Ruby3A Series PRP/HSR Switches

Web Operation manual

Date of issue: Mar. 2020

Version: V1.1

KYLAND

Disclaimer

Kyland try the best to keep the information in this manual as accurate and up-to-date as possible. Kyland is not liable for any errors, omissions or changes of any description of the manual, product description are subject to change without notice.

Publish: Beijing Kyland Technology Co., Ltd.

Website: http://www.kyland.com.cn

http://www.kyland.cn

Service hot line: 010-88796676

Fax: 010-88796678

Email: services@kyland.com.cn

Contents

Preface 1
1 Product Introduction 4
1.1 Overview 4
1.2 Software Features 4
1.3 Applicable Products 5
2 Switch Access 6
2.1 View Types 6
2.2 Switch Access by Console Port 7
2.3 Switch Access by Telnet 11
2.4 Switch Access by Web 11
3 Device information 14
3.1 Switch basic information 14
4 Switch Basic Configration 16
4.1 User Configuration 16
4.2 IP Configuration 16
4.2.1 DHCP Configration 18
4.2.2 Static IP Configuration 20
4.3 System Information 21
4.3.1 Clock Configuration 21
4.3.2 CPU Status 22
4.3.3 NETWORK Status 22
4.3.4 System Log 23
4.4 File Download 23
4.4.1 Mib File Download 24
4.4.2 Configuration File Download 25
4.5 Firmware Upgrade 25
4.5.1 Local Upgrade 26

4.5.2 FTP Upgrade 28
4.5.3 SFTP upgrade 32
4.6 File Upload 35
4.7 Reboot 35
5 FUNCTIONS 37
5.1 Redundancy 37
5.1.1 Principle 37
5.1.2 Web Configuration 40
5.1.3 Typical Configuration Example 43
5.2 PTP 46
5.2.1 Introduce 46
5.2.2 Concept 46
5.2.3 Synchronization principle 48
5.2.4 Web Configuration 49
5.3 Statistics 53
6 Other Configurations 57
6.1 Alarm 57
6.1.1 Introduce 57
6.1.2 Web Configuration 57
6.2 Port Configuration 59
6.3 Mac Configuration 61
6.3.1 Mac Queries 62
6.3.2 Mac Address Control 63
6.3.3 Mac Address Configuration 64
6.4 Sntp 65
6.4.1 Introducation 65
6.4.2 Web Configuration 66
6.5 Ntp 67

6.5.1 Introduction 67
6.5.2 NTP Working Modes 68
6.5.3 Web Configuration 69
6.6 IEC61850 MMS 70
6.6.1 Introduction 70
6.6.2 Web Configuration 70
6.7 SNMPv2c 72
6.7.1 Introduction 72
6.7.2 Implementation 72
6.7.3 Explanation 73
6.7.4 MIB Introduction 73
6.7.5 Web Configuration 74
6.7.6 Typical Configuration Example 77
6.8 SNMP v3 78
6.8.1 Introduce 78
6.8.2 Implementation 78
6.8.3 Web Configuration 78
6.8.4 Typical Configuration Example 86
6.9 File Server 87
6.9.1 FTP 87
6.9.2 SFTP 90
6.10 LLDP 92
6.10.1 Introduction 92
6.10.2 Web Configuration 93
6.11 DDMI 94
6.11.1 Introduction 94
6.11.2 Web Configuration 94
6.12 Virtual Cable Test 95

6.12.1 Introduction 95
6.12.2 Web Configuration 96
6.13 RADIUS 97
6.13.1 Introduction 97
6.13.2 Web Configuration 98
6.13.3 Typical Configuration Example 100
6.14 TACACS Plus 101
6.14.1 Introduction 101
6.14.2 Web Configuration 101
6.14.3 Typical Configuration Example 103
6.15 AAA 104
6.15.1 AAA Introducation 104
6.15.2 Web Configuration 105
6.16 LINE 106
6.16.1 Introducation 106
6.16.2 Web Configuration 106
7 Switch Maintenance 110
8 Network Nodes 111
Appendix List of abbreviations 113

Preface

This manual mainly introduces the access methods and software features of the Ruby3A series PRP/HSR switches, and details Web configuration methods.

Content Structure

The manual contains the following contents:

Main Content	Explanation
1. Product introduction	➢ Overview ➢ Software features ➢ Product models
2. Switch access	➢ View types ➢ Switch access by console port ➢ Switch access by Telnet ➢ Switch access by Web
3. Device information	Switch basic information
4. Switch Basic Configration	➢ User Configuration ➢ IP Configuration ➢ System Information ➢ File Download ➢ Firmware Upgrade ➢ File Upload ➢ Reboot
5. FUNCTIONS	➢ Redundancy ➢ PTP ➢ Statistics
6. Other Configurations	➢ Alarm ➢ Port Configuration ➢ Mac Configuration

	➢ Sntp ➢ Ntp ➢ IEC61850 MMS ➢ SNMPv2c ➢ SNMPv3 ➢ File Server ➢ LLDP ➢ DDMI ➢ Virtual Cable Test ➢ Radius ➢ Tacacs Plus ➢ AAA ➢ LINE
7. Switch Maintenance	
8. Network Nodes	

Conventions in the manual

1. Text format conventions

Format	Explanation
< >	The content in < > is a button name. For example, click <Apply> button.
[ ]	The content in [ ] is a window name or a menu name. For example, click [File] menu item.
{ }	The content in { } is a portfolio. For example, {IP address, MAC address} means IP address and MAC address are a portfolio and they can be configured and displayed together.
→	Multi-level menus are separated by "→". For example, Start → All Programs → Accessories. Click [Start] menu, click the sub menu [All programs], then click the submenu [Accessories].
/	Select one option from two or more options that are separated by "/". For example "Addition/Deduction" means addition or deduction.

~	It means a range. For example, "1~255" means the range from 1 to 255.

2. Symbol conventions

Symbol	Explanation
Caution	The matters need attention during the operation and configuration, and they are supplement to the operation description.
Note	Necessary explanations to the operation description.
Warning	The matters call for special attention. Incorrect operation might cause data loss or damage to devices.

Product Documents

The documents of Ruby3A series industrial Ethernet switches include:

Name of Document	Content Introduction
Ruby3A Industrial Ethernet Switches Hardware Installation Manual	Describes the hardware structure, hardware specifications, mounting and dismounting methods.
Ruby3A Series PRP / HSR Switches Web Operation Manual	Describes the switch software functions, Web configuration methods, and steps of all functions.

Document Obtainment

Product documents can be obtained by:

- CD shipped with the device
- Kyland website: www.kyland.com

1 Product Introduction

1.1 Overview

Ruby3A Series PRP/HSR switches are specially designed to meet high reliability industrial networks, implementing PRP (parallel redundancy protocol) and HSR(high availability seamless redundancy) protocols that meet IEC62439-3 standards. Ruby3A can achieve zero packet loss in case of network failure, providing maximum network reliability. The full FPGA hardware solution enables Ruby3A to implement HSR and PRP software configurable on the same hardware with very low network latency. Ruby3A support IEEE 1588v2, the high-accuracy clock synchronization can be achieved through the HSR/PRP network.

