.

- Statistics group

With the statistics group, the system collects statistics on all types of traffic on ports and stores the statistics in the Ethernet statistics table for further query by the management device. The statistics includes the number of network collisions, CRC error packets, undersized or oversized packets, broadcast and multicast packets, received bytes, and received packets. After creating a statistics entry on a specified port successfully, the statistics group counts the number of packets on the port and the statistics is a continuously accumulated value.

- History group

History group requires the system to periodically sample all kinds of traffic on ports and saves the sampling values in the history record table for further query by the management device. The history group counts the statistics values of all kinds of data in the sampling interval.

- Event group

Event group is used to define event indexes and event handing methods. Events defined in the event group is used in the configuration item of alarm group. An event is triggered when the monitored device meets the alarm condition. Events are addressed in the following ways:

Log: logs the event and related information in the event log table.

Trap: sends a Trap message to the NMS and inform the NMS of the event.

Log-Trap: logs the event and sends a Trap message to the NMS.

None: indicates no action.

- Alarm group

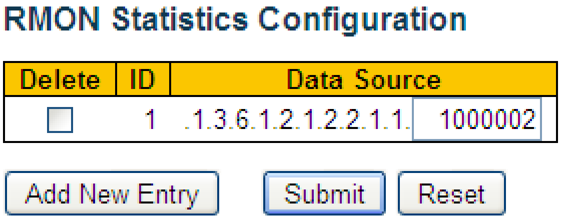
RMON alarm management can monitor the specified alarm variables. After alarm entries are defined, the system will acquire the values of monitored alarm variables in the defined period. When the value of an alarm variable is larger than or equal to the upper limit, a rising alarm event is triggered. When the value of an alarm variable is smaller than or equal to the lower limit, a falling alarm event is triggered. Alarms will be handled according to the event definition.

Caution:

If a sampled value of alarm variable exceeds the threshold multiple times in a same direction, then the alarm event is only triggered only the first time. Therefore the rising alarm and falling alarm are generated alternately.

3.8.8.3 Web Configuration

1. Configure statistics table, as shown in Figure 132.



RMON Statistics Configuration

Delete	ID	Data Source
□	1	.1.3.6.1.2.1.2.2.1.1. 1000002

Figure 132 Configure RMON Statistics Table

ID

Range: 1~65535

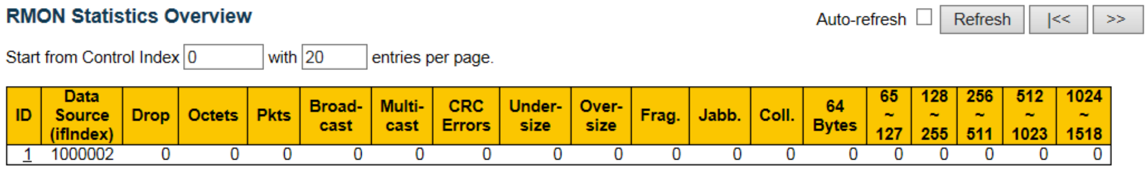
Function: Configure the number of the statistics entry. Statistics group supports up to 128 entries.

Data Source

Range: 10000portid

Function: Select the port whose statistics are to be collected.

2. View statistics group status, as shown in Figure 133.



RMON Statistics Overview

Auto-refresh □ Refresh |<< >>

Start from Control Index 0 with 20 entries per page.

ID	Data Source (ifIndex)	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	64 Bytes	65 ~ 127	128 ~ 255	256 ~ 511	512 ~ 1023	1024 ~ 1518
1	1000002	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure 133 Overview statistics group status

Drop: the number of packets dropped by the port.

Octets: the number of bytes received by the port.

Pkts: the number of packets received by the port.

Broadcast: the number of broadcast packets received by the port.

Multicast: the number of multicast packets received by the port.

CRC Errors: the number of CRC error packets with a length of between 64 and 9600 bytes received by the port.

Undersize: the number of packets with less than 64 bytes received by the port.

Oversize: the number of packets with more than 9600 bytes received by the port.

Frag.: the number of CRC error packets with less than 64 bytes received by the port.

Jabb.: the number of CRC error packets with more than 9600 bytes received by the port.

Coll.: the number of collisions received by the port under half duplex mode.

64 Bytes: the number of packets with a length of 64 bytes received by the port.

65~127: the number of packets with a length of between 65 and 127 bytes received by the port.

128~255: the number of packets with a length of between 128 and 255 bytes received by the port.

256~511: the number of packets with a length of between 256 and 511 bytes received by the port.

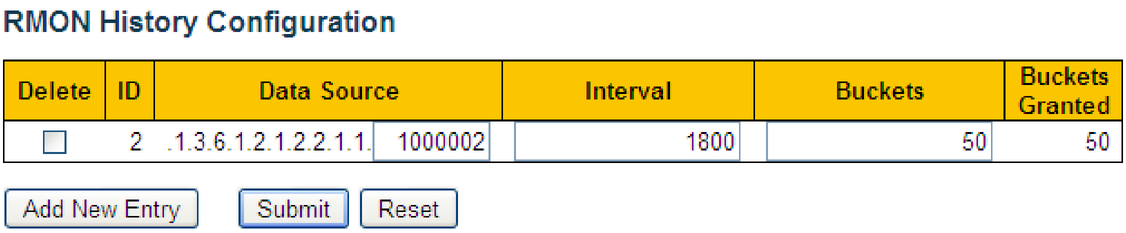
512~1023: the number of packets with a length of between 512 and 1023 bytes received by the port.

1024~1518: the number of packets with a length of between 1024 and 1588 bytes received by the port.

Note:

The oversize depends on the parameter ”Maximum Frame Size" in Port Configuration, as shown in Figure 59. In above example, the oversize is 9600 bytes.

3. Configure history table, as shown in Figure 134.



RMON History Configuration

Delete	ID	Data Source	Interval	Buckets	Buckets Granted
□	2	.1.3.6.1.2.1.2.2.1.1. 1000002	1800	50	50

Figure 134 Configure History Table

ID

Range: 1~65535

Function: Configure the number of the history entry. History group supports up to 256 entries.

Data Source

Options: 10000portid

Function: Select the port whose information is to be sampled.

Interval

Range: 1~3600s

Default: 1800s

Function: Configure the sampling period of the port.

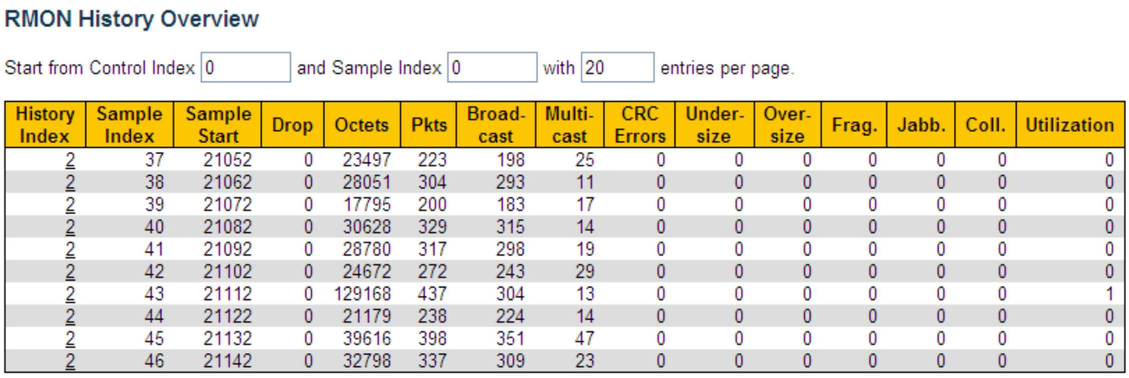
Buckets

Range: 1~65535

Default: 50

Function: Configures the number of latest sampling values of port information stored in RMON.

4. View history group status, as shown in Figure 135.



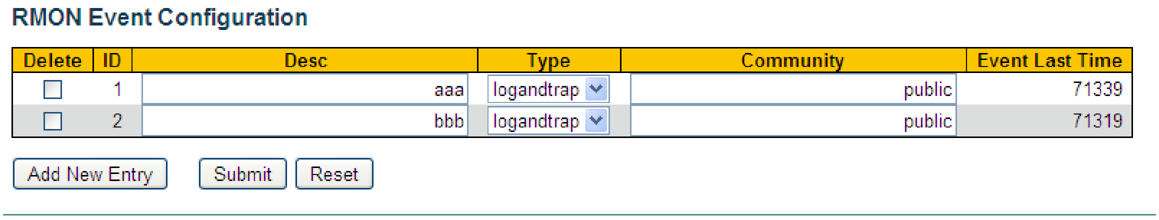
RMON History Overview

Start from Control Index 0 and Sample Index 0 with 20 entries per page.

History Index	Sample Index	Sample Start	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	Utilization
2	37	21052	0	23497	223	198	25	0	0	0	0	0	0	0
2	38	21062	0	28051	304	293	11	0	0	0	0	0	0	0
2	39	21072	0	17795	200	183	17	0	0	0	0	0	0	0
2	40	21082	0	30628	329	315	14	0	0	0	0	0	0	0
2	41	21092	0	28780	317	298	19	0	0	0	0	0	0	0
2	42	21102	0	24672	272	243	29	0	0	0	0	0	0	0
2	43	21112	0	129168	437	304	13	0	0	0	0	0	0	1
2	44	21122	0	21179	238	224	14	0	0	0	0	0	0	0
2	45	21132	0	39616	398	351	47	0	0	0	0	0	0	0
2	46	21142	0	32798	337	309	23	0	0	0	0	0	0	0

Figure 135 Overview History Group Status

5. Configure event table, as shown in Figure 136.



RMON Event Configuration

Delete	ID	Desc	Type	Community	Event Last Time
□	1	aaa	logandtrap	public	71339
□	2	bbb	logandtrap	public	71319

Figure 136 Configure Event Table

ID

Range: 1~65535

Function: Configure the index number of the event entry. Event group supports up to 128 entries.

Desc

Range: 0~127 characters

Function: Describe the event.

Type

Options: none/log/snmptrap/logandtrap

Default: none

Function: Configure the event type for alarms, that is, the processing mode towards alarms.

Community

Range: 0~127 characters

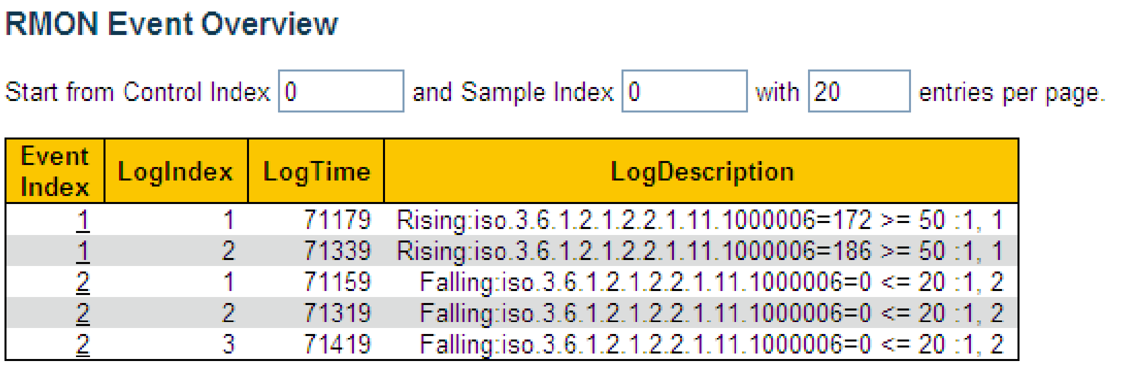
Default: public

Function: Configure the community name for sending a trap event. The value shall be identical with that in SNMP.

Event Last Time

Function: Displays the value of sysUpTime when the event is used last time.

6. View event group status, as shown in Figure 137.



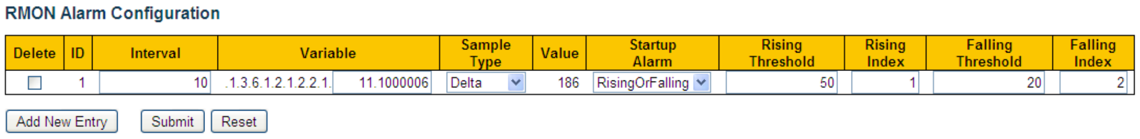
RMON Event Overview

Start from Control Index 0 and Sample Index 0 with 20 entries per page.

Event Index	LogIndex	LogTime	LogDescription
1	1	71179	Rising:iso.3.6.1.2.1.2.2.1.11.1000006=172 >= 50 :1, 1
1	2	71339	Rising:iso.3.6.1.2.1.2.2.1.11.1000006=186 >= 50 :1, 1
2	1	71159	Falling:iso.3.6.1.2.1.2.2.1.11.1000006=0 <= 20 :1, 2
2	2	71319	Falling:iso.3.6.1.2.1.2.2.1.11.1000006=0 <= 20 :1, 2
2	3	71419	Falling:iso.3.6.1.2.1.2.2.1.11.1000006=0 <= 20 :1, 2

Figure 137 Overview Event Group Status

7. Configure alarm table, as shown in Figure 138.



RMON Alarm Configuration

Delete	ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
□	1	10	.1.3.6.1.2.1.2.2.1. 11.1000006	Delta	186	RisingOrFalling	50	1	20	2

Figure 138 Configure Alarm Table

ID

Range: 1~65535

Function: Configure the number of the alarm entry. Alarm group supports up to 256 entries.

Interval

Range: 1~2147483647s

Deault: 30s

Function: Configure the sampling period.

Variable

Format: A.10000portid

Range: A：10~21

Function: Select the port MIB information to be monitored.

InOctets: A=10, the number of bytes received by the port.

InUcastPkts: A=11, the number of unicast packets received by the port.

InNUcastPkts: A=12, the number of broadcast and multicast packets received by the port.

InDiscards: A=13, the number of packets dropped by the port.

InErrors: A=14, the number of error packets received by the port.

InUnknownProtos: A=15, the number of unknown packets received by the port.

OutOctets: A=16, the number of bytes sent by the port.

OutUcastPkts: A=17, the number of unicast packets sent by the port.

OutNUcastPkts: A=18, the number of broadcast and multicast packets sent by the port.

OutDiscards: A=19, the number of discarded packets sent by the port.

OutErrors: A=20, the number of error packets sent by the port.

OutQLen: A=21, The length of packets in port outlet queue.

Sample Type

Options: Absolute/Delta

Default: Delta

Function: choose the method of comparing the sampling value and threshold.

Description: Absolute: directly compare each sampling value to threshold; Delta: the sampling value minus the previous sampling value, then use the difference to compare with threshold.

Startup Alarm

Options: Rising/Falling/RisingOrFalling

Default: RisingOrFalling

Function: choose the alarm type.

Rising Threshold

Range: 1~2147483647

Function: Set a rising threshold. When the sampling value exceeds the rising threshold and the alarm type is RisingAlarm or RisOrFallAlarm, the alarm will be triggered and the rising event index will be activated.

Rising Index

Range: 1~65535

Function: Set the index of a rising event. It is the handing method of a rising alarm.

Falling Threshold

Range: 1~2147483647

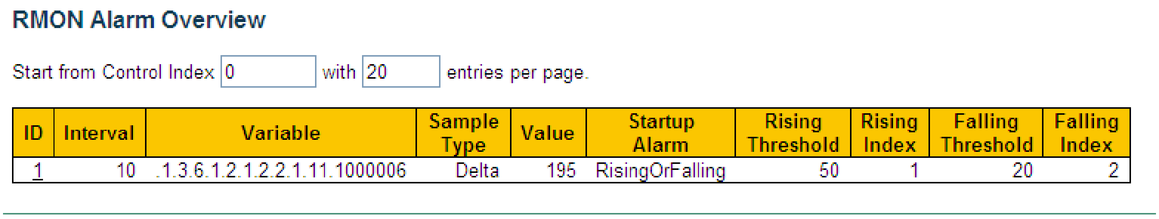
Function: Set a falling threshold. When the sampling value is lower than the falling threshold and the alarm type is FallingAlarm or RisOrFallAlarm, the alarm will be triggered and the falling event index will be activated.

Falling Index

Range: 1~65535

Function: Set the index of a falling event. It is the handling method of a falling alarm.

8. View alarm group status, as shown in Figure 139.



RMON Alarm Overview

Start from Control Index 0 with 20 entries per page.

ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
1	10	.1.3.6.1.2.1.2.2.1.11.1000006	Delta	195	RisingOrFalling	50	1	20	2

Figure 139 Overview Alarm Group Status

3.8.9 TACACS+ Configuration

3.8.9.1 Introduction

Terminal Access Controller Access Control System (TACACS+) is a TCP-based application. It adopts the client/server mode to implement the communication between Network Access Server (NAS) and TACACS+ server. The client runs on the NAS and user information is managed centrally on the server. The NAS is the server for users but client for the server. Figure 140 shows the structure.

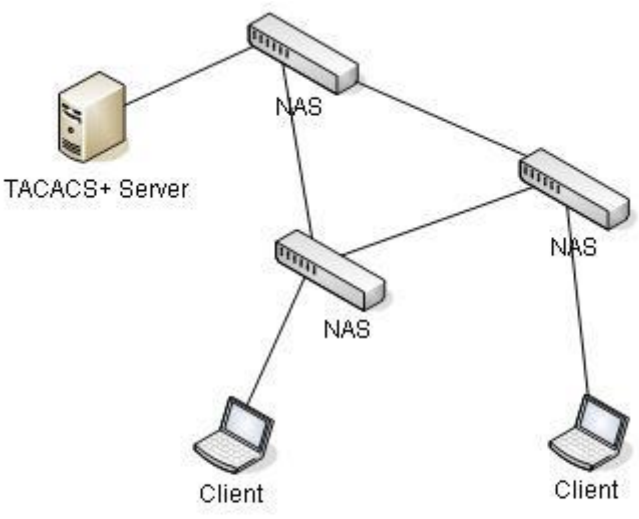
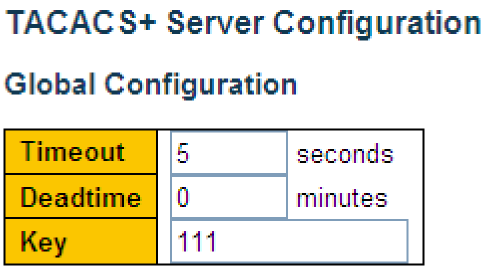


Figure 140 TACACS+ Structure

The protocol authenticates, authorizes, and charges terminal users that need to log in to the device for operations. The device serves as the TACACS+ client, and sends the user name and password to the TACACS+ server for authentication. The server receives TCP connection requests from users, responds to authentication requests, and checks the legitimacy of users. If a user passes authentication, it can log in to the device for operations.

3.8.9.2 Web Configuration

1. Configure global TACACS+ parameters, as shown in Figure 141.



TACACS+ Server Configuration

Global Configuration

Timeout	5	seconds
Deadtime	0	minutes
Key	111	

Figure 141 Configure Global TACACS+ Parameter

Timeout

Range: 1~1000s

Default: 5s

Function: Set the overtime for response from the TACACS+ server. After sending a TACACS+ request packet, if the device still receives no response from the TACACS+ server after the specified time, authentication fails, and the device will consider the TACACS+ server is invalid.

Deadtime

Range: 0~1440min

Default: 0min

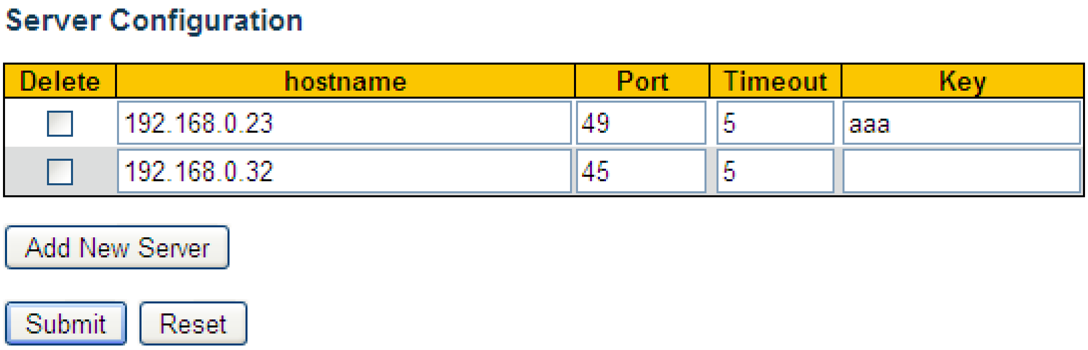
Function: Configures the period when the server is invalid. During this period, the device does not send TACACS+ request messages to the server. The value is 0 means diabling the function. You can enable this function only if more than one TACACS+ server has been configured.

Key

Range: 0~63 characters

Function: Set the key to improve the communication security between client and TACACS+ server. The two parties share the key to verify the legitimacy of packets. Both parties can receive packets from each other only when the keys are the same. Therefore, make sure the configured key is the same as the key on the TACACS+ server.

2. Configure the TACACS+ server, as shown in Figure 142.



Server Configuration

Delete	hostname	Port	Timeout	Key
□	192.168.0.23	49	5	aaa
□	192.168.0.32	45	5	

Figure 142 TACACS+ Server Configuration

Hostname

Function: Configure the IP address or hostname of TACACS+ server. A maximum of 5 TACACS+ server can be configured.

Port

Range: 0~65535

Default: 49

Function: Set TCP port of the TACACS+ server for authentication.

Timeout

Range: 1~1000s

Function: Set the overtime for response from the TACACS+ server. After sending a TACACS+ request packet, if the device still receives no response from the TACACS+ server after the specified time, authentication fails, and the device will consider the TACACS+ server is invalid.

Key

Range: 0~63 characters

Function: Set the key to improve the communication security between client and TACACS+ server. The two parties share the key to verify the legitimacy of packets. Both parties can receive packets from each other only when the keys are the same. Therefore, make sure the configured key is the same as the key on the TACACS+ server.

Note:

The priority of “Timeout” and “Key” in TACACS+ server configuration is higher than those in global configuration.

3.8.9.3 Typical Configuration Example

As shown in Figure 143, TACACS+ server can authenticate and authorize users by the switch. The server IP address is 192.168.0.23, and the shared key used when switch and server exchange packets is aaa.

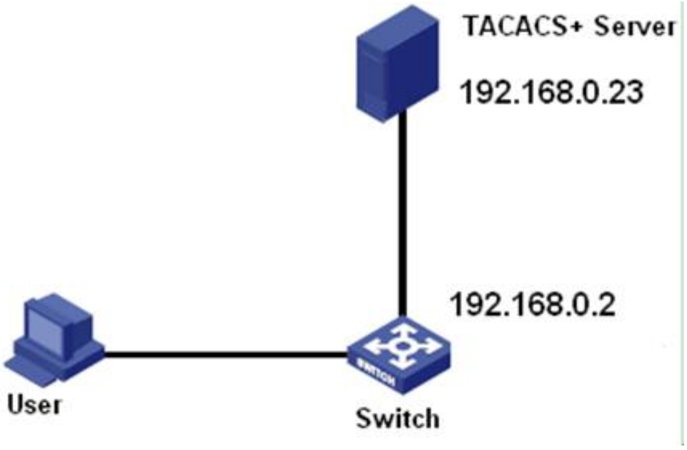


Figure 143 TACACS+ Authentication Example

1. TACACS+ server configuration. Set the server IP address to 192.168.0.23 and key to aaa, as shown in Figure 142.

2. When logging in to the switch through Web, select "Local", while logging in to the switch through telnet, select "Tacacs+", as shown in Figure 97.

3. Configure username and password "bbb", encrypt key “aaa” on TACACS+ server.

4. When logging in to the switch through Web, input the username "admin" and password "123" to pass the local authentication.

5. When logging in to the switch through Telnet, input the username and password "bbb" to pass the TACACS+ authentication.

3.8.10 RADIUS Configuration

3.8.10.1 Introduction

RADIUS (Remote Authentication Dial-In User Service) is a distributed information exchange protocol. It defines UDP-based RADIUS frame format and information transmission mechanism, protecting networks from unauthorized access. RADIUS is usually used in networks that require high security and remote user access.

RADIUS adopts client/server mode to achieve communication between the NAS (Network Access Server) and the RADIUS server. The RADIUS client runs on the NAS. The RADIUS server provides centralized management for user information. The NAS is the server for users but client for the RADIUS server. Figure 144 shows the structure.

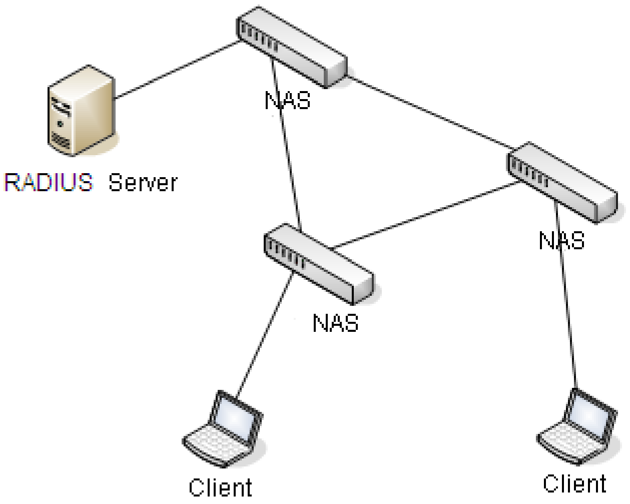
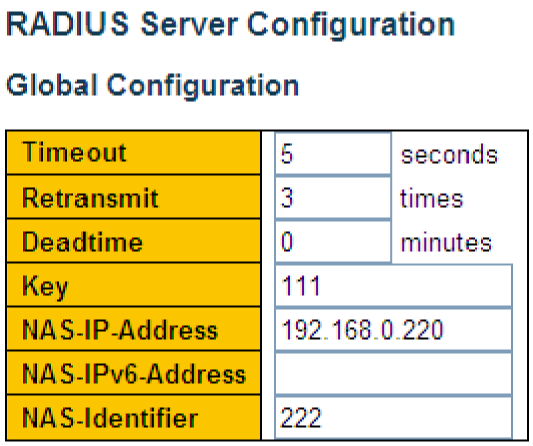


Figure 144 RADIUS Structure

The protocol authenticates terminal users that need to log in to the device for operation. Serving as the RADIUS client, the device sends user information to the RADIUS server for authentication and allows or disallows users to log in to the device according to authentication results.

3.8.10.2 Web Configuration

1. Configure global RADIUS parameters, as shown in Figure 145.



RADIUS Server Configuration

Global Configuration

Timeout	5	seconds
Retransmit	3	times
Deadtime	0	minutes
Key	111	
NAS-IP-Address	192.168.0.220	
NAS-IPv6-Address		
NAS-Identifier	222	

Figure 145 Configure Global RADIUS Parameters

Timeout

Range: 1~1000s

Default: 5s

Function: Set the overtime for response from the RADIUS server. After sending a RADIUS request packet, the device will retransmit a RADIUS request packet if it still receives no response from the RADIUS server after the specified time.

Retransmit

Range: 1~1000

Default: 3

Function: Set the maximum retransmission attempts for RADIUS request packets. If the device still receives no response packets from the RADIUS server after maximum retransmission attempts, authentication fails, and the device will consider the RADIUS server is invalid.

Deadtime

Range: 0~1440min

Default: 0min

Function: Configures the period when the server is invalid. During this period, the device does not send RADIUS request messages to the server. The value is 0 means diabling the function. You can enable this function only if more than one RADIUS server has been configured.

Key

Range: 0~63 characters

Function: Set the key to improve the communication security between client and RADIUS server. The two parties share the key to verify the legitimacy of packets. Both parties can receive packets from each other only when the keys are the same. Therefore, make sure the configured key is the same as the key on the RADIUS server.

NAS-IP-Address

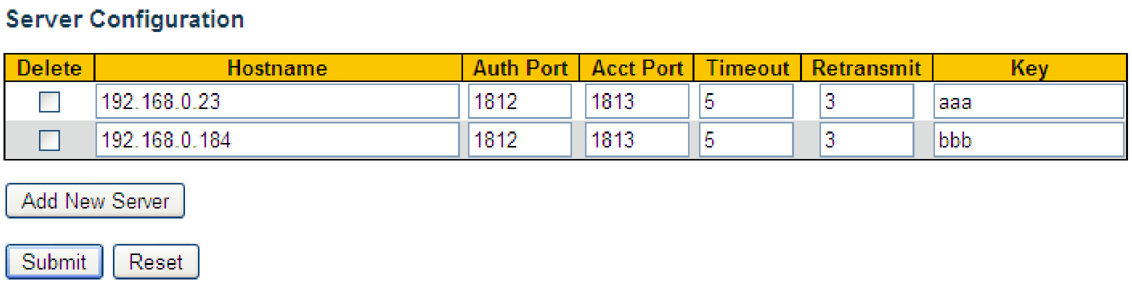
Function: Configures the source address used for sending RADIUS request messages by the equipment. If no source address is specified, the interface address for sending messages will be regarded as the source address.

NAS-Identifier

Range: 0~253 characters

Function: Configures the identifier used for sending RADIUS request messages by the equipment.

2. Configure the RADIUS server, as shown in Figure 146.



Server Configuration

Delete	Hostname	Auth Port	Acct Port	Timeout	Retransmit	Key
□	192.168.0.23	1812	1813	5	3	aaa
□	192.168.0.184	1812	1813	5	3	bbb

Figure 146 Configure the RADIUS Server

Hostname

Function: Configure the IP address or hostname of RADIUS server. A maximum of 5 RADIUS server can be configured.

Auth Port

Range: 0~65535

Default: 1812

Function: Set UDP port of the RADIUS server for authentication.

Acct Port

Range: 0~65535

Default: 1813

Function: Set UDP port of the RADIUS server for accounting. Since RADIUS uses different UDP ports for receiving and sending authentication and accounting messages, different port numbers must be configured for authentication and accounting.

Timeout

Range: 1~1000s

Function: Set the overtime for response from the RADIUS server. After sending a RADIUS request packet, the device will retransmit a RADIUS request packet if it still receives no response from the RADIUS server after the specified time.

Retransmit

Range: 1~1000

Function: Set the maximum retransmission attempts for RADIUS request packets. If the device still receives no response packets from the RADIUS server after maximum retransmission attempts, authentication fails, and the device will consider the RADIUS server is invalid.

Key

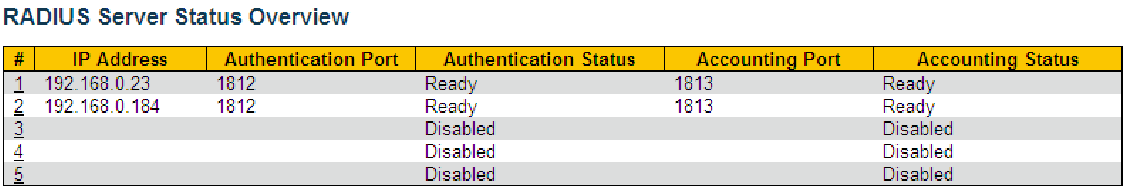
Range: 0~63 characters

Function: Set the key to improve the communication security between client and RADIUS server. The two parties share the key to verify the legitimacy of packets. Both parties can receive packets from each other only when the keys are the same. Therefore, make sure the configured key is the same as the key on the RADIUS server.

Note:

The priority of “Timeout”, “Retransmit”, and “Key” in RADIUS server configuration is higher than those in global configuration.

3. View RADIUS server status, as shown in Figure 147.



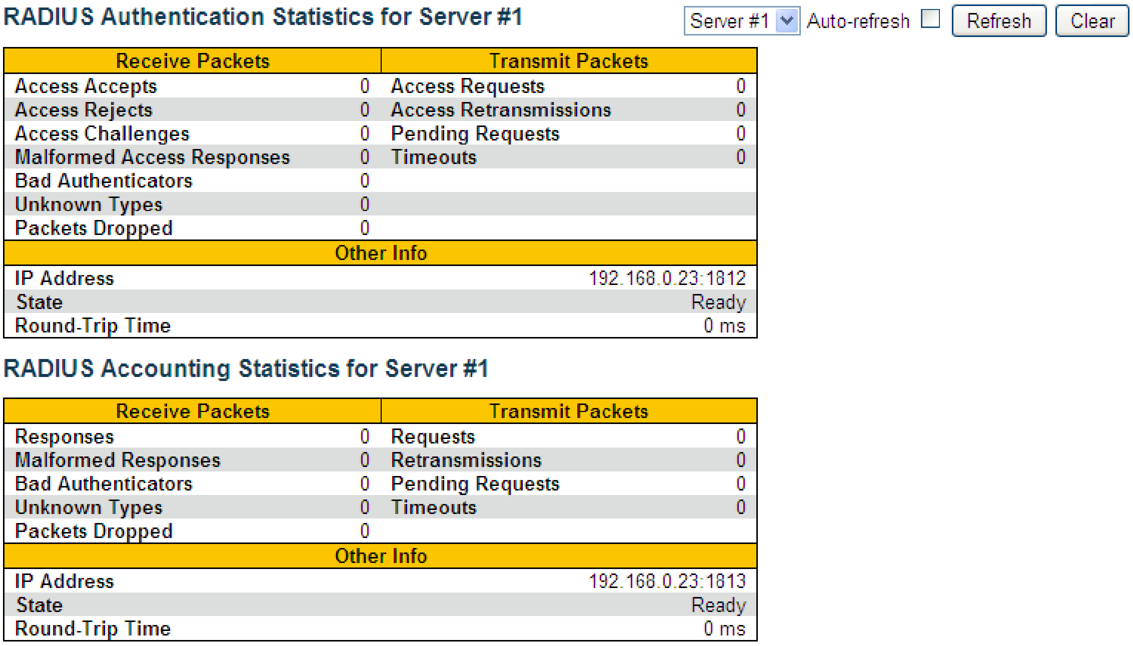
RADIUS Server Status Overview

#	IP Address	Authentication Port	Authentication Status	Accounting Port	Accounting Status
1	192.168.0.23	1812	Ready	1813	Ready
2	192.168.0.184	1812	Ready	1813	Ready
3			Disabled		Disabled
4			Disabled		Disabled
5			Disabled		Disabled

Figure 147 View RADIUS Server Status

Click the number to enter the “detailed RADIUS server statistics” page.

4. View detailed RADIUS server statistics, as shown in Figure 148.



RADIUS Authentication Statistics for Server #1

Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	0
Access Rejects	0	Access Retransmissions	0
Access Challenges	0	Pending Requests	0
Malformed Access Responses	0	Timeouts	0
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		
Other Info			
IP Address			192.168.0.23:1812
State			Ready
Round-Trip Time			0 ms

RADIUS Accounting Statistics for Server #1

Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		
Other Info			
IP Address			192.168.0.23:1813
State			Ready
Round-Trip Time			0 ms

Figure 148 View Detailed RADIUS Server Statistics

Select a server, and view the designated server detailed statistics.

3.8.10.3 Typical Configuration Example

As shown in Figure 149, IEEE802.1X is enabled on port 1of the switch. Then users can log in to the switch through port 1 after passing the authentication on the RADIUS server. The IP address of the server is 192.168.0.23. The key for packet exchange between the switch and the server is aaa.

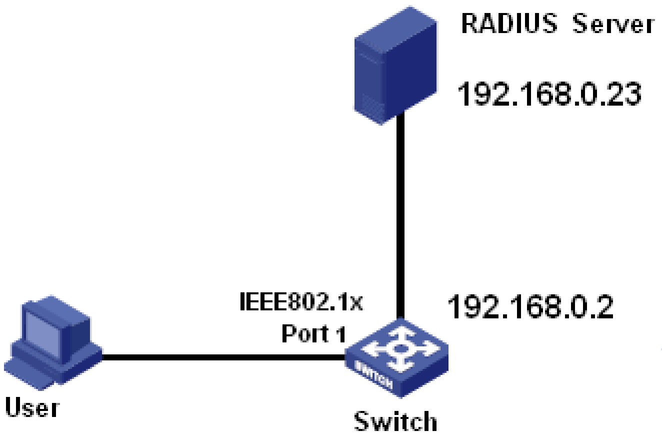


Figure 149 RADIUS Authentication Example

1. Set the IP address of the authentication server to 192.168.0.23 and password to aaa, as shown in Figure 146.

2. IEEE802.1x settings: enable IEEE802.1X globally. Set authentication type to radius, admin state of port 1 to port-based 802.1X, keep default settings for the other parameters. For details, see section " 3.9.1 IEEE802.1X Configuration".

3. Set both the user name and password on the RADIUS Server to ccc, encrypt key to aaa.

4. Install and run 802.1x client software on a PC. Enter ccc for the user name and password. Then the user can pass the authentication and access the switch through port 1.

3.9 Network

3.9.1 IEEE802.1X Configuration

3.9.1.1 Introduction

To ensure WLAN security, IEEE802 LAN/WAN committee proposed the 802.1X protocol. As a common access control mechanism for LAN ports in Ethernet, 802.1X implements Ethernet authentication and security. 802.1X is a port-based network access control. Port-based network access control is to implement authentication and control on the ports of LAN access devices. If a user passes the authentication, it can access the resources in the LAN. If it cannot pass the authentication, it cannot access the resources in the LAN.

802.1X systems adopt the Client/Server structure, as shown in Figure 150. User authentication and authorization of port-based access control requires the following elements:

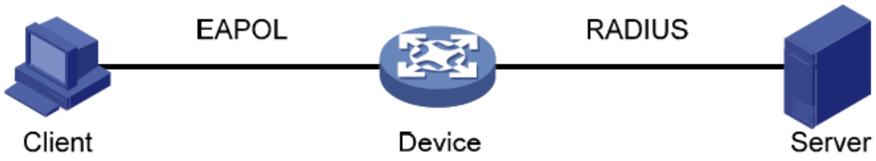


Figure 150 IEEE802.1X Structure

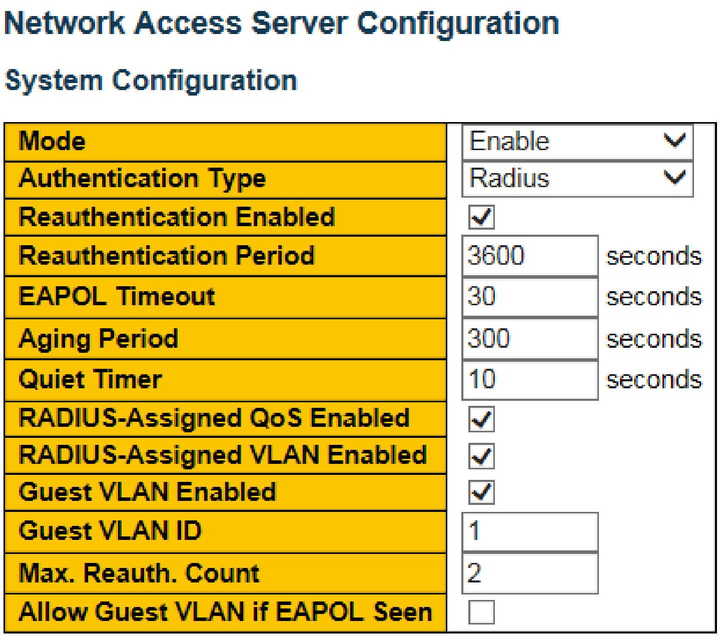
Client: usually indicates a user terminal. When a user wants to surf the Internet, it starts the client program and enters required user name and password. The client program will send a connection request. The client should support EAPOL (Extensible Authentication Protocol over LAN).

Device: indicates the authentication switch in an Ethernet system. It uploads and delivers user authentication information, and enables or disables a port based on the authentication result.

Authentication server: indicates the entity that provides authentication service for devices. It checks whether users have the permissions to use network services according to the identifiers (user names and passwords) sent by clients, and enables or disables ports according to authentication results.

3.9.1.2 Web Configuration

1. Configure global IEEE802.1X parameters, as shown in Figure 151.



Network Access Server Configuration

System Configuration

Mode	Enable
Authentication Type	Radius
Reauthentication Enabled	☑
Reauthentication Period	3600 seconds
EAPOL Timeout	30 seconds
Aging Period	300 seconds
Quiet Timer	10 seconds
RADIUS-Assigned QoS Enabled	☑
RADIUS-Assigned VLAN Enabled	☑
Guest VLAN Enabled	☑
Guest VLAN ID	1
Max. Reauth. Count	2
Allow Guest VLAN if EAPOL Seen	□

Figure 151 Configure Global IEEE802.1X Parameters

Mode

Options: Enable/Disable

Default: Disable

Function: Enable/Disable global IEEE802.1x security function.

Authentication Type

options: local / Radius

Default: Radius

Function: Select the Authentication Type.

Reauthentication Enabled

Options: Enable/Disable

Default: Disable

Function: Configure whether regular re-authentication is required when authentication succeeds.

Reauthentication Period

Range: 1~3600s

Default: 3600s

Function: When authentication succeeds, set the time interval for re-authentication. “Reauthentication Period” can be configured only if enabling “Reauthentication Enabled”.

EAPOL Timeout

Range: 1~65535s

Default: 30s

Function: Set the overtime for response from the client. After sending a Identity EAPOL request packet, the device will retransmit a Identity EAPOL request packet if it still receives no response from the client after the specified time.

Aging Period

Range: 10~1000000s

Default: 300s

Function: Configure aging period. When “Reauthentication Enabled” is diabled, the time interval for re-authentication is 2*aging period.

Quiet Timer

Range: 10~1000000s

Default: 10s

Function: If authentication fails, the device enters to quiet period. During the quiet period, the device does not respond to authentication requests from the client.

RADIUS-Assigned QoS Enabled

Options: Enable/Disable

Default: Disable

Function: When enabled, after the client passes authentication, the server transfers authorization information to the device. If **RADIUS-Assigned QoS Enabled** is checked on the server, the authorization information includes CoS information assigned for authorization. The equipment will modify the CoS value of the client authentication port based on the assigned value.

RADIUS-Assigned VLAN Enabled

Options: Enable/Disable

Default: Disable

Function: When enabled, after the client passes authentication, the server transfers authorization information to the device. If **RADIUS-Assigned VLAN Enabled** is checked on the server, the authorization information includes VLAN information assigned for authorization. The equipment will add the client authentication port to the assigned VLAN.

Guest VLAN Enabled

Options: Enable/Disable

Default: Disable

Function: When enabled, if a user is not authenticated or fails to be authenticated, the device adds the client authentication port to the guest VLAN. All users that access this port are authorized to access the resources in the guest VLAN.

Guest VLAN ID

Range: 1~4095

Default: 1

Function: Configure guest VLAN ID.

Max. Reauth. Count

Range: 1~255

Default: 2

Function: Set the maximum retransmission attempts for Identity EAPOL request packets. If the device still receives no response packets from the client after maximum retransmission attempts, the device will consider authentication fails.

Allow Guest VLAN if EAPOL Seen

Options: Enable/Disable

Default: Disable

Function: When enabled, if a user is not authenticated or fails to be authenticated, the device adds the client authentication port to the guest VLAN. When disabled, the device adds the port to the guest VLAN only when this port has no EAPOL frame record.

CAUTION

Caution:

- The precondition for configuring “Guest VLAN ID”, “Max. Reauth. Count”, and “Allow Guest VLAN if EAPOL Seen” is enabling “Guest VLAN ID”.
- It is recommended to disable “RADIUS-Assigned VLAN Enabled” and “Guest VLAN ID”, when the authentication port type is Trunk or Hybrid.
- The CoS value assigned for authorization does not change or affect the configuration of

the port. However, the priority of the COS value assigned for authorization is higher than a COS value configured by a user. In other words, what is valid after authentication is the CoS value assigned for authorization. If a user fails to be authenticated or goes offline, the CoS value configured by the user take effects.

➢ The VLAN assigned for authorization or the guest VLAN does not change or affect the configuration of the port. However, the VLAN assigned for authorization or the guest VLAN has a higher priority than a VLAN configured by a user.

After a user initiates authentication, and if the authentication is successful:

If the port enables **RADIUS-Assigned VLAN**, the port is added to the VLAN assigned by the RADIUS server.

If the port does not enable **RADIUS-Assigned VLAN**, the port is added to the VLAN configured by the user.

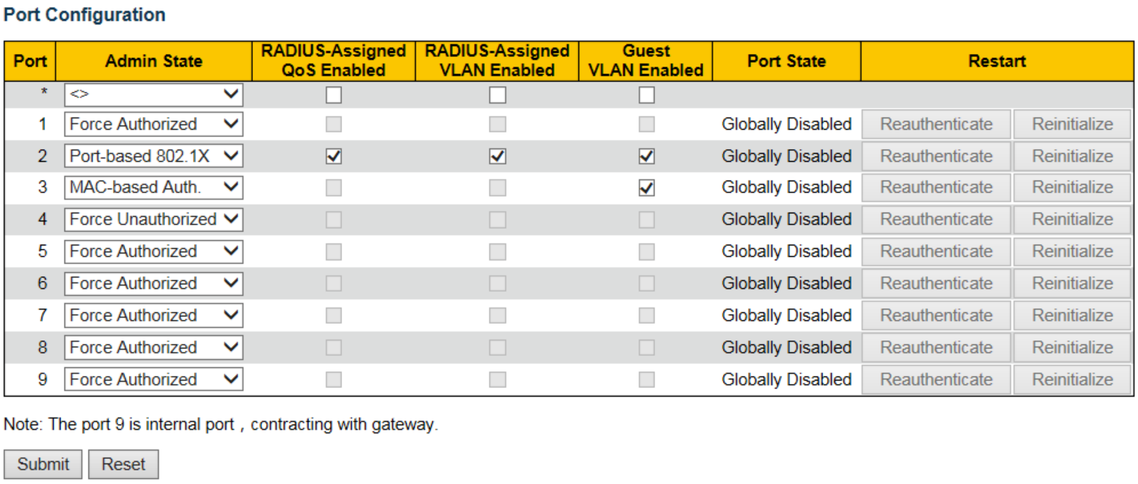
If a user fail to be authenticated or goes offline:

If the port enables **Guest VLAN** and **Allow Guest VLAN if EAPOL Seen**, the port is added to the VLAN.

If the port enables **Guest VLAN** but does not enable **Allow Guest VLAN if EAPOL Seen**, the port is added to the guest VLAN when no EAPOL fame record is available, and is added to the VLAN configured by the user when EAPOL frame record is available.

If the port does not enable **Guest VLAN**, the port is added to the VLAN configured by the user.

2. Configure IEEE802.1X port, as shown in Figure 152.



Port Configuration

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart	
*	<>	□	□	□			
1	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
2	Port-based 802.1X	☑	☑	☑	Globally Disabled	Reauthenticate	Reinitialize
3	MAC-based Auth.	□	□	☑	Globally Disabled	Reauthenticate	Reinitialize
4	Force Unauthorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
5	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
6	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
7	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
8	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize
9	Force Authorized	□	□	□	Globally Disabled	Reauthenticate	Reinitialize

Note: The port 9 is internal port，contracting with gateway.

Figure 152 Configure IEEE802.1X port

Port

Options: all switch ports.

Admin State

Options: Force Authorized/Force Unauthorized/Port-based 802.1X/MAC-based Auth.

Default: Force Authorized

Function: Select the port authentication mode.

Description: **Force Authorized** means port is always in an authorized state and allows users to access network resource without authentication.

Force Unauthorized means the port is always in unauthorized state and does not allow users to conduct authentication and the switch does not provide authentication services to clients that access the switch from this port. **MAC-based Auth** indicates that users using the port need to be authenticated respectively. When a user is offline, only the user cannot use the network. **Port-based 802.1X** indicates that users are authenticated based on port. After the first user using the port passes authentication, all the other users using the port do not need to be authenticated. However, when the first user is offline, the port is disabled and all the other users using the port cannot use the network.

RADIUS-Assigned QoS Enabled

Options: Enable/ Disable

Default: Disable

Function: Enable or disable RADIUS-Assigned QoS on port.

RADIUS-Assigned VLAN Enabled

Options: Enable/ Disable

Default: Disable

Function: Enable or disable RADIUS-Assigned VLAN on port.

Guest VLAN Enabled

Options: Enable/ Disable

Default: Disable

Function: Enable or disable guest VLAN on port.

Note:

This function is available only when **RADIUS-Assigned QoS**/**RADIUS-Assigned VLAN**/**Guest VLAN** is enabled at both the global and port levels.

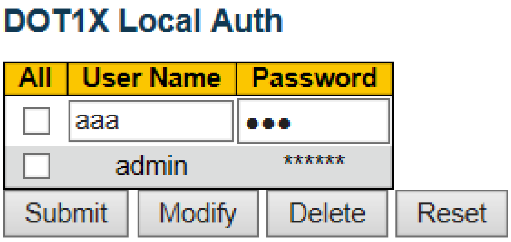
Port State

Options: Globally Disabled, Authorized, Unauthorized, Link Down, x Auth/y Unauth

Function: Display port authentication state. **Globally Disabled** indicates IEEE802.1X is diabled globally; **Authorized** indicates the user connected to the port passes authentication; **Unauthorized** indicates the user connected to the port fails to pass authentication; **Link Down** indicates the port is link down; x Auth/y Unauth indicates x users are authorized and y users are unauthorized when the port authentication mode is MAC-based Auth.

When the port authentication mode is MAC-based Auth or Port-based 802.1X, you can click <Reauthenticate>/<Reinitialize> button to reauthenticate. The port state changes to **Unauthorized** during reauthenticating.

3.Configure DOT1X local Auth, as shown below.



DOT1X Local Auth

All	User Name	Password
☐	aaa	●●●
☐	admin	******

Figure 153 Configure DOT1X local Auth

User name

Range: 1 ~ 16 characters

Function: Configure DOT1X local authentication user name.

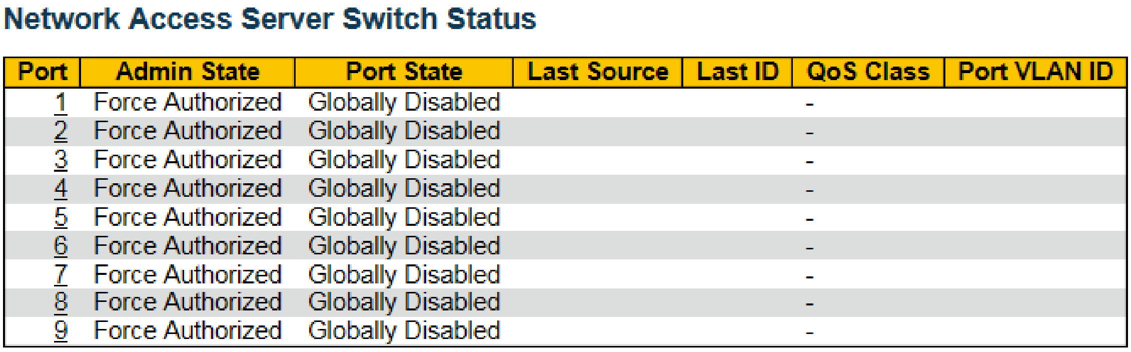
password

Range: 1 ~ 16 characters

Function: Configure DOT1X local authentication password.

Description: The DOT1X local authentication indicates that the local user name and password are used for authentication.

4. View IEEE802.1X configuration, as shown in Figure 154.



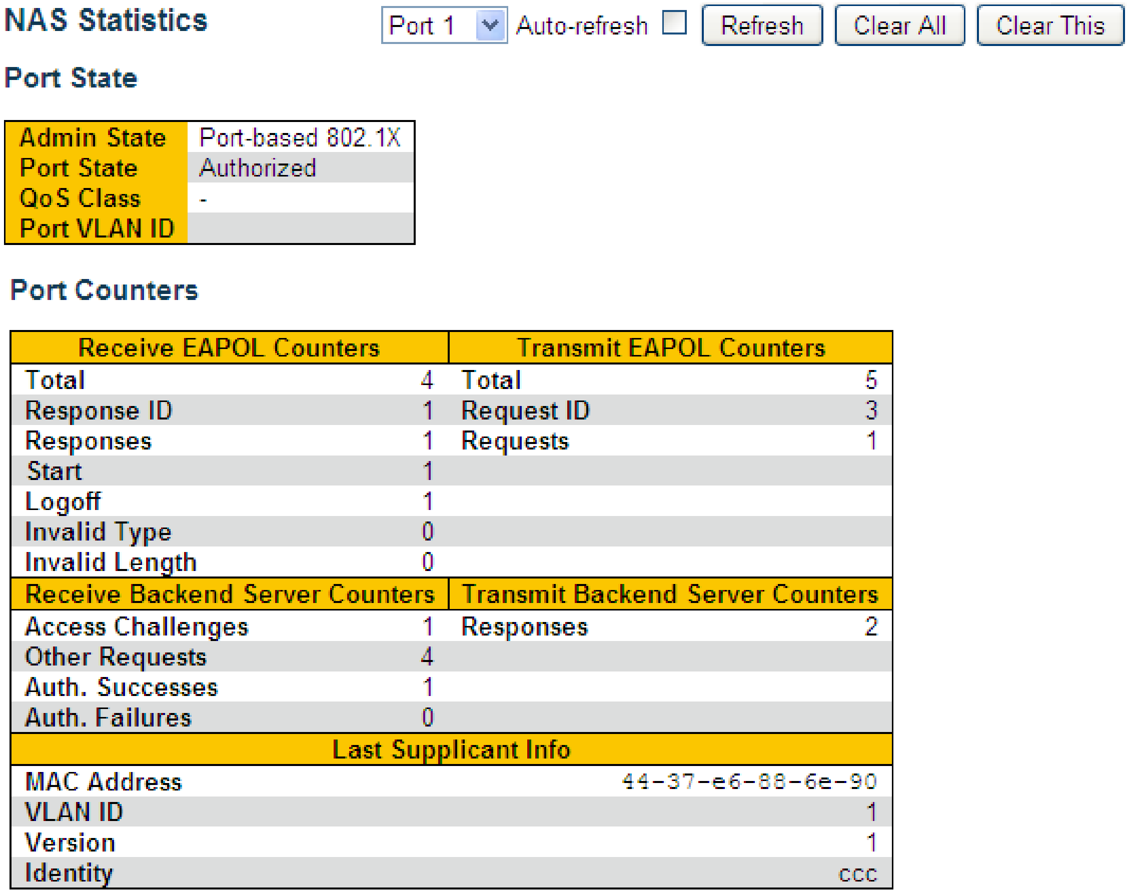
Network Access Server Switch Status

Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	Force Authorized	Globally Disabled			-	
2	Force Authorized	Globally Disabled			-	
3	Force Authorized	Globally Disabled			-	
4	Force Authorized	Globally Disabled			-	
5	Force Authorized	Globally Disabled			-	
6	Force Authorized	Globally Disabled			-	
7	Force Authorized	Globally Disabled			-	
8	Force Authorized	Globally Disabled			-	
9	Force Authorized	Globally Disabled			-	

Figure 154 View IEEE802.1X Configuration

Click <port> to enter the “IEEE802.1X statistics” page.

5. View IEEE802.1X statistics, as shown in Figure 155.



NAS Statistics

Port State

Admin State	Port-based 802.1X
Port State	Authorized
QoS Class	-
Port VLAN ID	

Port Counters

Receive EAPOL Counters		Transmit EAPOL Counters	
Total	4	Total	5
Response ID	1	Request ID	3
Responses	1	Requests	1
Start	1		
Logoff	1		
Invalid Type	0		
Invalid Length	0		
Receive Backend Server Counters		**Transmit Backend Server Counters**	
Access Challenges	1	Responses	2
Other Requests	4		
Auth. Successes	1		
Auth. Failures	0		
Last Supplicant Info			
MAC Address			44-37-e6-88-6e-90
VLAN ID			1
Version			1
Identity			ccc

Figure 155 View IEEE802.1X Statistics

Select a port, and view the designated port IEEE802.1X statistics.

3.9.1.3 Typical Configuration Example

As shown in Figure 156, client is connected to port 1 of the switch. Enable IEEE802.1x on port 1 and select Port-based 802.1X authentication mode. The username and password of the remote authentication are both ddd.

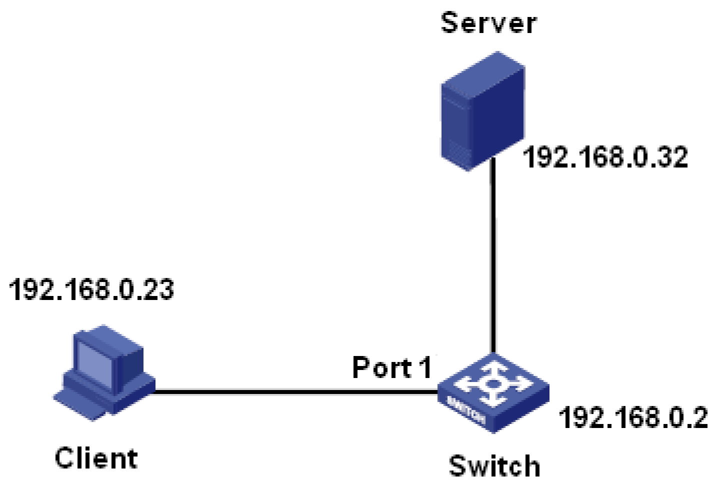


Figure 156 IEEE802.1x Configuration Example

You can refer to the typical configuration example in “3.8.10 RADIUS Configuration”.

3.9.2 ACL

3.9.2.1 Overview

With the development of network technologies, security issues have become increasingly prominent, calling for access control mechanism. With the Access Control List (ACL) function, the switch matches packets with the list to implement access control.

3.9.2.2 Implementation

The series switches filter packets according to the matched ACL. Each entry consists several conditions in the logical AND relationship. ACL entries are independent of each other.

The switch compares a packet with ACL entries in the ascending order of entry IDs. Once a match is found, the action is taken and no further comparison is conducted, as shown in the following figure.

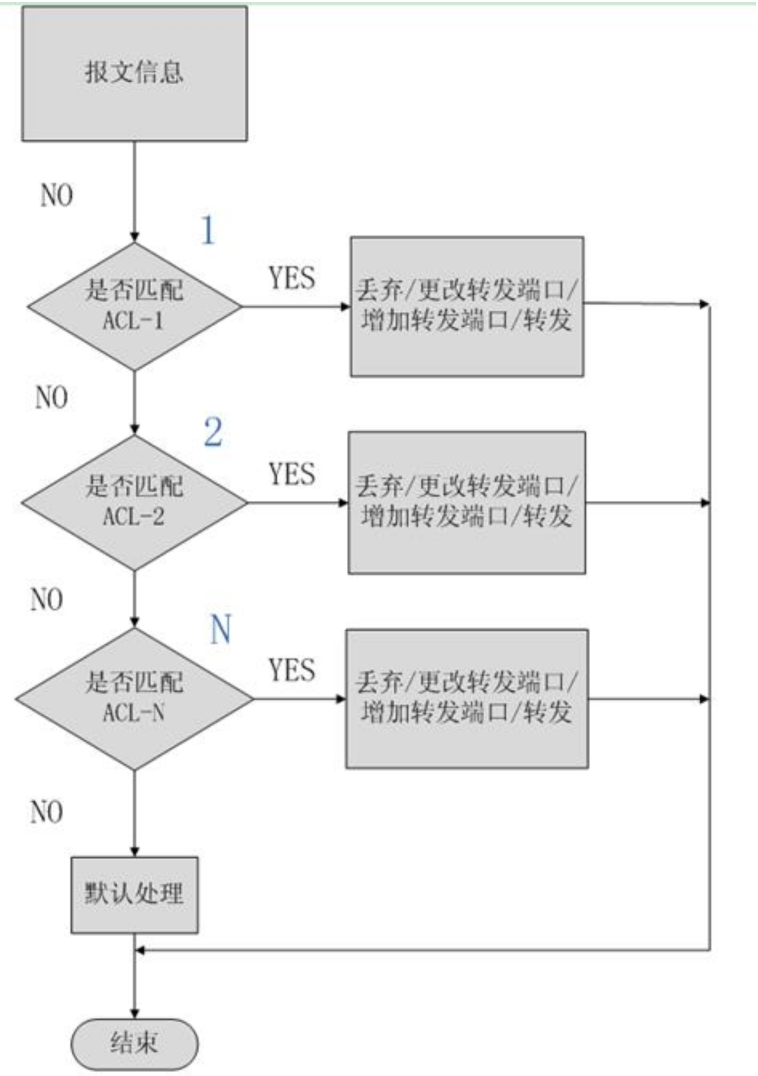


Figure 157 ACL Processing Flowchart

Note:

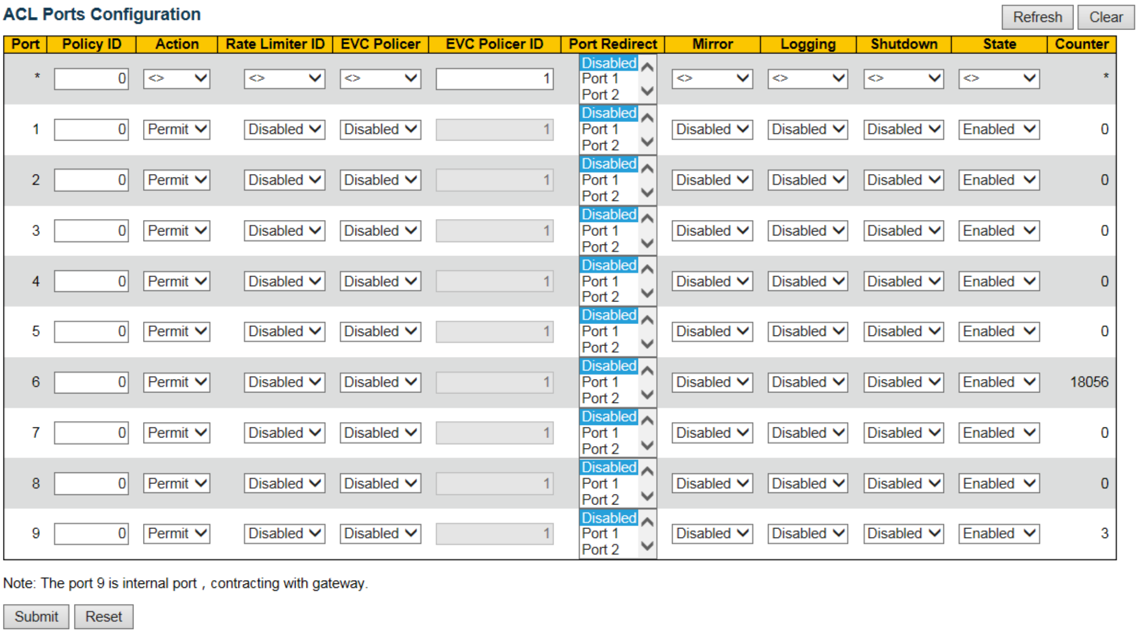
Default process indicates the processing mode towards packets matching no ACL entry.

3.9.2.3 Web Configuration

1. Configure ACL ports, as shown in Figure 158.

Caution:

The ACL port configuration specifies the processing mode of packets received by a port that do not match any ACL entry.



ACL Ports Configuration

Port	Policy ID	Action	Rate Limiter ID	EVC Policer	EVC Policer ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*	0	<>	<>	<>	1	Disabled Port 1 Port 2	<>	<>	<>	<>	*
1	0	Permit	Disabled	Disabled	1	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
2	0	Permit	Disabled	Disabled	1	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
3	0	Permit	Disabled	Disabled	1	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
4	0	Permit	Disabled	Disabled	1	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
5	0	Permit	Disabled	Disabled	1	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
6	0	Permit	Disabled	Disabled	1	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	18056
7	0	Permit	Disabled	Disabled	1	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
8	0	Permit	Disabled	Disabled	1	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
9	0	Permit	Disabled	Disabled	1	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	3

Note: The port 9 is internal port，contracting with gateway.

Figure 158 Configure ACL Ports

Policy ID

Range: 0~255

Default: 0

Function: Configure the port policy ID.

Action

Options: Deny/Permit

Default: Permit

Function: Configure the action towards a packet that mismatches any ACL entry. Deny: Packets mismatching any entry will be denied. Permit: Packets mismatching any entry will be forwarded.

Rate Limiter ID

Range: Disabled/1~16

Default: Disabled

Function: whether to enable port rate limite function, and select rate limiter ID.

EVC Policer

Options: Enabled/Disabled

Default: Disabled

Function: Enable/Disable port EVC policer.

EVC Policer ID

Range: 1~256

Default: 1

Function: After enabling EVC policer, configure port EVC policer ID.

Caution:

The port rate limit and EVC policy cannot be enabled simultaneously.

Port Redirect

Options: Disabled/ any port

Default: Disabled

Function: Enable/Disable port redirect function. After enabling port redirect function, packets mismatching any ACL entry will be forwarded to the specified port.

Caution:

Port redirection can be enabled only when Action is set to Deny.

Mirror

Options: Enabled/Disabled

Default: Disabled

Function: Enable/Disable port mirror function. After enabling port mirror function, packets mismatching any ACL entry will be forwarded to both the destination port and the mirror destination port.

Caution:

The prerequisite for enabling ACL port mirroring is that a mirroring destination port must exist.

Logging

Options: Enabled/Disabled

Default: Disabled

Function: Enable/Disable port logging function. Enabled: if a port receives a packet that does not match any ACL entry, the packet is written into the system log. Disabled: if a port receives a packet that does not match an ACL entry, the packet is not written into the system log.

Shutdown

Options: Enabled/Disabled

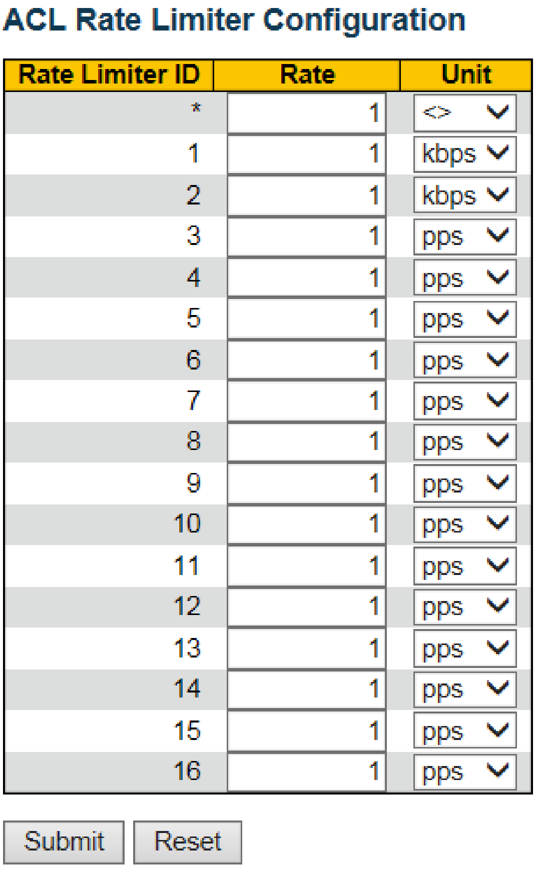
Default: Disabled

Function: whether to shutdown port or not. Enabled: if a port receives a packet that does not match any ACL entry, the port is shut down. Disabled: if a port receives a packet that does not match an ACL entry, the port is not shut down.

Counter

Function: Display the number of packets mismatching any ACL entry that each port receives.

2. Configure ACL rate limiter, as shown in Figure 159.



ACL Rate Limiter Configuration

Rate Limiter ID	Rate	Unit
*	1	<>
1	1	kbps
2	1	kbps
3	1	pps
4	1	pps
5	1	pps
6	1	pps
7	1	pps
8	1	pps
9	1	pps
10	1	pps
11	1	pps
12	1	pps
13	1	pps
14	1	pps
15	1	pps
16	1	pps

Figure 159 Configure ACL Rate Limiter

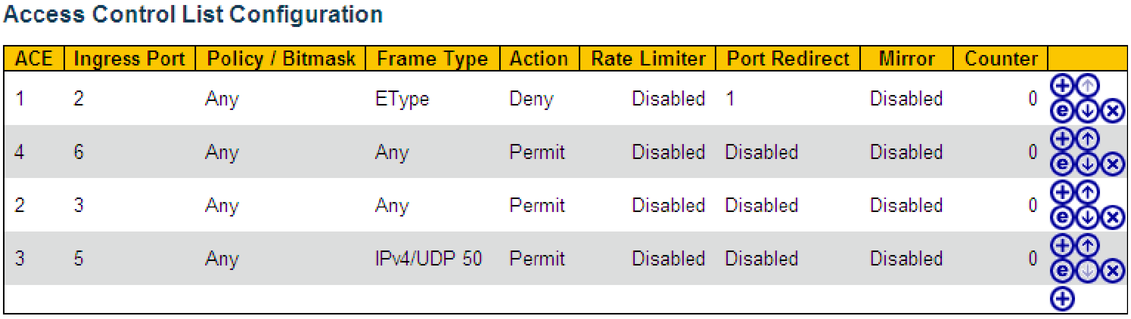
Rate Unit

Range: 0~3276700 pps/ 0~1000000 Kbps (the step is 100)

Default: 1 pps

Function: Set the limited rate of a rate limiter ID.

3. Configure ACL entry, as shown in Figure 160.



Access Control List Configuration

ACE	Ingress Port	Policy / Bitmask	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	Counter	
1	2	Any	EType	Deny	Disabled	1	Disabled	0	⊕ ↑ ⓔ ↓ ⊗
4	6	Any	Any	Permit	Disabled	Disabled	Disabled	0	⊕ ↑ ⓔ ↓ ⊗
2	3	Any	Any	Permit	Disabled	Disabled	Disabled	0	⊕ ↑ ⓔ ↓ ⊗
3	5	Any	IPv4/UDP 50	Permit	Disabled	Disabled	Disabled	0	⊕ ↑ ⓔ ↓ ⊗
									⊕

Figure 160 Configure ACL Entry

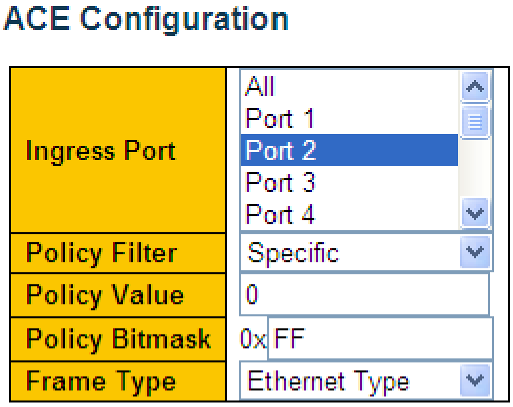
When there are multiple ACL entries, the device compares a packet with the ACL entries one by one (from top to bottom). Once a match is found, the action is taken and no further comparison is conducted.

Click <⊕> to add a new ACL entry; click <ⓔ> to edit the ACL entry; click <⊗> to delete the ACL entry, click <⌽> to move up the current entry; click <⌽> to move down the current entry.

ACE is the ID of a ACL entry, which is numbered based on the entry creation time sequence.

4. Configure the ACL entry parameters

➢ Configure the ACL entry parameters, as shown in Figure 161.



ACE Configuration

Ingress Port	All Port 1 Port 2 Port 3 Port 4
Policy Filter	Specific
Policy Value	0
Policy Bitmask	0x FF
Frame Type	Ethernet Type

Figure 161 Configure the ACL Entry Parameters

Ingress Port

Option: All/ any port

Default: All

Function: Select a port on which the access control entry (ACE) takes effect.

Policy Filter

Options: Any/Specific

Default: Any

Function: Set a ACE condition--policy ID. When it is set to Specific, a policy value and policy bitmask need to be set. When the policy value of a packet received by an ingress port meets settings of this parameter, the condition is matched successfully.

Policy Value

Range: 0~255

Function: Configure policy value.

Policy Bitmask

Range: 0x0~0xFF

Function: Set the policy bitmask. The policy value and policy bitmask are used for matching in the policy filtering. A policy bitmask is converted into binary digits and then right-aligned with the policy value (in binary mode). The value 1 indicates the same and the value 0 indicates that any value is allowed.

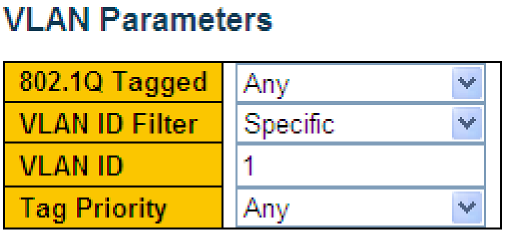
Frame Type

Options: Any/Ethernet Type/ARP/IPv4

Default: Any

Function: Set a condition--packet type. When the type of a packet received by an ingress port meets settings of this parameter, the condition is matched successfully.

➢ Configure VLAN parameters, as shown in Figure 162.



VLAN Parameters

802.1Q Tagged	Any
VLAN ID Filter	Specific
VLAN ID	1
Tag Priority	Any

Figure 162 Configure VLAN Parameters

802.1Q Tagged

Options: Any/ Disabled/ Enabled

Default: Any

Function: Set a condition--802.1Q tag. The value Disabled indicates untagged packets and the value Enabled indicates tagged packets. When a packet received by an ingress port meets settings of this parameter, the condition is matched successfully.

VLAN ID Filter

Options: Any/ Specific（1~4095）

Default: Any

Function: Set a condition--VID. When it is set to Specific, a VID value needs to be entered. When the VID in a packet received by an ingress port meets settings of this parameter, the condition is matched successfully. When 802.1Q Tagged is set to Disabled, this parameter needs to be set to Any.

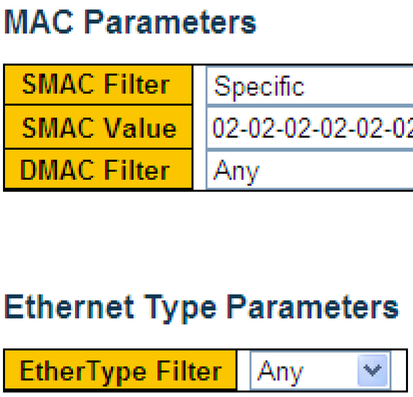
Tag Priority

Option: Any/0/1/2/3/4/5/6/7/0-1/2-3/4-5/6-7/0-3/4-7

Default: Any

Function: Set a condition--tag priority. When the priority in a packet received by an ingress port meets settings of this parameter, the condition is matched successfully. When 802.1Q Tagged is set to Disabled, this parameter needs to be set to Any.

- ➢ Configre EtherType frame parameters, as shown in Figure 163.



MAC Parameters

SMAC Filter	Specific
SMAC Value	02-02-02-02-02-02
DMAC Filter	Any

Ethernet Type Parameters

EtherType Filter	Any

Figure 163 Configre EtherType Frame Parameters

SMAC Filter

Options: Any/ Specific

Default: Any

Function: Set a condition--source MAC address. When it is set to Specific, a source MAC address needs to be set. When the source MAC address in a packet received by an ingress port meets settings of this parameter, the condition is matched successfully.

DMAC Filter

Options: Any/ UC/ MC / BC/ Specific

Default: Any

Function: Set a condition--destination MAC address. When it is set to Specific, a destination MAC address needs to be set. When the destination MAC address in a packet received by an ingress port meets settings of this parameter, the condition is matched successfully.

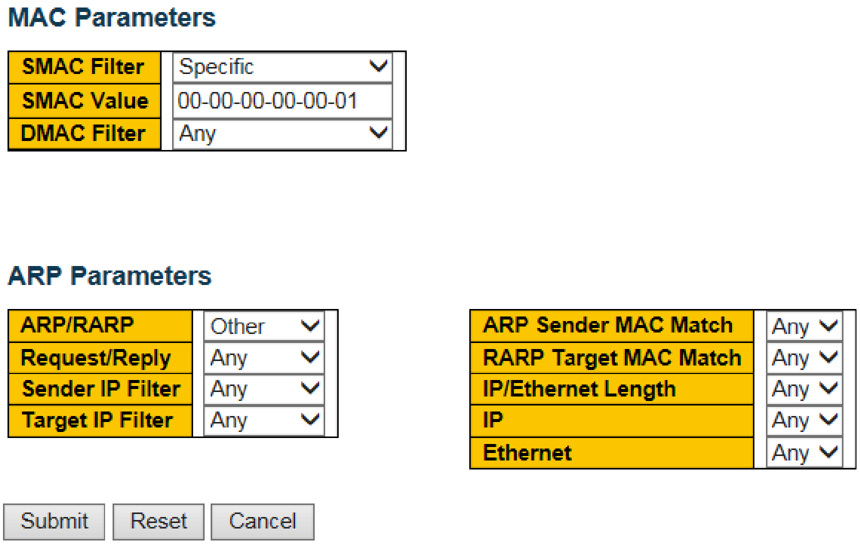
EtherType Filter

Options: Any/ Specific (0x600~0xFFFF, exclude 0x800(IPv4), 0x806(ARP), 0x86DD(IPv6))

Default: Any

Function: Set a condition--Ethernet type. When it is set to Specific, an Ethernet type needs to set. When an Ethernet packet received by an ingress port meets settings of this parameter, the condition is matched successfully.

Configure ARP frame parameters, as shown in the following figure.



MAC Parameters

SMAC Filter	Specific
SMAC Value	00-00-00-00-00-01
DMAC Filter	Any

ARP Parameters

ARP/RARP	Other
Request/Reply	Any
Sender IP Filter	Any
Target IP Filter	Any

ARP Sender MAC Match	Any
RARP Target MAC Match	Any
IP/Ethernet Length	Any
IP	Any
Ethernet	Any

Figure 164 Configure ARP Frame Parameters

SMAC Filter

Options: Any / Specific

Default: Any

Function: Configure the condition parameter - source MAC address. When you select

Specific, you need to configure a source MAC address. When the source MAC address of a packet received in the ingress port satisfies the parameter configuration, the condition matches successfully.

DMAC Filter

Options: Any / UC / MC / BC

Default: Any

Function: Configure the condition parameter - the destination MAC address.

ARP / RARP

Options: Any / ARP / RARP / Other

Default: Any

Function: Configuration Condition Parameter - ARP / RARP.

Request / Reply

Options: Any / Request / Reply

Default: Any

Function: Configure conditional parameters - Request / Reply.

Sender IP Filter

Options: Any / Host / Network

Default: Any

Function: Configure condition parameters - SenderIP filtering.

Tartget IP Filter

Options: Any / Host / Network

Default: Any

Function: Configure conditional parameters - Target IP Filter.

ARP Sender MAC Match

Options: Any / 0/1

Default: Any

Function: Configuration condition parameter -ARP Sender MAC Match.

RARP Target MAC Match

Options: Any / 0/1

Default: Any

Function: Configuration Condition Parameter -RARP Target MAC Match.

IP / Ethernet Length

Options: Any / 0/1

Default: Any

Function: Configure the condition parameter-IP / Ethernet length.

IP

Options: Any / 0/1

Default: Any

Function: Configure the condition parameter - IP.

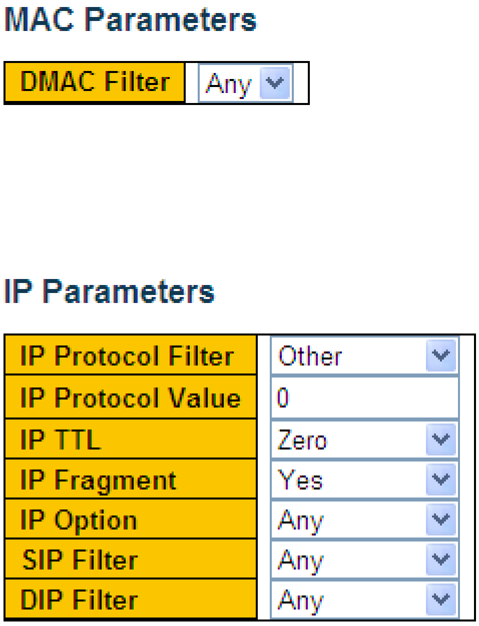
Ethernet

Options: Any / 0/1

Default: Any

Function: Configure the condition parameters - Ethernet.

➢ Configure IPv4 frame parameters, as shown in Figure 165.



MAC Parameters

DMAC Filter	Any

IP Parameters

IP Protocol Filter	Other
IP Protocol Value	0
IP TTL	Zero
IP Fragment	Yes
IP Option	Any
SIP Filter	Any
DIP Filter	Any

Figure 165 Configure IPv4 Frame Parameters

DMAC Filter

Options: Any/ UC/ MC / BC

Default: Any

Function: Set a condition--destination MAC address. When the destination MAC address in a packet received by an ingress port meets settings of this parameter, the condition is matched successfully.

IP Protocol Filter

Options: Any/ ICMP/ UDP/ TCP/ Other（0~255）

Default: Any

Function: Set a condition--IPv4 packet protocol type. When it is set to ICMP, UDP, or TCP, relevant parameters need to be set. When it is set to Other, a protocol ID needs to be set. When the protocol type in an IPv4 packet received by an ingress port meets settings of this parameter, the condition is matched successfully.

IP TTL

Options: Any/Non-zero/zero

Default: Any

Function: Set a condition--TTL field in IP packets. The value Non-zero indicates that the condition is matched when the IP TTL in an IPv4 packet is larger than 0, and the value Zero indicates that the condition is not matched when the IP TTL in an IPv4 packet is larger than 0.

IP Fragment

Options: Any/ Yes/ No

Default: Any

Function: Set a condition--IP fragment. When the IP fragment in an IPv4 packet received by an ingress port meets settings of this parameter, the condition is matched successfully.

IP Option

Options: Any/ Yes/ No

Default: Any

Function: Set a condition--IP option. When the IP option in an IPv4 packet received by an ingress port meets settings of this parameter, the condition is matched successfully.

SIP Filter

Options: Any/Host/Network

Default: Any

Function: Set a condition--source IP address. When it is set to Host, an IP address needs to be set. When it is set to Network, an IP address and a subnet mask need to be set. When the source IP address in an IPv4 packet received by an ingress port meets settings of this parameter, the condition is matched successfully.

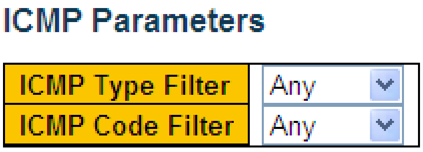
DIP Filter

Options: Any/Host/Network

Default: Any

Function: Set a condition--destination IP address. When it is set to Host, an IP address needs to be set. When it is set to Network, an IP address and a subnet mask need to be set. When the destination IP address in an IPv4 packet received by an ingress port meets settings of this parameter, the condition is matched successfully.

➢ Configure ICMP parameters, as shown in Figure 166.



ICMP Parameters

ICMP Type Filter	Any
ICMP Code Filter	Any

Figure 166 Configure ICMP Parameters

ICMP Type FFFilter

Options: Any/Specific（0~255）

Default: Any

Function: Set a condition--ICMP type. When it is set to Specific, an ICMP type needs to be set. When the ICMP type in an IPv4 packet received by an ingress port meets settings of this parameter, the condition is matched successfully.

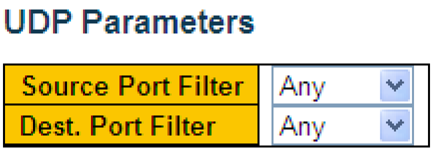
ICMP Code Filter

Options: Any/Specific（0~255）

Default: Any

Function: Set a condition--ICMP code. When it is set to Specific, an ICMP code needs to be set. When the ICMP code in an IPv4 packet received by an ingress port meets settings of this parameter, the condition is matched successfully.

➢ Configure UDP parameters, as shown in Figure 167.



UDP Parameters

Source Port Filter	Any
Dest. Port Filter	Any

Figure 167 Configure UDP Parameters

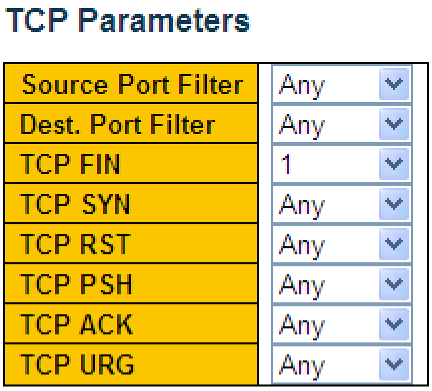
Source Port Filter/ Dest. Port Filter

Options: Any/ Specific（0~65535）/ Range（0~65535）

Default: Any

Function: Set a condition--UDP source port ID and destination port ID. When they are set to Specific, a port ID needs to be set. When they are set to Range, a port ID range needs to be set. When the UDP port IDs in an IPv4 packet received by an ingress port meets settings of the parameters, the condition is matched successfully.

➢ Configure TCP parameters, as shown in Figure 168.



TCP Parameters

Source Port Filter	Any
Dest. Port Filter	Any
TCP FIN	1
TCP SYN	Any
TCP RST	Any
TCP PSH	Any
TCP ACK	Any
TCP URG	Any

Figure 168 Configure TCP Parameters

Source Port Filter/ Dest. Port Filter

Options: Any/ Specific（0~65535）/ Range（0~65535）

Default: Any

Function: Set a condition--TCP source port ID and destination port ID. When they are set to Specific, a port ID needs to be set. When they are set to Range, a port ID range needs to be set. When the TCP port IDs in an IPv4 packet received by an ingress port meets settings of the parameters, the condition is matched successfully.

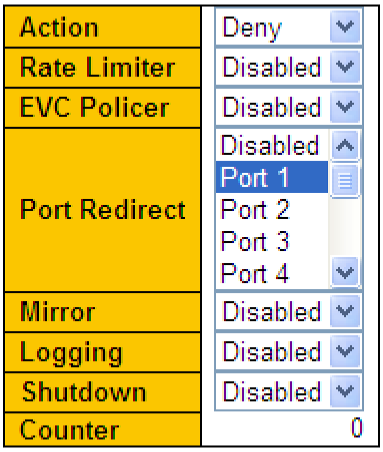
TCP FIN/SYN/RST/PSH/ACK/URG

Options: Any/1/0

Default: Any

Function: Set a condition--TCP control fields. When the TCP control fields in an IPv4 packet received by an ingress port meets settings of the parameters, the condition is matched successfully.

➢ Configure ACL entry action, as shown in Figure 169.



Action	Deny
Rate Limiter	Disabled
EVC Policer	Disabled
Port Redirect	Disabled Port 1 Port 2 Port 3 Port 4
Mirror	Disabled
Logging	Disabled
Shutdown	Disabled
Counter	0

Figure 169 Configure ACL Entry Action

Action

Options: Deny/Permit/Filter

Default: Permit

Function: Specify the mode for an ingress port to process a packet that matches an ACE. The value Deny indicates discarding the packet, the value Permit indicates forwarding the packet, and the value Filter indicates filtering the packet and a filtering port needs to be selected.

Rate Limiter

Options: Disabled/1~16

Default: Disabled

Function: whether to enable port rate limite function, and select rate limiter ID.

EVC Policer

Options: Enabled/Disabled

Default: Disabled

Function: Enable/Disable port EVC policer.

EVC Policer ID

Range: 1~256

Default: 1

Function: After enabling EVC policer, configure port EVC policer ID.

Caution:

The port rate limit and EVC policy cannot be enabled simultaneously.

Port Redirect

Options: Disabled/ any port

Default: Disabled

Function: Enable/Disable port redirect function. After enabling port redirect function, packets matching any entry will be forwarded to the specified port.

Caution:

Port redirection can be enabled only when Action is set to Deny.

Mirror

Options: Enabled/Disabled

Default: Disabled

Function: Enable/Disable port mirror function. After enabling port mirror function, packets matching any entry will be forwarded to both the destination port and the mirror destination port.

Caution:

The prerequisite for enabling ACL port mirroring is that a mirroring destination port must exist.

Logging

Options: Enabled/Disabled

Default: Disabled

Function: Enable/Disable port logging function.

Function: Enable/Disable port logging function. Enabled: if a port receives a packet that match any ACL entry, the packet is written into the system log. Disabled: if a port receives a packet that match an ACL entry, the packet is not written into the system log.

Shutdown

Options: Enabled/Disabled

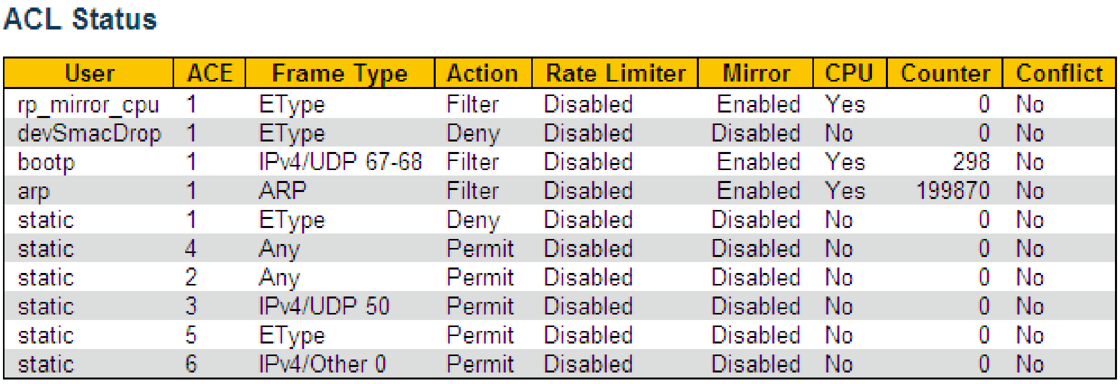
Default: Disabled

Function: whether to shutdown port or not. Enabled: if a port receives a packet that match any ACL entry, the port is shut down. Disabled: if a port receives a packet that match an ACL entry, the port is not shut down.

Counter

Function: Display the number of packets matching the ACE that each port receives.

➢ View ACL entries, as shown in Figure 170.



ACL Status

User	ACE	Frame Type	Action	Rate Limiter	Mirror	CPU	Counter	Conflict
rp_mirror_cpu	1	EType	Filter	Disabled	Enabled	Yes	0	No
devSmacDrop	1	EType	Deny	Disabled	Disabled	No	0	No
bootp	1	IPv4/UDP 67-68	Filter	Disabled	Enabled	Yes	298	No
arp	1	ARP	Filter	Disabled	Enabled	Yes	199870	No
static	1	EType	Deny	Disabled	Disabled	No	0	No
static	4	Any	Permit	Disabled	Disabled	No	0	No
static	2	Any	Permit	Disabled	Disabled	No	0	No
static	3	IPv4/UDP 50	Permit	Disabled	Disabled	No	0	No
static	5	EType	Permit	Disabled	Disabled	No	0	No
static	6	IPv4/Other 0	Permit	Disabled	Disabled	No	0	No

Figure 170 View ACL Entries

Conflict

Options: No/Yes

Function: Displays the conflict status of an ACL entry. If resources for creating an ACL entry are insufficient, **Conflict** is set to **Yes** for this entry. Otherwise, **Conflict** is set to **No** for this entry.

3.9.2.4 Typical Configuration Example

Connect port 2 of the switch. Configure the port to receive packets only from source MAC address 02-02-02-02-02-02 and forward the packets through port 1.

Configuration steps:

1. Configure the port action to Deny, as shown in Figure 158.

2. Configure ACL entry, set ingress port to 2, frame type to Ethernet Type, as shown in

Figure 161.

3. Set SMAC filter to 02-02-02-02-02-02, as shown in Figure 163.

4. Configuration ACL entry action to Deny, port redirect to port 1, as shown in Figure 169.

5. Keep all the other parameters default or empty.

3.10 Port Aggregation

3.10.1 Static Aggregation

3.10.1.1 Introduction

Port channel is to bind a group of physical ports that have the same configuration to a logical port to increase bandwidth and improve transmission speed. The member ports in a same group share traffic and serve as dynamic backups for each other, improving connection reliability.

Port group is a physical port group on the configuration layer. Only the physical ports that join in port group can participate in link aggregation and become a member of port channel. When physical ports in a port group meet certain conditions, they can conduct port aggregation and form a port channel and become an independent logical port, thereby increasing network bandwidth and providing link backup.

3.10.1.2 Implementation

As shown in Figure 171, three ports on Switch A and Switch B aggregate to form a port channel. The bandwidth of the port channel is the total bandwidth of these three ports.

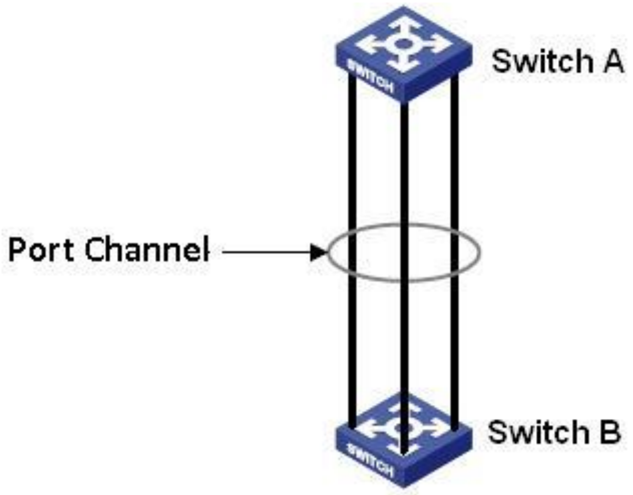


Figure 171 Port Channel

If Switch A sends packets to Switch B by way of the port channel, Switch A determines the member port for transmitting the traffic based on the calculation result of load sharing. When one member port of the port channel fails, the traffic transmitted through the port is taken over by another normal port based on load sharing algorithm.

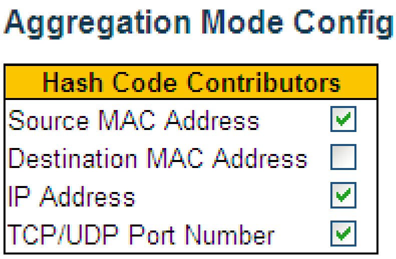
CAUTION

Caution:

- A port can be added to only one port group.
- Only full duplex ports can join an aggregation.
- The port in a port channel cannot be enabled LACP, and a port enabled LACP cannot be added to a port channel.
- Port channel and redundant port are mutually exclusive. The port in a port channel cannot be configured as a redundant port, and a redundant port cannot be added to a port channel.
- Redundant port in this document refers to DT-Ring ring port, DT-Ring backup port, DRP ring port, DRP backup port, RSTP port, and MSTP port.

3.10.1.3 Web Configuration

1. Configure load sharing mode of port channel, as shown in Figure 172.



Aggregation Mode Configuration

Hash Code Contributors	
Source MAC Address	☑
Destination MAC Address	□
IP Address	☑
TCP/UDP Port Number	☑

Figure 172 Load Sharing Mode Configuration

Hash Code Contributors

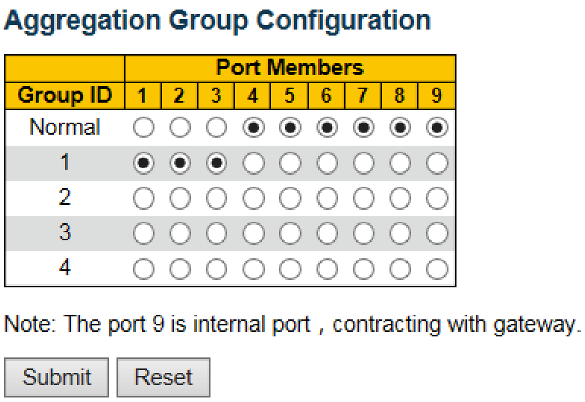
Options: Source MAC Address/Destination MAC Address/IP Address/ TCP/UDP Port Number

Default: Source MAC Address/IP Address/ TCP/UDP Port Number

Function: Set the load sharing mode of port channel.

Description: Source MAC Address indicates source MAC address-based load sharing. Destination MAC Address indicates destination MAC address-based load sharing. IP Address indicates IP address-based load sharing. TCP/UDP Port Number indicates load sharing based on TCP/UDP port number.

2. Configure aggregation group port members, as shown in Figure 173.



Aggregation Group Configuration

	Port Members								
Group ID	1	2	3	4	5	6	7	8	9
Normal	○	○	○	●	●	●	●	●	●
1	●	●	●	○	○	○	○	○	○
2	○	○	○	○	○	○	○	○	○
3	○	○	○	○	○	○	○	○	○
4	○	○	○	○	○	○	○	○	○

Note: The port 9 is internal port，contracting with gateway.

Figure 173 Configure Aggregation Group Port Members

Port Member

Function: Select aggregation group port members.

Description: All member ports in one aggregation group have the same configuration. The number of trunk groups depends on the number of switch ports. Each group can contain a maximum of 8 ports.

3.10.1.4 Typical Configuration Example

As shown in Figure 171, add three ports (port 1, 2, and 3) of Switch A to port group 1 and three ports (port 1, 2, and 3) of switch B to port group 1. Use network cables to connect these ports to form a port channel, realizing load sharing among ports. (It is assumed that the three ports on Switch A and B have the same attributes respectively).

Configuration on switches:

1. Add port 1, 2, and 3 of switch A to port group 1, as shown in Figure 173.
2. Add port 1, 2, and 3 of switch B to port group 1, as shown in Figure 173.