1.2 Software Features

This series of switches has rich software features and can meet the different requirments of customers.

Table 1 Software Features

Item	description
HSR/PRP	Support PRP，Failure recovery time 0ms Support HSR，Failure recovery time 0ms Support PRP/HSR Coupling
IEEE1588v2	Support PTPv2（IEEE1588-2008）TC mode, Accuracy less than 1us
VLAN & Port	Port speed (1000M/100M/10M/auto) Port duplex (full/half) 802.1Q (1~4093) Port Based VLAN
MAC Address	Auto Learning & VLAN aware configurable Up to 2K MAC-Address table Dynamic MAC-Address auto-aging & aging timer configurable;

Clock synchronization protocol	SNTP/NTP
network security	Centralized user management SSH、SSL
LLDP	Support LLDP Neighbor learning, neighbor information, message statistics view
IEC61850 MMS Server	Support IEC61850 MMS Server
Management	dhcp-client ftp client/ftp server/sftp client ping Console Managementtelnet client/telnet server WEB Management Centralized management SNMP（v1,v2c,v3） CPU running Power alarm Port alarm (LinkDown) reboot device (reboot) factory configuration recovery (set default) Display total device running time

1.3 Applicable Products

Ruby3A-3G-HV

Ruby3A-3G-L2-L2

SM6.6-HSR/PRP-GE-0.5U

SM6.6-HSR/PRP-GX-0.5U

2 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.

2.1 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 2 View Types

View Prompt	**View Type**	**View Function**	**Command for View Switching**
Switch >	General mode	➢ View system date and time. ➢ Show software version.	Input "**enable**" to enter the privileged mode.
Switch#	Privileged mode	➢ Configure system clock and date. ➢ Transmit file and update software. ➢ Delete switch file. ➢ Configure CLI language. ➢ View switch configuration and system information. ➢ Restore default configuration. ➢ Save current configuration.	➢ Input "**config**" to switch from privileged mode to configuration mode. ➢ Input "**exit**" to return to the general mode.

		➢ Reboot switch.	
Switch (config) #	Configuration mode	Configure all switch functions.	Input "**exit**" to return to 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; <H.H.H.H> means an IP address; <H: H: H: H: H: H> means a MAC address; word<1, 31> means a string range. In addition, ↑ and ↓ can be used to scroll through recently used commands.

2.2 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 9-pin serial port of a PC to the console port of the switch with the DB9-RJ45 console cable.

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

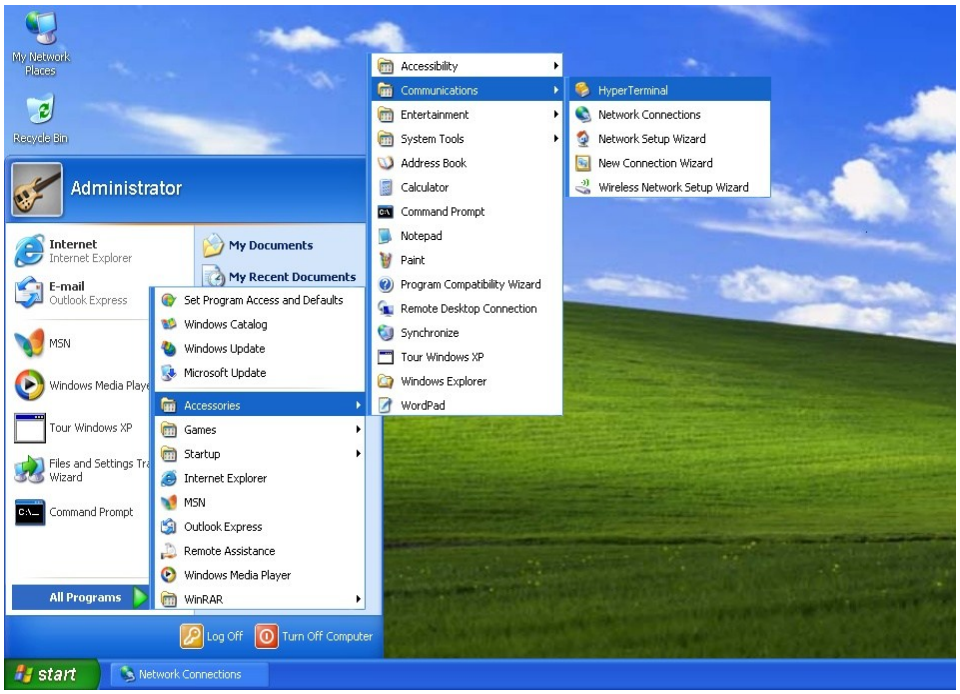


Figure 1 Starting the Hyper Terminal

3. Create a new connection "Switch", as shown below.

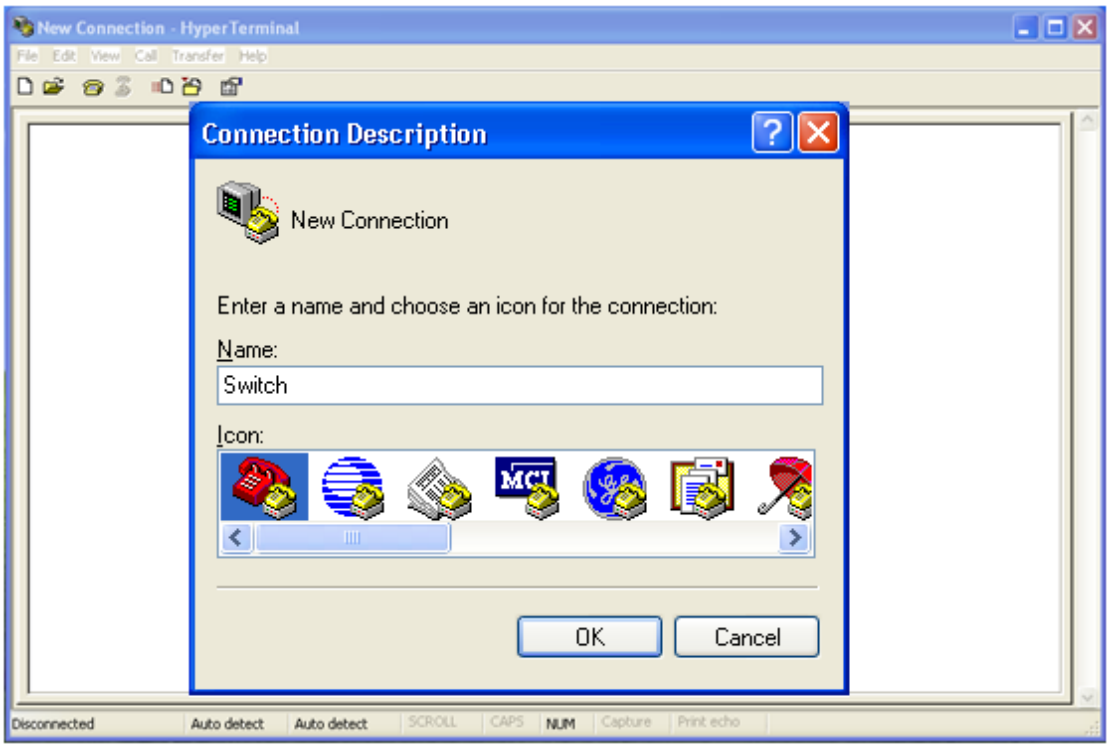


Figure 2 Creating a New Connection

4. Connect the communication port in use, as shown below.

Figure 3 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 below.

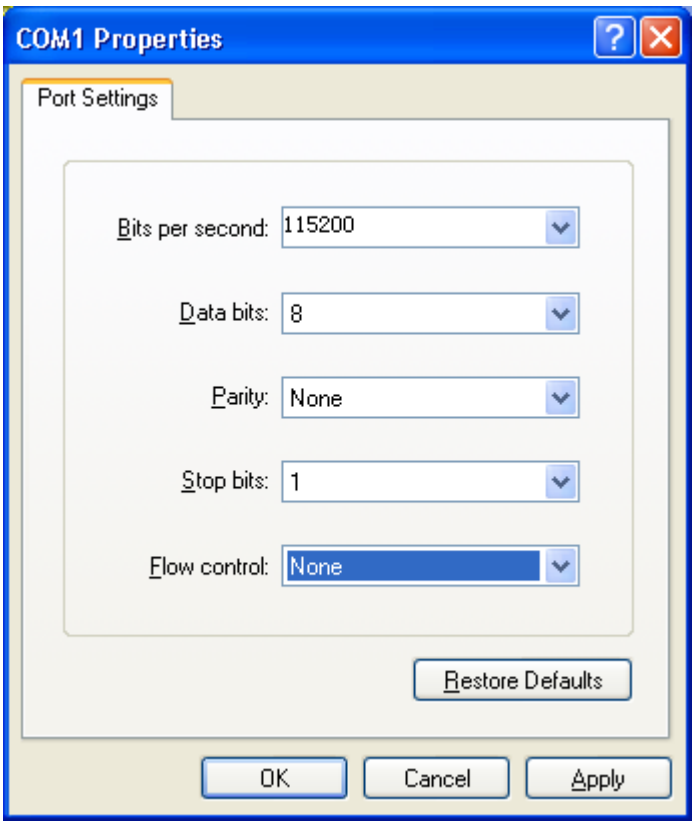


Figure 4 Setting Port Parameters

6. Click <OK> button to enter the switch CLI. Input password "admin" and press <Enter> to enter the General mode, as shown below.

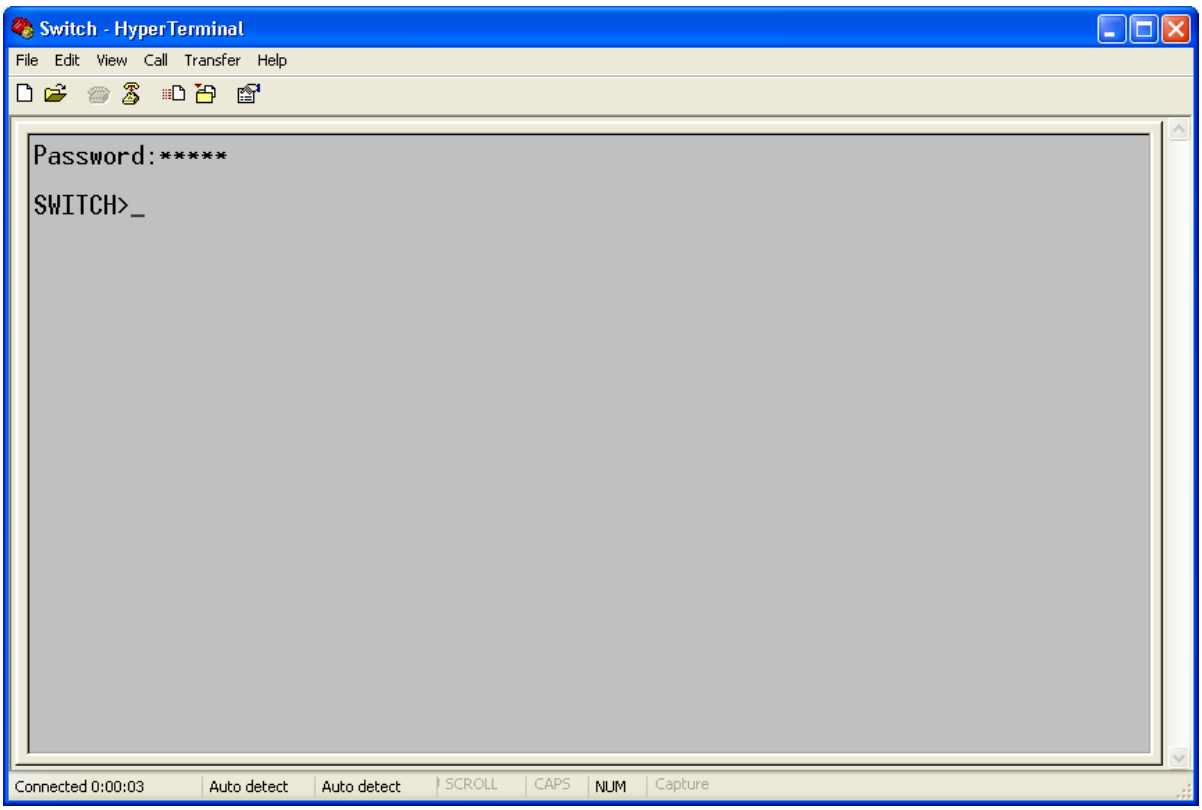


Figure 5 CLI

7. Input command “enable”, default user "123”, and password”123” to enter the privileged mode. You can also input other created users and password, as shown below.