3.10.2 LACP

3.10.2.1 Introduction

Link Aggregation Control Protocol (LACP) is based on the IEEE802.3ad standard. It is used to exchange information with the peer port over Link Aggregation Control Protocol Data Unit (LACPDU), in order to select a member port in the dynamic aggregation group.

3.10.2.2 Implementation

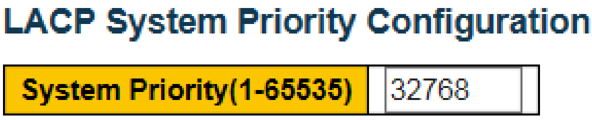
A port enabled with LACP informs the peer port of its LACP priority of the local equipment, equipment MAC address, LACP priority of the port, port number and key value by sending an LACPDU message. The peer port negotiates with the local port after receiving the LACPDU message:

1. Compare the IDs of the equipment at both ends (equipment ID = equipment LACP priority+ equipment MAC address). At first, compare the LACP priorities. If the LACP priorities are the same, compare their MAC addresses. Select the equipment with a smaller ID as the master equipment.
2. Compare the port IDs of the master equipment (port ID = LACP priority of the port + port number). At first, compare the LACP priorities of the ports. If the port LACP priorities are the same, compare the port numbers. Select the port with a smaller ID as the reference port.
3. If this port and reference port have the same key values, and the same port attribute configurations in Up state, and the peer ports of this port and the reference port have the

same key values and port attribute configurations, this port can become a member port of the dynamic aggregation group.

3.10.2.3 Web Configuration

1. Configure LACP system priority, as shown in the following figure.



LACP System Priority Configuration

System Priority(1-65535)	32768

Figure 174 Configure LACP System Priority

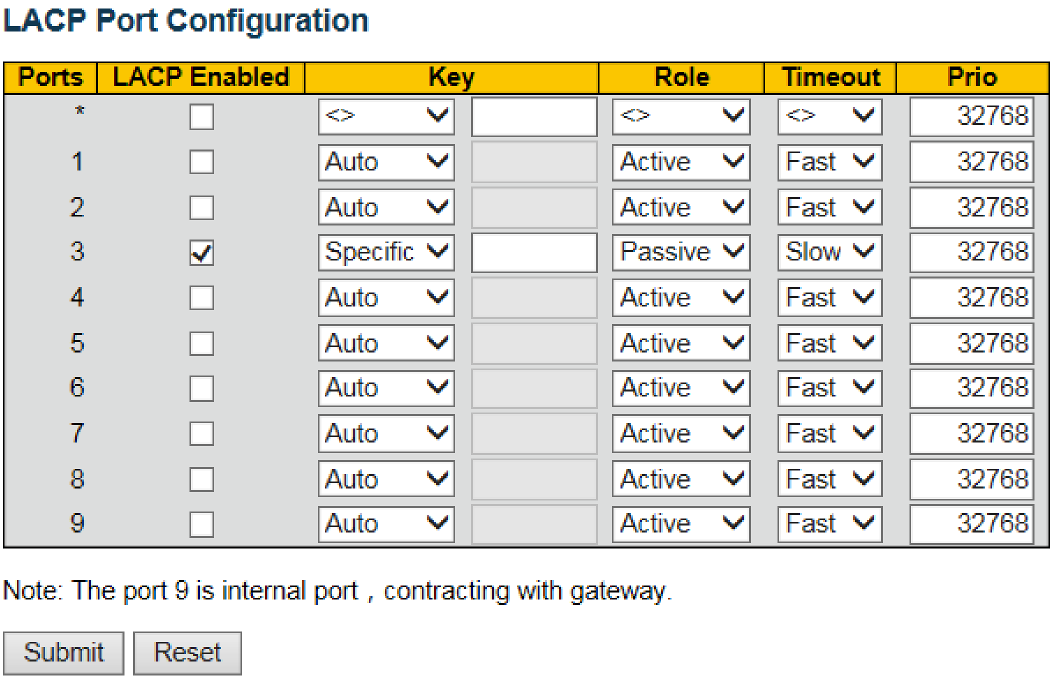
System Priority

Range: 1 ~ 65535

Default: 32768

Function: Configure the LACP system priority.

2.Configure LACP port, as shown in Figure 175.



LACP Port Configuration

Ports	LACP Enabled	Key		Role	Timeout	Prio
*	☐	<>		<>	<>	32768
1	☐	Auto		Active	Fast	32768
2	☐	Auto		Active	Fast	32768
3	☑	Specific		Passive	Slow	32768
4	☐	Auto		Active	Fast	32768
5	☐	Auto		Active	Fast	32768
6	☐	Auto		Active	Fast	32768
7	☐	Auto		Active	Fast	32768
8	☐	Auto		Active	Fast	32768
9	☐	Auto		Active	Fast	32768

Note: The port 9 is internal port , contracting with gateway.

Figure 175 Configure LACP Port

LACP Enabled

Options: Enable/Disable

Default: Disable

Function: Enable or disable LACP on port.

Key

Options: Auto/Specific (1~65535)

Default: Auto

Function: Configure the port key value. Auto means the key value depends on port speed, key=1 (10Mb), key=2 (100Mb), key=3 (1000Mb). Ports with different key values cannot be added to a aggregation group.

Role

Options: Active/Passive

Default: Active

Function: Selects the role state of LACP. An active port will actively send LACPDU messages to the peer port. A passive port will send LACPDU messages to the peer port after receiving LACPDU messages from the peer port.

CAUTION

Caution:

For two connected ports, at least one port should be active; otherwise, the two ports cannot exchange information with each other.

Timeout

Options: Fast/Slow

Default: Fast

Function: Configures the interval for the active port to send LACPDU messages. **Fast** indicates that the interval is 1s. **Slow** indicates that the interval is 30s.

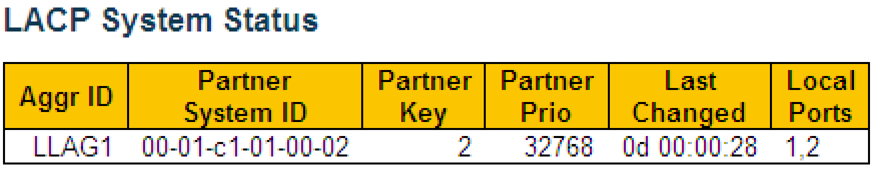
Prio

Default: 1~65535

Default: 32768

Function: Configures the LACP priority of a port, which is used for selecting a reference port. Port with a lower priority in the master equipment is selected as the reference port.

3. View LACP system status, as shown in Figure 176.

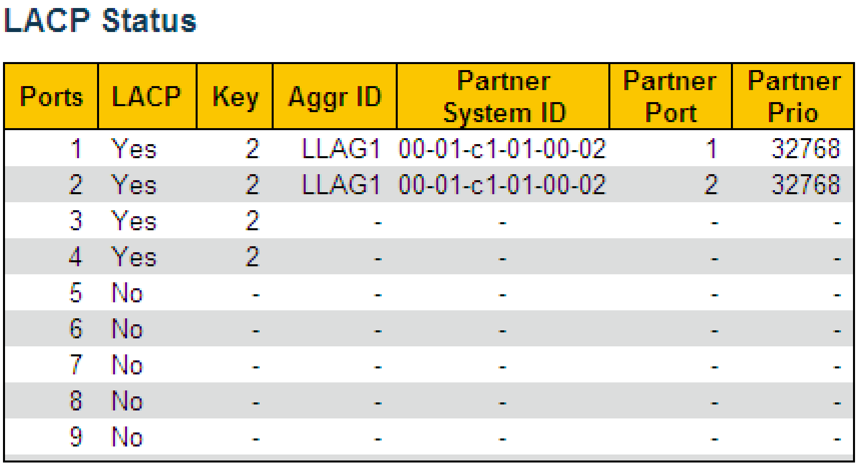


LACP System Status

Aggr ID	Partner System ID	Partner Key	Partner Prio	Last Changed	Local Ports
LLAG1	00-01-c1-01-00-02	2	32768	0d 00:00:28	1,2

Figure 176 View LACP System Status

4. View LACP port status, as shown in Figure 177.



LACP Status

Ports	LACP	Key	Aggr ID	Partner System ID	Partner Port	Partner Prio
1	Yes	2	LLAG1	00-01-c1-01-00-02	1	32768
2	Yes	2	LLAG1	00-01-c1-01-00-02	2	32768
3	Yes	2	-	-	-	-
4	Yes	2	-	-	-	-
5	No	-	-	-	-	-
6	No	-	-	-	-	-
7	No	-	-	-	-	-
8	No	-	-	-	-	-
9	No	-	-	-	-	-

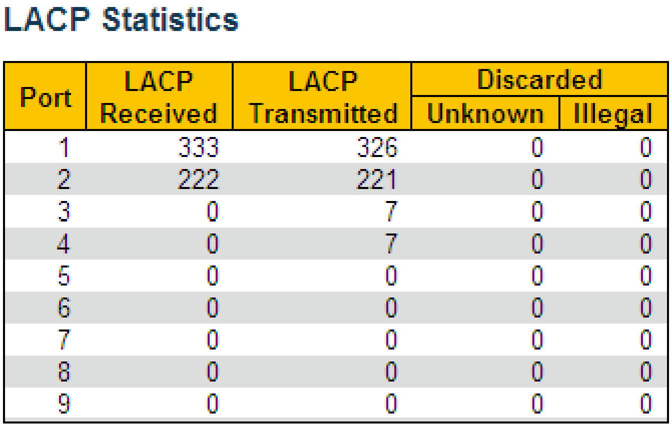
Figure 177 View LACP Port Status

LACP

Options: Yes/No

Function: View LACP port status. Yes means LACP is enabled and the port is link up. No means LACP is not enabled or the port is link down.

5. View LACP port statistics, as shown in Figure 178.



LACP Statistics

Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
1	333	326	0	0
2	222	221	0	0
3	0	7	0	0
4	0	7	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0

Figure 178 View LACP Port Statistics

3.10.2.4 Typical Configuration Example

As shown in Figure 171, add three ports (port 1, 2, and 3) of Switch A to port group 1 and three ports (port 1, 2, and 3) of switch B to port group 1. Use network cables to connect these ports to form a port channel, realizing load sharing among ports. (It is assumed that the three ports on Switch A and B have the same attributes respectively).

Configuration on switches:

1. Enable LACP on port 1, 2, and 3 of switch A , as shown in Figure 175.
2. Enable LACP on port 1, 2, and 3 of switch B , as shown in Figure 175.

3.11 Loop Detect Configuration

3.11.1 Overview

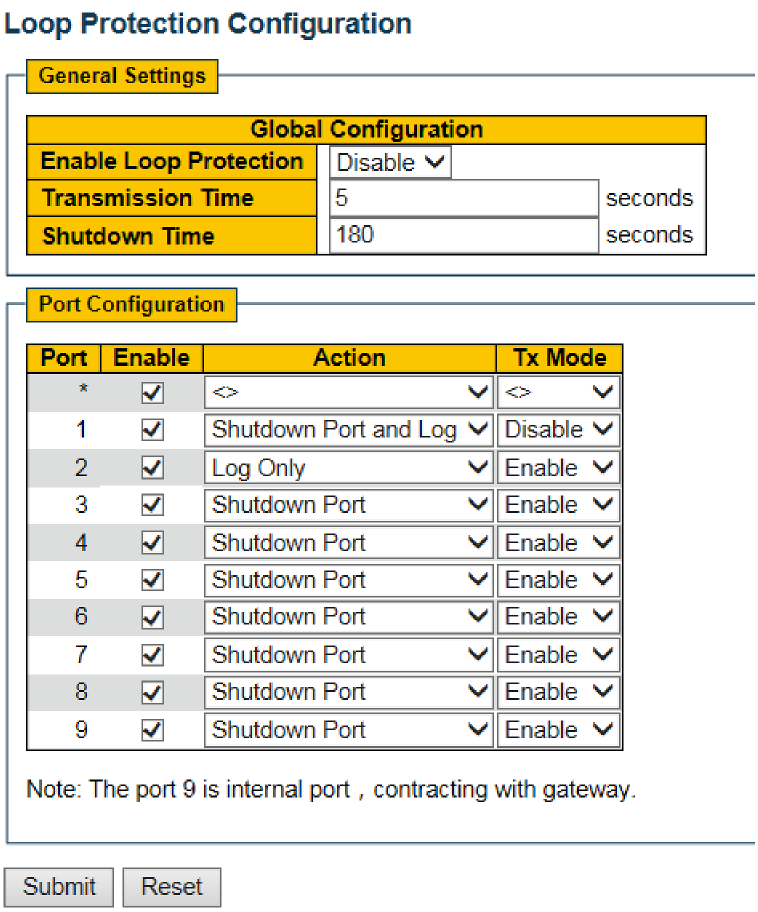
After loop detect is enabled for the port, loop detect packets would be sent out through the port to decide whether loops exist in the network connected to the port. The CPU send loop detect packets to the port periodically. If any port of the switch receives the loop detect packets, it is determined that the loops exist in the network. Shut down the port that is sending loop detect packets and the port would be linked up automatically after a while and continue detection. The time interval for sending loop detect packets and the port recover time can be configured in the software.

Note:

Loop detection and DT-Ring/DRP/RSTP/MSTP are mutually exclusive. A port enabled loop detection cannot be configured as a redandunt port; a redandunt port cannot be enabled loop detection.

3.11.2 Web Configuration

1. Configure the loop detect function of the port, as shown in Figure 179.



Loop Protection Configuration

General Settings

Global Configuration		
Enable Loop Protection	Disable ⌄	
Transmission Time	5	seconds
Shutdown Time	180	seconds

Port Configuration

Port	Enable	Action	Tx Mode
*	☑	<> ⌄	<> ⌄
1	☑	Shutdown Port and Log ⌄	Disable ⌄
2	☑	Log Only ⌄	Enable ⌄
3	☑	Shutdown Port ⌄	Enable ⌄
4	☑	Shutdown Port ⌄	Enable ⌄
5	☑	Shutdown Port ⌄	Enable ⌄
6	☑	Shutdown Port ⌄	Enable ⌄
7	☑	Shutdown Port ⌄	Enable ⌄
8	☑	Shutdown Port ⌄	Enable ⌄
9	☑	Shutdown Port ⌄	Enable ⌄

Note: The port 9 is internal port，contracting with gateway.

Figure 179 Enable the Loop Detect Function of the Port

Enable Loop Protection

Options: Enable/Disable

Default: Disable

Function：Enable or disable the global loop detect function of the port.

Transmission Time

Range: 1~10s

Default: 5s

Function: Configutr the time interval for sending loop detect packets.

Shutdown Time

Range: 0~604800s

Default: 180s

Function: Configure the port recover time, 0 indicates the port cannot be linked up automatically until restarting device.

Enable

Options: Enable/Disable

Default: Enable

Function：Enable or disable the loop detect function of the port.

Action

Option: Shutdown Port/Shutdown Port and Log/Log Only

Default: Shutdown Port

Function: Specify the action to be performed when a port detects that a loop exists.

Tx Mode

Options: Enable/Disable

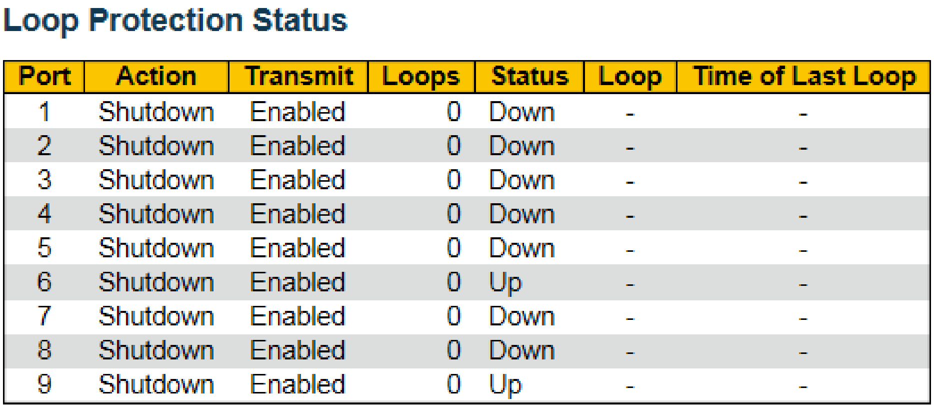
Default: Enable

Function: Whether to send loop detect packets or not.

Caution:

A port can accurately detect whether a loop exists only after the loop protection is enabled globally, the loop protection and Tx mode are enabled on the port.

2. View loop protection status, as shown in Figure 180.



Loop Protection Status

Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
1	Shutdown	Enabled	0	Down	-	-
2	Shutdown	Enabled	0	Down	-	-
3	Shutdown	Enabled	0	Down	-	-
4	Shutdown	Enabled	0	Down	-	-
5	Shutdown	Enabled	0	Down	-	-
6	Shutdown	Enabled	0	Up	-	-
7	Shutdown	Enabled	0	Down	-	-
8	Shutdown	Enabled	0	Down	-	-
9	Shutdown	Enabled	0	Up	-	-

Figure 180 View Loop Protection Status

Loop Protection Status

Options: -/Loop

Function: Loop detect status displays whether there are loops for the network in which the loop detect function of the port is enabled. Loop indicates there are loops while -- indicated no loop exists.

3.11.3 Typical Configuration Example

Networking Requirements:

Port 3 of the switch is connected to the external network. When there are loops for the network, shut down port 3, as shown in Figure 181.

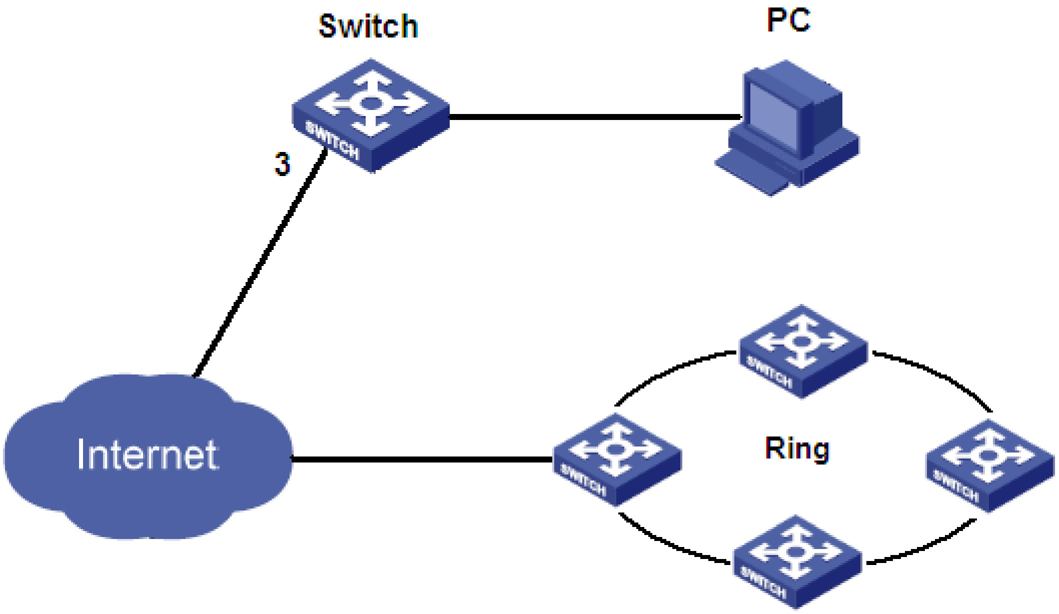


Figure 181 Loop Detect Instance

Specific configuration:

Enable the loop detect function of port 3, as shown in Figure 179.

3.12 IGMP Snooping

3.12.1 Introduction

Internet Group Management Protocol Snooping (IGMP Snooping) is a multicast protocol at the data link layer. It is used for managing and controlling multicast groups. IGMP Snooping-enabled switches analyze received IGMP packets, establish mapping between ports and MAC multicast addresses, and forward multicast packets according to the mapping.

There are three versions of the Internet Group Message Protocol (IGMP): IGMPv1, IGMPv2, and IGMPv3. IGMPv1 is defined in RFC1112, IGMPv2 is defined RFC2236, and IGMPv3 is defined in RFC3376.

IGMPv1 supports two types of packets (report and query packets) and defines the basic group member query and report process.

IGMPv2, on the basis of IGMPv1, provides the leave packet of the fast leave mechanism for group members. With this mechanism, when the last member leaves a multicast group, the router is instructed to conduct fast convergence. In comparison with IGMPv1, IGMPv2 supports two types of query packets: general query packet and group-specific query packet. The switch periodically sends a general query packet to query the membership. When a host leaves a multicast group, after the switch receives a leave message, the switch sends a group-specific query packet to determine whether all members leave the multicast group.

The host source filtering function is added to IGMPv3. This function enables a host to specify whether to receive or reject packets from some specific multicast group sources.

3.12.2 Basic Concepts

Querier: periodically sends IGMP general query packets to query the status of the members in the multicast group, maintaining the multicast group information. When multiple queriers exist on a network, they automatically elect the one with the smallest IP address to be the querier. Only the elected querier periodically sends IGMP general query packets. The other queriers only receive and forward IGMP query packets.

Router port: receives general query packets (on an IGMP-enabled switch) from the querier. Upon receiving an IGMP report, a switch establishes a multicast entry and adds the port that receives the IGMP report to the member port list. If a router port exists, it is also added to the member port list. Then the switch forwards the IGMP report to other devices through the router port, so that the other devices establish the same multicast entry.

IGMP snooping proxy: The IGMP snooping proxy function is configured on an edge device to reduce the number of IGMP report packets and leave packets received by an upstream device, thereby improving the overall performance of the upstream device. A device on which the IGMP snooping proxy function is configured functions as a host of its upstream device, and functions as a querier of its downstream host.

3.12.3 Principle

IGMP Snooping manages and maintains multicast group members by exchanging related packets among IGMP-enabled devices. The related packets are as follows:

General query packet: The querier periodically sends general query packets (destination IP address: 224.0.0.1) to confirm whether the multicast group has member ports. After receiving the query packet, a non-querier device forwards the packet to all its connected ports.

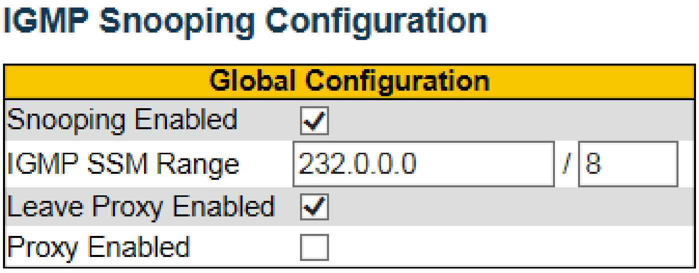
Specific query packet: If a device wants to leave a multicast group, it sends an IGMP leave packet. After receiving the leave packet, the querier sends a specific query packet (destination IP address: IP address of the multicast group) to confirm whether the group contains other member ports.

Membership report packet: If a device wants to receive the data of a multicast group, the device sends an IGMP report packet (destination IP address: IP address of the multicast group) immediately to respond to the IGMP query packet of the group.

Leave packet: If a device wants to leave a multicast group, the device will send an IGMP leave packet (destination IP address: 224.0.0.2).

3.12.4 Web Configuration

1. Enable IGMP Snooping, as shown in Figure 182.



IGMP Snooping Configuration

Global Configuration	
Snooping Enabled	☑
IGMP SSM Range	232.0.0.0 / 8
Leave Proxy Enabled	☑
Proxy Enabled	□

Figure 182 Enabling IGMP Snooping

Snooping Enabled

Options: Enable/Disable

Default: Disable

Function: Enable or disable the global IGMP Snooping protocol.

IGMP SSM Range

Format: A.B.C.D/ 4~32

Default: 232.0.0.0/8

Function: Only hosts and routers with the address within the value of this parameter can run the service model of IGMP source specific multicast (SSM) provided that the hosts and routers support the IGMP SSM service model. The SSM service model provides users with a transmission service of specifying multicast sources for a client.

Leave Proxy Enabled

Options: Enabled/Disabled

Default: Disabled

Function: Specify whether to forward leave packets to the querier. When it is enabled, leave packets are not forwarded.

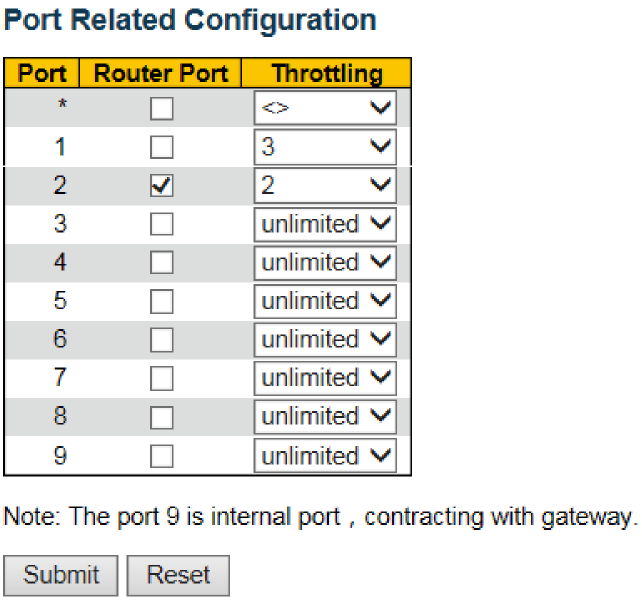
Proxy Enabled

Options: Enabled/Disabled

Default: Disabled

Function: Specify whether to forward leave packets and member report packets to the querier. When it is enabled, leave packets and member report packets are not forwarded.

2. Configure IGMP port, as shown in Figure 183.



Port Related Configuration

Port	Router Port	Throttling
*	□	<>
1	□	3
2	☑	2
3	□	unlimited
4	□	unlimited
5	□	unlimited
6	□	unlimited
7	□	unlimited
8	□	unlimited
9	□	unlimited

Note: The port 9 is internal port , contracting with gateway.

Figure 183 Configure IGMP Port

Router Port

Options: Enabled/Disabled

Default: Disabled

Function: Configure router port.

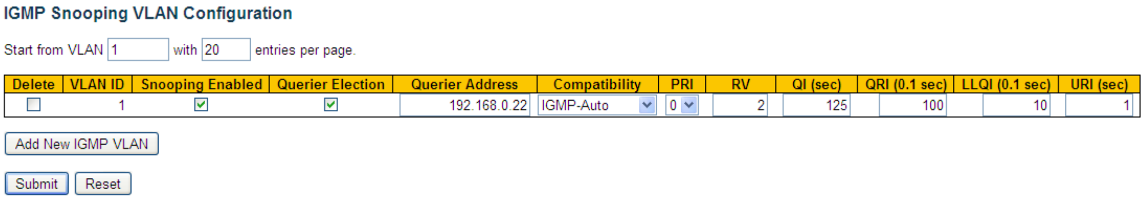
Throttling

Options: unlimited/1~10

Default: unlimited

Function: Whether to limit the number of multicast entries learnt by a port.

3. Configure IGMP Snooping VLAN, as shown in Figure 184.



IGMP Snooping VLAN Configuration

Start from VLAN 1 with 20 entries per page.

Delete	VLAN ID	Snooping Enabled	Querier Election	Querier Address	Compatibility	PRI	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
□	1	☑	☑	192.168.0.22	IGMP-Auto	0	2	125	100	10	1

Figure 184 Configure IGMP Snooping VLAN

VLAN ID

Options: all created VLAN IDs

Snooping Enabled

Options: Enable/Disable

Default: Disable

Function: Enable or disable the VLAN IGMP Snooping function. The precondition of this function is to enable global IGMP Snooping function.

Querier Election

Options: Enable/Disable

Default: Enable

Function: Enable or disable the IGMP query function for the selected VLAN. The precondition of this function is to enable global IGMP Snooping function and the VLAN IGMP Snooping function.

Description: If there are multiple queriers in network, they will automatically select the one with the smallest IP address to be the querier. If there is only one device which enables IGMP query function, it will be the querier.

Querier Address

Format: A.B.C.D

Function: Configure the source IP address of sending the query packet. When no querier address is set, the IP address of the VLAN port is used as the querier address.

Compatibility

Options: IGMP-Auto/Forced IGMPv1/Forced IGMPv2/Forced IGMPv3

Default: IGMP-Auto

Function: Configure IGMP version.

PRI（Priority of Interface）

Range: 0~7

Default: 0

Function: Configure the priority of IGMP control packet.

RV（Robustness Variable）

Range: 1~255

Default: 2

Function: Specify the robustness parameter of the IGMP query function.

Description: The larger the parameter, the worse the network environment. User can set a suitable robustness parameter according to the actual network.

QI（Query Interval）

Range: 1~31744s

Default: 125s

Function: Configure the interval of sending general query packet.

QRI（Query Response Interval）

Range: 0~31744（unit: 0.1s）

Default: 100

Function: Configure the max response time of responding general query packet.

LLQI（Last Member Query Interval）

Range: 0~31744（unit: 0.1s）

Default: 10

Function: Configure the max response time of responding specific query packet.

Caution:

QI, QRI, and LLQI configuration is valid only for querier.

URI（Unsolicited Report Interval）

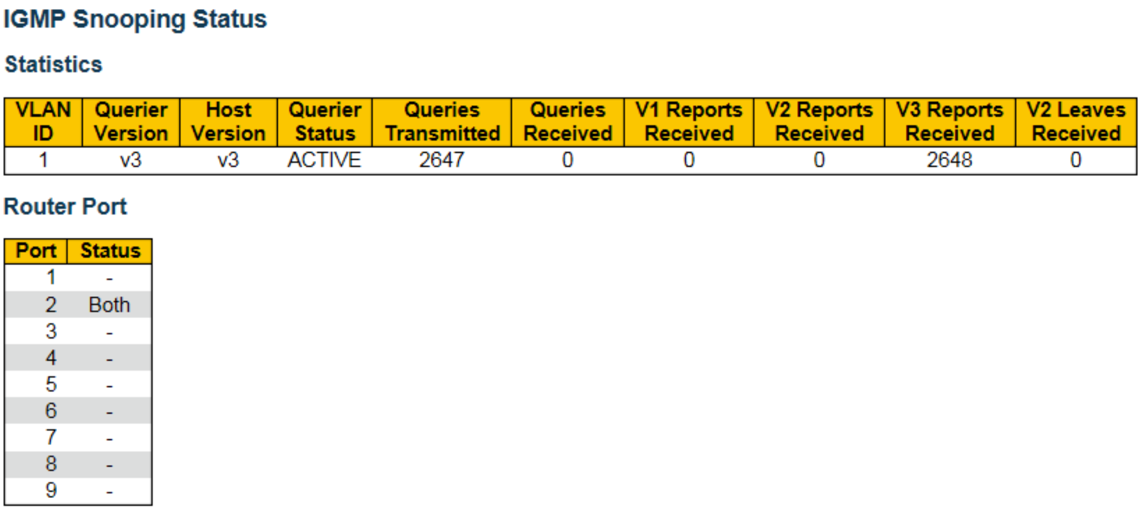
Range: 0~31744s

Default: 1s

Function: Set the interval for a host to re-send a report packet for joining a multicast group

Click <Add New IGMP VLAN> to configure IGMP Snooping VLAN entry. A maximum of 32 IGMP Snooping VLAN entries are suppoted.

4. View IGMP Snooping status, as shown in Figure 185.



IGMP Snooping Status

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received
1	v3	v3	ACTIVE	2647	0	0	0	2648	0

Router Port

Port	Status
1	-
2	Both
3	-
4	-
5	-
6	-
7	-
8	-
9	-

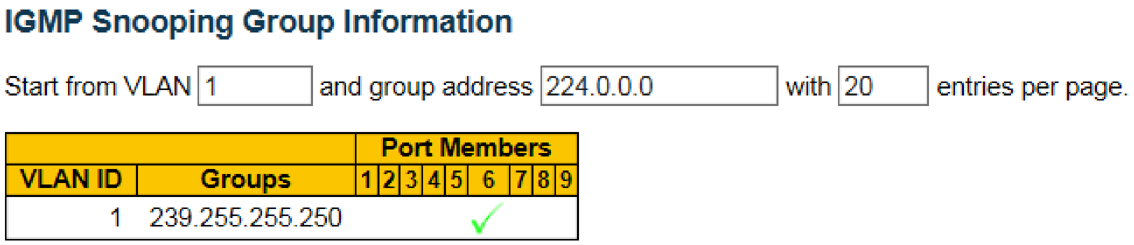
Figure 185 View IGMP Snooping Status

Router Port Status

Options: Both/Static/Dynamic

Function: Display router port status. Static indicates that a port is statically configured as a router port, Dynamic indicates that a port is dynamically learnt as a router port, and Both indicates that a port is statically configured as a router port or dynamically learnt as a router port.

5. View the multicast member list, as shown in Figure 186.



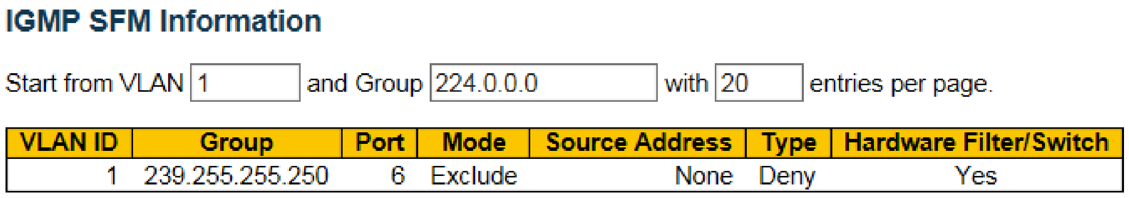
IGMP Snooping Group Information

Start from VLAN 1 and group address 224.0.0.0 with 20 entries per page.

		Port Members								
VLAN ID	Groups	1	2	3	4	5	6	7	8	9
1	239.255.255.250						✓			

Figure 186 IGMP Snooping Member List

6. View the IGMP SFM information as shown in the following figure:



IGMP SFM Information

Start from VLAN 1 and Group 224.0.0.0 with 20 entries per page.

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
1	239.255.255.250	6	Exclude	None	Deny	Yes

Figure 187 IGMP SFM information

3.12.5 Typical Application Example

As shown in Figure 188, enable IGMP Snooping function in Switch 1, Switch 2, and Switch 3. Enable auto query on Switch 2 and Switch 3. The IP address of Switch 2 is 192.168.1.2 and that of Switch 3 is 192.168.0.2, so Switch 3 is elected to querier.

1. Enable IGMP Snooping.

2. Enable IGMP Snooping and auto-query.

3. Enable IGMP Snooping and auto-query.

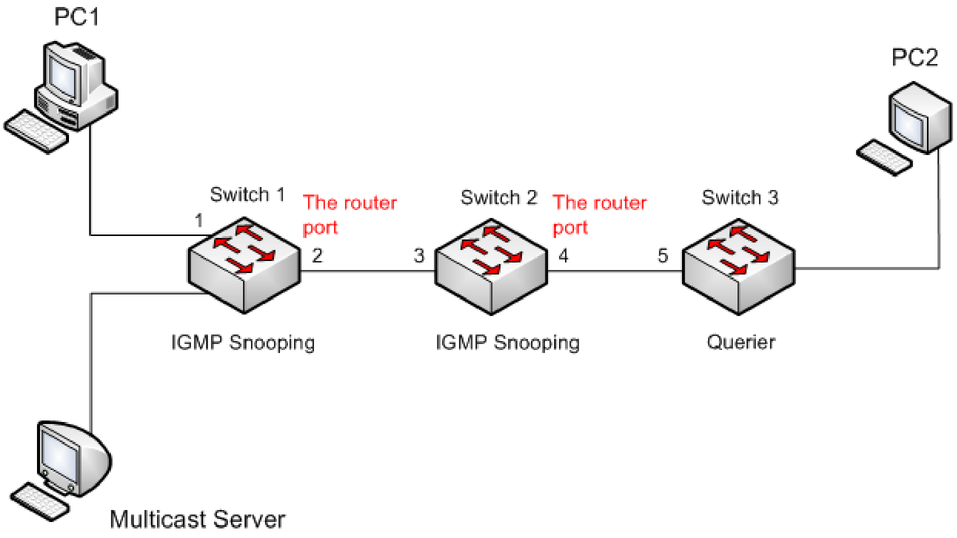


Figure 188 IGMP Snooping Application Example

- Because Switch 3 is elected as the querier, it periodically sends out a general query message.
- Port 4 of Switch 2 receives query message. It becomes router port. Meanwhile, Switch 2 forwards query message from port 3. Then port 2 of Switch 1 is elected to router port once it receives query message from Switch 2.
- When PC 1 joins in multicast group 225.1.1.1, it will send out IGMP report message, so port 1 and router port 2 of Switch 1 will also join in multicast group 225.1.1.1. Then, the IGMP report message will be forwarded to Switch 2 by router port 2, so port 3 and port 4 of Switch 2 will also join in 225.1.1.1, and then the IGMP report message will be forwarded to Switch 3 by router port 4, so port 5 of Switch 3 will join in 225.1.1.1 as well.
- When multicast server's multicast data reaches Switch 1, the data will be forwarded to PC1 by port 1; because router port 2 is also a multicast group member, so the multicast data will be forwarded by router port. In this way, when the data reaches port 5 of Switch 3, it will stop forwarding because there is no receiver any more, but if PC2 also joins in group 255.1.1.1, the multicast data will be forwarded to PC2.

3.13 GMRP

3.13.1 GARP Introduction

The Generic Attribute Registration Protocol (GARP) is used for spreading, registering, and cancelling certain information (VLAN, multicast address) among switches on the same network.

With GARP, the configuration information of a GARP member will spread the information to the entire switching network. A GARP member instructs the other GARP members to register or cancel its own configuration information by means of join/leave message respectively. The member also registers or cancels the configuration information of other members based on join/leave messages sent by other members.

GARP involves three types of messages: Join, Leave, and LeaveAll.

- When a GARP application entity wants to register its own information on other switches, the entity sends a Join message. Join messages fall into two types: JoinEmpty and JoinIn.

A JoinIn message is sent to declare a registered attribute, while a JoinEmpty message is sent to declare an attribute that is not registered yet.

- When a GARP application entity wants to cancel its own information on other switches, the entity sends a Leave message. Leave messages fall into two types: LeaveEmpty and LeaveIn. A LeaveIn message is sent to cancel a registered attribute, while a LeaveEmpty message is sent to cancel an attribute that is not registered yet.
- After a GARP entity starts, it starts the LeaveAll timer. When the timer expires, the entity sends a LeaveAll message.

Note:

An application entity indicates a GARP-enabled port.

GARP timers include Hold timer, Join timer, Leave timer, and LeaveAll timer.

Hold Timer: When receiving a registration message, a GARP entity does not send a Join message immediately, but starts Hold timer. When the timer expires, the entity sends all the registration messages received within the preceding period in one Join message, reducing packet sending for better network stability.

Join Timer: To ensure that Join messages are received by other application entities, a GARP application entity starts Join timer after sending a Join message. If receiving no JoinIn message before Join timer expires, the entity sends the Join message again. If receiving a JoinIn message before the timer expires, the entity does not send the second Join message.

Leave Timer: When a GARP application entity wants to cancel the information about an attribute, the entity sends a Leave message. The entity receiving the message starts Leave timer. If receiving no Join message before the timer expires, the entity receiving the message cancels the information about the attribute.

LeaveAll Timer: As a GARP application entity starts, it starts LeaveAll timer. When the timer expires, the entity sends a LeaveAll message, so that the other GARP application entities re-register all the attributes. Then the entity starts LeaveAll timer again for the new cycle.

3.13.2 GMRP Protocol

The GARP Multicast Registration Protocol (GMRP) is a multicast registration protocol based on GARP. It is used for maintaining the multicast registration information of switches. All GMRP-enabled switches can receive multicast registration information from other switches, update local multicast registration information dynamically, and spread local multicast registration information to other switches. This information exchange mechanism ensures the consistency of multicast information maintained by all GMRP-enabled switches on a network.

If a switch or terminal wants to join or leave a multicast group, the GMRP-enabled port broadcasts the information to all the ports in the same VLAN.

3.13.3 Explanation

Agent port: indicates the port on which GMRP and the agent function are enabled.

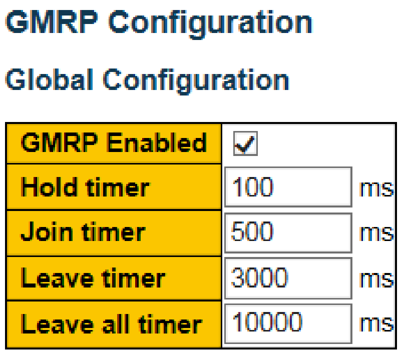
Propagation port: indicates the port on which only GMRP is enabled, but not the proxy function.

Dynamically learned GMRP multicast entry and agent entry are forwarded by the propagation port to the propagation ports of the lower-level devices.

All GMRP timers on the same network must keep consistent to prevent mutual interference. The timers should comply with the following rules: Hold timer<Join timer, 2*Join timer<Leave timer, and Leave timer<LeaveAll timer.

3.13.4 Web Configuration

1. Configure the global GMRP protocol ,as shown in the following figure.



GMRP Configuration

Global Configuration

GMRP Enabled	☑
Hold timer	100 ms
Join timer	500 ms
Leave timer	3000 ms
Leave all timer	10000 ms

Figure 189 Configure Global GMRP

GMRP Enabled

Options: Enable/Disable

Default: Disable

Function: Enable/Disable the global GMRP function. The function cannot be used together with the IGMP Snooping function.

Hold Timer

Range: 100ms~327600ms

Default: 100ms

Description: This value must be a multiple of 100. It is better to set same time of Hold timers on all GMRP-enabled ports

Join Timer

Range: 100ms~327600ms

Default: 500ms

This value must be a multiple of 100. It is better to set same time of Join timers on all GMRP-enabled ports

Leave Timer

Range: 100ms~327600ms

Default: 3000ms

This value must be a multiple of 100. It is better to set same time of Leave timers on all GMRP-enabled ports

Leave-All timer

Range: 100ms~327600ms

Default: 10000ms

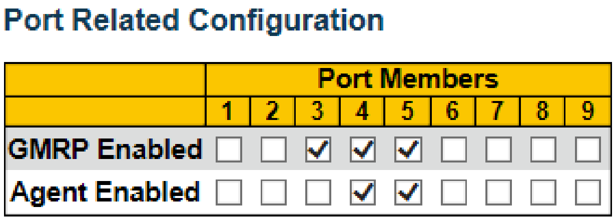
Function: The time interval for sending LeaveAll packets. The value must be a multiple of 100.

Explanation: if different devices' LeaveAll timers expire at the same time, they will send multiple LeaveAll messages at the same time, which increases message quantity. In order to avoid the expiration of LeaveAll timers of different devices at the same time, the actual running time of LeaveAll timer is a random value that is longer than the time of one LeaveAll timer, and less than 1.5 times of LeaveAll timer.

Note:

- Hold Timer < Join Timer;
- 2*Join Timer < Leave Timer;
- Leave Timer< LeaveAll Timer

2. Configure the GMRP function for each port ,as shown in the following figure.



Port Related Configuration

	Port Members								
	1	2	3	4	5	6	7	8	9
GMRP Enabled	□	□	☑	☑	☑	□	□	□	□
Agent Enabled	□	□	□	☑	☑	□	□	□	□

Figure 190 Port Related Configuration

GMRP Enabled

Options: Enable/Disable

Default: Disable

Function: Enable GMRP function on port or not.

Agent Enabled

Options:Enable/Disable

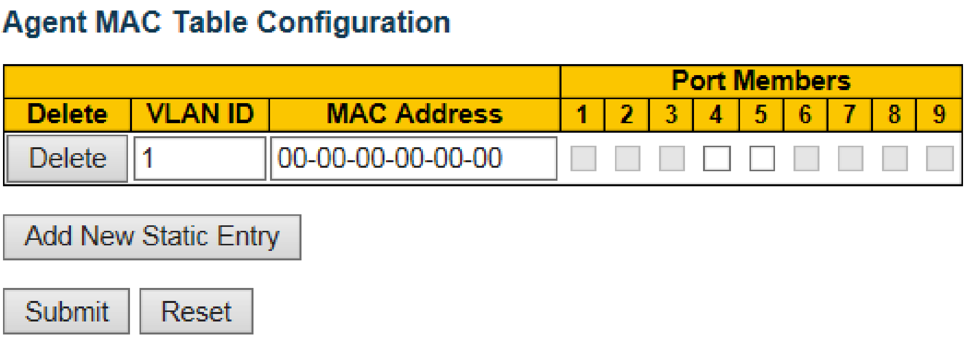
Default:Disable

Function: Enable GMRP agent function on port or not.

Caution:

- The Agent port can not propagate Agent entries.
- Enable the port GMRP Agent function on the assumption that the port GMRP function is enabled.

3. Add the Agent MAC Table, as shown in the following figure.



Agent MAC Table Configuration

			Port Members								
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9
Delete	1	00-00-00-00-00-00	□	□	□	□	□	□	□	□	□

Figure 191 Add Agent MAC Table

VLAN ID

Options: all created VLAN numbers

Function: Configure the VLAN ID for the GMRP agent entry.

Description: GMRP agent entry can only be forwarded from the propagation port with the VLAN ID same as this entry's VLAN ID.

MAC address

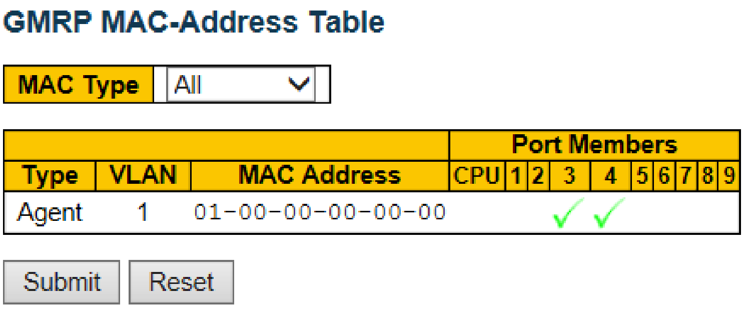
Format: HH-HH-HH-HH-HH-HH (H is a hexadecimal number)

Function: Configure the MAC address of multicast group. The lowest bit of the first byte is 1.

Port Members

Options: Configured Agent port

4. View the GMRP MAC-address table, as shown in the following figure.



GMRP MAC-Address Table

MAC Type: All

			Port Members									
Type	VLAN	MAC Address	CPU	1	2	3	4	5	6	7	8	9
Agent	1	01-00-00-00-00-00				✓	✓					

Figure 192 GMRP MAC-address table

3.13.5 Typical Configuration Example

As shown in Figure 193, Switch A and Switch B are connected by port 2. Port 1 of Switch A is set to an agent port and generates two multicast entries:

MAC address: 01-00-00-00-00-01, VLAN: 1

MAC address: 01-00-00-00-00-02, VLAN: 2

After configuring different VLAN attributes on ports, observe the dynamic registration between switches and multicast information update.

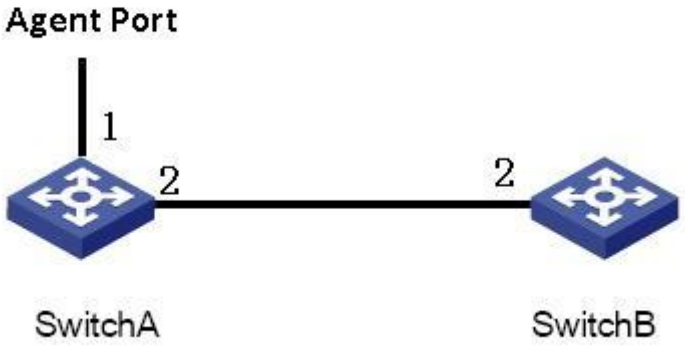


Figure 193 GMRP Networking

Configuration on Switch A:

1. Enable global GMRP function in switch A; set LeaveAll timer to the default value, as shown in Figure 189.

2. Enable GMRP function and agent function in port 1; enable only GMRP function in port 2; set the timers to default values, as shown in Figure 190.

3. Configure agent multicast entry. Set <MAC address, VLAN ID, Member port> to <01-00-00-00-00-01, 1, 1> and <01-00-00-00-00-02, 2, 1>, as shown in Figure 191.

Configuration on Switch B:

4. Enable global GMRP function in switch B; set LeaveAll timer to the default value, as shown in Figure 189.

5. Enable GMPR function in port 2; set the timers to default values, as shown in Figure 189.

Table 1 lists the dynamically learned GMRP multicast entries in Switch B.

Table 1 Dynamic Multicast Entries

Attribute of Port 2 on Switch A	**Attribute of Port 2 on Switch B**	**Multicast Entries Received on Switch B**
Access VID=1	Access VID=1	MAC: 01-00-00-00-00-01 VLAN ID: 1 Member port: 2
Access VID=2	Access VID= 2	MAC: 01-00-00-00-00-02

		VLAN ID: 2 Member port: 2
Access VID= 1	Access VID= 2	MAC: 01-00-00-00-00-01 VLAN ID: 2 Member port: 2

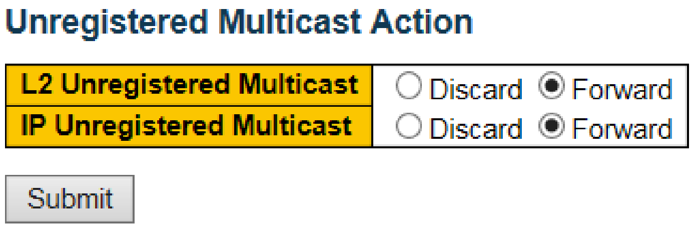
3.14 Unregistered Multicast Action Configuration

3.14.1 Introduction

Unregistered multicast packets refer to the multicast packets without corresponding forwarding entries on the switch. When receiving an unregistered multicast packet, the switch broadcasts the packet within the VLAN (all ports except the inlet port). This will occupy large network bandwidth, affecting the forwarding rate. In this case, the function of discarding unregistered multicast packets can be enabled. If this function is enabled, after receiving an unregistered multicast packet, the switch discards it rather than forwards it.

3.14.2 Web Configuration

1. Configure unregistered multicast action, as shown in the following figure.



Unregistered Multicast Action

L2 Unregistered Multicast	○ Discard ● Forward
IP Unregistered Multicast	○ Discard ● Forward

Figure 194 Configure Unregistered Multicast Action

L2 Unregistered Multicast Action

Options: Forward / Discard

Default: Forward

Function: Configure the processing mode of L2 Unregistered Multicast packets.

Ip Unregistered multicast

Options: Forward / Discard

Default: Forwarding

Function: Configure the handling mode of ip Unregistered multicast packets.

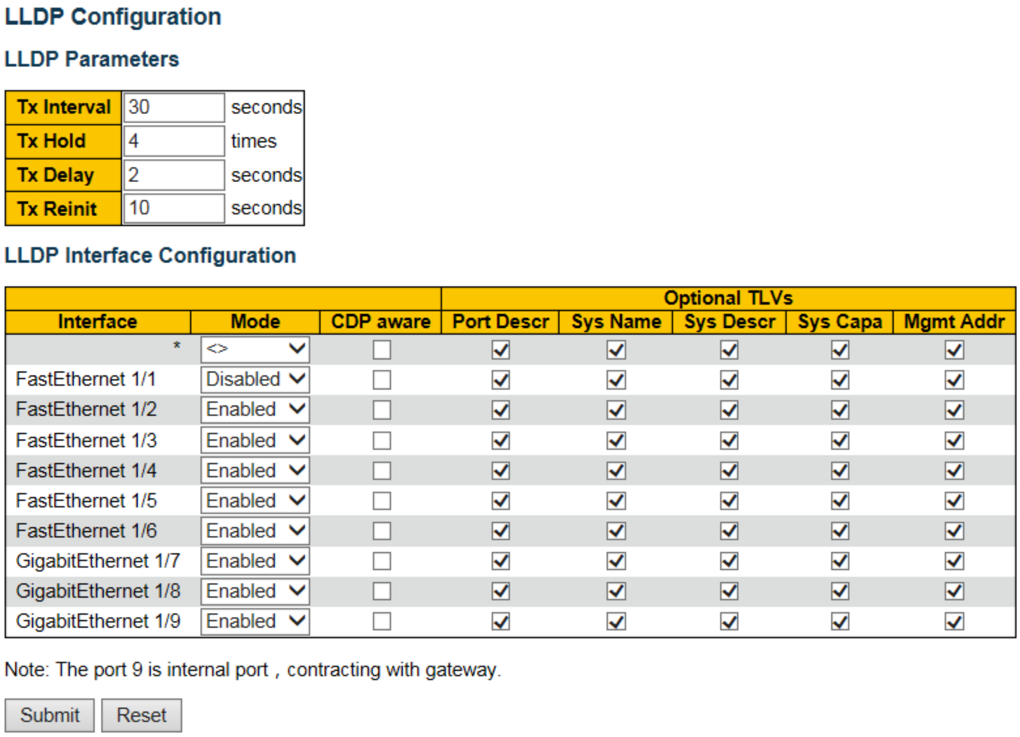
3.15 LLDP

3.15.1 Introduction

The Link Layer Discovery Protocol (LLDP) provides a standard link layer discovery mechanism. It encapsulates device information such as the capability, management address, device identifier, and interface identifier in a Link Layer Discovery Protocol Data Unit (LLDPDU), and advertises the LLDPDU to its directly connected neighbors. Upon receiving the LLDPDU, the neighbors save these information to MIB for query and link status check by the NMS.

3.15.2 Web Configuration

1. Configure LLDP, as shown in Figure 195.



LLDP Configuration

LLDP Parameters

Tx Interval	30	seconds
Tx Hold	4	times
Tx Delay	2	seconds
Tx Reinit	10	seconds

LLDP Interface Configuration

			Optional TLVs				
Interface	Mode	CDP aware	Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>	□	☑	☑	☑	☑	☑
FastEthernet 1/1	Disabled	□	☑	☑	☑	☑	☑
FastEthernet 1/2	Enabled	□	☑	☑	☑	☑	☑
FastEthernet 1/3	Enabled	□	☑	☑	☑	☑	☑
FastEthernet 1/4	Enabled	□	☑	☑	☑	☑	☑
FastEthernet 1/5	Enabled	□	☑	☑	☑	☑	☑
FastEthernet 1/6	Enabled	□	☑	☑	☑	☑	☑
GigabitEthernet 1/7	Enabled	□	☑	☑	☑	☑	☑
GigabitEthernet 1/8	Enabled	□	☑	☑	☑	☑	☑
GigabitEthernet 1/9	Enabled	□	☑	☑	☑	☑	☑

Note: The port 9 is internal port，contracting with gateway.

Figure 195 Configure LLDP

Tx Interval

Range: 5~32768s

Default: 30s

Function: Configutr the time interval for sending LLDP packets.

Tx Hold

Range: 2~10 times

Default: 4 times

Function: Set the number of Tx holding times. Effective duration of an LLDP packet = Tx Interval x Tx Hold.

Tx Delay

Range: 1~8192s

Default: 2s

Function: Set the transmission interval between a new LLDP packet and the previous LLDP packet after configuration information is changed. The value of Tx Delay cannot be larger than 1/4 of the value of Tx Interval.

Tx Reinit

Range: 1~10s

Default: 2s

Function: After LLDP is disabled on a port or a switch is restarted, the switch sends an LLDP shutdown frame to a neighboring node to announce that the previous LLDP packet is invalid. Tx Reinit refers to the interval between transmission of the LLDP shutdown frame and re-initialization of an LLDP packet.

Mode

Options: Enabled/Disabled/Rx only/Tx only

Default: Enabled

Function: Set the LLDP packet mode. The enabled mode indicates that the switch can send LLDP packets, and receive and identify LLDP packets; the disabled mode indicates that the switch neither sends LLDP packets nor receives LLDP packets; the only Rx mode indicates that the switch only receives and identifies LLDP packets; the only Tx mode indicates that the switch only sends LLDP packets.

CDP aware

Options: enable / disable

Default: disable

Function: When enabled, you can collect adjacent device information.

Port Descr

Options: Enabled/Disabled

Default: Enabled

Function: Enable indicates LLDP packets will carry port description.

Sys Name

Options: Enabled/Disabled

Default: Enabled

Function: Enable indicates LLDP packets will carry system name.

Sys Descr

Options: Enabled/Disabled

Default: Enabled

Function: Enable indicates LLDP packets will carry system description.

Sys Capa

Options: Enabled/Disabled

Default: Enabled

Function: Enable indicates LLDP packets will carry system capability.

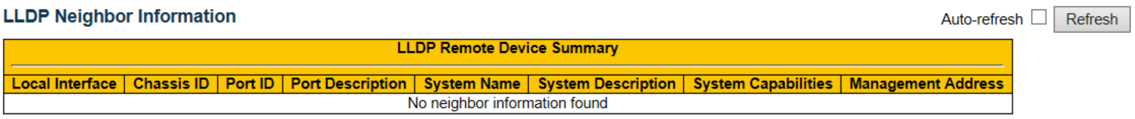
Mgmt Addr

Options: Enabled/Disabled

Default: Enabled

Function: Enable indicates LLDP packets will carry management address.

2. View LLDP connection information, as shown in Figure 196.



LLDP Neighbor Information

Auto-refresh □ Refresh

LLDP Remote Device Summary

Local Interface	Chassis ID	Port ID	Port Description	System Name	System Description	System Capabilities	Management Address
No neighbor information found							

Figure 196 LLDP Information

Caution:

To display LLDP information, LLDP must be enabled on the two connected devices.

3.16 MAC Table

3.16.1 Introduction

When forwarding a packet, the switch searches for the forwarding port in the MAC address table based on the destination MAC address of the packet.

A MAC address can be either static or dynamic.

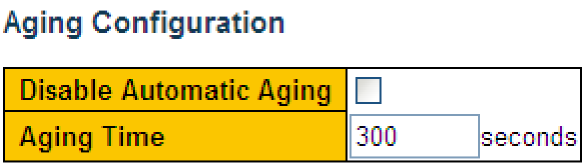
A static MAC address is configured by a user. It has the highest priority (not overridden by dynamic MAC addresses) and is permanently valid.

Dynamic MAC addresses are learned by the switch in data forwarding. They are valid only for a certain period. The switch periodically updates its MAC address table. When receiving a data frame to be forwarded, the switch learns the source MAC address of the frame, establishes a mapping with the receiving port, and queries the forwarding port in the MAC address table based on the destination MAC address of the frame. If a match is found, the switch forwards the data frame from the corresponding port. If no match is found, the switch broadcasts the frame in its broadcast domain.

Aging time starts from when a dynamic MAC address is added to the MAC address table. If no port receives a frame with the MAC address within one to two times the aging time, the switch deletes the entry of the MAC address from the dynamic forwarding address table. Static MAC addresses do not involve the concept of aging time.

3.16.2 Web Configuration

1. Configure MAC address aging time, as shown in Figure 197.



Aging Configuration

Disable Automatic Aging	□
Aging Time	300 seconds

Figure 197 MAC Address Aging Time Configuration

Disable Automatic Aging

Options: Enable/Disable

Default: Default

Function: Enable/Disable MAC address aging. Enable indicates you need to configure a aging time. Disable indicates the address dynamically learned does not age with time.

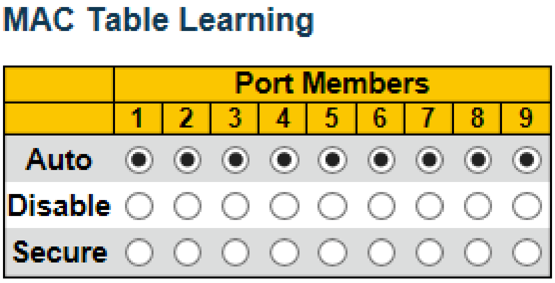
Aging Time

Range: 10~1000000s

Default: 300s

Function: Set the aging time for the dynamic MAC address entry.

2. Configure dynamic MAC address, as shown in Figure 198.



MAC Table Learning

	Port Members								
	1	2	3	4	5	6	7	8	9
Auto	●	●	●	●	●	●	●	●	●
Disable	○	○	○	○	○	○	○	○	○
Secure	○	○	○	○	○	○	○	○	○

Figure 198 Configure Dynamic MAC Address

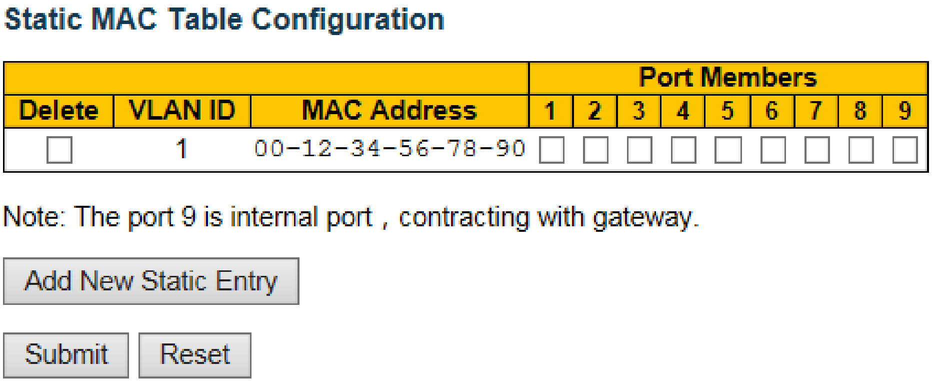
Port Members

Options: Auto/Disable

Default: Auto

Function: Whether a port dynamically learns an MAC address table. Auto indicates a port can dynamically learn the MAC address table. Disable indicates that a port is forbidden to dynamically learn the MAC address table.

3. Configure static MAC address, as shown in Figure 199.



Static MAC Table Configuration

			Port Members								
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9
□	1	00-12-34-56-78-90	□	□	□	□	□	□	□	□	□

Note: The port 9 is internal port , contracting with gateway.

Figure 199 Configure Static MAC Address

VLAN ID

Options: all created VLAN IDs

Default: VLAN 1

Function: Configuration the VLAN ID of static MAC address.

MAC address

Format: HH-HH-HH-HH-HH-HH (H is a hexadecimal number)

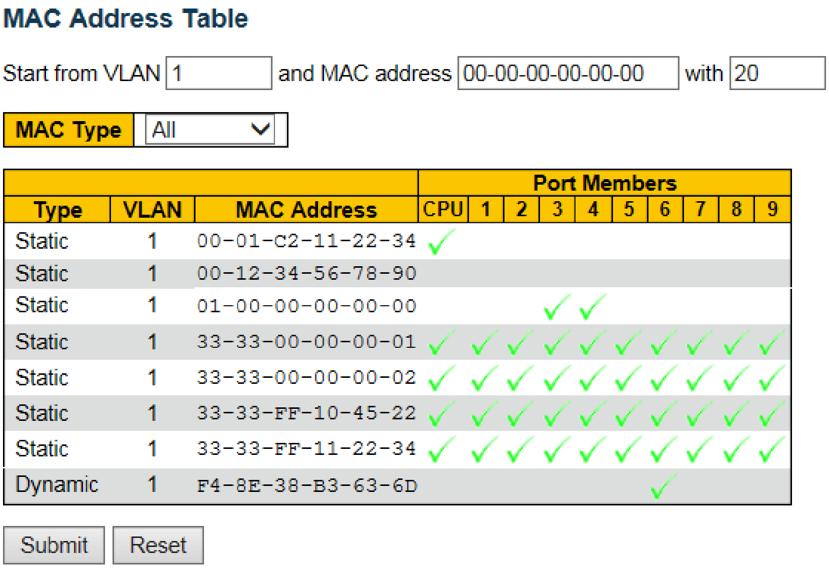
Function: Configure MAC address. For unicast MAC address, the lowest bit in the first byte is 0. For multicast MAC address, the lowest bit in the first byte is 1.

Port Members

Function: Select ports to forward the packets with this destination MAC address.

Click <Add New Static Entry> to configure static MAC address entry. A maximum of 64 static MAC address entries are supported.

4. View MAC address table, as shown in Figure 200.



Start from VLAN 1 and MAC address 00-00-00-00-00-00 with 20 entries per page.

MAC Type: All

			Port Members									
Type	VLAN	MAC Address	CPU	1	2	3	4	5	6	7	8	9
Static	1	00-01-C2-11-22-34	✓									
Static	1	00-12-34-56-78-90										
Static	1	01-00-00-00-00-00				✓	✓					
Static	1	33-33-00-00-00-01	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-00-00-00-02	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-FF-10-45-22	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-FF-11-22-34	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Dynamic	1	F4-8E-38-B3-63-6D							✓			

Figure 200 View MAC address table

3.17 VLAN

3.17.1 VLAN Configuration

3.17.1.1 Introduction

One LAN can be divided into multiple logical Virtual Local Area Networks (VLANs). A device can only communicate with the devices on the same VLAN. As a result, broadcast packets are restricted to a VLAN, optimizing LAN security.

VLAN partition is not restricted by physical location. Each VLAN is regarded as a logical network. If a host in one VLAN needs to send data packets to a host in another VLAN, a router or layer-3 device must be involved.

3.17.1.2 Principle

To enable network devices to distinguish packets from different VLANs, fields for identifying VLANs need to be added to packets. At present, the most commonly used protocol for VLAN identification is IEEE802.1Q. Table 6 shows the structure of an 802.1Q frame.

Table 6 802.1Q Frame Structure

DA	SA	802.1Q header				Length/type	Data	FCS
		TPID	PRI	CFI	VID			

A 4-byte 802.1Q header, as the VLAN tag, is added to the traditional Ethernet data frame.

TPID: 16 bits. It is used to identify a data frame carrying a VLAN tag. The value is 0x8100. The value of TPID specified in the 802.1Q protocol is 0x8100.

PRI: three bits, identifying the 802.1p priority of a packet.

CFI: 1 bit, specifies whether an MAC address is encapsulated in the standard format in different transmission media. The value 0 indicates that an MAC address is encapsulated in the standard format and the value 1 indicates that an MAC address is encapsulated in non-standard format.

VID: 12 bits, indicating the VLAN number. The value ranges from 1 to 4093. 0, 4094, and 4095 are reserved values.

Note：

- VLAN 1 is the default VLAN and cannot be manually created and deleted.
- Reserved VLANs are reserved to realize specific functions by the system and cannot be manually created and deleted.

The packet containing 802.1Q header is a tagged packet; the one without 802.1Q header is an untagged packet. All packets carry an 802.1Q tag in the switch.

3.17.1.3 Port-based VLAN

VLAN partition can be either port-based or MAC address-based. This series switches support port-based VLAN partition. VLAN members can be defined based on switch ports. After a port is added to a specified VLAN, the port can forward the packets with the tag for the VLAN.

1. Port Mode

Ports fall into three types according to how they handle VLAN tags when they forward packets.

Access: In access mode, the port can be added to only one VLAN. By default, all switch ports are access ports and belong to VLAN1. Packets forwarded by an access port do not have VLAN tags. Access ports are usually used to connect to terminals that do not support 802.1Q.

Trunk：In trunk mode, the port can be added to many VLAN. When sending PVID packets, the Trunk port can be set whether to carry the tag. It carries the tag when sending other packets. Trunk ports are usually used to connect network transmission devices.

Hybrid：In hybrid mode, the port can be added to many VLAN. You can set the type of packets to be received by a Hybrid port and whether the tag is carried when the Hybrid port sends packets. The Hybrid port can be used to connect network devices and user devices. The difference between a Hybrid port and a Trunk port is as follows: The Hybrid port does not carry the tag when sending packets from multiple VLANs and the Trunk port does not carry the tag only when sending PVID packets.

2. PVID

Each port has a PVID. When receiving an untagged packet, a port adds a tag to the packet according to the PVID. The default PVID of all ports is 1.

CAUTION

Caution:

- When configuring the PVID of a port, select one of the VLAN IDs allowed through the port; otherwise, the port may fail to forward packets.
- When the PVID tag is added to untagged packets, you can refer to PCP and DEI settings in Figure 64 for the default PRI and CFI values of a port.

Table 7 shows how the switch processes received and forwarded packets according to the port mode, and PVID.

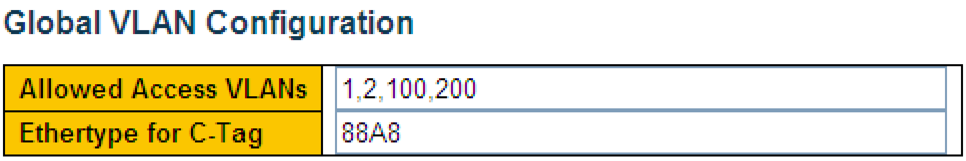
Table 7 Different Processing Modes for Packets

Processing Received Packets		Processing Packets to Be Forwarded	
Untagged packets	**Tagged packets**	**Port Mode**	**Packet Processing**
Add PVID tags to packets: ➢ If the PVID is in the list of VLANs allowed through, accept the packet. ➢ If the PVID is not in the list of VLANs allowed through, discard the packet.	➢ If the VLAN ID in a packet is in the list of VLANs allowed through, accept the packet. ➢ If the VLAN ID in a packet is not in the list of VLANs allowed through, discard the packet.	Access	Forward the packet after removing the tag.
		Trunk	Forward the packet according to the "Egress Tagging" configuration: ➢ Untag Port VLAN: If the VLAN ID in a packet is the same as PVID, and in the list of VLANs allowed through, forward the packet after removing the tag. If the VLAN ID in a packet is different from PVID, and in the list of VLANs allowed through, keep the tag and forward the packet. ➢ Tag All: If the VLAN ID in a packet is in the list of VLANs allowed through, keep the tag and forward the packet.
		Hybrid	Forward the packet according to the "Egress Tagging" configuration: ➢ Untag Port VLAN: the same as above. ➢ Tag All: the same as above. ➢ Untag All: If the VLAN ID in a packet is in the list of VLANs

			allowed through, forward the packet after removing the tag.

3.17.1.4 Web Configuration

1. Configure allowed VLANs for access port, as shown in Figure 201.



Global VLAN Configuration

Allowed Access VLANs	1,2,100,200
Ethertype for C-Tag	88A8

Figure 201 Configuring Allowed VLANs for a Access Port

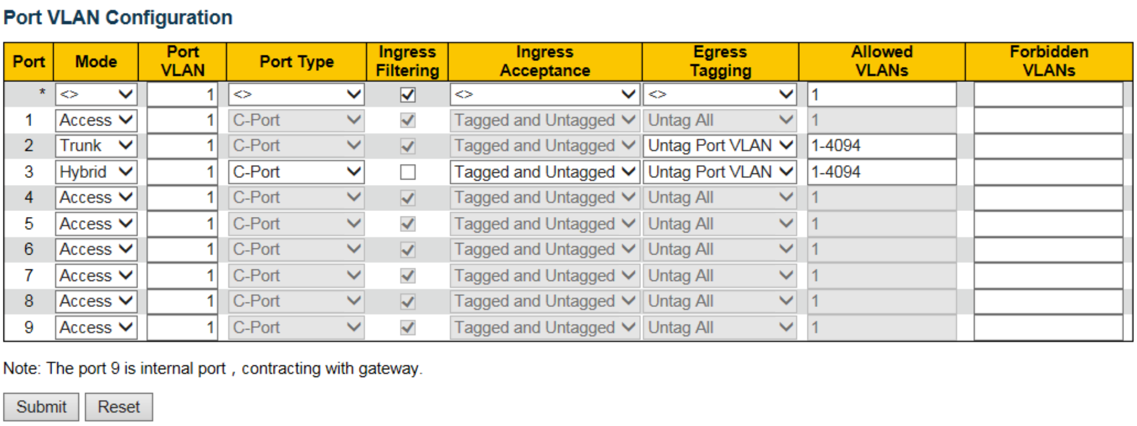
Allowed Access VLANs

Options: 1~4093

Default: 1

Function: Configure allowed VLANs for access port. When there are multiple VLANs, you can separate the VLANs by a comma (,) and an en dash (-), where an en dash is used to separate two consecutive VLAN IDs and a comma is used to separate two inconsecutive VLAN IDs.

2. Configure port VLAN, as shown in Figure 202.



Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
2	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-4094	
3	Hybrid	1	C-Port	☐	Tagged and Untagged	Untag Port VLAN	1-4094	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
7	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
8	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
9	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

Note: The port 9 is internal port，contracting with gateway.

Figure 202 Configure Port VLAN

Mode

Options: Access/Trunk/Hybrid

Default: Access

Function: Select the mode for the specified port. Each port supports only one mode.

Port VLAN（PVID）

Range: 1~4094

Default: 1

Function: Each port has a PVID. When receiving an untagged packet, a port adds a tag to the packet according to the PVID.

Caution:

- The PVID of the Access port should be selected from the list of VLANs allowed by the Access port. You can see the settings of Allowed Access VLANs in Figure 201.
- The PVID of a Trunk port or Hybrid port should be selected from the list of VLANs allowed by the port. See the settings of the following Allowed VLANs parameter.

Port type

Options: Unaware / C-Port / S-Port / S-Custom-Port

Default: C-Port

Functions: Access and trunk port types are mandatory for C-Port, can not be configured, and are used in industrial environments. Hybrid ports can be configured. S-PORT and S-CUSTOMER-PORT are generally used in the operator Ethernet, and the matching data is marked with the S-Tag.

Ingress Filtering

Options: Enable/Disable

Default: Disable

Function: Enable/Disable ingress filtering function of the hybrid port. The ingress filtering is enabled forcibly for access port and trunk port, you cannot configure the parameter. Enable: If the VLAN ID in a packet is not in the list of VLANs allowed through, discard the packet. Disable: If the VLAN ID in a packet is not in the list of VLANs allowed through, accept the packet and forward to MAC engine.

Ingress Acceptance

Options: Tagged and Untagged/ Tagged Only/ Untagged Only

Default: Tagged and Untagged

Function: Set the type of packets to be received by a Hybrid port. It is forcibly set to Tagged and Untagged for the Access port and Trunk port and cannot be modified. The value Tagged and Untagged indicates that the Hybrid port can receive tagged packets and untagged packets; the value Tagged Only indicates that the Hybrid port receives only tagged packets and discards untagged packets; the value Untagged Only indicates that the Hybrid port receives only untagged packets and discards tagged packets.

Egress Tagging

Options: Untag Port VLAN/ Unatg All/ Tag All

Default: Untag Port VLAN

Fucniton: Set the packet transmission processing for the Trunk port or Hybrid port. The egress tagging is configured to Unatg All forcibly for access port, you cannot configure the parameter. Untag Port VLAN: If the VLAN ID in a packet is the same as PVID, and in the list of VLANs allowed through, forward the packet after removing the tag. If the VLAN ID in a packet is different from PVID, and in the list of VLANs allowed through, keep the tag and forward the packet. Tag All: If the VLAN ID in a packet is in the list of VLANs allowed through, keep the tag and forward the packet. Untag All: If the VLAN ID in a packet is in the list of VLANs allowed through, forward the packet after removing the tag.

Allowed VLANs

Range: 1-4094

Range: 1-4094

Function: Configure allowed VLANs for trunk/hybrid port. When the Access port allows only one VLAN, the value of this parameter is consistent with the value of Port VLAN and it cannot be changed. When this parameter is set to multiple VLANs, you can separate the VLANs by a comma (,) and an en dash (-), where an en dash is used to separate two consecutive VLAN IDs and a comma is used to separate two inconsecutive VLAN IDs.

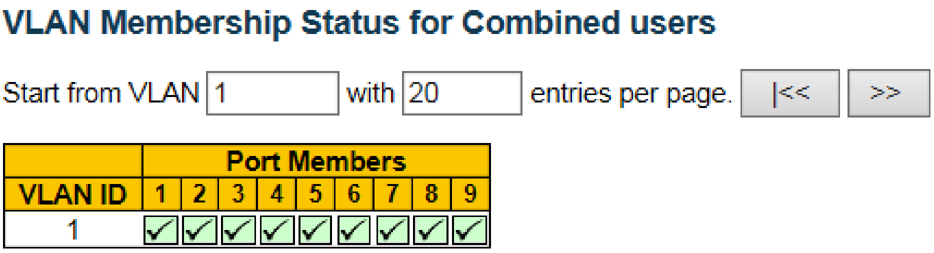
Forbidden VLANs

Range: 1-4094

Function: Configure forbidden VLANs for a port. After this parameter is set for a port, the port will never become a member port of the VLAN, including the dynamically registered VLAN

Through GVRP. When this parameter is set to multiple VLANs, you can separate the VLANs by a comma (,) and an en dash (-), where an en dash is used to separate two consecutive VLAN IDs and a comma is used to separate two inconsecutive VLAN IDs.

3. View all created VLANs and port members, as shown in Figure 203.



VLAN Membership Status for Combined users

Start from VLAN 1 with 20 entries per page.

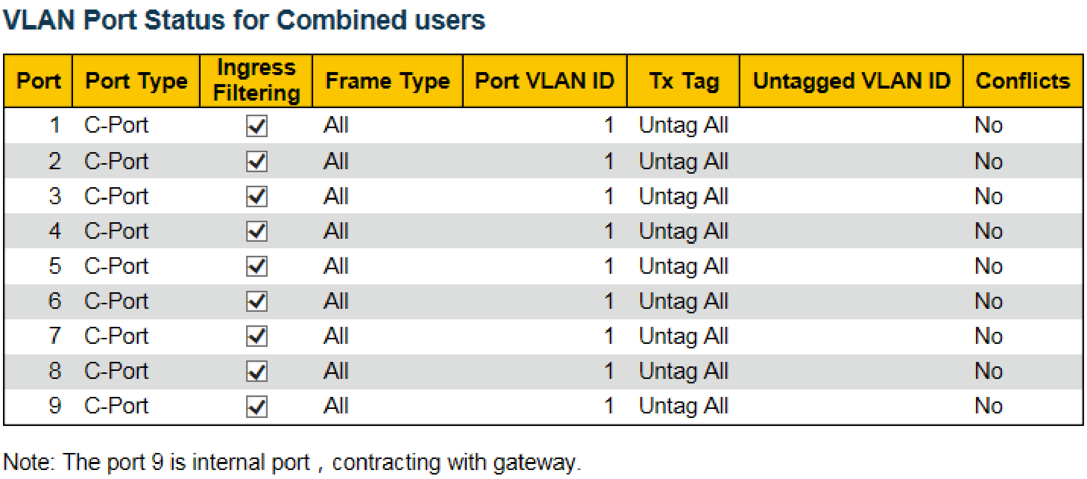
	Port Members								
VLAN ID	1	2	3	4	5	6	7	8	9
1	☑	☑	☑	☑	☑	☑	☑	☑	☑

Figure 203 View All Created VLANs and Port Members

☑ indicates that a port is a member port of the current VLAN; ☒ indicates that the current VLAN belongs to forbidden VLANs of a port.

1 to 99 VLAN entries can be displayed on each page and 20 VLAN entries are displayed by default. You can specify the first VLAN entry ID on the first page.

4. View port VLAN configuration, as shown in Figure 204.



VLAN Port Status for Combined users

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN ID	Tx Tag	Untagged VLAN ID	Conflicts
1	C-Port	☑	All	1	Untag All		No
2	C-Port	☑	All	1	Untag All		No
3	C-Port	☑	All	1	Untag All		No
4	C-Port	☑	All	1	Untag All		No
5	C-Port	☑	All	1	Untag All		No
6	C-Port	☑	All	1	Untag All		No
7	C-Port	☑	All	1	Untag All		No
8	C-Port	☑	All	1	Untag All		No
9	C-Port	☑	All	1	Untag All		No

Note: The port 9 is internal port , contracting with gateway.

Figure 204 View Port VLAN Configuration

3.17.1.5 Typical Configuration Example

As shown in Figure 205, the entire LAN is divided into 3 VLANs: VLAN2, VLAN100, and VLAN200. It is required that the devices in the same VLAN can communicate with each other, but different VLANs are isolated. The terminal PCs cannot distinguish tagged packets, so the ports connecting Switch A and Switch B with PCs are set to access port. VLAN2, VLAN100, and VLAN200 packets need to be transmitted between Switch A and Switch B, so the ports connecting Switch A and Switch B should be set to trunk port, permitting the packets of VLAN 2, VLAN 100, and VLAN 200 to pass through. Table 8 shows specific configuration.

Table 8 VLAN Configuration

VLAN	Configuration
VLAN2	Set port 1 and port 2 of Switch A and B to access ports, and port 7 to trunk port.
VLAN100	Set port 3 and port 4 of Switch A and B to access ports, and port 7 to trunk port.
VLAN200	Set port 5 and port 6 of Switch A and B to access ports, and port 7 to trunk port.

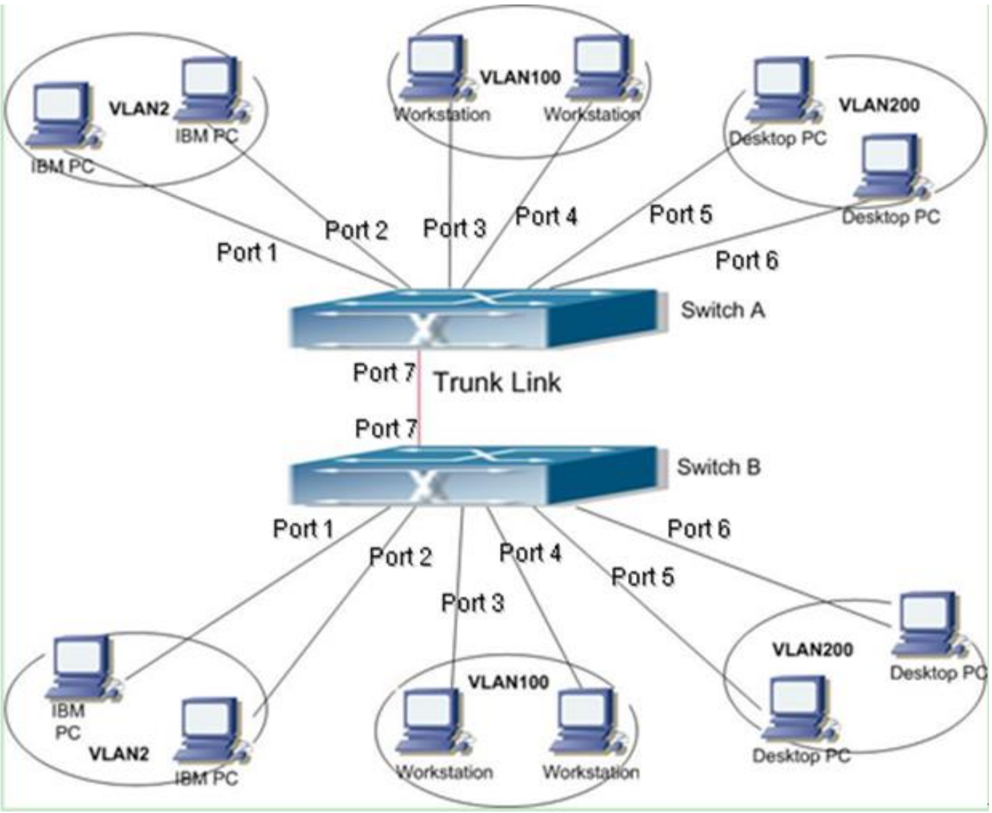


Figure 205 VLAN Application

Configurations on Switch A and Switch B:

1. Configure allowed access VLANs to 1,2,100,200, as shown in Figure 201.

2. Configure ports 1, 2 as access ports, port VLAN as 2. Configure ports 3, 4 as access ports, port VLAN as 100. Configure ports 5, 6 as access ports, port VLAN as 200. Configure port 7 as trunk port, port VLAN as 1, allowed VLANs as 1,2,100,200, as shown in Figure 202.

3. Keep all the other parameters default.

3.17.2 PVLAN Configuration

3.17.2.1 Introduction

PVLAN (Private VLAN) uses two layers isolation technologies to realize the complex port traffic isolation function, achieving network security and broadcast domain isolation.

The upper VLAN is a shared domain VLAN in which ports are uplink ports. The lower VLANs are isolation domains in which ports are downlink ports. Downlink ports can be assigned to different isolation domains and they can communicate with uplink port at the same time. Isolation domains cannot communicate to each other.

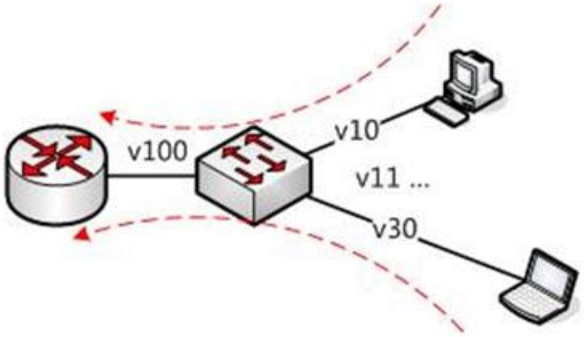


Figure 206 PVLAN Application

As shown in Figure 206, the shared domain is VLAN100 and the isolation domains are VLAN 10 and VLAN 30; the devices in the isolation domains can communicate with the device in the share domain, such as VLAN 10 can communicate with VLAN 100; VLAN 30 can also communicate with VLAN 100, but the devices in different isolation domains cannot communicate with each other, such as VLAN 10 cannot communicate with VLAN 30.

3.17.2.2 Explanation

PVLAN function can be implemented through special configuration on ports.

- The PVID of uplink ports are the same as shares domain VLAN ID; the PVID of downlink ports are the same as their own isolation domain VLAN ID.
- The uplink ports are set to hybrid and are assigned to the shares domain VLAN and all

isolation domains; the downlink ports are set to hybrid and are assigned to the shared domain VLAN and own isolation domain.

- The packets sent by PVLAN member ports are Untag.

3.17.2.3 Typical Configuration Example

Figure 207 shows PVLAN application. VLAN300 is a shared domain and port 1 and port 2 are uplink ports; VLAN100 and VLAN200 are isolation domains and ports 3, 4, 5, and 6 are downlink ports.

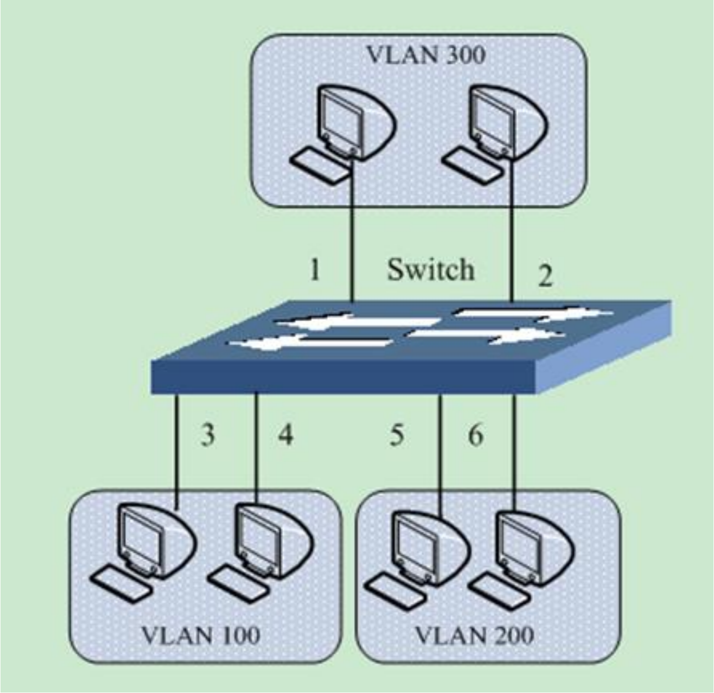


Figure 207 PVLAN Configuration Example

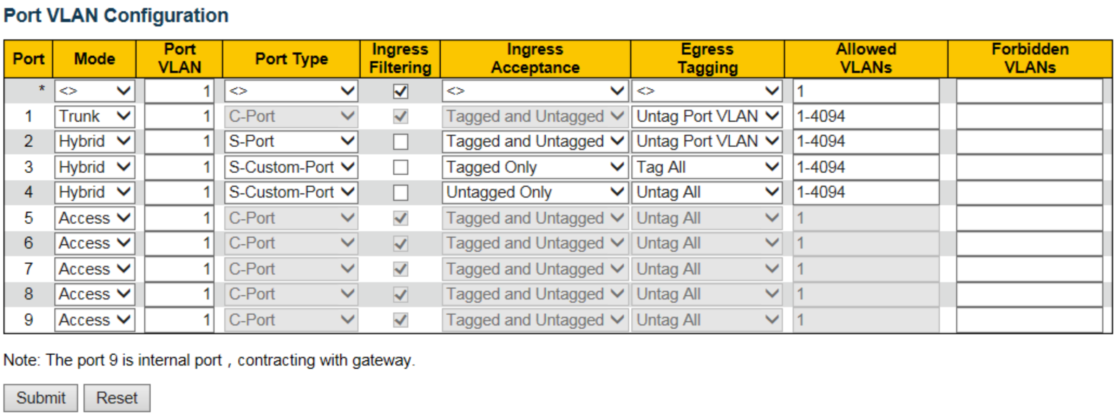
Switch configuration:

1. Configure ports 1, 2 to hybrid ports, port VLAN to 300, egress tagging to Untag All, allowed VLANs to 100,200,300.

2. Configure ports 3, 4 to hybrid ports, port VLAN to 100, egress tagging to Untag All, allowed VLANs to 100,300.

3. Configure ports 5, 6 to hybrid ports, port VLAN to 200, egress tagging to Untag All, allowed VLANs to 200,300, as shown in Figure 208.

4. Keep all the other parameters default.



Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-4094	
2	Hybrid	1	S-Port	□	Tagged and Untagged	Untag Port VLAN	1-4094	
3	Hybrid	1	S-Custom-Port	□	Tagged Only	Tag All	1-4094	
4	Hybrid	1	S-Custom-Port	□	Untagged Only	Untag All	1-4094	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
7	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
8	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
9	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

Note: The port 9 is internal port，contracting with gateway.

Figure 208 PVLAN Ports Configuration

3.17.3 GVRP

3.17.3.1 GARP Introduction

The Generic Attribute Registration Protocol (GARP) is used for spreading, registering, and cancelling certain information (VLAN, multicast address) among switches on the same network.

With GARP, the configuration information of a GARP member will spread the information to the entire switching network. A GARP member instructs the other GARP members to register or cancel its own configuration information by means of join/leave message respectively. The member also registers or cancels the configuration information of other members based on join/leave messages sent by other members.

GARP involves three types of messages: Join, Leave, and LeaveAll.

When a GARP application entity wants to register its own information on other switches, the entity sends a Join message. Join messages fall into two types: JoinEmpty and JoinIn. A JoinIn message is sent to declare a registered attribute, while a JoinEmpty message is sent to declare an attribute that is not registered yet.

When a GARP application entity wants to cancel its own information on other switches, the entity sends a Leave message.

After a GARP entity starts, it starts the LeaveAll timer. When the timer expires, the entity sends a LeaveAll message.

Note:

An application entity indicates a GARP-enabled port.

GARP timers include Hold timer, Join timer, Leave timer, LeaveAll timer.

Hold Timer: when a GARP-enabled switch receives a registration message, it starts s Hold timer rather than sending out the Join message immediately. When the Hold timer times out, it will put all registration information received during this time in a same Join message and send it out, reducing the message quantity for network stability.

Join Timer: in order to guarantee that the Join message can be reliably transmitted to other switches, the GARP-enabled switch will wait for a time interval of a Join timer after sending the first Join message. If the switch does not receive a Join In message during this time, it will send out a Join message again, otherwise, it won't send the second message.

Leave Timer: when a GARP-enabled switch wishes other switches to cancel its attribute information, it sends out a Leave message. Other GARP-enabled switches that receive this message will enable a Leave timer. If they do not receive a Join message until the timer times out, they will cancel this attribute information.

LeaveAll Timer: When a switch enables GARP, it starts a LeaveAll timer at the same time. When the timer times out, the switch will send a LeaveAll message to other GARP-Enabled switches and let them re-register their all attribute information, and then restart the LeaveAll timer to begin a new cycle.

3.17.3.2 GVRP Introduction

GVRP (GARP VLAN Registration Protocol) is a GARP application and is based on the GARP working mechanism to maintain the VLAN dynamic registration information of the device and propagate the information to other devices.

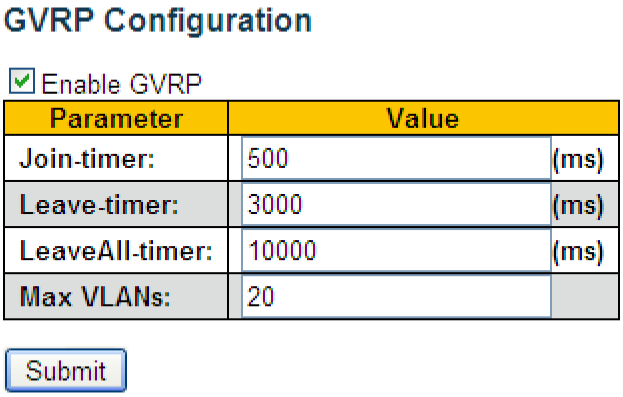
The GVRP-enabled device can receive VLAN registration information from other devices and dynamically update the local VLAN registration information, and the device can propagate the local VLAN registration information to other devices, reaching the consistency of VLAN information in all devices in the same LAN. The VLAN registration information propagated by GVRP contains not only the manually configured local static registration information, but also the dynamic registration information from other devices.

Caution:

GVRP port and port channel are mutually exclusive. The port in a port channel cannot be configured as a GVRP port; the GVRP port cannot be added to a port channel.

3.17.3.3 Web Configuration

1. Enable GVRP protocol and set the corresponding timers, as shown in Figure 209.



GVRP Configuration

☑ Enable GVRP

Parameter	Value	
Join-timer:	500	(ms)
Leave-timer:	3000	(ms)
LeaveAll-timer:	10000	(ms)
Max VLANs:	20	

Figure 209 GVRP Protocol Configuration

Enable GVRP

Options: Enable/Disable

Default: Disable

Function: Enable/Disable GVRP protocol.

Join-timer

Range: 100ms~327600ms

Default: 500ms

Function: Configure the join-timer value. The value must be a multiple of 100.

Leave-timer

Range: 100ms~327600ms

Default: 3000ms

Function: Configure the level-timer value. The value must be a multiple of 100.

LeaveAll-timer

Range: 100ms~327600ms

Default: 10000ms

Function: Configure the leave all-timer value. The value must be a multiple of 100.

Explanation: If LeaveAll timers of different devices time out at the same time, the devices will send out a LeaveAll message at the same time, which increases the message quantity. In order to avoid this, the actual running time of a LeaveAll timer is a random value and is longer than the time of one LeaveAll timer, and less than 1.5 times of a LeaveAll timer.

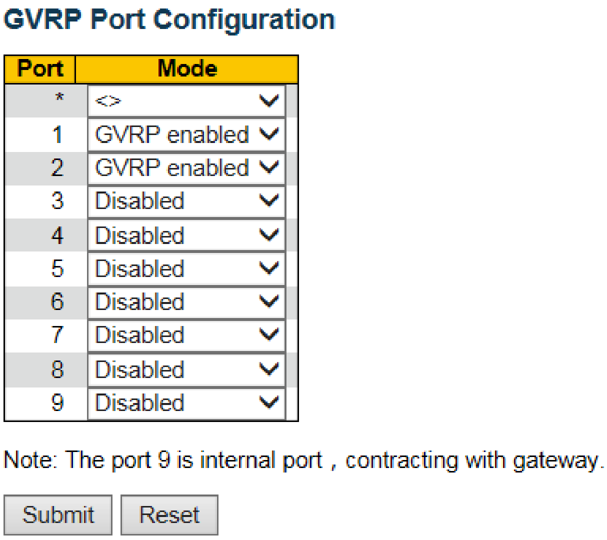
Max VLANs

Range: 1~4094

Default: 20

Function: Set the maximum number of VLANs that are dynamically registered with a GVRP port. The GVRP function needs to be disabled for the setting of this parameter.

2. Configure GVRP port, as shown in Figure 210.



GVRP Port Configuration

Port	Mode
*	<>
1	GVRP enabled
2	GVRP enabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled

Note: The port 9 is internal port , contracting with gateway.

Figure 210 GVRP Port Setting

Mode

Options: GVRP enabled/Disabled

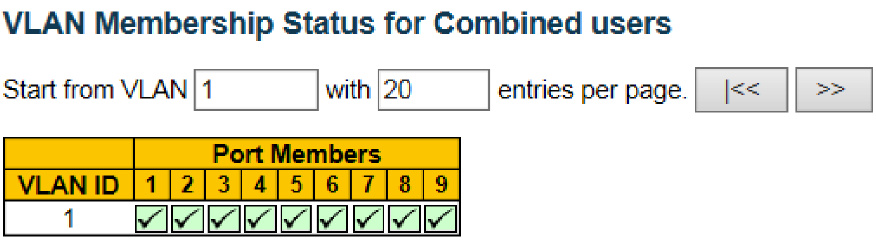
Default: Disabled

Function: Enable/Disable port GVRP function.