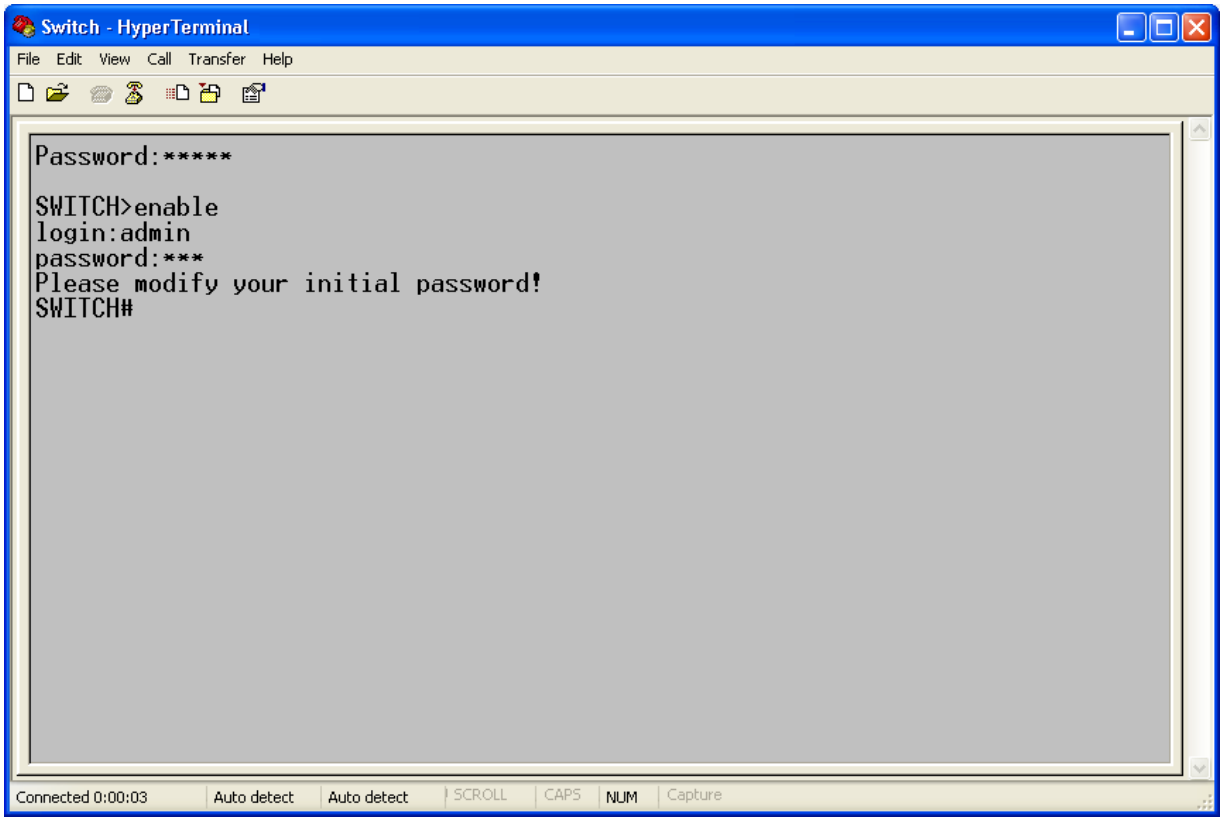


Figure 6 Privileged mode

2.3 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 below. The default IP address of a Kyland switch is 192.168.0.2.

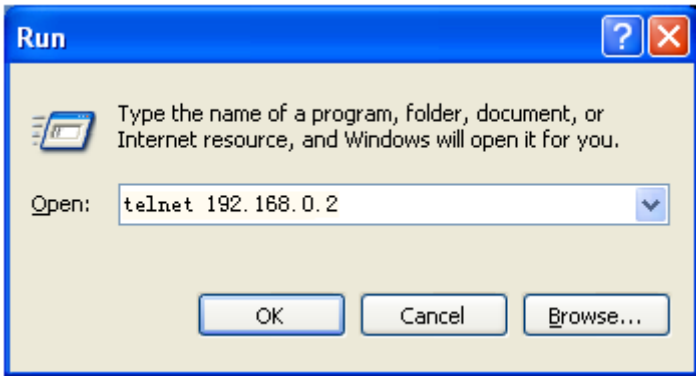


Figure 7 Telnet Access

Note:

To confirm the switch IP address, please refer to "4.2 IP Configuration" to learn how to obtain IP address.

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

```
Password: *****
SWITCH> en
Password: *****
SWITCH#
```

Figure 8 Telnet Interface

2.4 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 below. Input the default user name "admin", password "123", and the Verification. Click <Login>. You can also input other created users and password.

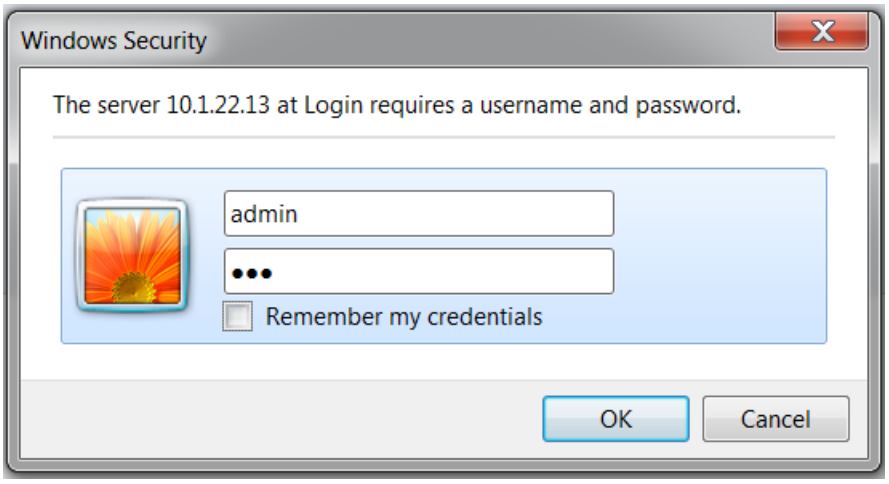


Figure 9 Web Login

The English login interface is displayed by default.

Note：

To confirm the switch IP address, please refer to "4.2 IP Configuration" to learn how to obtain IP address.

2. Successful login to switch web management page, the top area is the configuration navigation tree, the configuration mode can be switched in the left area, the Green is basic mode, the Red is advanced mode, advanced mode has higher permissions than basic mode, users can configure more device modules, as shown below.