Caution:

- A GVRP port should be configured as a Trunk port.
- A GVRP port is used to transmit the VLAN attributes of other GVRP ports in the up state.

3. Show statically configured and dynamically registered VLAN information, as shown in Figure 211.



VLAN Membership Status for Combined users

Start from VLAN 1 with 20 entries per page. |<< >>

	Port Members								
VLAN ID	1	2	3	4	5	6	7	8	9
1	✓	✓	✓	✓	✓	✓	✓	✓	✓

Figure 211 VLAN Information

3.17.3.4 Typical Configuration Example

As Figure 212 shows, GVRP needs to be enabled on devices so that VLAN information is dynamically registered and updated between device A and device B.

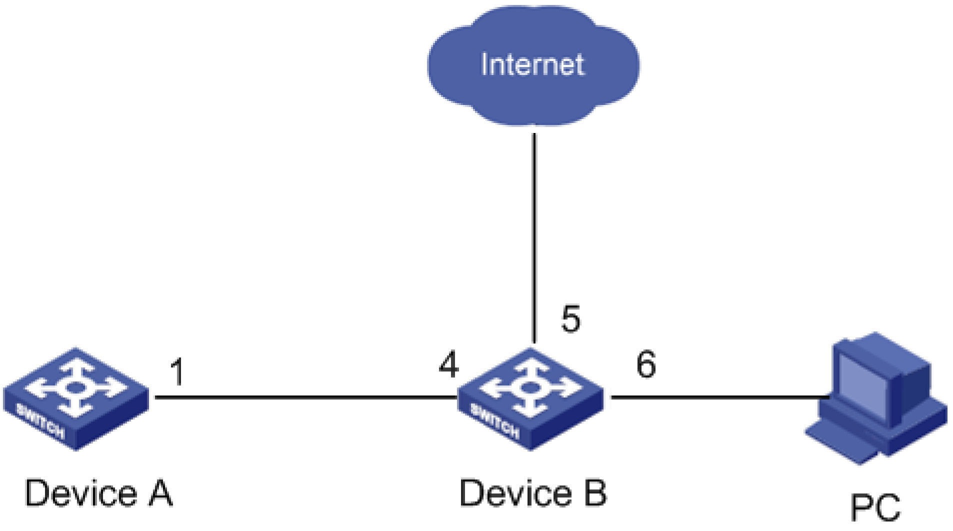


Figure 212 GVRP Configuration Example

Device A configuration are as follows:

1. Configure port 1 to trunk port, allowed VLANs to 1.

2. Enable global GVRP, as shown in Figure 209.

3. Enable GVRP on port 1, as shown in Figure 210.

Device B configuration are as follows:

1. Configure port 4 to trunk port, allowed VLANs to 1; configure port 5 to access port, allowed VLANs to 5; configure port 6 to trunk port, allowed VLANs to 1, 6.

2. Enable global GVRP, as shown in Figure 209.

3. Enable GVRP on port 4, 5, 6, as shown in Figure 210.

Port 1 of Switch A can register the same VLAN information as that of port 5 and 6 of Switch B, as shown in Figure 211.

3.18 Redundancy

3.18.1 DT-Ring

3.18.1.1 Introduction

DT-Ring and DT-Ring+ are Kyland-proprietary redundancy protocols. They enable a network to recover within 50ms when a link fails, ensuring stable and reliable communication.

DT rings fall into two types: port-based (DT-Ring-Port) and VLAN-based (DT-Ring-VLAN).

DT-Ring-Port: specifies a port to forward or block packets.

DT-Ring-VLAN: specifies a port to forward or block the packets of a specific VLAN. This allows multiple VLANs on a tangent port, that is, one port is part of different redundant rings based on different VLANs.

DT-Ring-Port and DT-Ring-VLAN cannot be used together.

3.18.1.2 Concepts

Master: One ring has only one master. The master sends DT-Ring protocol packets and detects the status of the ring. When the ring is closed, the two ring ports on the master are in forwarding and blocking state respectively.

Note：

The first port whose link status changes to up when the ring is closed is in forwarding state. The other ring port is in blocking state.

Slave: A ring can include multiple slaves. Slaves listen to and forward DT-Ring protocol packets and report fault information to the master.

Backup port: The port for communication between DT rings is called the backup port.

Master backup port: When a ring has multiple backup ports, the backup port with the larger MAC address is the master backup port. It is in forwarding state.

Slave backup port: When a ring has multiple backup ports, all the backup ports except the master backup port are slave backup ports. They are in blocking state.

Forwarding state: If a port is in forwarding state, the port can both receive and send data.

Blocking state: If a port is in blocking state, the port can receive and forward DT-Ring ring packets and can not forward other data packets.

3.18.1.3 Implementation

DT-Ring-Port Implementation

The forwarding port on the master periodically sends DT-Ring protocol packets to detect ring status. If the blocking port of the master receives the packets, the ring is closed; otherwise, the ring is open.

Working process of switch A, Switch B, Switch C, and Switch D:

1. Configure Switch A as the master and the other switches as slaves.

2. Ring port 1 on the master is in forwarding state while ring port 2 is in blocking state. Both two ports on the slave are in forwarding state.

3. If link CD is faulty, as shown in Figure 213.

a) When link CD is faulty, port 6 and port 7 on the slave are in blocking state. Port 2 on the master changes to forwarding state, ensuring normal link communication.

b) When the fault is rectified, port 6 and port 7 on the slave are in forwarding state. Port 2 on the master changes to blocking state. Link switchover occurs and links restore to the state before CD is faulty.

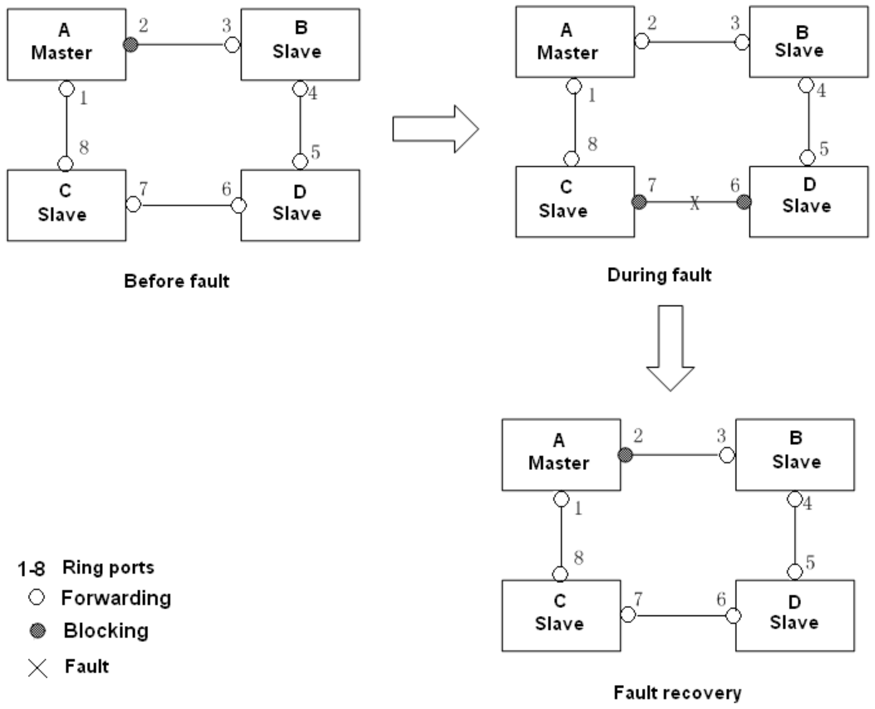


Figure 213 CD Link Fault

4. If link AC is faulty, as shown in Figure 214.

a) When link AC is faulty, port 1 is in blocking state and port 2 changes to forwarding state, ensuring normal link communication.

b) After the fault is rectified, port 1 is still in blocking state and port 8 is in forwarding state. No switchover occurs.

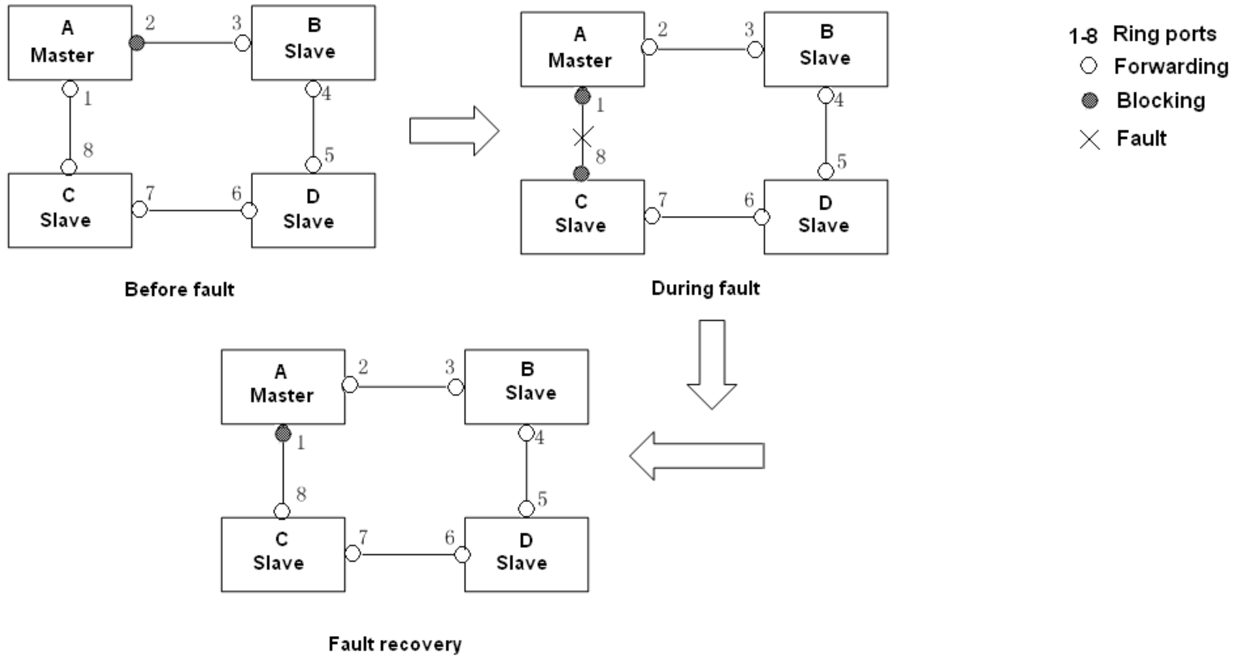


Figure 214 DT-Ring Link Fault

Caution:

Link status change affects the status of ring ports.

DT-Ring-VLAN Implementation

DT-Ring-VLAN allows the packets of different VLANs to be forwarded in different paths. Each forwarding path for a VLAN forms a DT-Ring-VLAN. Different DT-VLAN-Rings can have different masters. As shown in Figure 215, two DT-Ring-VLANs are configured.

Ring links of DT-Ring-VLAN 10: AB-BC-CD-DE-EA.

Ring links of DT-Ring-VLAN 20: FB-BC-CD-DE-EF.

The two rings are tangent at link BC, CD, and DE. Switch C and Switch D share the same ports in the two rings, but use different logical links based on VLANs.

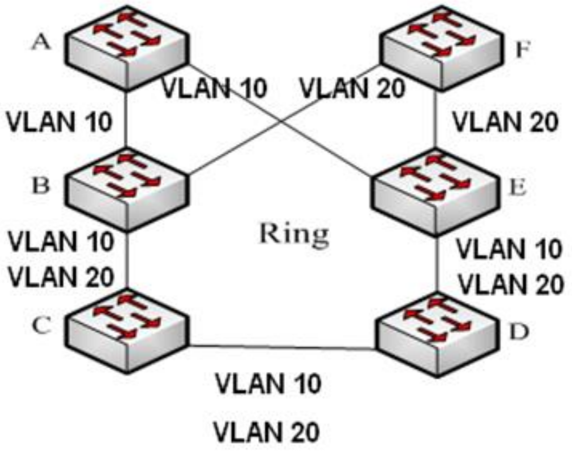


Figure 215 DT-Ring-VLAN

Note:

In each DT-Ring-VLAN logical ring, the implementation is identical with that of DT-Ring-Port.

DT-Ring+ Implementation

DT-Ring+ can provide backup for two DT rings, as shown in Figure 216. One backup port is configured respectively on Switch C and Switch D. Which port is the master backup port depends on the MAC addresses of the two ports. If the master backup port or its link fails, the slave backup port will forward packets, preventing loops and ensuring normal communication between redundant rings.

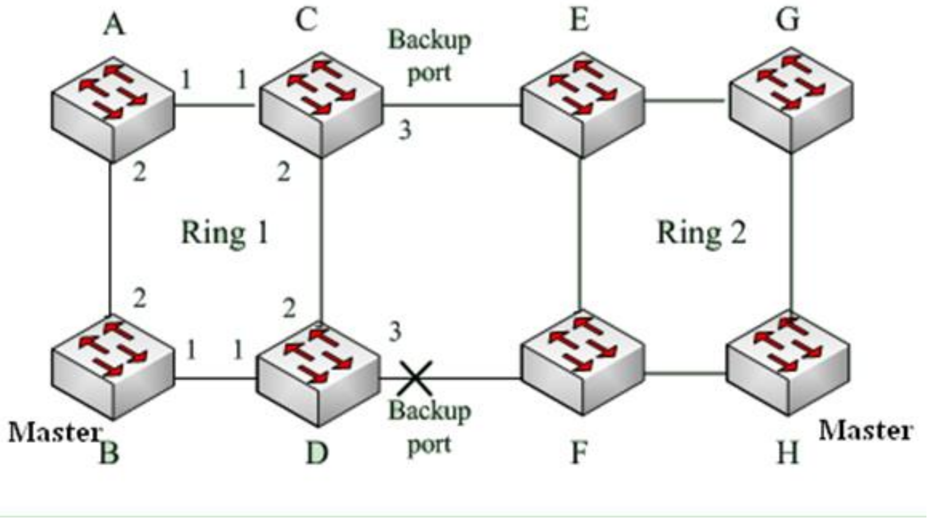


Figure 216 DT-Ring+ Topology

Caution:

Link status change affects the status of backup ports.

3.18.1.4 Explanation

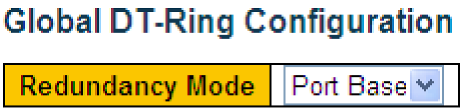
DT-Ring configurations should meet the following conditions:

- All switches in the same ring must have the same domain number.
- Each ring can only have one master and multiple slaves.
- Only two ports can be configured on each switch for a ring.
- For two connected rings, backup ports can be configured only in one ring.

- On a switch, only one backup port can be configured for one ring.
- DT-Ring-Port and DT-Ring-VLAN cannot be configured on one switch at the same time.

3.18.1.5 Web Configuration

1. Configure DT-Ring redundant ring mode, as shown in Figure 217.


Global DT-Ring Configuration

Redundancy Mode	Port Base

Figure 217 Redundant Ring Mode Configuration

Redundancy Mode

Options: Port Based/Vlan Based

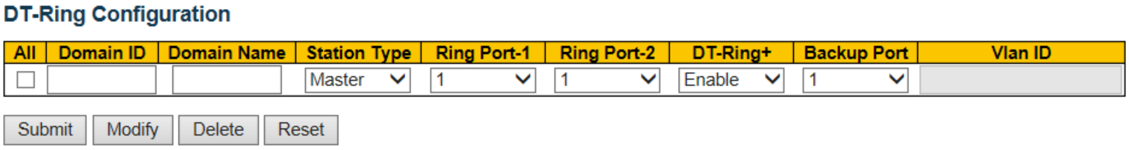
Default: Port Based

Function: Choose DT-Ring redundant ring mode.

Caution:

- Port-based ring protocols include RSTP, DT-Ring-Port, and DRP-Port, and VLAN-based ring protocols include MSTP, DT-Ring-VLAN, and DRP-VLAN.
- VLAN-based ring protocols are mutually exclusive, and only type of VLAN-based ring protocol can be configured for one device.
- Port-based ring protocol and VLAN-based ring protocol are mutually exclusive, and only one ring protocol mode can be selected for one device.

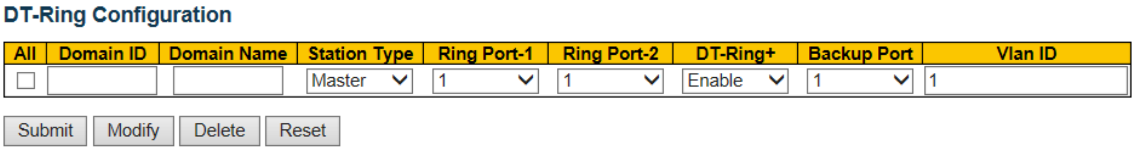
2. Configure DT-Ring-Port and DT-Ring-VLAN, as shown in Figure 218 and Figure 219.



DT-Ring Configuration

All	Domain ID	Domain Name	Station Type	Ring Port-1	Ring Port-2	DT-Ring+	Backup Port	Vlan ID
□			Master	1	1	Enable	1	

Figure 218 DT-Ring-Port Configuration



DT-Ring Configuration

All	Domain ID	Domain Name	Station Type	Ring Port-1	Ring Port-2	DT-Ring+	Backup Port	Vlan ID
□			Master	1	1	Enable	1	1

Figure 219 DT-Ring-VLAN Configuration

Domain ID

Range: 1~32

Function: The domain ID is used to distinguish different rings. One switch supports a maximum of 16 VLAN-based rings, the number of port-based rings depends on the number of switch ports.

Domain Name

Range: 1~31 characters

Function: Configure the domain name.

Station Type

Options: Master/Slave

Default: Master

Function: Select the switch role in a ring.

Ring Port-1/Ring Port-2

Options: all switch ports

Function: Select two ring ports.

CAUTION

Caution:

- DT-Ring ring port or backup port and port channel are mutually exclusive. A DT-Ring ring port or backup port cannot be added to a port channel; a port in a port channel cannot be configured as a DT-Ring ring port or backup port.
- Ring ports between port-based ring protocols RSTP, DT-Ring-Port, and DRP-Port are mutually exclusive, that is, the ring port and backup port of DT-Ring-Port cannot be configured as RSTP port, DRP-Port ring port, or DRP-Port backup port; RSTP port, DRP-Port ring port, and DRP-Port backup port cannot be configured as DT-Ring-Port ring port or backup port.
- It is recommended that you do not configure the ports in the isolation group as DT-Ring rings and backup ports. The DT-Ring ring port and the backup port do not join the isolation group at the same time.

DT-Ring+

Options: Enable/Disable

Default: Disable

Function: Enable/disable DT-Ring+.

Backup Port

Options: all switch ports

Function: Set a port to backup port.

Explanation: Enable DT-Ring+ before setting backup port.

CAUTION

Caution:

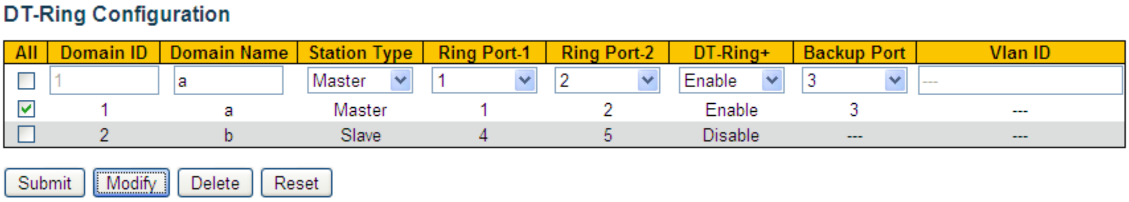
Do not configure a ring port as a backup port.

VLAN ID

Options: all created VLANs

Function: Select the VLANs for the ring port. When there are multiple VLANs, you can separate the VLANs by a comma (,) and an en dash (-), where an en dash is used to separate two consecutive VLAN IDs and a comma is used to separate two inconsecutive VLAN IDs.

3. View and modify DT-Ring configuration, as shown in Figure 220.



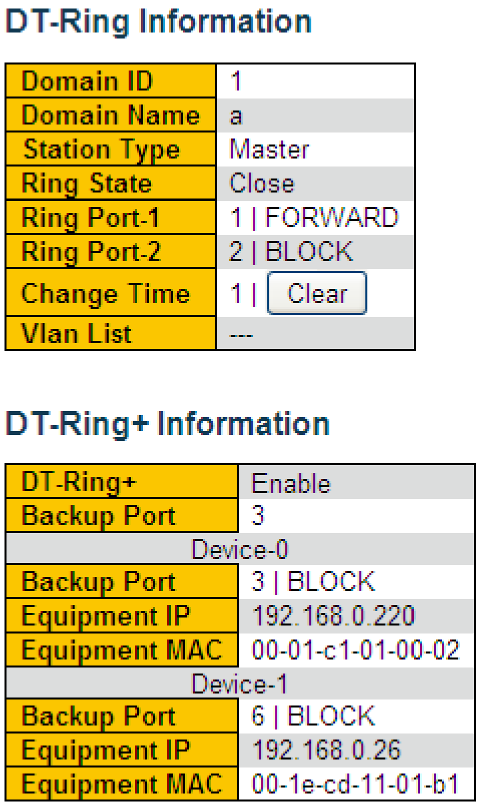
DT-Ring Configuration

All	Domain ID	Domain Name	Station Type	Ring Port-1	Ring Port-2	DT-Ring+	Backup Port	Vlan ID
□	1	a	Master	1	2	Enable	3	---
☑	1	a	Master	1	2	Enable	3	---
□	2	b	Slave	4	5	Disable	---	---

Figure 220 DT-Ring Configuration

Select a DT-Ring entry, click <Modify> to edit the DT-Ring entry configuration; click <Delete> to delete the designated DT-Ring entry.

4. Click a DT-Ring entry in Figure 220 to show DT-Ring and port status, as shown in Figure 221.



DT-Ring Information

Domain ID	1
Domain Name	a
Station Type	Master
Ring State	Close
Ring Port-1	1 | FORWARD
Ring Port-2	2 | BLOCK
Change Time	1 | Clear
Vlan List	---

DT-Ring+ Information

DT-Ring+	Enable
Backup Port	3
Device-0	
Backup Port	3 | BLOCK
Equipment IP	192.168.0.220
Equipment MAC	00-01-c1-01-00-02
Device-1	
Backup Port	6 | BLOCK
Equipment IP	192.168.0.26
Equipment MAC	00-1e-cd-11-01-b1

Figure 221 DT-Ring State

3.18.1.6 Typical Configuration Example

As shown in Figure 216, Switch A, B, C, and D form Ring 1; Switch E, F, G, and H form ring 2. Links CE and DF are the backup links between Ring 1 and Ring 2.

Configuration on Switch A:

1. Configure domain ID to 1, domain name to a, ring port to 1, 2, station type to slave, DT-Ring+ to disable, do not set backup port, as shown in Figure 218.

Configuration on Switch B:

2. Configure domain ID to 1, domain name to a, ring port to 1, 2, station type to master, DT-Ring+ to disable, do not set backup port, as shown in Figure 218;

Configuration on Switch C and Switch D:

3. Configure domain ID to 1, domain name to a, ring port to 1, 2, station type to slave, DT-Ring+ to enable, backup port to 3, as shown in Figure 218;

Configuration on Switch E, Switch F, and Switch G:

4. Configure domain ID to 2, domain name to b, ring port to 1, 2, station type to slave, DT-Ring+ to disable, do not set backup port, as shown in Figure 218;

Configuration on Switch H:

5. Configure domain ID to 2, domain name to b, ring port to 1, 2, station type to master, DT-Ring+ to disable, do not set backup port, as shown in Figure 218;

3.18.2 DRP

3.18.2.1 Overview

Kyland develops the Distributed Redundancy Protocol (DRP) for data transmission on ring-topology networks. It can prevent broadcast storms for ring networks. When a link or node is faulty, the backup link can take over services in real time to ensure continuous data transmission.

Compliant with the IEC 62439-6 standard, DRP uses the master election mechanism with no fixed master. DRP provides the following features:

- Network scale-independent recovery time

DRP achieves network scale-independent recovery time by optimizing the ring detection packet forwarding mechanism. DRP enables networks to recover within 20ms, with the introduction of real-time reporting interruption, improving reliability for real-time data transmission. This feature enables switches to provide higher reliability for the applications in the power, rail transit, and many other industries that require real-time control.

- Diversified link detection functions

To improve network stability, DRP provides diversified link detection functions for typical network faults, including fast disconnection detection, optical fiber unidirectional link detection, link quality inspection, and equipment health check, ensuring proper data transmission.

- Applicable to multiple network topologies

Besides rapid recovery for simple ring networks, DRP also supports complex ring topologies, such as intersecting rings and tangent rings. Additionally, DRP supports VLAN-based multiple instances, thereby suiting various network applications with flexible networking.

- Powerful diagnosis and maintenance functions

DRP provides powerful status query and alarm mechanisms for network diagnosis and maintenance, as well as mechanism for preventing unintended operation and incorrect configurations that may lead to ring network storms.

3.18.2.2 Concept

1. DRP Modes

DRP involves two modes: DRP-Port-Based and DRP-VLAN-Based.

DRP-Port-Based: forwards or blocks packets based on specific ports.

DRP-VLAN-Based: forwards or blocks packets based on VLANs. If a port is in blocking state, only the data packets of the specified VLAN are blocked. Therefore, multiple VLANs can be configured on tangent ring ports. A port can belong to different DRP rings according to VLAN configurations.

2. DRP Port Statuses

Forwarding state: If a port is in forwarding state, it can receive and forward data packets.

Blocking state: If a port is in blocking state, it can receive forward DRP packets and can not forward other data packets Primary port: indicates the ring port (on the root) whose status is configured as forwarding forcibly by user when the ring is closed.

Caution:

- If no primary port is configured on the root, the first port whose link status changes to up when the ring is closed is in forwarding state. The other ring port is in blocking state.
- A port in blocking state on the Root can proactively send DRP packets.

3. DRP Roles

DRP determines the roles of switches by forwarding Announce packets, preventing redundancy rings to form loops.

INIT: indicates the device on which DRP is enabled and the two ring ports are in Link down state.

Root: indicates the device on which DRP is enabled and at least one ring port is in Link up state. In a ring, the Root is elected according to the vectors of Announce packets. It may change with the network topology. The Root sends its own Announce packets to other devices periodically. Statuses of ring ports: One ring port is in forwarding state and the other is in blocking state. Upon receiving the Announce packet of another device, the Root compares the vector of the packet with that of its own Announce packet. If the vector of the received packet is larger, the Root changes its role to Normal or B-Root according to the link status and CRC degradation of ports.

B-Root: indicates the device on which DRP is enabled, meeting at least one of the following conditions: one ring port is in Link up state while the other is in Link down, CRC degradation, the priority is not less than 200. The B-Root compares and forwards Announce packets. If the vector of a received Announce packet is smaller than that of its own announce packet, the B-Root changes its role to Root; otherwise, it forwards the received packet and does not change its own role. Statuses of ring ports: One ring port is in forwarding state.

Normal: indicates the device on which DRP is enabled and both ring ports are in Link up state without CRC degradation and the priority is more than 200. The Normal only forwards

Announce packets, but does not check the content of packets. Statuses of ring ports: Both ring ports are in forwarding state.

Note:

CRC degradation: indicates that the number of CRC packets exceed the threshold in 15 minutes.

3.18.2.3 Implementation

Each switch maintains its own vector of Announce packet. The switch with the larger vector will be elected as the Root.

The vector of Announce packet contains the following information for role assignment.

Table 9 Vector of Announce Packet

Link status	CRC degradation		Role priority	IP address of the device	MAC address of the device
	CRC degradation status	CRC degradation rate			

Link status: The value is set to 1 if one ring port is in Link down state and set to 0 if both ring ports are in Link up state.

CRC degradation status: If CRC degradation occurs on one port, the value is set to 1. If CRC degradation does not occur on the two ring ports, the value is set to 0.

CRC degradation rate: The ratio of the number of CRC packets and the threshold in 15 minutes.

Role priority: The value can be set on the Web UI.

The parameters in Table 9 are compared in the following procedure:

1. The value of link status is checked first. The device with a larger link status value is considered to have a larger vector.
2. If the two compared devices have the same link status value, the values of CRC degradation status are compared. The device with a larger CRC degradation status value is considered to have a larger vector. If the CRC degradation status value of all compared devices is 1, the device with a larger CRC degradation rate value is considered to have a larger vector.
3. If the two compared devices have the same link status value and CRC degradation value,

the values of role priority, IP addresses, and MAC addresses are compared sequentially. The device with a larger value is considered to have a larger vector.

4. The device with the larger vector is elected as the Root.

Note:

Only when CRC degradation status value is 1, the CRC degradation rate value participates in vector comparison. Otherwise, the vectors are compared regardless of CRC degradation rate value.

➢ Implementation of DRP-Port-Based mode

The roles of switches are as follows:

1. Upon startup, all switches are in INIT state. When the state of one port changes to Link up, the switch becomes the Root and sends Announce packets to the other switches in the ring for election.

2. The switch with the largest vector of Announce packet is elected as the Root. The ring port that links up first on the Root is in forwarding state and the other ring port is in blocking state. Among the other switches in the ring, the switch with one ring port in Link down or CRC degradation state is the B-Root. The switch with both ring ports in Link up state and no CRC degradation is the Normal.

The fault recovery procedure is shown in Figure 222:

1. In the initial topology, A is the Root; port 1 is in forwarding state and port 2 in blocking state. B, C, and D are Normal(s), and their ring ports are in forwarding state.

2. When link CD is faulty, DRP changes the statuses of port 6 and port 7 to blocking. As a result, C and D become the Roots. Because A, C, and D are Roots at the moment, they all send Announce packets. The vectors of C and D are larger than that of A because port 7 and port 6 are in Link down status. In this case, if the vector of D is larger than that of C, D is elected as the Root and C becomes the B-Root. When receiving the Announce packet of D, A finds that the vector of D is larger than its own vector and both its ring ports are in Link up state. Therefore, A becomes a Normal and changes the status of port 2 to forwarding.

3. When link CD recovers, D is still the Root because its vector is larger than the vector of C.

- If no primary port is configured on D, port 7 is still in blocking state and port 8 is in forwarding state.
- If port 7 on D is configured as primary port, port 7 changes to forwarding state and port 8 is in blocking state.

DRP changes the state of port 6 to forwarding. As a result, C becomes a Normal. Therefore, the roles of switches do not change for link recovery.

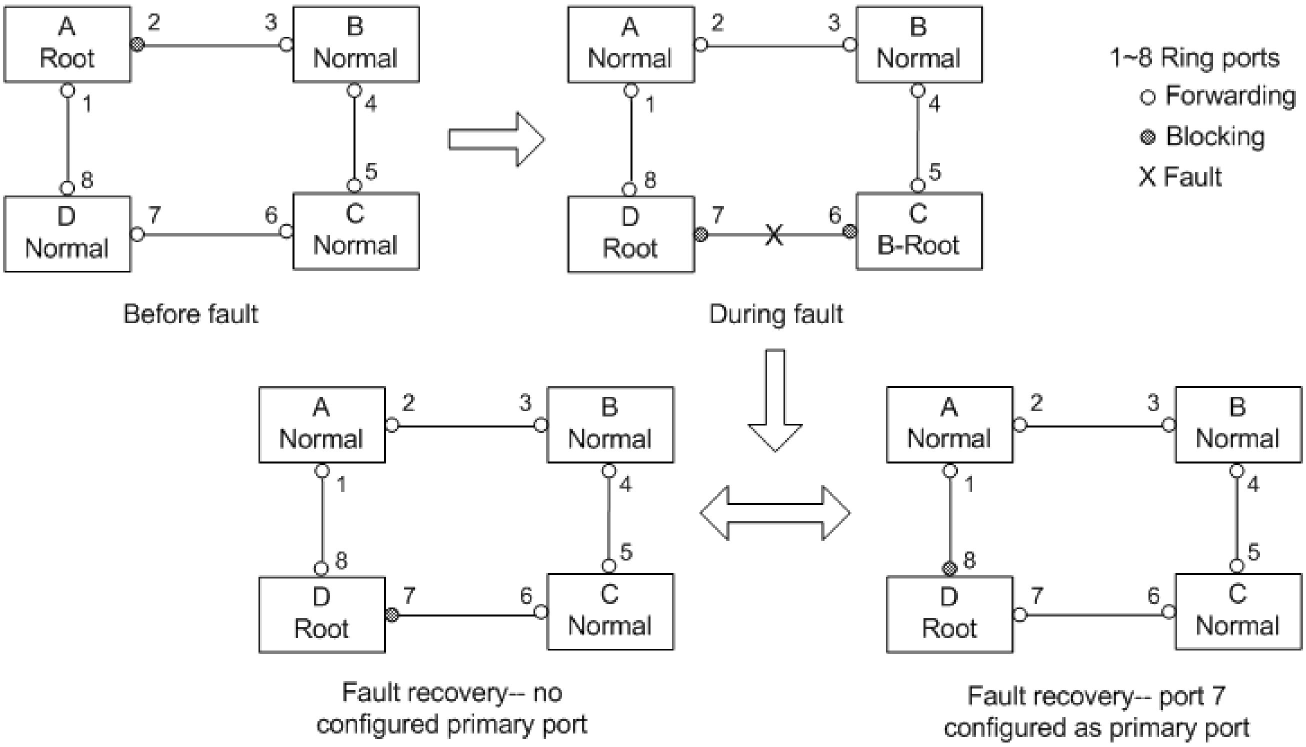


Figure 222 DRP Link Fault

Note:

On a DRP ring network, the roles of switches change upon a link fault, but do not change when the link recovers. This mechanism improves network security and reliability of data transmission.

- Implementation of DRP-VLAN-Based mode

DRP-VLAN-Based ring allows the packets of different VLANs to be forwarded in different paths. Each forwarding path for a VLAN forms a DRP-VLAN-Based. Different DRP-VLAN-Based ring can have different roots. As shown in the following figure, two DRP-VLAN-Based rings are configured.

Ring links of DRP-VLAN10/20-Based: AB-BC-CD-DE-EA.

Ring links of DRP-VLAN30-Based: FB-BC-CD-DE-EF.

The two rings are tangent at link BC, CD, and DE. Switch C and Switch D share the same ports in the two rings, but use different logical links based on VLANs

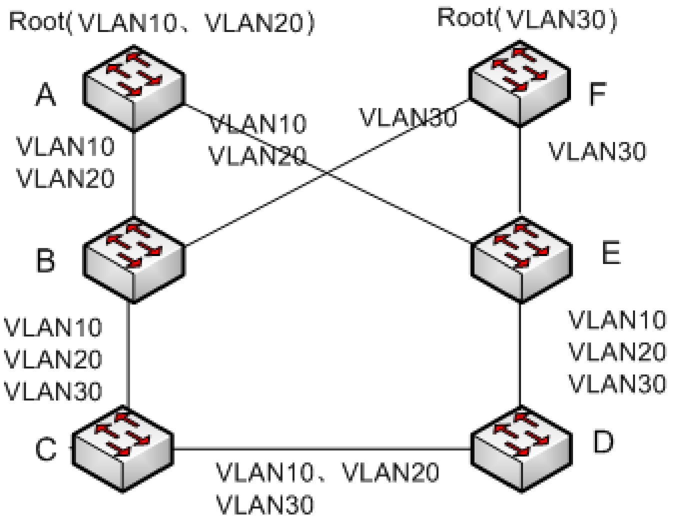


Figure 223 DRP-VLAN-Based

Note:

The port status and role assignment of each DRP-VLAN-Based ring are the same as those of DRP-Port-Based ring.

- DRP Backup

DRP can also provide backup for two DRP rings, preventing loops and ensuring normal communication between rings.

Backup port: indicates the communication port between DRP rings. Multiple backup ports can be configured, but must be in the same ring. The first backup port that links up is the master backup port, which is in forwarding state. All the other backup ports are slave. They are in blocking state.

As shown in Figure 224, one backup port can be configured on each switch. The master backup port is in forwarding state and the other backup ports are in blocking state. If the master backup port or its link is faulty, a slave backup port will be selected to forward data.

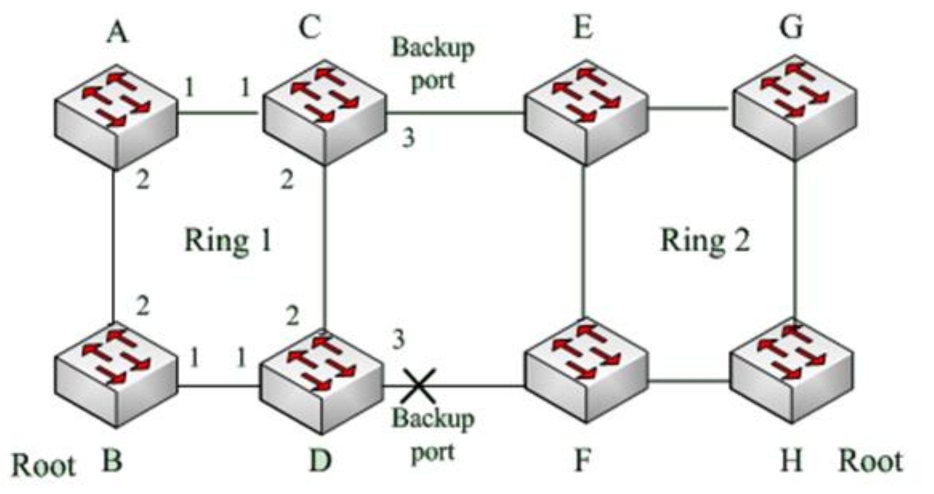


Figure 224 DRP Backup

Caution:

Link status change affects the status of backup ports.

3.18.3 DHP

3.18.3.1 Overview

As shown in Figure 225, A, B, C, and D are mounted to a ring. Dual Homing Protocol (DHP) achieves the following functions if it is enabled on A, B, C, and D:

- A, B, C, and D can communicate with each other, without affecting the proper running of devices in the ring.
- If the link between A and B is faulty, A can still communicate with B, C, and D by way of Device 1 and Device 2.

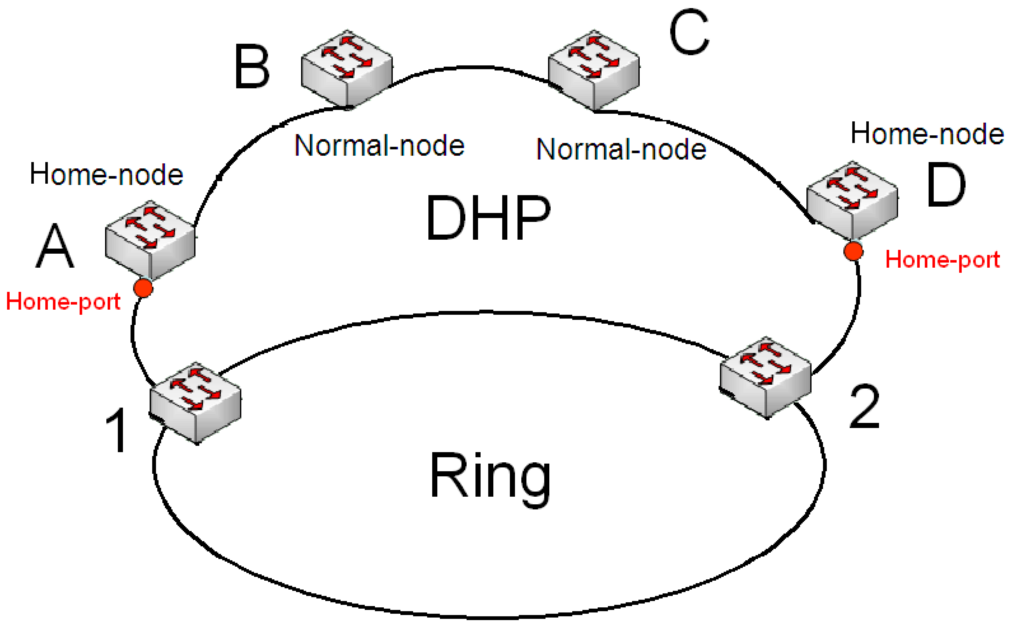


Figure 225 DHP Application

3.18.3.2 Concepts

The implementation of DHP is based on DRP. The role election and assignment mechanism of DHP is the same as that of DRP. DHP provides link backup through the configuration of Home-node, Normal-node, and Home-port.

Home-node: indicates the devices at both ends of the DHP link and terminates DRP packets.

Home-port: indicates the port connecting a Home node to the external network. A Home-port provides the following functions:

- Sending response packets to the Root upon receiving Announce packets from the Root. The Root identifies the ring status as closed if it receives response packets. If the Root does not receive response packets, it identifies the ring status as open.
- Blocking the DRP packets of external networks and isolating the DHP link from external networks.
- Sending entry clearing packets to connected devices on external networks upon a topology change of the DHP link.

Normal-node: indicates the devices in the DHP link, excluding the devices at both ends. Normal-nodes transmit the response packets of Home-nodes.

3.18.3.3 Implementation

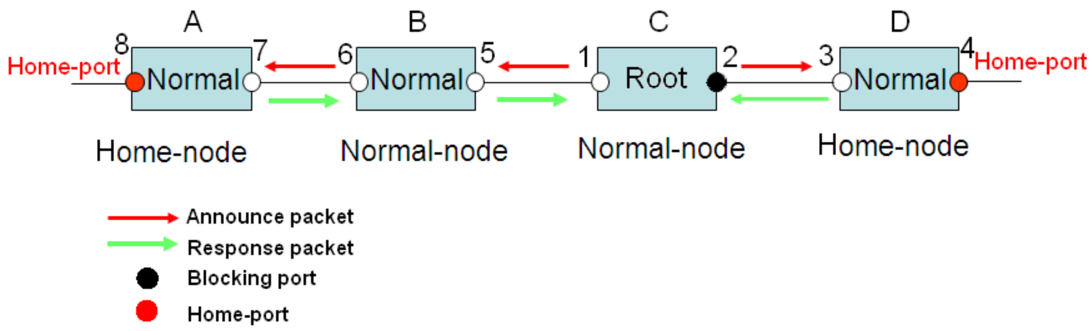


Figure 226 DHP Configuration

As shown in Figure 225, the configurations of A, B, C, and D in Figure 226 are as follows:

- DRP configuration: C is the Root; port 2 is in blocking state; A, B, and D are Normal; all the other ring ports are in forwarding state.
- DHP configuration: A and D are Home-nodes; port 8 and port 4 are Home-ports; B and C are Normal-nodes.

Implementation:

1. C, the Root, sends Announce packets through its two ring ports. Home-port 8 and Home-port 4 terminate the received Announce packets and send response packets to C. C identifies the ring status as closed. Port 2 is in blocking state.

2. When the link between A and B is blocked, the topology involves two links: A and B-C-D.

- A is elected as the Root. Port 7 is in blocking state.
- In link B-C-D, B is elected as the Root. Port 6 is in blocking state. C becomes the Normal. Port 2 is forwarding state. A can communicate with B, C, and D by way of Device 1 and Device 2, as shown in Figure 227.

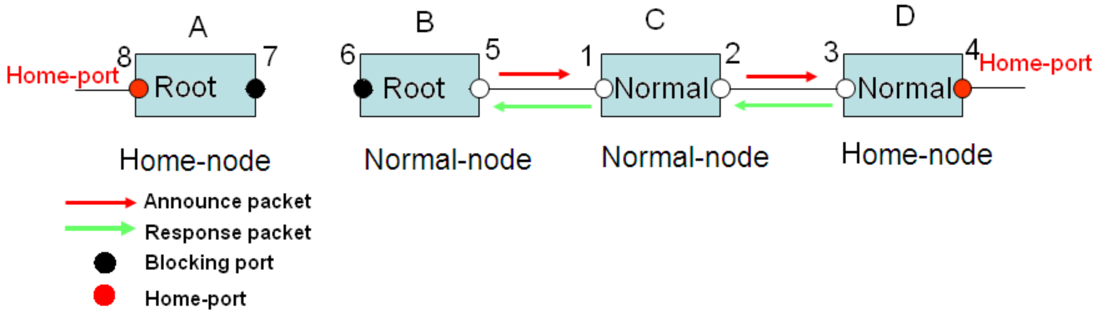


Figure 227 DHP Fault Recovery

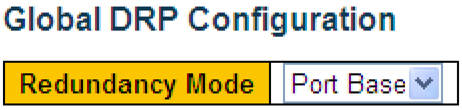
3.18.3.4 Description

DRP configurations meet the following requirements:

- All switches in the same ring must have the same domain number.
- One ring contains only one Root, but can contain multiple B-Roots or Normal(s).
- Only two ports can be configured on each switch for a ring.
- For two connected rings, backup ports can be configured only in one ring.
- Multiple backup ports can be configured in one ring.
- On a switch, only one backup port can be configured for one ring.

3.18.3.5 Web Configuration

1. Configure the DRP redundancy mode, as shown in Figure 228.



Global DRP Configuration

Redundancy Mode	Port Base

Figure 228 Configure the DRP Redundancy Mode

Redundancy Mode

Options: Port Based/Vlan Based

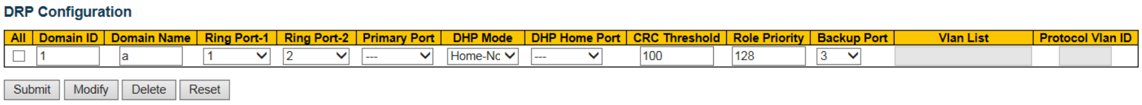
Default: Port Based

Function: Configure the DRP redundancy mode.

Caution:

- Port-based ring protocols include RSTP, DT-Ring-Port, and DRP-Port, and VLAN-based ring protocols include MSTP, DT-Ring-VLAN, and DRP-VLAN.
- VLAN-based ring protocols are mutually exclusive, and only type of VLAN-based ring protocol can be configured for one device.
- Port-based ring protocol and VLAN-based ring protocol are mutually exclusive, and only one ring protocol mode can be selected for one device.

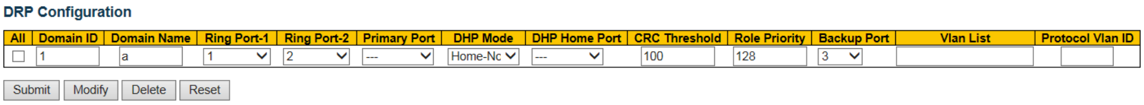
2. Configure DRP-Port-Based and DRP-VLAN-Based, as shown in Figure 229 and Figure 230.



DRP Configuration

All	Domain ID	Domain Name	Ring Port-1	Ring Port-2	Primary Port	DHP Mode	DHP Home Port	CRC Threshold	Role Priority	Backup Port	Vlan List	Protocol Vlan ID
□	1	a	1	2	---	Home-Nc	---	100	128	3		

Figure 229 DRP-Port-Based Configuration



DRP Configuration

All	Domain ID	Domain Name	Ring Port-1	Ring Port-2	Primary Port	DHP Mode	DHP Home Port	CRC Threshold	Role Priority	Backup Port	Vlan List	Protocol Vlan ID
□	1	a	1	2	---	Home-Nc	---	100	128	3		

Figure 230 DRP-VLAN-Based Configuration

Domain ID

Range: 1~32

Function: Each ring has a unique domain ID. One switch supports a maximum of 8 VLAN-based rings, the number of port-based rings depends on the number of switch ports.

Domain Name

Range: 1~31 characters

Function: Configure the domain name.

Ring Port-1/Ring Port-2

Options: all switch ports

Function: Select two ring ports.

Caution:

- DRP ring port or backup port and port channel are mutually exclusive. A DRP ring port or backup port cannot be added to a port channel; a port in a port channel cannot be configured as a DRP ring port or backup port.
- Ring ports between port-based ring protocols RSTP, DT-Ring-Port, and DRP-Port are mutually exclusive, that is, the ring port and backup port of DRP-Port cannot be configured as RSTP port, DT-Ring-Port ring port, or DT-Ring-Port backup port; RSTP port, DT-Ring-Port ring port, and DT-Ring-Port backup port cannot be configured as DRP-Port ring port or backup port.
- It is recommended that you do not configure the ports in the isolation group as DRP ring ports and backup ports. The DRP ring port and the backup port do not join the isolation group at the same time.

Primary Port

Options: ---/Ring Port-1/Ring Port-2

Default: ---

Function: Configure the primary port. When the ring is closed, the primary port on root is in forwarding state.

DHP Mode

Options: Disable/Normal-Node/Home-Node

Default: Disable

Function: Disable DHP or configure the DHP mode.

DHP Home Port

Options: ---/Ring-Port-1/Ring-Port-2/Ring-Port-1-2

Function: Configure the Home-port for a DHP Home-node.

Description: If there is only one device in DHP link, the both ring ports of the Home-node must be configured as the Home-port.

CRC Threshold

Range: 25~65535

Default: 100

Function: Configure the CRC threshold.

Description: This parameter is used in root election. The system counts the number of received CRCs. If the number of CRCs of one ring port exceeds the threshold, the system considers the port to have CRC degradation. As a result, the CRC degradation value is set to 1 in the vector of the Announce packet of the port.

Role Priority

Range: 0~255

Default: 128

Function: Configure the priority of a switch.

Backup Port

Options: all switch ports

Function: Configure the backup port.

Caution:

Do not configure a ring port as a backup port.

VLAN List

Options: All created VLANs

Function: Select the VLANs managed by current DRP-VLAN-Based ring.

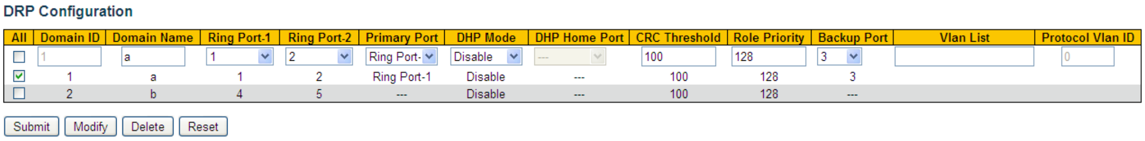
Protocol Vlan ID

Range: 1~4093

Description: The VLAN ID must be one of service VLAN.

Function: DRP packets with the VLAN ID serve as the basis for the diagnosis and maintenance of the DRP-VLAN-Based ring.

3. View and modify DRP configuration, as shown in Figure 231.



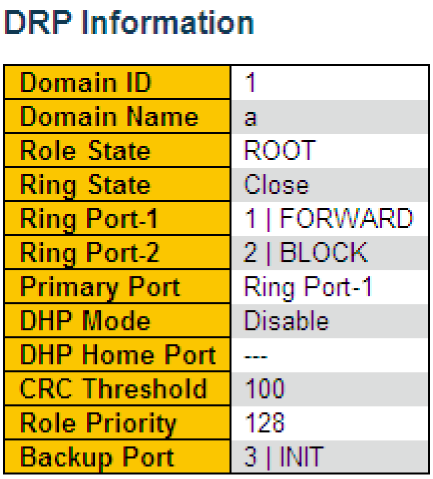
DRP Configuration

All	Domain ID	Domain Name	Ring Port-1	Ring Port-2	Primary Port	DHP Mode	DHP Home Port	CRC Threshold	Role Priority	Backup Port	Vlan List	Protocol Vlan ID
□	1	a	1	2	Ring Port-	Disable	---	100	128	3		0
☑	1	a	1	2	Ring Port-1	Disable	---	100	128	3		
□	2	b	4	5	---	Disable	---	100	128	---		

Figure 231 View and Modify DRP Configuration

Select a DRP entry, click <Modify> to edit the DRP entry configuration; click <Delete> to delete the designated DRP entry.

4. Click a DRP entry in Figure 231 to show DRP and port status, as shown in Figure 232.



DRP Information

Domain ID	1
Domain Name	a
Role State	ROOT
Ring State	Close
Ring Port-1	1 | FORWARD
Ring Port-2	2 | BLOCK
Primary Port	Ring Port-1
DHP Mode	Disable
DHP Home Port	---
CRC Threshold	100
Role Priority	128
Backup Port	3 | INIT

Figure 232 DRP State

3.18.3.6 Typical Configuration Example

As shown in Figure 224, A, B, C, and D form Ring 1; E, F, G, and H form Ring 2; CE and DF are the backup links of Ring 1 and Ring 2.

Configuration on switch A and switch B:

1. Set Domain ID to 1 and Domain name to a. Select ring port 1 and ring port 2. Keep default values for role priority and backup port, as shown in Figure 229.

Configuration on switch C and switch D:

2. Set Domain ID to 1, Domain name to a, and Backup port to 3. Select ring port 1 and ring port 2. Keep the default value for role priority, as shown in Figure 229;

Configuration on switch E, F, G, and H:

3. Set Domain ID to 2 and Domain name to b. Select ring port 1 and ring port 2. Keep default values for role priority and backup port, as shown in Figure 229.

3.18.4 RSTP/STP

3.18.4.1 Introduction

Standardized in IEEE802.1D, the Spanning Tree Protocol (STP) is a LAN protocol used for preventing broadcast storms caused by link loops and providing link backup. STP-enabled devices exchange packets and block certain ports to prune "loops" into "trees", preventing proliferation and endless loops. The drawback of STP is that a port must wait for twice the forwarding delay to transfer to the forwarding state.

To overcome the drawback, IEEE creates 802.1w standard to supplement 802.1D. IEEE802.1w defines the Rapid Spanning Tree Protocol (RSTP). Compared with STP, RSTP achieves much more rapid convergence by adding alternate port and backup port for the root port and designated port respectively. When the root port is invalid, the alternate port can enter the forwarding state quickly.

3.18.4.2 Concepts

Root bridge: serves as the root for a tree. A network has only one root bridge. The root bridge changes with network topology. The root bridge periodically sends BPDU to the other devices, which forward the BPDU to ensure topology stability.

Root port: indicates the best port for transmission from the non-root bridges to the root bridge. The best port is the port with the smallest cost to the root bridge. A non-root bridge communicates with the root bridge through the root port. A non-root bridge has only one root port. The root bridge has no root port.

Designated port: indicates the port for forwarding BPDU to other devices or LANs. All ports on the root bridge are designated ports.

Alternate port: indicates the backup port of the root port. If the root port fails, the alternate port becomes the new root port.

Backup port: indicates the backup port of the designated port. When a designated port fails, the backup port becomes the new designated port and forwards data.

3.18.4.3 BPDU

To prevent loops, all the bridges of a LAN calculate a spanning tree. The calculation process involves transmitting BPDUs among devices to determine the network topology. Table 10 shows the data structure of a BPDU.

Table 10 BPDU

…	Root bridge ID	Root path cost	Designated bridge ID	Designated port ID	Message age	Max age	Hello time	Forward delay	…
…	8 bytes	4 bytes	8 bytes	2 bytes	2 bytes	2 bytes	2 bytes	2 bytes	…

Root bridge ID: priority of the root bridge (2 bytes) +MAC address of the root bridge (6 bytes).

Root path cost: cost of the path to the root bridge.

Designated bridge ID: priority of the designated bridge (2 bytes) +MAC address of the designated bridge (6 bytes).

Designated port ID: port priority+port number.

Message age: duration that a BPDU can be spread in a network.

Max age: maximum duration that a BPDU can be saved on a device. When Message age is larger than Max age, the BPDU is discarded.

Hello time: interval for sending BPDUs.

Forward delay: status change delay (discarding--learning--forwarding).

3.18.4.4 Implementation

The process for all bridges calculating the spanning tree with BPDUs is as follows:

1. In the initial phase

Each port of all devices generates the BPDU with itself as the root bridge; both root bridge ID and designated bridge ID are the ID of the local device; the root path cost is 0; the designated port is the local port.

2. Best BPDU selection

All devices send their own BPDUs and receive BPDUs from other devices. Upon receiving a BPDU, each port compares the received BPDU with its own.

- If the priority of its own BPDU is higher, then the port does not perform any operation.
- If the priority of the received BPDU is higher, then the port replaces the local BPDU with the received one.

Devices compare the BPDUs of all ports and figure out the best BPDU. Principles for comparing BPDUs are as follows:

- The BPDU with a smaller root bridge ID has a higher priority.
- If the root bridge IDs of two BPDUs are the same, their root path costs are compared. If the root path cost in a BPDU plus the path cost of the local port is smaller, then the priority of the BPDU is higher.
- If the root path costs of two BPDUs are also the same, the designated bridge IDs, designated port IDs, and IDs of the port receiving the BPDUs are further compared in order. The BPDU with a smaller ID has a higher priority. The BPDU with a smaller root bridge ID has a higher priority.

3. Selection of the root bridge

The root bridge of the spanning tree is the bridge with the smallest bridge ID.

4. Selection of the root port

A non-root-bridge device selects the port receiving the best BPDU as the root port.

5. BPDU calculation of the designated port

Based on the BPDU of the root port and the path cost of the root port, a device calculates a designated port BPDU for each port as follows:

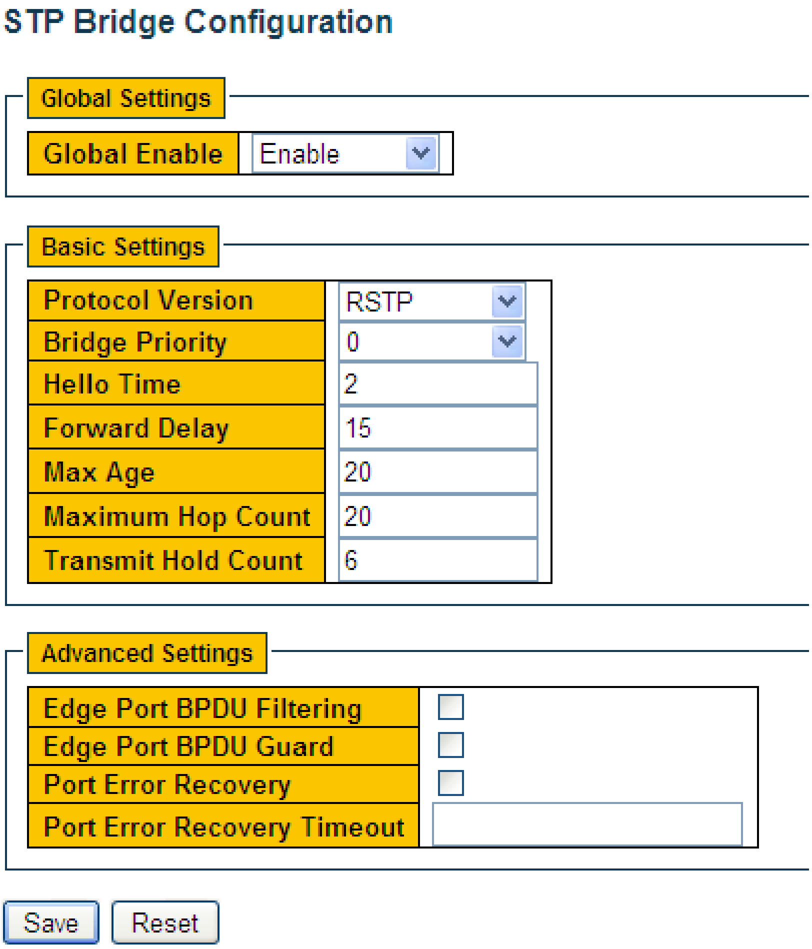
- Replace the root bridge ID with the root bridge ID of the BPDU of the root port.
- Replace the root path cost with the root path cost of the root port BPDU plus the path cost of the root port.
- Replace designated bridge ID with the ID of the local device.
- Replace the designated port ID with the ID of the local port.

6. Selection of the designated port

If the calculated BPDU is better, then the device selects the port as the designated port, replaces the port BPDU with the calculated BPDU, and sends the calculated BPDU. If the port BPDU is better, then the device does not update the port BPDU and blocks the port. Blocked ports can receive and forward only RSTP packets, but not other packets.

3.18.4.5 Web Configuration

1. Set the time parameters of the network bridge, as shown in Figure 233.



STP Bridge Configuration

Global Settings

Global Enable	Enable

Basic Settings

Protocol Version	RSTP
Bridge Priority	0
Hello Time	2
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

Advanced Settings

Edge Port BPDU Filtering	□
Edge Port BPDU Guard	□
Port Error Recovery	□
Port Error Recovery Timeout	

Figure 233 Setting Time Parameters of the Network Bridge

Global Enable

Options: Enable/Disable

Default: Disable

Function: Disable or enable spanning tree.

Caution:

- Port-based ring protocols include RSTP, DT-Ring-Port, and DRP-Port, and VLAN-based ring protocols include MSTP, DT-Ring-VLAN, and DRP-VLAN.
- Port-based ring protocol and VLAN-based ring protocol are mutually exclusive, and only one ring protocol mode can be selected for one device.

Protocol Priority

Options: MSTP/RSTP/STP

Default: MSTP

Function: Select the spanning tree protocol.

Brigde Priority

Range: 0~61440. The step is 4096.

Default: 32768

Function: Configure the priority of the network bridge.

Description: The priority is used for selecting the root bridge. The smaller the value, the higher the priority.

Hello Time

Range: 1~10s

Default: 2s

Function: Configure the interval for sending BPDU.

Forward Delay

Range: 4~30s

Default: 15s

Function: Configure status change time from Discarding to Learning or from Learning to Forwarding.

Max Age

Range: 6~40s

Default: 20s

Function: Maximum duration that a BPDU can be saved on a device.

Description: If the value of message age in the BPDU is larger than the specified value, then the BPDU is discarded.

CAUTION

Caution:

- ➢ The values of Forward Delay Time, Hello Time and Max Age Time should meet the following requirements: 2 * (Forward Delay Time–1.0 seconds) >= Max Age Time; Max Age Time >= 2 * (Hello Time + 1.0 seconds)**.**
- ➢ The default setting is recommended.

Transmit Hold Count

Range: 1~10

Default: 6

Function: Set the maximum number of BPDU packets that can be sent by a port within each Hello Time.

Edge Port BPDU Filtering

Options: Enable/Disable

Default: Disable

Function: Control whether an edge port receives and forwards BPDU packets.

Edge Port BPDU Guard

Options: Enable/Disable

Default: Disable

Function: Control whether an edge port enters the Error-Disable state and is shut down when receiving BPDU packets.

Port Error Recovery

Options: Enable/Disable

Default: Disable

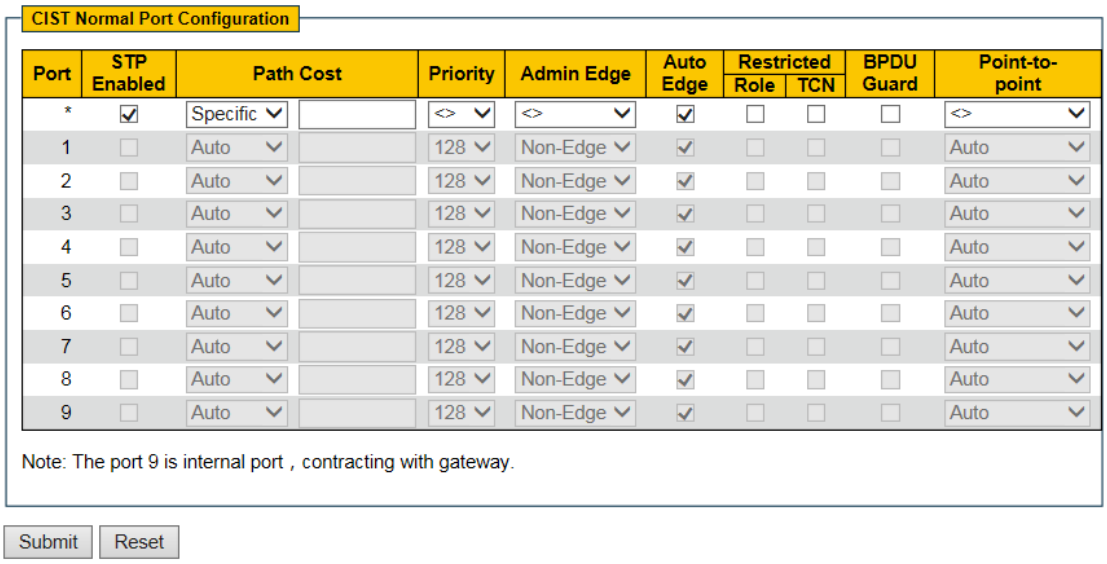
Function: Control whether a port can automatically recover from the error state to the normal state.

Port Error Recovery Timeout

Range: 30~86400s

Function: Set the time for a port to recover from the error state to the normal state.

2. Configure RSTP port, as shown in Figure 234.



CIST Normal Port Configuration

Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
							Role	TCN		
*	☑	Specific		<>	<>	☑	□	□	□	<>
1	□	Auto		128	Non-Edge	☑	□	□	□	Auto
2	□	Auto		128	Non-Edge	☑	□	□	□	Auto
3	□	Auto		128	Non-Edge	☑	□	□	□	Auto
4	□	Auto		128	Non-Edge	☑	□	□	□	Auto
5	□	Auto		128	Non-Edge	☑	□	□	□	Auto
6	□	Auto		128	Non-Edge	☑	□	□	□	Auto
7	□	Auto		128	Non-Edge	☑	□	□	□	Auto
8	□	Auto		128	Non-Edge	☑	□	□	□	Auto
9	□	Auto		128	Non-Edge	☑	□	□	□	Auto

Note: The port 9 is internal port，contracting with gateway.

Figure 234 Configure RSTP Port

STP Enabled

Options: Enable/Disable

Default: Disable

Function: Enable or disable STP/RSTP on ports.

Caution:

- RSTP port and port channel are mutually exclusive. A RSTP port cannot be added to a port channel; a port in a port channel cannot be configured as a RSTP port.
- Ring ports between port-based ring protocols RSTP, DT-Ring-Port, and DRP-Port are mutually exclusive, that is, a RSTP port cannot be configured as DRP-Port/DT-Ring-Port ring port, or DRP-Port/DT-Ring-Port backup port; DRP-Port/DT-Ring-Port ring port, and DRP-Port/DT-Ring-Port backup port cannot be configured as a RSTP port.
- It is recommended that you do not configure ports in the same isolation group as RSTP ports at the same time. RSTP ports do not join the same isolation group.

Path Cost

Options: Auto/Specific (1~200000000)

Default: Auto

Description: The path cost of a port is used to calculate the best path. The value of the parameter depends on the bandwidth. The larger the value, the lower the cost. You can change the role of a port by changing the value of the path cost parameter. To configure the value manually, select No for Cost Count.

Priority

Range: 0~240. The step is 16.

Default: 128

Function: Configure the port priority, which determines the roles of ports.

Admin Edge

Options: Non-Edge/Edge

Default: Non-Edge

Function: Set whether the current port is an edge port.

Description: When a port is directly connected to a terminal and is not connected to other devices or a shared network segment, the port is considered as an edge port. An edge port can rapidly migrate from the blocking state to the forwarding state without waiting delay. After an edge port receives BPDU packets, it becomes a non-edge port.

Auto Edge

Options: Enable/Disable

Default: Enable

Function: Specify whether to enable the automatic detection function of an edge port.

Restricted Role

Options: Enable/Disable

Default: Disable

Function: A restricted port will be never selected as a root node even if it is granted the highest priority.

Restricted TCN

Options: Enable/Disable

Default: Disable

Function: A port with restricted TCN will not actively send TCN messages.

BPDU Guard

Options: Enable/Disable

Default: Disable

Function: Control whether an edge port enters the Error-Disable state and is shut down when receiving BPDU packets.

Point-to-point

Options: Auto/Forced True/Forced False

Default: Auto

Function: Set the connection type for a port. If a port is connected to a point-to-point link, the port can rapidly migrate to another state.

Description: **Auto** indicates that the switch automatically detects the link type based on the duplex status of a port. When a port works in full-duplex mode, the switch considers that the type of the link connected to the port is point-to-point; when a port works in half-duplex mode, the switch considers that the type of the link connected to the port is shared. Forced point-to-point refers that a link connected to a port is a point-to-point link and forced sharing refers that a link connected to a port is a shared link.

3.18.4.6 Typical Configuration Example

The priorities of Switch A, B, and C are 0, 4096, and 8192. Path costs of links are 4, 5, and 10, as shown in Figure 235.

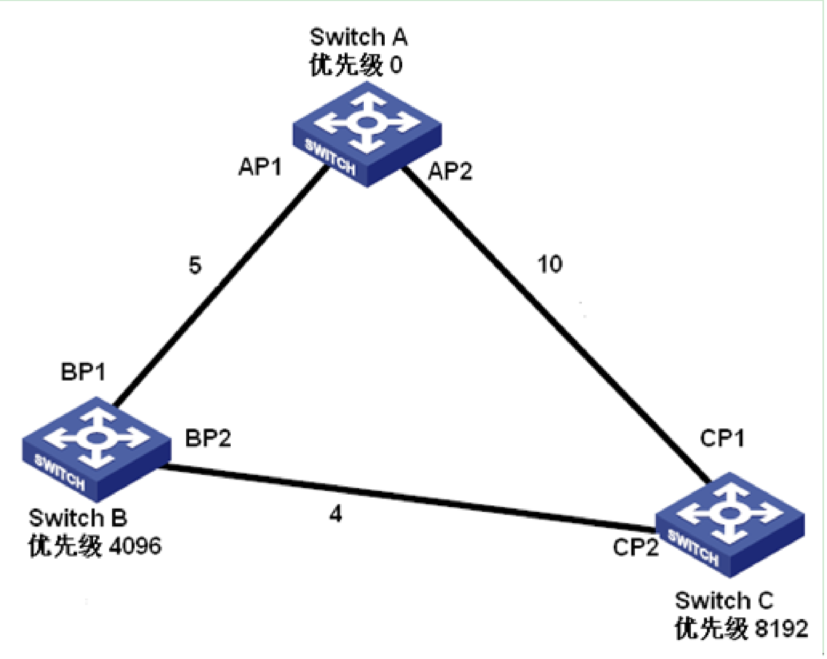


Figure 235 RSTP Configuration Example

Configuration on Switch A:

1. Set bridge priority to 0 and time parameters to default values, as shown in Figure 233.

2. Set the path cost of port 1 to 5 and that of port 2 to 10, as shown in Figure 234.

Configuration on Switch B:

1. Set bridge priority to 4096 and time parameters to default values, as shown in Figure 233**.**

2. Set the path cost of port 1 to 5 and that of port 2 to 4, as shown in Figure 234.

Configuration on Switch C:

1. Set bridge priority to 8192 and time parameters to default values, as shown in Figure 233.

2. Set the path cost of port 1 to 10 and that of port 2 to 4, as shown in Figure 234.

- The priority of Switch A is 0 and its root ID is the smallest. Therefore, Switch A is the root bridge.
- The path cost from AP1 to BP1 is 5 and that from AP2 to BP2 is 14. Therefore, BP1 is the root port.
- The path cost from AP1 to CP2 is 9 and that from AP2 to CP1 is 10. Therefore, CP2 is the root port and BP2 is the designated port.

3.18.5 MSTP Configuration

3.18.5.1 Introduction

Although RSTP achieves rapid convergence, it also has the following defect just as the STP: all bridges in the LAN share one spanning tree and packets of all VLANs are forwarded along the spanning tree. As shown in Figure 236, certain configurations may block the link between switch A and switch C. Because switch B and switch D are not in VLAN 1, they cannot forward the packets of VLAN 1. As a result, the VLAN 1 port of switch A cannot communicate with that of switch C.

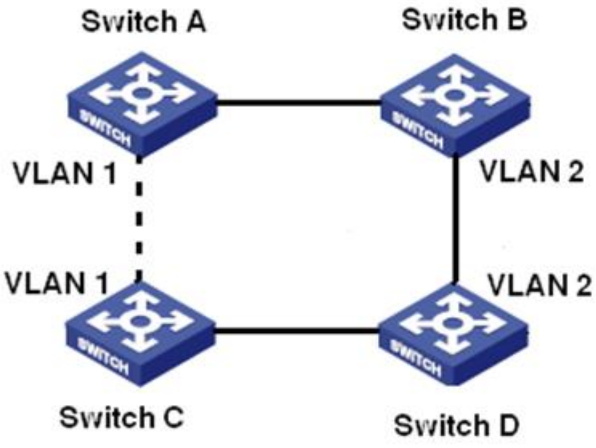


Figure 236 RSTP Disadvantage

To solve this problem, the Multiple Spanning Tree Protocol (MSTP) came into being. It achieves both rapid convergence and separate forwarding paths for the traffic of different VLANs, providing a better load sharing mechanism for redundant links.

MSTP maps one or multiple VLANs into one instance. Switches with the same configuration form a region. Each region contains multiple mutually independent spanning trees. The region serves as a switch node. It participates in the calculation with other regions based on the spanning tree algorithm, calculating an overall spanning tree. Based on this algorithm, the network in Figure 236 forms the topology shown in Figure 237. Both switch A and switch C are in Region1. No link is blocked because the region contains no loops. This is the same with Region2. Region1 and Region2 are similar to switch nodes. These two "switches" form a loop. Therefore, a link should be blocked.

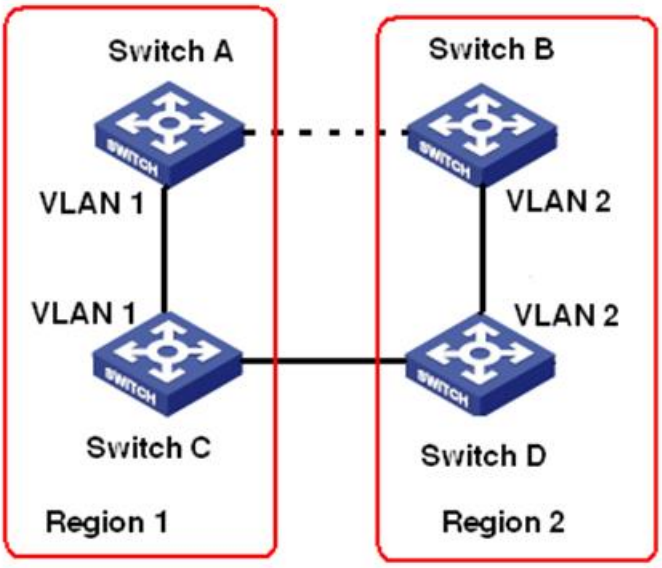


Figure 237 MSTP Topology

3.18.5.2 Basic Concepts

Learn MSTP concepts based on Figure 238 - Figure 241.

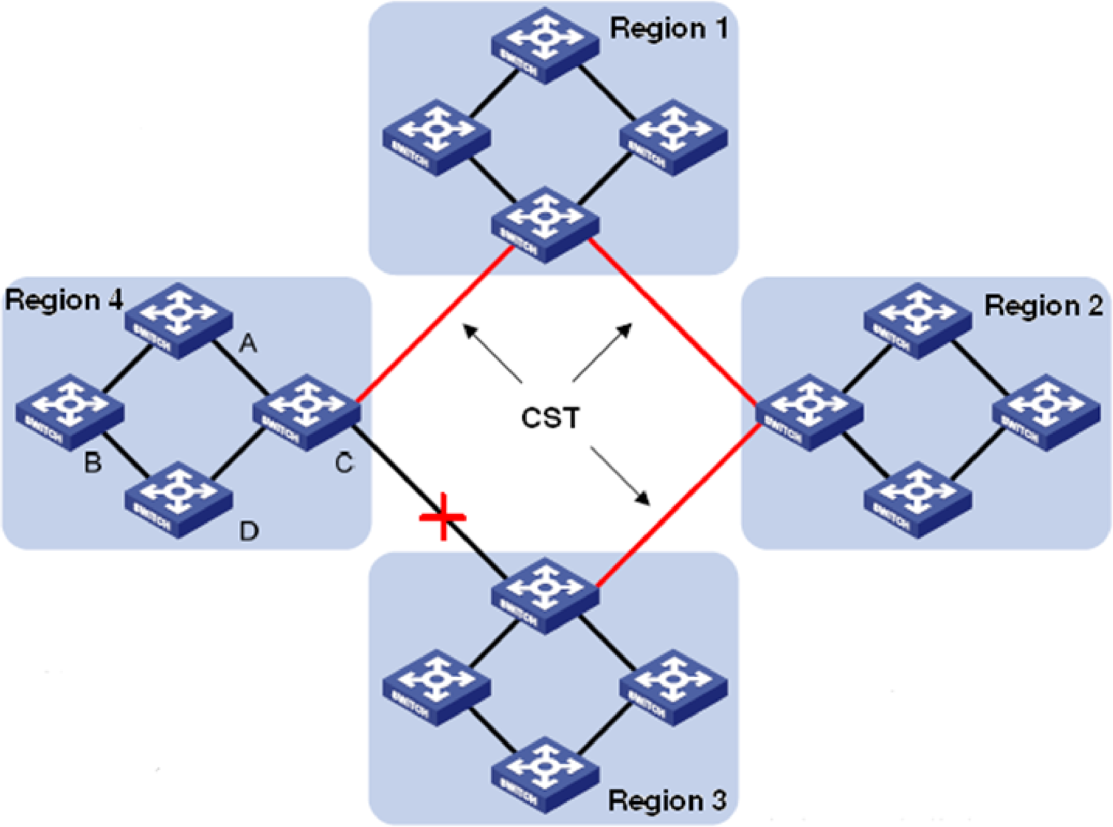


Figure 238 MSTP Concepts

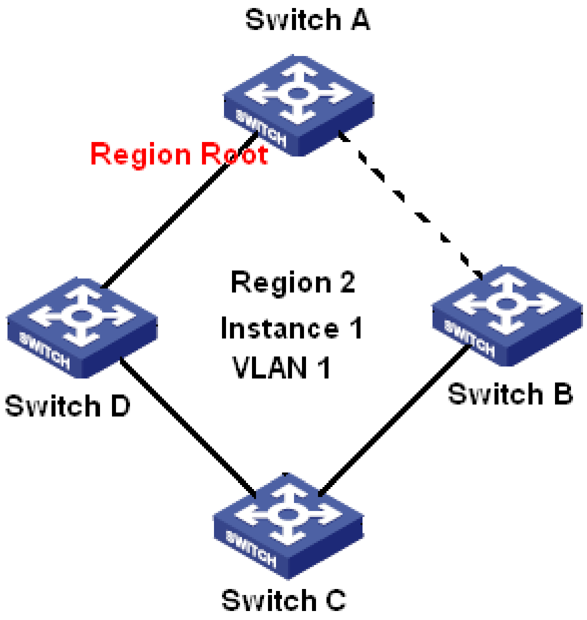


Figure 239 VLAN 1 Mapping to Instance 1

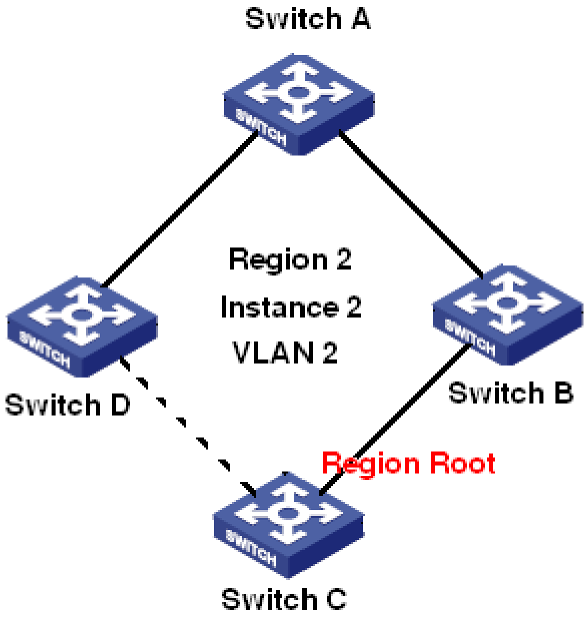


Figure 240 VLAN2 Mapping to Instance 2

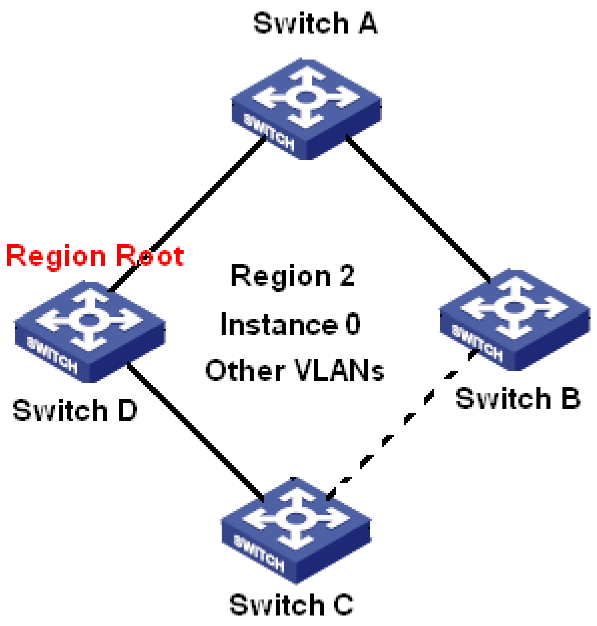


Figure 241 Other VLAN Mapping to Instance 0

Instance: a collection of multiple VLANs. One VLAN (as shown in Figure 239 and Figure 240) or multiple VLANs with the same topology (as shown in Figure 241) can be mapped to one instance; that is, one VLAN can form a spanning tree and multiple VLANs can share one spanning tree. Different instances are mapped to different spanning trees. Instance 0 is the spanning tree for the devices of all regions, while the other instances are the spanning trees for the devices of a specific region.

Multiple Spanning Tree Region (MST region): Switches with the same MSTP region name, revision level, and VLAN-to-instance mapping are in the same MST region. As shown in Figure 238, Region1, Region2, Region3, and Region4 are four different MST regions.

VLAN mapping table: consists of the mapping between VLANs and spanning trees. In Figure 238, VLAN mapping table of region 2 is the mapping between VLAN 1 and instance 1, as shown in Figure 239; VLAN 2 is mapped to instance 2, as shown in Figure 240. The other VLANs are mapped to instance 0, as shown in Figure 241.

Common and Internal Spanning Tree (CIST): indicates instance 0, that is, the spanning tree covering all the devices on a switching network. As shown in Figure 238, the CIST comprises IST and CST.

Internal Spanning Tree (IST): indicates the CIST segment in the MST region, that is, instance 0 of each region, as shown in Figure 241.

Common Spanning Tree (CST): indicates the spanning tree connecting all MST regions in a switching network. If each MST region is a device node, the CST is the spanning tree calculated based on STP/RSTP by these device nodes. As shown in Figure 238, the red lines indicate the spanning tree.

MSTI (Multiple Spanning Tree Instance): one MST region can form multiple spanning trees and they are independent of each other. Each spanning tree is a MSTI, as shown in Figure 239 and Figure 240. IST is also a special MSTI.

Common root: indicates the root bridge of the CIST. The switch with the smallest root bridge ID in a network is the common root.

In an MST region, spanning trees have different topologies, and their regional roots can also be different. As shown in Figure 239, Figure 240, and Figure 241, the three instances have different regional roots. The root bridge of the MSTI is calculated based on STP/RSTP in the current MST region. The root bridge of the IST is the device that is connected to another MST region and selected based on the priority information received.

Boundary port: indicates the port that connects an MST region to another MST region, STP running region, or RSTP running region.

Port state: A port can be in either of the following states based on whether it is learning MAC addresses and forwarding traffic.

Forwarding state: indicates that a port learns MAC addresses and forwards traffic.

Learning state: indicates that a port learns MAC addresses but does not forward traffic.

Discarding state: indicates that a port neither learns MAC addresses nor forwards traffic.

Root port: indicates the best port from a non-root bridge to the root bridge, that is, the port with the smallest cost to the root bridge. A non-root bridge communicates with the root bridge through the root port. A non-root bridge has only one root port. The root bridge has no root port. The root port can be in forwarding, learning, or discarding state.

Designated port: indicates the port for forwarding BPDU to other devices or LANs. All ports on the root bridge are designated ports. The designated port can be in forwarding, learning, or discarding state.

Master port: indicates the port that connects an MST region to the common root. The port is in the shortest path to the common root. From the CST, the master port is the root port of a region (as a node). The master port is a special boundary port. It is the root port for the CIST and master port for other instances. The master port can be in forwarding, learning, or discarding state.

Alternate port: indicates the backup port of the root port or master port. When the root port or master port fails, the alternate port becomes the new root port or master port. The master port can only be in discarding state.

Backup port: indicates the backup port of the designated port. When a designated port fails, the backup port becomes the designated port and forwards data without any delay. The backup port can only be in discarding state.

3.18.5.3 MSTP Implementation

MSTP divides a network into multiple MST regions. CST is calculated between regions. Multiple spanning trees are calculated in a region. Each spanning tree is an MSTI. Instance 0 is the IST, and other instances are MSTIs.

1. CIST calculation

- A device sends and receives BPDU packets. Based on the comparison of MSTP configuration messages, the device with the highest priority is selected as the common root of the CIST.
- An IST is calculated in each MST region.
- Each MST region is considered as a single device and CST is calculated between regions.
- CST and IST constitute the CIST of the entire network.

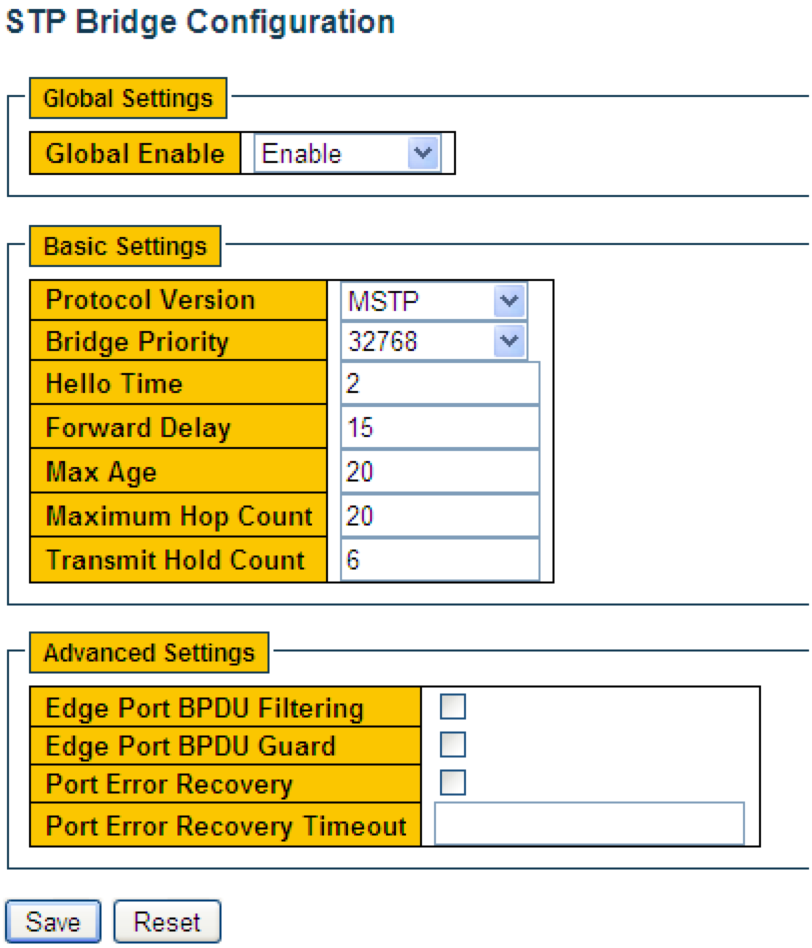
2. MSTI calculation

In an MST region, MSTP generates different spanning trees for VLANs based on the mapping between VLANs and spanning trees. Each spanning tree is calculated independently. The calculation process is similar to that in STP.

In an MST region, VLAN packets are forwarded along corresponding MSTIs. Between MST regions, VLAN packets are forwarded along the CST.

3.18.5.4 Web Configuration

1. Set the time parameters of the network bridge, as shown in Figure 242.



STP Bridge Configuration

Global Settings

Global Enable	Enable

Basic Settings

Protocol Version	MSTP
Bridge Priority	32768
Hello Time	2
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

Advanced Settings

Edge Port BPDU Filtering	□
Edge Port BPDU Guard	□
Port Error Recovery	□
Port Error Recovery Timeout	

Figure 242 Setting Time Parameters of the Network Bridge

Global Enable

Options: Enable/Disable

Default: Disable

Function: Disable or enable spanning tree.

Caution:

- Port-based ring protocols include RSTP, DT-Ring-Port, and DRP-Port, and VLAN-based ring protocols include MSTP, DT-Ring-VLAN, and DRP-VLAN.
- Port-based ring protocol and VLAN-based ring protocol are mutually exclusive, and only one ring protocol mode can be selected for one device.

- A port-based ring protocol and a VLAN-based ring protocol are mutually exclusive, and a device can only select a ring protocol mode.

Protocol Version

Options: MSTP/RSTP/STP

Default: MSTP

Function: Select the spanning tree protocol.

Brigde Priority

Range: 0~61440. The step is 4096.

Default: 32768

Function: Configure the priority of the network bridge.

Description: The priority is used for selecting the root bridge. The smaller the value, the higher the priority.

Hello Time

Range: 1~10s

Default: 2s

Function: Configure the interval for sending BPDU.

Forward Delay

Range: 4~30s

Default: 15s

Function: Configure status change time from Discarding to Learning or from Learning to Forwarding.

Max Age

Range: 6~40s

Default: 20s

Function: Maximum duration that a BPDU can be saved on a device.

Description: If the value of message age in the BPDU is larger than the specified value, then the BPDU is discarded.

Caution:

- The values of Forward Delay Time, Hello Time and Max Age Time should meet the following requirements: 2 * (Forward Delay Time–1.0 seconds) >= Max Age Time; Max Age Time >= 2 * (Hello Time + 1.0 seconds).
- The default setting is recommended.

Maximum Hop Count

Range: 6~40

Default: 20

Function: Configure the maximum hops of MST region. The maximum hops of MST region limit the scale of MST region; the maximum number of hops of regional root is the maximum number of hops of MST region.

Description: Starting from the root bridge of spanning tree in MST region, the hop number deducts 1 when the BPDU passes through a device in the region. Device drops the BPDU with the hop number of 0.

Caution:

- Only the maximum hop configuration of root bridge in MST region is valid. Non-root bridge device adopts the maximum hop configuration of root bridge.
- The default setting is recommended.

Transmit Hold Count

Range: 1~10

Default: 6

Function: Set the maximum number of BPDU packets that can be sent by a port within each Hello Time.

Edge Port BPDU Filtering

Options: Enable/Disable

Default: Disable

Function: Control whether an edge port receives and forwards BPDU packets.

Edge Port BPDU Guard

Options: Enable/Disable

Default: Disable

Function: Control whether an edge port enters the Error-Disable state and is shut down when receiving BPDU packets.

Port Error Recovery

Options: Enable/Disable

Default: Disable

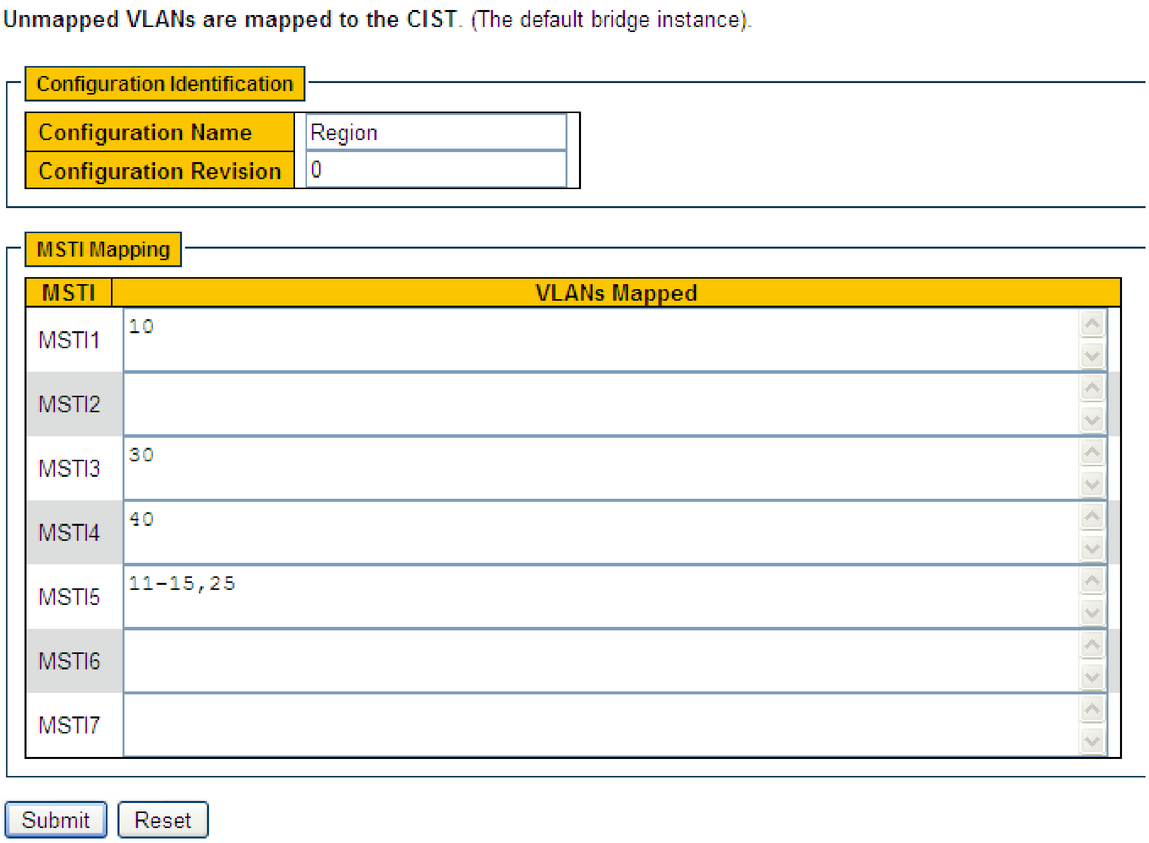
Function: Control whether a port can automatically recover from the error state to the normal state.

Port Error Recovery Timeout

Range: 30~86400s

Function: Set the time for a port to recover from the error state to the normal state.

2. Configure MSTI mapping, as shown in Figure 243.



Unmapped VLANs are mapped to the CIST. (The default bridge instance).

Configuration Identification

Configuration Name	Region
Configuration Revision	0

MSTI Mapping

MSTI	VLANs Mapped
MSTI1	10
MSTI2	
MSTI3	30
MSTI4	40
MSTI5	11-15,25
MSTI6	
MSTI7	

Figure 243 Configure MSTI Mapping

Configuration Name

Range: 1-32 characters

Default: device MAC address

Function: Configure the name of MST region.

Configuration Revision

Options: 0~65535

Default: 0

Function: Configure the revision parameter of MSTP region.

Description: Revision parameter, MST region name, and VLAN mapping table codetermines the MST region that the device belongs to. When all configurations are the same, the devices are in same MST region.

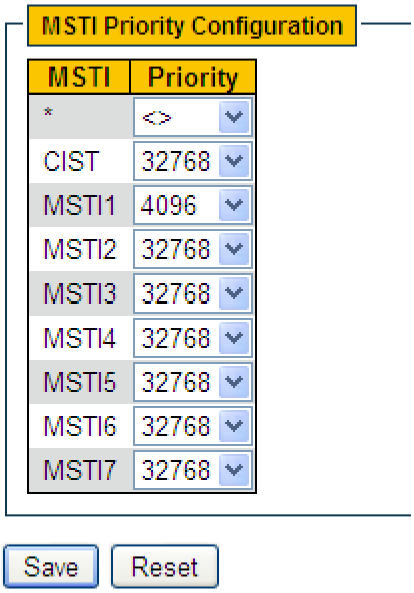
VLANs Mapped

Range: 1~4094

Function: Configure the VLAN mapping table in MST region. When there are multiple VLANs, you can separate the VLANs by a comma (,) and an en dash (-), where an en dash is used to separate two consecutive VLAN IDs and a comma is used to separate two inconsecutive VLAN IDs.

Description: By default, all VLANs map to instance 0. One VLAN maps to only one spanning tree instance. If a VLAN with an existing mapping is mapped to another instance, the previous mapping is cancelled. If the mapping between the designated VLAN and instance is deleted, this VLAN will be mapped to instance 0.

3. Configure the bridge priority of the switch in designated instance, as shown in Figure 244.



MSTI Priority Configuration

MSTI	Priority
*	<>
CIST	32768
MSTI1	4096
MSTI2	32768
MSTI3	32768
MSTI4	32768
MSTI5	32768
MSTI6	32768
MSTI7	32768

Figure 244 Configuring Bridge Priority in Designated Instance

Priority

Range: 0~61440 with the step length of 4096

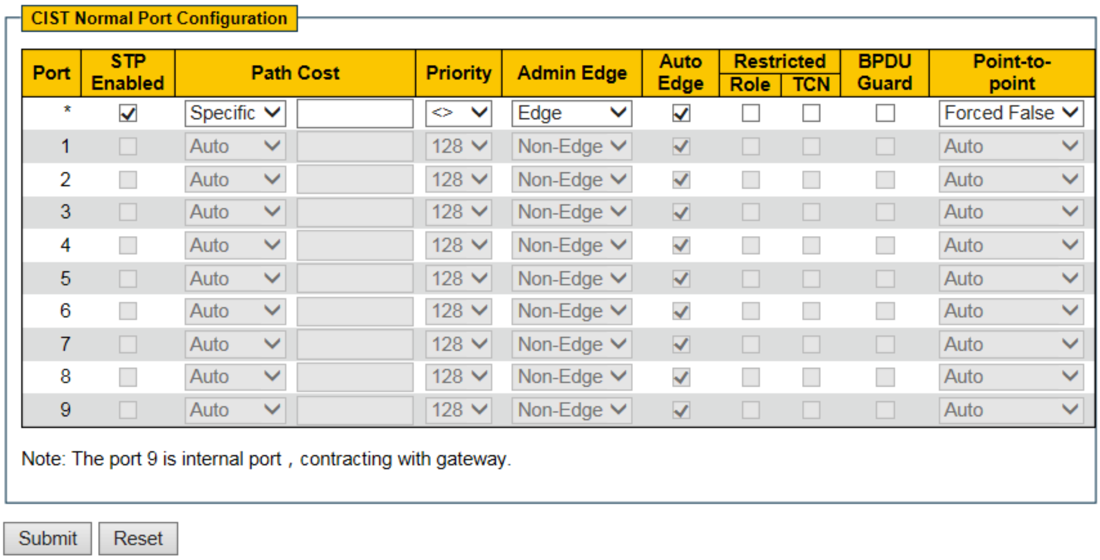
Default: 32768

Function: Configure the bridge priority of the switch in designated instance.

Description: The bridge priority determines whether the switch can be elected to regional root of spanning tree instance. The smaller value is, the higher priority is. By setting a lower priority, a certain device can be designated to root bridge of spanning tree. The MSTP-enabled device can be configured with different priorities in different spanning tree instance.

Click <Save> to make current configurations take effect.

4. Configure CIST ports, as shown in Figure 245.



CIST Normal Port Configuration

Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
							Role	TCN		
*	☑	Specific		<>	Edge	☑	□	□	□	Forced False
1	□	Auto		128	Non-Edge	☑	□	□	□	Auto
2	□	Auto		128	Non-Edge	☑	□	□	□	Auto
3	□	Auto		128	Non-Edge	☑	□	□	□	Auto
4	□	Auto		128	Non-Edge	☑	□	□	□	Auto
5	□	Auto		128	Non-Edge	☑	□	□	□	Auto
6	□	Auto		128	Non-Edge	☑	□	□	□	Auto
7	□	Auto		128	Non-Edge	☑	□	□	□	Auto
8	□	Auto		128	Non-Edge	☑	□	□	□	Auto
9	□	Auto		128	Non-Edge	☑	□	□	□	Auto

Note: The port 9 is internal port , contracting with gateway.

Figure 245 Configure CIST Ports

STP Enabled

Options: Enable/Disable

Default: Disable

Function: Enable or disable STP/RSTP on ports.

Caution:

- MSTP port and port channel are mutually exclusive. A MSTP port cannot be added to a port channel; a port in a port channel cannot be configured as a MSTP port.
- It is recommended that you do not configure ports in the same isolation group as MSTP ports at the same time. Do not add MSTP ports to the same isolation group.

Path Cost

Options: Auto/Specific (1~200000000)

Default: Auto

Description: The path cost of a port is used to calculate the best path. The value of the parameter depends on the bandwidth. The larger the value, the lower the cost. You can change the role of a port by changing the value of the path cost parameter. To configure the value manually, select No for Cost Count.

Priority

Range: 0~240. The step is 16.

Default: 128

Function: Configure the port priority, which determines the roles of ports.

Admin Edge

Options: Non-Edge/Edge

Default: Non-Edge

Function: Set whether the current port is an edge port.

Description: When a port is directly connected to a terminal and is not connected to other devices or a shared network segment, the port is considered as an edge port. An edge can rapidly migrate from the blocking state to the forwarding state without waiting delay. After an edge port receives BPDU packets, it becomes a non-edge port.

Auto Edge

Options: Enable/Disable

Default: Enable

Function: Whether to enable the automatic detection function of an edge port.

Restricted Role

Options: Enable/Disable

Default: Disable

Function: A restricted port will be never selected as a root node even if it is granted the highest priority.

Restricted TCN

Options: Enable/Disable

Default: Disable

Function: A port with restricted TCN will not actively send TCN messages.

BPDU Guard

Options: Enable/Disable

Default: Disable

Function: Control whether an edge port enters the Error-Disable state and is shut down when receiving BPDU packets.

Point-to-point

Options: Auto/Forced True/Forced False

Default: Auto

Function: Set the connection type for a port. If a port is connected to a point-to-point link, the port can rapidly migrate to another state.

Description: Auto indicates that the switch automatically detects the link type based on the duplex status of a port. When a port works in full-duplex mode, the switch considers that the type of the link connected to the port is point-to-point; when a port works in half-duplex mode, the switch considers that the type of the link connected to the port is shared. Forced point-to-point refers that a link connected to a port is a point-to-point link, and forced sharing refers that a link connected to a port is a shared link.

5. Configure MSTI ports, as shown in Figure 246.

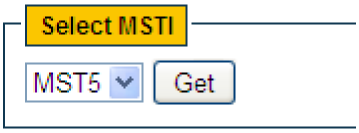


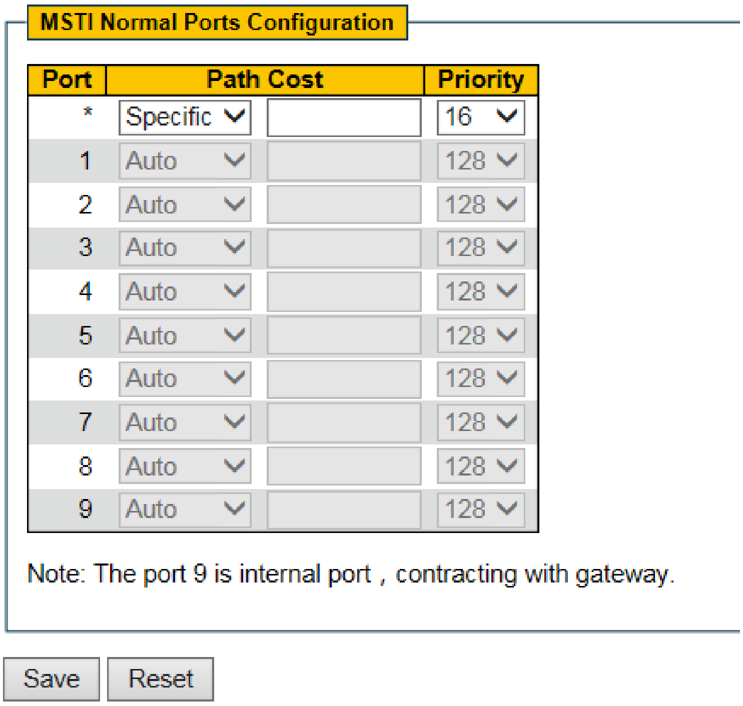
Figure 246 Select MSTI

Select MSTI

Range: MST1~MST7

Default: MST1

Function: Select a MSTI, click <Get> to enter the MSTI ports configuration page, as shown in following figure.



MSTI Normal Ports Configuration

Port	Path Cost		Priority
*	Specific		16
1	Auto		128
2	Auto		128
3	Auto		128
4	Auto		128
5	Auto		128
6	Auto		128
7	Auto		128
8	Auto		128
9	Auto		128

Note: The port 9 is internal port , contracting with gateway.

Figure 247 Configure MSTI Ports

Path Cost

Options: Auto/Specific (1~200000000)

Default: Auto

Function: Configure the path cost of the port in the designated instance.

Description: Port path cost is used to calculate the optimum path. This parameter depends on bandwidth. The bigger bandwidth is, the lower cost is. Changing port path costs can change the transmission path between the device and root bridge, thereby changing port role. The MSTP-enabled port can be configured with different path costs in different spanning tree instances.

Priority

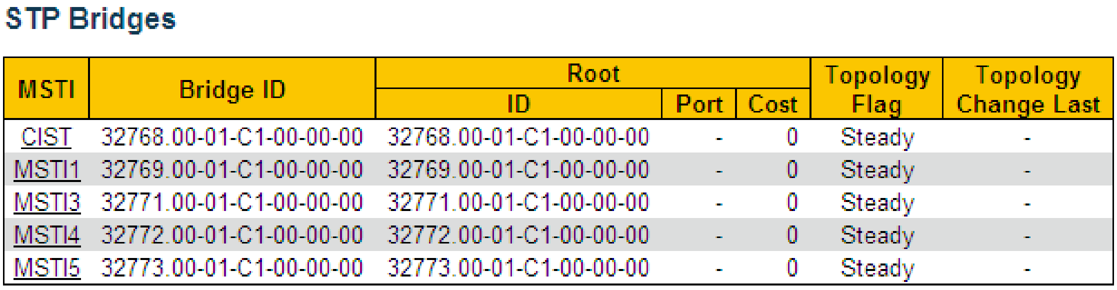
Range: 0~240. The step is 16.

Default: 128

Function: Configure the priority of the port in the designated instance.

Description: Port priority determines whether it will be elected to root port. In the same condition, the port with lower priority will be elected to root port. The MSTP-enabled ports can be configured with different priorities and play different port roles in different spanning tree instances.

6. View bridge status, as shown in Figure 248.

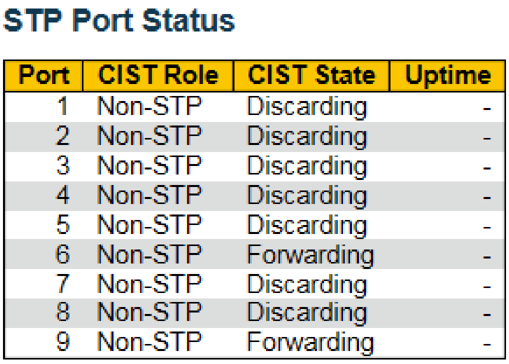


STP Bridges

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	32768.00-01-C1-00-00-00	32768.00-01-C1-00-00-00	-	0	Steady	-
MSTI1	32769.00-01-C1-00-00-00	32769.00-01-C1-00-00-00	-	0	Steady	-
MSTI3	32771.00-01-C1-00-00-00	32771.00-01-C1-00-00-00	-	0	Steady	-
MSTI4	32772.00-01-C1-00-00-00	32772.00-01-C1-00-00-00	-	0	Steady	-
MSTI5	32773.00-01-C1-00-00-00	32773.00-01-C1-00-00-00	-	0	Steady	-

Figure 248 View Bridge Status

7. View STP ports status, as shown in Figure 249.

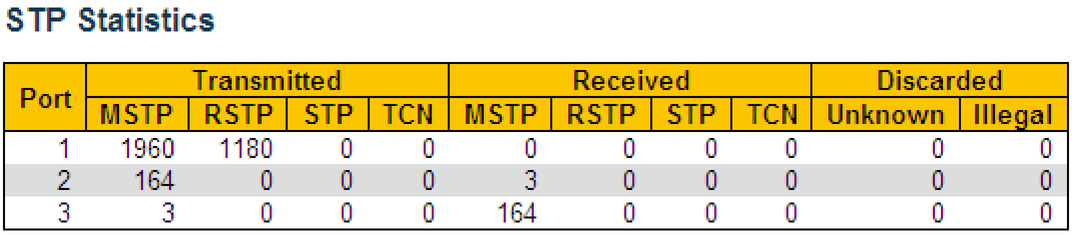


STP Port Status

Port	CIST Role	CIST State	Uptime
1	Non-STP	Discarding	-
2	Non-STP	Discarding	-
3	Non-STP	Discarding	-
4	Non-STP	Discarding	-
5	Non-STP	Discarding	-
6	Non-STP	Forwarding	-
7	Non-STP	Discarding	-
8	Non-STP	Discarding	-
9	Non-STP	Forwarding	-

Figure 249 View STP Ports Status

8. View STP ports packets statistics, as shown in Figure 250.



STP Statistics

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
1	1960	1180	0	0	0	0	0	0	0	0
2	164	0	0	0	3	0	0	0	0	0
3	3	0	0	0	164	0	0	0	0	0

Figure 250 View STP Ports Packets Statistics

3.18.5.5 Typical Configuration Example

As shown in Figure 251, Switch A, B, C, and D belong to the same MST region. The VLANs marked in red indicate the VLAN packets can be transmitted through the links. After configurations are completed, VLAN packets can be forwarded along different spanning tree instances. VLAN 10 packets are forwarded along instance 1 and the root bridge of instance 1 is Switch A; VLAN 30 packets are forwarded along instance 3 and the root bridge of instance 3 is Switch B. VLAN 40 packets are forwarded along instance 4 and the root bridge of instance 4 is Switch C. VLAN 20 packets are forwarded along instance 0 and the root bridge of instance 0 is Switch B.

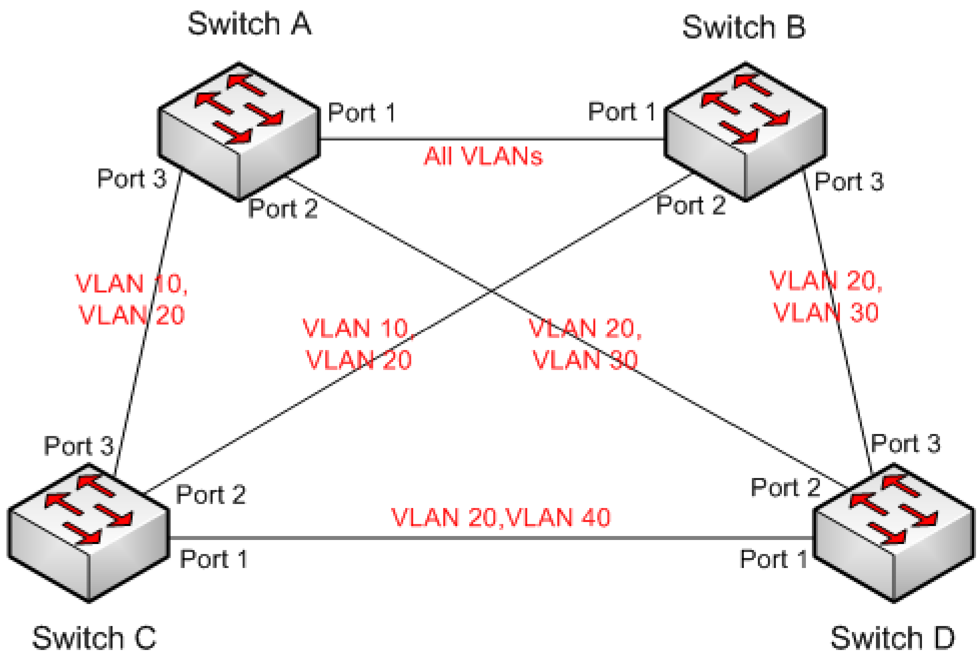


Figure 251 MSTP Typical Configuration Example

Configuration on Switch A:

1. Create VLAN 10, 20, and 30 on Switch A; set the ports and allow the packets of corresponding VLANs to pass through.

2. Enable global MSTP protocol, as shown in Figure 242.

3. Set the name of MST region to Region and the revision parameter to 0, as shown in Figure 243.

4. Create MSTI 1, 3, and 4 and map VLAN 10, 30, and 40 to instance 1, 3, and 4 respectively, as shown in Figure 243.

5. Set the switch bridge priority in MSTI 1 to 4096, and keep default priority in other instances, as shown in Figure 244.

Configuration on Switch B:

6. Create VLAN 10, 20, and 30 on Switch B; set the ports and allow the packets of corresponding VLANs to pass through.

7. Enable global MSTP protocol, as shown in Figure 242.

8. Set the name of MST region to Region and the revision parameter to 0, as shown in

Figure 243.

9. Create MSTI 1, 3, and 4 and map VLAN 10, 30, and 40 to instance 1, 3, and 4 respectively, as shown in Figure 243.

10. Set switch bridge priority in MSTI 3 and MSTI 0 to 4096, and keep default priority in other instances, as shown in Figure 244.

Configuration on Switch C:

11. Create VLAN 10, 20, and 40 on Switch C; set the ports and allow the packets of corresponding VLANs to pass through.

12. Enable global MSTP protocol, as shown in Figure 242.

13. Set the name of MST region to Region and the revision parameter to 0, as shown in Figure 243.

14. Create MSTI 1, 3, and 4 and map VLAN 10, 30, and 40 to instance 1, 3, and 4 respectively, as shown in Figure 243.

15. Set switch bridge priority in MSTI 4 to 4096, and keep default priority in other instances, as shown in Figure 244.

Configuration on Switch D:

16. Create VLAN 20, 30, and 40 on Switch D; set the ports and allow the packets of corresponding VLANs to pass through.

17. Enable global MSTP protocol, as shown in Figure 242.

18. Set the name of MST region to Region and the revision parameter to 0, as shown in Figure 243.

19. Create MSTI 1, 3, and 4 and map VLAN 10, 30, and 40 to instance 1, 3, and 4 respectively, as shown in Figure 243.

When MSTP calculation is completed, the MSTI of each VLAN is as follows:

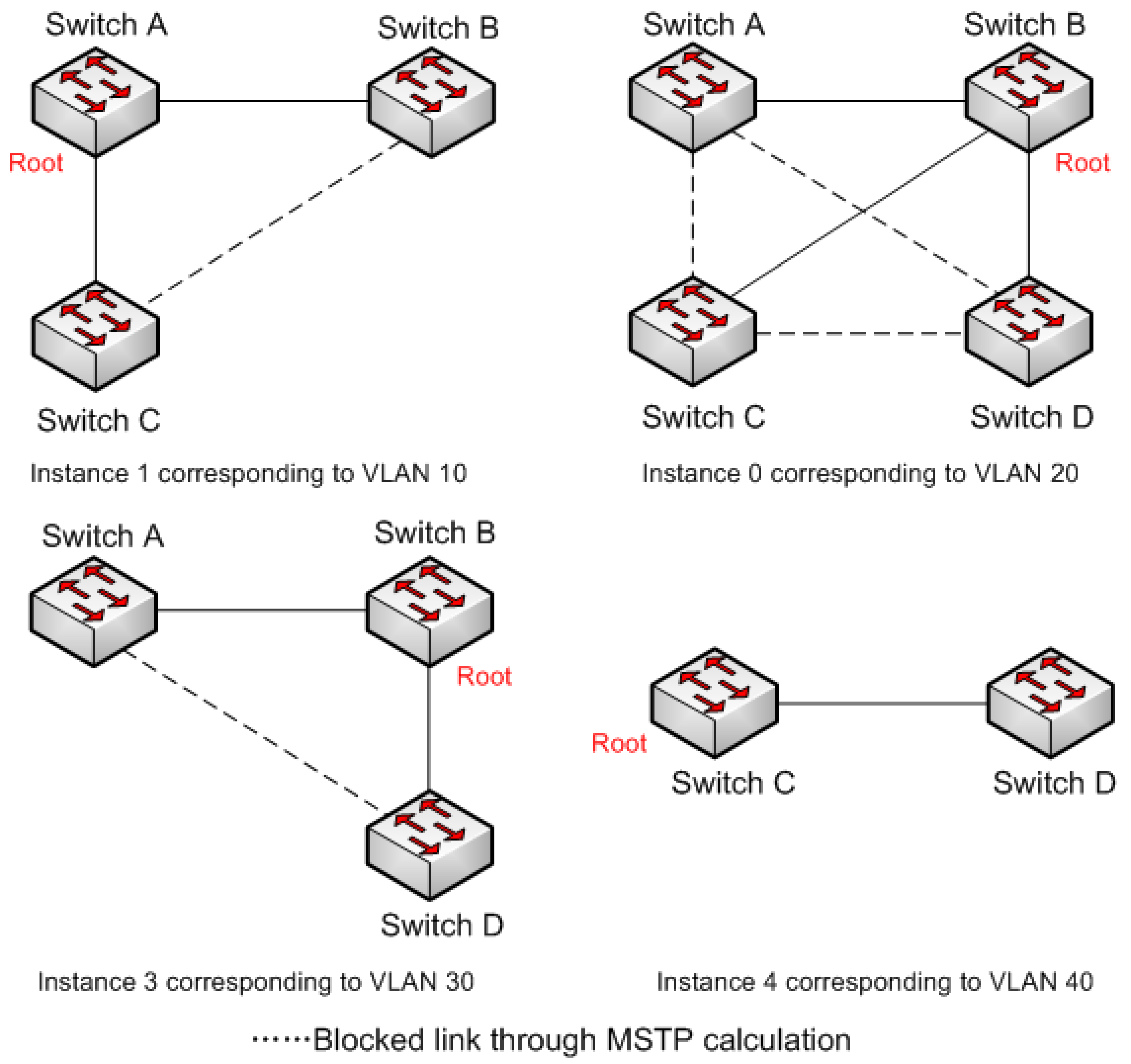

Switch A
Switch B
Root
Switch C
Instance 1 corresponding to VLAN 10
Switch A
Switch B
Root
Switch C
Switch D
Instance 0 corresponding to VLAN 20
Switch A
Switch B
Root
Switch D
Instance 3 corresponding to VLAN 30
Root
Switch C
Switch D
Instance 4 corresponding to VLAN 40
······Blocked link through MSTP calculation

Figure 252 Spanning Tree Instance of each VLAN

3.19 Alarm

3.19.1 Introduction

This series switches support the following types of alarms:

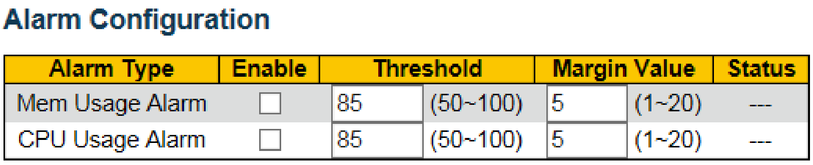
- Power alarm: If the function is enabled, then an alarm will be generated for a single power input.
- IP/MAC conflict alarm: If the function is enabled, then an alarm will be triggered for an IP/MAC conflict.
- Port alarm: If this function is enabled, an alarm is triggered when the port is in link down state.
- Ring alarm: If this function is enabled, an alarm is triggered when the ring is open.

Caution：

Only the master station of a DT ring and the root of a DRP support the ring alarm function.

3.19.2 Web Configuration

1. Memory and CPU Usage Alarm configuration and display, as shown in Figure 253.



Alarm Configuration

Alarm Type	Enable	Threshold		Margin Value		Status
Mem Usage Alarm	□	85	(50~100)	5	(1~20)	---
CPU Usage Alarm	□	85	(50~100)	5	(1~20)	---

Figure 253 Power Alarm

Mem Usage Alarm/CPU Usage Alarm

Options: Enable / Disable

Default: Disable

Function: Enable/ Disable memory/ CPU usage alarm.

Threshold (%)

Range: 50~100

Default: 85

Function: Set the memory/ CPU usage threshold. When the memory/ CPU usage of the switch is higher than the threshold, an alarm is generated.

Margin Value (%)

Range: 1~20

Default: 5

Function: Set the memory/ CPU usage margin value.

Description: If the memory/ CPU usage fluctuates around the threshold, alarms may be generated and cleared repeatedly. To prevent this phenomenon, you can specify a margin value (5% by default). The alarm will be cleared only if the memory/ CPU usage is lower than the threshold by the margin value or more. For example, the memory usage threshold is set to 60% and the margin value is set to 5%. If the memory usage of the switch is lower than or equal to 60%, no alarm is generated. If the memory usage is higher than 60%, an alarm will be generated. The alarm will be cleared only if the memory usage is equal to or lower than

55%.

Status

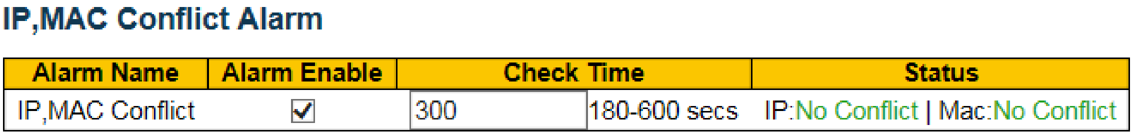
Options: Normal /Alarm

Function: View the memory/ CPU usage status of switch. Alarm means the memory/ CPU usage exceeds the threshold and triggers alarm.

Caution:

The CPU usage in this document refers to the average CPU usage in five minutes.

2. Configure and display IP/MAC conflict alarm, as shown in Figure 254.



IP,MAC Conflict Alarm

Alarm Name	Alarm Enable	Check Time	Status
IP,MAC Conflict	☑	300 180-600 secs	IP:No Conflict | Mac:No Conflict

Figure 254 IP/MAC Conflict Alarm

IP, MAC Conflict

Options: Enable/Disable

Default: Enable

Function: Enable/Disable IP/MAC conflict alarm.

Status

Options: Conflict / No Conflict

Description: When an IP/MAC conflict occurs, Conflictis displayed; otherwise, No Conflictis displayed.

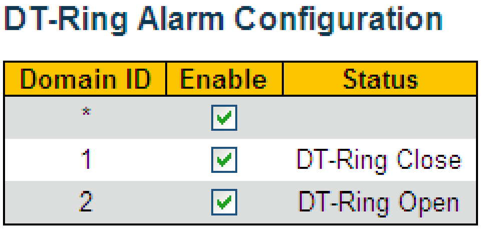
Check Time

Range: 180~600s

Default: 300s

Function: Configure the interval for detecting IP/MAC conflicts.

3. Configure and display DT-Ring ring alarm, as shown in Figure 255.



DT-Ring Alarm Configuration

Domain ID	Enable	Status
*	☑	
1	☑	DT-Ring Close
2	☑	DT-Ring Open

Figure 255 DT-Ring Alarm

DT-Ring Alarm Configuration

Options: Enable/Disable

Default: Disable

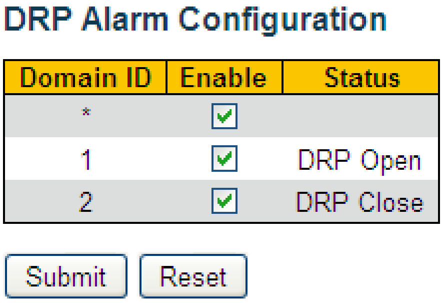
Function: Enable/Disable DT-Ring alarm.

Status

Options: DT-Ring Close / DT-Ring Open

Description: DT-Ring Close means DT-Ring is closed. DT-Ring Open means DT-Ring is open or in abnormal state.

4. Configure and display DRP ring alarm, as shown in Figure 256.



DRP Alarm Configuration

Domain ID	Enable	Status
*	☑	
1	☑	DRP Open
2	☑	DRP Close

Figure 256 DRP Alarm

DRP Alarm Configuration

Options: Disable/Enable

Default: Disable

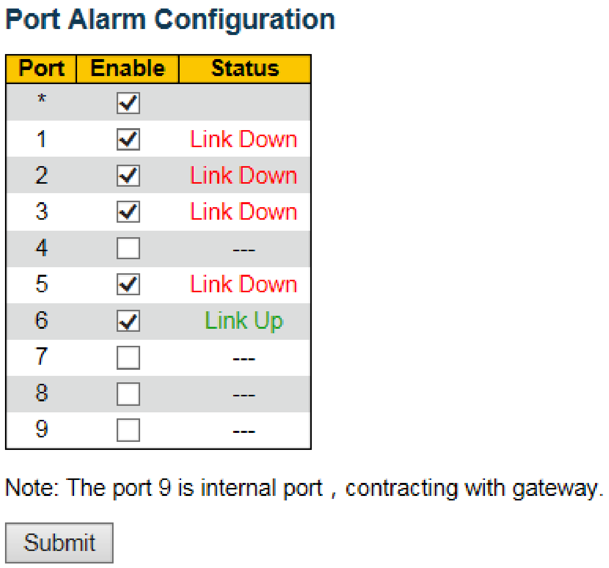
Function: Enable/Disable DRP alarm.

Status

Options: DRP Close / DRP Open

Description: DRP Close means DRP is closed. DRP Open means DRP is open or in abnormal state.

5. Configure and display port alarm, as shown in Figure 257.



Port Alarm Configuration

Port	Enable	Status
*	☑	
1	☑	Link Down
2	☑	Link Down
3	☑	Link Down
4	□	---
5	☑	Link Down
6	☑	Link Up
7	□	---
8	□	---
9	□	---

Note: The port 9 is internal port，contracting with gateway.

Figure 257 Port Alarm

Port Alarm Configuration

Options: Disable/Enable

Default: Disable

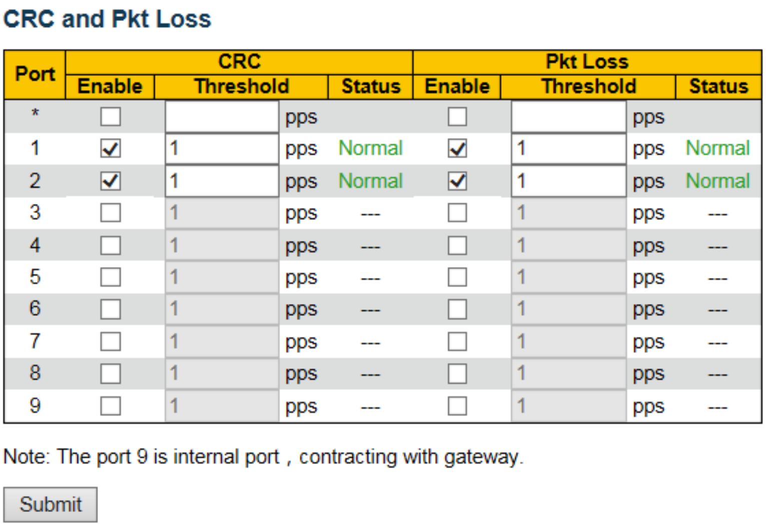
Function: Enable/Disable port alarm.

Status

Options: Link Up/Link Down

Description: Link Up means the port is in connection state and supports normal communication. Link Down means the port is disconnected or in abnormal connection (communication failure).

6.Configure and display CRC and Pkt loss alarm. as shown in the following figure.



CRC and Pkt Loss

Port	CRC			Pkt Loss		
	Enable	Threshold	Status	Enable	Threshold	Status
*	□	pps		□	pps	
1	☑	1 pps	Normal	☑	1 pps	Normal
2	☑	1 pps	Normal	☑	1 pps	Normal
3	□	1 pps	---	□	1 pps	---
4	□	1 pps	---	□	1 pps	---
5	□	1 pps	---	□	1 pps	---
6	□	1 pps	---	□	1 pps	---
7	□	1 pps	---	□	1 pps	---
8	□	1 pps	---	□	1 pps	---
9	□	1 pps	---	□	1 pps	---

Note: The port 9 is internal port，contracting with gateway.

Figure 258 CRC and Pkt Loss Alarm Configuration

CRC/Pkt Loss Alarm

Options: Enable/Disable

Default: Disable

Function: Enable/Disable CRC/ Pkt loss alarm.

Threshold

Range: 1 to 1000000pps.

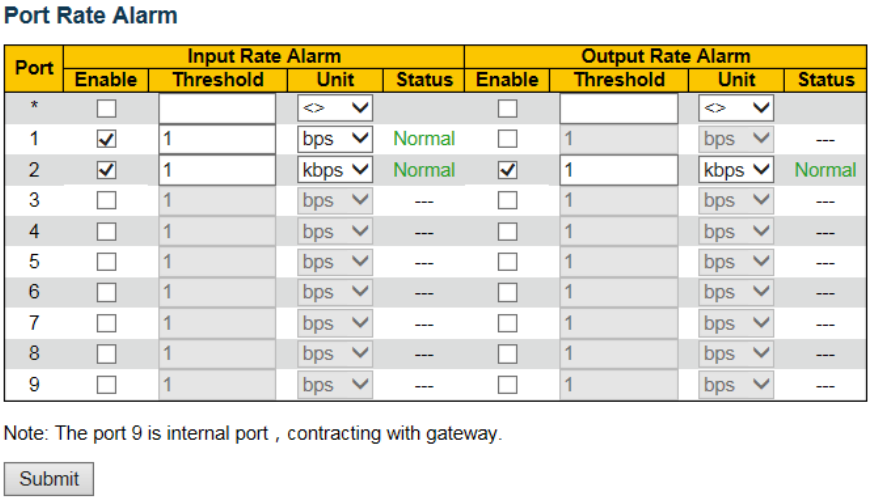
Function: Configure the threshold for the port CRC/ Pkt loss alarm.

Status

Options: Alarm/ Normal

Function: View the port CRC/ Pkt loss status. Alarm means the port CRC/ Pkt loss exceeds the threshold and triggers alarm.

7.Configure and display Port Rate alarm. as shown in the following figure.



Port Rate Alarm

Port	Input Rate Alarm				Output Rate Alarm			
	Enable	Threshold	Unit	Status	Enable	Threshold	Unit	Status
*	□		<>		□		<>	
1	☑	1	bps	Normal	□	1	bps	---
2	☑	1	kbps	Normal	☑	1	kbps	Normal
3	□	1	bps	---	□	1	bps	---
4	□	1	bps	---	□	1	bps	---
5	□	1	bps	---	□	1	bps	---
6	□	1	bps	---	□	1	bps	---
7	□	1	bps	---	□	1	bps	---
8	□	1	bps	---	□	1	bps	---
9	□	1	bps	---	□	1	bps	---

Note: The port 9 is internal port，contracting with gateway.

Figure 259 Port Rate Alarm Configuration

input rate alarm/output rate alarm

Options: Enable/Disable

Default: Disable

Function: Enable/Disable port traffic alarm.

Threshold

Range: 1 to 1000000000bps or 1 to 1000000kbps.

Function: Configure the threshold for the port traffic.

Status

Options: Alarm/ Normal

Function: View the port traffic status. Alarm means the incoming / outgoing traffic rate exceeds the threshold and triggers alarm.

3.20 Link Check

3.20.1 Introduction

Link check adopts periodic interaction of protocol packets to judge the link connectivity and display the port communication status. In case of a fault, the problem can be found and handled in time.

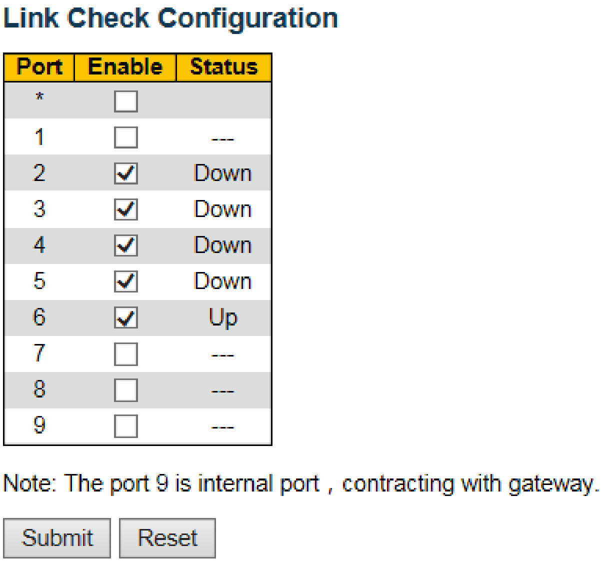
The port for which link status check is enabled sends link-check packets periodically (every

1s) to check the link status. If the port does not receive a link-check packet from the peer end within the receive timeout period (5s), it indicates that the link is abnormal and the port displays Rx fault state. If the port receives a link-check packet from the peer end and the packet shows that the link-check packet is received from local within the receive timeout period (5s), the port displays the normal state. If the port receives a link-check packet from the peer end but the packet shows that the link-check packet is not received from local within the receive timeout period (5s), the port displays Tx fault state. If the link to the port is down, the port displays link down state.

The port for which link status check is disabled works in passive mode. That is, it does not send a link-check packet in active mode. However, after receiving a link-check packet from the peer end, this port returns a link-check packet immediately to inform the peer end that it has received the link-check packet.

3.20.2 Web Configuration

Configure link check, as shown in Figure 260.



Link Check Configuration

Port	Enable	Status
*	☐	
1	☐	---
2	☑	Down
3	☑	Down
4	☑	Down
5	☑	Down
6	☑	Up
7	☐	---
8	☐	---
9	☐	---

Note: The port 9 is internal port , contracting with gateway.

Figure 260 Configure Link Check

Enable

Options: Disable/Enable

Default: Disable

Function: Enable/Disable link check on port.

Caution:

If the peer device does not support the function, the function shall be disabled on the connected port of the local device.

Status

Options: Up/Normal/--/Rx Fault/Tx Fault/Down

Description: If Link Check is enabled on a port and the port sends and receives data normally, Normal is displayed. If the peer end does not receive the detection packets from the device, Tx Fault is displayed. If the device does not receive detection packets from the peer end, Rx Fault is displayed. If port is link down, Down is displayed. If Link Check is not enabled on a port, -- is displayed. At the moment of link check being enabled on a link up port, up is displayed.

3.21 Log

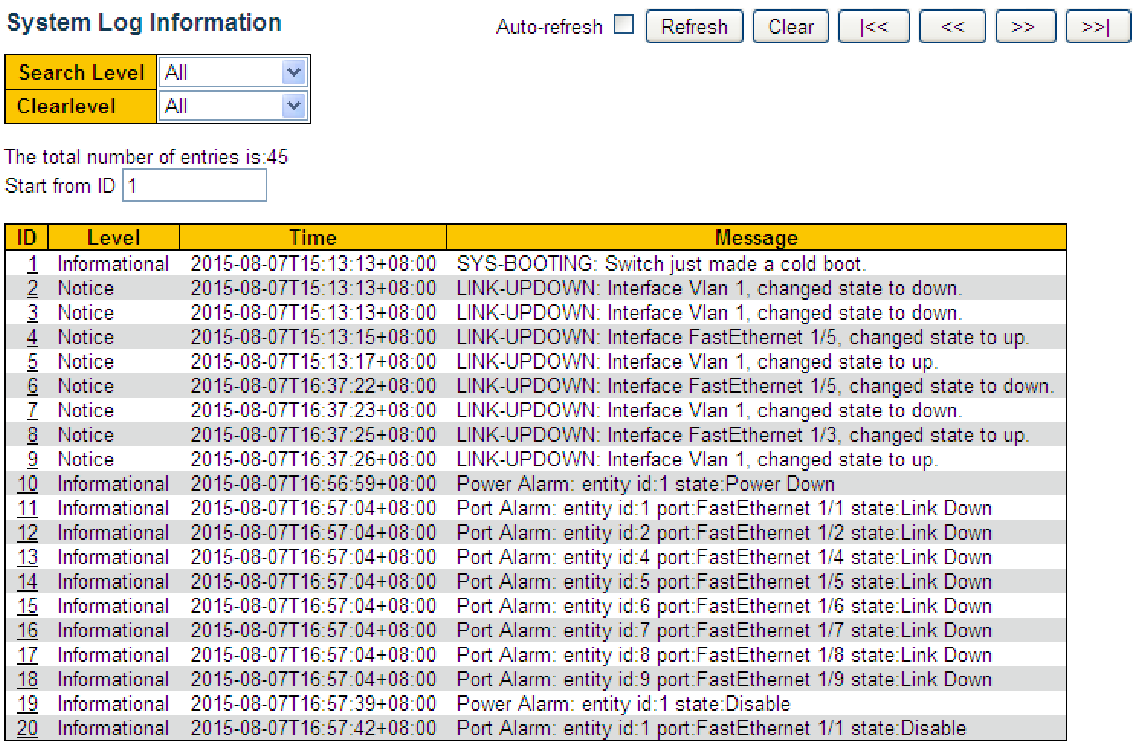
3.21.1 Introduction

The log function mainly records system status, fault, debugging, anomaly, and other information. With appropriate configuration, the switch can upload logs into a Syslog-supported server in real time.

Log contains information about alarms, broadcast storm, reboot, memory, and information about users' operations.

3.21.2 Web Configuration

1. Configure system log, as shown in Figure 261.



System Log Information

Search Level	All
Clearlevel	All

The total number of entries is:45

Start from ID 1

ID	Level	Time	Message
1	Informational	2015-08-07T15:13:13+08:00	SYS-BOOTING: Switch just made a cold boot.
2	Notice	2015-08-07T15:13:13+08:00	LINK-UPDOWN: Interface Vlan 1, changed state to down.
3	Notice	2015-08-07T15:13:13+08:00	LINK-UPDOWN: Interface Vlan 1, changed state to down.
4	Notice	2015-08-07T15:13:15+08:00	LINK-UPDOWN: Interface FastEthernet 1/5, changed state to up.
5	Notice	2015-08-07T15:13:17+08:00	LINK-UPDOWN: Interface Vlan 1, changed state to up.
6	Notice	2015-08-07T16:37:22+08:00	LINK-UPDOWN: Interface FastEthernet 1/5, changed state to down.
7	Notice	2015-08-07T16:37:23+08:00	LINK-UPDOWN: Interface Vlan 1, changed state to down.
8	Notice	2015-08-07T16:37:25+08:00	LINK-UPDOWN: Interface FastEthernet 1/3, changed state to up.
9	Notice	2015-08-07T16:37:26+08:00	LINK-UPDOWN: Interface Vlan 1, changed state to up.
10	Informational	2015-08-07T16:56:59+08:00	Power Alarm: entity id:1 state:Power Down
11	Informational	2015-08-07T16:57:04+08:00	Port Alarm: entity id:1 port:FastEthernet 1/1 state:Link Down
12	Informational	2015-08-07T16:57:04+08:00	Port Alarm: entity id:2 port:FastEthernet 1/2 state:Link Down
13	Informational	2015-08-07T16:57:04+08:00	Port Alarm: entity id:4 port:FastEthernet 1/4 state:Link Down
14	Informational	2015-08-07T16:57:04+08:00	Port Alarm: entity id:5 port:FastEthernet 1/5 state:Link Down
15	Informational	2015-08-07T16:57:04+08:00	Port Alarm: entity id:6 port:FastEthernet 1/6 state:Link Down
16	Informational	2015-08-07T16:57:04+08:00	Port Alarm: entity id:7 port:FastEthernet 1/7 state:Link Down
17	Informational	2015-08-07T16:57:04+08:00	Port Alarm: entity id:8 port:FastEthernet 1/8 state:Link Down
18	Informational	2015-08-07T16:57:04+08:00	Port Alarm: entity id:9 port:FastEthernet 1/9 state:Link Down
19	Informational	2015-08-07T16:57:39+08:00	Power Alarm: entity id:1 state:Disable
20	Informational	2015-08-07T16:57:42+08:00	Port Alarm: entity id:1 port:FastEthernet 1/1 state:Disable

Figure 261 Configure System Log

Search Level

Options: Error/Warning/Notice/Informational/All

Default: all

Function: Select the level of log information to be displayed.

Clear level

Options: Error/Warning/Notice/Informational/All

Default: all

Function: Select the level of log information to be deleted. Click <Clear> to delete the designated level log information.

The total number

Function: Displays the number of logs that meet the query conditions.

Start from ID

Function: set the start ID of log entries on the current page. You can click Refresh to update log entries on the current page. 20 log entries can be displayed on each page.

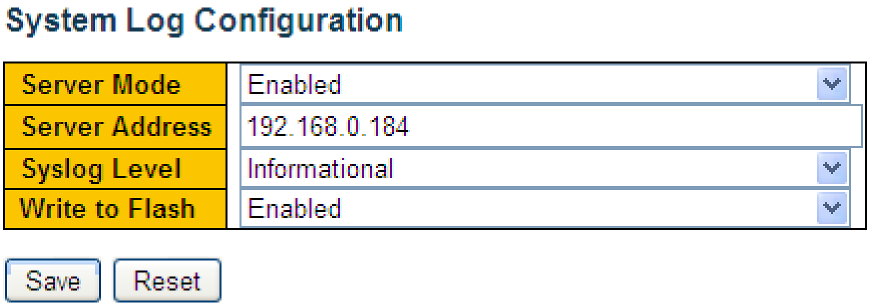
Click >> to view log entries on the next page. The start ID of the next page is the ID of the last log entry on the current page.

Click << to view log entries on the previous page.

Click >>| to view log entries on the last page. The end ID is the ID of the last log entry.

Click |<< to view log entries on the first page. The start ID is the ID of the first log entry.

2. Upload Log to server in real time, as shown in Figure 262.



System Log Configuration

Server Mode	Enabled
Server Address	192.168.0.184
Syslog Level	Informational
Write to Flash	Enabled

Figure 262 Upload Log in Real Time

Server Mode

Options: Disable/Enable

Default: Disable

Function: Enable/Disable uploading Log to server in real time.

Server Address

Function: Configure the IP address of the server that log informational is uploaded to.

Syslog Level

Option: Error/Warning/Notice/Informational

Default: Informational

Function: Select the level of log information to be uploaded to server.

Write to Flash

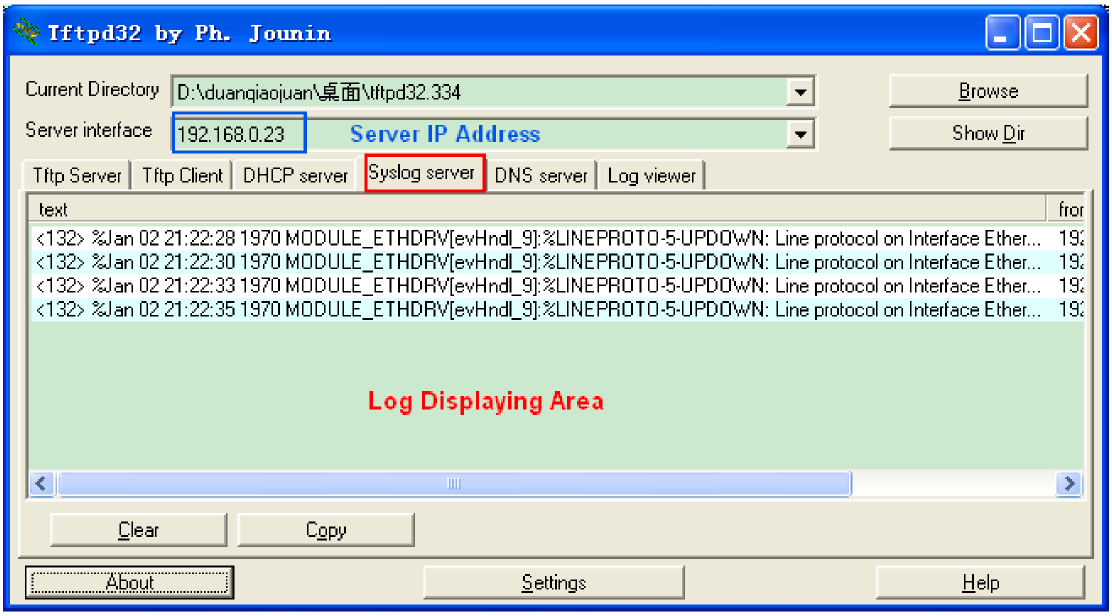
Option: Enabled/Disabled

Default: Disabled

Function: whether to write log to flash or not.

You can install Syslog Server software, for example, Tftp32, on a PC to build a "Syslog Server".

Log information can be displayed in real time on the Syslog Server, as shown in Figure 263.



Current Directory: D:\duanqiaojuan\桌面\tftpd32.334

Server interface: 192.168.0.23

Server IP Address

```
<132> %Jan 02 21:22:28 1970 MODULE_ETHDRV[evHndl_9]:%LINEPROTO-5-UPDOWN: Line protocol on Interface Ether...   19
<132> %Jan 02 21:22:30 1970 MODULE_ETHDRV[evHndl_9]:%LINEPROTO-5-UPDOWN: Line protocol on Interface Ether...   19
<132> %Jan 02 21:22:33 1970 MODULE_ETHDRV[evHndl_9]:%LINEPROTO-5-UPDOWN: Line protocol on Interface Ether...   19
<132> %Jan 02 21:22:35 1970 MODULE_ETHDRV[evHndl_9]:%LINEPROTO-5-UPDOWN: Line protocol on Interface Ether...   19
```

Log Displaying Area

Figure 263 Uploading Log Information in Real Time

3.22 Port Mirroring

3.22.1 Introduction

With port mirroring function, the switch copies all received or transmitted data frames in a port (mirroring source port) to another port (mirroring destination port). The mirroring destination port is connected to a protocol analyzer or RMON monitor for network monitoring, management, and fault diagnosis.

3.22.2 Explanation

A switch supports only one mirroring destination port but multiple source ports.

Multiple source ports can be either in the same VLAN, or in different VLANs. Mirroring source port and destination port can be in the same VLAN or in different VLANs.

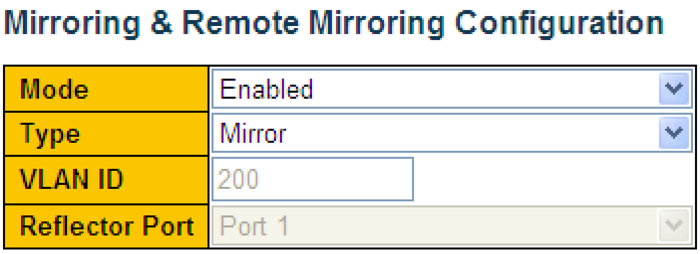
The source port and destination port cannot be the same port.

Caution:

The dynamic MAC address learning must be disabled on a destination port.

3.22.3 Web Configuration

1. Cofigure port mirror function, as shown in Figure 264.



Mirroring & Remote Mirroring Configuration

Mode	Enabled
Type	Mirror
VLAN ID	200
Reflector Port	Port 1

Figure 264 Cofigure Port Mirror Function

Mode

Options: Enable/Disable

Default: Disable

Function: Enable/Disable port mirror function.

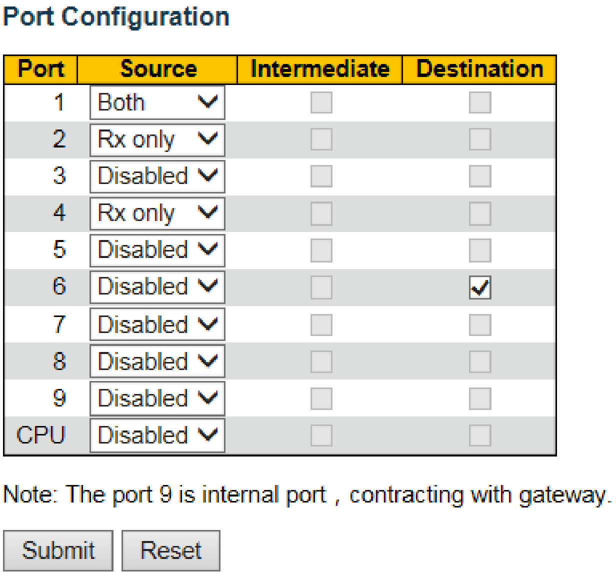
Type

Options: Mirror/Source(RMirror)/Intermediate(RMirror)/Destination(RMirror)

Function: Use port mirror function.

Description: The mirror is configured for the local port mirroring, and the source (RMirror) / Intermediate (RMirror) / destination (RMirroring) is configured for remote mirroring. When the Mirror is selected, the remote port can not be configured. When the type selection source (RMirroring) is configured, only the source and Intermediate ports of the remote mirroring can be configured. The destination port can not be configured. When the type is selected for Intermediate (RMirroring) You can configure only the Intermediate port for remote mirroring. When you select the destination (RMirroring), you can configure only the Intermediate and destination ports of the remote mirroring. You can not configure the source port.

2. Configure the mirror port, as shown in Figure 265.



Port Configuration

Port	Source	Intermediate	Destination
1	Both	□	□
2	Rx only	□	□
3	Disabled	□	□
4	Rx only	□	□
5	Disabled	□	□
6	Disabled	□	☑
7	Disabled	□	□
8	Disabled	□	□
9	Disabled	□	□
CPU	Disabled	□	□

Note: The port 9 is internal port , contracting with gateway.

Figure 265 Select the Mirroring Destination and Source Port

Source

Options: Rx only/Tx only /Both

Function: Select the data to be mirrored in the mirroring source port.

Rx only: indicates only the received packets are mirrored in the source port.

Tx only: indicates only the transmitted packets are mirrored in the source port.

Both: indicates both transmitted and received packets are mirrored in the source port.

Intermediate

Function: Select the mirror Intermediate port to forward the received data.

Destination

Function: Select a port to be the mirroring destination port. There is one and only one mirroring destination port.

3.22.4 Typical Configuration Example

As shown in Figure 266, the mirroring destination port is port 2 and the mirroring source port is port 1. Both transmitted and received packets on port 1 are mirrored to port 2.

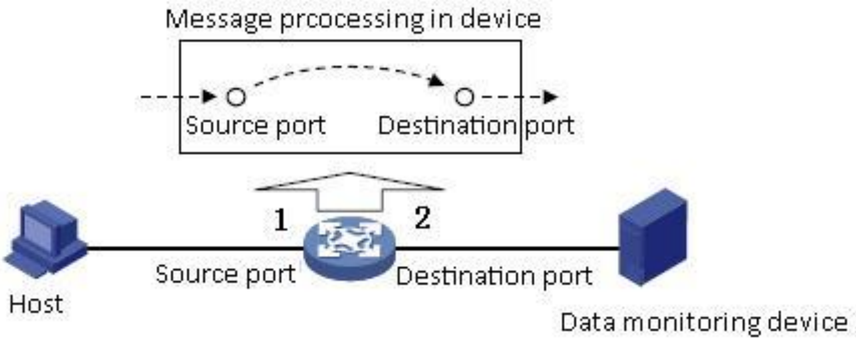


Figure 266 Port Mirroring Example

Configuration process:

1. Enable port mirror function, as shown in Figure 264.

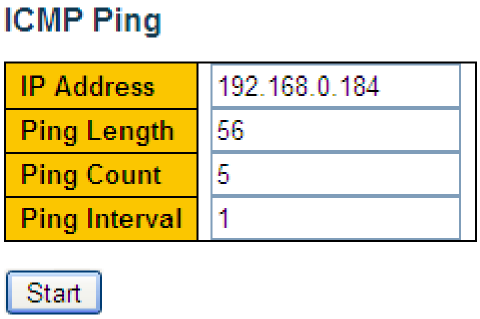
2. Set port 2 to the mirroring destination port, port 1 to the mirroring source port and the port mirroring mode to both, as shown in Figure 265.

3.23 Diagnostics

3.23.1 Ping

Users can run the ping command to check whether the device of a specified address is reachable and whether the network connection is faulty during routine system maintenance.

1. Configure ping command, as shown in Figure 267.


ICMP Ping

IP Address	192.168.0.184
Ping Length	56
Ping Count	5
Ping Interval	1

Figure 267 Configure Ping Command

IP Address

Format: A.B.C.D

Description: Input the IP address of the destinate device.

Ping Length

Range: 2~1452 bytes

Default: 56 bytes

Function: Specify the length of an ICMP request (excluding the IP and ICMP packet header) for transmission.

Ping Count

Range: 1~60

Default: 5

Function: Specify the number of times for sending an ICMP request.

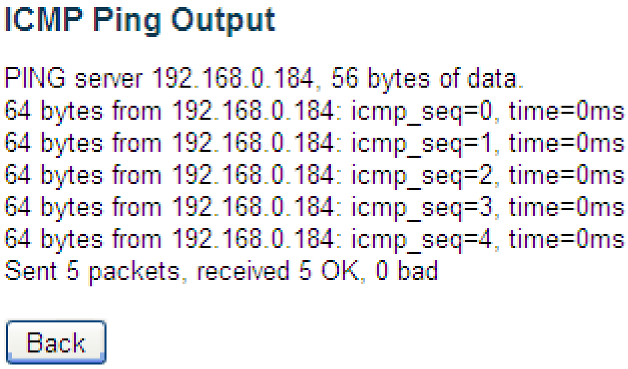
Ping Interval

Range: 0~30s

Default: 1s

Function: Specify the interval for sending an ICMP request.

2. View ping output, as shown in Figure 268.



ICMP Ping Output

```
PING server 192.168.0.184, 56 bytes of data.
64 bytes from 192.168.0.184: icmp_seq=0, time=0ms
64 bytes from 192.168.0.184: icmp_seq=1, time=0ms
64 bytes from 192.168.0.184: icmp_seq=2, time=0ms
64 bytes from 192.168.0.184: icmp_seq=3, time=0ms
64 bytes from 192.168.0.184: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad
```

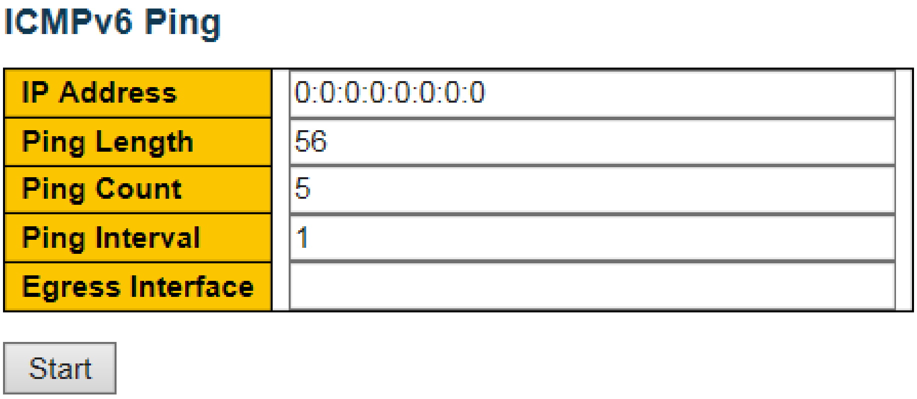
Figure 268 Viewe Ping Output

The output of the ping command includes response of the destination device to each ICMP request packet and packet statistics collected during the running of the ping command.

3.23.2 Ping6

ICMPv6 is an Internet control information protocol developed with IPv6 to check whether the device with the specified IPv6 address is reachable and test whether the network connection is faulty.

1.configure ICMPv6 Ping , as shown in the following figure.



ICMPv6 Ping

IP Address	0:0:0:0:0:0:0:0
Ping Length	56
Ping Count	5
Ping Interval	1
Egress Interface	

Figure 269 ICMPv6 Ping

IP address

Format: A.B.C.D.E.F.G.H

Function: Configure the IP address of the destination device.

Ping length

Range: 2 ~ 1452 bytes

Default: 56 bytes

Function: Specifies the length of the ICMP request packets (excluding IP and ICMP packet headers).

Ping Count

Range: 1 ~ 60

Default: 5

Function: Specifies the number of times to send ICMP request packets.

Ping interval

Range: 0 ~ 30s

Default: 1s

Function: Specifies the interval for sending ICMP request packets.

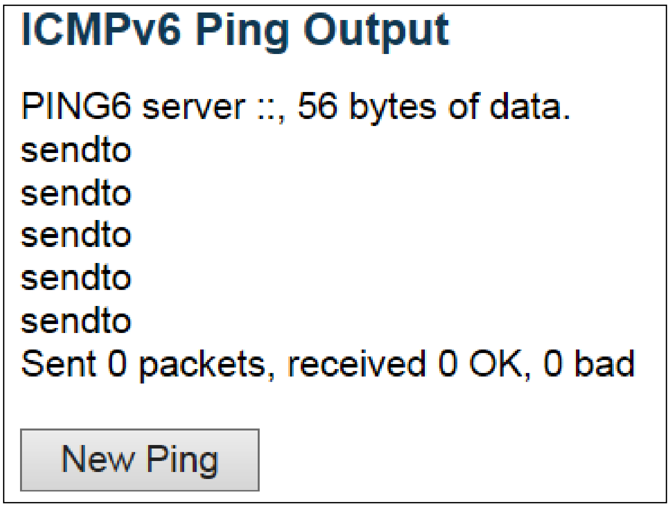
Egress Interface

Configuration Range: 1-4094

Default configuration: None

Function: Sends test data in the specified VLAN to verify that the network is unobstructed.

2. View the information output from the ping command, as shown in the following figure:



ICMPv6 Ping Output

```
PING6 server ::, 56 bytes of data.
sendto
sendto
sendto
sendto
sendto
Sent 0 packets, received 0 OK, 0 bad
```

Figure 270 ICMPv6 Ping Output

The ping command output includes the response of the destination device to each ICMP request packet and the statistics of the ping process packets.

4 Gateway Function Configuration

4.1.Device Information

4.1.1.Main Information

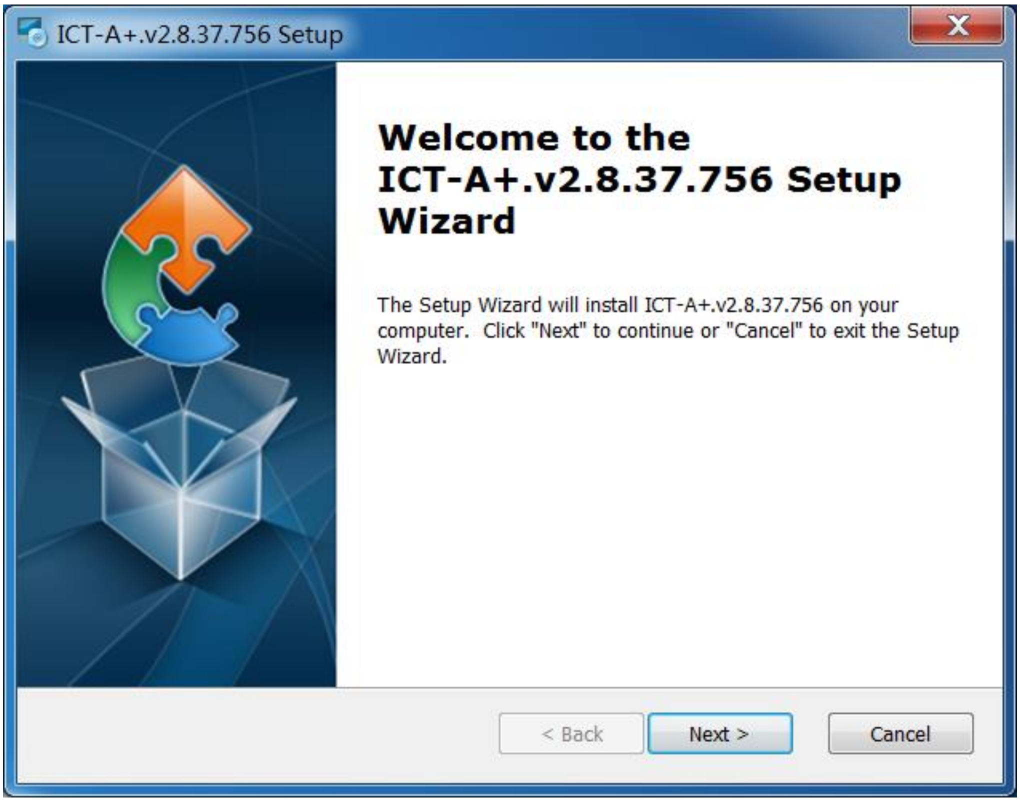
The integration configuration environment tool, EDPS ICT-A+, allows users to make simple configuration on DG gateways. Users can access the disc delivered with the device via the friendly UI to complete installation in one-click mode. Currently, the EDPS ICT-A+ can be installed on Win2000/Win XP/Win7/Win8/Win10. The installation package of the EDPS ICT-A+ includes executable files, configuration files, a language package, and a firmware package. The firmware package includes run files provided by the system for the target unit. The EDPS ICT-A+ can transfer firmware to any target unit that meets conditions.

4.1.2.Installation of ICT-A+

Perform the following steps to install the ICT-A+ Toolset:

1. Insert the installation disc into the CD-ROM of a computer, locate the installation file **ICT-A (CN).msi** or **ICT- A (CN).exe**, and run this file to install the ICT-A+ Toolset.

2. After completing the OS self-test, the system automatically displays the welcome wizard dialog box.



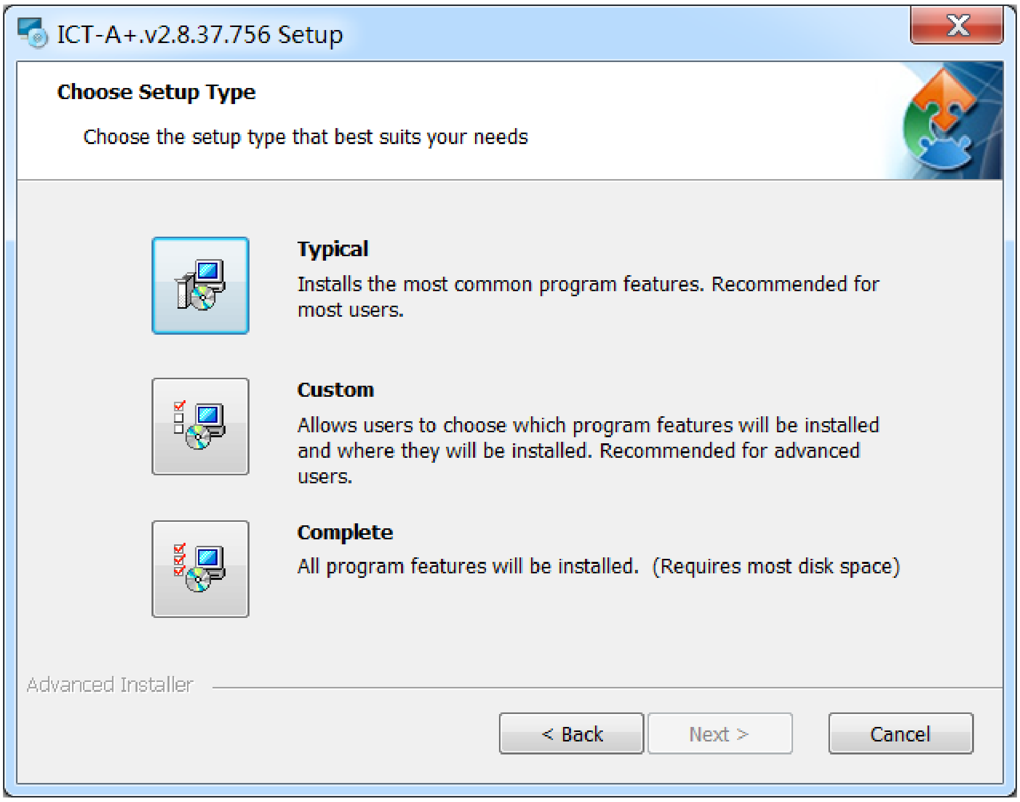
ICT-A+.v2.8.37.756 Setup

Welcome to the ICT-A+.v2.8.37.756 Setup Wizard

The Setup Wizard will install ICT-A+.v2.8.37.756 on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.

Note: The system automatically selects the required software components to complete installation.

3. Click **Next**.



ICT-A+.v2.8.37.756 Setup

Choose Setup Type

Choose the setup type that best suits your needs

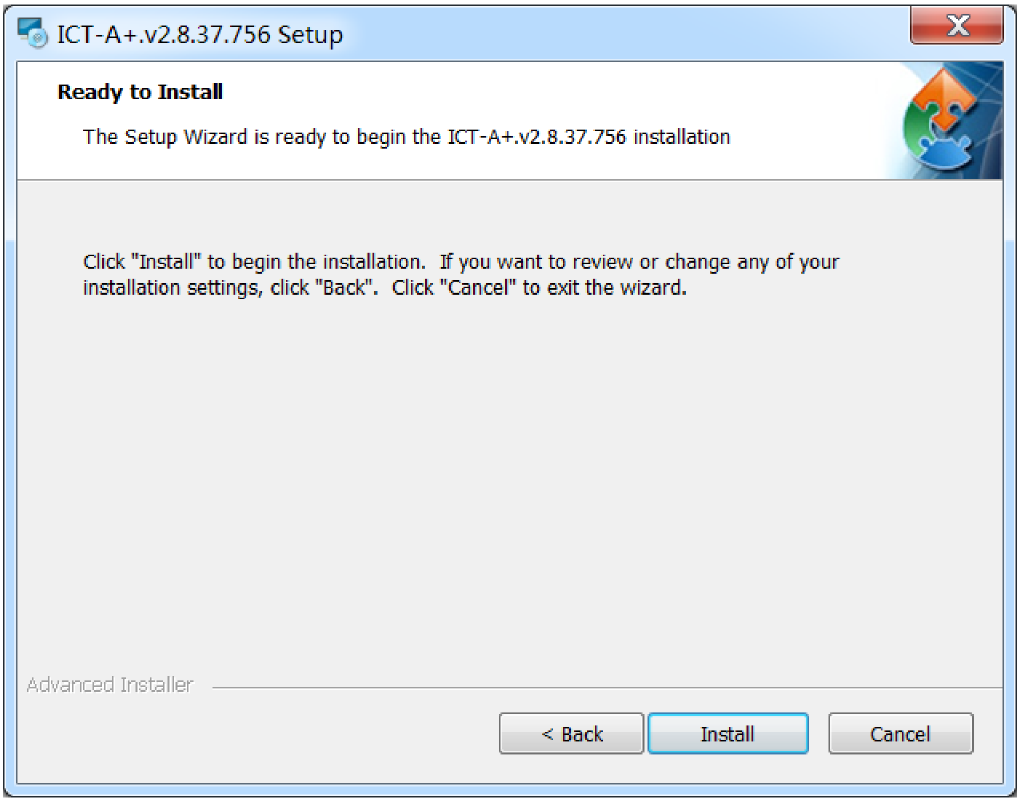
Typical
Installs the most common program features. Recommended for most users.

Custom
Allows users to choose which program features will be installed and where they will be installed. Recommended for advanced users.

Complete
All program features will be installed. (Requires most disk space)

You can select **Typical**, **Custom**, or **Complete** during installation. When you select **Typical**, the default installation path is C:\Program Files\ and you are allowed to define the installation directory. Click **Next**.

4. Click **Install**. Or click **Cancel**.



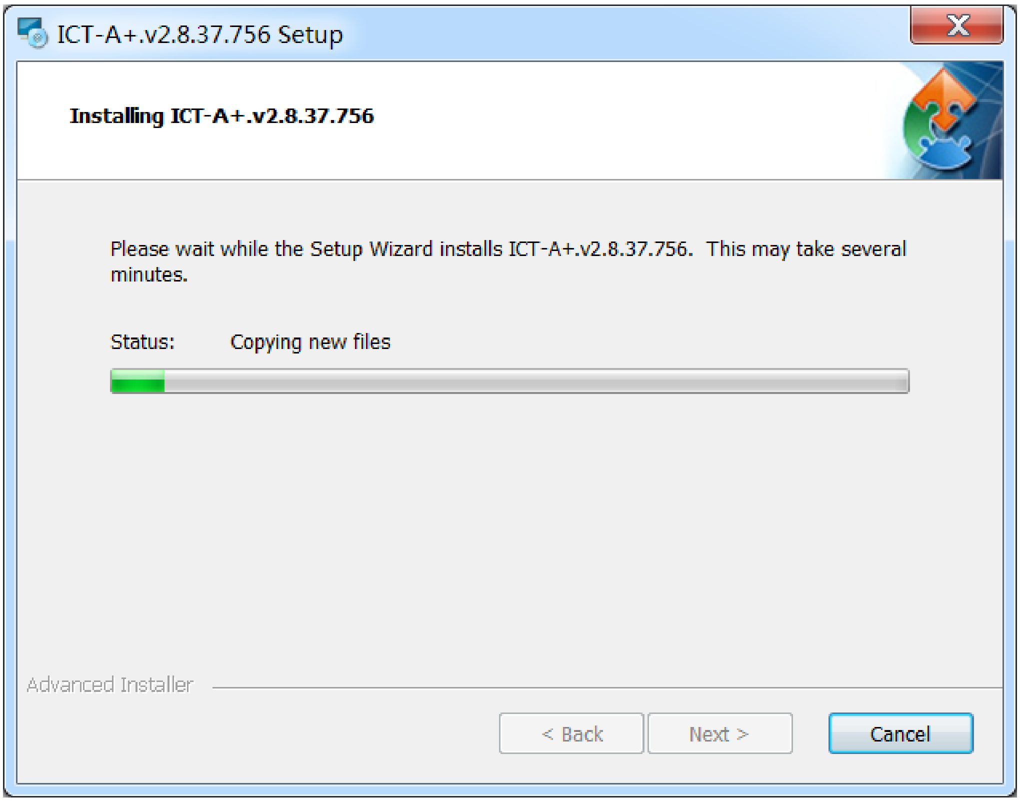
ICT-A+.v2.8.37.756 Setup

Ready to Install

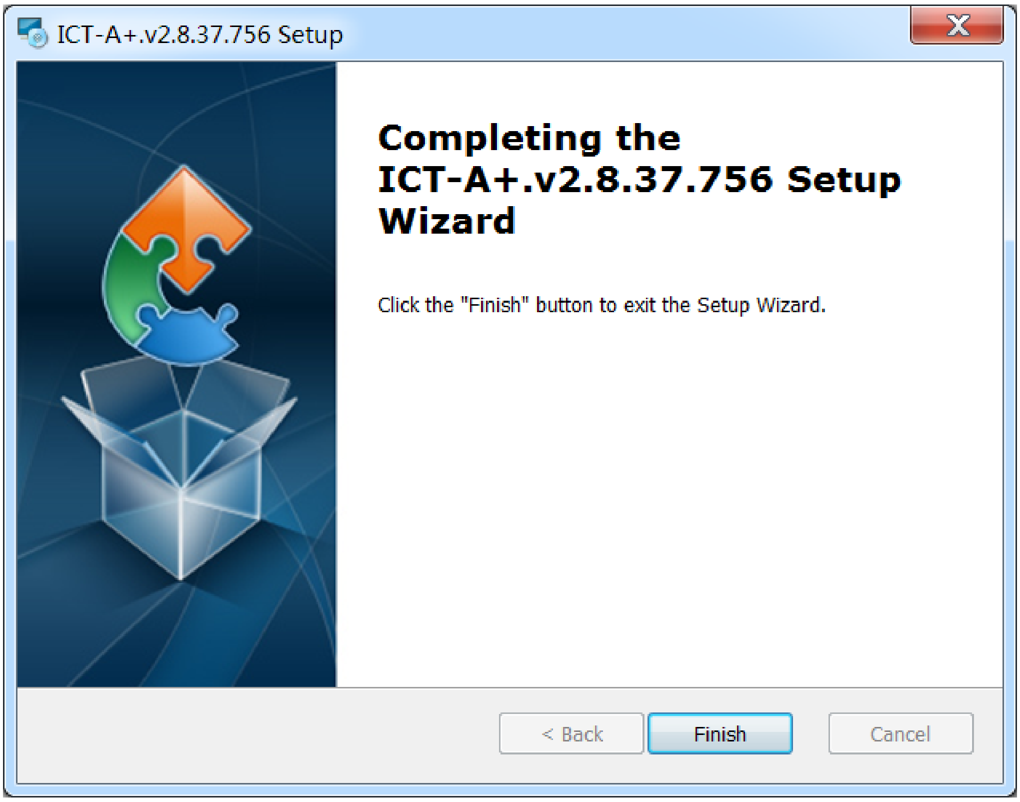
The Setup Wizard is ready to begin the ICT-A+.v2.8.37.756 installation

Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.

5. The installation progress page is displayed.


ICT-A+.v2.8.37.756 Setup
Installing ICT-A+.v2.8.37.756
Please wait while the Setup Wizard installs ICT-A+.v2.8.37.756. This may take several minutes.
Status: Copying new files
Advanced Installer
< Back
Next >
Cancel

6. After the installation is complete, the system displays the completion wizard page, asking you whether to start the application immediately. Click **Finish**.


ICT-A+.v2.8.37.756 Setup
Completing the ICT-A+.v2.8.37.756 Setup Wizard
Click the "Finish" button to exit the Setup Wizard.
< Back
Finish
Cancel

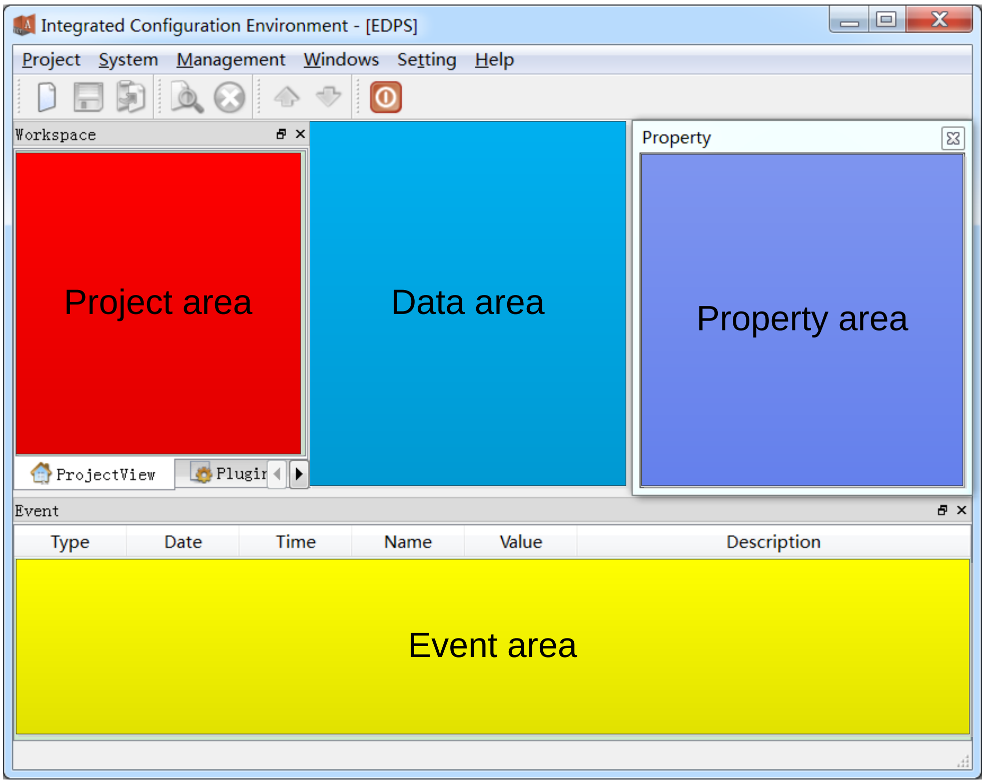
Note: Users can run the setup program again to uninstall or fix the program after

successful installation.

4.1.3.Screen Layout

You must get familiar with the overall layout of the software before use. Each layout structure can implement multiple application configuration and operation management functions.

The EDPS ICT-A+ adopts the classical dock window structure. Dock windows are a type of windows that reside in an area of the main window. The dock area of a dock window includes the east, west, south, and north areas. A dock window can be docked, floated, displayed, hidden, or closed independently. Dock windows deliver a visual effect of stereoscopic shock to users and allow users to perform independent operations within their ranges.



Menu bar	Provides basic menu operation functions of a window.
Tool bar	Provides basic toolbar operation functions of a window.
Project area	Area for managing project data
Data area	Basic area for displaying data

Property area	Basic area for displaying properties
Event area	Basic area for displaying events

4.2.Protocol Configuration

4.2.1.Modbus Protocol Configuration

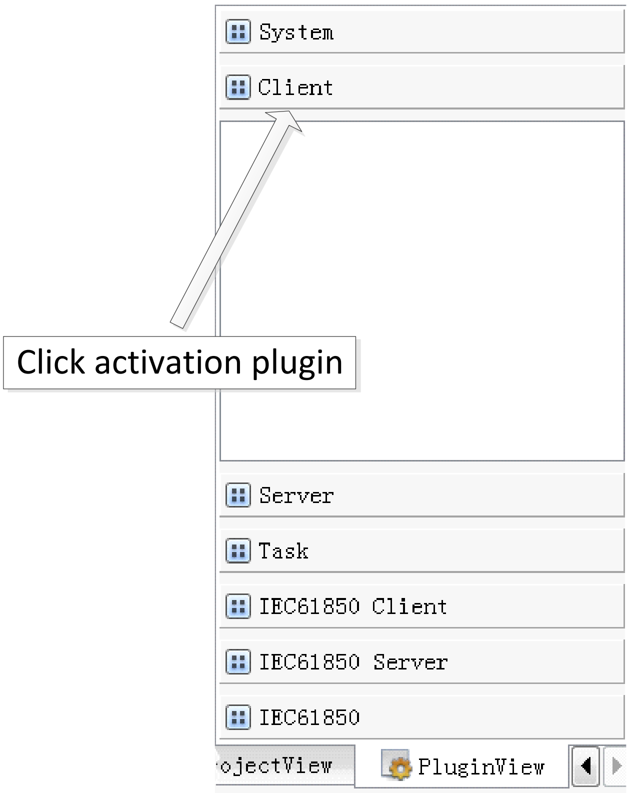
4.2.1.1.Configuration of the Modbus Collection Module

4.2.1.1.1.Driver Information

Overview Describe the detailed configuration of the collection driver.

Create Create a Modbus collection driver.

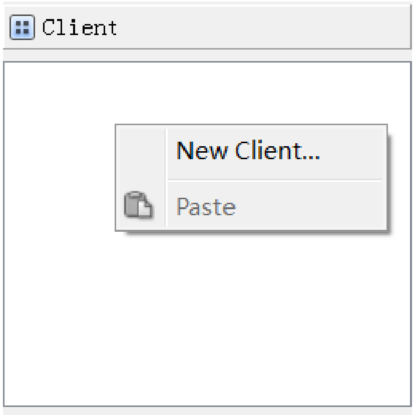
1. Open a project file.
2. Click the **PluginView** tab in the EDPS ICT-A+ management area.
3. Activate the collection service plugin.



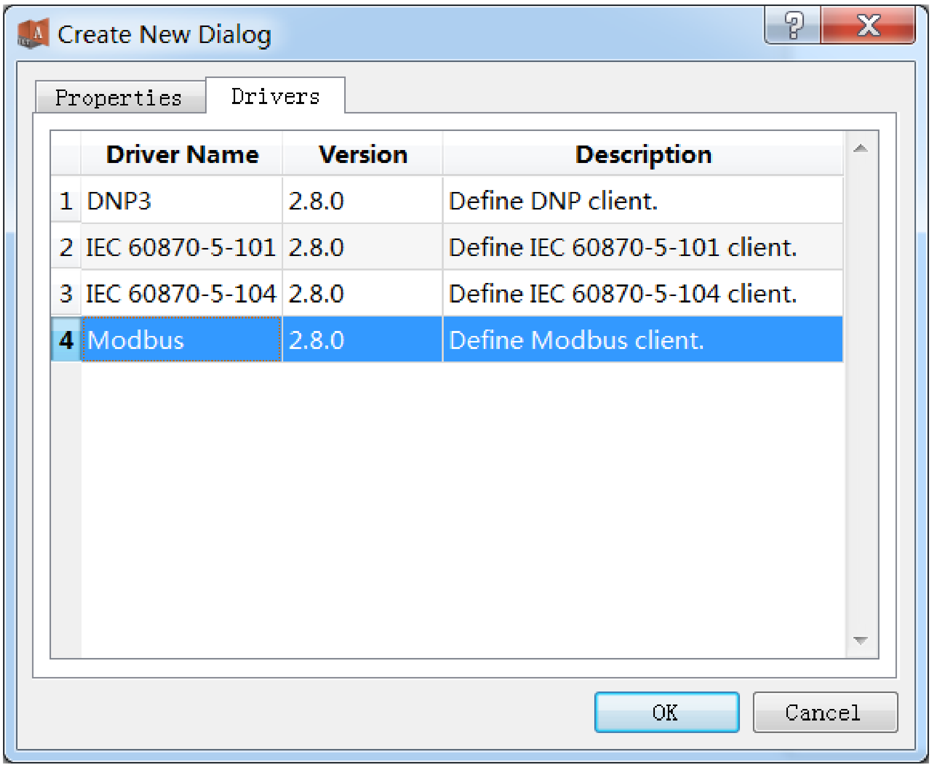
Click activation plugin

4. Right-click in the blank area and choose **New Client** from the shortcut menu. The driver

creation dialog box is displayed.

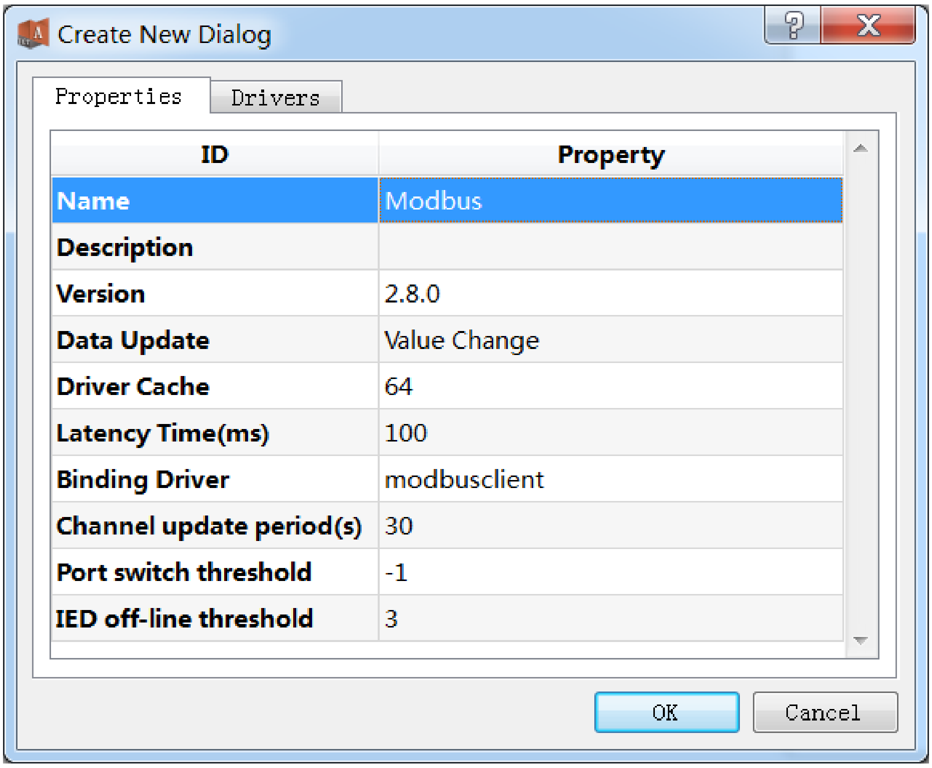


5. On the **Drivers** tab page, select the driver to be created.



	Driver Name	Version	Description
1	DNP3	2.8.0	Define DNP client.
2	IEC 60870-5-101	2.8.0	Define IEC 60870-5-101 client.
3	IEC 60870-5-104	2.8.0	Define IEC 60870-5-104 client.
4	Modbus	2.8.0	Define Modbus client.

6. On the **Properties** tab page, configure basic properties for the target driver.



ID	Property
Name	Modbus
Description	
Version	2.8.0
Data Update	Value Change
Driver Cache	64
Latency Time(ms)	100
Binding Driver	modbusclient
Channel update period(s)	30
Port switch threshold	-1
IED off-line threshold	3

7. Click **OK**.

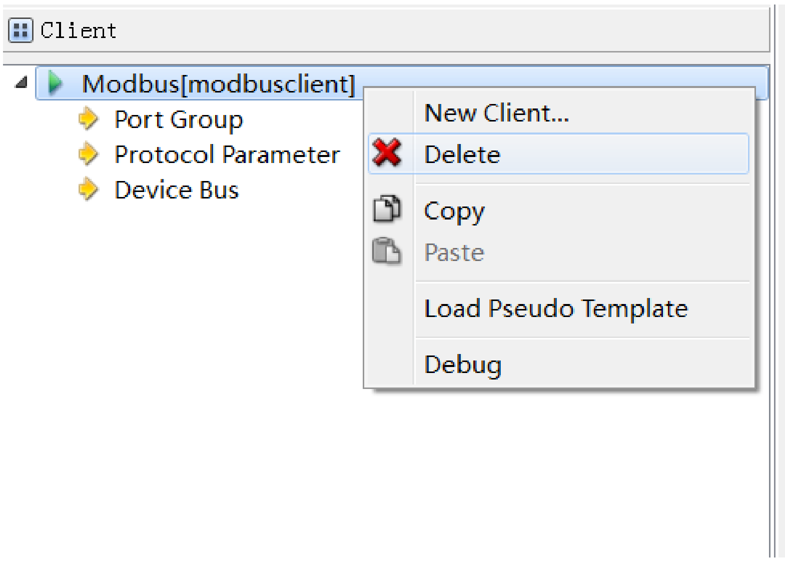
Note: Driver information

No.	Name	**Description**
1	Name	Driver name to be displayed
2	Description	Driver description
3	Version	Driver version
4	Data Update	Data update mode Value Change: The database is updated and other driver protocols are notified only when the value changes. Time Change: The value or time is updated into the database and other driver protocols are notified whenever the value or time changes. Time Update: The value or time is updated whenever it changes, and other driver protocols are notified only when the value changes.
5	Driver Cache	Cache size of the driver

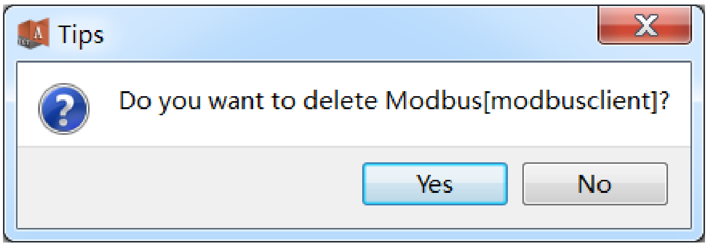
No.	Name	Description
6	Latency Time(ms)	Latency for updating the real-time database The system writes raw data into the real-time database only after the latency time.
7	Binding Driver	Name of the driver module. The value is unique and cannot be modified.
8	Channel update period(s)	Period for updating the IED communication times
9	Port switch threshold	Conditions for multi-port switching. When the number of consecutive communication failures of the master port reaches this threshold, the system switches to another port. The value **-1** indicates that port switching is not performed.
10	IED off-line threshold	IED off-line threshold. When the number of communication failures of a device reaches this threshold, the device is set to be in the off-line state.

Delete Delete a Modbus collection driver.

8. Right-click the collection driver to be deleted and choose **Delete** from the shortcut menu.



9. A dialog box is displayed, asking you whether to delete the driver.

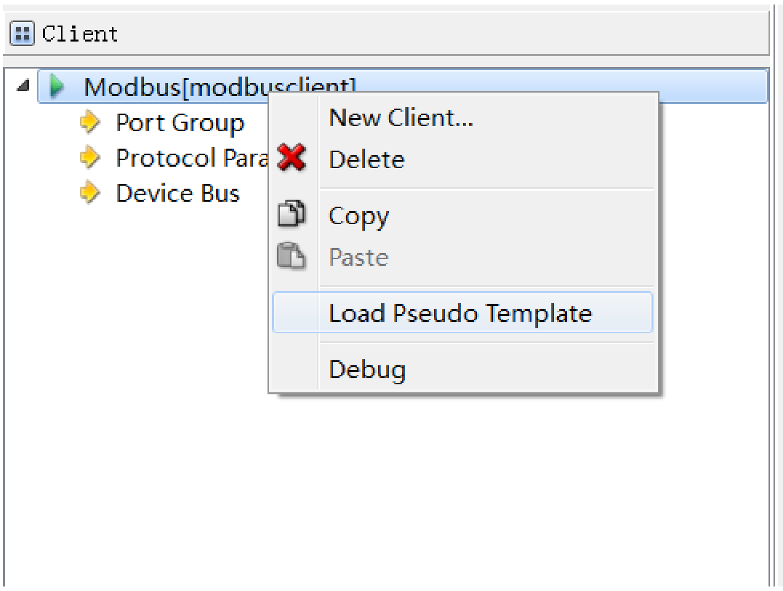


Do you want to delete Modbus[modbusclient]?

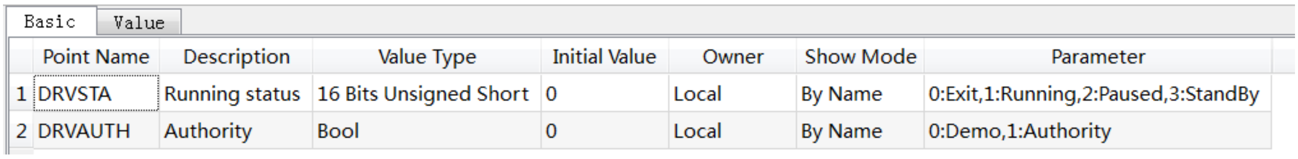
10. Click **Yes** to complete deletion.

Pseudo Template Load a pseudo template from the system template library to the driver.

11. Right-click the driver bar and choose **Load Pseudo Template** from the shortcut menu, to load a pseudo template to the driver.



Note:



	Point Name	Description	Value Type	Initial Value	Owner	Show Mode	Parameter
1	DRVSTA	Running status	16 Bits Unsigned Short	0	Local	By Name	0:Exit,1:Running,2:Paused,3:StandBy
2	DRVAUTH	Authority	Bool	0	Local	By Name	0:Demo,1:Authority

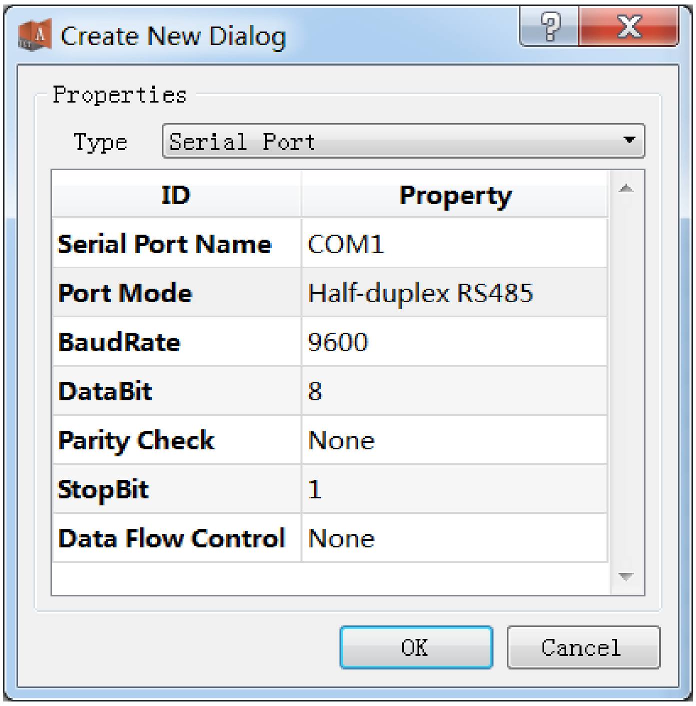
No.	Name	Description
1	DRVSTA	Running status information about the driver
2	DRVAUTH	Authority status of the driver

4.2.1.1.2.Port Group Information

Overview Describe the configuration of a communication channel.

Create Create a communication channel.

1. Right-click **Port Group** and choose **Create** from the shortcut menu. The port creation dialog box is displayed.



Type: Serial Port

ID	Property
Serial Port Name	COM1
Port Mode	Half-duplex RS485
BaudRate	9600
DataBit	8
Parity Check	None
StopBit	1
Data Flow Control	None

2. Select **Serial Port** or **Network Port** as required.

Note: Properties of a serial channel

No.	Name	Description
1	Serial Port Name	Name of a serial port
2	Port Mode	Work mode of the serial port
3	BaudRate	Baud rate of the serial port
4	DataBit	Data bit of the serial port
5	Parity Check	Parity bit of the serial port
6	StopBit	Stop bit of the serial port
7	Data Flow Control	Data flow control mode of the serial port

Properties of a network channel

No.	Name	Description
1	Port Mode	Work mode of a network port
2	Service IP	IP address of the TCP server or UDP destination address
3	Port Number	Work port number of the network port

4	Broadcast Address	Broadcast address of the network port

Delete Delete a communication channel.

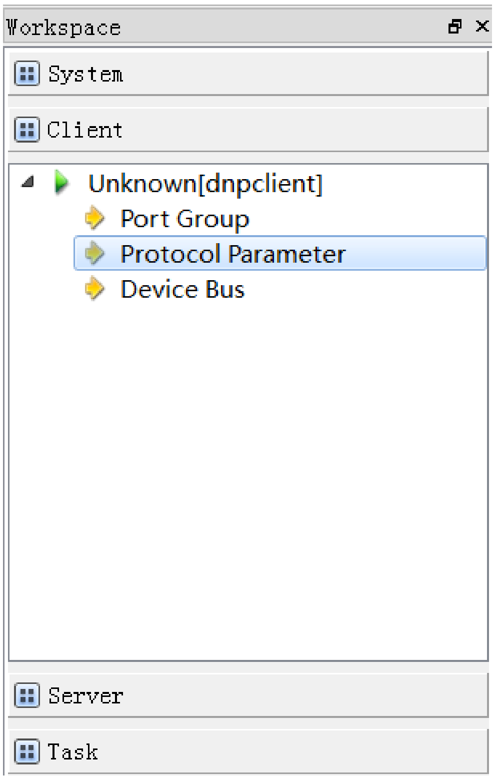
Right-click a channel and choose **Delete** from the shortcut menu. Click **Yes** to complete the deletion.