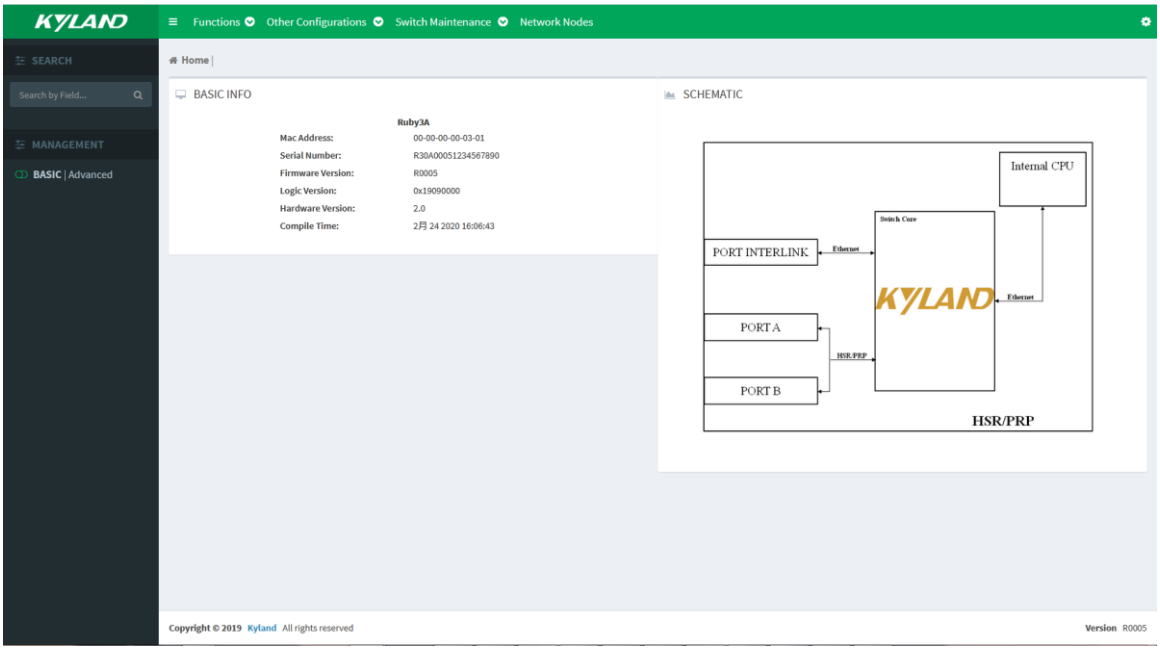


Figure 10 Web interface

Click the icon of top left corner KYLAND, can be linked to the Web interface shown in Figure 10, click the icon in any case to switch to the web interface; Click the icon like gear wheel of top right corner , and select Logout to exit Web login interface, it also can configure the other function of switch.

3 Device information

3.1 Switch basic information

1. BASIC INFO

BASIC INFO mainly contains the basic configuration information of the Ruby3A device, including mac address, serial number, firmware version, logic version, hardware version, compile time, as shown below.

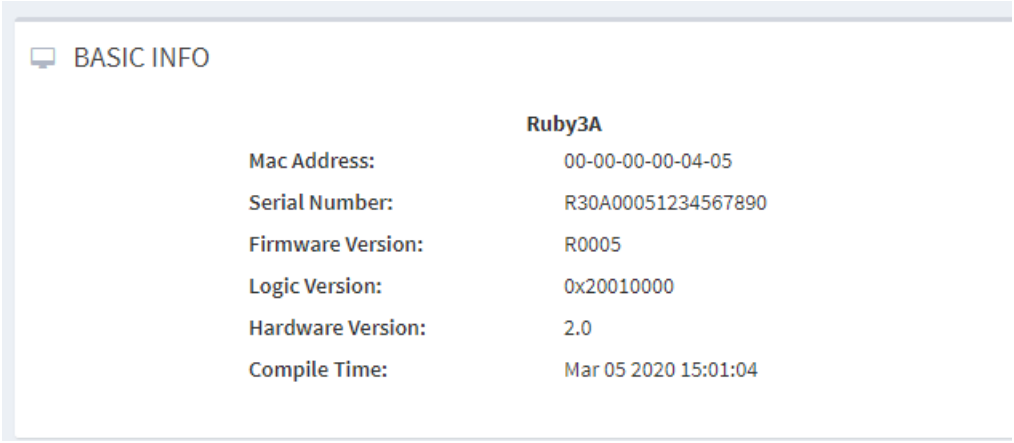


Figure 11 Switch basic information

2. SCHEMATIC

Switch schematic, as shown below.

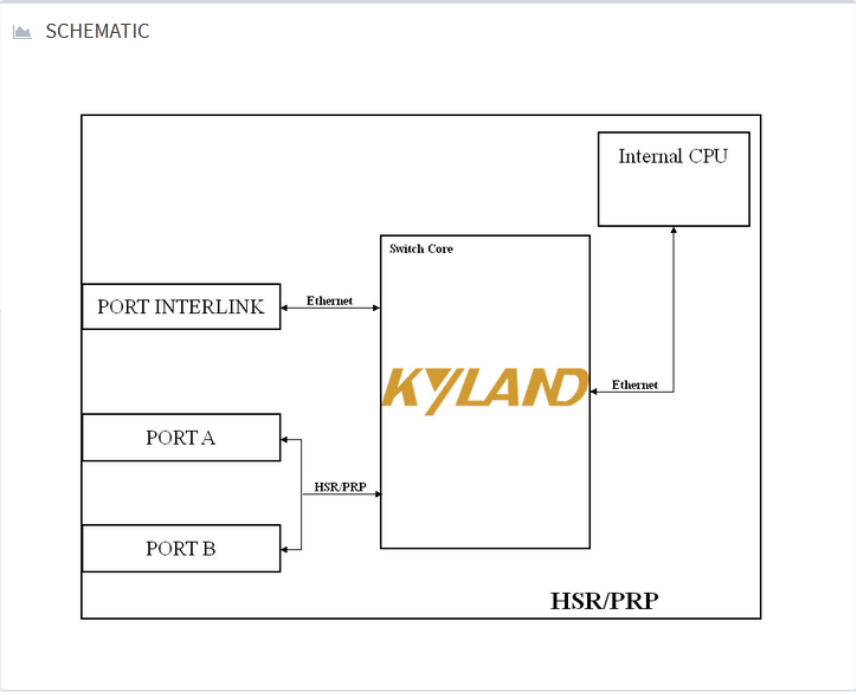


Figure 12 Switch schematic

4 Switch Basic Configration

Click the gear wheel iron in the top right corner of the main interface to configure the basic information of user, there are two modes, basic and advanced, which have different basic configuration options, advanced mode has higher permissions and more configurable items. Configurable item of switch in advanced and basic modes, as shown below.

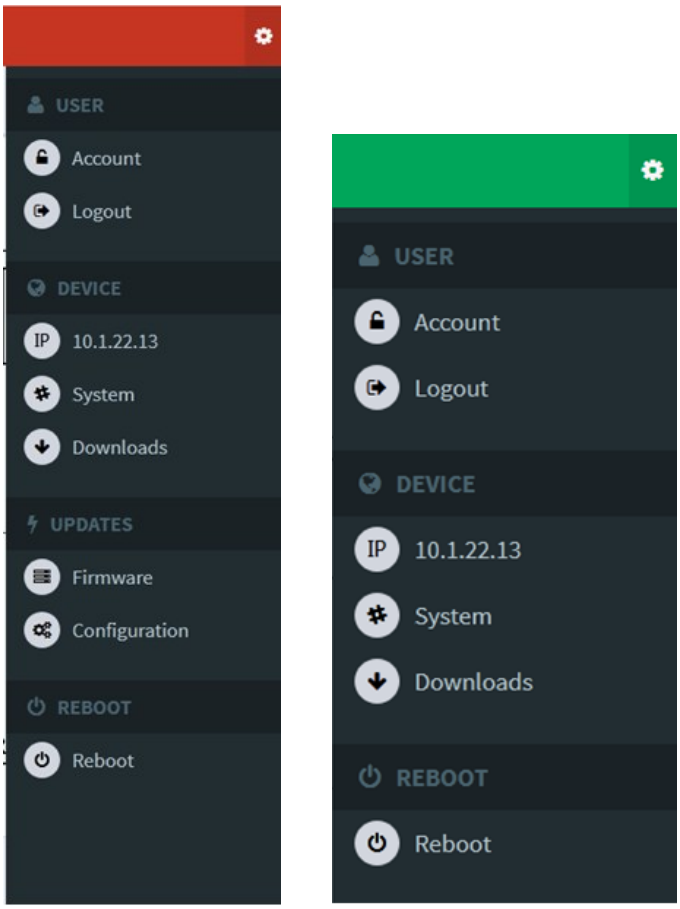


Figure 13 advanced and basic modes

4.1 User Configuration

The Accout under the User option is to modify the user's password; Logout is the option to exit the web login page.