4.2.1.1.3.Protocol Parameters

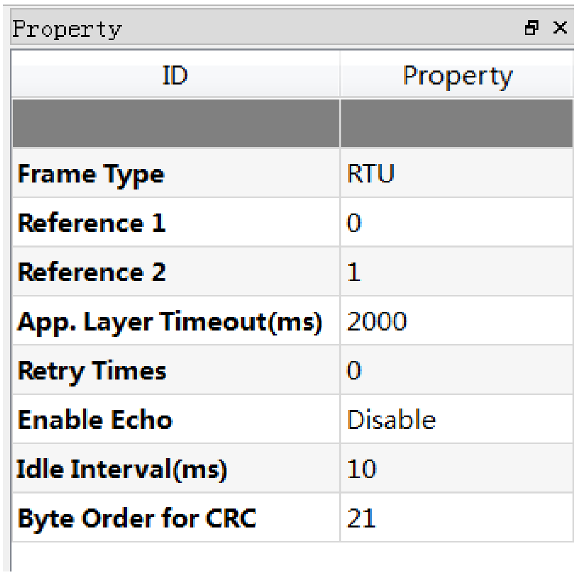
Overview Define the communication protocol parameters of the protocol.

Properties Display the properties of the protocol parameters on the EDPS ICT-A+.

1. Open a project and click the **PluginView** tab in the EDPS ICT-A+ management area.
2. Activate the collection service plugin.
3. Select **Protocol Parameter** in the management area.



4. View the properties of the protocol parameters.



Property

ID	Property
Frame Type	RTU
Reference 1	0
Reference 2	1
App. Layer Timeout(ms)	2000
Retry Times	0
Enable Echo	Disable
Idle Interval(ms)	10
Byte Order for CRC	21

Note: Protocol parameters

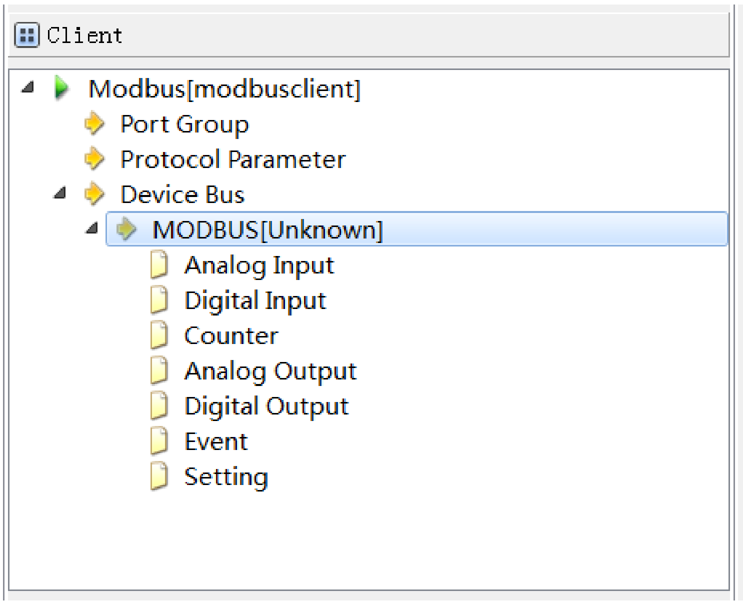
No.	Name	Description
1	Frame Type	Format of communication data frames
2	Reference 1	First reference parameter of the TCP frame type
3	Reference 2	Second reference parameter of the TCP frame type
4	App. Layer Timeout(ms)	Timeout interval for the application-layer response. The unit is milliseconds.
5	Retry Times	Number of times that request data is sent when no valid data is received at the application layer within the allowed time
6	Enable Echo	Whether to check the validity of echo data
7	Idle Interval (ms)	Idle communication interval. The unit is milliseconds.
8	Byte Order for CRC	Byte order of the CRC check code

4.2.1.1.4.Device Parameters

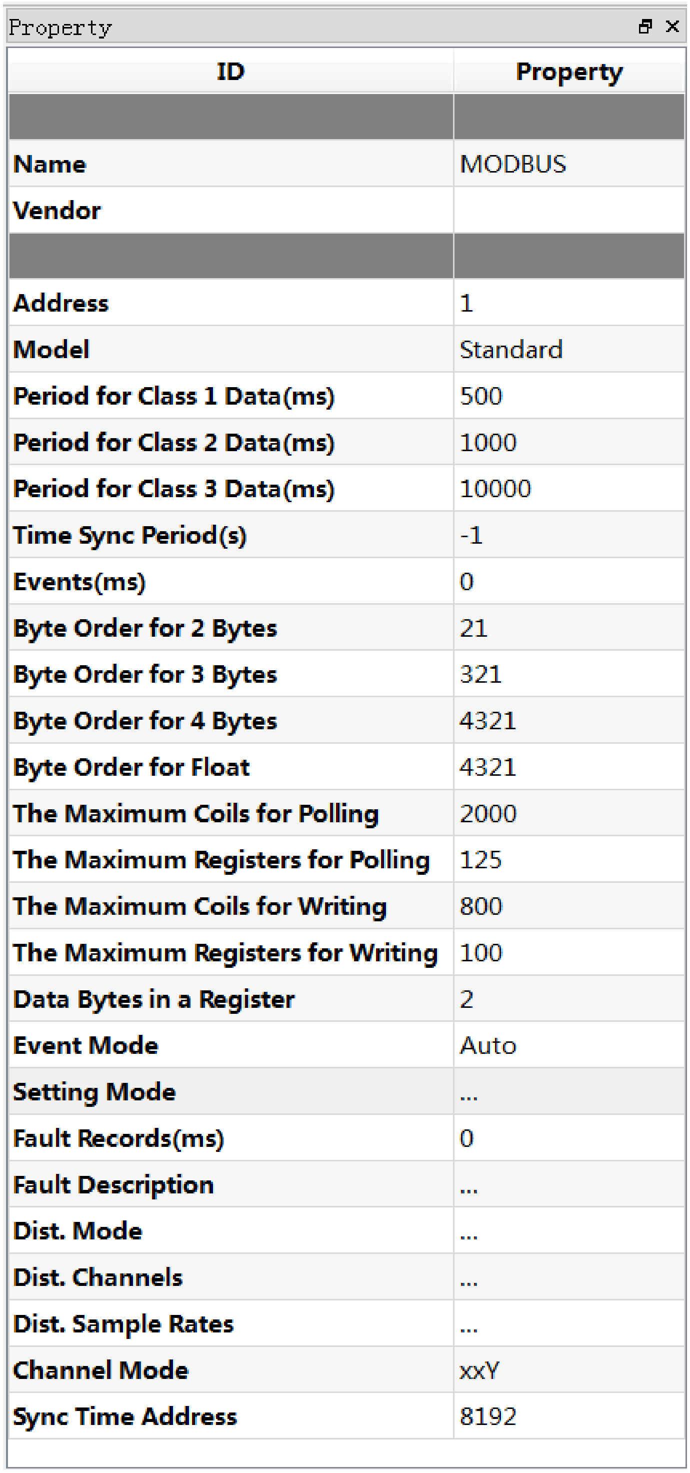
Overview Define the device parameters of the protocol.

Properties Display the properties of the device parameters.

1. Open a project and click the **PluginView** tab in the EDPS ICT-A+ management area.
2. Activate the collection service plugin.
3. Select any subnode under **Device Bus** in the management area.



4. View the property area of the EDPS ICT-A+.



Property

ID	Property
Name	MODBUS
Vendor	
Address	1
Model	Standard
Period for Class 1 Data(ms)	500
Period for Class 2 Data(ms)	1000
Period for Class 3 Data(ms)	10000
Time Sync Period(s)	-1
Events(ms)	0
Byte Order for 2 Bytes	21
Byte Order for 3 Bytes	321
Byte Order for 4 Bytes	4321
Byte Order for Float	4321
The Maximum Coils for Polling	2000
The Maximum Registers for Polling	125
The Maximum Coils for Writing	800
The Maximum Registers for Writing	100
Data Bytes in a Register	2
Event Mode	Auto
Setting Mode	...
Fault Records(ms)	0
Fault Description	...
Dist. Mode	...
Dist. Channels	...
Dist. Sample Rates	...
Channel Mode	xxY
Sync Time Address	8192

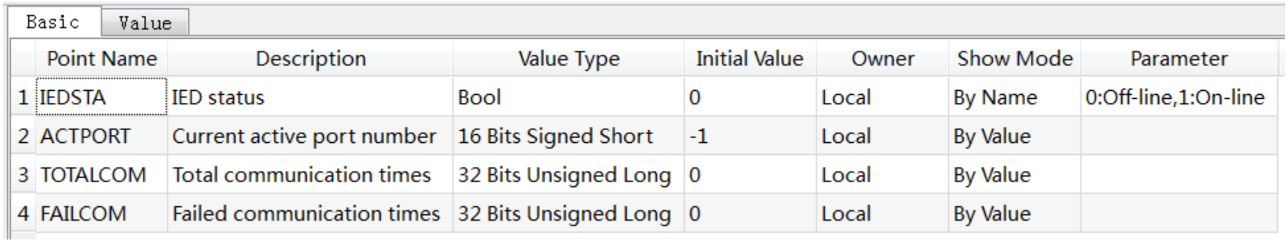
Note: Device properties

No.	Name	Description
1	Name	Device name
2	Vendor	Device vendor
3	Address	Device address

No.	Name	Description
4	Model	Device model ● Standard ● AREVA Px2x ● AREVA Px3x ● AREVA Px4x ● WIT Mx
5	Period for Class 1 Data(ms)	Period for querying class 1 data. The unit is milliseconds.
6	Period for Class 2 Data(ms)	Period for querying class 2 data. The unit is milliseconds.
7	Period for Class 3 Data(ms)	Period for querying class 3 data. The unit is milliseconds.
8	Time Sync Period(s)	Time synchronization period of the device. The unit is seconds.
9	Events(ms)	Event reading period of the device. The unit is milliseconds. Min: 0 ms Max: 3,600,000 ms
10	Byte Order for 2 Bytes	Byte order of two bytes of the device
11	Byte Order for 3 Bytes	Byte order of three bytes of the device
12	Byte Order for 4 Bytes	Byte order of four bytes of the device
13	Byte Order for Float	Byte order of floating-point bytes
14	The Maximum Coils for Polling	Maximum number of coils for query
15	The Maximum Registers for Polling	Maximum number of registers for query
16	The Maximum Coils	Maximum number of coils for writing

No.	Name	Description
	for Writing	
17	The Maximum Registers for Writing	Maximum number of registers for query
18	Data Bytes in a Register	Number of bytes occupied by each register
19	Event Mode	Event confirmation mode. It is valid only to AREVA Series 2 devices.
20	Setting Mode	Setting processing mode
21	Fault Records(ms)	Period of device fault detection. The unit is milliseconds.
22	Fault Description	Device fault description, which should be IEEE-standardized.
23	Dist. Mode	Processing mode of disturbance data
24	Dist. Channels	Channel information about device disturbance data
25	Dist. Sample Rates	Sampling rate of device disturbance data
26	Channel Mode	Channel read mode. It is available only to AREVA Series 2 devices.

Properties of a Pseudo Point View the data area of the EDPS ICT-A+.



	Point Name	Description	Value Type	Initial Value	Owner	Show Mode	Parameter
1	IEDSTA	IED status	Bool	0	Local	By Name	0:Off-line,1:On-line
2	ACTPORT	Current active port number	16 Bits Signed Short	-1	Local	By Value	
3	TOTALCOM	Total communication times	32 Bits Unsigned Long	0	Local	By Value	
4	FAILCOM	Failed communication times	32 Bits Unsigned Long	0	Local	By Value	

No.	Name	Description
1	IED status	Communication status of the current device. The value shows whether the device is on-line or off-line.

2	Current active port number	Port used by the current channel for communication. For a multi-port link, the value helps locate the active port easily.
3	Total communication times	Total number of communications
4	Failed communication times	Number of failed communications. A communication failure means data is not transmitted successfully or data is received incorrectly.

4.2.1.1.5.IO Parameters

Overview The IO information page in the data area of the EDPS ICT-A+ displays IO parameters of each information point. The system, based on parameter settings, conducts accurate boundary test and data check for IO parameters of each type of data, so as to effectively reduce the configuration data error rate during data input.

1) Analog input

Function Code Function code for reading an information point

- 3 - Holding Register
- 4 - Input Register

Address Address of the information point register

Start Priority Byte start position of the current information point in the register

Priority Processing priority of the information point

- Class 1 data
- Class 2 data
- Class 3 data

Data Length Data length of the information point in the register

Value Type Type of values in the register

- Discrete

- Integer
- Unsigned integer
- Floating point

2) Status input

Function Code Function code for reading an information point

- 1 - Coil Status
- 2 - Input Status
- 3 - Holding Register
- 4 - Input Register
- 7 - Exception Status

Address Address of the information point register

Start Byte Byte start position of the current information point in the register

Priority Processing priority of the information point

- Class 1 data
- Class 2 data
- Class 3 data

3) Counter input

Function Code Function code for reading an information point

- 3 - Holding Register
- 4 - Input Register

Address Address of the information point register

Start Byte Byte start position of the current information point in the register

Priority Processing priority of the information point

- Class 1 data
- Class 2 data
- Class 3 data

Data Length Data length of the information point in the register

Value Type Type of values in the register

- Discrete
- Integer
- Unsigned integer
- Floating point

4) Analog output

Function Code Function code for reading an information point

- 3 - Holding Register
- 4 - Input Register

Address Address of the information point register

Start Byte Byte start position of the current information point in the register

Priority Processing priority of the information point

- Class 1 data
- Class 2 data
- Class 3 data

Data Length Data length of the information point in the register

Value Type Type of values in the register

- Discrete
- Integer
- Unsigned integer
- Floating point

Write Function Code Function code for writing data to an information point

- 6 - Preset Register
- 16 - Preset Multiple Registers

5) Status output

Function Code Function code for reading an information point

- 5 - Force Coil
- 15 - Force Multiple Coils

- 6 - Preset Register
- 10 - Preset Multiple Register

Address Address of the information point register

Start Byte Byte start position of the current information point in the register

Pulse Count Number of pulse outputs. It is available when the control mode is pulse mode.

High Level Time Duration of the rising edge in pulse output mode

Low Level Time Duration of the falling edge in pulse output mode

Trip Value Substitute numeric in the execution of a trip command

Close Value Substitute numeric in the execution of a close command

6) Events

Event Code Event code. It is used for retrieving event information.

7) Setting

Function Code Function code for reading an information point

- 3 - Holding Register
- 4 - Input Register

Address Address of the register

Start Byte Byte start position of the current information point in the register

Data Length Data length of the information point

Value Type Data length of the information point

- Discrete
- Integer
- Unsigned integer
- Floating point

Write Function Code Function code for writing data to an information point

- 6 - Force Register

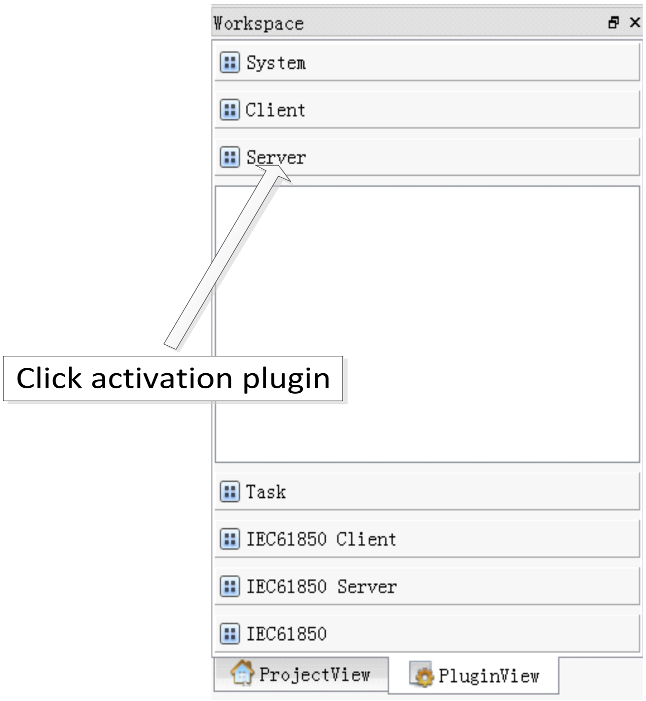
4.2.1.2.Configuration of the Modbus Forwarding Module

4.2.1.2.1.Driver Information

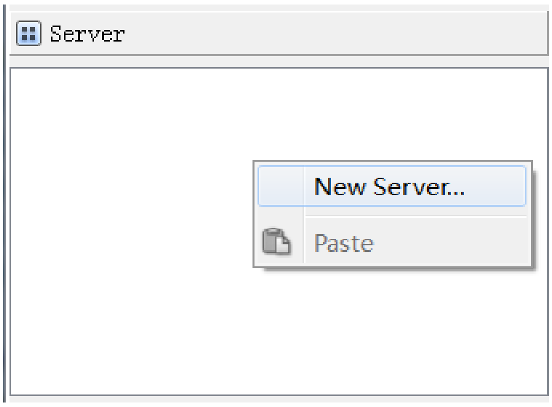
Overview Describe the detailed configuration of the forwarding driver.

Create Create a Modbus forwarding driver.

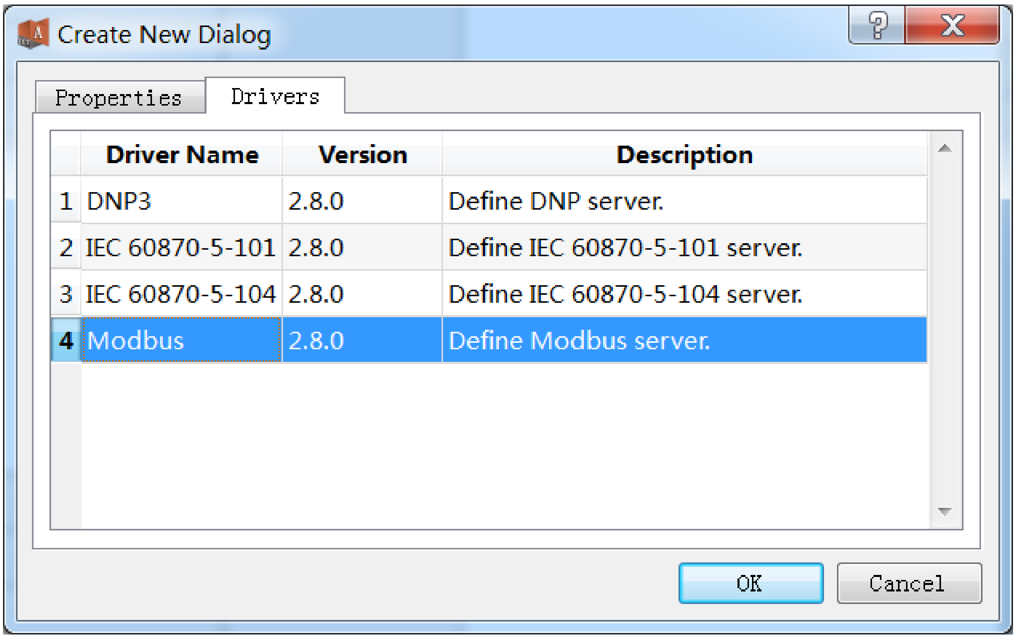
1. Open a project file.
2. Click the **PluginView** tab in the EDPS ICT-A+ management area.
3. Activate the forwarding service plugin.



4. Right-click in the blank area and choose **New Server** from the shortcut menu. The driver creation dialog box is displayed.

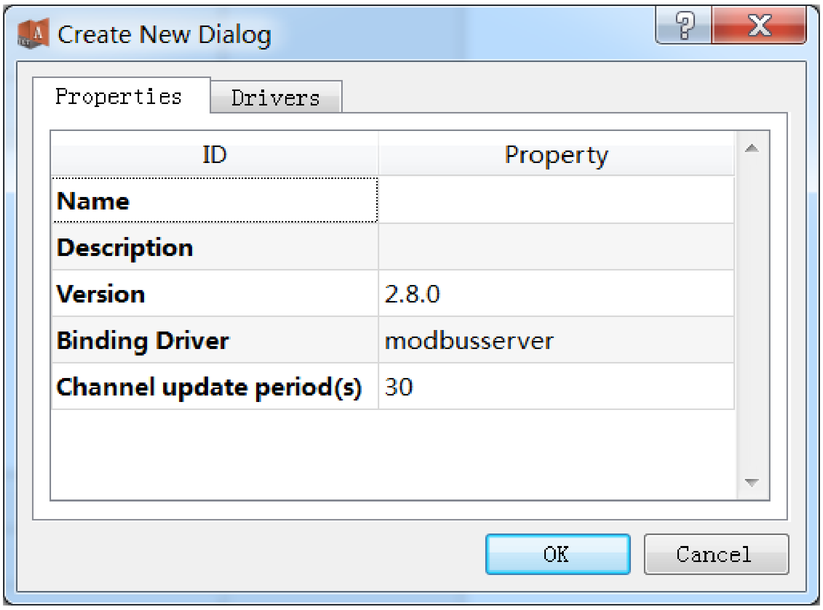


5. On the **Drivers** tab page, select the driver to be created.



	Driver Name	Version	Description
1	DNP3	2.8.0	Define DNP server.
2	IEC 60870-5-101	2.8.0	Define IEC 60870-5-101 server.
3	IEC 60870-5-104	2.8.0	Define IEC 60870-5-104 server.
4	Modbus	2.8.0	Define Modbus server.

6. On the **Properties** tab page, configure basic properties for the target driver.



ID	Property
Name	
Description	
Version	2.8.0
Binding Driver	modbusserver
Channel update period(s)	30

7. Click **OK**.

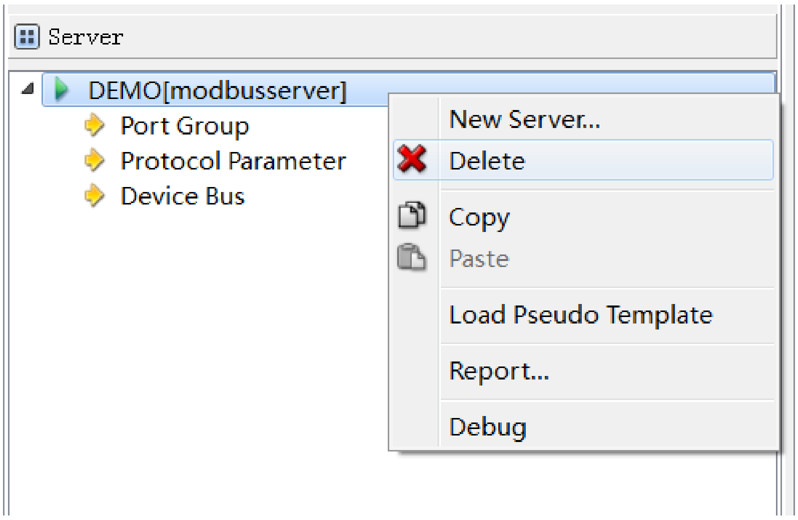
Note: Driver information

No.	Name	Description
1	Name	Driver name to be displayed
2	Description	Driver description
3	Version	Driver version
4	Binding Driver	Name of the driver module. The value is unique

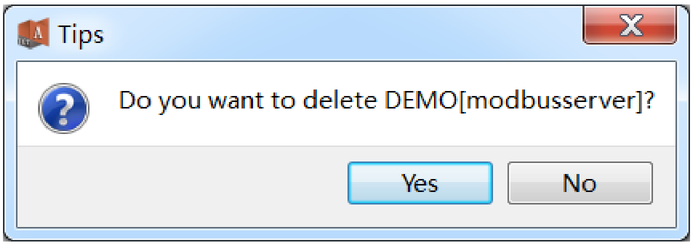
No.	Name	Description
		and cannot be modified.
5	Channel update period(s)	Period for updating the IED communication times

Delete Delete a Modbus forwarding driver.

8. Right-click the driver to be deleted and choose **Delete** from the shortcut menu.



9. A dialog box is displayed, asking you whether to delete the driver.

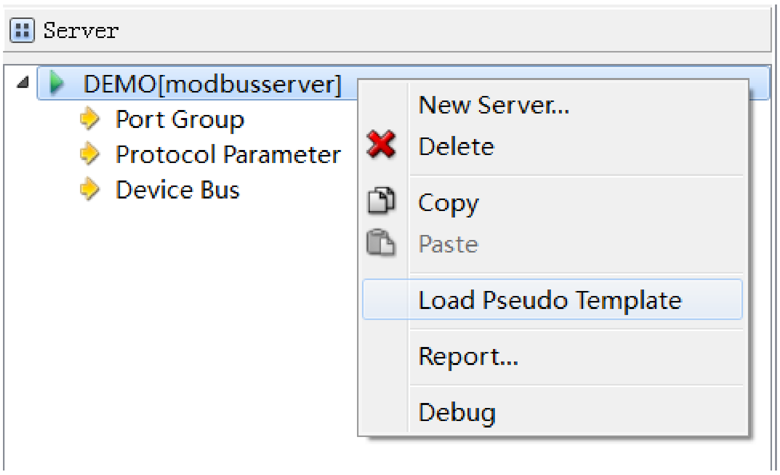


Do you want to delete DEMO[modbusserver]?

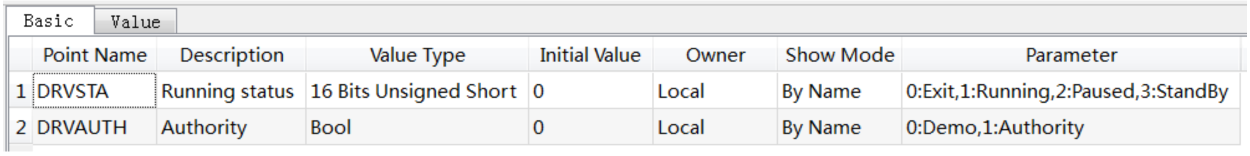
10. Click **Yes** to complete deletion.

Pseudo Template Load a pseudo template from the system template library to the driver.

11. Right-click the driver bar and choose **Load Pseudo Template** from the shortcut menu, to load a pseudo template to the driver.



Note:



	Point Name	Description	Value Type	Initial Value	Owner	Show Mode	Parameter
1	DRVSTA	Running status	16 Bits Unsigned Short	0	Local	By Name	0:Exit,1:Running,2:Paused,3:StandBy
2	DRVAUTH	Authority	Bool	0	Local	By Name	0:Demo,1:Authority

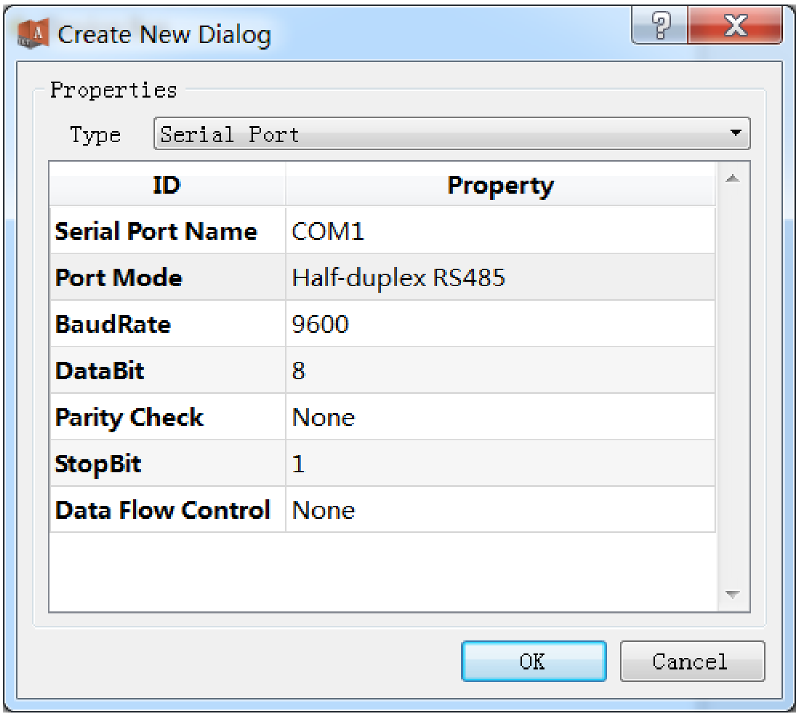
No.	Name	Description
1	Running status	Running status information about the driver
2	Authority	Authority status of the driver

4.2.1.2.2.Port Group Information

Overview Describe a communication channel.

Create Create a communication channel.

1. Right-click **Port Group** and choose **Create** from the shortcut menu. The port creation dialog box is displayed.



Type: Serial Port

ID	Property
Serial Port Name	COM1
Port Mode	Half-duplex RS485
BaudRate	9600
DataBit	8
Parity Check	None
StopBit	1
Data Flow Control	None

2. Select **Serial Port** or **Network Port** as required.

Note: Properties of a serial channel

No.	Name	Description
1	Serial Port Name	Name of a serial port
2	Port Mode	Work mode of the serial port
3	BaudRate	Baud rate of the serial port
4	DataBit	Data bit of the serial port
5	Parity Check	Parity bit of the serial port
6	StopBit	Stop bit of the serial port
7	Data Flow Control	Data flow control mode of the serial port

Properties of a network channel

No.	Name	Description
1	Port Mode	Work mode of a network port
2	Service IP	IP address of the TCP server or UDP destination address
3	Port Number	Work port number of the network port
4	Broadcast Address	Broadcast address of the network port

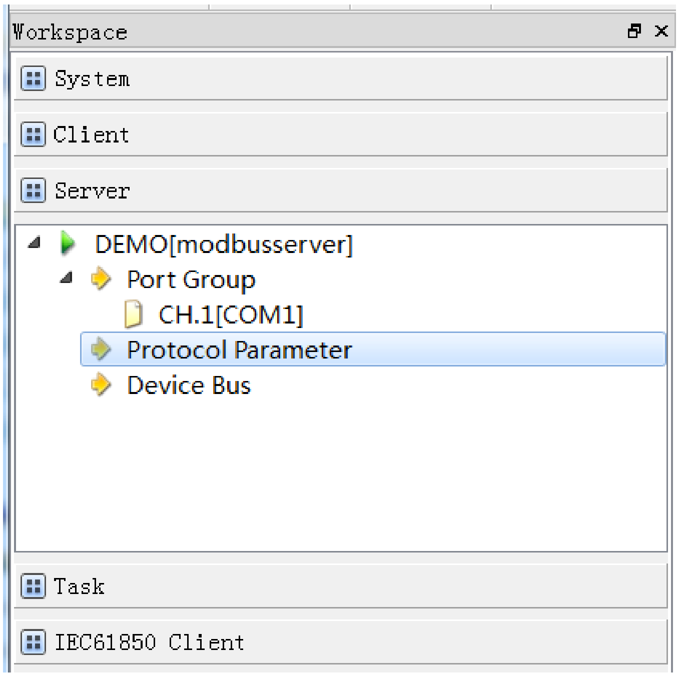
Delete Delete a communication channel.

3. Right-click a channel and choose **Delete** from the shortcut menu. Click **Yes** to complete the deletion.

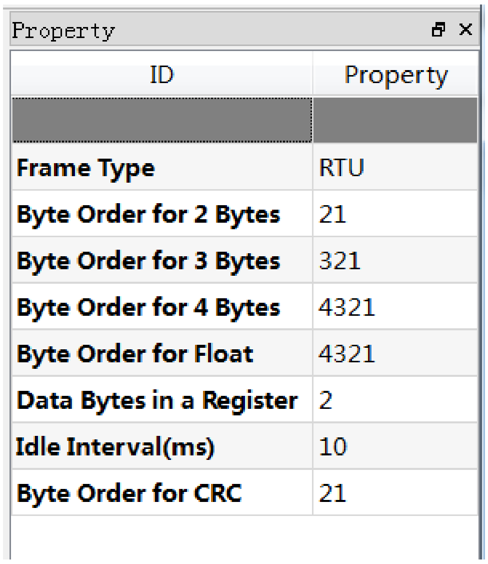
4.2.1.2.3.Protocol Parameters

Overview Define the communication protocol parameters of the protocol.

1. Open a project and click the **PluginView** tab in the EDPS ICT-A+ management area.
2. Activate the forwarding service plugin.
3. Select **Protocol Parameter** in the management area.



4. View the properties of the protocol parameters.



ID	Property
Frame Type	RTU
Byte Order for 2 Bytes	21
Byte Order for 3 Bytes	321
Byte Order for 4 Bytes	4321
Byte Order for Float	4321
Data Bytes in a Register	2
Idle Interval(ms)	10
Byte Order for CRC	21

Note: Protocol parameters

No.	Name	Description
1	Frame Type	Format of communication data frames
2	Byte Order for 2 Bytes	Byte order of two bytes of the device
3	Byte Order for 3 Bytes	Byte order of three bytes of the device
4	Byte Order for 4 Bytes	Byte order of four bytes of the device
5	Byte Order for Float	Byte order of floating-point numbers of the device
6	Data Bytes in a Register	Number of bytes occupied by each register
7	Idle Interval(ms)	Idle communication interval. The unit is milliseconds.
8	Byte Order for CRC	Byte order of the CRC check code

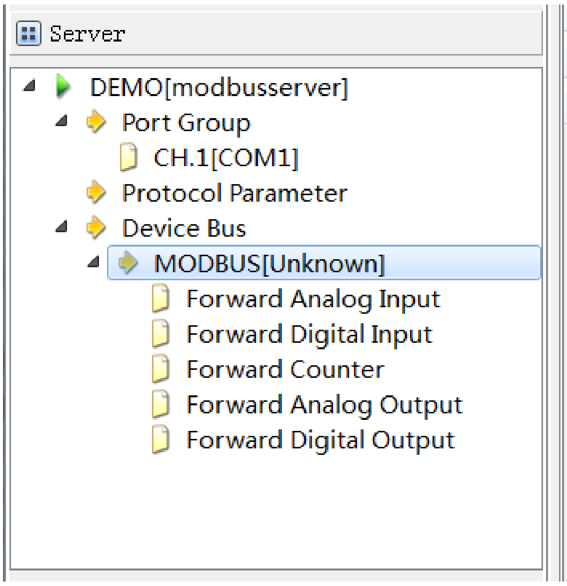
4.2.1.2.4.Device Parameters

Overview Define the device parameters of the protocol.

Properties Display the properties of the device parameters.

1. Open a project and click the **PluginView** tab in the EDPS ICT-A+ management area.
2. Activate the forwarding service plugin.

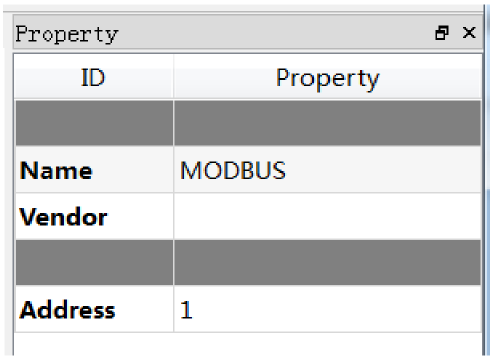
3. Select any subnode under **Device Bus** in the management area.



Server

- DEMO[modbusserver]
  - Port Group
    - CH.1[COM1]
  - Protocol Parameter
  - Device Bus
    - MODBUS[Unknown]
      - Forward Analog Input
      - Forward Digital Input
      - Forward Counter
      - Forward Analog Output
      - Forward Digital Output

4. View the property area of the EDPS ICT-A+.



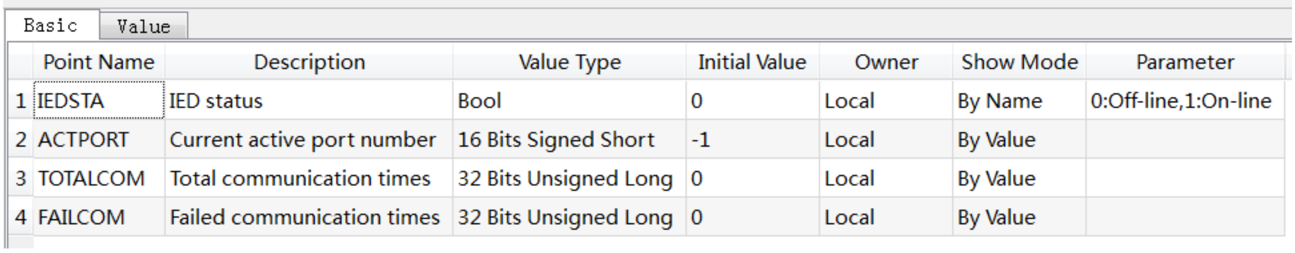
Property

ID	Property
Name	MODBUS
Vendor	
Address	1

Note: Device properties

No.	Name	Description
1	Name	Device name
2	Vendor	Device vendor
3	Address	Device address

Properties of a Pseudo Point View the data area of the EDPS ICT-A+.



	Point Name	Description	Value Type	Initial Value	Owner	Show Mode	Parameter
1	IEDSTA	IED status	Bool	0	Local	By Name	0:Off-line,1:On-line
2	ACTPORT	Current active port number	16 Bits Signed Short	-1	Local	By Value	
3	TOTALCOM	Total communication times	32 Bits Unsigned Long	0	Local	By Value	
4	FAILCOM	Failed communication times	32 Bits Unsigned Long	0	Local	By Value	

No.	Name	Description
1	IED STA	Communication status of the current device. The value shows whether the device is on-line or off-line.
2	ACTPORT	Port used by the current channel for communication. For a multi-port link, the value helps locate the active port easily.
3	TOTALCOM	Total number of communications
4	FAILCOM	Number of failed communications. A communication failure means data is not transmitted successfully or data is received incorrectly.

4.2.1.2.5.IO Parameters

Overview The IO information page in the data area of the EDPS ICT-A+ displays IO parameters of each information point. The system, based on parameter settings, conducts accurate boundary test and data check for IO parameters of each type of data, so as to effectively reduce the configuration data error rate during data input.

1) Analog input

Function Code Function code for reading an information point

- 3 - Holding Register
- 4 - Input Register

Address Address of the register

Start Byte Byte start position of the current information point in the register

Data Length Data length

Value Type Type of the data value

- Discrete
- Integer
- Unsigned integer
- Floating point

Offset Offset of the value of the information point

Divisor Division factor required in data changes of the information point

2) Status input

Function Code Function code for reading an information point

- 1 - Coil Status
- 2 - Input Status
- 3 - Holding Register
- 4 - Input Register

Address Address of the information point register

Start Byte Byte start position of the current information point in the register

3) Counter input

Function Code Function code for reading an information point

- 3 - Holding Register
- 4 - Input Register

Address Address of the information point register

Start Byte Byte start position of the current information point in the register

Data Length Data length of the information point in the register

Value Type Type of values in the register

- Discrete
- Integer
- Unsigned integer
- Floating point

Offset Offset of the value of the information point

Divisor Division factor required in data changes of the information point

4) Analog output

Function Code Function code for reading an information point

- 3 - Holding Register
- 4 - Input Register

Address Address of the information point register

Start Byte Byte start position of the current information point in the register

Data Length Data length of the information point in the register

Value Type Type of values in the register

- Discrete
- Integer
- Unsigned integer
- Floating point

Offset Offset of the value of the information point

Divisor Division factor required in data changes of the information point

5) Status output

Function Code Function code for reading an information point

- 5 - Force Coil
- 15 - Force Multiple Coils

Address Address of the information point register

4.2.2.IEC60870-5-101 Protocol Configuration on the Software

This section describes how to configure the IEC60870-5-101 collection and forwarding driver modules on the EDPS ICT-A+. The driver information, protocol parameters, device parameters, and IO parameters of each information point are described in the configuration manual. The IEC60870-5-101 collection and forwarding modules of the EDPS ICT-A+ fully comply with the protocol. The EDPS ICT-A+ provides a simple and fast way to help users complete the configuration.

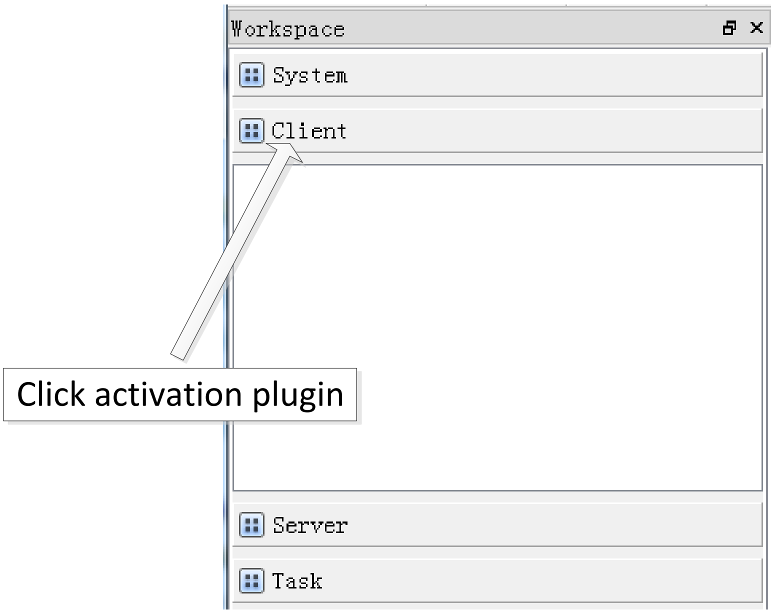
4.2.2.1.Configuration of the IEC60870-5-101 Collection Module

4.2.2.1.1.Driver Information

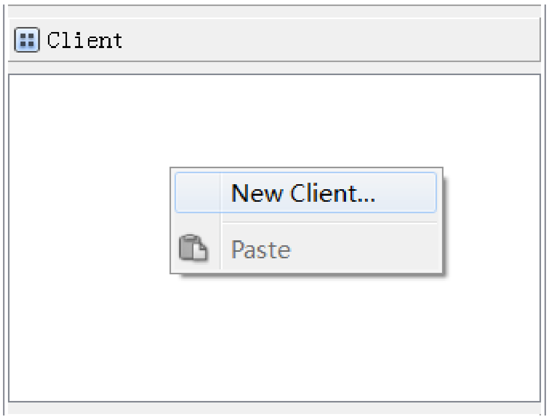
Overview Describe the details about the collection driver.

Create Create an IEC60870-5-101 collection driver.

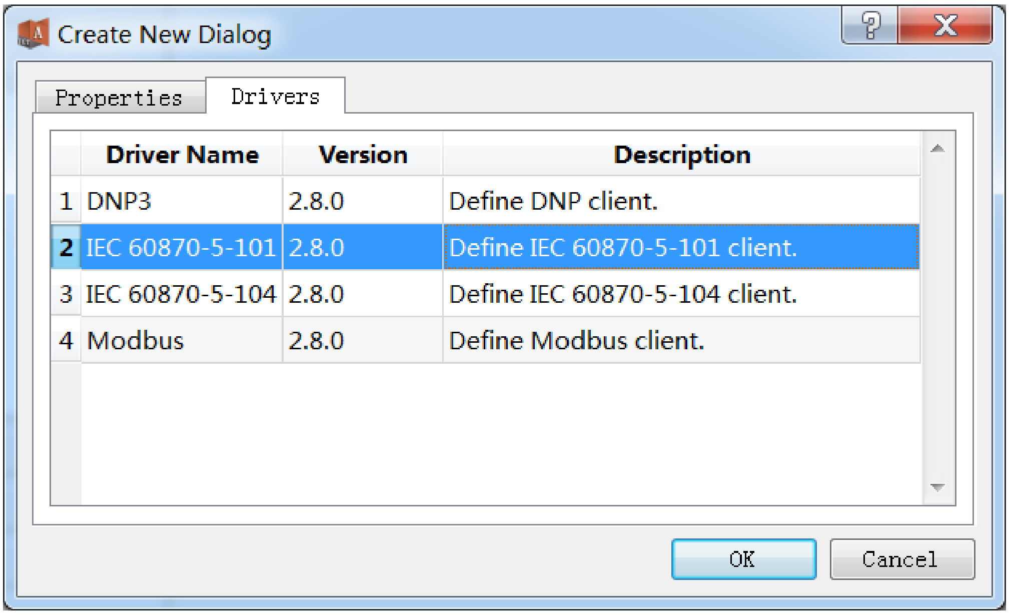
1. Open a project file.
2. Click the **PluginView** tab in the EDPS ICT-A+ management area.
3. Activate the collection service plugin.



4. Right-click in the blank area and choose **New Client** from the shortcut menu. The driver creation dialog box is displayed.

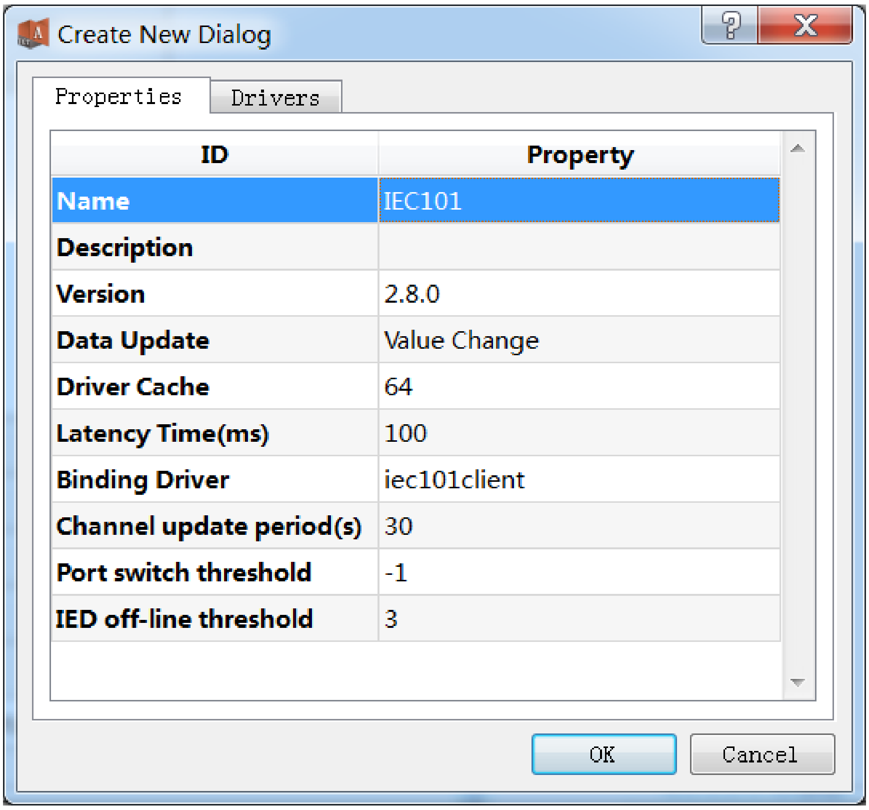


5. On the **Drivers** tab page, select the driver to be created.



	Driver Name	Version	Description
1	DNP3	2.8.0	Define DNP client.
2	IEC 60870-5-101	2.8.0	Define IEC 60870-5-101 client.
3	IEC 60870-5-104	2.8.0	Define IEC 60870-5-104 client.
4	Modbus	2.8.0	Define Modbus client.

6. On the **Properties** tab page, configure basic properties for the target driver.



ID	Property
Name	IEC101
Description	
Version	2.8.0
Data Update	Value Change
Driver Cache	64
Latency Time(ms)	100
Binding Driver	iec101client
Channel update period(s)	30
Port switch threshold	-1
IED off-line threshold	3

7. Click **OK**.

Note: Driver information

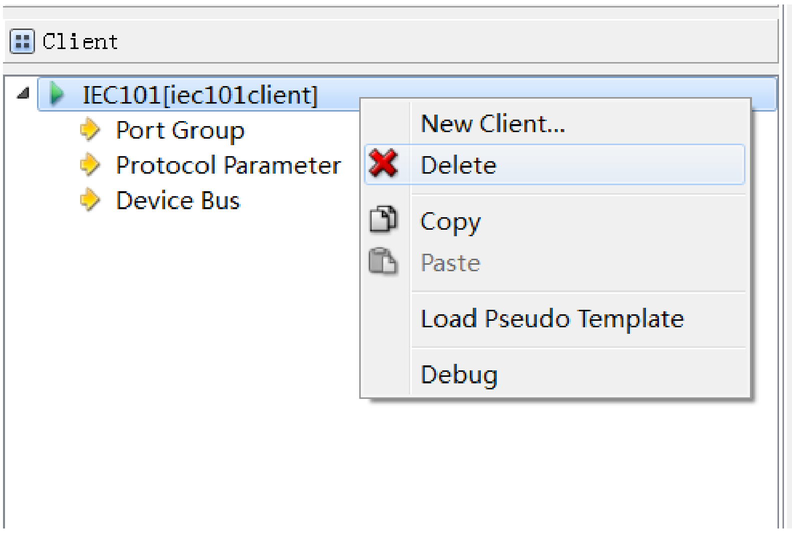
No.	Name	Description
1	Name	Driver name to be displayed
2	Description	Driver description

No.	Name	Description
3	Version	Driver version
4	Data Update	Data update mode Value Change: The database is updated and other driver protocols are notified only when the value changes. Time Change: The value or time is updated into the database and other driver protocols are notified whenever the value or time changes. Time Update: The value or time is updated whenever it changes, and other driver protocols are notified only when the value changes.
5	Driver Cache	Cache size of the driver
6	Latency Time(ms)	Latency for updating the real-time database The system writes raw data into the real-time database only after the latency time.
7	Binding Driver	Name of the driver module. The value is unique and cannot be modified.
8	Channel update period (s)	Period for updating the IED communication times
9	Port switch threshold	Conditions for multi-port switching. When the number of consecutive communication failures of the master port reaches this threshold, the system switches to another port. The value **-1** indicates that port switching is not performed.
10	IED off-line threshold	IED off-line threshold. When the number of communication failures of a device reaches this threshold, the device is set to be in the off-line

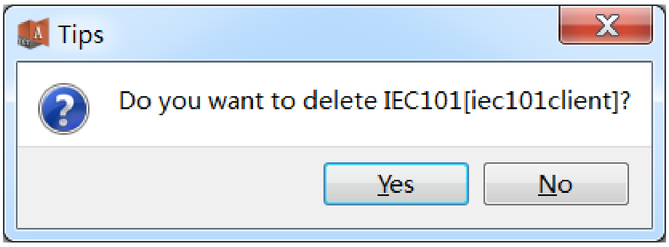
No.	Name	Description
		state.

Delete Delete an IEC60870-5-101 collection driver.

8. Right-click the driver to be deleted and choose **Delete** from the shortcut menu.



9. A dialog box is displayed, asking you whether to delete the driver.

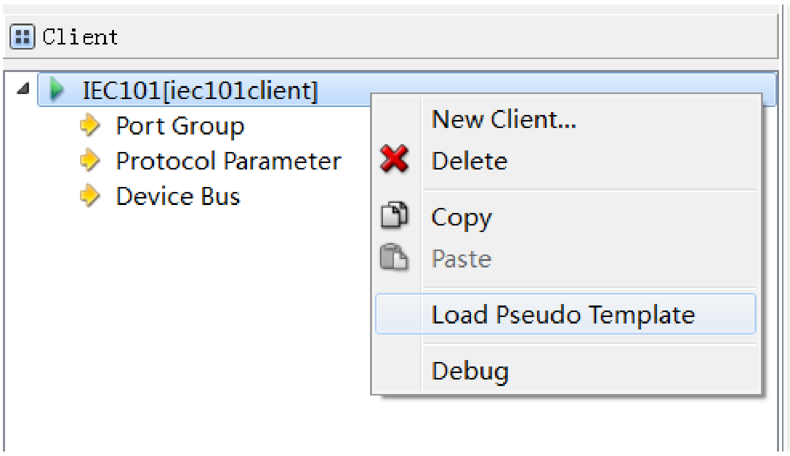


Do you want to delete IEC101[iec101client]?

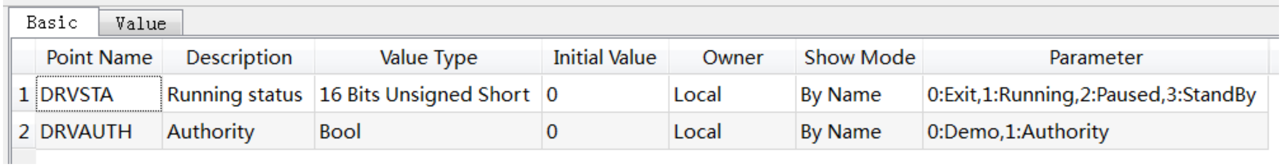
10. Click **Yes** to complete deletion.

Pseudo Template Load a pseudo template from the system template library to the driver.

11. Right-click the driver bar and choose **Load Pseudo Template** from the shortcut menu, to load a pseudo template to the driver.



Note:



	Point Name	Description	Value Type	Initial Value	Owner	Show Mode	Parameter
1	DRVSTA	Running status	16 Bits Unsigned Short	0	Local	By Name	0:Exit,1:Running,2:Paused,3:StandBy
2	DRVAUTH	Authority	Bool	0	Local	By Name	0:Demo,1:Authority

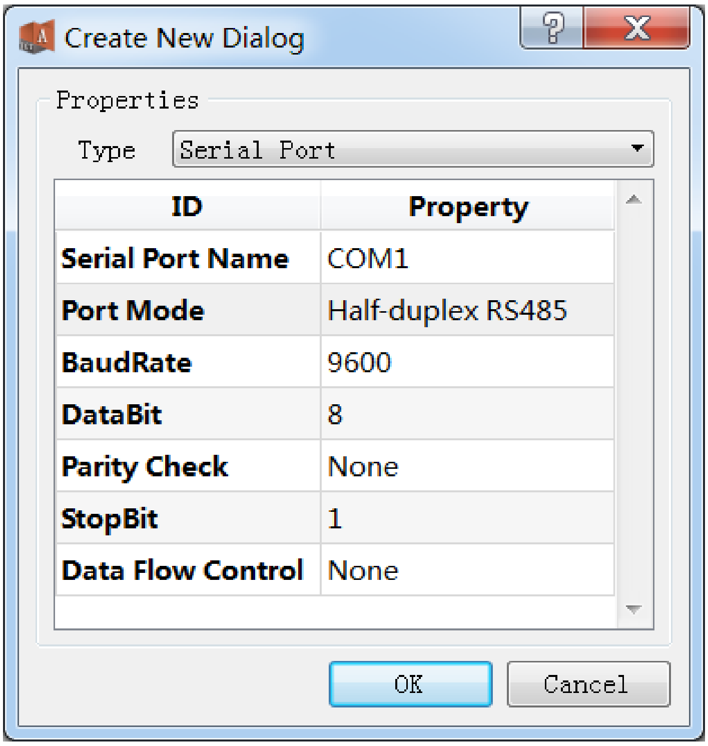
No.	Name	Description
1	DRVSTA	Running status information about the driver
2	DRVAUTH	Authority status of the driver

4.2.2.1.2.Port Group Information

Overview Describe a communication channel.

Create Create a communication channel.

1. Right-click **Port Group** and choose **Create** from the shortcut menu. The port creation dialog box is displayed.
2. Select **Serial Port**.



Type: Serial Port

ID	Property
Serial Port Name	COM1
Port Mode	Half-duplex RS485
BaudRate	9600
DataBit	8
Parity Check	None
StopBit	1
Data Flow Control	None

Note: Properties of a serial channel

No.	Name	Description
1	Serial Port Name	Name of a serial port

No.	Name	Description
2	Port Mode	Work mode of the serial port
3	BaudRate	Baud rate of the serial port
4	DataBit	Data bit of the serial port
5	Parity Check	Parity bit of the serial port
6	StopBit	Stop bit of the serial port
7	Data Flow Control	Data flow control mode of the serial port

Delete Delete a communication channel.

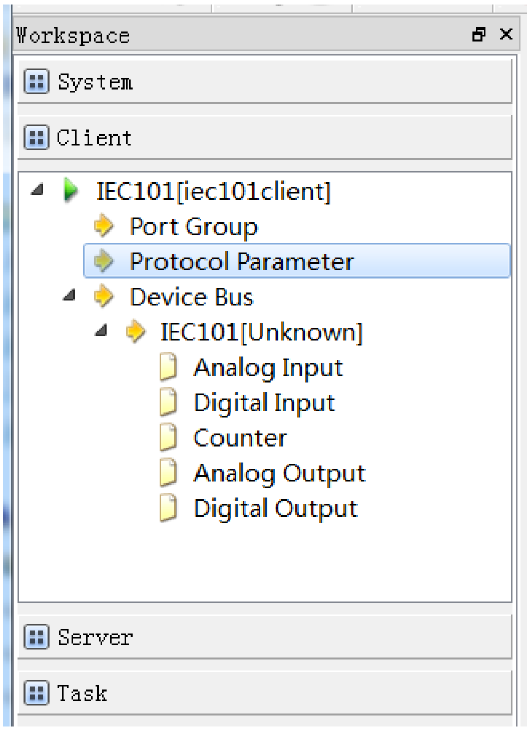
3. Right-click a channel and choose **Delete** from the shortcut menu. Click **Yes** to complete the deletion.

4.2.2.1.3.Protocol Parameters

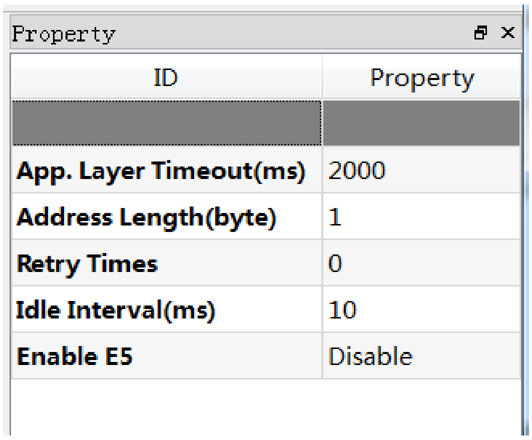
Overview Define the communication protocol parameters of the protocol.

Properties Display the protocol parameter properties on the EDPS ICT-A+.

1. Open a project and click the **PluginView** tab in the EDPS ICT-A+ management area.
2. Activate the collection service plugin.
3. Select **Protocol Parameter** in the management area.



4. View the properties of the protocol parameters.



ID	Property
App. Layer Timeout(ms)	2000
Address Length(byte)	1
Retry Times	0
Idle Interval(ms)	10
Enable E5	Disable

Note: Protocol parameters

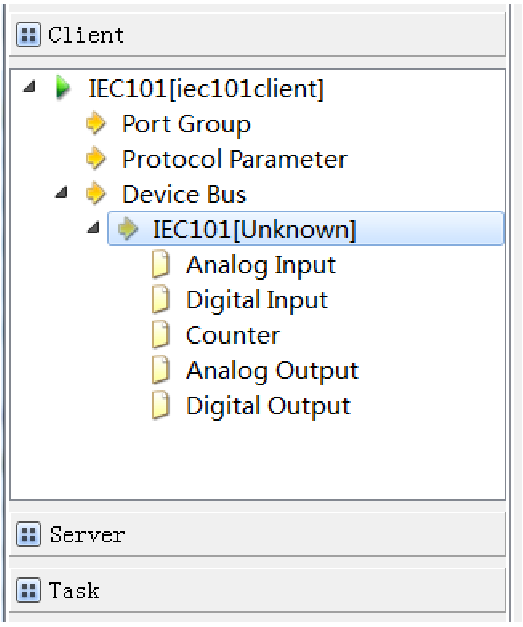
No.	Name	Description
1	App. Layer Timeout(ms)	Timeout interval of the application-layer data response. When the system fails to receive an application-layer response within this interval, the system considers that the device does not respond.
2	Address Length(byte)	Length of the link address. This property enhances the driver compatibility.
3	Retry Times	Number of times that data needs to be resent when it fails to be sent
4	Idle Interval(ms)	Idle waiting duration between two adjacent complete communication processes. A complete communication process starts from the transmission of a data request and ends with the receiving of all valid data.
5	Enable E5	Whether to process E5 during IEC60870-5-101 data processing

4.2.2.1.4.Device Parameters

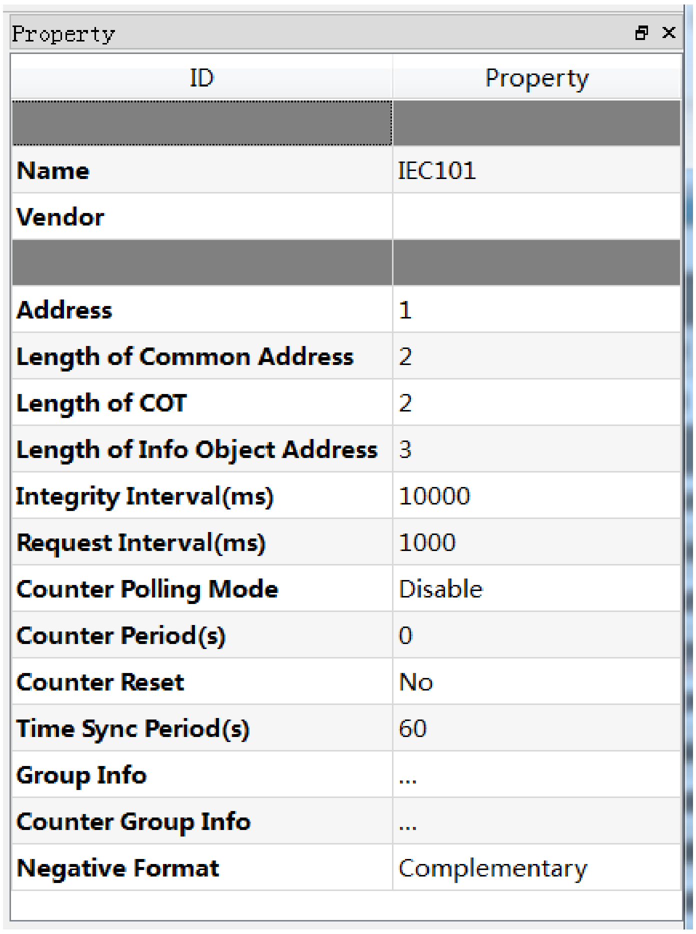
Overview Define the device parameters of the protocol.

Properties Display the properties of the device parameters.

1. Open a project and click the **PluginView** tab in the EDPS ICT-A+ management area.
2. Activate the collection service plugin.
3. Select any subnode under **Device Bus** in the management area.



4. Check the property area of the EDPS ICT-A+.



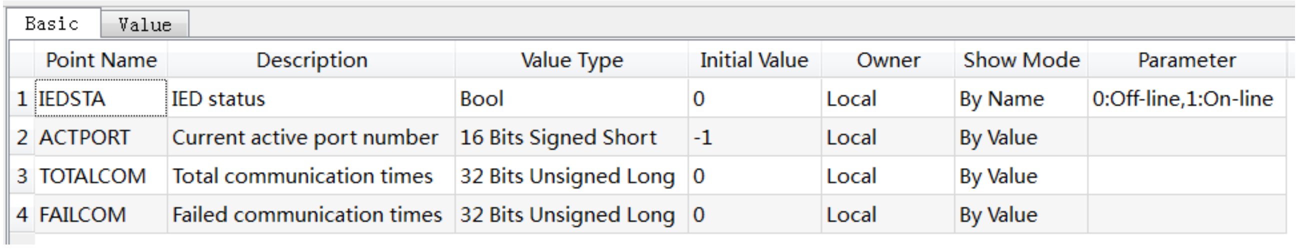
ID	Property
Name	IEC101
Vendor	
Address	1
Length of Common Address	2
Length of COT	2
Length of Info Object Address	3
Integrity Interval(ms)	10000
Request Interval(ms)	1000
Counter Polling Mode	Disable
Counter Period(s)	0
Counter Reset	No
Time Sync Period(s)	60
Group Info	...
Counter Group Info	...
Negative Format	Complementary

Note: Device properties

No.	Name	Description
1	Name	Device name
2	Vendor	Device vendor
3	Address	Physical address of the device
4	Length of Common Address	Number of bytes occupied by the common address in the IEC60870-5-101 communication byte flow
5	Length of COT	Number of bytes occupied by the COT in the IEC60870-5-101 communication byte flow
6	Length of Info Object Address	Number of bytes occupied by the information object address in the IEC60870-5-101 communication byte flow
7	Integrity Interval(ms)	General interrogation period of the device. The

No.	Name	Description
		unit is milliseconds.
8	Request Interval (ms)	Interval for querying class 2 data in unbalance mode. The unit is milliseconds.
9	Counter Polling Mode	Counter polling mode. The modes include mode A, mode B, mode C, and mode D. For details, see the IEC60780-5-101 protocol.
10	Counter Period(s)	Period for sending a counter interrogation command. It is available only in mode B, mode C, and mode D. The value **0** indicates that interrogation is not performed periodically.
11	Counter Reset	Whether to reset the counter in the counter interrogation
12	Time Sync Period(s)	Period for sending time synchronization commands. The value **-1** indicates invalid while the value **0** indicates that a time synchronization command is sent upon system startup.
13	Group Info	Details about the group in the group interrogation
14	Counter Group Info	Details about the group in the grouped counter interrogation
15	Negative Format	Method of decoding negative analog values

Properties of the Pseudo Point　View the data area of the EDPS ICT-A+.



	Point Name	Description	Value Type	Initial Value	Owner	Show Mode	Parameter
1	IEDSTA	IED status	Bool	0	Local	By Name	0:Off-line,1:On-line
2	ACTPORT	Current active port number	16 Bits Signed Short	-1	Local	By Value	
3	TOTALCOM	Total communication times	32 Bits Unsigned Long	0	Local	By Value	
4	FAILCOM	Failed communication times	32 Bits Unsigned Long	0	Local	By Value	

No.	Name	Description
1	IED STA	Communication status of the current device. The value shows whether the device is on-line or off-line.
2	ACTPORT	Port used by the current channel for communication. For a multi-port link, the value helps locate the active port easily.
3	TOTALCOM	Total number of communications
4	FAILCOM	Number of failed communications. A communication failure means that data is not transmitted successfully or data is received incorrectly.

4.2.2.1.5.IO Parameters

Overview The IO information page in the data area of the EDPS ICT-A+ displays IO parameters of each information point. The system conducts accurate boundary test and data check for IO parameters of each type of data, so as to effectively reduce the configuration data error rate during data input.

1) Analog input

Common Address Common address in the communication

Point Number Information object address of the information point

2) Status input

Common Address Common address in the communication

Point Number Information object address of the information point

3) Counter input

Common Address Common address in the communication

Point Information object address of the information point

Number

4) Analog output

Common Address Common address in the communication

Point Number Information object address of the information point

Output Type ASDU type of the information point. See the IEC60870-5-101 protocol.

- C_SE_NA_1 (scale value)
- C_SC_NB_1 (normalized value)
- C_SC_NC_1(short floating-point value)

5) Status output

Common Address Common address in the communication

Point Number Information object address of the information point

Output Code Command execution mode. See the IEC60870-5-101 protocol.

- None
- Short pulse
- Long pulse
- Continuous output

Output Type ASDU type of a command. See the IEC60870-5-101 protocol.

- Single-point command
- Dual-point command
- Step position command

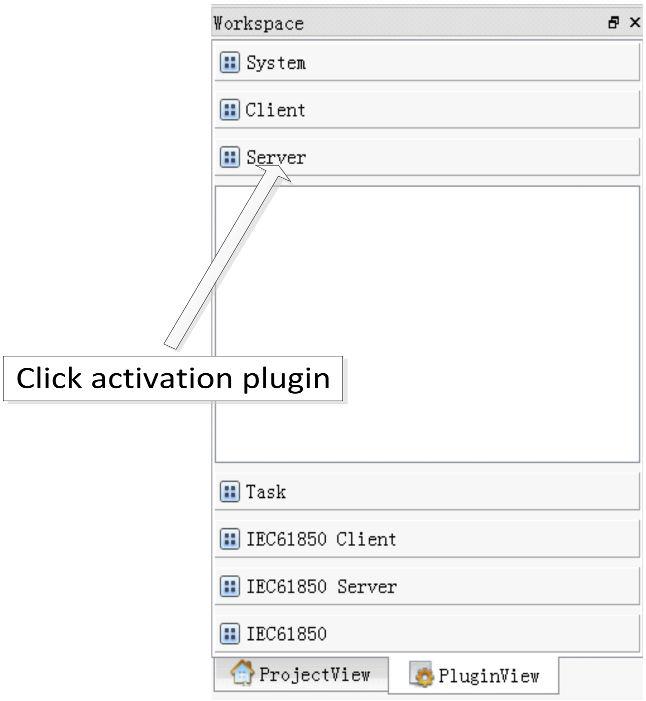
4.2.2.2.Configuration of the IEC60870-5-101 Forwarding Module

4.2.2.2.1.Driver Information

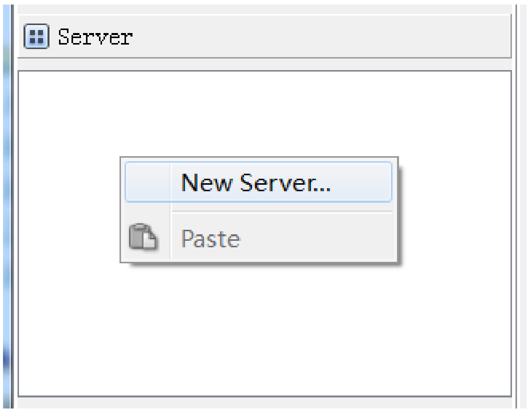
Overview Describe the details about the forwarding driver.

Create Create an IEC60870-5-101 forwarding driver.

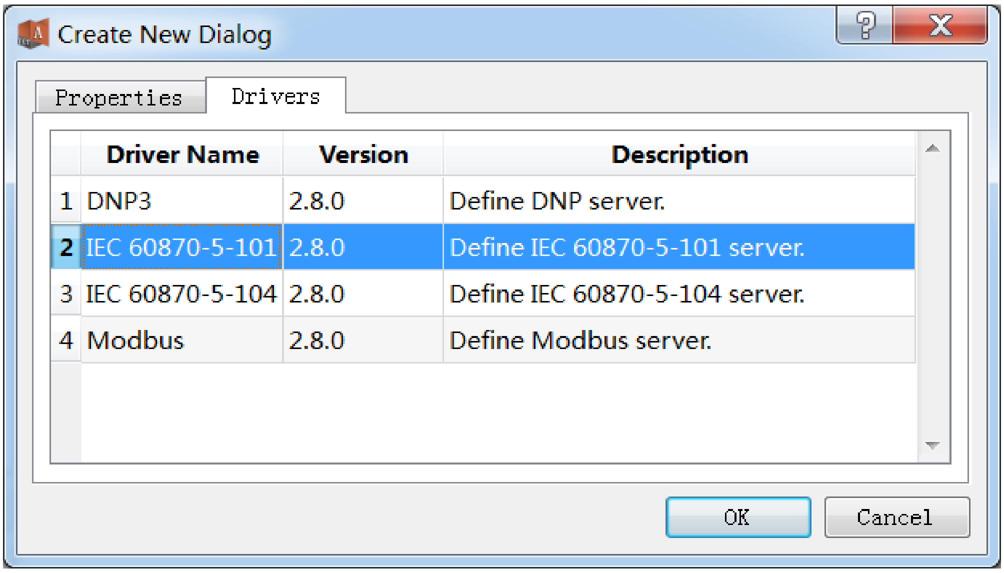
1. Open a project file.
2. Click the **PluginView** tab in the EDPS ICT-A+ management area.
3. Activate the forwarding service plugin.



4. Right-click in the blank area and choose **New Server** from the shortcut menu. The driver creation dialog box is displayed.



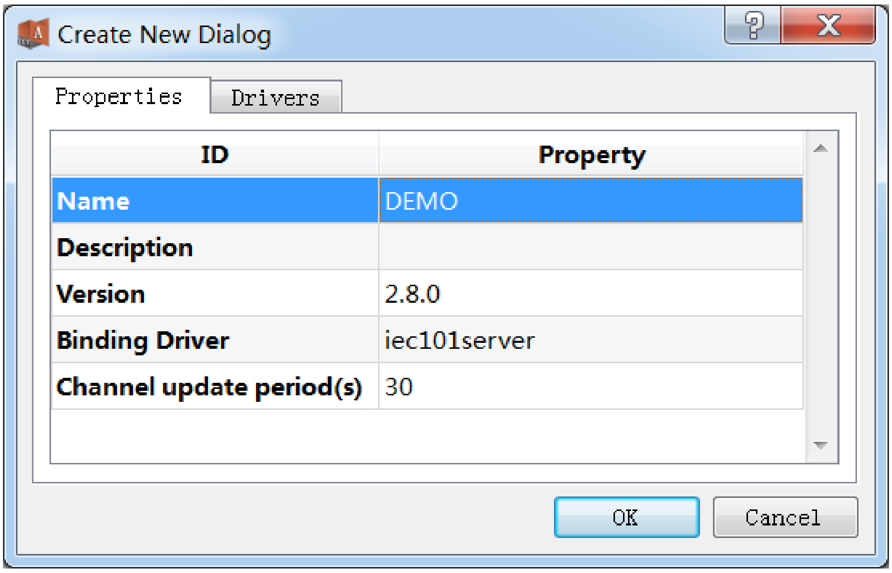
5. On the **Drivers** tab page, select the driver to be created.



Create New Dialog

	Driver Name	Version	Description
1	DNP3	2.8.0	Define DNP server.
2	IEC 60870-5-101	2.8.0	Define IEC 60870-5-101 server.
3	IEC 60870-5-104	2.8.0	Define IEC 60870-5-104 server.
4	Modbus	2.8.0	Define Modbus server.

6. On the **Properties** tab page, configure basic properties for the target driver.



Create New Dialog

ID	Property
Name	DEMO
Description	
Version	2.8.0
Binding Driver	iec101server
Channel update period(s)	30

7. Click **OK**.

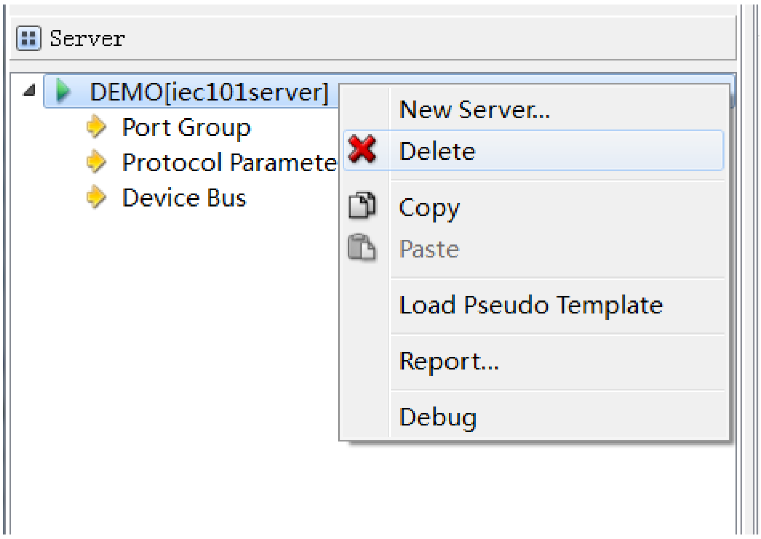
Note: Driver information

No.	Name	Description
1	Name	Driver name to be displayed
2	Description	Driver description
3	Version	Driver version
4	Binding Driver	Name of the driver module. The value is unique and cannot be modified.
5	Channel update	Period for updating the IED communication

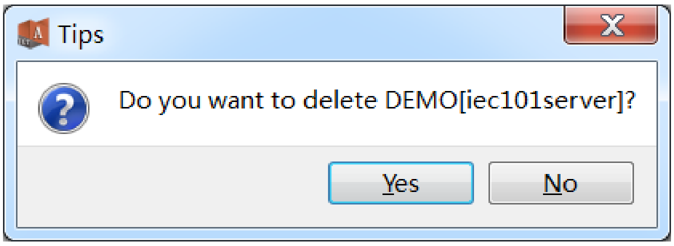
	period(s)	times

Delete Delete an IEC60870-5-101 forwarding driver.

8. Right-click the driver to be deleted and choose **Delete** from the shortcut menu.



9. A dialog box is displayed, asking you whether to delete the driver.

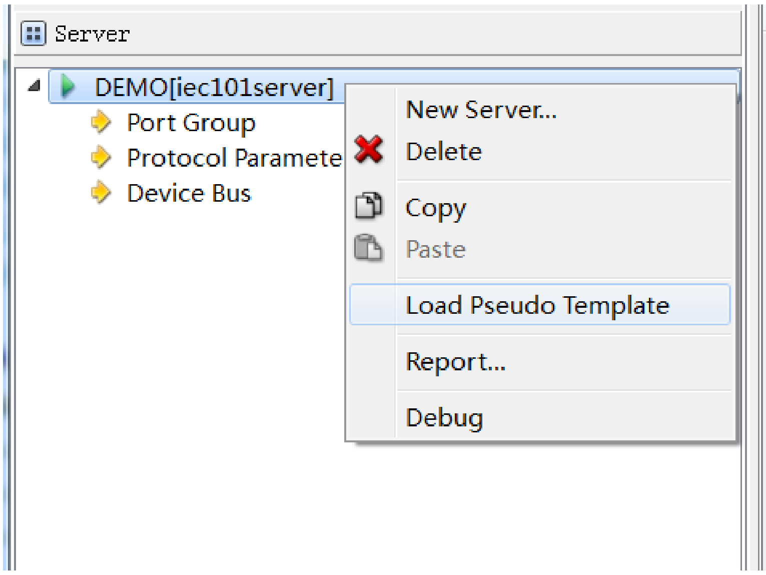


Do you want to delete DEMO[iec101server]?

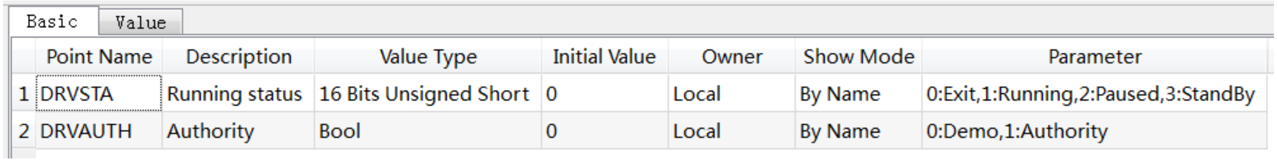
10. Click **Yes** to complete deletion.

Pseudo Template Load a pseudo template from the system template library to the driver.

11. Right-click the driver bar and choose **Load Pseudo Template** from the shortcut menu, to load a pseudo template to the driver.



Note:



Basic | Value

	Point Name	Description	Value Type	Initial Value	Owner	Show Mode	Parameter
1	DRVSTA	Running status	16 Bits Unsigned Short	0	Local	By Name	0:Exit,1:Running,2:Paused,3:StandBy
2	DRVAUTH	Authority	Bool	0	Local	By Name	0:Demo,1:Authority

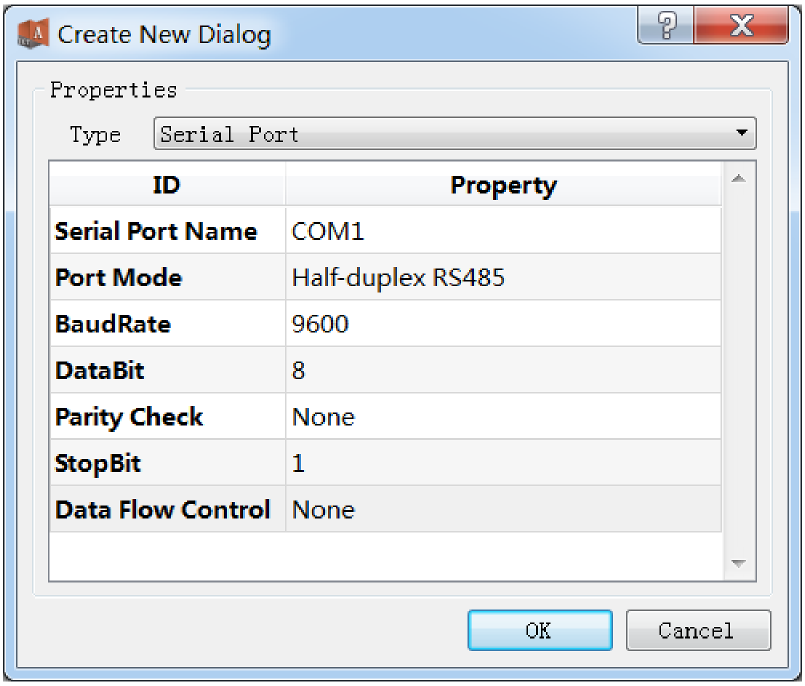
No.	Name	Description
1	DRVSTA	Running status information about the driver
2	DRVAUTH	Authority status of the driver

4.2.2.2.2.Port Group Information

Overview Describe a communication channel.

Create Create a communication channel.

1. Right-click **Port Group** and choose **Create** from the shortcut menu. The port creation dialog box is displayed.
2. Select **Serial Port**.



Type: Serial Port

ID	Property
Serial Port Name	COM1
Port Mode	Half-duplex RS485
BaudRate	9600
DataBit	8
Parity Check	None
StopBit	1
Data Flow Control	None

Note: Properties of a serial channel

No.	Name	Description
1	Serial Port Name	Name of a serial port
2	Port Mode	Work mode of the serial port
3	BaudRate	Baud rate of the serial port
4	DataBit	Data bit of the serial port
5	Parity Check	Parity bit of the serial port
6	StopBit	Stop bit of the serial port
7	Data Flow Control	Data flow control mode of the serial port

Delete Delete a communication channel.

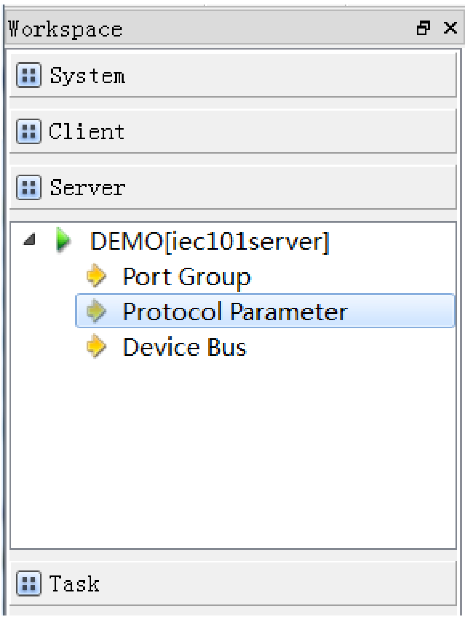
3. Right-click a channel and choose **Delete** from the shortcut menu. Click **Yes** to complete the deletion.

4.2.2.2.3.Protocol Parameters

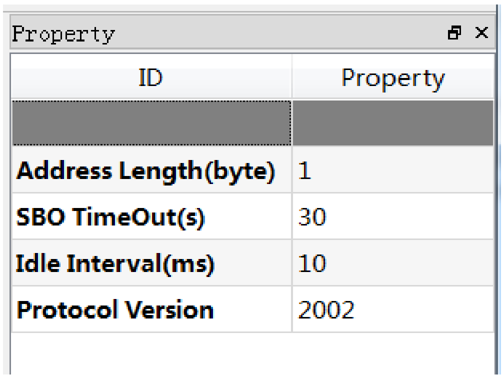
Overview Define the communication protocol parameters of the protocol.

1. Open a project and click the **PluginView** tab in the EDPS ICT-A+ management area.
2. Activate the forwarding service plugin.

3. Select **Protocol Parameter** in the management area.



4. View the properties of the protocol parameters.



ID	Property
Address Length(byte)	1
SBO TimeOut(s)	30
Idle Interval(ms)	10
Protocol Version	2002

Note: Protocol parameters

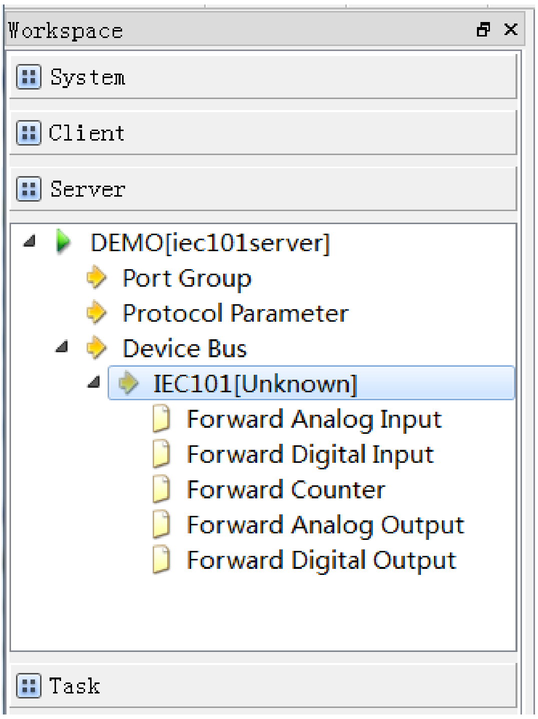
No.	Name	Description
1	Address Length(byte)	Length of a link address. The unit is bytes.
2	SBO TimeOut(s)	Waiting timeout interval for executing an SBO command. The unit is seconds.
3	Idle Interval(ms)	Idle communication interval. The unit is milliseconds.
4	Protocol Version	Version of the communication protocol

4.2.2.2.4.Device Parameters

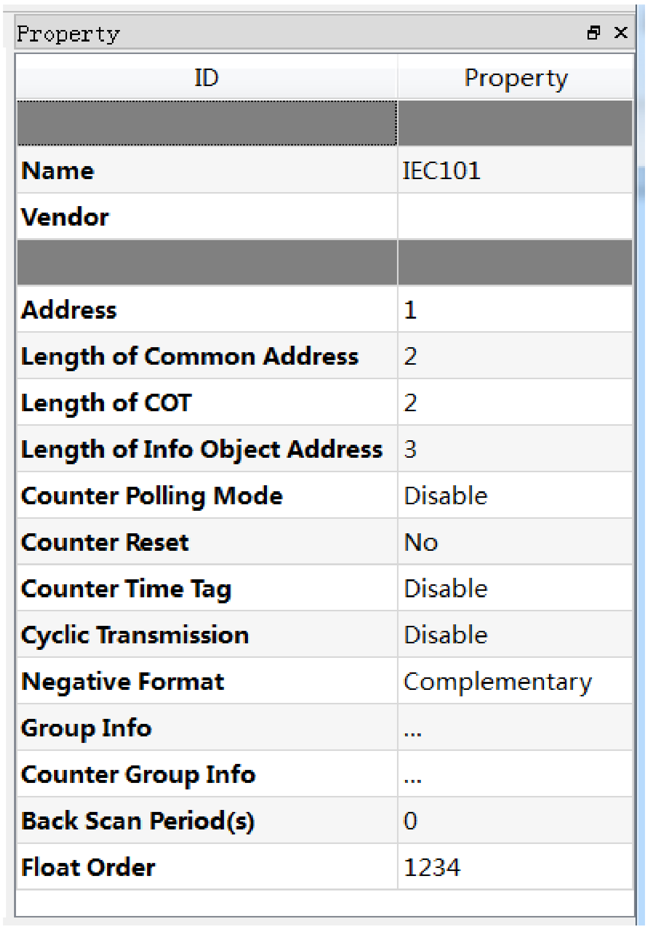
Overview Define the device parameters of the protocol.

Properties Display the properties of the device parameters.

1. Open a project and click the **PluginView** tab in the EDPS ICT-A+ management area.
2. Activate the forwarding service plugin.
3. Select any subnode under **Device Bus** in the management area.



4. View the property area of the EDPS ICT-A+.



Property

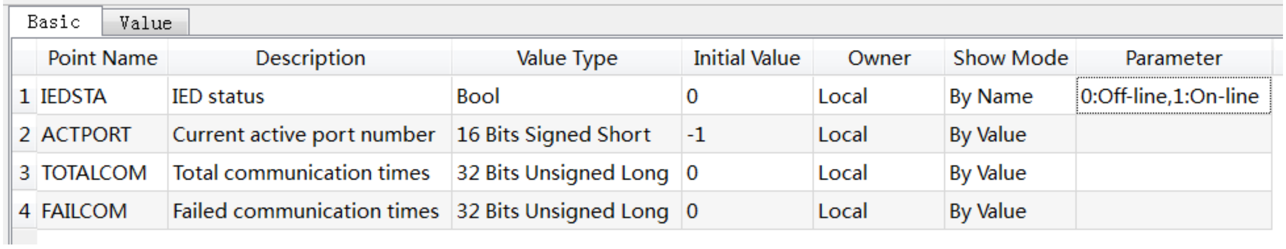
ID	Property
Name	IEC101
Vendor	
Address	1
Length of Common Address	2
Length of COT	2
Length of Info Object Address	3
Counter Polling Mode	Disable
Counter Reset	No
Counter Time Tag	Disable
Cyclic Transmission	Disable
Negative Format	Complementary
Group Info	...
Counter Group Info	...
Back Scan Period(s)	0
Float Order	1234

Note: Device properties

No.	Name	Description
1	Name	Device name
2	Vendor	Device vendor
3	Address	Physical address of the device
4	Length of Common Address	Number of bytes occupied by the common address in the IEC60870-5-101 communication byte flow
5	Length of COT	Number of bytes occupied by the COT in the IEC60870-5-101 communication byte flow
6	Length of Info Object Address	Number of bytes occupied by the information object address in the IEC60870-5-101 communication byte flow
7	Counter Polling Mode	Counter polling mode. The modes include mode

No.	Name	Description
		A, mode B, mode C, and mode D. For details, see the IEC60780-5-101 protocol.
8	Counter Reset	Whether counter reset is allowed
9	Counter Time Tag	Whether to add the time tag to the counter
10	Cyclic Transmission	Whether to cyclically send data based on group definition information
11	Negative Format	Method of decoding negative analog values
12	Group Info	Details about the group in the group interrogation
13	Counter Group Info	Details about the group in the grouped counter interrogation
14	Back Scan Period(s)	Period for sending background scanning data frames. The value **0** indicates that data frames are not transmitted.
15	Floating Order	Coding sequence of floating-point numbers

Properties of the Pseudo Point View the data area of the EDPS ICT-A+.



	Point Name	Description	Value Type	Initial Value	Owner	Show Mode	Parameter
1	IEDSTA	IED status	Bool	0	Local	By Name	0:Off-line,1:On-line
2	ACTPORT	Current active port number	16 Bits Signed Short	-1	Local	By Value	
3	TOTALCOM	Total communication times	32 Bits Unsigned Long	0	Local	By Value	
4	FAILCOM	Failed communication times	32 Bits Unsigned Long	0	Local	By Value	

No.	Name	Description
1	IED STA	Communication status of the current device. The value shows whether the device is on-line or off-line.
2	ACTPORT	Port used by the current channel for communication. For a multi-port link, the value helps locate the active port easily.
3	TOTALCOM	Total number of communications
4	FAILCOM	Number of failed communications. A communication

No.	Name	Description
		failure means that data is not transmitted successfully or data is received incorrectly.

4.2.2.2.5.IO Parameters

Overview The IO information page in the data area of the EDPS ICT-A+ displays IO parameters of each information point. The system, based on parameter settings, conducts accurate boundary test and data check for IO parameters of each type of data, so as to effectively reduce the configuration data error rate during data input.

1) Analog input

Common Address Common address in the communication

Point Number Point number of the information point

ASDU Type Function type of the application to which the information point belongs

- M_ME_NA_1 (normalized value)
- M_ME_NB_1 (scale value)
- M_ME_NC_1 (short floating-point value)
- M_ME_ND_1(normalized value with quality)
- M_ST_NA_1 (step position information)

Work Mode Work mode of the information point

- Cyclic
- Spontaneous

Time Tag Whether the information point carries the time tag during frame transmission

Offset Offset of the raw data calculated by the information point

Divisor Division factor used by the information point in the calculation of raw data

Dead Zone Value Dead zone value for generating event data. Event data is generated when the absolute value of the difference between the previous transmission value and the current value is greater than the dead zone value.

2) Status input

Common Address Common address in the communication

Point Number Point number of the information point

ASDU Type ASDU transmission type of the information point

- M_SP_NA_1 (single point)
- M_DP_NA_1 (dual points)

Work Mode Work mode of the information point

- Cyclic
- Spontaneous

Automatic SOE Whether the system uses changed data as the SOE for transmission based on settings after receiving the status change information.

- Disable
- Enabled when open
- Enabled when close
- Enabled when changed

SOE Whether the system directly uses the valid SOE data of the device after receiving

COS The system sends change information after receiving status change information.

3) Counter input

Common Address Common address in the communication

Point Number Point number of the information point

Minimum Minimum value for calculating raw data

Maximum Maximum value for calculating raw data

Offset Offset of the raw data calculated by the information point

Divisor Division factor used by the information point in the calculation of raw data

4) Analog output

Common Address Common address in the communication

Point Number Point number of the information point

ASDU Type Output Type Function type of the application to which the information point belongs

- Normalized value
- Scale value
- Short floating-point number

Offset Offset of the raw data calculated by the information point

Divisor Division factor used by the information point in the calculation of raw data

5) Status output

Common Address Common address in the communication

Point Number Point number of the information point

Control Mode Mode for executing control operation commands by the information point

- Direct execution
- SBO

4.2.3.IEC60870-5-104 Protocol Configuration

Appendix D describes how to configure the IEC60870-5-104 collection and forwarding driver modules on the EDPS ICT-A+. The driver information, protocol parameters, device parameters, and IO parameters of each information point are described in the configuration manual. The IEC60870-5-104 collection and forwarding modules of the EDPS ICT-A+ fully comply with the protocol. The EDPS ICT-A+ provides a simple and fast way to help users complete the configuration.

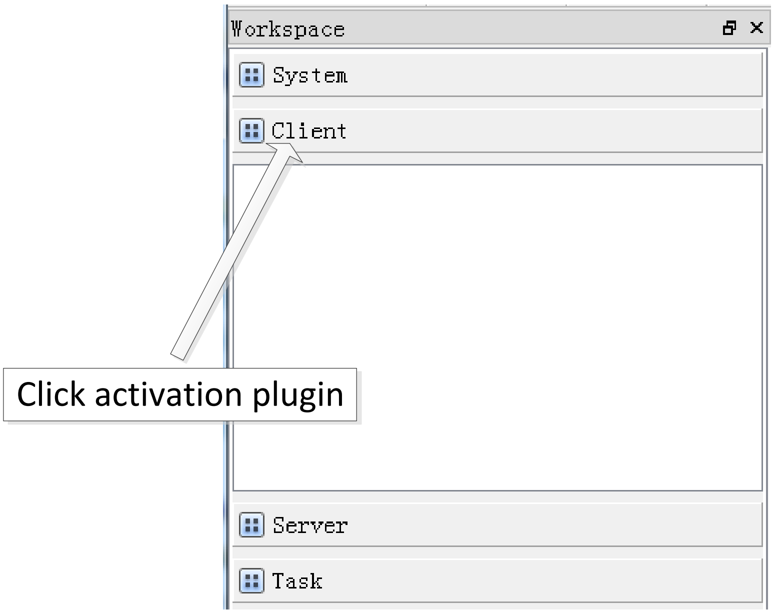
4.2.3.1.Configuration of the IEC60870-5-104 Collection Module

4.2.3.1.1.Driver Information

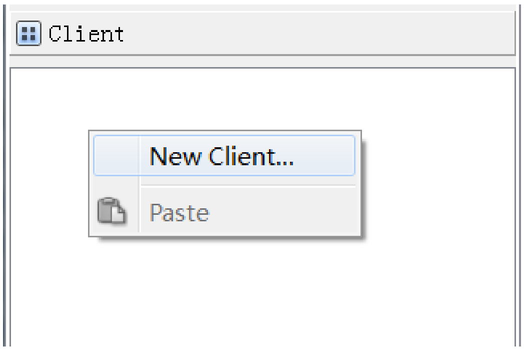
Overview Describe the details about the collection driver.

Create Create an IEC60870-5-104 collection driver.

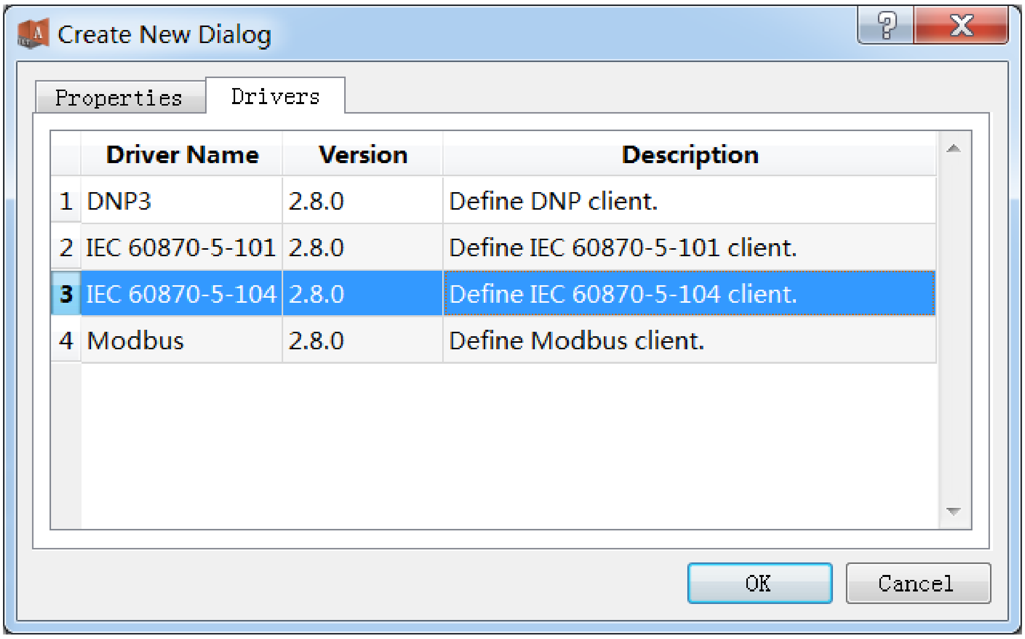
1. Open a project file.
2. Click the **PluginView** tab in the EDPS ICT-A+ management area.
3. Activate the collection service plugin.



4. Right-click in the blank area and choose **New Client** from the shortcut menu. The driver creation dialog box is displayed.

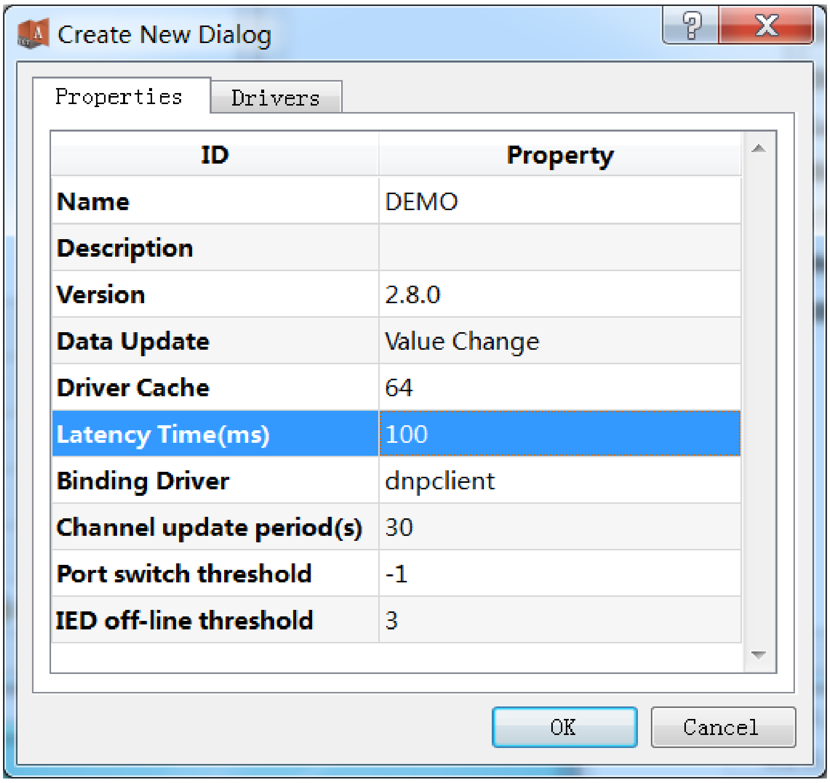


5. On the **Drivers** tab page, select the driver to be created.



	Driver Name	Version	Description
1	DNP3	2.8.0	Define DNP client.
2	IEC 60870-5-101	2.8.0	Define IEC 60870-5-101 client.
3	IEC 60870-5-104	2.8.0	Define IEC 60870-5-104 client.
4	Modbus	2.8.0	Define Modbus client.

6. On the **Properties** tab page, configure basic properties for the target driver.



ID	Property
Name	DEMO
Description	
Version	2.8.0
Data Update	Value Change
Driver Cache	64
Latency Time(ms)	100
Binding Driver	dnpclient
Channel update period(s)	30
Port switch threshold	-1
IED off-line threshold	3

7. Click **OK**.

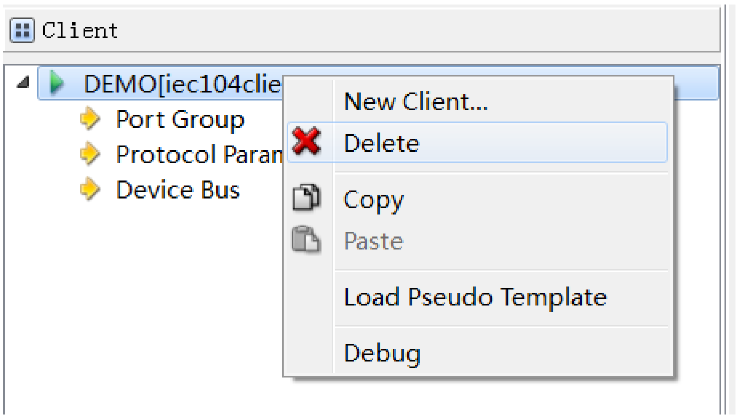
Note: Driver information

No.	Name	Description
1	Name	Driver name to be displayed
2	Description	Driver description
3	Version	Driver version
4	Data Update	Data update mode Value Change: The database is updated and other driver protocols are notified only when the value changes. Time Change: The value or time is updated into the database and other driver protocols are notified whenever the value or time changes. Time Update: The value or time is updated whenever it changes, and other driver protocols are notified only when the value changes.
5	Driver Cache	Cache size of the driver

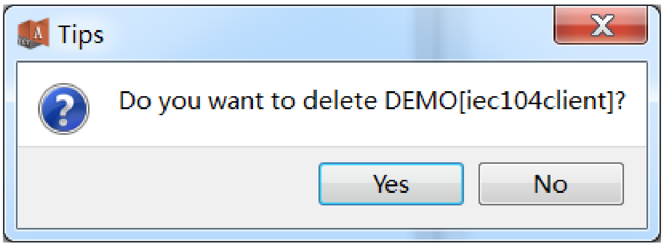
No.	Name	Description
6	Latency Time(ms)	Latency for updating the real-time database The system writes raw data into the real-time database only after the latency time.
7	Binding Driver	Name of the driver module. The value is unique and cannot be modified.
8	Channel update period(s)	Period for updating the IED communication times
9	Port switch threshold	Conditions for multi-port switching. When the number of consecutive communication failures of the master port reaches this threshold, the system switches to another port. The value **-1** indicates that port switching is not performed.
10	IED off-line threshold	IED off-line threshold. When the number of communication failures of a device reaches this threshold, the device is set to be in the off-line state.

Delete Delete an IEC60870-5-104 collection driver.

8. Right-click the driver to be deleted and choose **Delete** from the shortcut menu.



9. A dialog box is displayed, asking you whether to delete the driver.

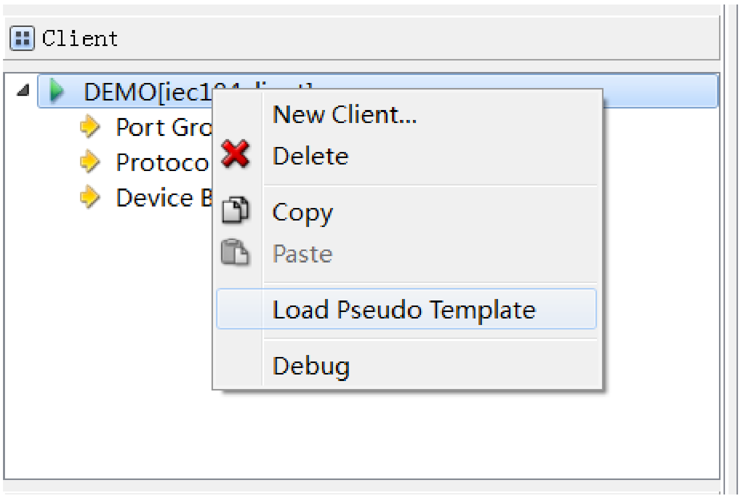


Do you want to delete DEMO[iec104client]?

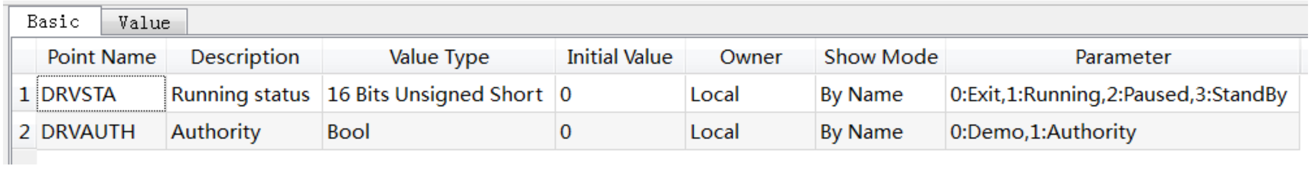
10. Click **Yes** to complete deletion.

Pseudo Template Load a pseudo template from the system template library to the driver.

11. Right-click the driver bar and choose **Load Pseudo Template** from the shortcut menu, to load a pseudo template to the driver.



Note:



	Point Name	Description	Value Type	Initial Value	Owner	Show Mode	Parameter
1	DRVSTA	Running status	16 Bits Unsigned Short	0	Local	By Name	0:Exit,1:Running,2:Paused,3:StandBy
2	DRVAUTH	Authority	Bool	0	Local	By Name	0:Demo,1:Authority

No.	Name	Description
1	DRVSTA	Running status information about the driver
2	DRVAUTH	Authority status of the driver

4.2.3.1.2.Port Group Information

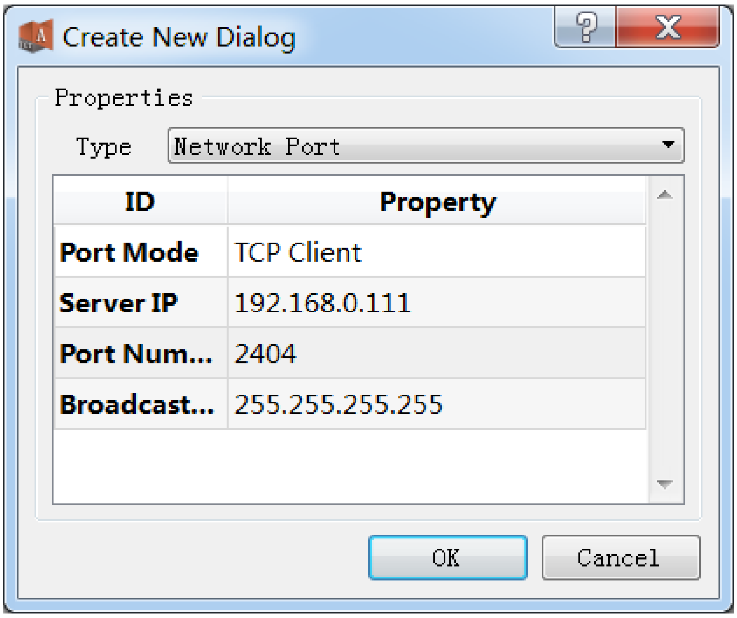
Overview Describe a communication channel.

Create Create a communication channel.

1. Right-click **Port Group** and choose **Create** from the shortcut menu. The port creation

dialog box is displayed.

2. Select **Network Port**.



Type: Network Port

ID	Property
Port Mode	TCP Client
Server IP	192.168.0.111
Port Num...	2404
Broadcast...	255.255.255.255

Note: Properties of a network channel

No.	Name	Description
1	Port Mode	Work mode of the network port
2	Service IP	IP address of the TCP server or UDP destination address
3	Port Number	Work port number of the network port
4	Broadcast Address	Broadcast address of the network port

Delete Delete a communication channel.

3. Right-click a channel and choose **Delete** from the shortcut menu. Click **Yes** to complete the deletion.

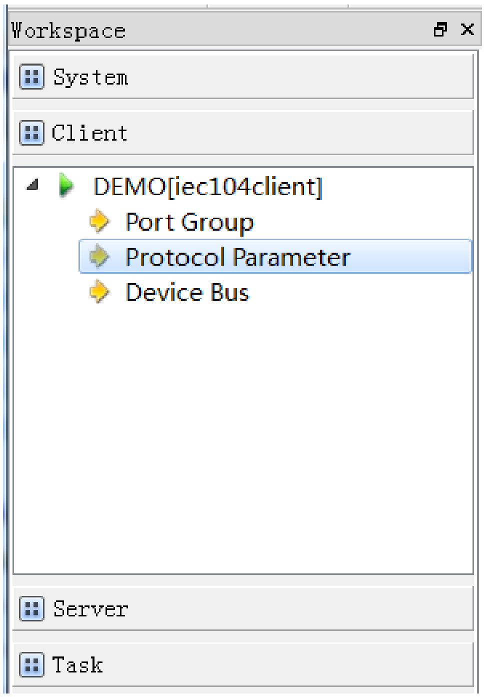
4.2.3.1.3.Protocol Parameters

Overview Define the communication protocol parameters of the protocol.

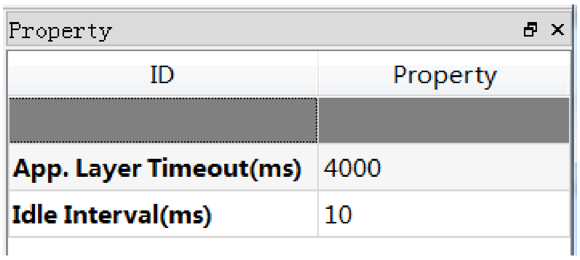
Properties Display the properties of the protocol parameters on the EDPS ICT-A+.

1. Open a project and click the **PluginView** tab in the EDPS ICT-A+ management area.
2. Activate the collection service plugin.

3. Select **Protocol Parameter** in the management area.



4. View the properties of the protocol parameters.



ID	Property
App. Layer Timeout(ms)	4000
Idle Interval(ms)	10

Note: Protocol parameters

No.	Name	Description
1	App. Layer Timeout(ms)	Timeout interval of the application-layer data response. When the system fails to receive an application-layer response within this interval, the system considers that the device does not respond.
2	Idle Interval(ms)	Idle waiting duration between two adjacent complete communication processes. A complete communication process starts from the transmission of a data request and ends with the

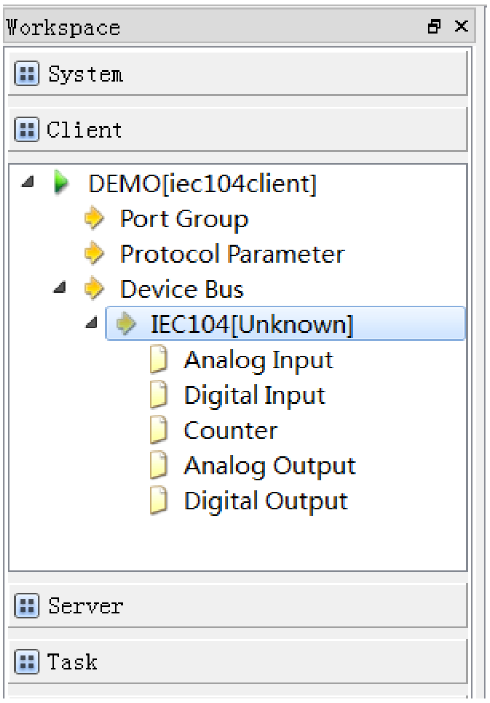
		receiving of all valid data.

4.2.3.1.4.Device Parameters

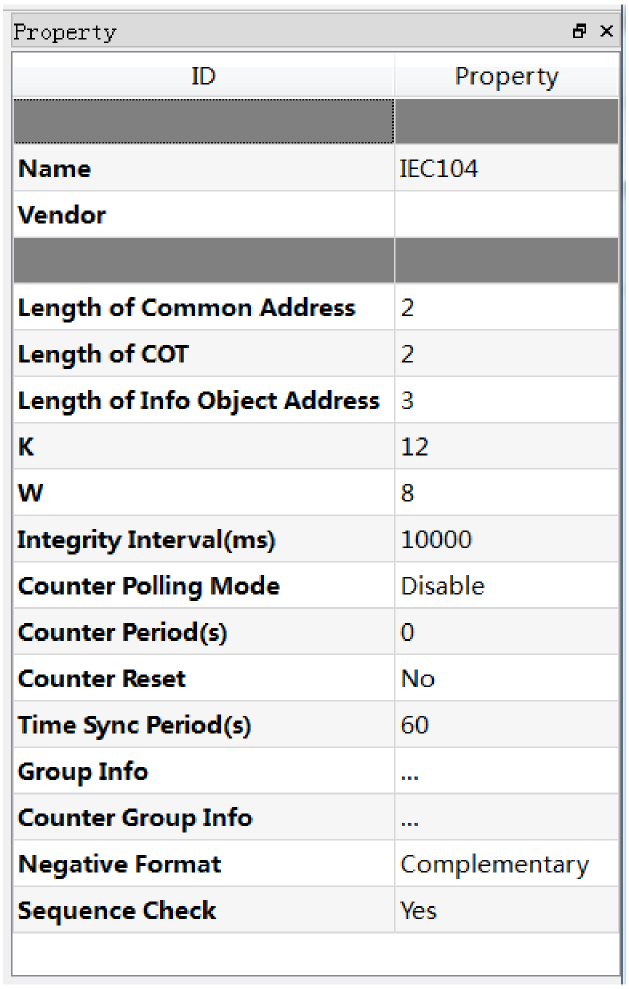
Overview Define the device parameters of the protocol.

Properties Display the properties of the device parameters.

1. Open a project and click the **PluginView** tab in the EDPS ICT-A+ management area.
2. Activate the collection service plugin.
3. Select any subnode under **Device Bus** in the management area.



4. View the property area of the EDPS ICT-A+.



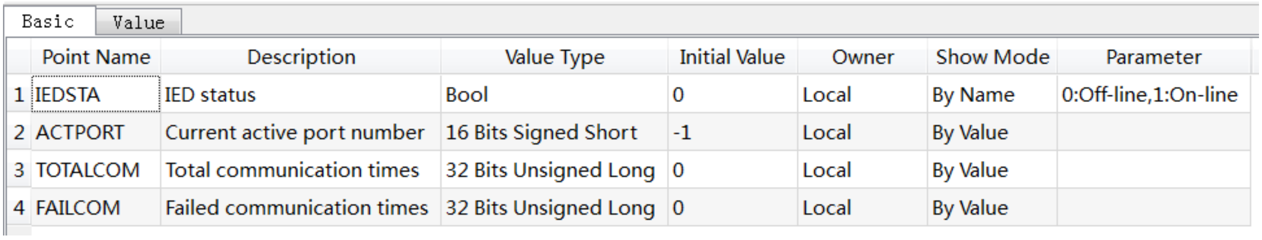
ID	Property
Name	IEC104
Vendor	
Length of Common Address	2
Length of COT	2
Length of Info Object Address	3
K	12
W	8
Integrity Interval(ms)	10000
Counter Polling Mode	Disable
Counter Period(s)	0
Counter Reset	No
Time Sync Period(s)	60
Group Info	...
Counter Group Info	...
Negative Format	Complementary
Sequence Check	Yes

Note: Device properties

No.	Name	Description
1	Name	Device name
2	Vendor	Device vendor
3	Length of Common Address	Number of bytes used by the common address in the communication byte flow
4	Length of COT	Number of bytes used by COT in the communication byte flow
5	Length of Info Object Address	Number of bytes used by the information object address in the communication byte flow
6	K	Maximum number of unconfirmed frames in the buffer

No.	Name	Description
7	W	Maximum number of I frames that can be received by the buffer prior to device confirmation. It should not be greater than 2/3 of K.
8	Integrity Interval(ms)	General interrogation period of the device
9	Counter Polling Mode	Counter polling mode. The modes include mode A, mode B, mode C, and mode D. For details, see the IEC60780-5-101 protocol.
10	Counter Period(s)	Period for sending a counter interrogation or freezing command. It is available only in mode B, mode C, and mode D. The value **0** indicates that interrogation is not performed periodically.
11	Counter Reset	Whether to reset the counter in the counter interrogation
12	Time Sync Period(s)	Time synchronization period of the device. The value **-1** indicates invalid while the value **0** indicates that a time synchronization command is sent upon system startup.
13	Group Info	Details about the group in the group interrogation
14	Counter Group Info	Details about the group in the grouped counter interrogation
15	Negative Format	Method of decoding negative analog values
16	Sequence Check	Whether to check that the sequences of received frames and received frames are matched

Properties of the Pseudo Point View the data area of the EDPS ICT-A+.



	Point Name	Description	Value Type	Initial Value	Owner	Show Mode	Parameter
1	IEDSTA	IED status	Bool	0	Local	By Name	0:Off-line,1:On-line
2	ACTPORT	Current active port number	16 Bits Signed Short	-1	Local	By Value	
3	TOTALCOM	Total communication times	32 Bits Unsigned Long	0	Local	By Value	
4	FAILCOM	Failed communication times	32 Bits Unsigned Long	0	Local	By Value	

No.	Name	Description
1	IED STA	Communication status of the current device. The value shows whether the device is on-line or off-line.
2	ACTPORT	Port used by the current channel for communication. For a multi-port link, the value helps locate the active port easily.
3	TOTALCOM	Total number of communications
4	FAILCOM	Number of failed communications. A communication failure means that data is not transmitted successfully or data is received incorrectly.

4.2.3.1.5.IO Parameters

Overview The IO information page in the data area of the EDPS ICT-A+ displays IO parameters of each information point. The system, based on parameter settings, conducts accurate boundary test and data check for IO parameters of each type of data, so as to effectively reduce the configuration data error rate during data input.

1) Analog input

Common Address	Common address in the communication
Point Number	Information object address of the information point

2) Status input

Common Address	Common address in the communication
Point	Information object address of the information point

Number

3) Counter input

Common Address Common address in the communication

Point Number Information object address of the information point

4) Analog output

Common Address Common address in the communication

Point Number Information object address of the information point

Output Type ASDU type of the information point. See the IEC60870-5-101 protocol.

- C_SE_NA_1 (scale value)
- C_SC_NB_1 (normalized value)
- C_SC_NC_1(short floating-point value)

5) Status output

Common Address Common address in the communication

Point Number Information object address of the information point

Output Code Command execution mode. See the IEC60870-5-101 protocol.

- None
- Short pulse
- Long pulse
- Continuous output

Output Type ASDU type of a command. See the IEC60870-5-101 protocol.

- Single-point command
- Dual-point command

- Step position command

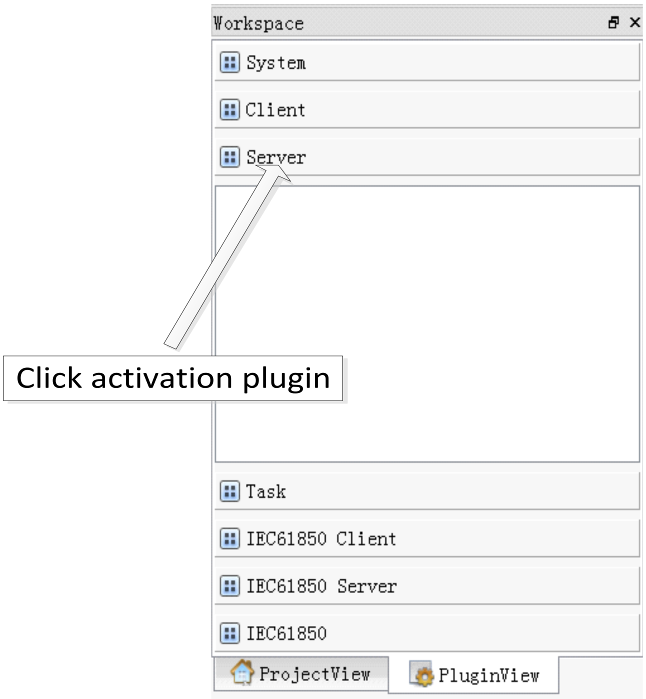
4.2.3.2.Configuration of the IEC60870-5-104 Forwarding Module

4.2.3.2.1.Driver Information

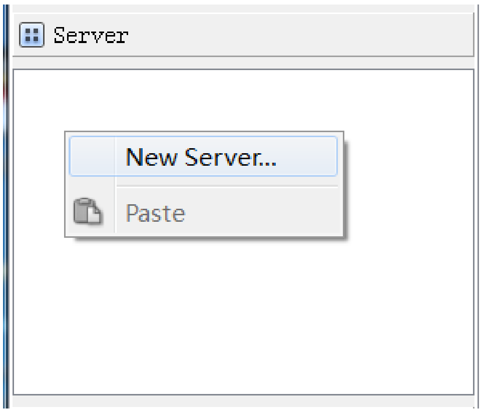
Overview Describe the details about the forwarding driver.

Create Create an IEC60870-5-104 forwarding driver.

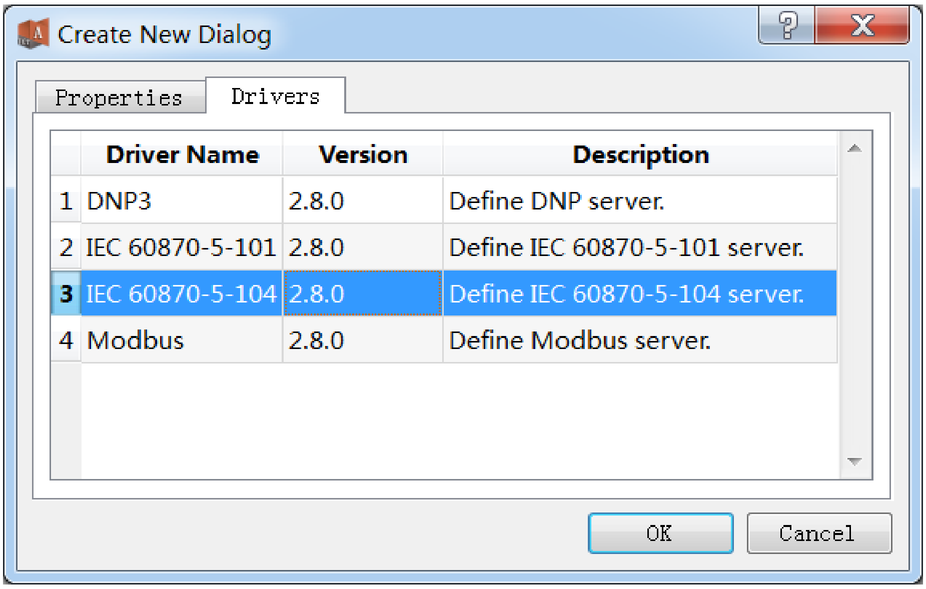
1. Open a project file.
2. Click the **PluginView** tab in the EDPS ICT-A+ management area.
3. Activate the forwarding service plugin.



4. Right-click in the blank area and choose **New Server** from the shortcut menu. The driver creation dialog box is displayed.

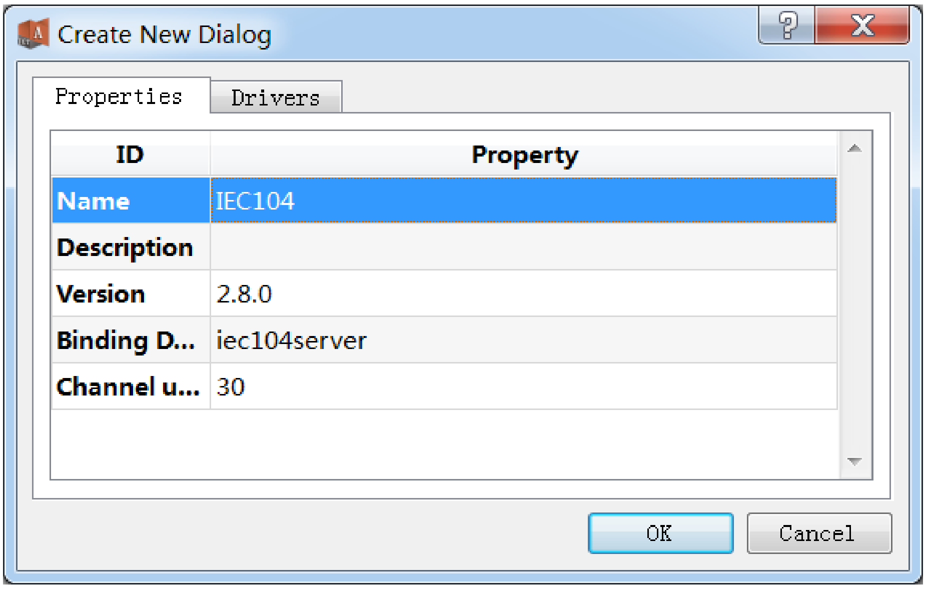


5. On the **Drivers** tab page, select the driver to be created.



	Driver Name	Version	Description
1	DNP3	2.8.0	Define DNP server.
2	IEC 60870-5-101	2.8.0	Define IEC 60870-5-101 server.
3	IEC 60870-5-104	2.8.0	Define IEC 60870-5-104 server.
4	Modbus	2.8.0	Define Modbus server.

6. On the **Properties** tab page, configure basic properties for the target driver.



ID	Property
Name	IEC104
Description	
Version	2.8.0
Binding D...	iec104server
Channel u...	30

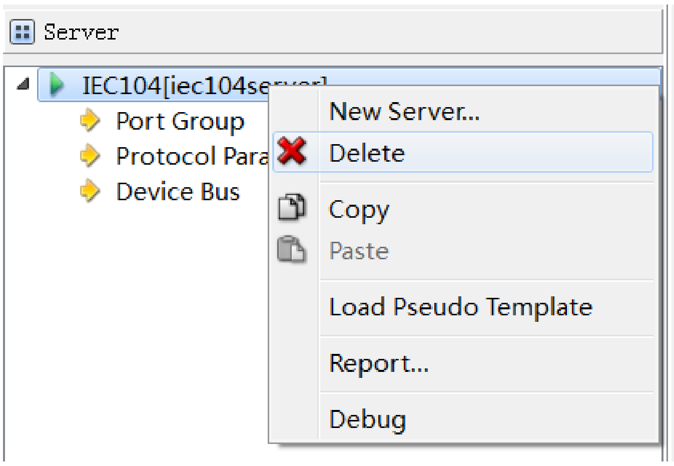
7. Click **OK**.

Note: Driver information

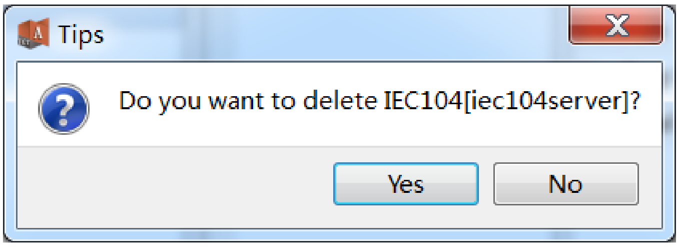
No.	Name	Description
1	Name	Driver name to be displayed
2	Description	Driver description
3	Version	Driver version
4	Binding Driver	Name of the driver module. The value is unique and cannot be modified.
5	Channel update period(s)	Period for updating the IED communication times

Delete Delete an IEC60870-5-104 forwarding driver.

8. Right-click the driver to be deleted and choose **Delete** from the shortcut menu.



9. A dialog box is displayed, asking you whether to delete the driver.

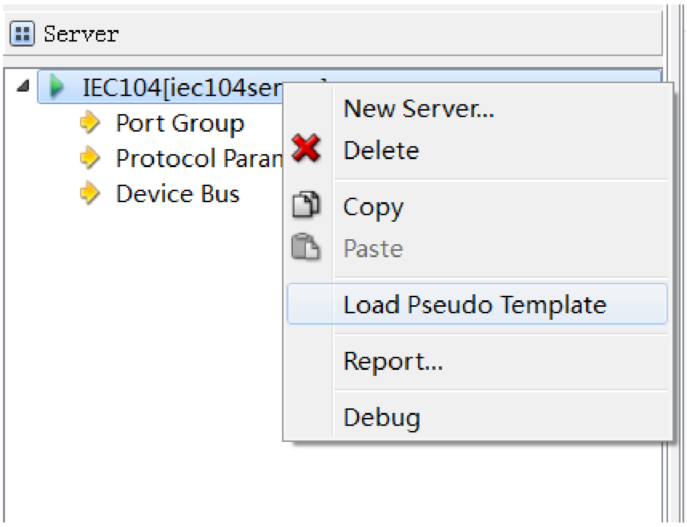


Do you want to delete IEC104[iec104server]?

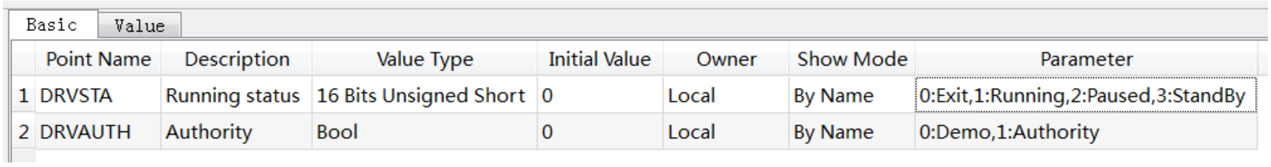
10. Click **Yes** to complete deletion.

Pseudo Template Load a pseudo template from the system template library to the driver.

11. Right-click the driver bar and choose **Load Pseudo Template** from the shortcut menu, to load a pseudo template to the driver.



Note:



	Point Name	Description	Value Type	Initial Value	Owner	Show Mode	Parameter
1	DRVSTA	Running status	16 Bits Unsigned Short	0	Local	By Name	0:Exit,1:Running,2:Paused,3:StandBy
2	DRVAUTH	Authority	Bool	0	Local	By Name	0:Demo,1:Authority

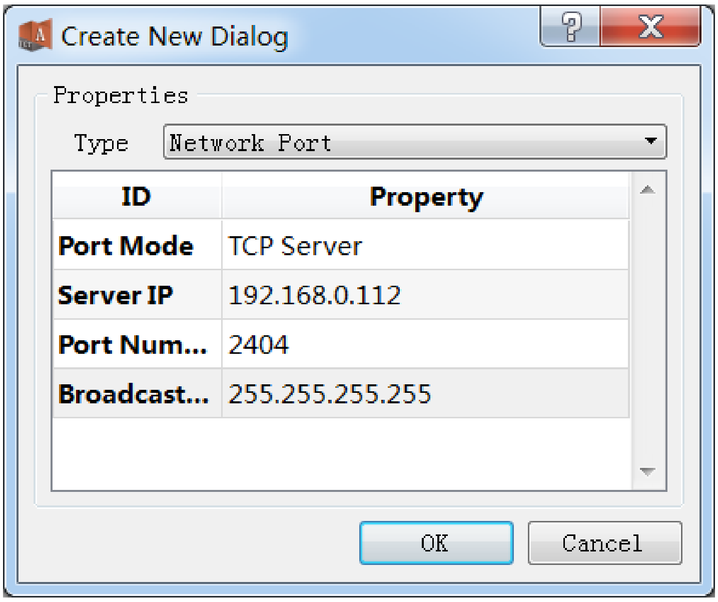
No.	Name	Description
1	DRVSTA	Running status information about the driver
2	DRVAUTH	Authority status of the driver

4.2.3.2.2.Port Group Information

Overview Describe a communication channel.

Create Create a communication channel.

1. Right-click **Port Group** and choose **Create** from the shortcut menu. The port creation dialog box is displayed.



ID	Property
Port Mode	TCP Server
Server IP	192.168.0.112
Port Num...	2404
Broadcast...	255.255.255.255

2. Select **Network Port**.

Note: Properties of a network channel

No.	Name	Description
1	Port Mode	Work mode of the network port
2	Service IP	IP address of the TCP server or UDP destination address
3	Port Number	Work port number of the network port
4	Broadcast Address	Broadcast address of the network port

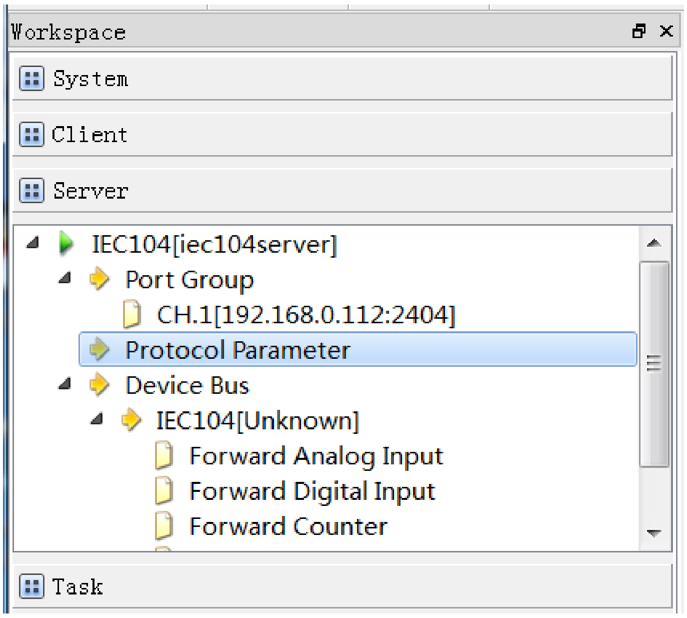
Delete Delete a communication channel.

3. Right-click a channel and choose **Delete** from the shortcut menu. Click **Yes** to complete the deletion.

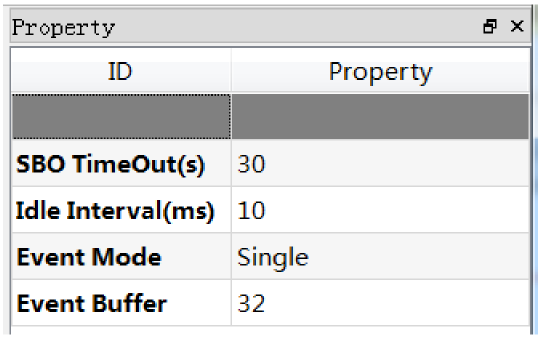
4.2.3.2.3.Protocol Parameters

Overview Define the communication protocol parameters of the protocol.

1. Open a project and click the **PluginView** tab in the EDPS ICT-A+ management area.
2. Activate the forwarding service plugin.
3. Select **Protocol Parameter** in the management area.



4. View the properties of the protocol parameters.


Property

ID	Property
SBO TimeOut(s)	30
Idle Interval(ms)	10
Event Mode	Single
Event Buffer	32

Note: Protocol parameters

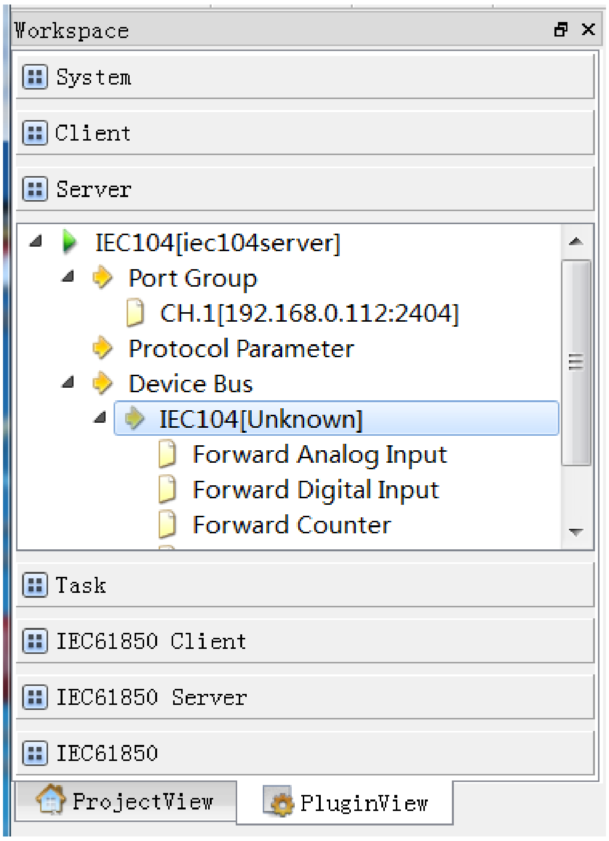
No.	Name	Description
1	SBO TimeOut(s)	Waiting timeout interval for executing an SBO command. The unit is seconds.
2	Idle Interval (ms)	Idle communication interval. The unit is milliseconds.
3	Event Mode	Event processing mechanism. A single channel is used for a single connection while multiple channels are used for all connections.
4	Event Buffer	Size of the event buffer

4.2.3.2.4.Device Parameters

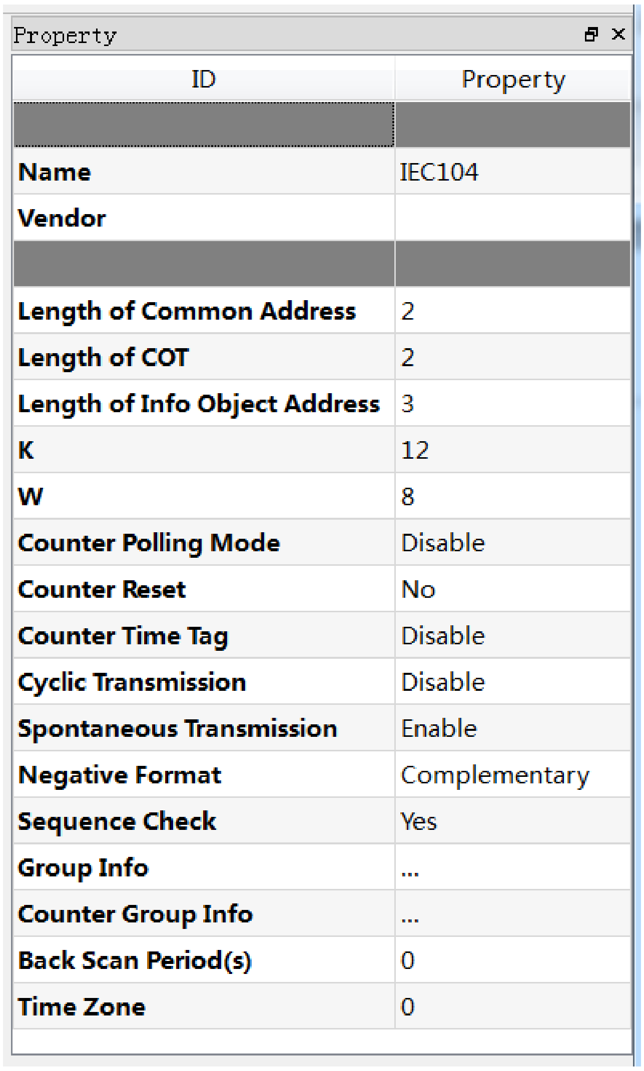
Overview Define the device parameters of the protocol.

Properties Display the properties of the device parameters.

1. Open a project and click the **PluginView** tab in the EDPS ICT-A+ management area.
2. Activate the forwarding service plugin.
3. Select any subnode under **Device Bus** in the management area.



4. View the property area of the EDPS ICT-A+.



Property

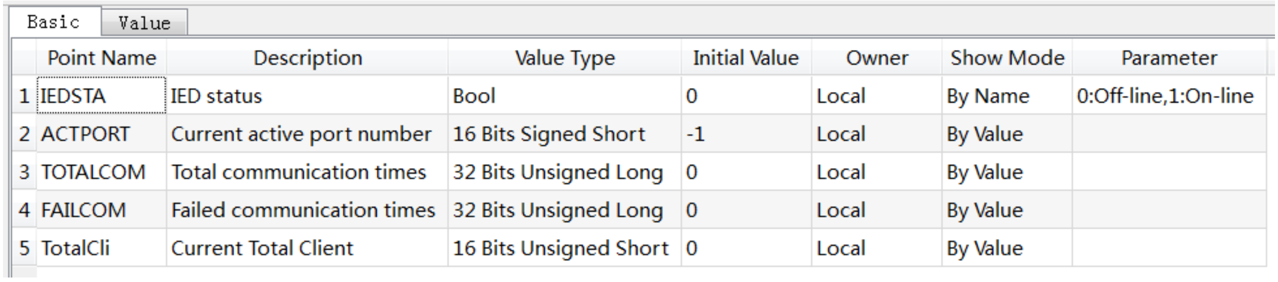
ID	Property
Name	IEC104
Vendor	
Length of Common Address	2
Length of COT	2
Length of Info Object Address	3
K	12
W	8
Counter Polling Mode	Disable
Counter Reset	No
Counter Time Tag	Disable
Cyclic Transmission	Disable
Spontaneous Transmission	Enable
Negative Format	Complementary
Sequence Check	Yes
Group Info	...
Counter Group Info	...
Back Scan Period(s)	0
Time Zone	0

Note: Device properties

No.	Name	Description
1	Name	Device name
2	Vendor	Device vendor
3	Length of Common Address	Number of bytes used by the common address in the communication byte flow
4	Length of COT	Number of bytes used by COT in the communication byte flow
5	Length of Info Object Address	Number of bytes used by the information object address in the communication byte flow
6	K	Maximum number of unconfirmed frames in the buffer

No.	Name	Description
7	W	Maximum number of I frames that can be received by the buffer prior to device confirmation. It should not be greater than 2/3 of K.
8	Counter Polling Mode	Counter polling mode. The modes include mode A, mode B, mode C, and mode D. For details, see the IEC60780-5-101 protocol.
9	Counter Reset	Whether to reset the counter in the counter interrogation
10	Counter Time Tag	Whether counter data carries the time tag during transmission
11	Cyclic Transmission	Whether to cyclically send data based on group definition information
12	Spontaneous Transmission	Whether data can be transmitted spontaneously
13	Negative Format	Method of decoding negative analog values
14	Sequence Check	Whether to check that the sequences of received frames and received frames are matched
15	Group Info	Address range of the information object that transmits data in group mode
16	Counter Group Info	Address range of the information object that transmits counter data in group mode
17	Back Scan Period(s)	Period for sending background scanning data
18	Time Zone	Time zone

Properties of the Pseudo Point View the data area of the EDPS ICT-A+.



	Point Name	Description	Value Type	Initial Value	Owner	Show Mode	Parameter
1	IEDSTA	IED status	Bool	0	Local	By Name	0:Off-line,1:On-line
2	ACTPORT	Current active port number	16 Bits Signed Short	-1	Local	By Value	
3	TOTALCOM	Total communication times	32 Bits Unsigned Long	0	Local	By Value	
4	FAILCOM	Failed communication times	32 Bits Unsigned Long	0	Local	By Value	
5	TotalCli	Current Total Client	16 Bits Unsigned Short	0	Local	By Value	

No.	Name	Description
1	IED STA	Communication status of the current device. The value shows whether the device is on-line or off-line.
2	ACTPORT	Port used by the current channel for communication. For a multi-port link, the value helps locate the active port easily.
3	TOTALCOM	Total number of communications
4	FAILCOM	Number of failed communications. A communication failure means that data is not transmitted successfully or data is received incorrectly.
5	TotalCli	Current number of clients

4.2.3.2.5.IO Parameters

Overview The IO information page in the data area of the EDPS ICT-A+ displays IO parameters of each information point. The system, based on parameter settings, conducts accurate boundary test and data check for IO parameters of each type of data, so as to effectively reduce the configuration data error rate during data input.

1) Analog input

Common Address	Common address in the communication
Point	Point number of the information point

Number

ASDU Type Function type of the application to which the information point belongs

- M_ME_NA_1 (normalized value)
- M_ME_NB_1 (scale value)
- M_ME_NC_1 (short floating-point value)
- M_ME_ND_1(normalized value with quality)
- M_ST_NA_1 (step position information)

Work Mode Work mode of the information point

- Cyclic
- Spontaneous

Time Tag Whether the information point carries the time tag during frame transmission

Offset Offset of the raw data calculated by the information point

Divisor Division factor used by the information point in the calculation of raw data

Dead Zone Value Dead zone value for generating event data. Event data is generated when the absolute value of the difference between the previous transmission value and the current value is greater than the dead zone value.

2) Status input

Common Address Common address in the communication

Point Number Point number of the information point

ASDU Type ASDU transmission type of the information point

- M_SP_NA_1 (single point)
- M_DP_NA_1 (dual points)

Work Work mode of the information point

Mode

- Cyclic
- Spontaneous

Automatic SOE Whether the system uses changed data as the SOE for transmission based on settings after receiving the status change information

- Invalid
- Enabled in the case of the trip value
- Enabled in the case of the close value
- Enabled in the case of status change

SOE Whether the system directly uses the valid SOE data of the device after receiving

COS The system sends change information after receiving status change information.

3) Counter input

Common Address Common address in the communication

Point Number Point number of the information point

Minimum Minimum value for calculating raw data

Maximum Maximum value for calculating raw data

Offset Offset of the raw data calculated by the information point

Divisor Division factor used by the information point in the calculation of raw data

4) Analog output

Common Address Common address in the communication

Point Number Point number of the information point

ASDU Function type of the application to which the information point

Type belongs

- Normalized value
- Scale value
- Short floating-point number

Offset Offset of the raw data calculated by the information point

Divisor Division factor used by the information point in the calculation of raw data

5) Status output

Common Address Common address in the communication

Point Number Point number of the information point

Control Mode Mode for executing control operation commands by the information point

- Direct execution
- SBO

4.2.4.DNP3.0 Protocol Configuration

This section describes how to configure the DNP3.0 collection and forwarding driver modules on the EDPS ICT-A+. The driver information, protocol parameters, device parameters, and IO parameters of each information point are described in the configuration manual. The DNP3.0 collection and forwarding modules of the EDPS fully comply with the protocol. The EDPS ICT-A+ provides a simple and fast way to help users complete the configuration.

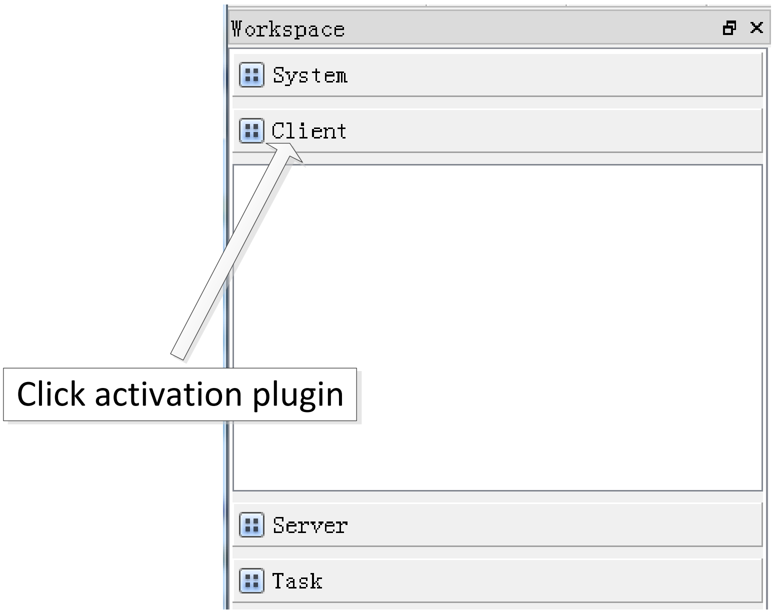
4.2.4.1.Configuration of the DNP3.0 Collection Module

4.2.4.1.1.Driver Information

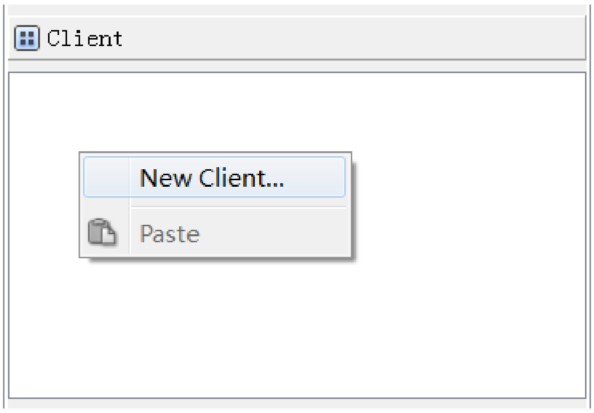
Overview Describe the details about the collection driver.

Create Create a DNP collection driver.

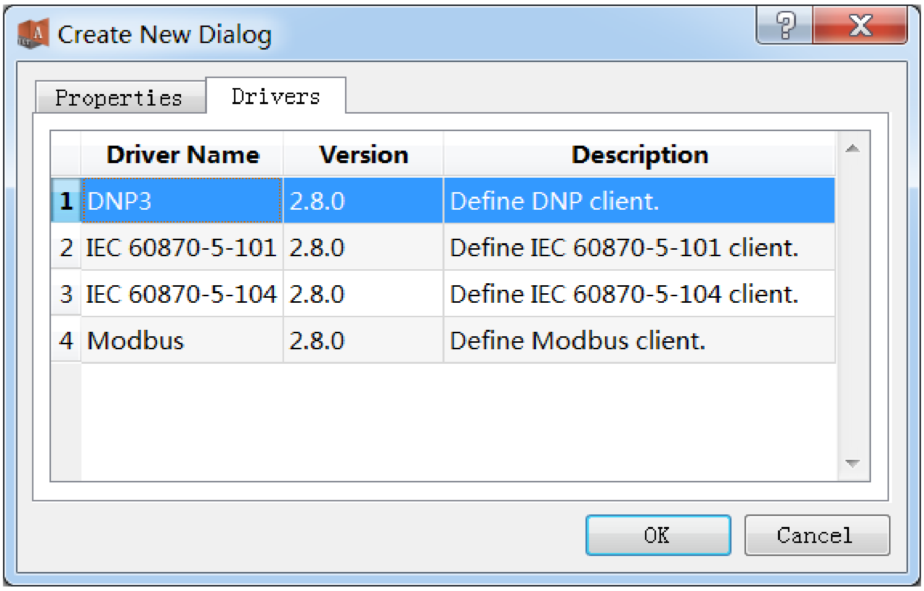
1. Open a project file.
2. Click the **PluginView** tab in the EDPS ICT-A+ management area.
3. Activate the collection service plugin.



4. Right-click in the blank area and choose **New Client** from the shortcut menu. The driver creation dialog box is displayed.

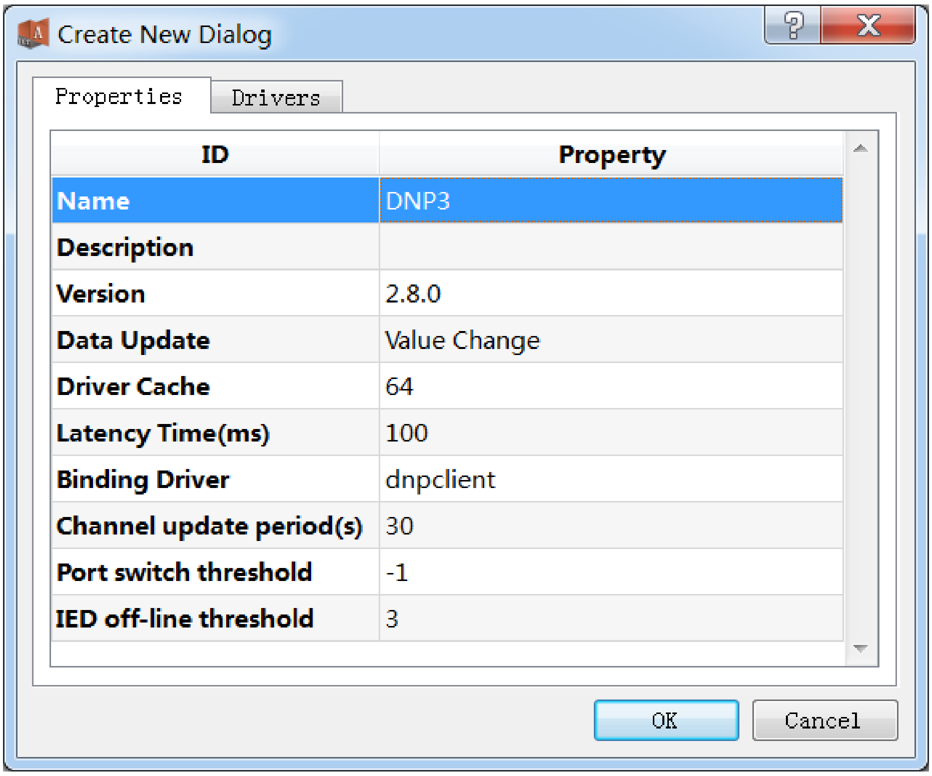


5. On the **Drivers** tab page, select the driver to be created.



	Driver Name	Version	Description
1	DNP3	2.8.0	Define DNP client.
2	IEC 60870-5-101	2.8.0	Define IEC 60870-5-101 client.
3	IEC 60870-5-104	2.8.0	Define IEC 60870-5-104 client.
4	Modbus	2.8.0	Define Modbus client.

6. On the **Properties** tab page, configure basic properties for the target driver.



ID	Property
Name	DNP3
Description	
Version	2.8.0
Data Update	Value Change
Driver Cache	64
Latency Time(ms)	100
Binding Driver	dnpclient
Channel update period(s)	30
Port switch threshold	-1
IED off-line threshold	3

7. Click **OK**.

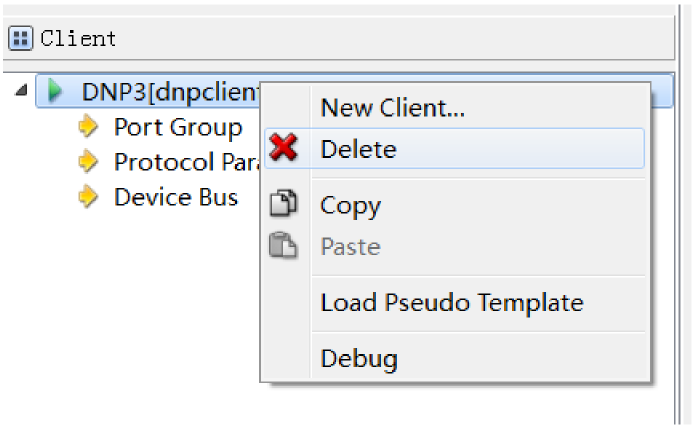
Note: Driver information

No.	Name	Description
1	Name	Driver name to be displayed
2	Description	Driver description
3	Version	Driver version

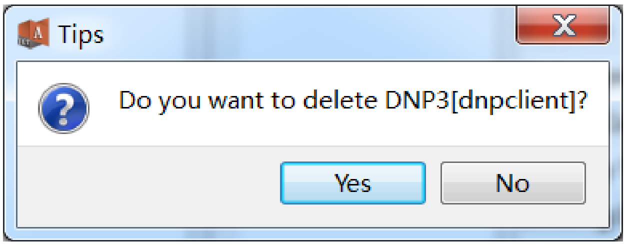
No.	Name	Description
4	Data Update	Data update mode Value Change: The database is updated and other driver protocols are notified only when the value changes. Time Change: The value or time is updated into the database and other driver protocols are notified whenever the value or time changes. Time Update: The value or time is updated whenever it changes, and other driver protocols are notified only when the value changes.
5	Driver Cache	Cache size of the driver
6	Latency Time(ms)	Latency for updating the real-time database The system writes raw data into the real-time database only after the latency time.
7	Binding Driver	Name of the driver module. The value is unique and cannot be modified.
8	Channel update period(s)	Period for updating the IED communication times
9	Port switch threshold	Conditions for multi-port switching. When the number of consecutive communication failures of the master port reaches this threshold, the system switches to another port. The value **-1** indicates that port switching is not performed.
10	IED off-line threshold	IED off-line threshold. When the number of communication failures of a device reaches this threshold, the device is set to be in the off-line state.

Delete Delete a DNP collection driver.

8. Right-click the driver to be deleted and choose **Delete** from the shortcut menu.



9. A dialog box is displayed, asking you whether to delete the driver.

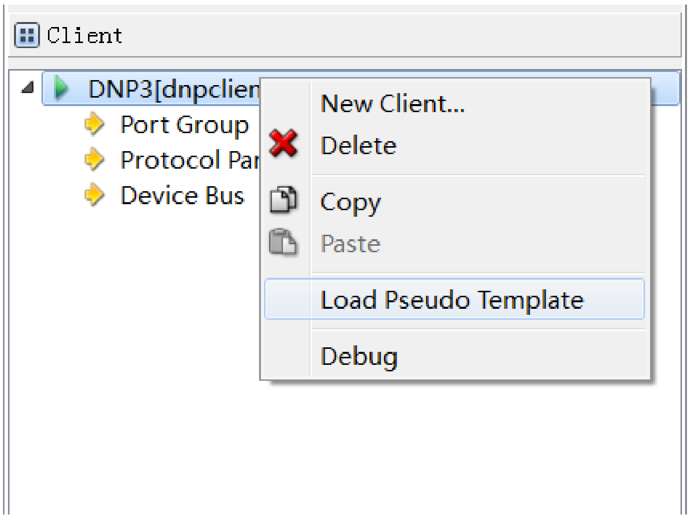


Do you want to delete DNP3[dnpclient]?

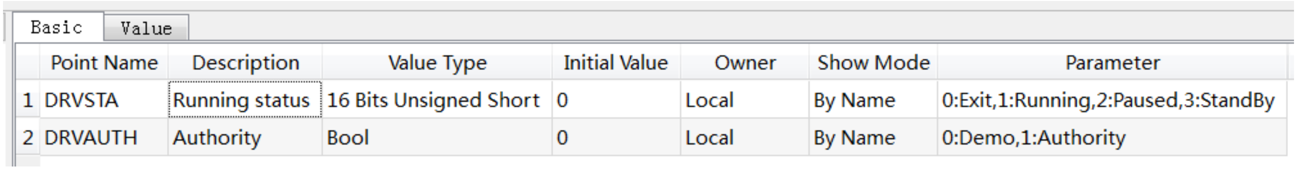
10. Click **Yes** to complete deletion.

Pseudo Template Load a pseudo template from the system template library to the driver.

11. Right-click the driver bar and choose **Load Pseudo Template** from the shortcut menu, to load a pseudo template to the driver.



Note:



	Point Name	Description	Value Type	Initial Value	Owner	Show Mode	Parameter
1	DRVSTA	Running status	16 Bits Unsigned Short	0	Local	By Name	0:Exit,1:Running,2:Paused,3:StandBy
2	DRVAUTH	Authority	Bool	0	Local	By Name	0:Demo,1:Authority

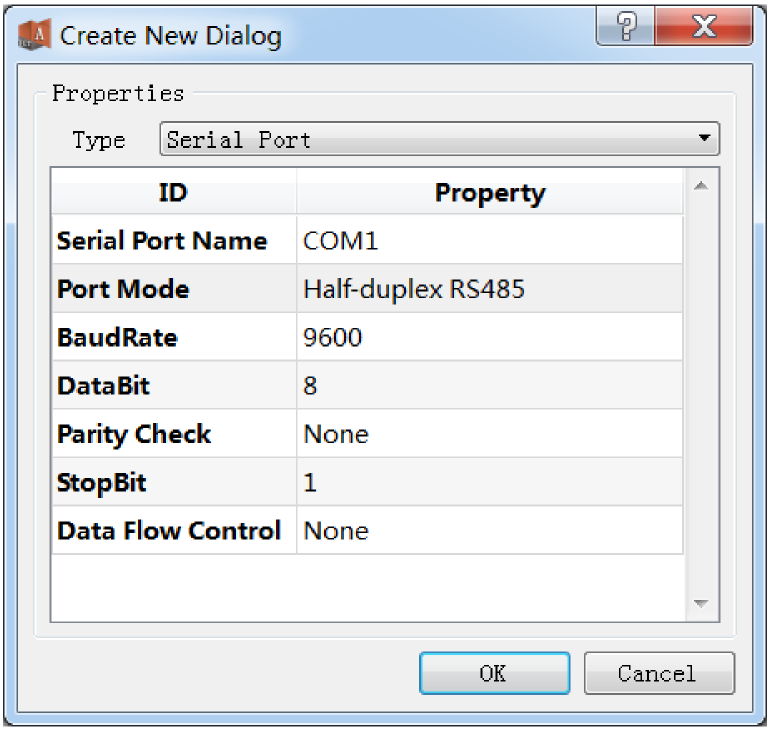
No.	Name	Description
1	DRVSTA	Running status information about the driver
2	DRVAUTH	Authority status of the driver

4.2.4.1.2.Port Group Information

Overview Describe a communication channel.

Create Create a communication channel.

1. Right-click **Port Group** and choose **Create** from the shortcut menu. The port creation dialog box is displayed.



Create New Dialog

Properties

Type: Serial Port

ID	Property
Serial Port Name	COM1
Port Mode	Half-duplex RS485
BaudRate	9600
DataBit	8
Parity Check	None
StopBit	1
Data Flow Control	None

2. Select **Serial Port** or **Network Port** as required.

Note: Properties of a serial channel

No.	Name	Description
1	Serial Port Name	Name of a serial port
2	Port Mode	Work mode of the serial port
3	BaudRate	Baud rate of the serial port
4	DataBit	Data bit of the serial port
5	Parity Check	Parity bit of the serial port

6	StopBit	Stop bit of the serial port
7	Data Flow Control	Data flow control mode of the serial port

Properties of a network channel

No.	Name	Description
1	Port Mode	Work mode of the network port
2	Service IP	IP address of the TCP server or UDP destination address
3	Port Number	Work port number of the network port
4	Broadcast Address	Broadcast address of the network port

Delete Delete a communication channel.

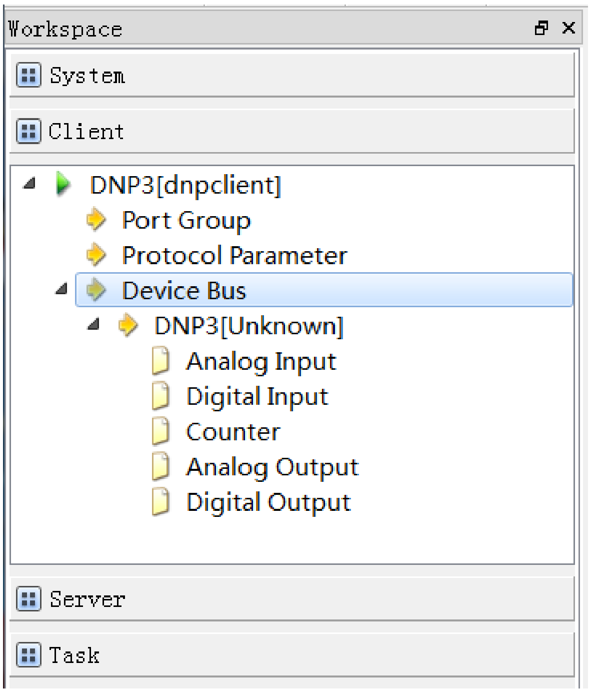
3. Right-click a channel and choose **Delete** from the shortcut menu. Click **Yes** to complete the deletion.

4.2.4.1.3.Protocol Parameters

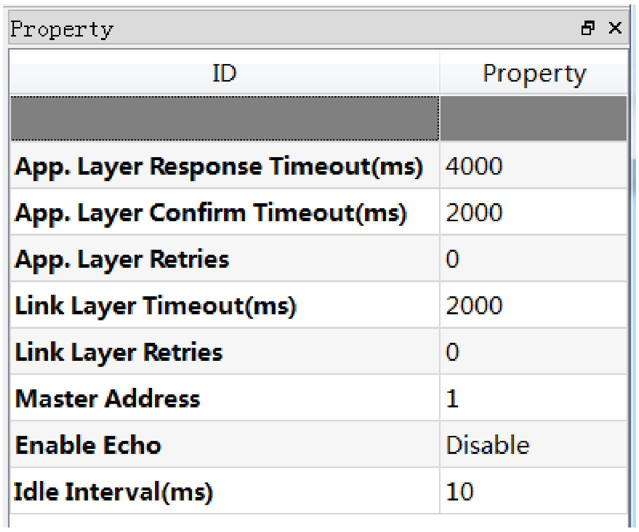
Overview Define the communication protocol parameters of the protocol.

Properties Display the properties of the protocol parameters on the EDPS ICT-A+.

1. Open a project and click the **PluginView** tab in the EDPS ICT-A+ management area.
2. Activate the collection service plugin.
3. Select **Protocol Parameter** in the management area.



4. View the properties of the protocol parameters.



ID	Property
App. Layer Response Timeout(ms)	4000
App. Layer Confirm Timeout(ms)	2000
App. Layer Retries	0
Link Layer Timeout(ms)	2000
Link Layer Retries	0
Master Address	1
Enable Echo	Disable
Idle Interval(ms)	10

Note: Protocol parameters

No.	Name	Description
1	App. Layer Response Timeout(ms)	Timeout interval of the application-layer data response. When the system fails to receive an application-layer response within this interval, the system considers that the device does not respond.
2	App. Layer Confirm	Timeout interval of the frame confirmation. When

No.	Name	Description
	Timeout(ms)	the system fails to receive an application-layer confirmation frame within this interval, the system considers that the communication fails.
3	App. Layer Retries	Retransmission count of data after application-layer data fails to be processed
4	Link Layer Timeout(ms)	Timeout interval of link-layer data processing. When the system fails to receive correct link-layer data within this interval, the system considers that the communication fails.
5	Link Layer Retries	Retransmission count of link data after link data fails to be processed
6	Master Address	Address of the source site for data communication
7	Enable Echo	Whether to process the Echo frames that may appear during information communication. When the Echo frames are not processed, received Echo frames will be deemed as communication error frames.
8	Idle Interval (ms)	Idle waiting duration between two adjacent complete communication processes. A complete communication process starts from the transmission of a data request and ends with the receiving of all valid data.

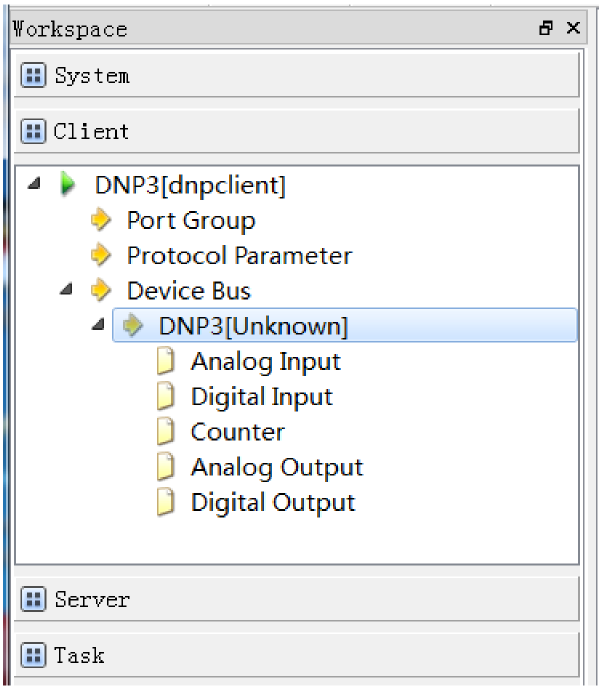
4.2.4.1.4.Device Parameters

Overview Define the device parameters of the protocol.

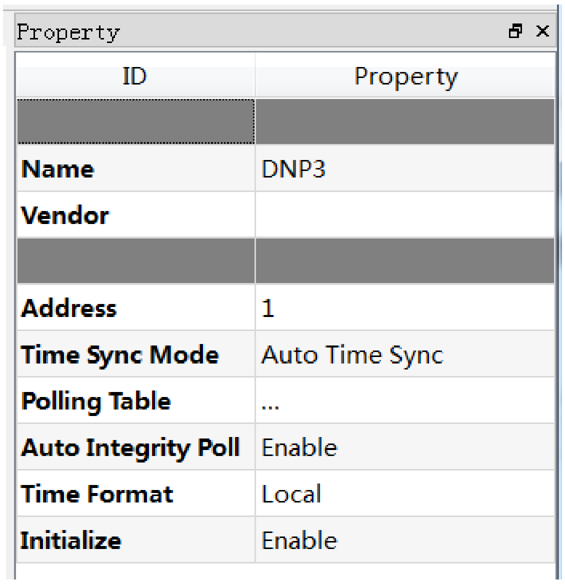
Properties Display the properties of the device parameters.

1. Open a project and click the **PluginView** tab in the EDPS ICT-A+ management area.
2. Activate the collection service plugin.

3. Select any subnode under **Device Bus** in the management area.



4. View the property area of the EDPS ICT-A+.



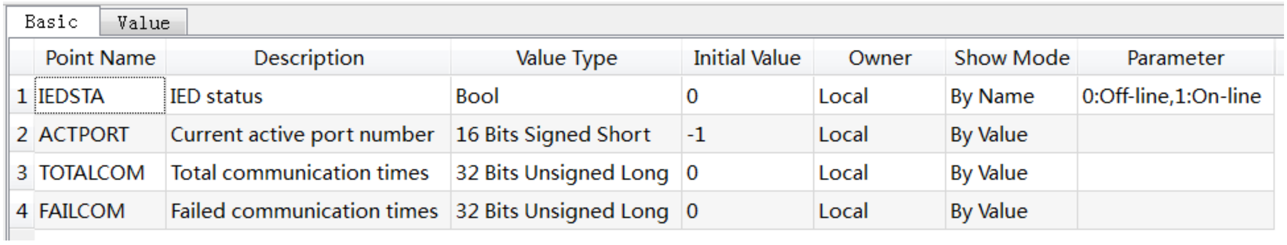
ID	Property
Name	DNP3
Vendor	
Address	1
Time Sync Mode	Auto Time Sync
Polling Table	...
Auto Integrity Poll	Enable
Time Format	Local
Initialize	Enable

Note: Device properties

No.	Name	Description
1	Name	Device name
2	Vendor	Device vendor
3	Address	Physical address of the device
4	Time Sync Mode	Processing mode ● Invalid mode

		● Time synchronization based on time change status (unavailable temporarily) ● Time synchronization based on IIN status ● Automatic time synchronization
5	Polling Table	Polling table for DNP processing
6	Auto Integrity Poll	Whether to conduct general interrogation
7	Time Format	Time conversion mode in the time operation ● UTC ● Local
8	Initialize	Whether to initialize the handshake link

Properties of the Pseudo Point View the data area of the EDPS ICT-A+.



	Point Name	Description	Value Type	Initial Value	Owner	Show Mode	Parameter
1	IEDSTA	IED status	Bool	0	Local	By Name	0:Off-line,1:On-line
2	ACTPORT	Current active port number	16 Bits Signed Short	-1	Local	By Value	
3	TOTALCOM	Total communication times	32 Bits Unsigned Long	0	Local	By Value	
4	FAILCOM	Failed communication times	32 Bits Unsigned Long	0	Local	By Value	

No.	Name	Description
1	IED STA	Communication status of the current device. The value shows whether the device is on-line or off-line.
2	ACTPORT	Port used by the current channel for communication. For a multi-port link, the value helps locate the active port easily.
3	TOTALCOM	Total number of communications
4	FAILCOM	Number of failed communications. A communication failure means that data is not transmitted successfully or data is received incorrectly.

4.2.4.1.5.IO Parameters

Overview The IO information page in the data area of the EDPS ICT-A+ displays IO parameters of each information point. The system, based on parameter settings, conducts accurate boundary test and data check for IO parameters of each type of data, so as to effectively reduce the configuration data error rate during data input.

1) Analog input

Point Number Point number of the information point

2) Status input

Point Number Point number of the information point

3) Counter input

Object Number Number of the object in the counter processing

- 20 - binary counter
- 21 - frozen counter

Point Number Point number of the counter input

4) Analog output

Point Number Point number of the analog output

Data Length Data length of the analog output

- 16-bit integer
- 32-bit integer

5) Status output

Point Number Point number of the status output

Output Mode Output mode of status output

- Open/Close
- Pulse
- Block

Pulse Count Number of pulse outputs

High Level Time Output duration of the pulse rising edge

Low Level Time Output duration of the pulse falling edge

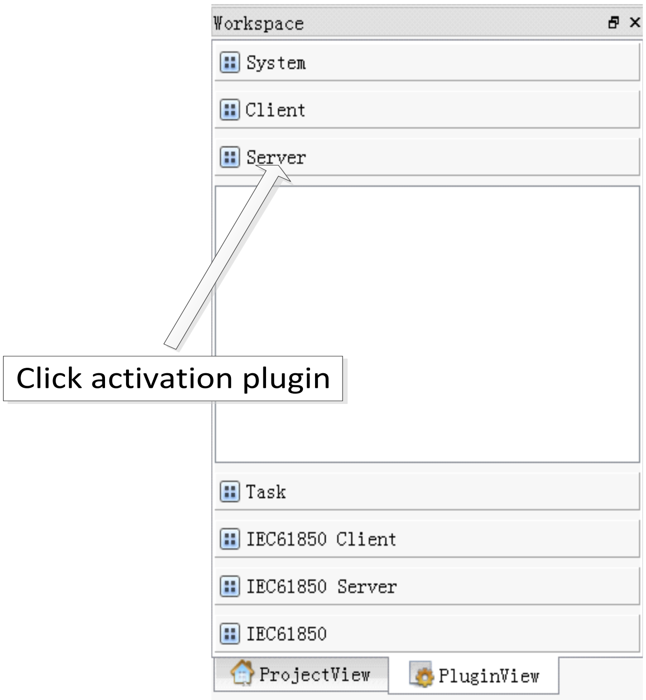
4.2.4.2.Configuration of the DNP3.0 Forwarding Module

4.2.4.2.1.Driver Information

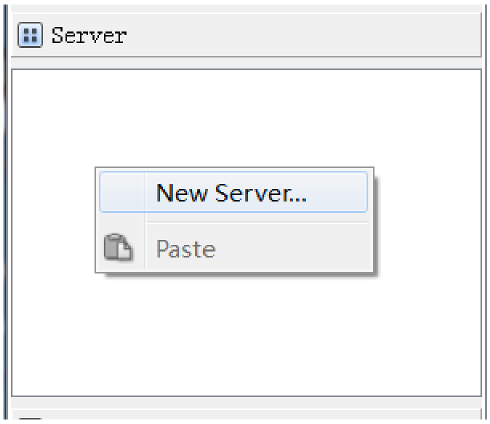
Overview Describe the details about the forwarding driver.

Create Create a DNP forwarding driver.

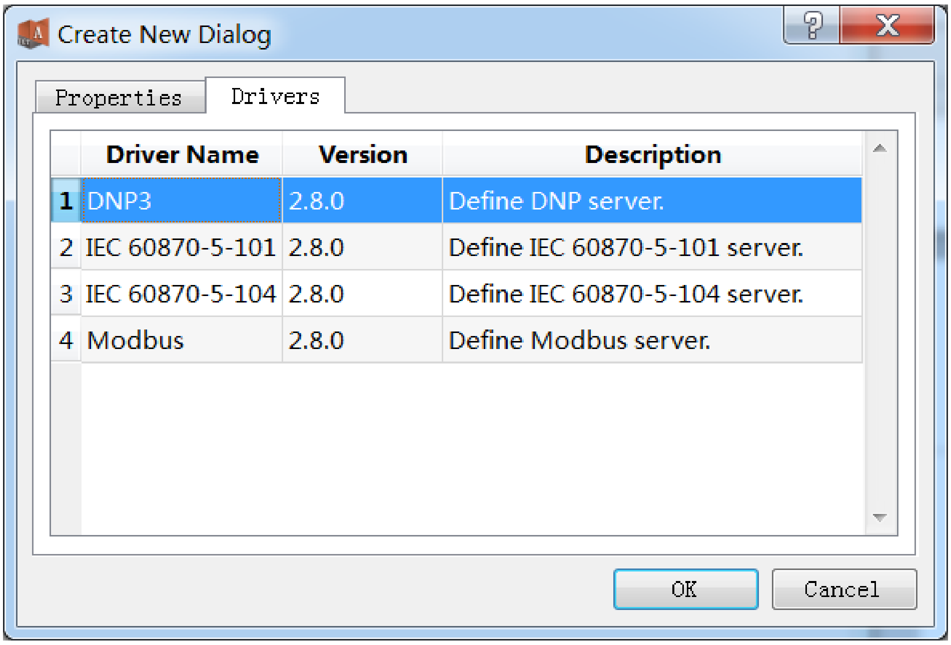
1. Open a project file.
2. Click the **PluginView** tab in the EDPS ICT-A+ management area.
3. Activate the forwarding service plugin.



4. Right-click in the blank area and choose **New Server** from the shortcut menu. The driver creation dialog box is displayed.

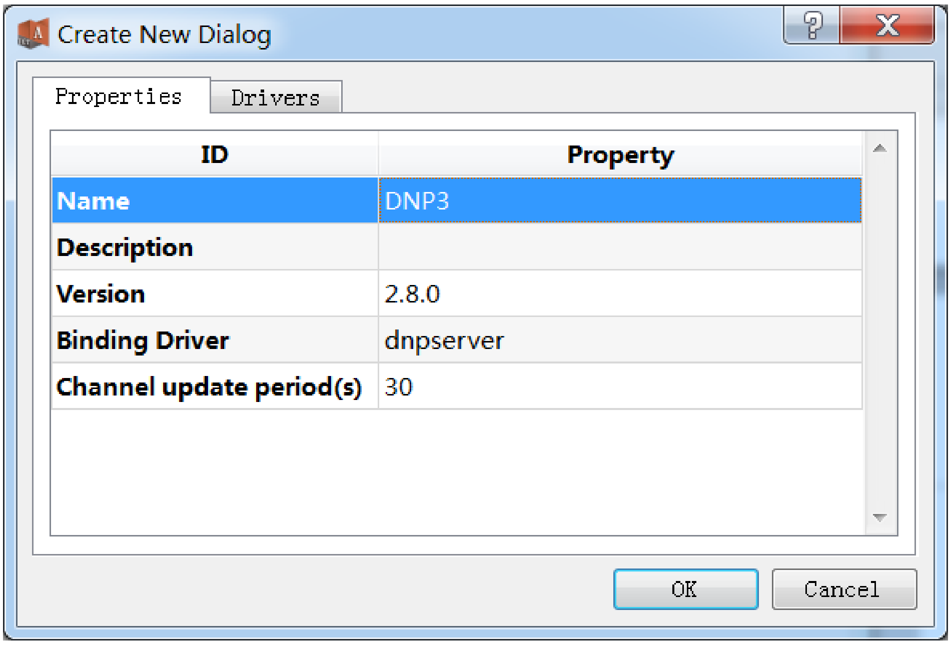


5. On the **Drivers** tab page, select the driver to be created.



	Driver Name	Version	Description
1	DNP3	2.8.0	Define DNP server.
2	IEC 60870-5-101	2.8.0	Define IEC 60870-5-101 server.
3	IEC 60870-5-104	2.8.0	Define IEC 60870-5-104 server.
4	Modbus	2.8.0	Define Modbus server.

6. On the **Properties** tab page, configure basic properties for the target driver.



ID	Property
Name	DNP3
Description	
Version	2.8.0
Binding Driver	dnpserver
Channel update period(s)	30

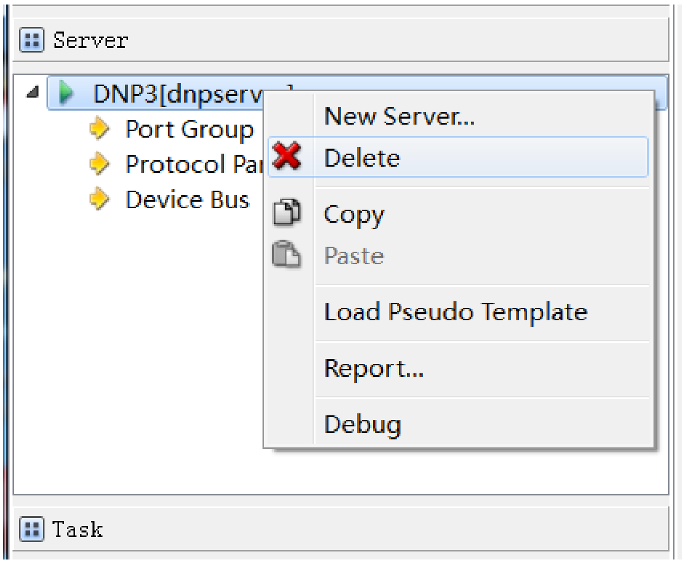
7. Click **OK**.

Note: Driver information

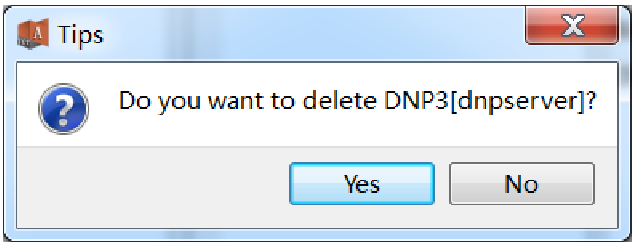
No.	Name	Description
1	Name	Driver name to be displayed
2	Description	Driver description
3	Version	Driver version
4	Binding Driver	Name of the binding module. The value is unique and cannot be modified.
5	Channel update period(s)	Period for updating the IED communication times

Delete Delete a DNP forwarding driver.

8. Right-click the driver to be deleted and choose **Delete** from the shortcut menu.



9. A dialog box is displayed, asking you whether to delete the driver.

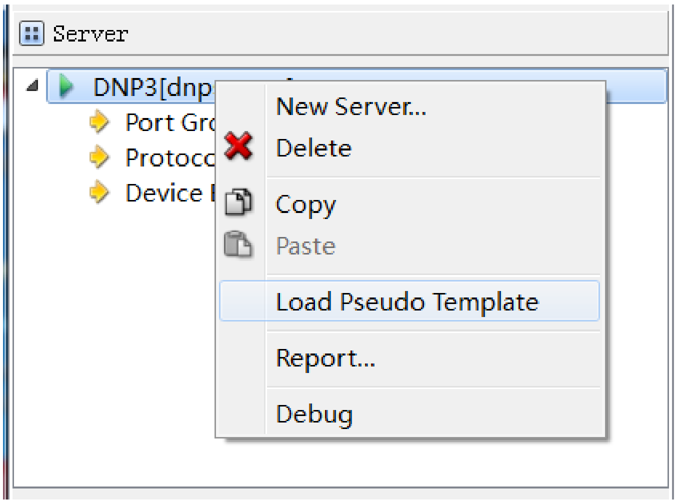


Do you want to delete DNP3[dnpserver]?

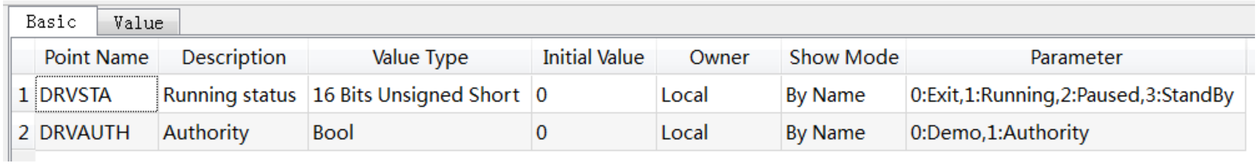
10. Click **Yes** to complete deletion.

Pseudo Template Load a pseudo template from the system template library to the driver.

11. Right-click the driver bar and choose **Load Pseudo Template** from the shortcut menu, to load a pseudo template to the driver.



Note:



	Point Name	Description	Value Type	Initial Value	Owner	Show Mode	Parameter
1	DRVSTA	Running status	16 Bits Unsigned Short	0	Local	By Name	0:Exit,1:Running,2:Paused,3:StandBy
2	DRVAUTH	Authority	Bool	0	Local	By Name	0:Demo,1:Authority

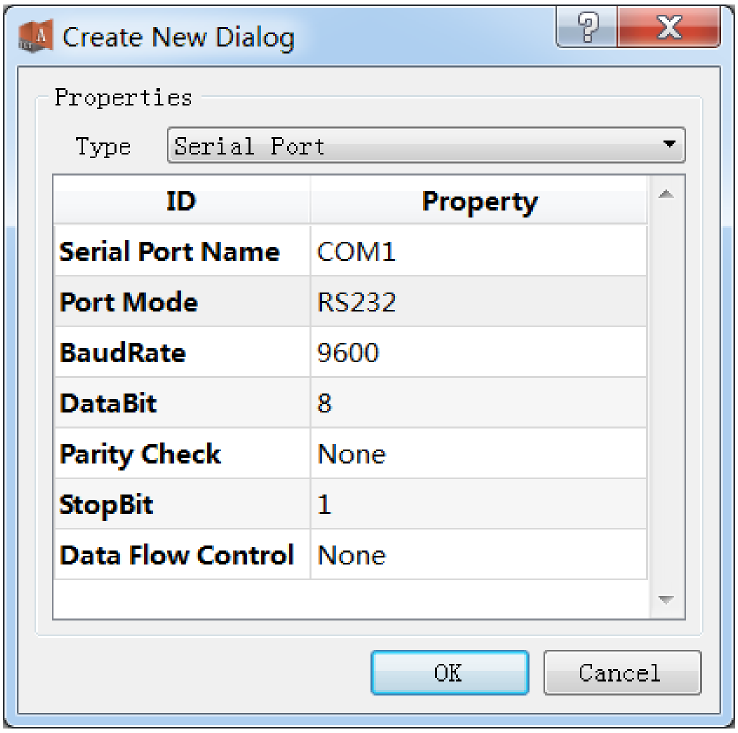
No.	Name	Description
1	DRVSTA	Running status information about the driver
2	DRVAUTH	Authority status of the driver

4.2.4.2.2.Port Group Information

Overview Describe a communication channel.

Create Create a communication channel.

1. Right-click **Port Group** and choose **Create** from the shortcut menu. The port creation dialog box is displayed.



Type: Serial Port

ID	Property
Serial Port Name	COM1
Port Mode	RS232
BaudRate	9600
DataBit	8
Parity Check	None
StopBit	1
Data Flow Control	None

2. Select **Serial Port** or **Network Port** as required.

   Note: Properties of a serial channel

No.	Name	Description
1	Serial Port Name	Name of a serial port

No.	Name	Description
2	Port Mode	Work mode of the serial port
3	BaudRate	Baud rate of the serial port
4	DataBit	Data bit of the serial port
5	Parity Check	Parity bit of the serial port
6	StopBit	Stop bit of the serial port
7	Data Flow Control	Data flow control mode of the serial port

Properties of a network channel

No.	Name	Description
1	Port Mode	Work mode of the network port
2	Service IP	IP address of the TCP server or UDP destination address
3	Port Number	Work port number of the network port
4	Broadcast Address	Broadcast address of the network port

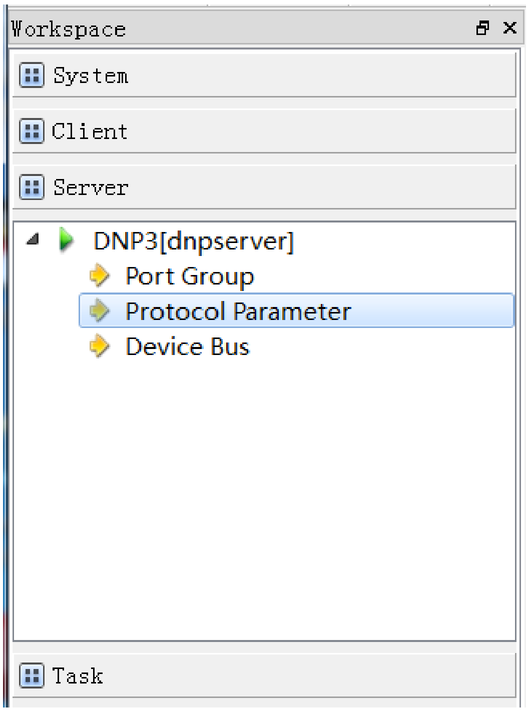
Delete Delete a communication channel.

3. Right-click a channel and choose **Delete** from the shortcut menu. Click **Yes** to complete the deletion.

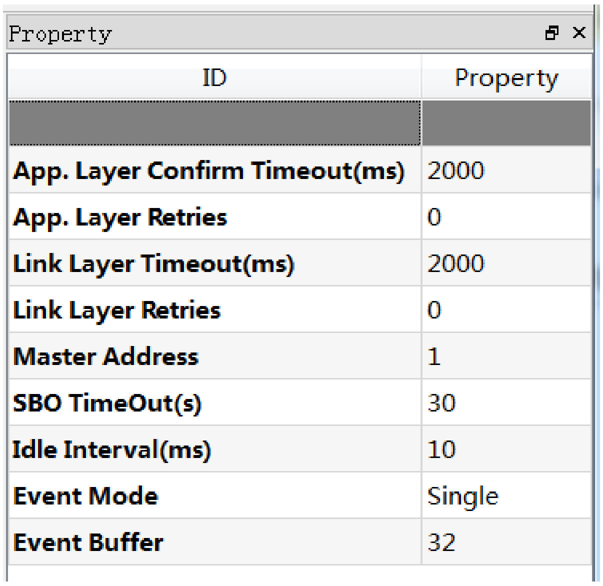
4.2.4.2.3.Protocol Parameters

Overview Define the communication protocol parameters of the protocol.

1. Open a project and click the **PluginView** tab in the EDPS ICT-A+ management area.
2. Activate the forwarding service plugin.
3. Select **Protocol Parameter** in the management area.



4. View the properties of the protocol parameters.



ID	Property
App. Layer Confirm Timeout(ms)	2000
App. Layer Retries	0
Link Layer Timeout(ms)	2000
Link Layer Retries	0
Master Address	1
SBO TimeOut(s)	30
Idle Interval(ms)	10
Event Mode	Single
Event Buffer	32

Note: Protocol parameters

No.	Name	Description
1	App. Layer Confirm Timeout(ms)	Timeout interval of the frame confirmation. When the system fails to receive an application-layer confirmation frame within this interval, the system considers that the communication fails.
2	App. Layer Retries	Retransmission count after application-layer data fails to be processed

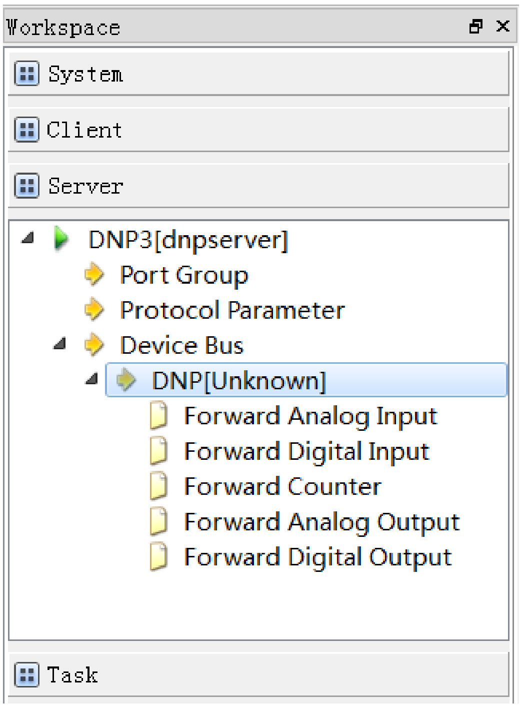
No.	Name	Description
3	Link Layer Timeout(ms)	Timeout interval of link-layer data processing. When the system fails to receive correct link-layer data within this interval, the system considers that the communication fails.
4	Link Layer Retries	Retransmission count of link data after link data fails to be processed
5	Master Address	Address of the source site for data communication
6	SBO Timeout(s)	Waiting timeout interval for executing an SBO command
7	Idle Interval(ms)	Idle waiting duration between two adjacent complete communication processes. A complete communication process starts from the transmission of a data request and ends with the receiving of all valid data.
8	Event Mode	Event processing mode. Single-channel or multi-channel mode is supported.
9	Event Buffer	Size of the event buffer

4.2.4.2.4.Device Parameters

Overview Define the device parameters of the protocol.

Properties Display the properties of the device parameters.

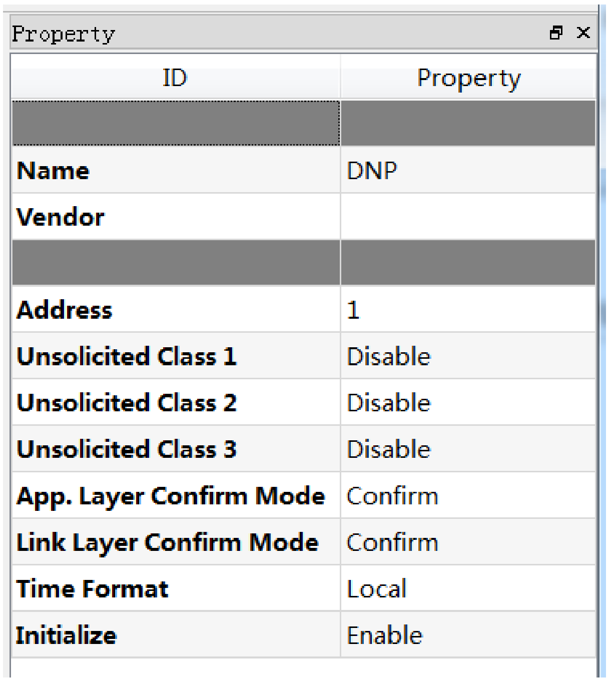
1. Open a project and click the **PluginView** tab in the EDPS ICT-A+ management area.
2. Activate the forwarding service plugin.
3. Select any subnode under **Device Bus** in the management area.