4.2 IP Configuration

1. Show the IP address of the switch through the Console port

Login to the command line interface though the Console port, in privileged user

configuration mode input command "show interface ip brief", the IP address of switch can be shown, as shown below.

```
SWITCH# show interface ip brief
Interface            Kname        IP-mode      Ipaddress          Mask               Gateway
-------------------------------------------------------------------------------------------
port_interlink       eth1         Static       10.1.22.13         255.0.0.0          0.0.0.0
mgmt                 eth0         Static       192.168.10.2       255.255.255.0      --

SWITCH#
```

Figure 14 Show IP address

2. Click the gear wheel iron in the top right corner of the main web page, select the IP under the [DEVICE], enter into the IP configuration page, the IP address of L port and M port also can be shown, as shown below.

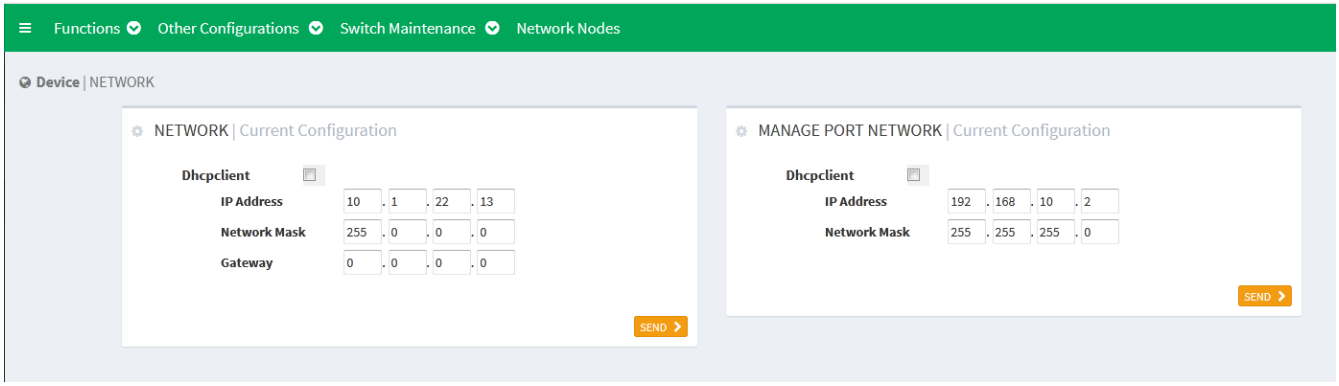


Figure 15 Ruby3a IP configuration page

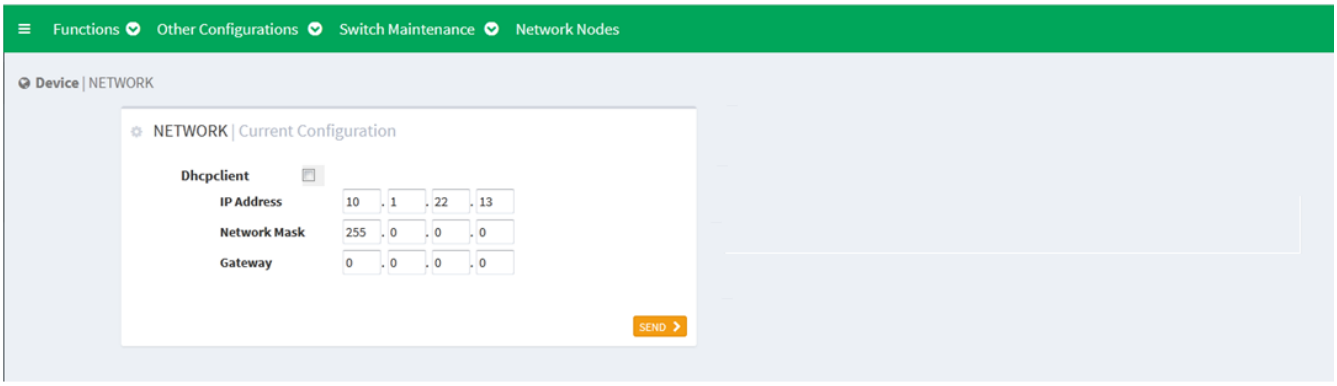


Figure 16 HSR/PRP sub-card IP configuration page

NETWORK

Function: Configure the IP address of L port.

MANAGE PORT NETWORK

Function description：Configure IP address of management port.

On the this configraiton page, the left area is to configrate IP of L port, the right area is to configurate IP of M port.

It supports dynamic IP and static IP configuration.

Caution:

Ruby3a has independent management port, SM6.6-HSR/PRP sub-card has no independent management port.

4.2.1 DHCP Configration

4.2.1.1 DHCP Introduction

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 below figure.

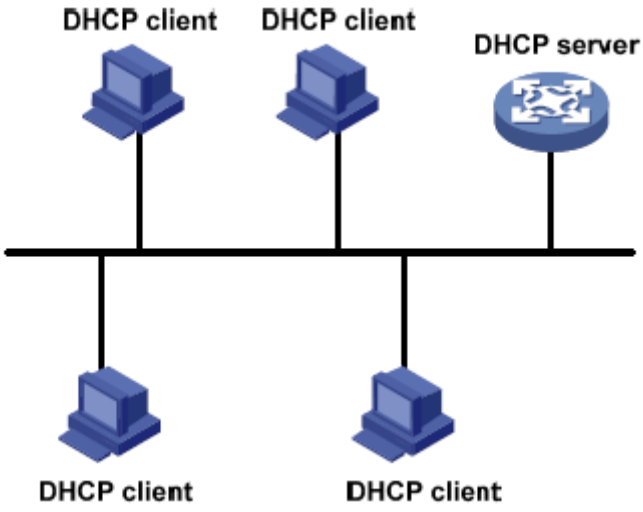


Figure 17 DHCP Typical Application

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.

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.