Workspace

- System
- Client
- Server
  - DNP3[dnpserver]
    - Port Group
    - Protocol Parameter
    - Device Bus
      - DNP[Unknown]
        - Forward Analog Input
        - Forward Digital Input
        - Forward Counter
        - Forward Analog Output
        - Forward Digital Output
- Task

4. View the property area of the EDPS ICT-A+.



Property

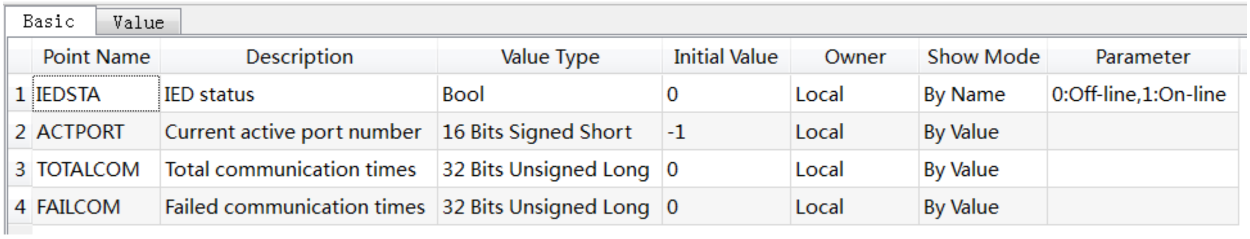
ID	Property
Name	DNP
Vendor	
Address	1
Unsolicited Class 1	Disable
Unsolicited Class 2	Disable
Unsolicited Class 3	Disable
App. Layer Confirm Mode	Confirm
Link Layer Confirm Mode	Confirm
Time Format	Local
Initialize	Enable

Note: Device properties

No.	Name	Description
1	Name	Device name
2	Vendor	Device vendor
3	Address	Physical address of the device
4	Unsolicited Class 1	Whether to report class 1 data actively

No.	Name	Description
5	Unsolicited Class 2	Whether to report class 2 data actively
6	Unsolicited Class 3	Whether to report class 3 data actively
7	App. Layer Confirm Mode	Application-layer communication confirmation mode. The default value is **Confirm**.
8	Link Layer Confirm Mode	Link-layer communication confirmation mode. The default value is **Confirm**.
9	Time Format	Time format of the device
10	Initialize	Whether to initialize the handshake link

Properties of the Pseudo Point View the data area of the EDPS ICT-A+.



	Point Name	Description	Value Type	Initial Value	Owner	Show Mode	Parameter
1	IEDSTA	IED status	Bool	0	Local	By Name	0:Off-line,1:On-line
2	ACTPORT	Current active port number	16 Bits Signed Short	-1	Local	By Value	
3	TOTALCOM	Total communication times	32 Bits Unsigned Long	0	Local	By Value	
4	FAILCOM	Failed communication times	32 Bits Unsigned Long	0	Local	By Value	

No.	Name	Description
1	IED STA	Communication status of the current device. The value shows whether the device is on-line or off-line.
2	ACTPORT	Port used by the current channel for communication. For a multi-port link, the value helps locate the active port easily.
3	TOTALCOM	Total number of communications
4	FAILCOM	Number of failed communications. A communication failure means that data is not transmitted successfully or data is received incorrectly.

4.2.4.2.5.IO Parameters

Overview The IO information page in the data area of the EDPS ICT-A+ displays IO parameters of each information point. The system, based on parameter settings, conducts accurate boundary test and data check for IO parameters of each type of data, so as to effectively reduce the configuration data error rate during data input.

1) Analog input

Point Number Index number of the information point

Category Processing level of the current information point

- Invalid
- Class 1 data
- Class 2 data
- Class 3 data

Data Length Data length

- 16-bit integer
- 32-bit integer
- 32-bit floating-point number
- 64-bit double-precision number

Time Tag Whether to add time tag to data

Offset Offset of the value of the information point

Divisor Division factor required in data changes of the information point

Dead Zone Value Dead zone value for generating event data. Event data is generated when the absolute value of the difference between the previous transmission value and the current value is greater than the dead zone value.

2) Status input

Point Number Index number of the information point

Category Processing level of the current information point

- Invalid
- Class 1 data
- Class 2 data

- Class 3 data

Automatic SOE Whether the system uses changed data as the SOE for transmission based on settings after receiving the status change information

- Invalid
- Enabled in the case of the trip value
- Enabled in the case of the close value
- Enabled in the case of status change

SOE Whether the system directly forwards valid SOE data after receiving

Data Length Data length of the information point

- 1-bit status
- 2-bit status

3) Counter input

Point Number Index number of the information point

Category Processing level of the current information point

- Invalid
- Class 1 data
- Class 2 data
- Class 3 data

Data Type Data type of the information point

- Binary counter
- Frozen counter

Data Length Data length

- 16-bit integer
- 32-bit integer

Minimum Minimum value of the information point in data conversion

Maximum Maximum value of the information point in data conversion

Offset Offset of the value of the information point

Divisor Division factor required in data changes of the information point

Dead Zone Value Dead zone value for generating event data. Event data is generated when the absolute value of the difference between the previous transmission value and the current value is greater than the dead zone value.

4) Analog output

Point Number Index number of the information point

Data Length Processing level of the current information point

- 16-bit integer
- 32-bit integer

Offset Offset of the value of the information point

Divisor Division factor required in data changes of the information point

5) Status output

Point Number Index number of the information point

4.3.FAQs

4.3.1.Hardware Faults and Troubleshooting

4.3.1.1.Indicators on the Panel Are Off After Power-on

- The power voltage is lower than the normal startup voltage.

  Before switching on the power supply, use a multimeter to measure the voltage at both ends (+/L and -/N) of the power supply. If the voltage does not reach the startup voltage, check the input power.
- The fuse burns out.

Disconnect the power supply, remove the cover, and check whether the fuse burns out. If yes, replace it with a new one. If no, check whether the +/L and -/N ends are short-circuited.

4.3.1.2.The Working Power Supply Is Normal but the Main Board Is Not Working

- The connection between the CPU board and the main board is insecure.
  Remove and then insert the CPU board to ensure that the bus connection is secure.
- The working power supply of the main board is faulty.
  Use a multimeter to measure the 3.3 V DC on the main board.

4.3.1.3.The Network and Device Communication Are Interrupted

- The network cable is abnormal.
  Check whether the network cable connection is correct.
- The network connection mode is incorrect.
  If the network port of the PC is not self-adaptive, use a crossover cable to connect to the device or use two straight-through network cables to connect to the device through a switch or hub.
- The PC and the device are not in the same network segment.
  Check whether the local network address of the PC and the device are in the same network segment.
- There is interference from the wireless network.
  Check whether the wireless network is within the same network segment as the local network address. If yes, disable the wireless network or use another network segment.

4.3.1.4.The Serial Port Communication Is Abnormal

- The communication cable does not meet requirements.

The on-site communication environment is very harsh and Category 5 enhanced twisted pairs must be used to basically meet technical requirements. Communication cables of the general type may cause communication instability and bit errors.

- The communication distance is very long and there are too many devices in the communication link.

  Each communication mode has strict requirements for the communication cable length. The communication distance supported by RS485 cables is 32 devices in 1200 m in ideal cases. The on-site environment is complex and the best communication distance supported may be 10 devices in 400 m to 500 m.

- No terminal resistor is used.

  When RS485 communication is adopted, capacitor interference and echo signals may be generated during communication because there is more than one device in the communication link. Therefore, a 120-ohm terminal resistor needs to be added to the receive end of the last device in the communication link, to eliminate interference.

- The level does not match.

  The RS-485 communication ports on old devices of some vendors use the TTL level rather than the differentiated level. Therefore, a converter is required.

- The voltage of the communication port is very low.

  The protection devices of some vendors need 5 V or 12 V power to supply power to the communication ports. Therefore, a power supply needs to be connected.

- The serial port communication mode is not configured correctly on the software.

  The serial port communication mode of the software is configured based on actual conditions. Instead, the serial port channel should be configured based on the actual link.

- The configuration of serial port properties does not match the device.

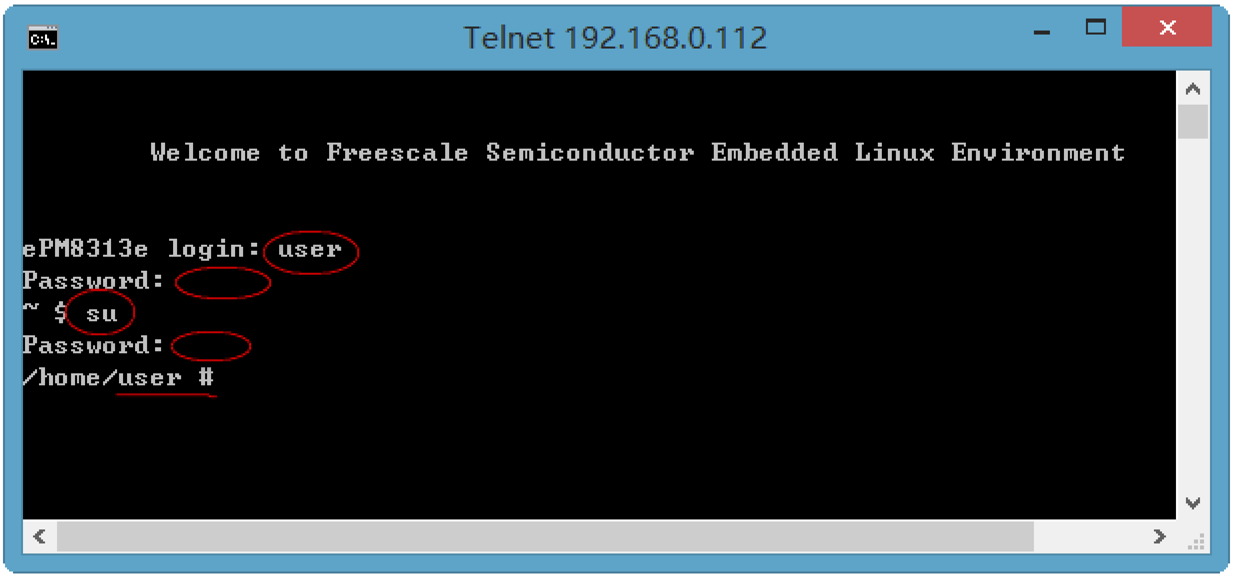
  The properties of serial port communication vary with the vendor and protocol. Therefore, configure the serial port properties based on actual conditions of IEDs.

4.3.2.Software Problems and Solutions

4.3.2.1.How Do I Telnet to an Access Device Remotely

- Enter **cmd** in the **Run** dialog box. A dialog box is displayed.
- Enter **telnet 192.168.0.112** (server IP address).
- Enter the user name and password to log in to the device, as shown in the following figure.

  Note*: The first password is **user** and the second password is **root**. Both passwords are not displayed when entered.*

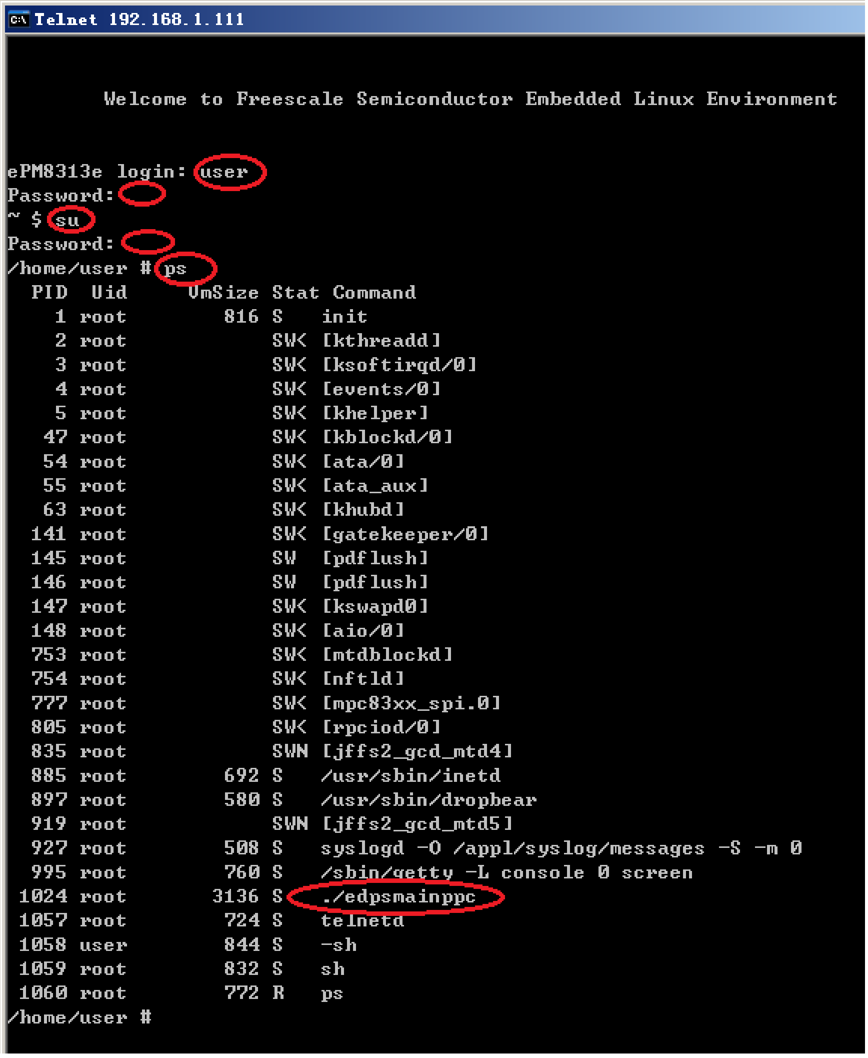


```
        Welcome to Freescale Semiconductor Embedded Linux Environment

ePM8313e login: user
Password:
~ $ su
Password:
/home/user #
```

Figure 271 Telnet screen

4.3.2.2.How do I Check Whether the Main Application Is Running

- Telnet to the device.
- Enter **ps**. If information as shown in the following figure is displayed, the main application **dpsmainppc** is running.



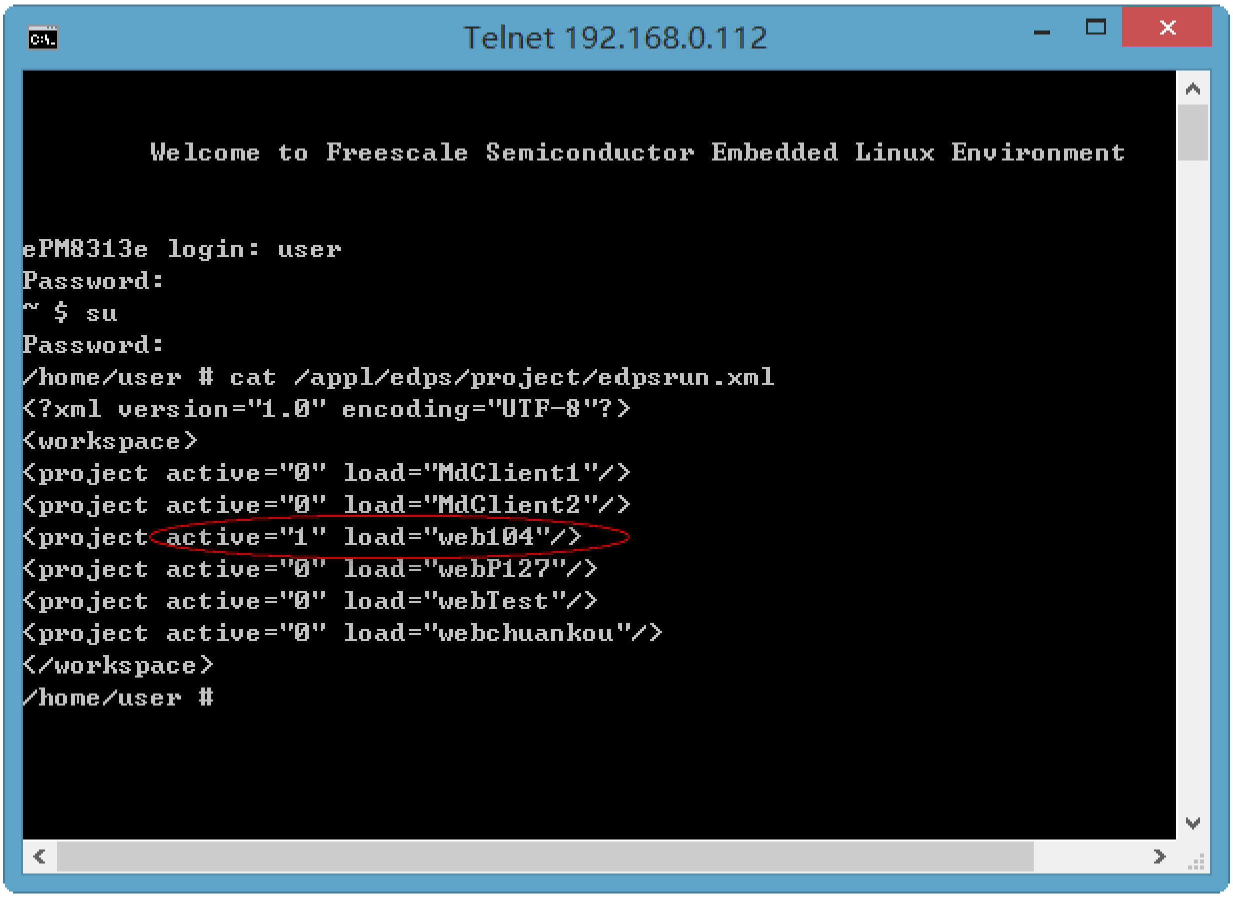
```
Telnet 192.168.1.111

        Welcome to Freescale Semiconductor Embedded Linux Environment

ePM8313e login: user
Password:
~ $ su
Password:
/home/user # ps
  PID  Uid     VmSize Stat Command
    1 root        816 S   init
    2 root            SW< [kthreadd]
    3 root            SW< [ksoftirqd/0]
    4 root            SW< [events/0]
    5 root            SW< [khelper]
   47 root            SW< [kblockd/0]
   54 root            SW< [ata/0]
   55 root            SW< [ata_aux]
   63 root            SW< [khubd]
  141 root            SW< [gatekeeper/0]
  145 root            SW  [pdflush]
  146 root            SW  [pdflush]
  147 root            SW< [kswapd0]
  148 root            SW< [aio/0]
  753 root            SW< [mtdblockd]
  754 root            SW< [nftld]
  777 root            SW< [mpc83xx_spi.0]
  805 root            SW< [rpciod/0]
  835 root            SWN [jffs2_gcd_mtd4]
  885 root        692 S   /usr/sbin/inetd
  897 root        580 S   /usr/sbin/dropbear
  919 root            SWN [jffs2_gcd_mtd5]
  927 root        508 S   syslogd -O /appl/syslog/messages -S -m 0
  995 root        760 S   /sbin/getty -L console 0 screen
 1024 root       3136 S   ./edpsmainppc
 1057 root        724 S   telnetd
 1058 user        844 S   -sh
 1059 root        832 S   sh
 1060 root        772 R   ps
/home/user #
```

Figure 272 Main application running screen

4.3.2.3.How Can I Check the Current Running Project

- Telnet to the device.
- Enter **cat /appl/edps/project/edpsrun.xml** and press **Enter**, as shown in the following figure.

Note: active="1" indicates the project that is running currently.



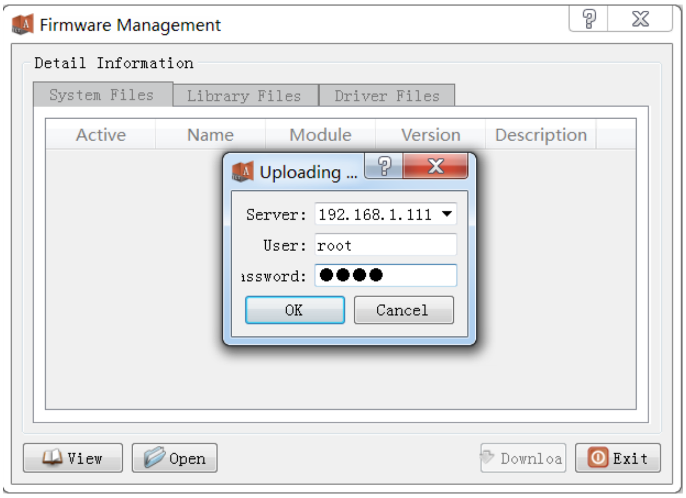
```
        Welcome to Freescale Semiconductor Embedded Linux Environment

ePM8313e login: user
Password:
~ $ su
Password:
/home/user # cat /appl/edps/project/edpsrun.xml
<?xml version="1.0" encoding="UTF-8"?>
<workspace>
<project active="0" load="MdClient1"/>
<project active="0" load="MdClient2"/>
<project active="1" load="web104"/>
<project active="0" load="webP127"/>
<project active="0" load="webTest"/>
<project active="0" load="webchuankou"/>
</workspace>
/home/user #
```

Figure 273 Screen of current running project

4.3.2.4.How Do I View and Update the Driver File

Use the Integration Configuration Environment (ICT-A+) tool to view the driver.

- Start the ICT-A+ tool and choose **Management** > **Firmwares** from the main menu. In **Firmware Management** dialog box, click **View** and enter the server address (IP address of the network port), user name (**root**), and password (**root**), as shown in the following figure.



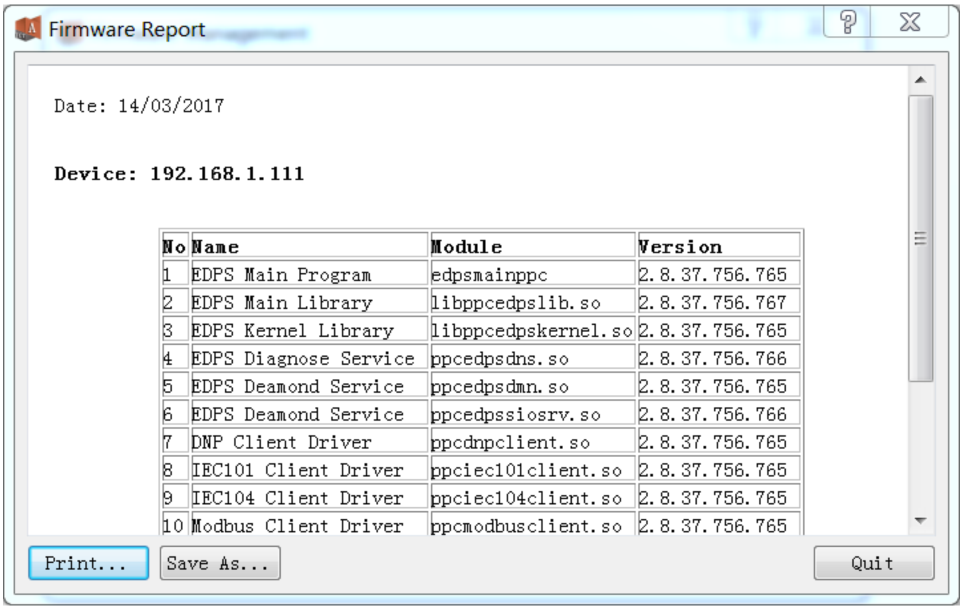
Server: 192.168.1.111

User: root

ıssword: ●●●●

Figure 274 Firmware query

- Click **OK**. Information about drivers in the device is displayed, as shown in the following figure.



Date: 14/03/2017

Device: 192.168.1.111

No	Name	Module	Version
1	EDPS Main Program	edpsmainppc	2.8.37.756.765
2	EDPS Main Library	libppcedpslib.so	2.8.37.756.767
3	EDPS Kernel Library	libppcedpskernel.so	2.8.37.756.765
4	EDPS Diagnose Service	ppcedpsdns.so	2.8.37.756.766
5	EDPS Deamond Service	ppcedpsdmn.so	2.8.37.756.765
6	EDPS Deamond Service	ppcedpssiosrv.so	2.8.37.756.766
7	DNP Client Driver	ppcdnpclient.so	2.8.37.756.765
8	IEC101 Client Driver	ppciec101client.so	2.8.37.756.765
9	IEC104 Client Driver	ppciec104client.so	2.8.37.756.765
10	Modbus Client Driver	ppcmodbusclient.so	2.8.37.756.765

Figure 275 Firmware information

Update the drivers as follows.

- Start the ICT-A+ tool and choose **Management** > **Firmwares** from the shortcut menu. In the **Firmware Management** dialog box, click **Open** and locate the **linux_ppc** folder where firmware is stored, as shown in the following figure.

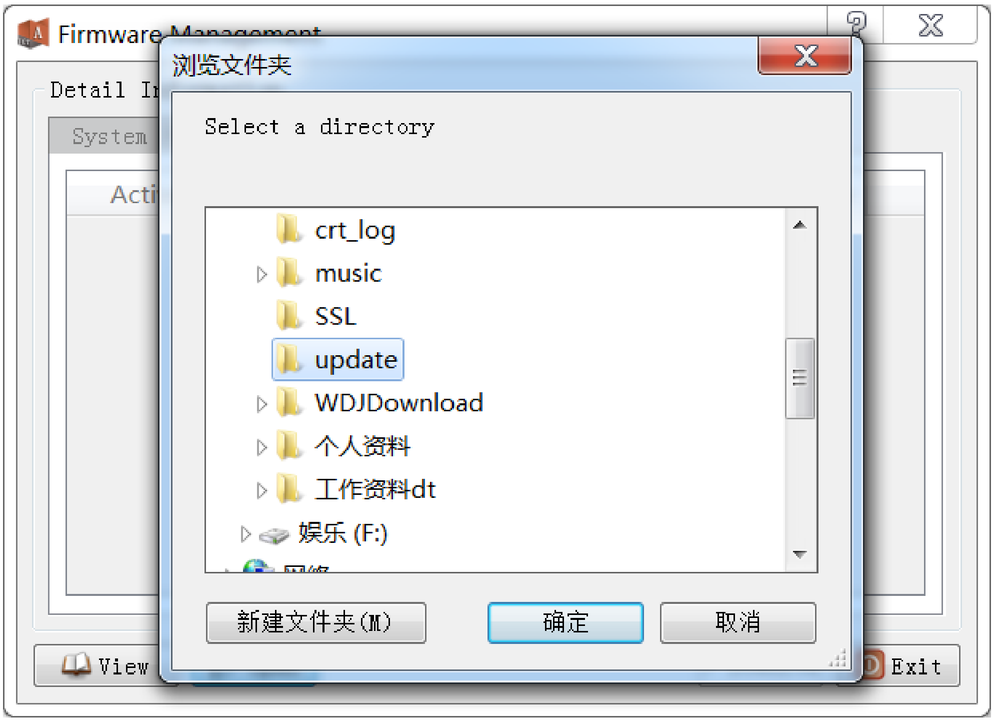
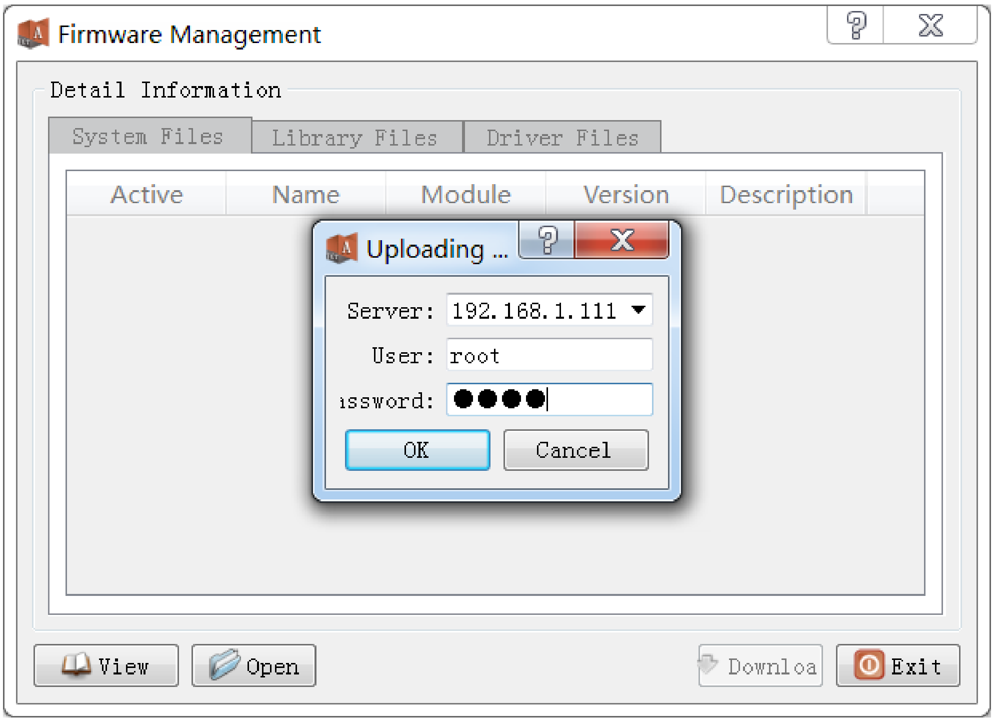


Figure 276 Driver storage folder

- Click **OK**. The detailed information about the drivers is displayed. Select a driver file and click **Download**. In the displayed dialog box, enter the server IP address, user name (**root**), and password (**root**), and click **OK**, as shown in the following figure. Restart the device.



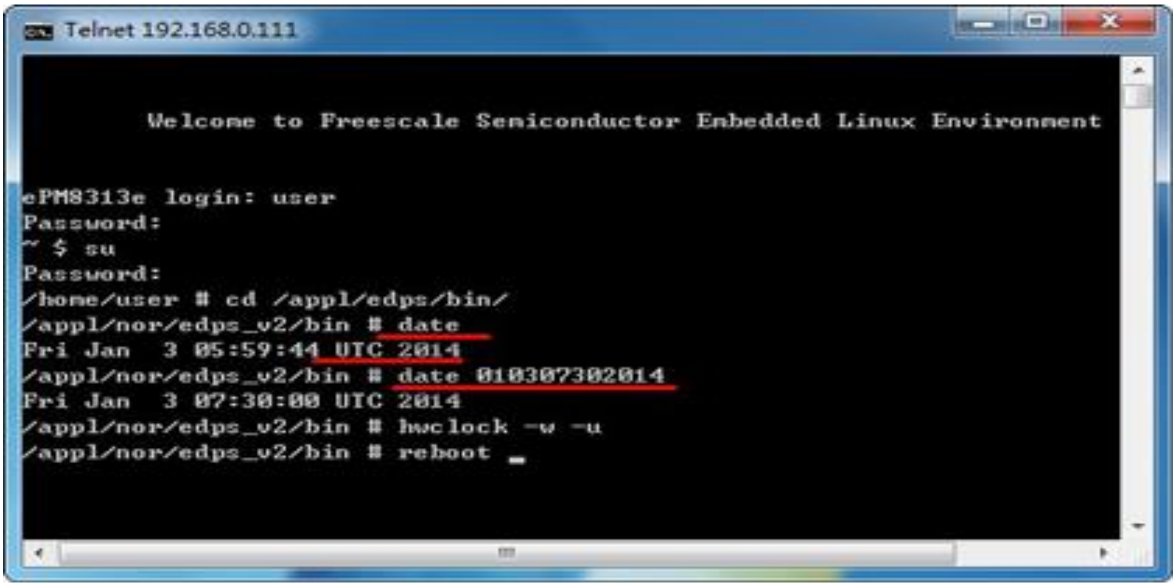
Server: 192.168.1.111
User: root
issword: ●●●●

Figure 277 Driver update

4.3.2.5.How Do I Change System Time

Use the command as shown in the following figure to change the system time.

Note: The date is in the format of MMDDHHMMYYYY (M-month, D-date, H-hour, M-minute, Y-year). The system time of the device uses the UTC time.



```
        Welcome to Freescale Semiconductor Embedded Linux Environment

ePM8313e login: user
Password:
~ $ su
Password:
/home/user # cd /appl/edps/bin/
/appl/nor/edps_v2/bin # date
Fri Jan  3 05:59:44 UTC 2014
/appl/nor/edps_v2/bin # date 010307302014
Fri Jan  3 07:30:00 UTC 2014
/appl/nor/edps_v2/bin # hwclock -w -u
/appl/nor/edps_v2/bin # reboot _
```

Figure 278 Changing the system time

4.3.2.6.How Do I Modify the Device IP Address

Method 1: Use the ICT-A+ tool to modify the device IP address in the project configuration.

- Start the ICT-A+ tool, access **System** and select **Property**.
- Select **Network Configigiguration** in the property area on the right side and double-click to open the table editor.
- Click **New**, as shown in the following figure. Modify the IP address of the relevant network port (select the network adapter based on the device model).
- Click **OK** to save the project and download it to the device. Then, power off and restart the device.

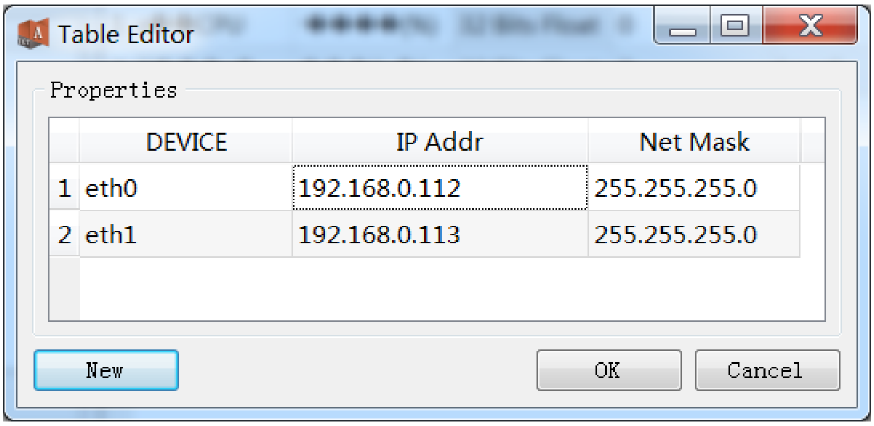


Table Editor

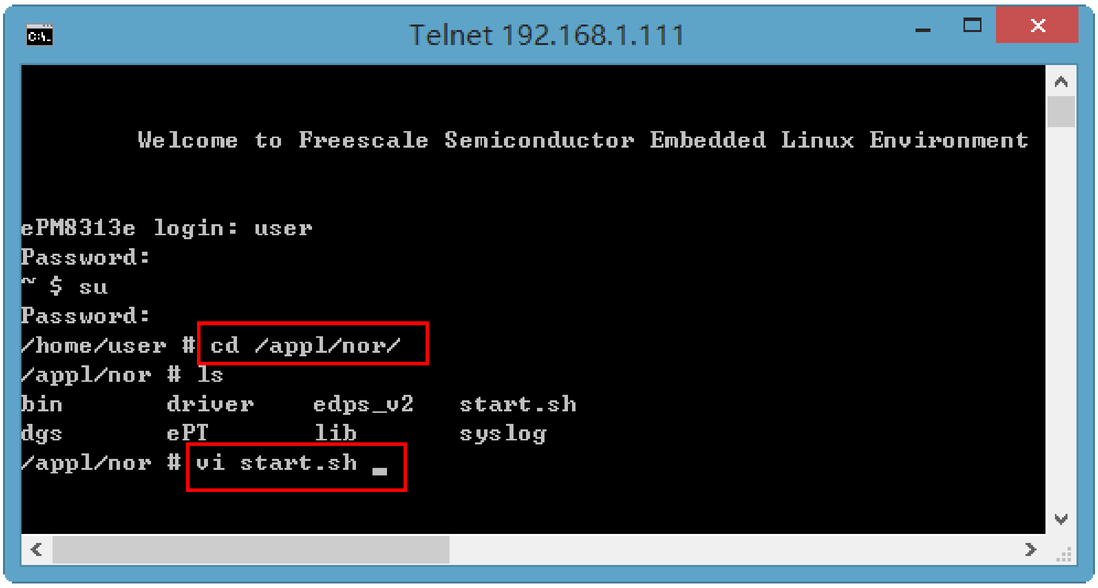
Properties

	DEVICE	IP Addr	Net Mask
1	eth0	192.168.0.112	255.255.255.0
2	eth1	192.168.0.113	255.255.255.0

Figure 279 Network configuration

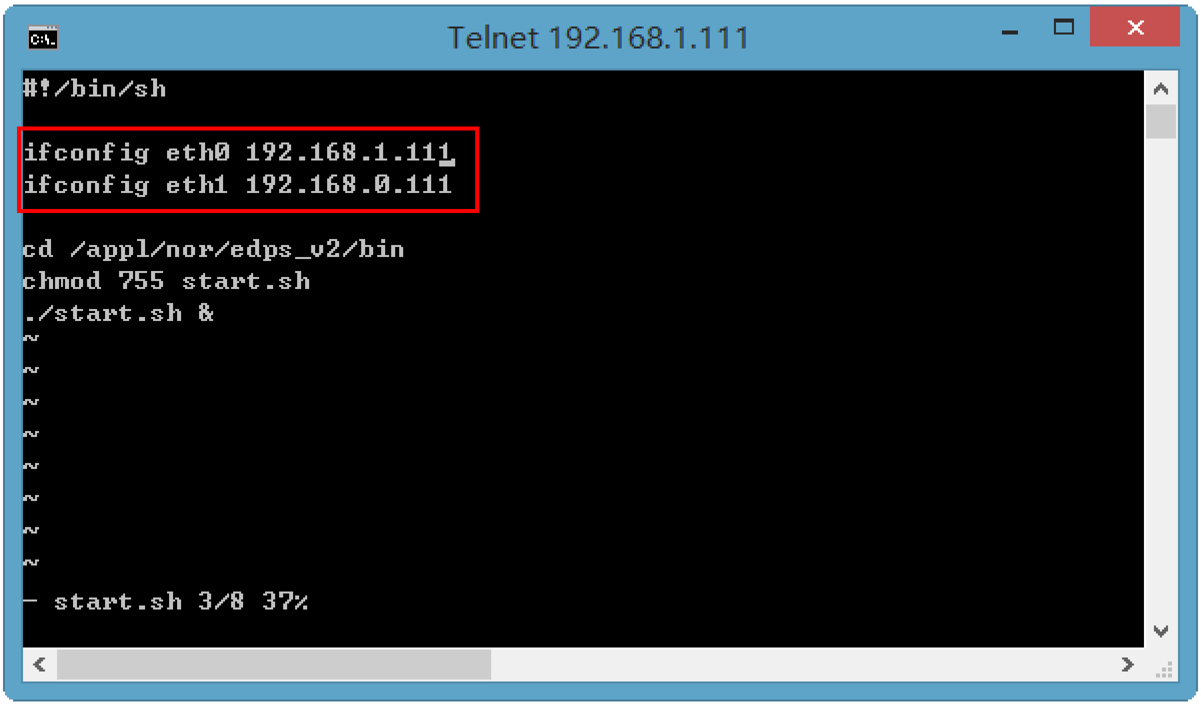
Method 2: Remotely log in to the device using Telnet, and modify the device IP address in the start.sh script. (Recommended).

- Log in to the device, type "cd /appl/nor", and press Enter to access the appl directory.
- Type "ls" and check whether the start.sh file exists.
- Type "vi start.sh", press Enter, and edit the file, as shown in the following figure.
- Move the cursor to the position marked in the following figure, and press Insert or i to enter the editing mode.
- Modify the IP address, and then press Esc to exit the editing mode.
- Press Shift+:, enter "wq" to save the modification.
- Enter "reboot" to restart the device.



```
        Welcome to Freescale Semiconductor Embedded Linux Environment


ePM8313e login: user
Password:
~ $ su
Password:
/home/user # cd /appl/nor/
/appl/nor # ls
bin       driver    edps_v2   start.sh
dgs       ePT       lib       syslog
/appl/nor # vi start.sh _
```

Figure 280 Editing the start.sh script



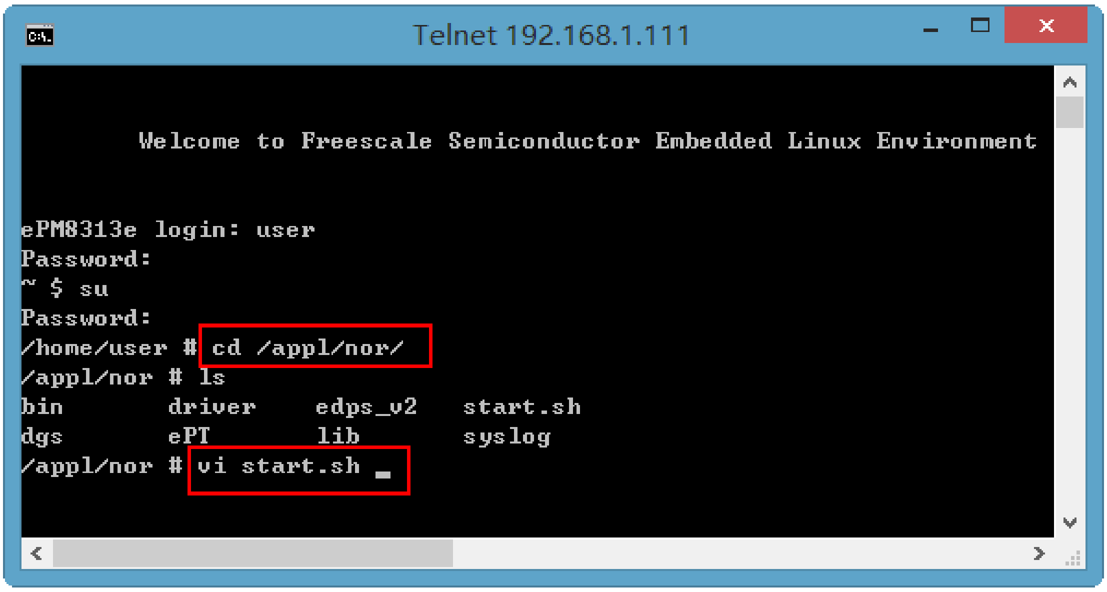
```
#!/bin/sh

ifconfig eth0 192.168.1.111
ifconfig eth1 192.168.0.111

cd /appl/nor/edps_v2/bin
chmod 755 start.sh
./start.sh &
~
~
~
~
~
~
~
~
- start.sh 3/8 37%
```

Figure 281 Modifying the IP address

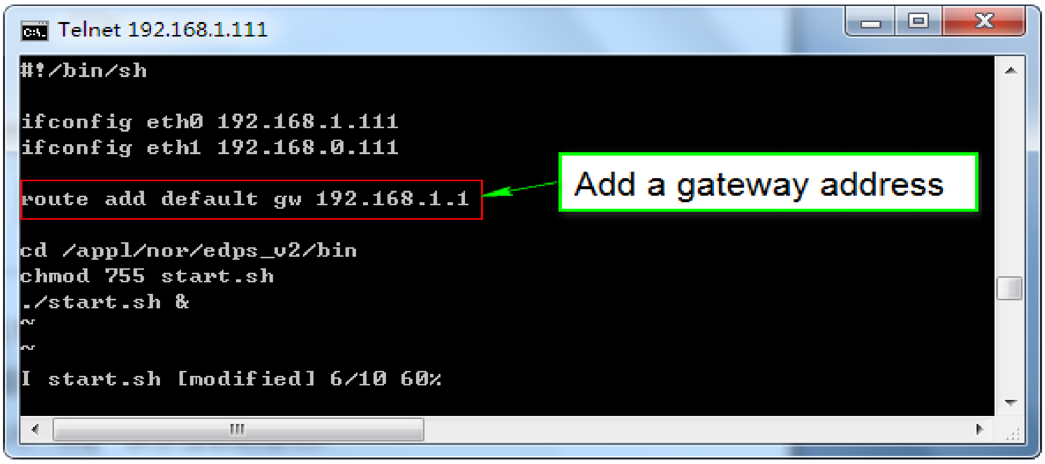
4.3.2.7.How to Add a Device Gateway Address

Remotely log in to the device using Telnet, and modify the device gateway address in the start.sh script.

- Log in to the device, type "**cd /appl/nor**", and press **Enter** to access the **nor** directory.
- Type "vi start.sh", press **Enter**, and edit the file, as shown in the following figure.
- Move the cursor to the position marked in the following figure, and press **Insert** or **i** to enter the editing mode.
- Add a gateway address, and then press **Esc** to exit the editing mode.
- Press **Shift**+**:**, enter "wq" to save the modification.
- Enter "reboot" to restart the device.



```
        Welcome to Freescale Semiconductor Embedded Linux Environment


ePM8313e login: user
Password:
~ $ su
Password:
/home/user # cd /appl/nor/
/appl/nor # ls
bin         driver      edps_v2     start.sh
dgs         ePT         lib         syslog
/appl/nor # vi start.sh _
```

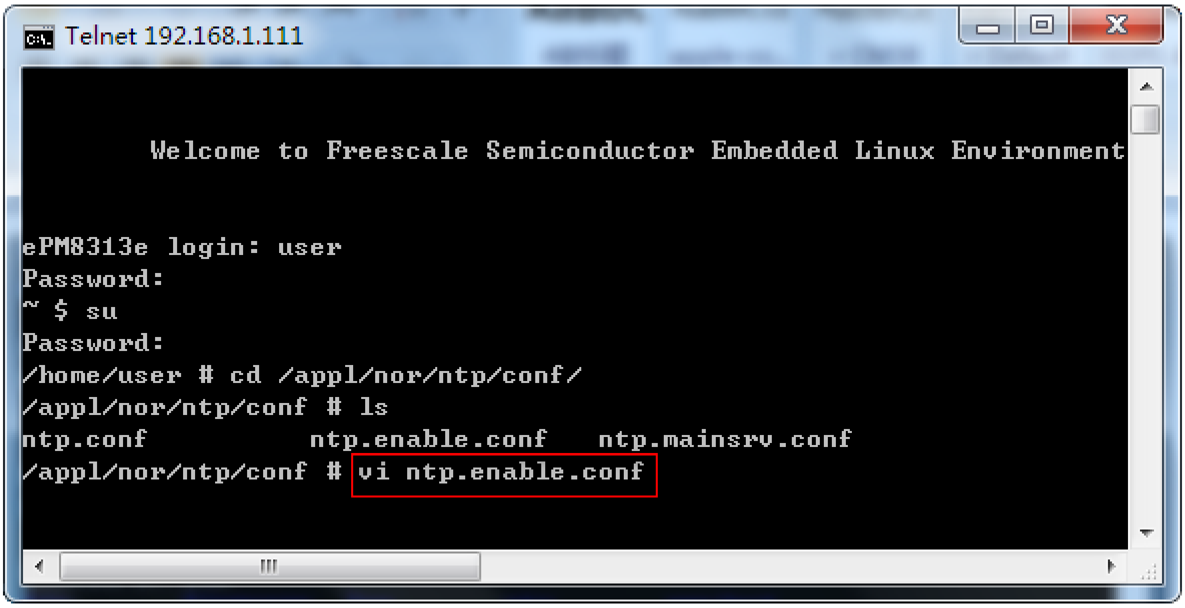


```
#!/bin/sh

ifconfig eth0 192.168.1.111
ifconfig eth1 192.168.0.111

route add default gw 192.168.1.1

cd /appl/nor/edps_v2/bin
chmod 755 start.sh
./start.sh &
~
~
I start.sh [modified] 6/10 60%
```

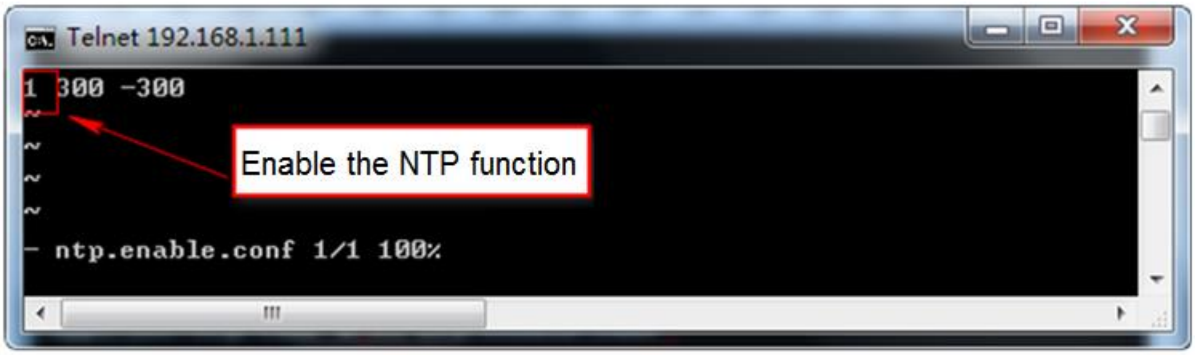
Add a gateway address

4.3.2.8.How to Configure NTP

- Remotely log in to the device using Telnet.
- Type "cd /appl/nor/ntp/conf".
- Edit the **ntp.enable.conf** file in the **conf** folder by changing **0** to **1** to enable the NTP function, as shown in the following figure.



```
       Welcome to Freescale Semiconductor Embedded Linux Environment

ePM8313e login: user
Password:
~ $ su
Password:
/home/user # cd /appl/nor/ntp/conf/
/appl/nor/ntp/conf # ls
ntp.conf          ntp.enable.conf   ntp.mainsrv.conf
/appl/nor/ntp/conf # vi ntp.enable.conf
```

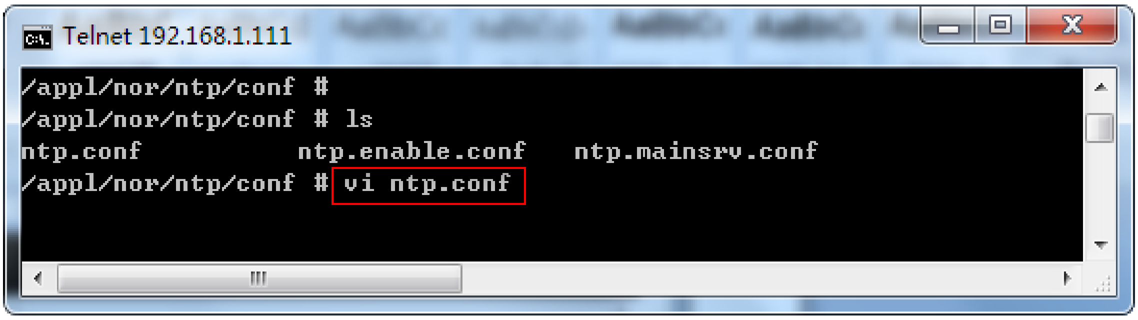


```
1 300 -300
~
~
~
~
- ntp.enable.conf 1/1 100%
```

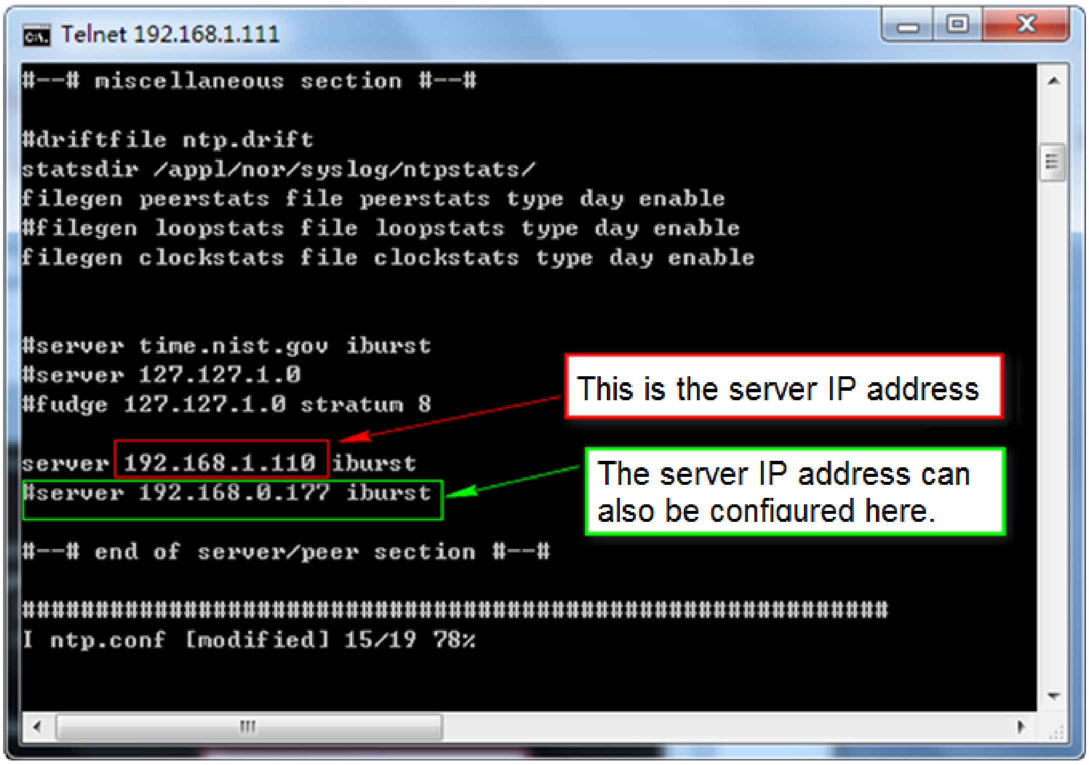
- ➢ **1** indicates that the NTP function is enabled, and **0** indicates that the NTP function is disabled.
- ➢ **300** or **-300**: It is the offset threshold, which can be modified.

- Edit the **ntp.conf** file by adding the IP address of the NTP server, as shown in the following figure.

Note**:** You can configure multiple server IP addresses.



```
/appl/nor/ntp/conf #
/appl/nor/ntp/conf # ls
ntp.conf          ntp.enable.conf   ntp.mainsrv.conf
/appl/nor/ntp/conf # vi ntp.conf
```

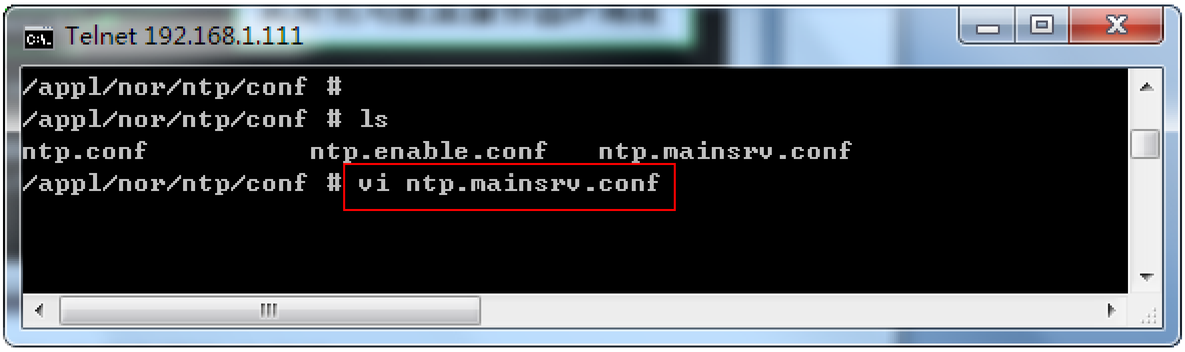


```
#--# miscellaneous section #--#

#driftfile ntp.drift
statsdir /appl/nor/syslog/ntpstats/
filegen peerstats file peerstats type day enable
#filegen loopstats file loopstats type day enable
filegen clockstats file clockstats type day enable


#server time.nist.gov iburst
#server 127.127.1.0
#fudge 127.127.1.0 stratum 8

server 192.168.1.110 iburst
#server 192.168.0.177 iburst

#--# end of server/peer section #--#

###########################################################
I ntp.conf [modified] 15/19 78%
```

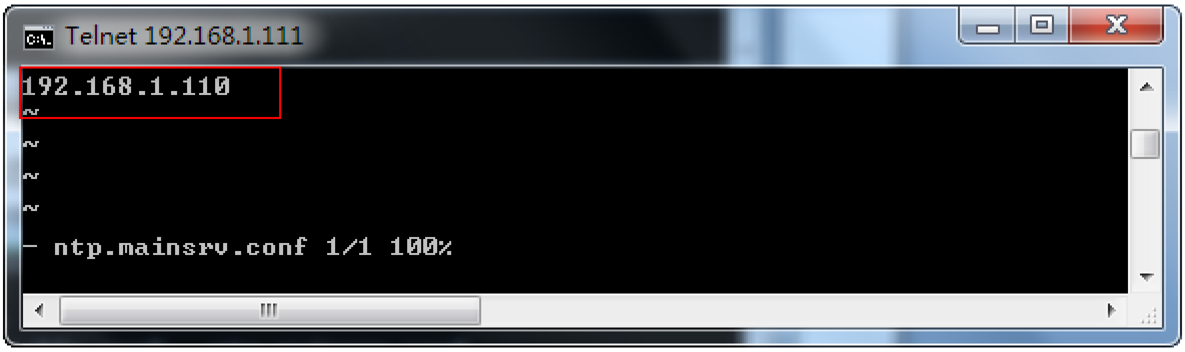
This is the server IP address

The server IP address can also be configured here.

- Edit the **ntp.mainsrv.conf** file by adding the IP address of the active server.



```
/appl/nor/ntp/conf #
/appl/nor/ntp/conf # ls
ntp.conf           ntp.enable.conf   ntp.mainsrv.conf
/appl/nor/ntp/conf # vi ntp.mainsrv.conf
```



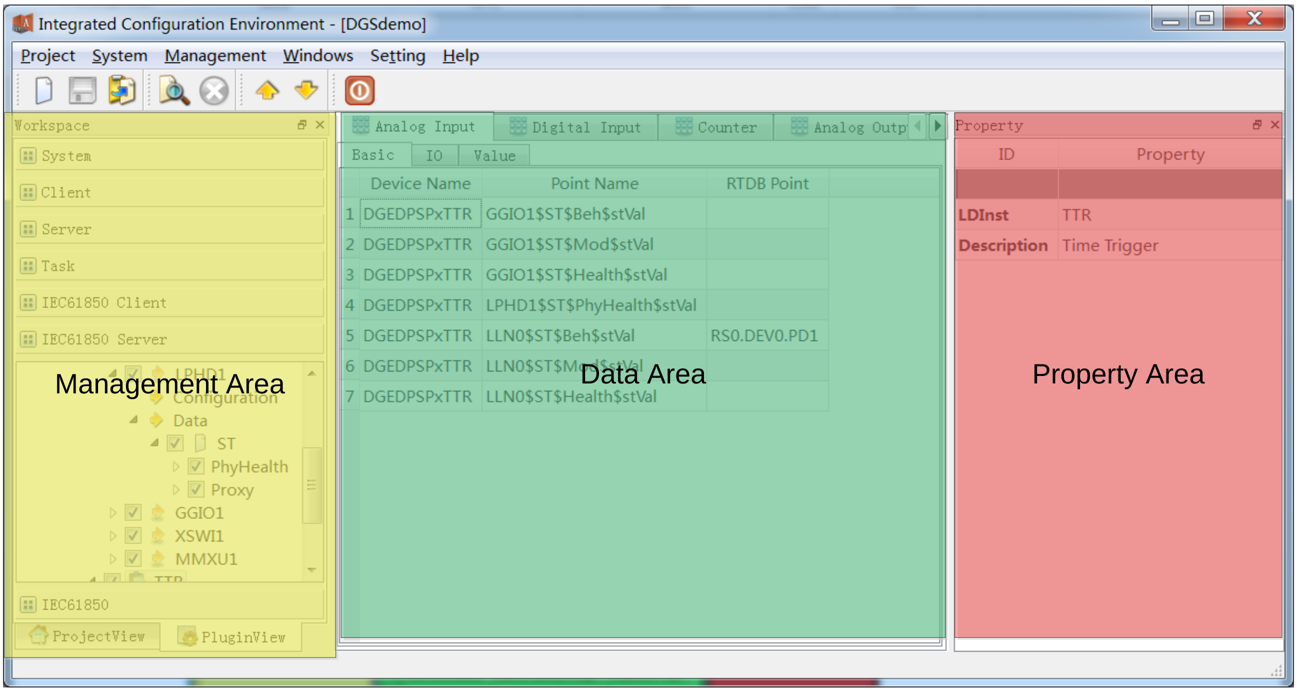
```
192.168.1.110
~
~
~
~
- ntp.mainsrv.conf 1/1 100%
```

After the file is edited, power off and then restart the device.

Appendix A IEC 61850 Configuration

Appendix A describes how to configure the IEC 61850 collection and proxy (forwarding) modules on the EDPS ICT-A+. In consideration of the independence of the IEC 61850 modules, the EDPS ICT-A+ uses the independent custom plugins, that is, IEC 61850 collection or proxy plugin, to customize and manage the data of the IEC 61850 collection or proxy module. The configuration manual details the driver information, communication parameters, device parameters, and the IO parameters of each information point. For IEC 61850-relevant terms mentioned in the configuration manual, see the IEC 61850 specifications.

The EDPS ICT-A+ integrates the configuration software by using plugins. An IEC 61850 plugin is an EDPS ICT-A+ configuration plugin that meets plugin interface requirements of the EDPS ICT-A+ and specifically serves the IEC 61850 proxy. The plugins are managed using the plugin manager of the EDPS ICT-A+. An EDPS ICT-A+ plugin provides three view areas: management area, data area, and property area.



	Device Name	Point Name	RTDB Point
1	DGEDPSPxTTR	GGIO1$ST$Beh$stVal	
2	DGEDPSPxTTR	GGIO1$ST$Mod$stVal	
3	DGEDPSPxTTR	GGIO1$ST$Health$stVal	
4	DGEDPSPxTTR	LPHD1$ST$PhyHealth$stVal	
5	DGEDPSPxTTR	LLN0$ST$Beh$stVal	RS0.DEV0.PD1
6	DGEDPSPxTTR	LLN0$ST$Mod$stVal	
7	DGEDPSPxTTR	LLN0$ST$Health$stVal	

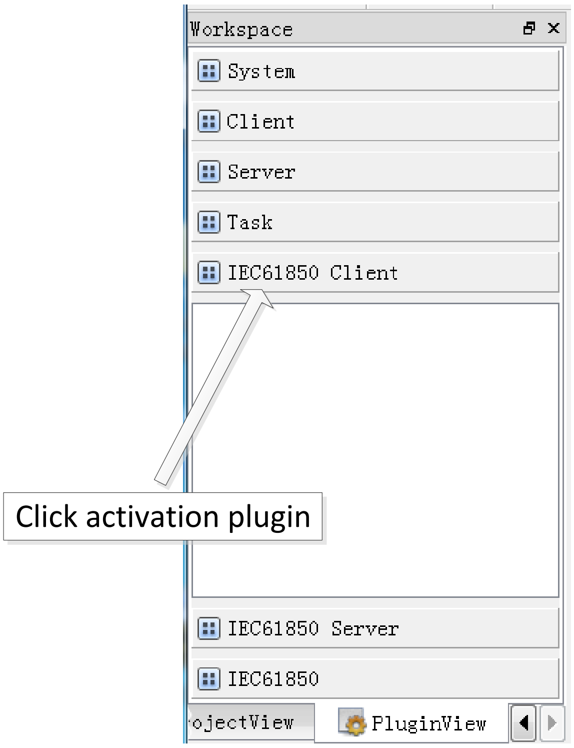
ID	Property
LDInst	TTR
Description	Time Trigger

A.1. IEC 61850 Collection Module

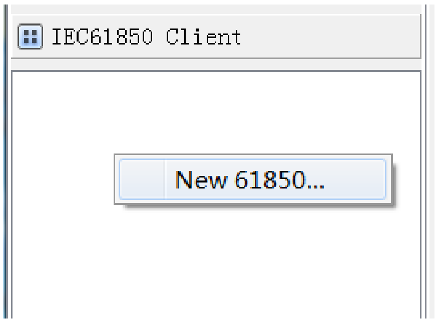
A.1.1.Driver Management

Create Create an IEC 61850 collection driver.

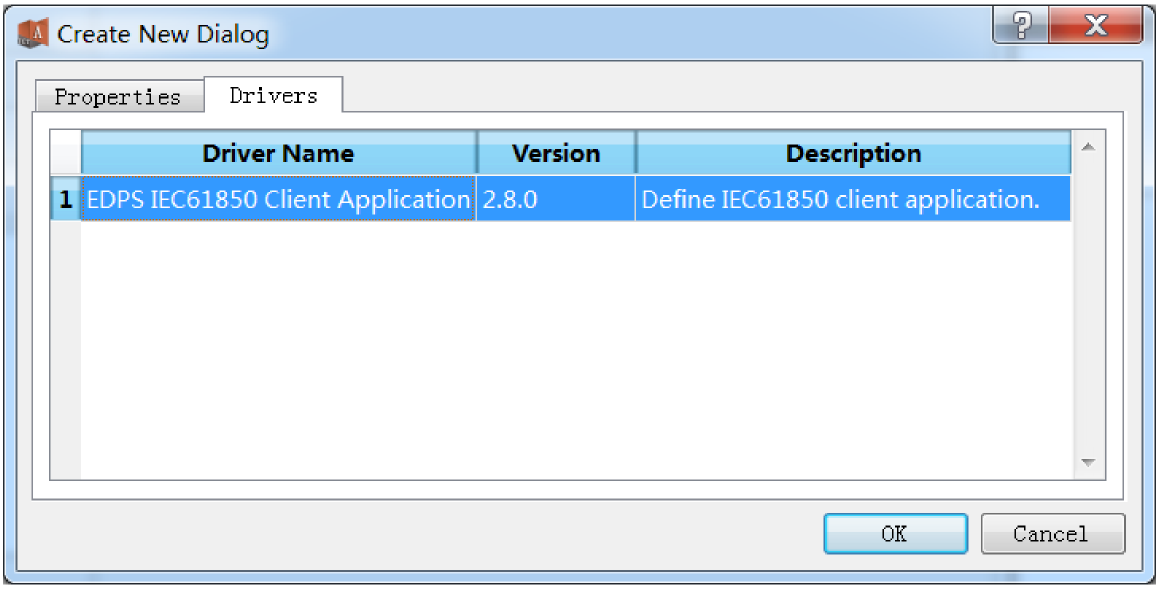
1. Open a project file.
2. Click the **PluginView** tab in the EDPS ICT-A+ management area.
3. Activate the IEC 61850 collection plugin.



4. Right-click in the blank area and choose **New 61850...** from the shortcut menu. The driver creation dialog box is displayed.

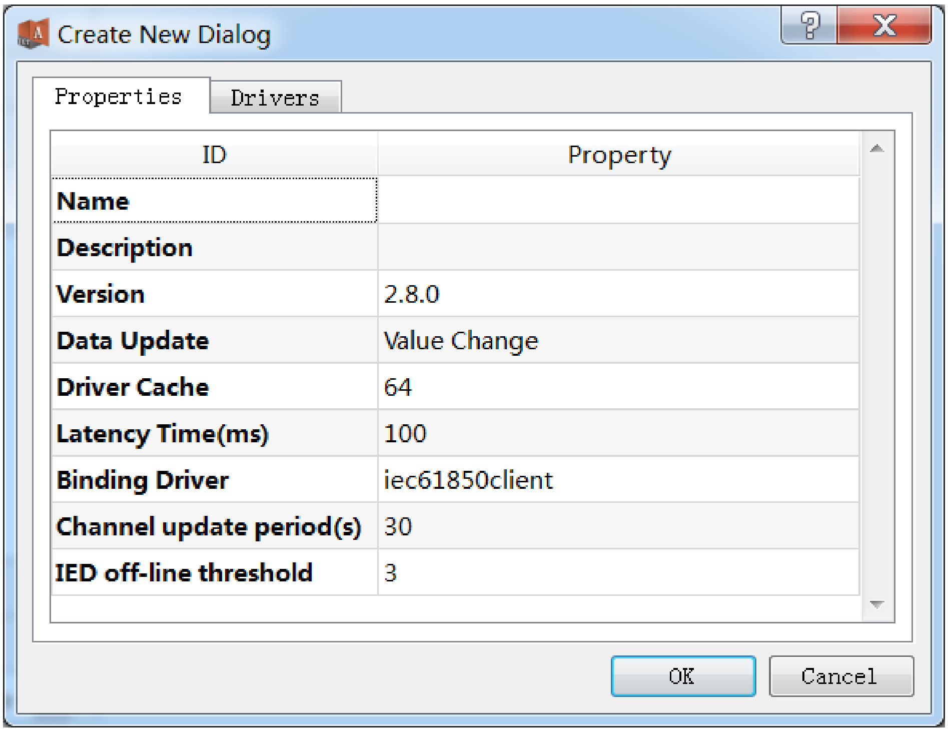


5. On the **Drivers** tab page, select the driver to be created.



	Driver Name	Version	Description
1	EDPS IEC61850 Client Application	2.8.0	Define IEC61850 client application.

6. On the **Properties** tab page, configure basic properties for the target driver.



ID	Property
Name	
Description	
Version	2.8.0
Data Update	Value Change
Driver Cache	64
Latency Time(ms)	100
Binding Driver	iec61850client
Channel update period(s)	30
IED off-line threshold	3

7. Click **OK**.

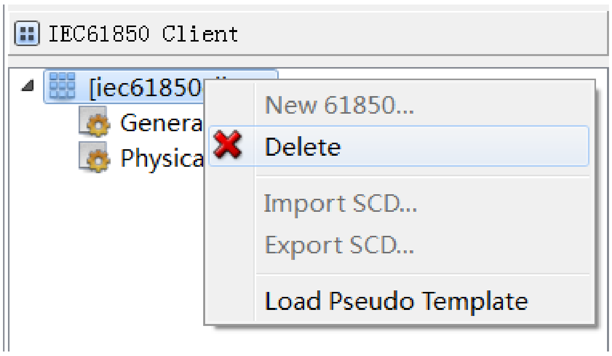
Note: Driver information

No.	Name	Description
1	Name	Driver name to be displayed
2	Description	Driver description
3	Version	Driver version
4	Data Update	Data update mode

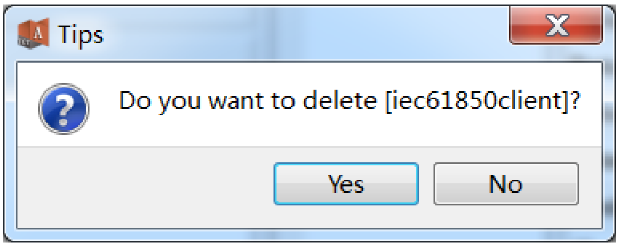
No.	Name	Description
		Value Change: The database is updated and other driver protocols are notified only when the value changes. Time Change: The value or time is updated into the database and other driver protocols are notified whenever the value or time changes. Time Update: The value or time is updated whenever it changes, and other driver protocols are notified only when the value changes.
5	Driver Cache	Cache size of the driver
6	Latency Time(ms)	Latency for updating the real-time database The system writes raw data into the real-time database only after the latency time.
7	Binding Driver	Name of the driver module. The value is unique and cannot be modified.
8	Channel update period(s)	Period for updating the IED communication times
9	IED off-line threshold	IED off-line threshold. When the number of communication failures of a device reaches this threshold, the device is set to be in the off-line state.

Delete Delete an IEC 61850 collection driver.

8. Right-click the driver to be deleted and choose **Delete** from the shortcut menu.



9. A dialog box is displayed, asking you whether to delete the driver.

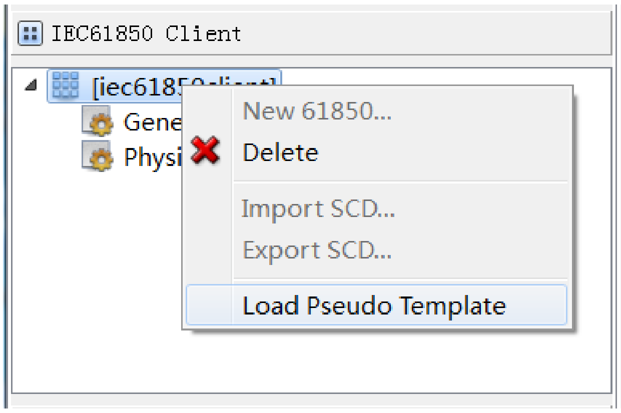


Do you want to delete [iec61850client]?

10. Click **Yes** to complete deletion.

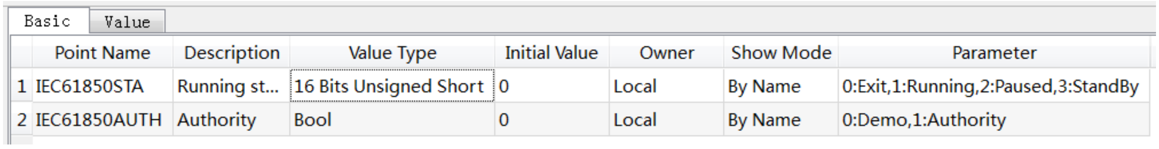
Pseudo Template Load a pseudo template from the system template library to the driver.

11. Right-click the driver bar and choose **Load Pseudo Template** from the shortcut menu.



12. Load a pseudo template to complete the loading of the pseudo point to the driver.

Note:



	Point Name	Description	Value Type	Initial Value	Owner	Show Mode	Parameter
1	IEC61850STA	Running st...	16 Bits Unsigned Short	0	Local	By Name	0:Exit,1:Running,2:Paused,3:StandBy
2	IEC61850AUTH	Authority	Bool	0	Local	By Name	0:Demo,1:Authority

No.	Name	Description
1	Running status	Running status information about the driver
2	Authority	Authority status of the driver

A.1.2.General Parameters

Overview View and configure the general parameters of the IEC 61850 driver.

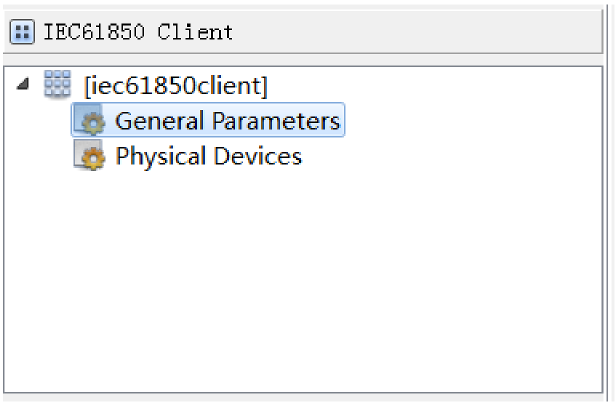
View and Configure View and configure the properties of communication parameters.

1. Open a project file.

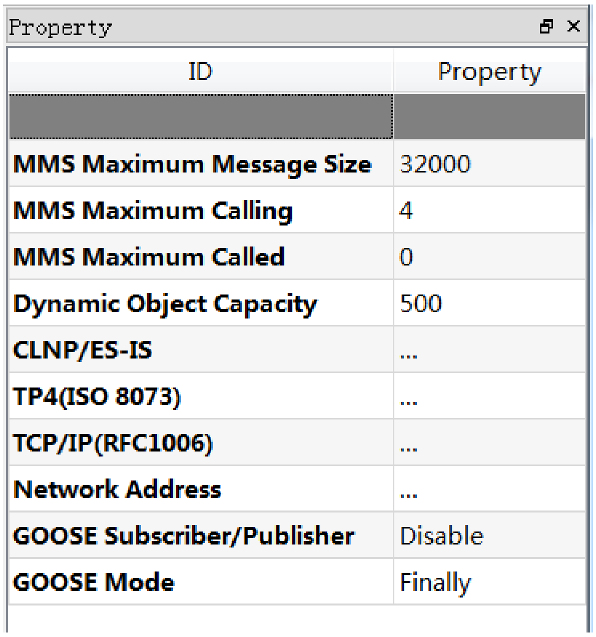
2. Click the **PluginView** tab in the EDPS ICT-A+ management area.

3. Activate the IEC 61850 collection plugin.

4. Select **General Parameters** in the management area.



5. View information in the property area.



Property

ID	Property
MMS Maximum Message Size	32000
MMS Maximum Calling	4
MMS Maximum Called	0
Dynamic Object Capacity	500
CLNP/ES-IS	...
TP4(ISO 8073)	...
TCP/IP(RFC1006)	...
Network Address	...
GOOSE Subscriber/Publisher	Disable
GOOSE Mode	Finally

Note: Information in the property area (including configuration operations)

No.	Name	Description	Remarks
1	MMS Maximum Message Size	Maximum PDU size	Use the default parameter value.
2	MMS Maximum Calling	Maximum number of calling connections of the MMS service	Configure the parameter based on actual conditions and refer to the value in the preceding figure.
3	MMS Maximum Called	Maximum number of called connections of the MMS	Configure the parameter based on actual conditions

No.	Name	Description	Remarks
		service	and refer to the value in the preceding figure.
4	Dynamic Object Capacity	Maximum number of dynamic objects	Configure the parameter based on actual conditions and refer to the value in the preceding figure.
5	CLNP/ES-IS	Network layer in the OSI protocol stack	Add one line in the table editor and use the default parameter value.
6	TP4(ISO 8073)	Transport layer in the OSI protocol stack	Add one line in the table editor and use the default parameter value.
7	TCP/IP(RFC1006)	TCP/IP protocol stack	Add one line in the table editor and use the default parameter value.
8	Network address	Local network address	Add one line in the table editor and use the default parameter value.
9	GOOSE Subscriber/Publisher	Whether to enable GOOSE information subscription	Configure the parameter based on actual conditions.
10	GOOSE Mode	Parsing mode of GOOSE information	Configure the parameter based on actual conditions.

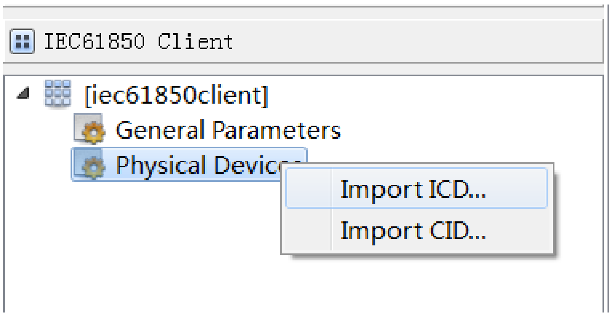
A.1.3.Physical Device Management

Import an ICD File Create an IEC 61850 collection device by importing the IEC 61850 ICD file.

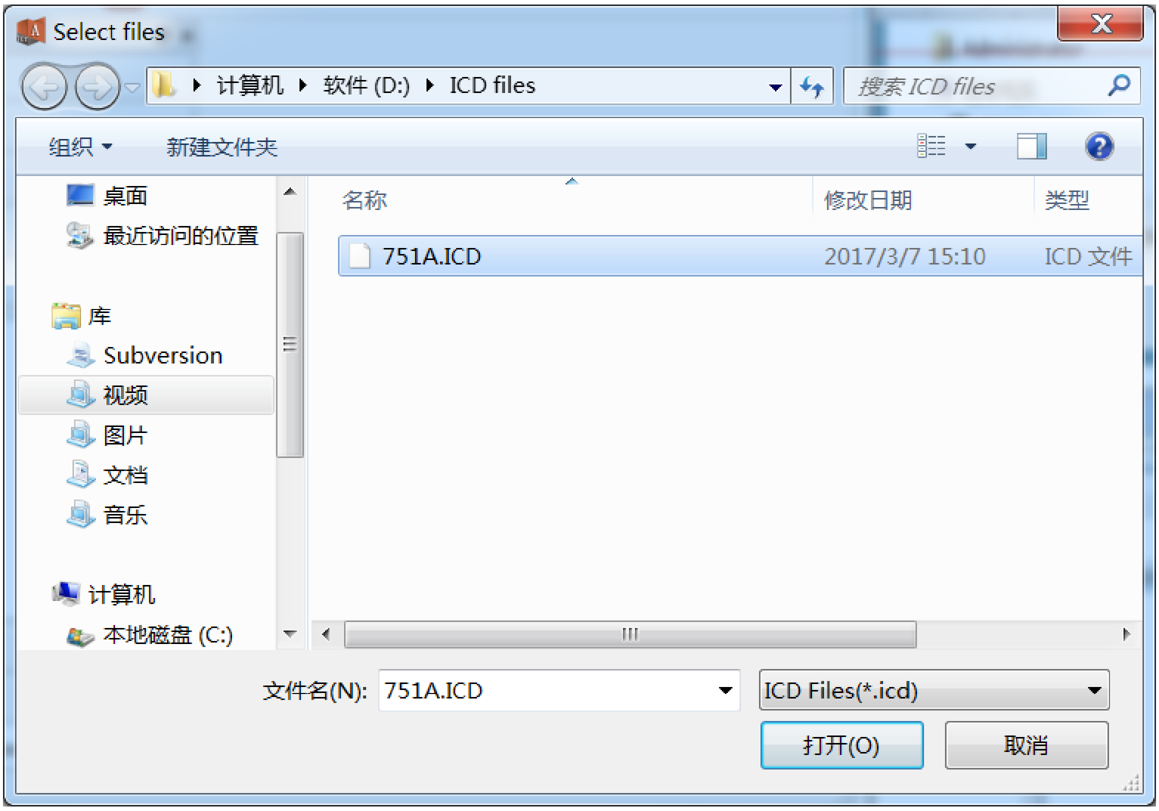
1. Open a project file.
2. Click the **PluginView** tab in the EDPS ICT-A+ management area.

3. Activate the IEC 61850 collection plugin.

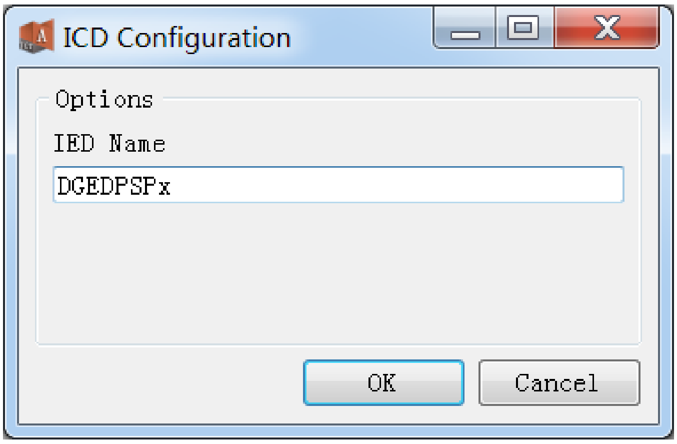
4. Right-click **Physical Devices** and choose **Import ICD** from the shortcut menu.



5. In the **Select files** dialog box, select a file and click **Open**.



6. The **ICD Configuration** dialog box is displayed.



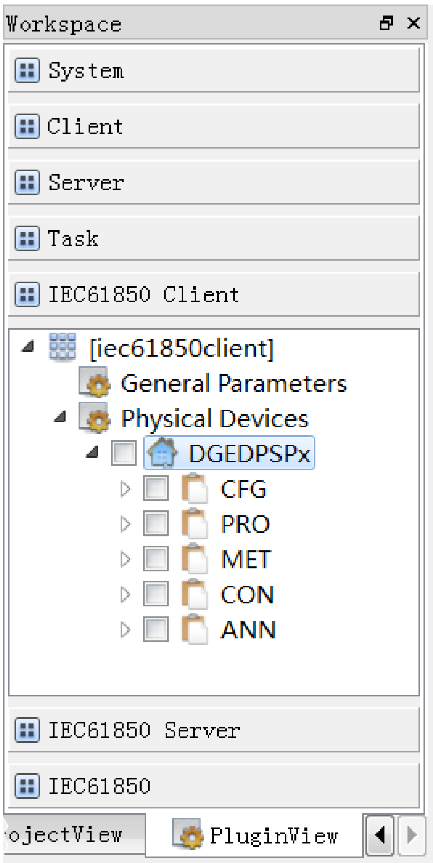
ICD Configuration

Options

IED Name

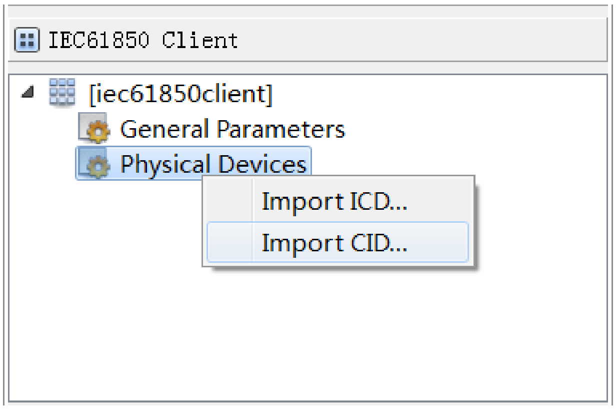
DGEDPSPx

7. Set the instance name of the IED device and click **OK** to create the IEC 61850 device.

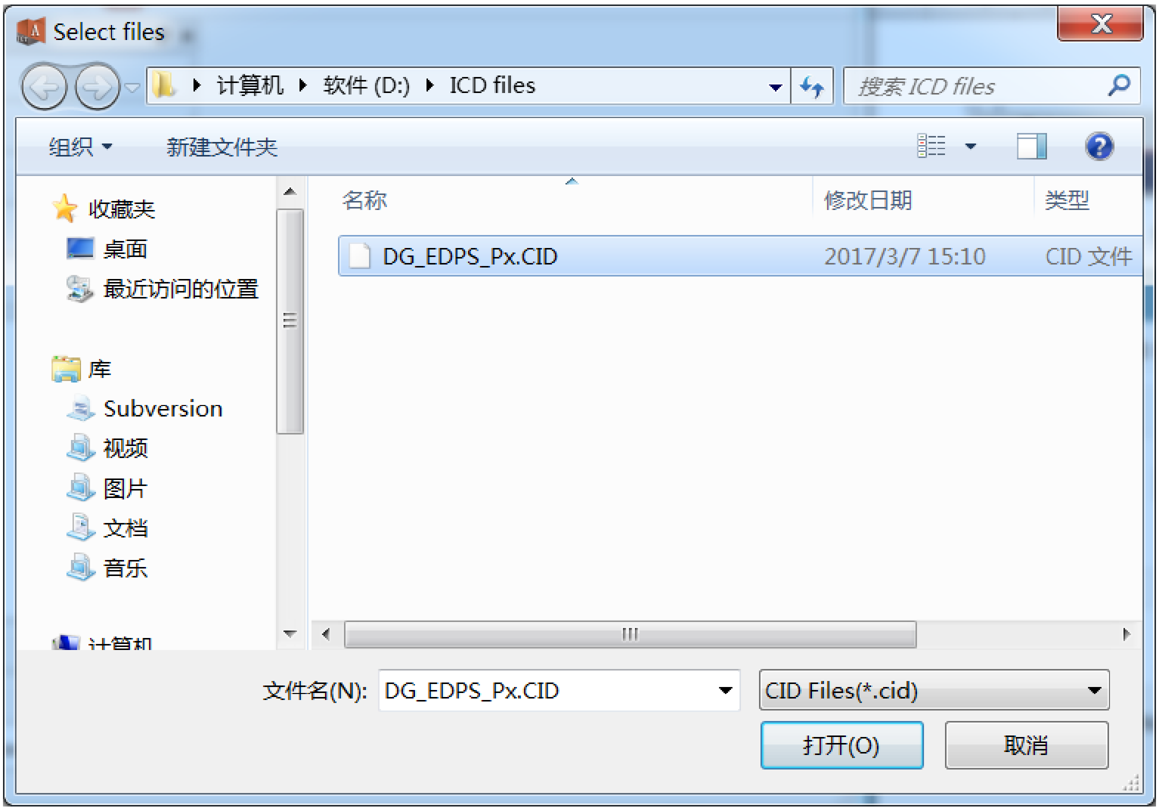


Import a CID File Create an IEC 61850 collection device by importing the IEC 61850 CID file.

8. Right-click **Physical Devices** and choose **Import CID** from the shortcut menu.



9. In the **Select files** dialog box, select a file and click **Open**.

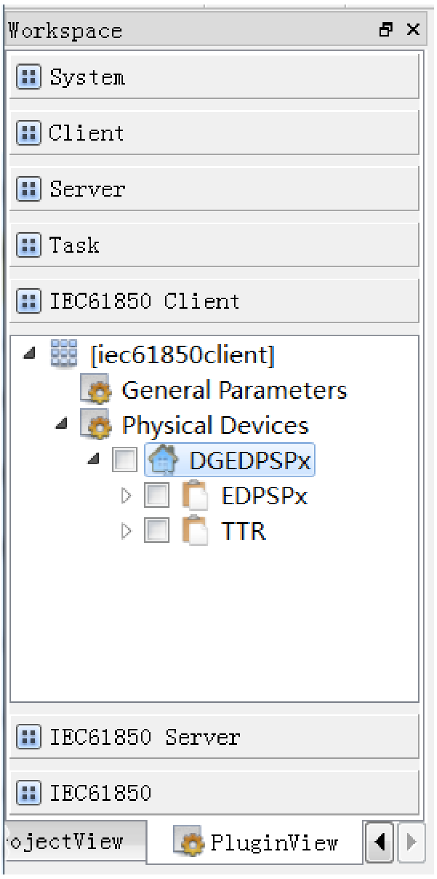


名称	修改日期	类型
DG_EDPS_Px.CID	2017/3/7 15:10	CID 文件

文件名(N): DG_EDPS_Px.CID

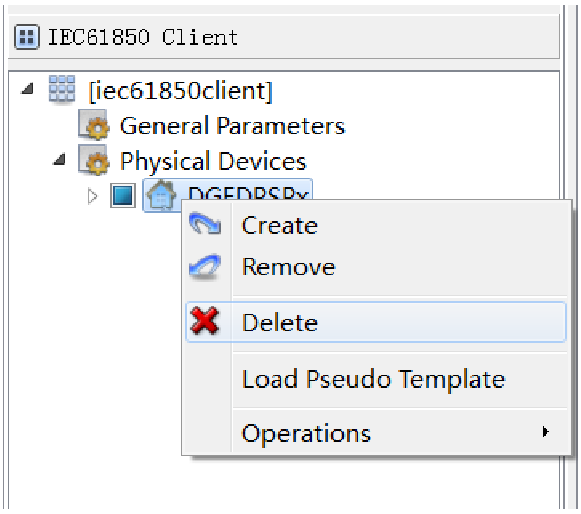
CID Files(*.cid)

10. Confirm the IED name and click **OK** to complete the creation of the IEC 61850 device.

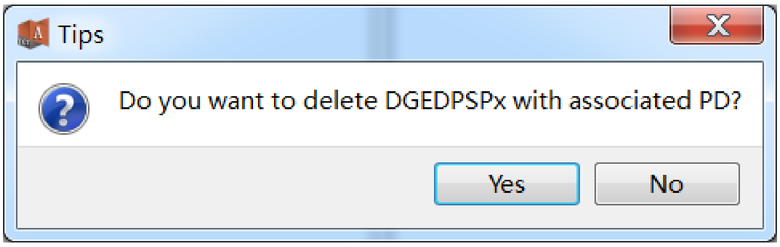


Delete a Device Delete the imported IEC 61850 device thoroughly.

11. Right-click a Level-1 subnode under **Physical Devices**.



12. Choose **Delete** from the shortcut menu.

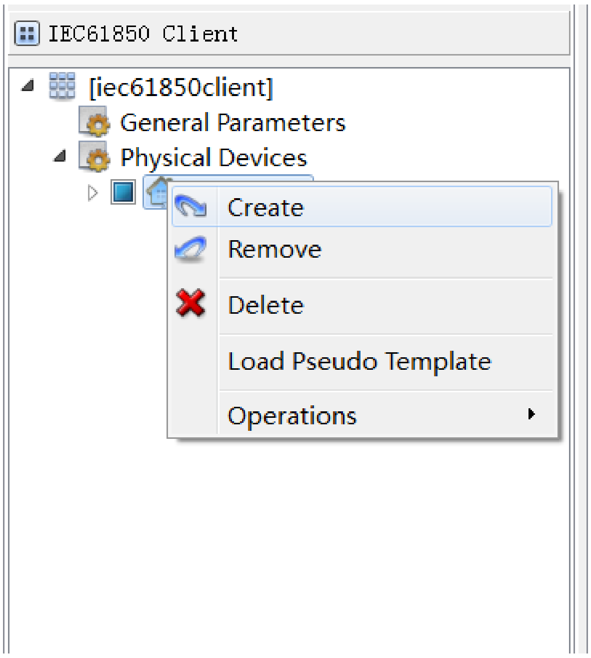


Do you want to delete DGEDPSPx with associated PD?

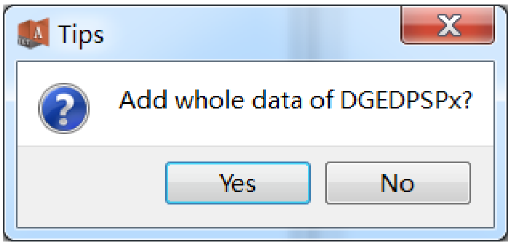
13. Click **Yes** to complete the deletion of the IEC 61850 physical device.

Create a Device Establish the mapping between an IEC 61850 physical device and the EDPS ICT-A+.

14. Right-click a Level-1 subnode under **Physical Devices**.



15. Choose **Create** from the shortcut menu to add the data mapping between the IEC 61850 physical device and the EDPS ICT-A+.



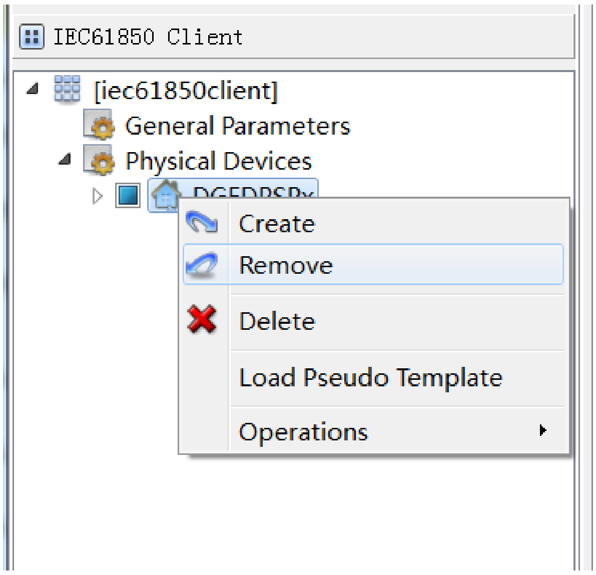
Add whole data of DGEDPSPx?

16. Click **Yes** to complete the establishment of the mapping between all information points in the IEC 61850 device and the EDPS ICT-A+.

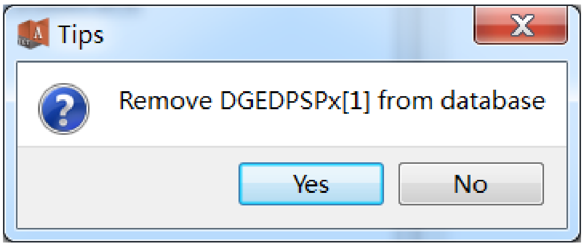
Note: Selectively add required information points for mapping based on actual conditions.

Remove a Device Remove the mapping between an IEC 61850 physical device and the EDPS ICT-A+.

17. Right-click a Level-1 subnode under **Physical Devices**.



18. Choose **Remove** from the shortcut menu.



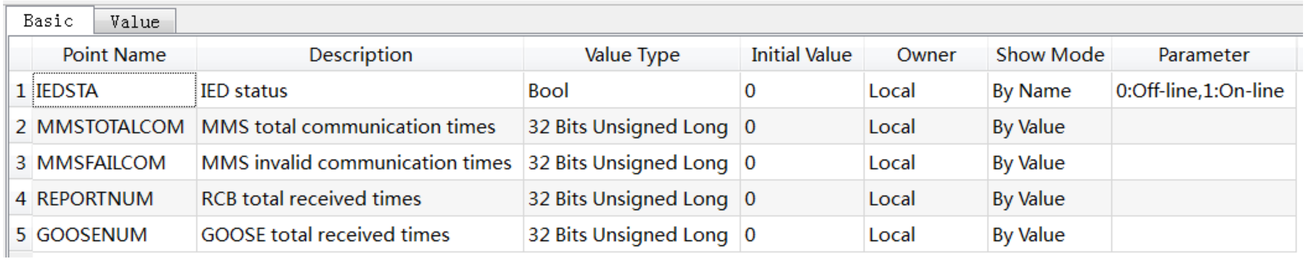
Remove DGEDPSPx[1] from database

19. Click **Yes** to remove the mapping between an IEC 61850 physical device and the EDPS ICT-A+.

Device Parameters Configure physical device parameters for the IEC 61850 driver.

20. Click a Level-1 subnode under **Physical Devices**.

21. View the pseudo point in the data area of the EDPS ICT-A+.

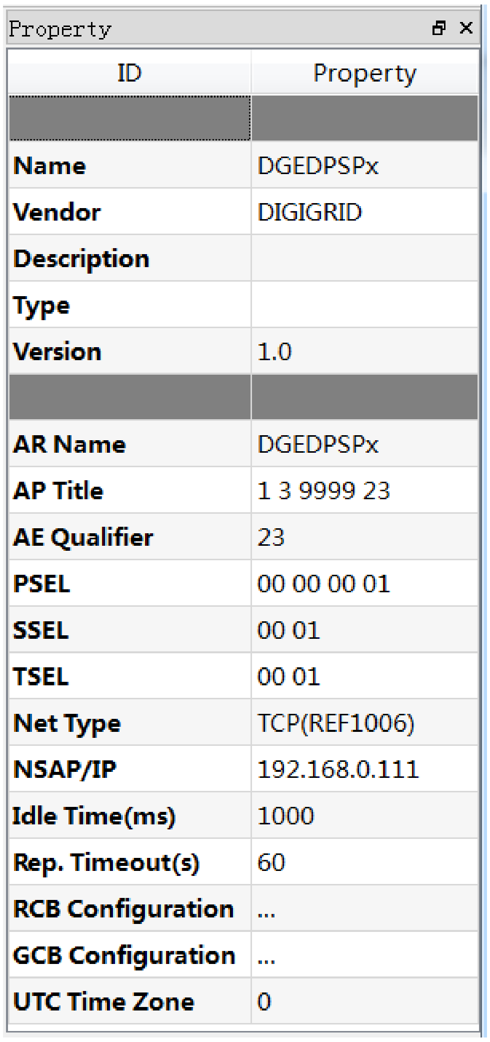


	Point Name	Description	Value Type	Initial Value	Owner	Show Mode	Parameter
1	IEDSTA	IED status	Bool	0	Local	By Name	0:Off-line,1:On-line
2	MMSTOTALCOM	MMS total communication times	32 Bits Unsigned Long	0	Local	By Value	
3	MMSFAILCOM	MMS invalid communication times	32 Bits Unsigned Long	0	Local	By Value	
4	REPORTNUM	RCB total received times	32 Bits Unsigned Long	0	Local	By Value	
5	GOOSENUM	GOOSE total received times	32 Bits Unsigned Long	0	Local	By Value	

No.	Name	Description
1	IED status	Communication status of the current device
2	MMS total communication times	Number of MMS communication times
3	MMS invalid communication times	Number of failed MMS communication times

4	RCB total received times	Number of received event reports
5	GOOSE total received times	Number of received GOOSE information

22. View the property area of the EDPS ICT-A+.



Property

ID	Property
Name	DGEDPSPx
Vendor	DIGIGRID
Description	
Type	
Version	1.0
AR Name	DGEDPSPx
AP Title	1 3 9999 23
AE Qualifier	23
PSEL	00 00 00 01
SSEL	00 01
TSEL	00 01
Net Type	TCP(REF1006)
NSAP/IP	192.168.0.111
Idle Time(ms)	1000
Rep. Timeout(s)	60
RCB Configuration	...
GCB Configuration	...
UTC Time Zone	0

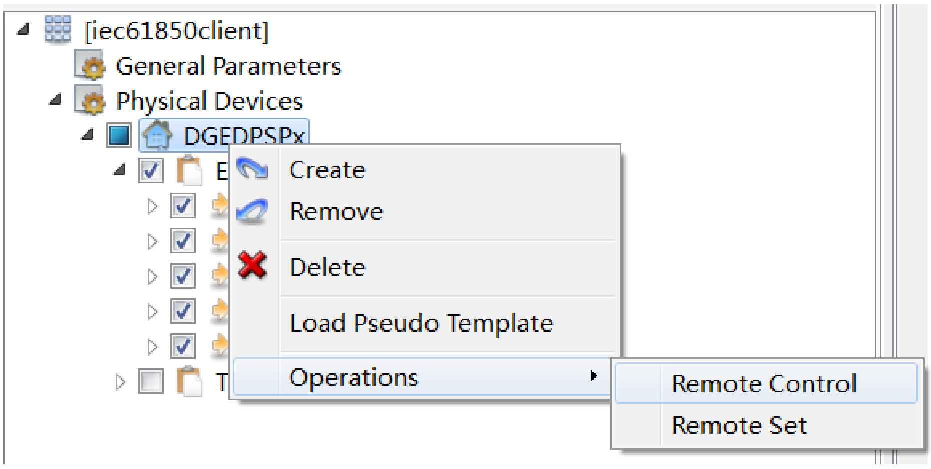
No.	Name	Description	Remarks
1	Name	Device name	Configure it based on actual conditions. Edit it when importing an ICD or CID file.
2	Vendor	Device vendor	It is configured in the ICD/CID file.
3	Description	Device description	It is configured in the ICD/CID file.
4	Type	Device type	It is configured in the ICD/CID file.
5	Version	Device version	It is configured in the ICD/CID file.

No.	Name	Description	Remarks
6	AR Name	Reference name of the MMS application	Configure it based on actual conditions. Edit it when importing an ICD or CID file.
7	AP Title	Object identification named by the network authorization organization, to identify the process title	Use the default value as shown in the figure.
8	AE Qualifier	Integer to identify the application qualifier	Use the default value as shown in the figure.
9	PSEL	Access point of the representation layer in the OSI protocol stack. It is a 4-byte value by default.	It is defined in the ICD/CID file. Use the default value as shown in the figure.
10	SSEL	Access point of the session layer in the OSI protocol stack. It is a 2-byte value by default.	It is defined in the ICD/CID file. Use the default value as shown in the figure.
11	TSEL	Access point of the transport layer in the OSI protocol stack. It is a 2-byte value by default.	It is defined in the ICD/CID file. Use the default value as shown in the figure.
12	Net Type	TP4 or TCP to which a network address belongs	Configure the parameter based on actual conditions. Use the default value.
13	NSAP/IP	Network address ● TP4 is represented with 20 strings in hexadecimal notation.	Use the actual IP address of the device.

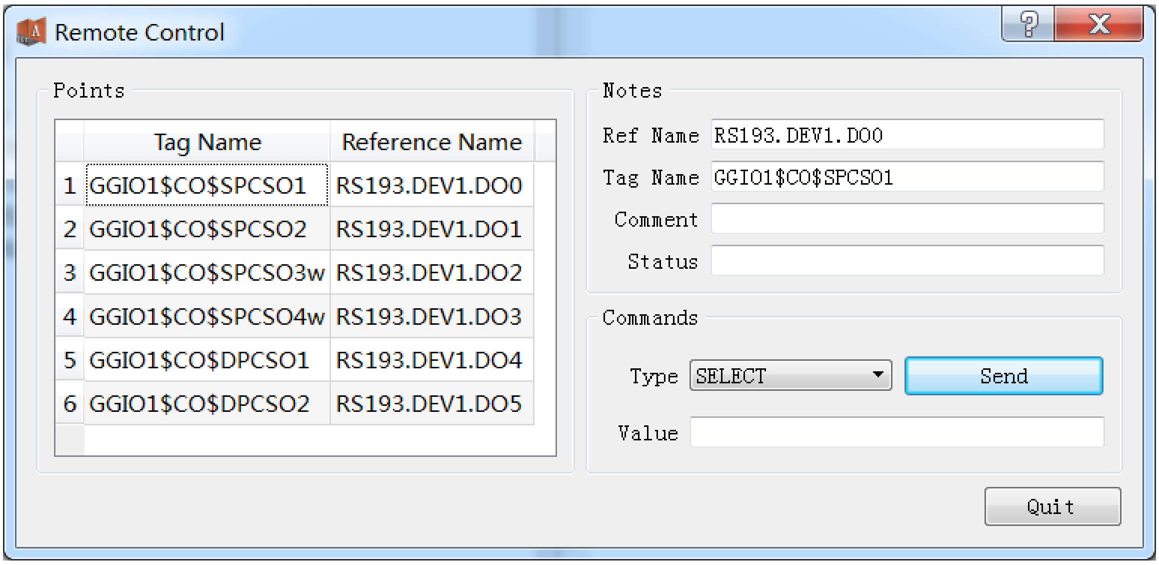
No.	Name	Description	Remarks
		● TCP is represented with a network alias or an IP address.	
14	Idle Time(ms)	Idle interval for MMS query. The unit is milliseconds.	Configure the parameter based on actual conditions.
15	Rep. Timeout(s)	Timeout interval of MMS request data. The unit is seconds.	Configure the parameter based on actual conditions.
16	RCB Configuration	Configuration of the Report Control Block	Configure the parameter based on actual conditions.
17	GCB Configuration	Configuration of the GSE Control Block	Configure the parameter based on actual conditions.
18	UTC Time Zone	UTC time zone correction value of the device	Configure the parameter based on actual conditions.

Remote Control, Remote Set Send remote control and remote set commands to a device via the EDPS ICT-A+.

23. Right-click a Level-1 subnode under **Physical Devices**.



24. Choose **Operations** > **Remote Control** from the shortcut menu. The **Remote Control** dialog box is displayed.



Remote Control

Points

	Tag Name	Reference Name
1	GGIO1$CO$SPCSO1	RS193.DEV1.DO0
2	GGIO1$CO$SPCSO2	RS193.DEV1.DO1
3	GGIO1$CO$SPCSO3w	RS193.DEV1.DO2
4	GGIO1$CO$SPCSO4w	RS193.DEV1.DO3
5	GGIO1$CO$DPCSO1	RS193.DEV1.DO4
6	GGIO1$CO$DPCSO2	RS193.DEV1.DO5

Notes

Ref Name RS193.DEV1.DO0

Tag Name GGIO1$CO$SPCSO1

Comment

Status

Commands

Type SELECT

Value

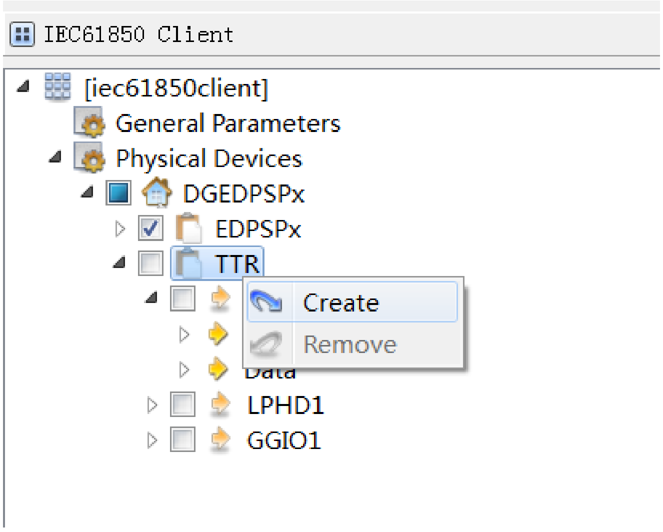
25. Select an information point, set the control type and control value.

26. Click **Send** to complete the write command operation and wait for the execution result.

A.1.4.Information Point Management

Create Create an information point to implement mapping between an IEC 61850 device and the EDPS ICT-A+.

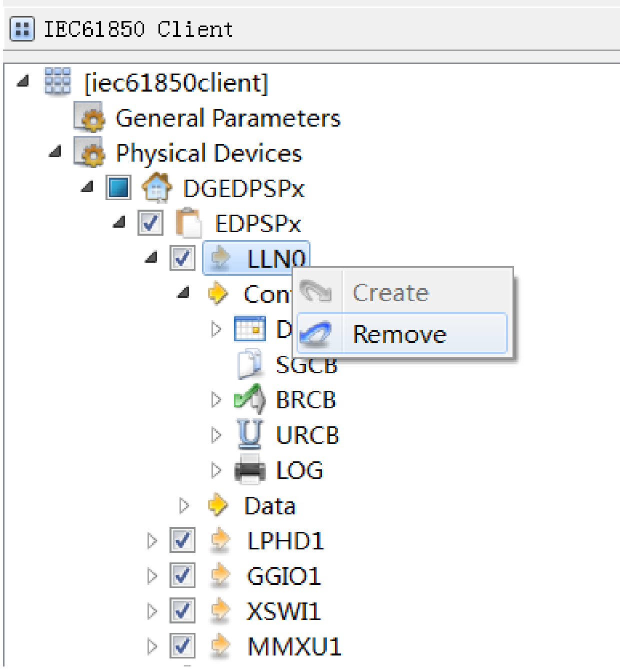
1. Open a project file.
2. Click the **PluginView** tab in the EDPS ICT-A+ management area.
3. Activate the IEC 61850 collection plugin.
4. Right-click a data management node under **Physical Devices**.



5. Choose **Create** from the shortcut menu to create an information point.

Delete Delete an information point to remove data mapping between the IEC61850 device and the EDPS ICT-A+.

6. Right-click a data management node under **Physical Devices**.



7. Choose **Remove** from the shortcut menu to delete the information point.

View Properties View the properties of internal objects of an IEC61850 device.

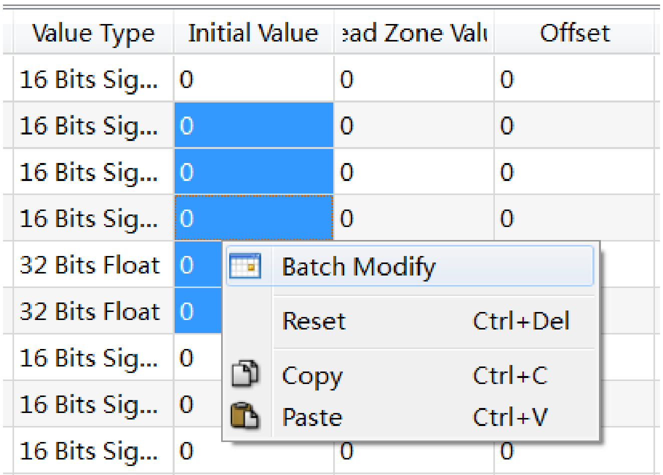
8. Select any subnode under **Physical Devices** and view the object properties in the property area.

A.1.5.Data Management

Batch Modify Modify data in the data area in batches.

View parameters of an information point in a data type in the data area of the EDPS ICT-A+. The device name, point name, and IO parameters in basic information cannot be edited and their values depend on the IEC 61850 device.

1. Open a project file.
2. Click the **PluginView** tab in the EDPS ICT-A+ management area.
3. Activate the IEC 61850 collection plugin.
4. In the data area, click the tab of basic information of different data types.
5. Select multiple objects, right-click the objects and choose **Batch Modify** from the shortcut menu. A dialog box is displayed.



Value Type	Initial Value	ead Zone Valı	Offset
16 Bits Sig...	0	0	0
16 Bits Sig...	0	0	0
16 Bits Sig...	0	0	0
16 Bits Sig...	0	0	0
32 Bits Float	0		
32 Bits Float	0		
16 Bits Sig...	0		
16 Bits Sig...	0		
16 Bits Sig...	0	0	0

6. Modify data and click **OK** to complete data batch modification.

Reset Use initialized values of table data properties to replace current values.

7. Right-click an object and choose **Reset** from the shortcut menu. Click **Yes** to complete modification.

Copy and Paste Copy and paste data.

Data can be copied and pasted across plugins, links, devices, and types.

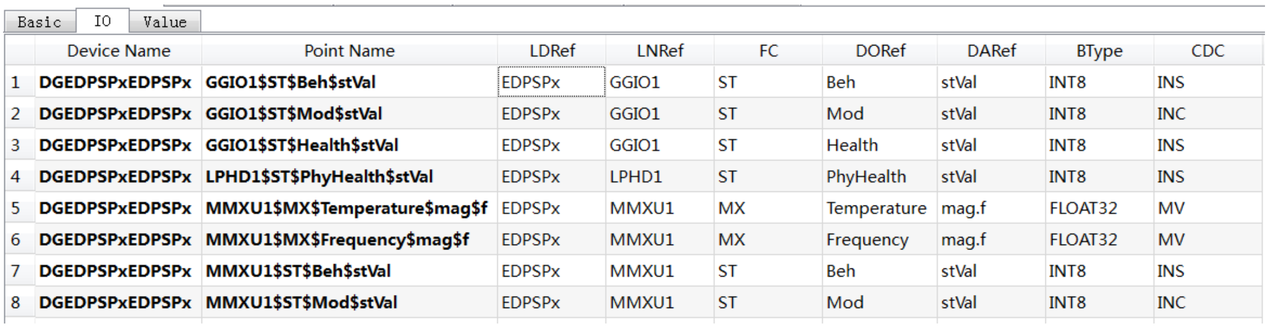
Data can be copied and pasted between an EXCEL sheet and the EDPS ICT-A+.

The copy operation is allowed in all data areas.

The paste operation is allowed in editable areas.

8. Right-click an object and choose **Copy/Paste** from the shortcut menu (the paste operation is not supported in areas that cannot be edited).

Note: IO information parameters



	Device Name	Point Name	LDRef	LNRef	FC	DORef	DARef	BType	CDC
1	DGEDPSPxEDPSPx	GGIO1$ST$Beh$stVal	EDPSPx	GGIO1	ST	Beh	stVal	INT8	INS
2	DGEDPSPxEDPSPx	GGIO1$ST$Mod$stVal	EDPSPx	GGIO1	ST	Mod	stVal	INT8	INC
3	DGEDPSPxEDPSPx	GGIO1$ST$Health$stVal	EDPSPx	GGIO1	ST	Health	stVal	INT8	INS
4	DGEDPSPxEDPSPx	LPHD1$ST$PhyHealth$stVal	EDPSPx	LPHD1	ST	PhyHealth	stVal	INT8	INS
5	DGEDPSPxEDPSPx	MMXU1$MX$Temperature$mag$f	EDPSPx	MMXU1	MX	Temperature	mag.f	FLOAT32	MV
6	DGEDPSPxEDPSPx	MMXU1$MX$Frequency$mag$f	EDPSPx	MMXU1	MX	Frequency	mag.f	FLOAT32	MV
7	DGEDPSPxEDPSPx	MMXU1$ST$Beh$stVal	EDPSPx	MMXU1	ST	Beh	stVal	INT8	INS
8	DGEDPSPxEDPSPx	MMXU1$ST$Mod$stVal	EDPSPx	MMXU1	ST	Mod	stVal	INT8	INC

No.	Name	Description
1	Device Name	Instance name of the logic device to which an information point belongs

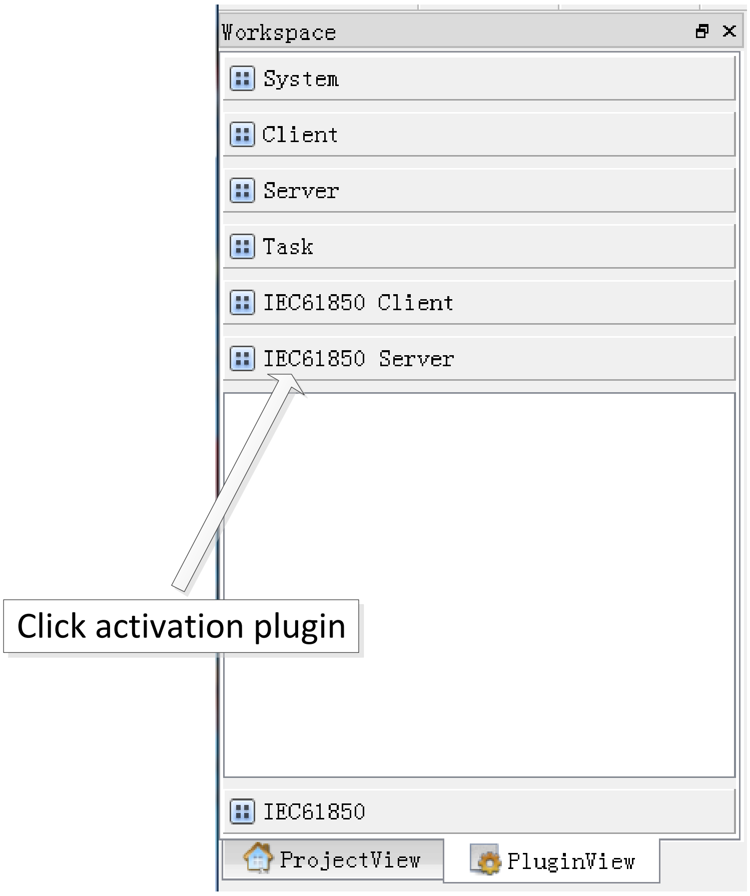
2	Point Name	Complete reference name of the MMS index of the information point
3	LDRef	Reference name of the logic device to which the information point belongs
4	LNRef	Reference name of the logic node to which the information point belongs
5	FC	Function constraint of the information point
6	DORef	Reference name of the data object of the information point
7	DARef	Reference name of the data attribute of the information point
8	BType	Basic data type of the information point
9	CDC	Common data class to which the information point belongs

A.2. IEC61850 Proxy

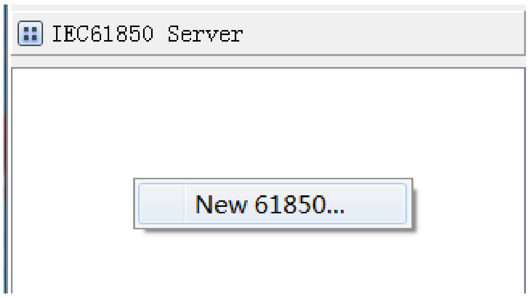
A.2.1.Driver Management

Create Create an IEC 61850 proxy driver.

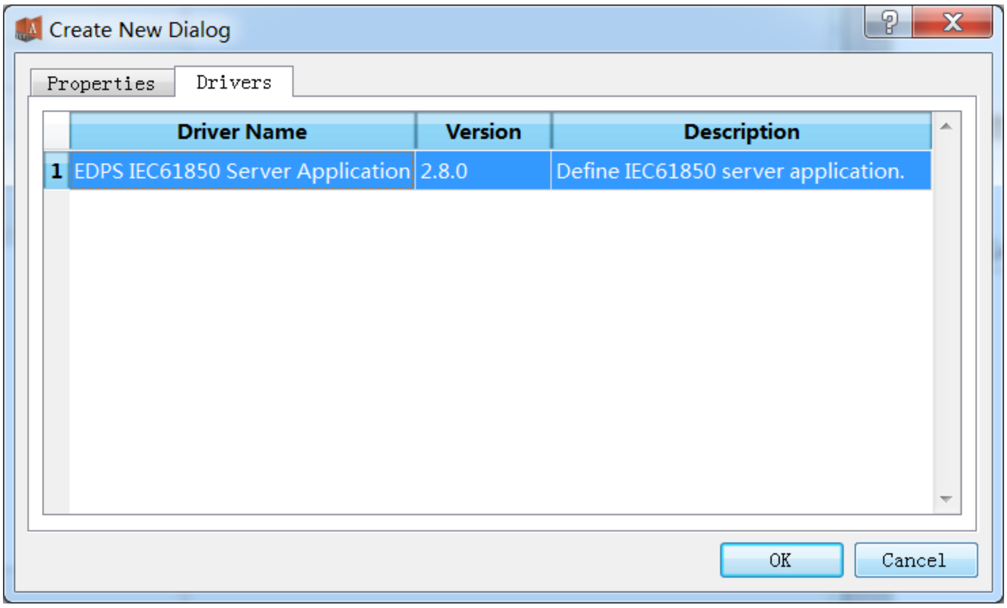
1. Open a project file.
2. Click the **PluginView** tab in the EDPS ICT-A+ management area.
3. Activate the IEC 61850 proxy plugin.



4. Right-click in the blank area and choose **New 61850...** from the shortcut menu. The driver creation dialog box is displayed.

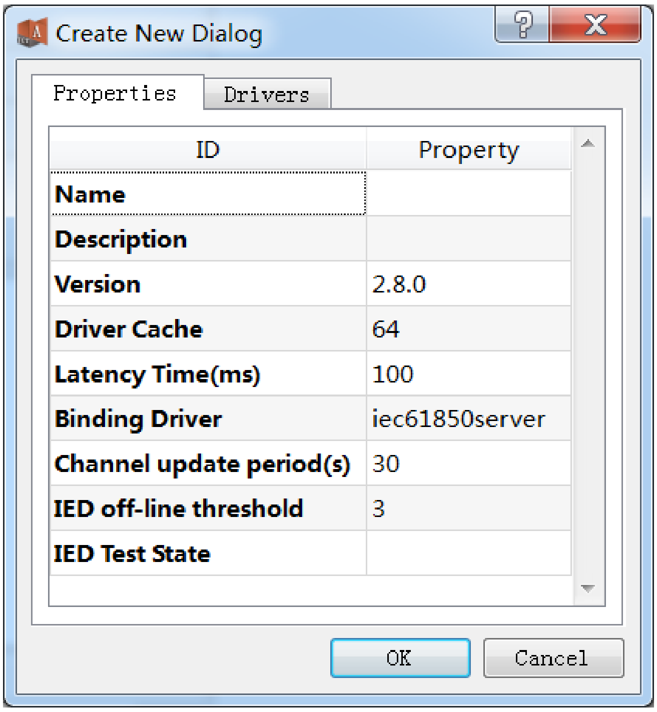


5. On the **Drivers** tab page, select the driver to be created.



	Driver Name	Version	Description
1	EDPS IEC61850 Server Application	2.8.0	Define IEC61850 server application.

6. On the **Properties** tab page, configure basic properties for the target driver.



ID	Property
Name	
Description	
Version	2.8.0
Driver Cache	64
Latency Time(ms)	100
Binding Driver	iec61850server
Channel update period(s)	30
IED off-line threshold	3
IED Test State	

7. Click **OK**.

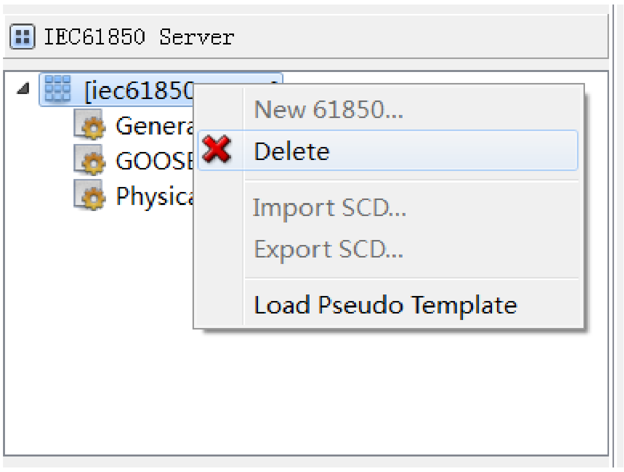
Note: Driver information

No.	Name	Description
1	Name	User-defined name
2	Description	Driver description
3	Version	Module version
4	Driver Cache	Cache size of the driver. The default value is 64

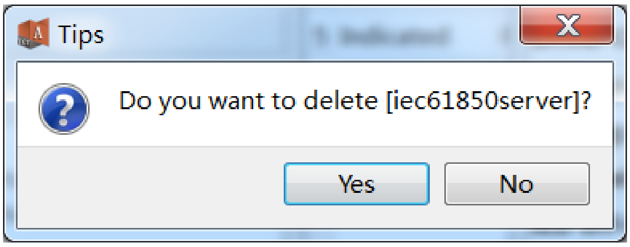
No.	Name	Description
		KB and the maximum value is 128 KB.
5	Latency Time(ms)	Latency time for updating real-time data. The unit is milliseconds.
6	Binding Driver	Name of the driver module. The value is unique and cannot be modified.
7	Channel update period(s)	Period for updating the channel communication status information. The unit is seconds.
8	IED off-line threshold	Device status threshold. When the number of consecutive failures in a channel exceeds the threshold, it is considered that the device is in the off-line state.
9	IED Test State	The internal test status point of the collected device is usually associated. The test status may affect the behavior of the forwarding end.

Delete Delete an IEC 61850 proxy driver.

8. Right-click the driver to be deleted and choose **Delete** from the shortcut menu.



9. A dialog box is displayed, asking you whether to delete the driver.

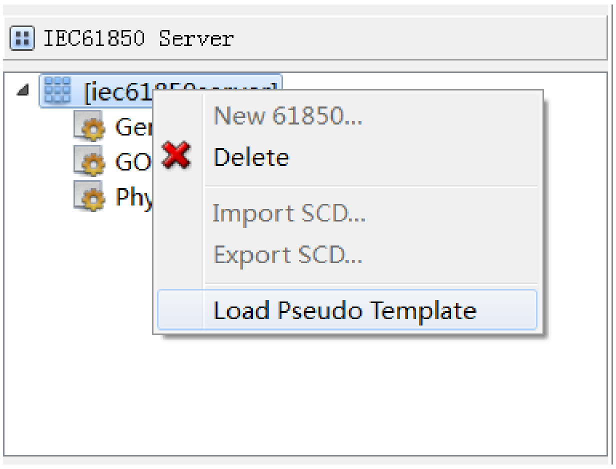


Do you want to delete [iec61850server]?

10. Click **Yes** to complete deletion.

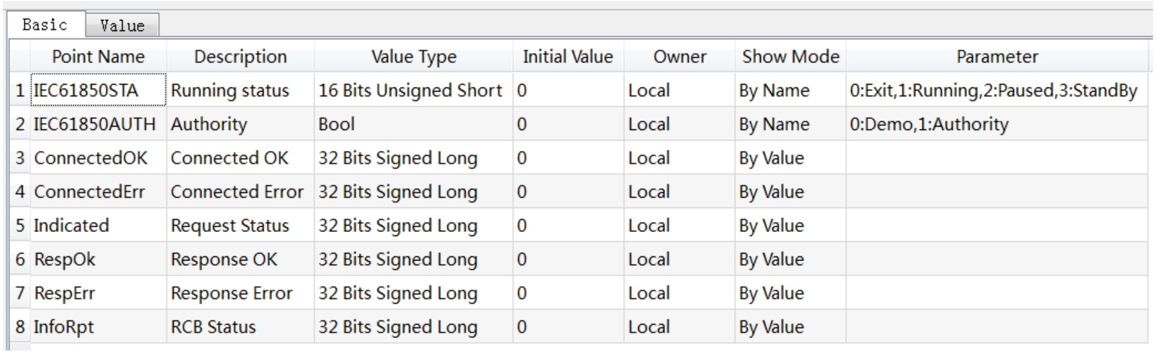
Pseudo Template Load a pseudo template from the system template library to the driver.

11. Right-click the driver bar and choose **Load Pseudo Template** from the shortcut menu.



12. Load a pseudo template to complete the loading of the pseudo point to the driver.

Note:



	Point Name	Description	Value Type	Initial Value	Owner	Show Mode	Parameter
1	IEC61850STA	Running status	16 Bits Unsigned Short	0	Local	By Name	0:Exit,1:Running,2:Paused,3:StandBy
2	IEC61850AUTH	Authority	Bool	0	Local	By Name	0:Demo,1:Authority
3	ConnectedOK	Connected OK	32 Bits Signed Long	0	Local	By Value	
4	ConnectedErr	Connected Error	32 Bits Signed Long	0	Local	By Value	
5	Indicated	Request Status	32 Bits Signed Long	0	Local	By Value	
6	RespOk	Response OK	32 Bits Signed Long	0	Local	By Value	
7	RespErr	Response Error	32 Bits Signed Long	0	Local	By Value	
8	InfoRpt	RCB Status	32 Bits Signed Long	0	Local	By Value	

No.	Name	Description
1	Running status	Running status information about the driver
2	Authority	Authority status of the driver
3	Connected OK	Number of successful connections
4	Connected Error	Number of connection errors

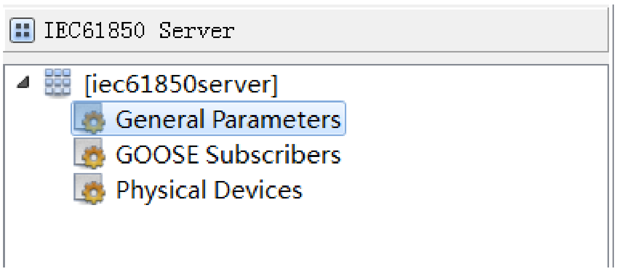
No.	Name	Description
5	Request Status	Number of service requests
6	Response OK	Number of correct service responses
7	Response Error	Number of service response errors
8	RCB Status	Number of BRCB/URCB information reports

A.2.2.General Parameters

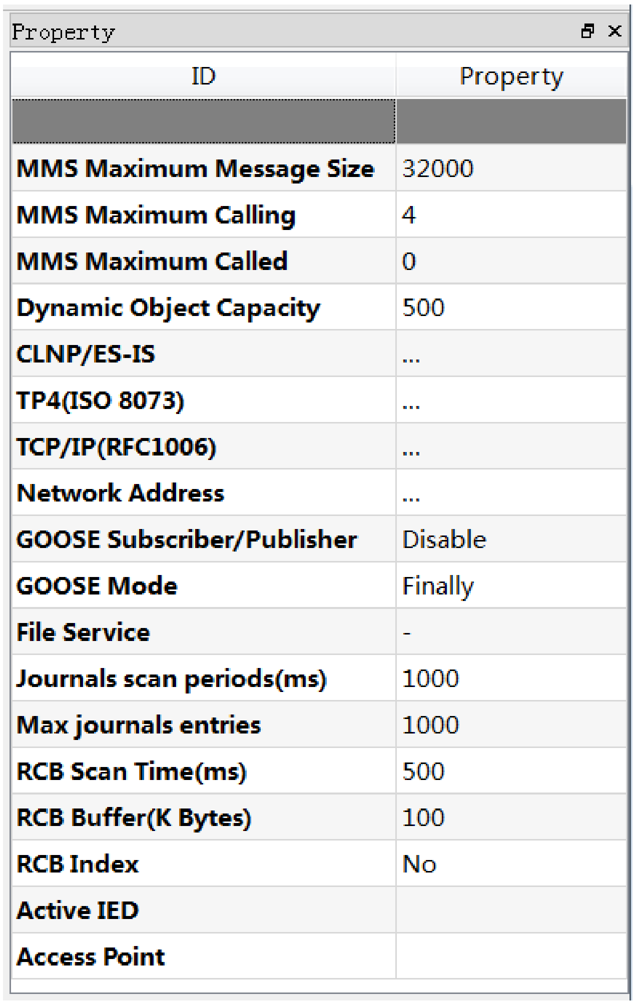
Overview View and configure the general parameters of the IEC 61850 proxy driver.

View and Configure View and configure the properties of communication parameters.

1. Open a project file.
2. Click the **PluginView** tab in the EDPS ICT-A+ management area.
3. Activate the IEC 61850 proxy plugin.
4. Select **General Parameters** in the management area.



5. View information in the property area.



ID	Property
MMS Maximum Message Size	32000
MMS Maximum Calling	4
MMS Maximum Called	0
Dynamic Object Capacity	500
CLNP/ES-IS	...
TP4(ISO 8073)	...
TCP/IP(RFC1006)	...
Network Address	...
GOOSE Subscriber/Publisher	Disable
GOOSE Mode	Finally
File Service	-
Journals scan periods(ms)	1000
Max journals entries	1000
RCB Scan Time(ms)	500
RCB Buffer(K Bytes)	100
RCB Index	No
Active IED	
Access Point	

Note: Information in the property area

No.	Name	Description	Remarks
1	MMS Maximum Message Size	Allowed maximum length of the PDU in the MMS	Use the default parameter value.
2	MMS Maximum Calling	Maximum number of calling connections allowed by the client	It must be set to 0.
3	MMS Maximum Called	Maximum number of called connections allowed by the server	Configure the parameter based on actual conditions and refer to the value in the preceding figure.
4	Dynamic Object Capacity	Capacity of the dynamic data object type supported	Configure the parameter based on actual conditions

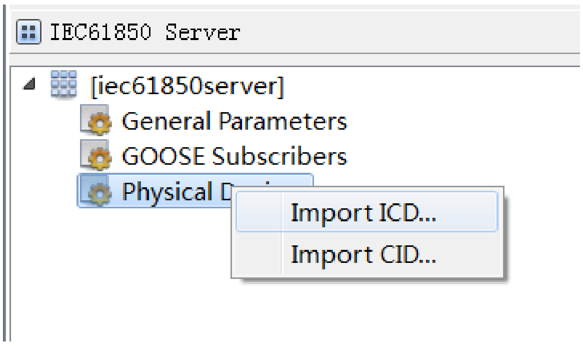
No.	Name	Description	Remarks
		by the client	and refer to the value in the preceding figure.
5	CLNP/ES-IS	Configuration of the network layer in the OSI protocol stack	Add one line in the table editor and use the default parameter value.
6	TP4(ISO 8073)	Configuration of the transport layer in the OSI protocol stack	Add one line in the table editor and use the default parameter value.
7	TCP/IP(RFC1006)	Configuration of the TCP/IP protocol stack in RFC1006 mode	Add one line in the table editor and use the default parameter value.
8	Network address	Set at least one network address.	Add one line in the table editor and use the default parameter value.
9	GOOSE Subscriber/Publisher	Whether to enable the GOOSE subscription/publishing function	Configure the parameter based on actual conditions.
10	GOOSE Mode	GOOSE information parsing mode: **Finally**, **Immediately**.	Configure the parameter based on actual conditions.
11	File Service	Root path of the file service	Configure the parameter based on actual conditions.
12	Journals scan periods(ms)	Log scanning period. The unit is milliseconds.	Configure the parameter based on actual conditions.
13	Max journals entries	Maximum number of log entries that can be stored	Configure the parameter based on actual conditions.
14	RCB Scan	RCB scanning time. The	Configure the parameter

No.	Name	Description	Remarks
	Time(ms)	unit is milliseconds.	based on actual conditions.
15	RCB Buffer(KBytes)	Default size of the RCB buffer. The unit is Kbytes.	Configure the parameter based on actual conditions.
16	RCB Index	Whether to automatically add the RCB index suffix	Configure the parameter based on actual conditions.
17	Active IED	Name of the active IED. It is usually the value of the **iedName** property in ConnectedAP in the .ICD/CID instance file.	Configure the parameter based on actual conditions.
18	Access Point	Name of the service access point. It is usually the value of the **apName** property in ConnectedAP in the .ICD/CID instance file.	Configure the parameter based on actual conditions.

A.2.3.Physical Device Management

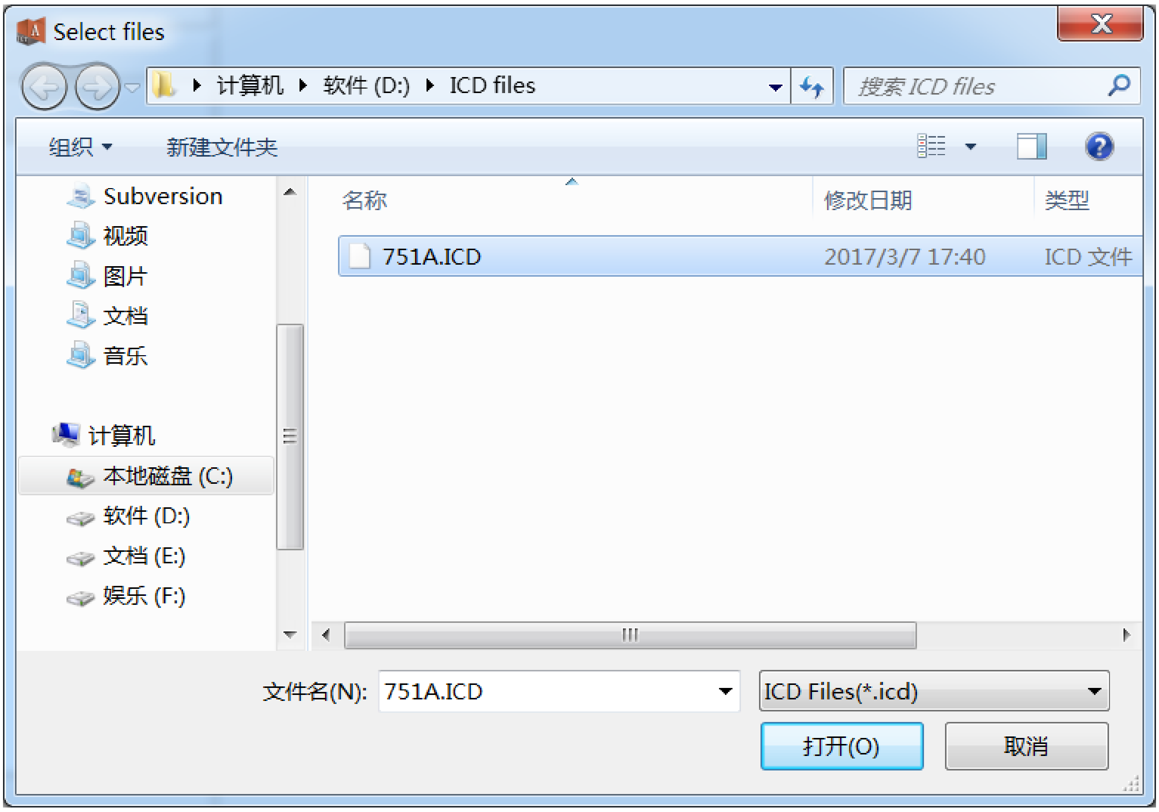
Import an ICD File Create an IEC 61850 proxy device by importing the IEC 61850 ICD file.

1. Open a project file.
2. Click the **PluginView** tab in the EDPS ICT-A+ management area.
3. Activate the IEC 61850 proxy plugin.
4. Right-click **Physical Devices** and choose **Import ICD** from the shortcut menu.



5. In the **Select files** dialog box, select a file and click **Open**.

6.

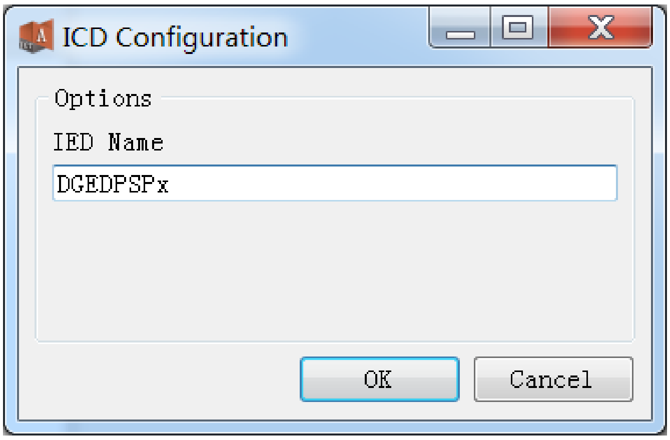


名称	修改日期	类型
751A.ICD	2017/3/7 17:40	ICD 文件

文件名(N): 751A.ICD

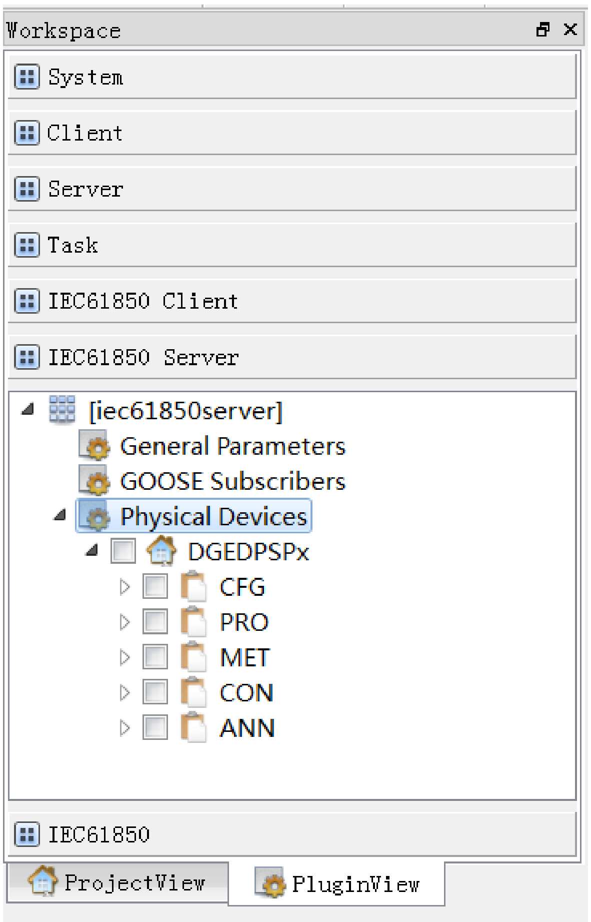
ICD Files(*.icd)

7. The **ICD Configuration** dialog box is displayed.



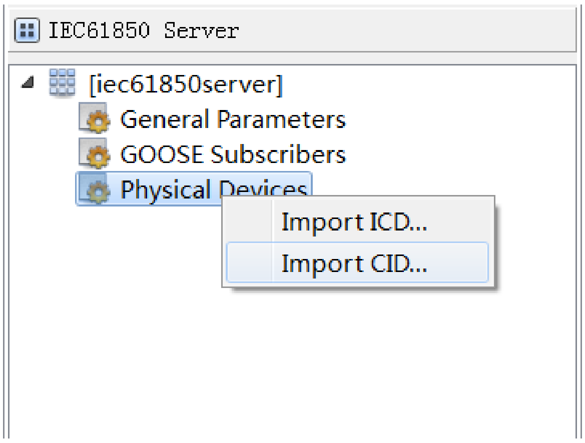
IED Name: DGEDPSPx

8. Set the instance name of the IED device and click **OK** to create the IEC 61850 device.

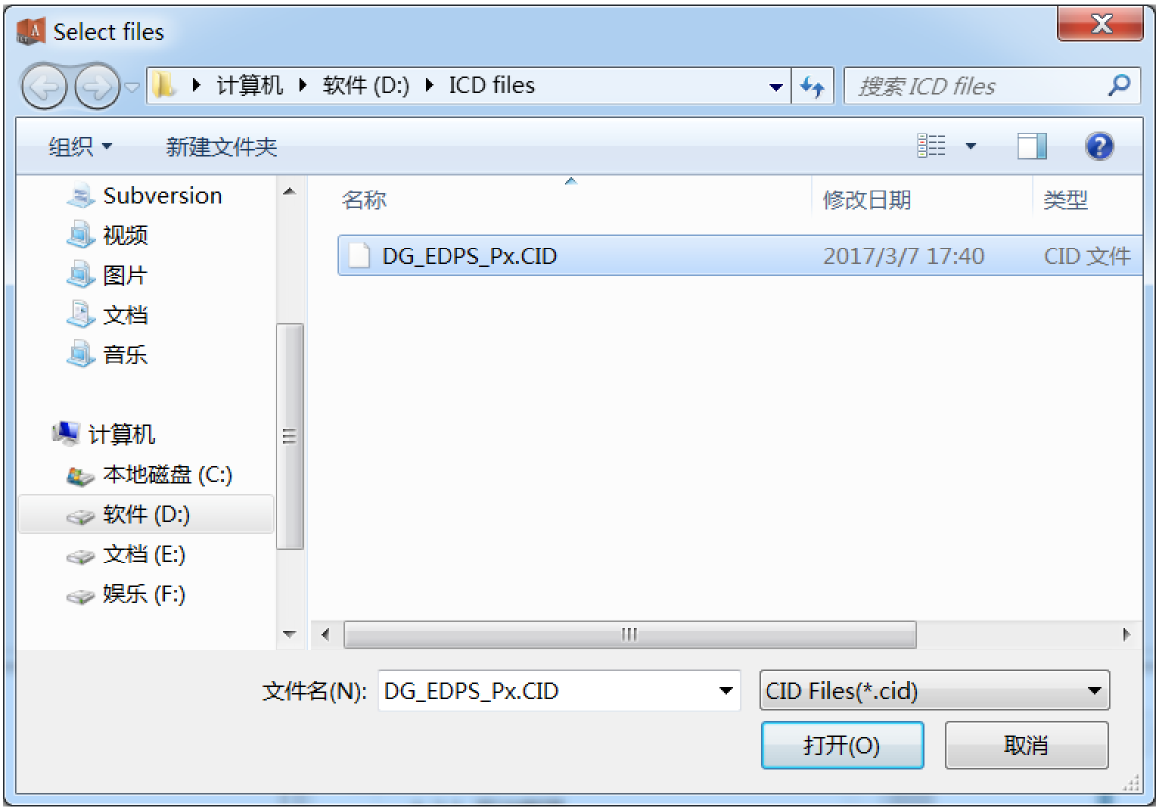


Import a CID File Create an IEC 61850 proxy device by importing an IEC 61850 CID file.

9. Right-click **Physical Devices** and choose **Import CID** from the shortcut menu.



10. In the **Select files** dialog box, select a file and click **Open**.

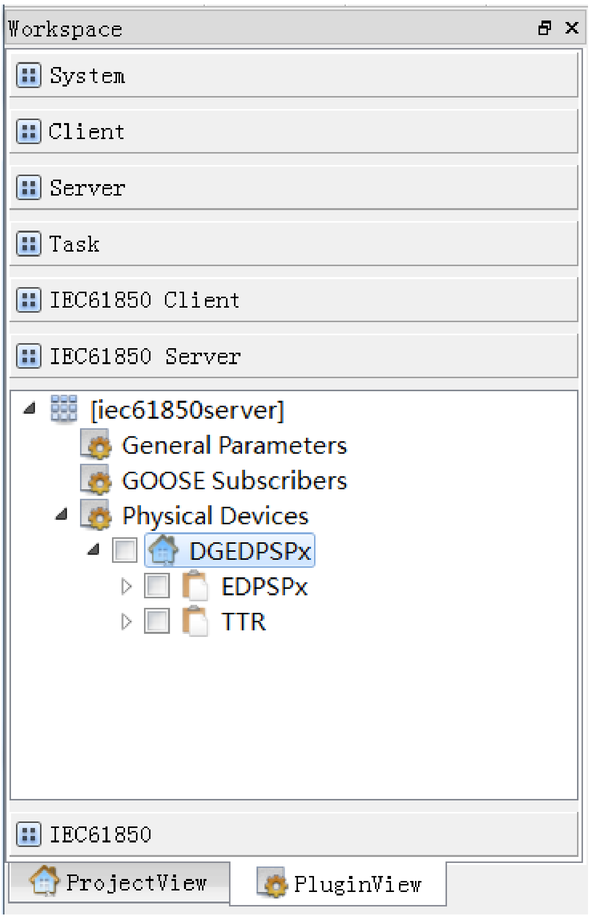


名称	修改日期	类型
DG_EDPS_Px.CID	2017/3/7 17:40	CID 文件

文件名(N): DG_EDPS_Px.CID

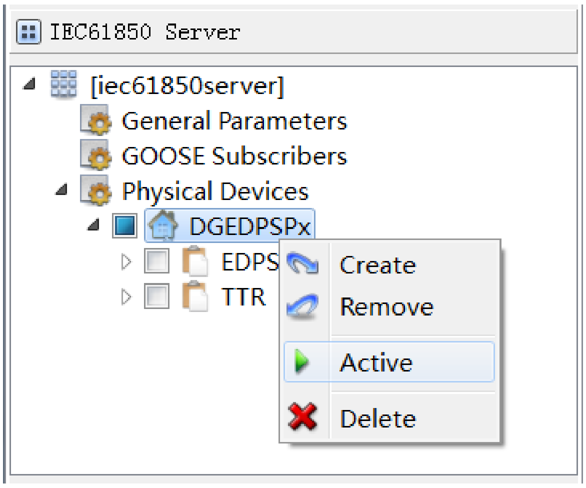
CID Files(*.cid)

11. Confirm the IED name and click **OK** to complete the creation of the IEC 61850 device.



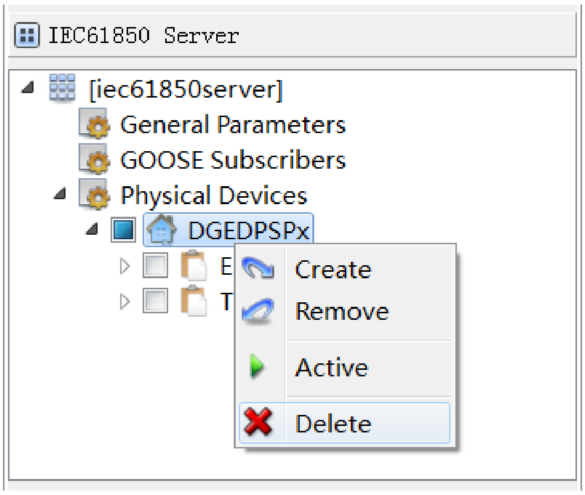
Activate a Device Activate the IEC 61850 physical device.

12. Right-click a physical device and choose **Active** from the shortcut menu to activate the physical device and access service point. After activation, information about the active device is displayed in the general parameter property area.

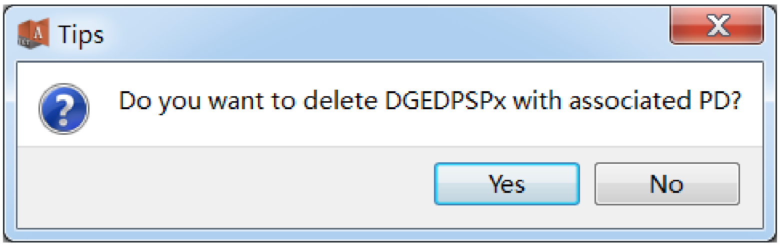


Delete a Device Delete the imported IEC 61850 device thoroughly.

13. Right-click a Level-1 subnode under **Physical Devices**.



14. Choose **Delete** from the shortcut menu.

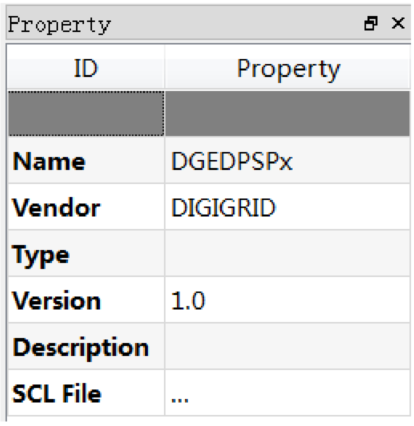


Do you want to delete DGEDPSPx with associated PD?

15. Click **Yes** to complete the deletion of the IEC 61850 physical device.

Device Parameters View physical device parameters of the IEC 61850 driver.

16. View the property area of the EDPS ICT-A+.



Property

ID	Property
Name	DGEDPSPx
Vendor	DIGIGRID
Type	
Version	1.0
Description	
SCL File	...

No.	Name	Description
1	Name	Device name
2	Vendor	Device vendor
3	Type	Device type
4	Version	Device version
6	Description	Device description
5	SCL File	SCL file relevant to the physical device

A.2.4.Information Point Management

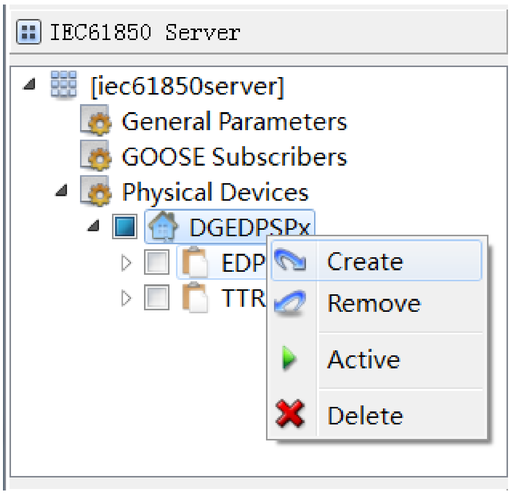
Create Establish the mapping between the EDPS ICT-A+ and an IEC 61850 client.

1. Open a project file.

2. Click the **PluginView** tab in the EDPS ICT-A+ management area.

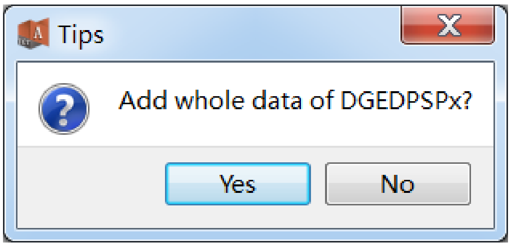
3. Activate the IEC 61850 proxy plugin.

4. Right-click a data management node under **Physical Devices**.



5. Choose **Create** from the shortcut menu to add the mapping between the EDPS ICT-A+

and the IEC 61850 client.



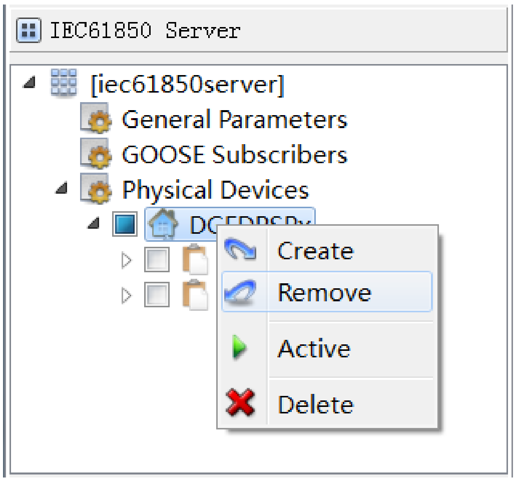
Add whole data of DGEDPSPx?

6. Click **Yes** to complete the establishment of the mapping between all information points in the IEC 61850 device and the EDPS ICT-A+.

Note: Selectively add required information points for mapping based on actual conditions.

Delete Remove the mapping between the EDPS ICT-A+ and an IEC 61850 client.

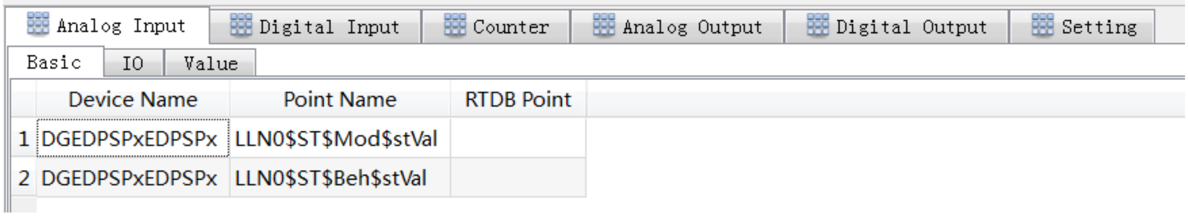
7. Right-click a data management node under **Physical Devices**.



8. Choose **Remove** from the shortcut menu. Click **Yes** to remove the mapping between the EDPS ICT-A+ and the IEC 61850 client.

Mapping Create the mapping between a traditional protocol data point and an IEC 61850 data object.

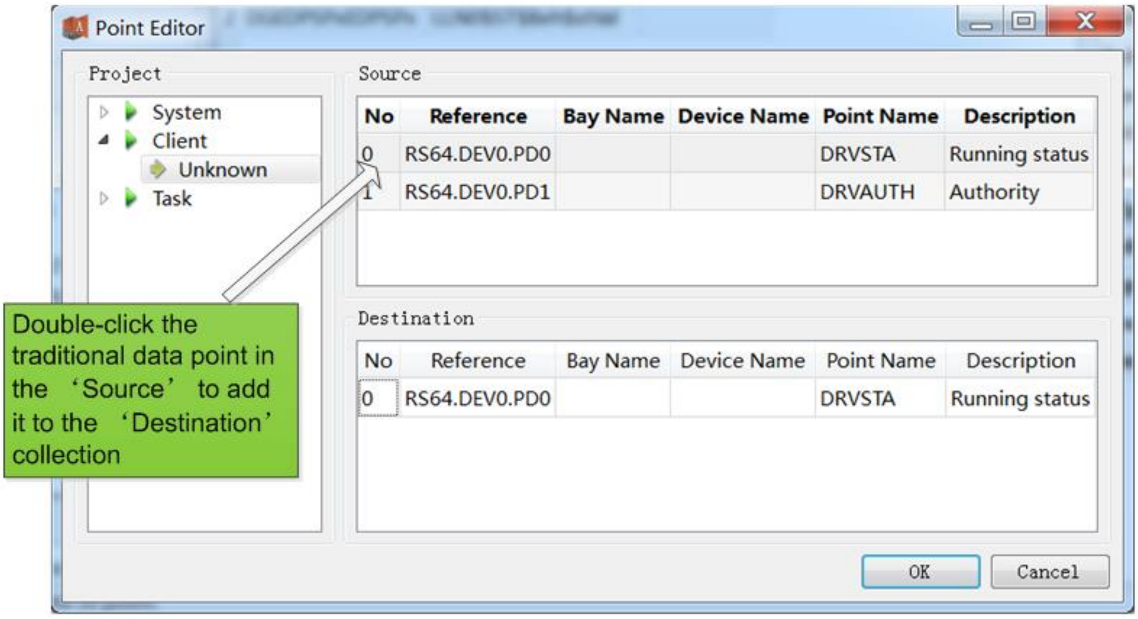
9. Select any subnode under **Physical Devices** and view the mapping table in the data area of the EDPS ICT-A+.



	Device Name	Point Name	RTDB Point
1	DGEDPSPxEDPSPx	LLN0$ST$Mod$stVal	
2	DGEDPSPxEDPSPx	LLN0$ST$Beh$stVal	

10. Click the edit box in the **RTDB Point** column next to the data object.

11. In the displayed **Pointer Editor** dialog box, select a traditional data point.



Source

No	Reference	Bay Name	Device Name	Point Name	Description
0	RS64.DEV0.PD0			DRVSTA	Running status
1	RS64.DEV0.PD1			DRVAUTH	Authority

Destination

No	Reference	Bay Name	Device Name	Point Name	Description
0	RS64.DEV0.PD0			DRVSTA	Running status

Double-click the traditional data point in the ‘Source’ to add it to the ‘Destination’ collection

12. Click **OK** to complete the creation of the mapping between the traditional data point and the IEC 61850 data object.

View Properties View the properties of internal objects of an IEC61850 device.

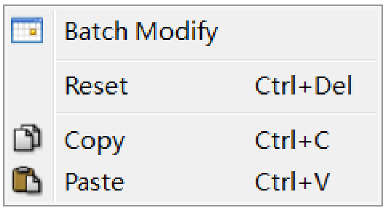
13. Select any subnode under **Physical Devices** and view the object properties in the property area.

A.2.5.Data Management

Batch Modify Modify data in the data area in batches.

View parameters of an information point in a data type in the data area of the EDPS ICT-A+. The device name, point name, and IO parameters in basic information cannot be edited and their values depend on the IEC 61850 device.

1. Open a project file.
2. Click the **PluginView** tab in the EDPS ICT-A+ management area.
3. Activate the IEC 61850 proxy plugin.
4. In the data area, click the tab of basic information of different data types.
5. Select multiple objects, right-click the objects and choose **Batch Modify** from the shortcut menu. A dialog box is displayed.



6. Modify data and click **OK** to complete batch modification of the data.

Reset Use initialized values of table data properties to replace current values.

7. Right-click an object and choose **Reset** from the shortcut menu. Click **Yes** to complete modification.

Copy and Paste Copy and paste data.

Data can be copied and pasted across plugins, links, devices, and types.

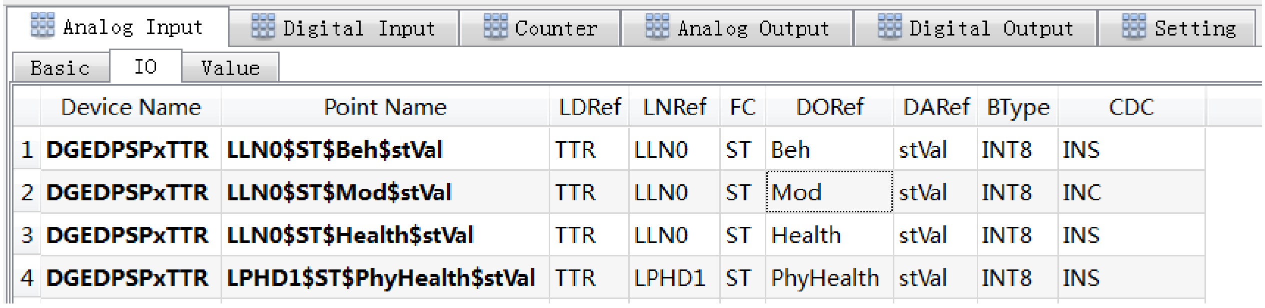
Data can be copied and pasted between an EXCEL sheet and the EDPS ICT-A+.

The copy operation is allowed in all data areas.

The paste operation is allowed in editable areas.

8. Right-click an object and choose **Copy**/**Paste** from the shortcut menu (the paste operation is not supported in areas that cannot be edited).

Note: IO information parameters



	Device Name	Point Name	LDRef	LNRef	FC	DORef	DARef	BType	CDC
1	**DGEDPSPxTTR**	**LLN0$ST$Beh$stVal**	TTR	LLN0	ST	Beh	stVal	INT8	INS
2	**DGEDPSPxTTR**	**LLN0$ST$Mod$stVal**	TTR	LLN0	ST	Mod	stVal	INT8	INC
3	**DGEDPSPxTTR**	**LLN0$ST$Health$stVal**	TTR	LLN0	ST	Health	stVal	INT8	INS
4	**DGEDPSPxTTR**	**LPHD1$ST$PhyHealth$stVal**	TTR	LPHD1	ST	PhyHealth	stVal	INT8	INS

No.	Name	Description
1	Device Name	Instance name of the logic device to which an information point belongs
2	Point Name	Complete reference name of the MMS index of the information point
3	LDRef	Reference name of the logic device to which the information point belongs
4	LNRef	Reference name of the logic node to which the information point belongs

No.	Name	Description
5	FC	Function constraint of the information point
6	DORef	Reference name of the data object of the information point
7	DARef	Reference name of the data attribute of the information point
8	BType	Basic data type of the information point
9	CDC	Common data class to which the information point belongs

A.2.6.GOOSE Subscriber

Configure the GOOSE subscribers module of the IEC 61850 device.

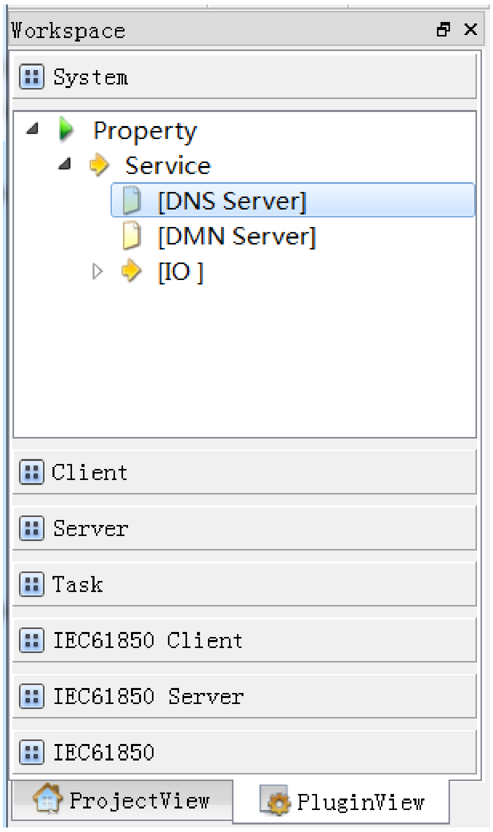
Note: In the configuration of the GOOSE subscription module, the ICD/CID file with GOOSE control block needs to be imported, the object points covered by the GOOSE block need to be added, the GOOSE control block needs to be activated, and other operations are the same as those in A.2.3 and A.2.4.

Appendix B DNS Service Configuration

Appendix B describes the configuration of the DNS service module on the EDPS ICT-A+. You can correctly load and use the DNS service after configuration. The property information and pseudo point information are described in the configuration manual. The EDPS ICT-A+ provides a simple and fast way to help users complete the configuration.

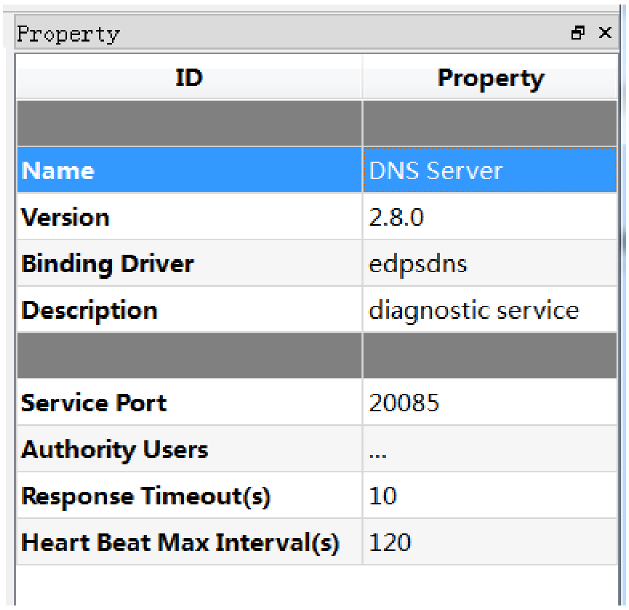
Operation View service information.

1. Open a project file.
2. Click the **PluginView** tab in the EDPS ICT-A+ management area.
3. Activate the system information plugin.



4. Right-click the **DNS Server** node and choose **Load Pseudo Template** from the shortcut menu. The node name can be modified.

Property View the property area of the EDPS ICT-A+.

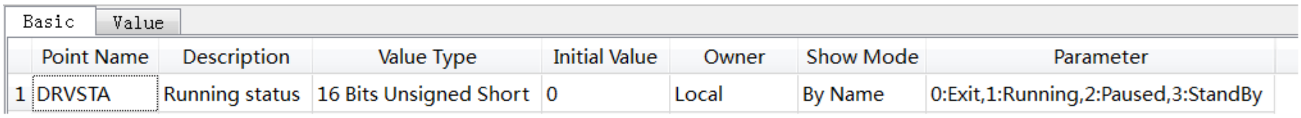


Property

ID	Property
Name	DNS Server
Version	2.8.0
Binding Driver	edpsdns
Description	diagnostic service
Service Port	20085
Authority Users	...
Response Timeout(s)	10
Heart Beat Max Interval(s)	120

No.	Name	Description
1	Name	Service name
2	Version	Service version
3	Binding Driver	Name of the module to which the service is bound. The value is unique and cannot be modified.
4	Description	Service description
5	Service Port	Port of the service communication
6	Authority Users	Authorized user
7	Response Timeout(s)	Maximum waiting response interval of DNS commands
8	Heart Beat Max Interval(s)	Maximum heartbeat interval of the client

Pseudo Point View the data area of the EDPS ICT-A+.



Basic | Value

	Point Name	Description	Value Type	Initial Value	Owner	Show Mode	Parameter
1	DRVSTA	Running status	16 Bits Unsigned Short	0	Local	By Name	0:Exit,1:Running,2:Paused,3:StandBy

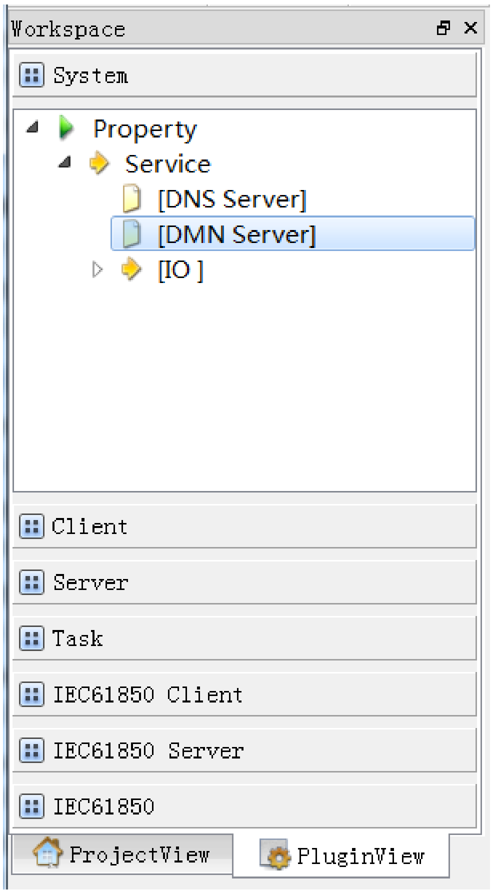
No.	Name	Description
1	Running status	Running status information about the service

Appendix C DMN Service Configuration

Appendix C describes the configuration of the DMN service module on the EDPS ICT-A+. You can correctly load and use the DMN service after configuration. The property information and pseudo point information are described in the configuration manual. The EDPS ICT-A+ provides a simple and fast way to help users complete the configuration.

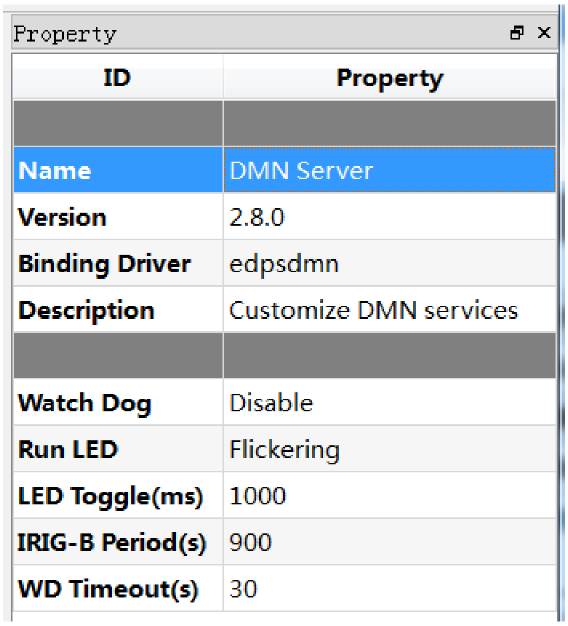
Operation View service information.

1. Open a project file.
2. Click the **PluginView** tab in the EDPS ICT-A+ management area.
3. Activate the system information plugin.



4. Right-click the **DMN Server** node and choose **Load Pseudo Template** from the shortcut menu. The node name can be modified.

Property View the property area of the EDPS ICT-A+.

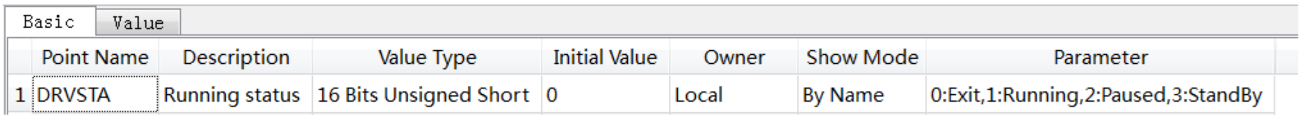


Property

ID	Property
Name	DMN Server
Version	2.8.0
Binding Driver	edpsdmn
Description	Customize DMN services
Watch Dog	Disable
Run LED	Flickering
LED Toggle(ms)	1000
IRIG-B Period(s)	900
WD Timeout(s)	30

No.	Name	Description
1	Name	Service name
2	Version	Service version
3	Binding Driver	Name of the module to which the service is bound. The value is unique and cannot be modified.
4	Description	Service description
5	Watch Dog	Whether to enable the watchdog function
6	Run LED	Work mode of the run LED
7	LED Toggle(ms)	Blinking period of the run LED in blinking mode. The unit is milliseconds.
8	IRIG-B Period(s)	Period of synchronization between IRIG-B signals and system time. The unit is seconds.
9	WD Timeout(s)	Watchdog timeout time. The unit is seconds.

Pseudo Point View the data area of the EDPS ICT-A+.



	Point Name	Description	Value Type	Initial Value	Owner	Show Mode	Parameter
1	DRVSTA	Running status	16 Bits Unsigned Short	0	Local	By Name	0:Exit,1:Running,2:Paused,3:StandBy

No.	Name	Description
1	Running status	Running status information about the service

Appendix D Script Calculation Application Configuration

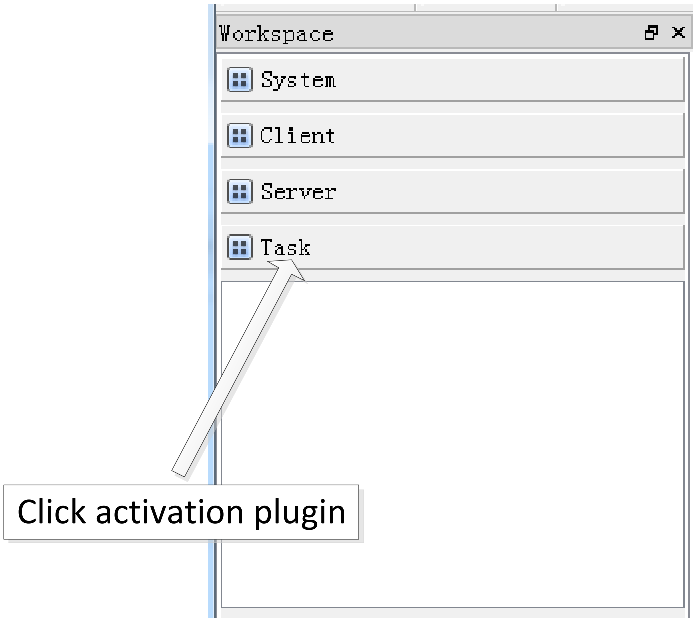
Appendix D describes how to configure the advanced application module of the logic script on the EDPS ICT-A+. The application information, parameters, configuration, and calculation are described in the configuration manual. The advanced application module of the logic script of the EDPS ICT-A+ is logically programmed using the standard C language. The EDPS ICT-A+ provides a simple and fast way to help users complete the configuration.

Application Information

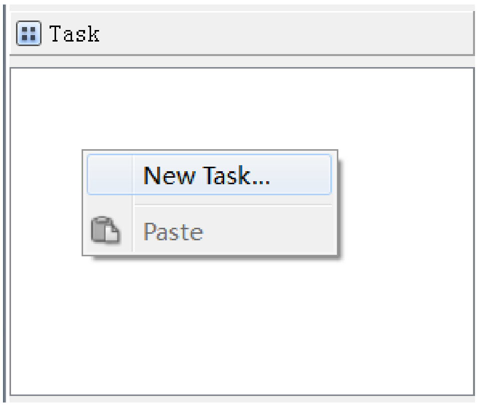
Overview Describe the driver for script calculation as well as basic applications of parameters.

Create Create a script calculation driver.

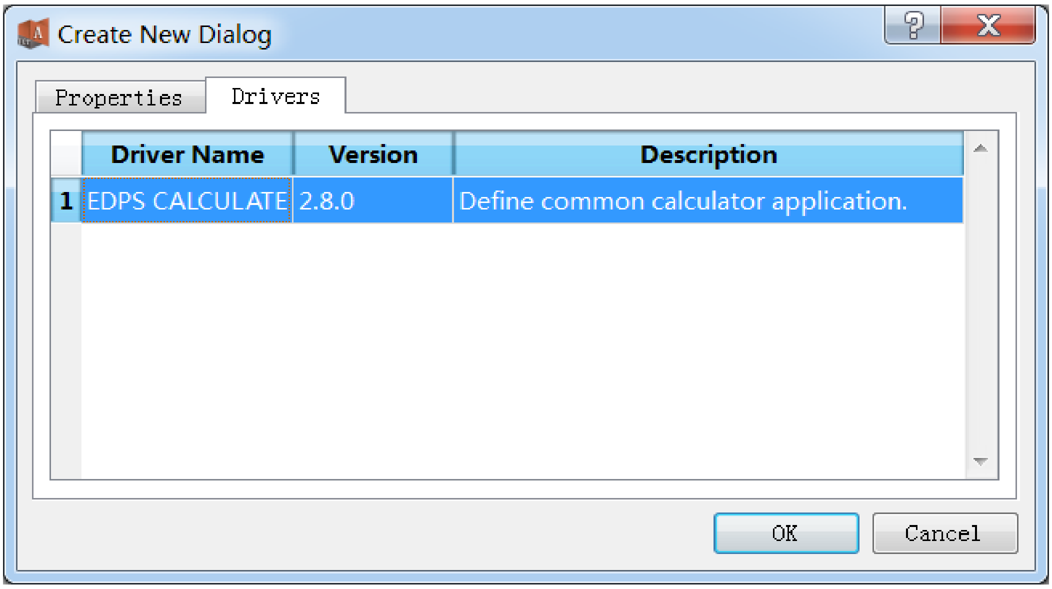
1. Open a project file.
2. Click the **PluginView** tab in the EDPS ICT-A+ management area.
3. Activate the advanced application plugin.



4. Right-click in the blank area and choose **New Task** from the shortcut menu. The driver creation dialog box is displayed.

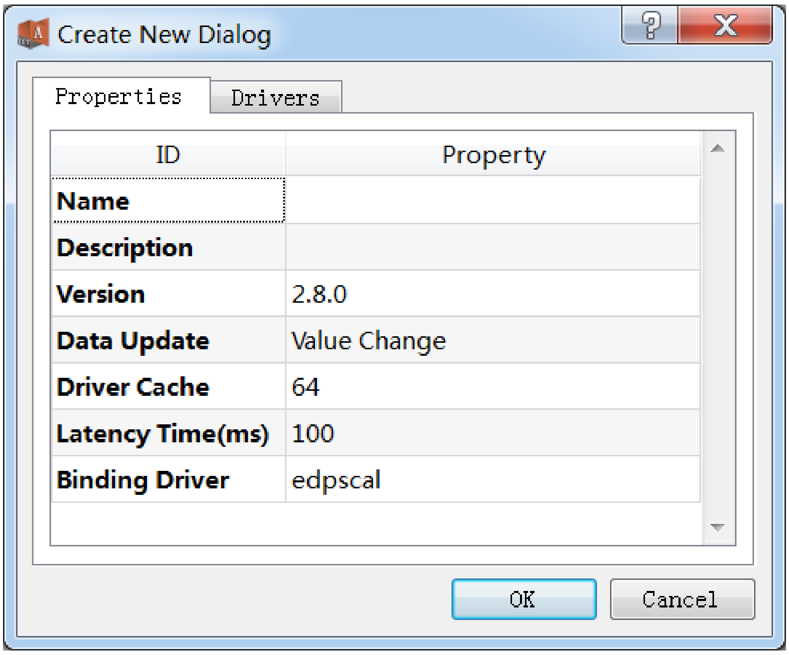


5. On the **Drivers** tab page, select the driver to be created.



	Driver Name	Version	Description
1	EDPS CALCULATE	2.8.0	Define common calculator application.

6. On the **Properties** tab page, configure basic properties for the target driver.



ID	Property
Name	
Description	
Version	2.8.0
Data Update	Value Change
Driver Cache	64
Latency Time(ms)	100
Binding Driver	edpscal

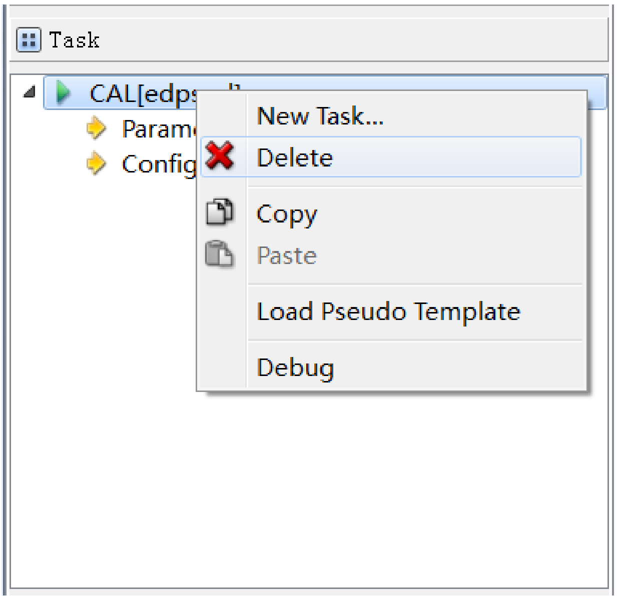
7. Click **OK**.

Note: Driver information

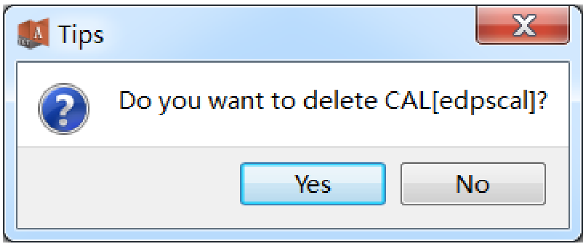
No.	Name	Description
1	Name	Driver name to be displayed
2	Description	Driver description
3	Version	Driver version
4	Data Update	Mode of updating data into the database Value Change: The database is updated and other driver protocols are notified only when the value changes. Time Change: The value or time is updated into the database and other driver protocols are notified whenever the value or time changes. Time Update: If the value keeps unchanged but the time changes, the change is updated into the database but other driver protocols are not notified.
5	Driver Cache	Cache size
6	Latency Time(ms)	Latency for updating the real-time database The system writes raw data into the real-time database only after the latency time.
7	Binding Driver	Name of the application to which the driver is bound. The value is unique and cannot be modified.

Delete Delete a script calculation driver.

8. Right-click the driver to be deleted and choose **Delete** from the shortcut menu.



9. A dialog box is displayed, asking you whether to delete the driver.

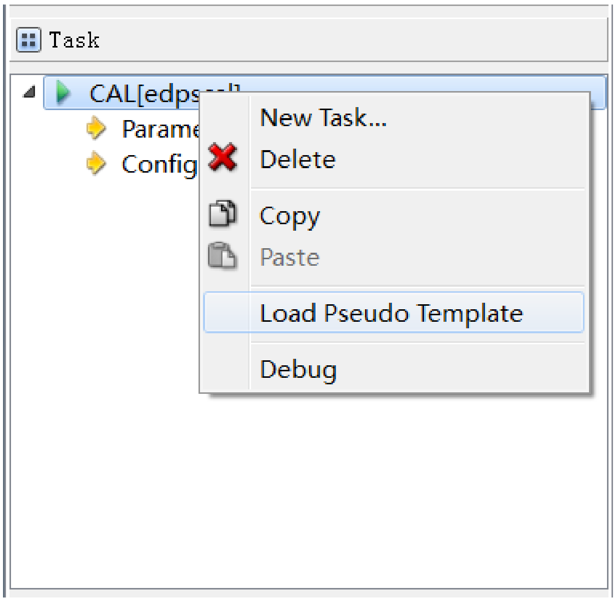


Do you want to delete CAL[edpscal]?

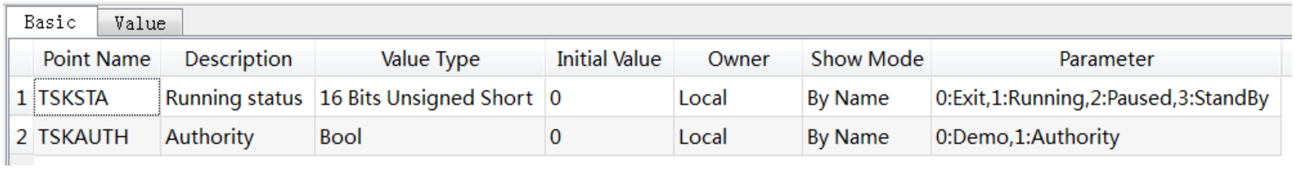
10. Click **Yes** to complete deletion.

Pseudo Template Load a pseudo template from the system template library to the driver.

11. Right-click the driver bar and choose **Load Pseudo Template** from the shortcut menu, to load a pseudo template to the driver.



Note:

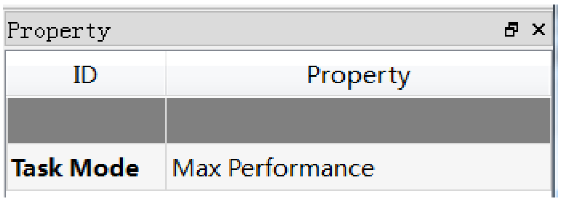


	Point Name	Description	Value Type	Initial Value	Owner	Show Mode	Parameter
1	TSKSTA	Running status	16 Bits Unsigned Short	0	Local	By Name	0:Exit,1:Running,2:Paused,3:StandBy
2	TSKAUTH	Authority	Bool	0	Local	By Name	0:Demo,1:Authority

No.	Name	Description
1	Running status	Running status information about the driver
2	Authority	Authority status of the driver

Parameters Define parameters for the advanced application module.

View parameter properties.



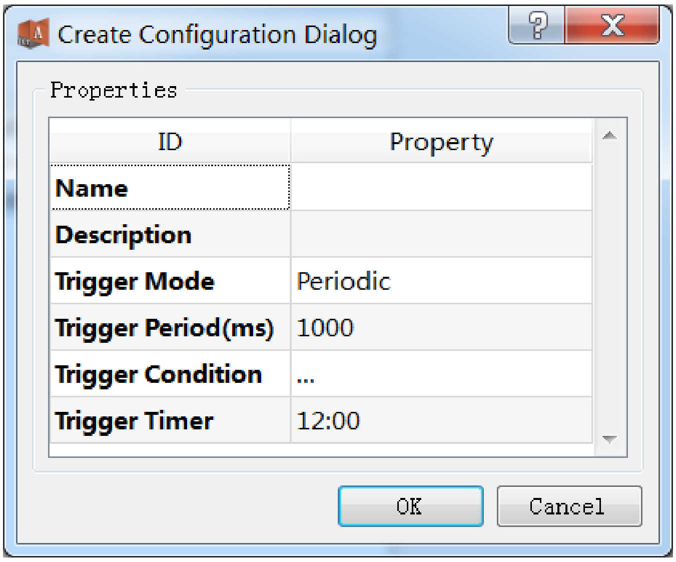
ID	Property
Task Mode	Max Performance

Note: Run parameter information

No.	Name	Description
1	Task Mode	Work mode of the application. The default value is **Max Performance**. ● Normal ● Max Performance

Configuration Define the configuration for the advanced application module.

Right-click **Configuration** and choose **Create** from the shortcut menu. The **Create Configuration Dialog** box is displayed. After confirming the configuration, click **OK** to complete creation.



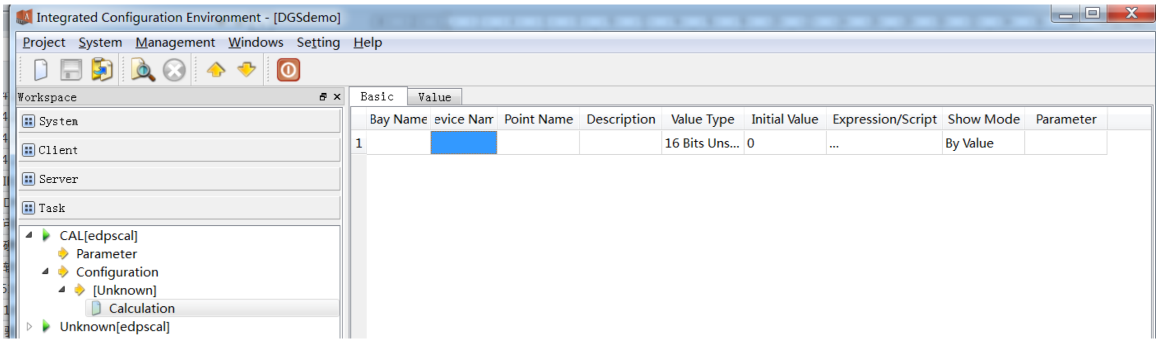
ID	Property
Name	
Description	
Trigger Mode	Periodic
Trigger Period(ms)	1000
Trigger Condition	...
Trigger Timer	12:00

Note:

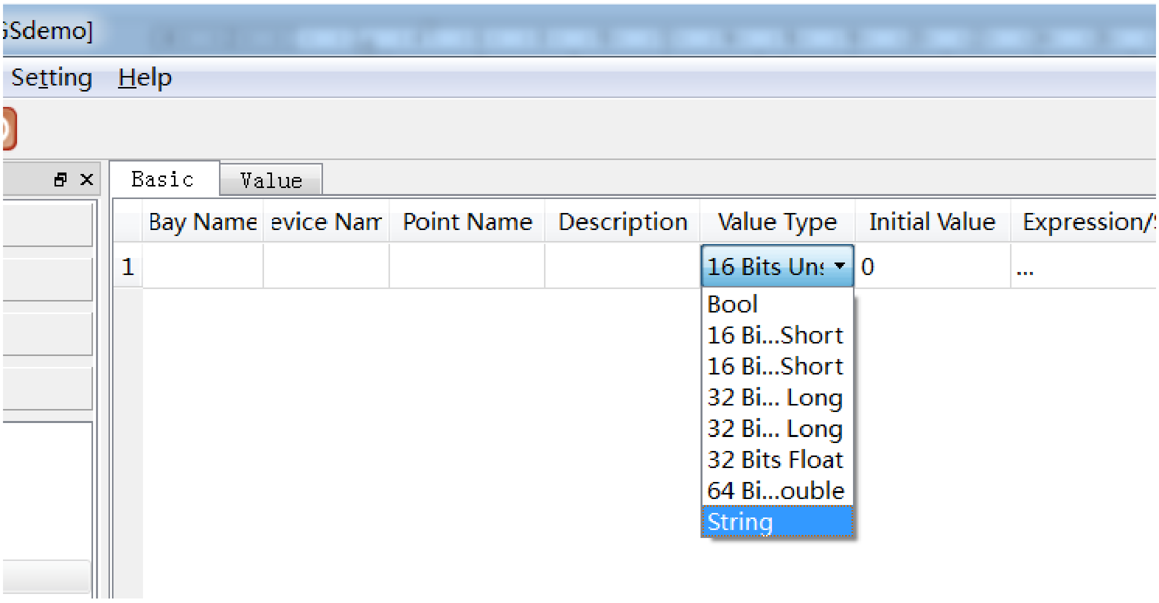
No.	Name	Description
1	Name	Script application name
2	Description	Script application description
3	Trigger Mode	Trigger mode of the script calculation task ● Periodic ● Conditional ● Scheduled
4	Trigger Period(ms)	Interval of periodic trigger. The unit is milliseconds.
5	Trigger Condition	Work parameter of conditional trigger
6	Trigger Timer	Scheduled trigger time in 24-hour system. The value is accurate to minutes and is in the format of HH:MM.

Calculation Information

Right-click **Calculation** and choose **Create** from the shortcut menu to create a calculation point. Change the value type, double-click the edit box in the **Expression/Script** column for editing as required, and use the standard C language for logical programming.



	Bay Name	evice Narr	Point Name	Description	Value Type	Initial Value	Expression/Script	Show Mode	Parameter
1					16 Bits Uns...	0	...	By Value	



	Bay Name	evice Narr	Point Name	Description	Value Type	Initial Value	Expression/:
1					16 Bits Un:	0	...

Appendix E Acronyms and Abbreviations

Acronym and Abbreviation	**Full Spelling**
ACE	Access Control Entry
ACL	Access Control List
ARP	Address Resolution Protocol
BootP	Bootstrap Protocol
BPDU	Bridge Protocol Data Unit
CIST	Common and Internal Spanning Tree
CLI	Command Line Interface
CoS	Class of Service
CST	Common Spanning Tree
DHCP	Dynamic Host Configuration Protocol
DHP	Dual Homing Protocol
DNS	Domain Name System
DRP	Distributed Redundancy Protocol
DSCP	Differentiated Services Code Point
DST	Daylight Saving Time
EAPOL	Extensible Authentication Protocol over LAN
GARP	Generic Attribute Registration Protocol
GMRP	GARP Multicast Registration Protocol
GVRP	GARP VLAN Registration Protocol
HTTP	Hyper Text Transfer Protocol
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IGMP Snooping	Internet Group Management Protocol Snooping
IST	Internal Spanning Tree
LACP	Link Aggregation Control Protocol

Acronym and Abbreviation	**Full Spelling**
LACPDU	Link Aggregation Control Protocol Data Unit
LLDP	Link Layer Discovery Protocol
LLDPDU	Link Layer Discovery Protocol Data Unit
MIB	Management Information Base
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
NAS	Network Access Server
NetBIOS	Network Basic Input/Output System
NMS	Network Management Station
NTP	Network Time Protocol
OID	Object Identifier
PCP	Priority Code Point
PVLAN	Private VLAN
QCL	QoS Control List
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RMON	Remote Network Monitoring
RSTP	Rapid Spanning Tree Protocol
SFTP	Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SP	Strict Priority
SSH	Secure Shell
SSL	Secure Sockets Layer
SSM	Source Specific Multicast
STP	Spanning Tree Protocol
TACACS+	Terminal Access Controller Access Control System

Acronym and Abbreviation	**Full Spelling**
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
USM	User-Based Security Model
VLAN	Virtual Local Area Network
WINS	Windows Internet Naming Service
WRR	Weighted Round Robin