4.2.1.2 DHCP Configration

Caution:

Current device do not support to configurate DHCP Server, only support DHCP Client。

The below figure shows the IP configuration page of L port:

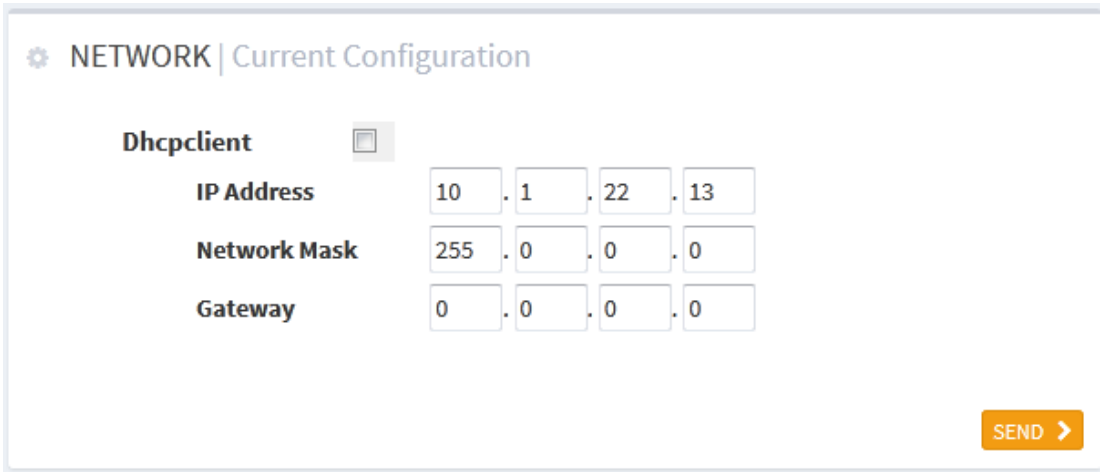


Figure 18 IP configuration of L port

When the port Dhcpclient is checked，dhcp client is enabled, client can apply for IP address to remote server. When the dhcpclient is enabled, the other configuration items in the page are set to unselected state. By refreshing the page, we can see the IP address is obtained successfully by the DHCP. If obtaining the IP address fails, the previous IP address can be used as the current address. Mask and Gateway are same, recovery the last configuration value.

4.2.2 Static IP Configuration

L port IP configuration as shown in Figure 18, configure IP address by configuring manually IP and mask.

IP Address

Configuration format: A.B.C.D

Function: configure manually IP address

Network Mask

Configuration format: A.B.C.D

Function: The subnet mask can be converted to a number of 32 bits in length, consisting of a continuous string of "1" and "0". "1" corresponds to the network number field and the subnet number field, and "0" corresponds to the host number field. Mask length refers to the number of 1 in the mask.

Caution:

- The current switch only supports IP configuration of L port and M port, each IP interface corresponds to a IP address;
- Different IP interface should be configurted to IP address with different network segments

Gateway

Configuration format: A.B.C.D

Function: Configure manually gateway address.

Gateway address must be in the same network segment as IP address, otherwise

configuration fails.

4.3 System Information

Click the gear wheel iron in the top right corner of the main web page, select [SYSTEM] under the [DEVICE], enter into the system information page, as shown below;

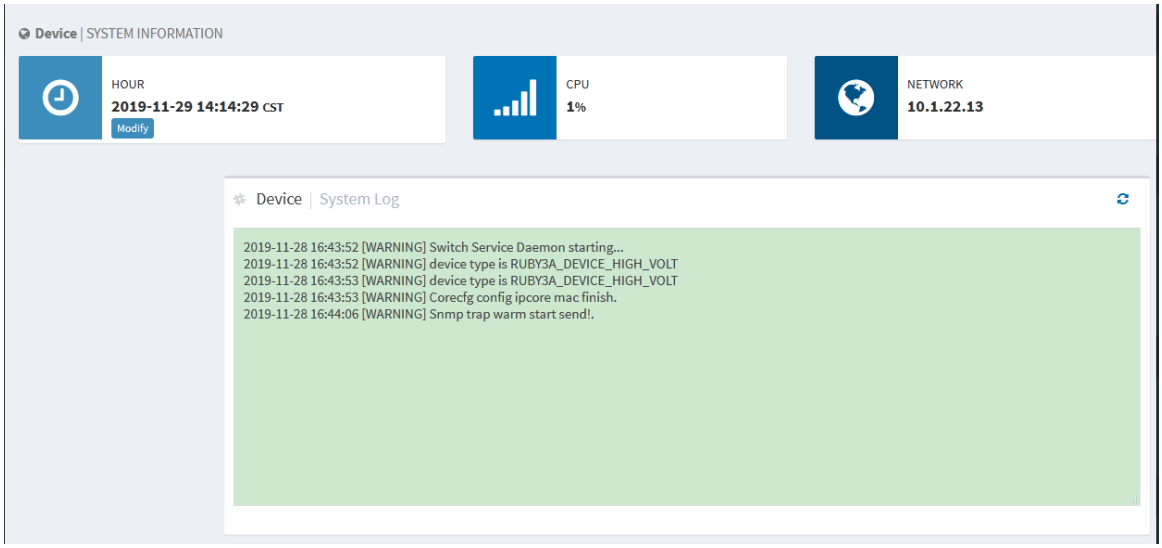


Figure 19 System information page

This page is mainly for system information viewing and configuration of switch, including time configuration, CPU, network and log.

4.3.1 Clock Configuration

To configurate system date and time, click the gear wheel iron in the top right corner of the main web page, select [SYSTEM] menu and enter into the clock configuration page, as shown below;

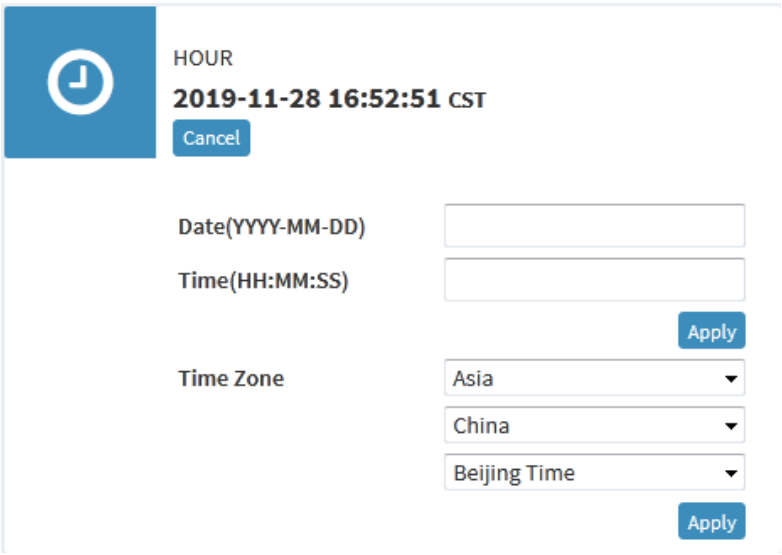


Figure 20 Clock configuration

The current time can be viewed and the time can be configurted manually in this page.

Date (YYYY.MM.DD)

Configuration range: YYYY(year) with range1970~2099，MM(month) with range 1~12，DD(date) with range 1~31.

Time (HH:MM: SS)

Configuration range: HH(hour) with range 0~23，MM(minute) and SS(second) with range 0~59.

Time Zone

Zone configuration, select the corresponding continent, country and city

4.3.2 CPU Status

CPU status shows the current CPU average utilization, as shown below;

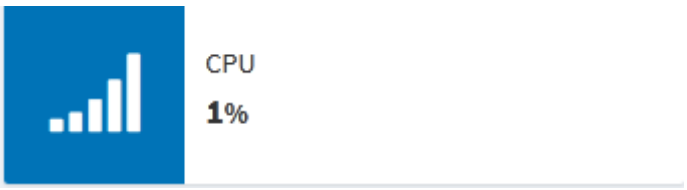


Figure 21 CPU status

4.3.3 NETWORK Status

Shows the IP address of the login web interface, indicates that the interface is being used,

as shown below;

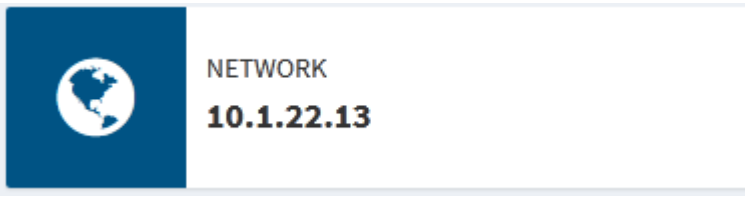


Figure 22 NETWORK Status

4.3.4 System Log

The log function of the switch mainly records the status change, fault, debugging, exception, user operation and other information of the switch system, which is convenient to find out the fault. the log information can be uploaded to the server supporting the syslog protocol in real time by configuration.

The messages in the log include: various alarm information, broadcast storm, restart, memory and user operation information. Log information is shown below;

Figure 23 Log Information

Click the refresh button in the top right corner to refresh the log information manually.

4.4 File Download

Click the gear wheel iron in the top right corner of the main web page, select [downloads] under [DEVICE], enter into file download page. As shown in below figure, the MIB and Startup-config file can be downloaded, startup-config file is switch startup file that contains saved configuration of switch.

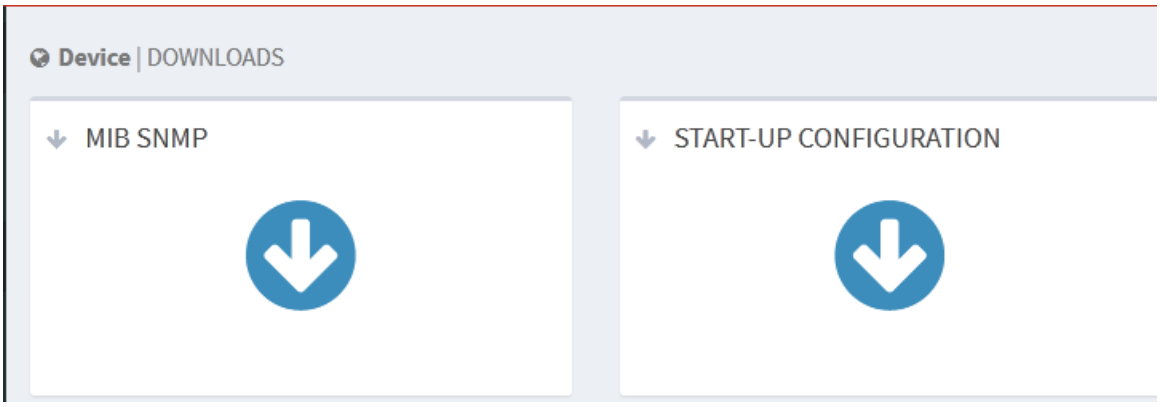
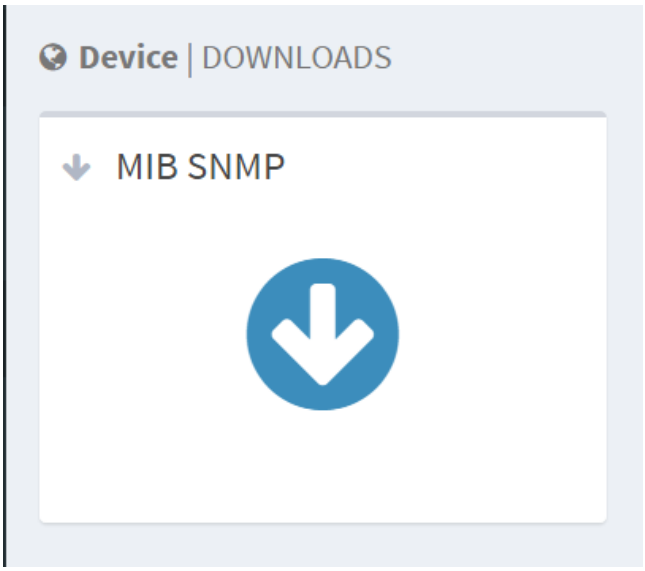


Figure 24 File download

4.4.1 Mib File Download

Click the botton in MIB SNMP, pop up the below window, click OK to download the SWITCH-DESING-MIB.mib file to the specified path. As shown below;



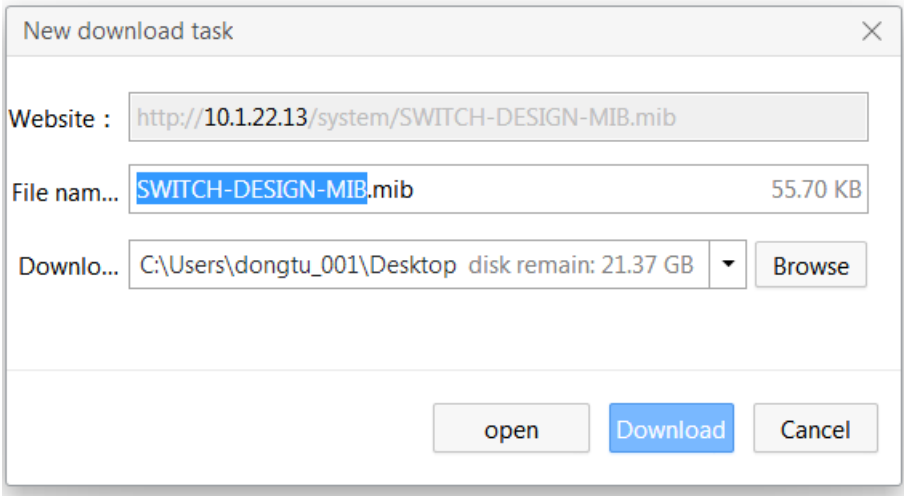
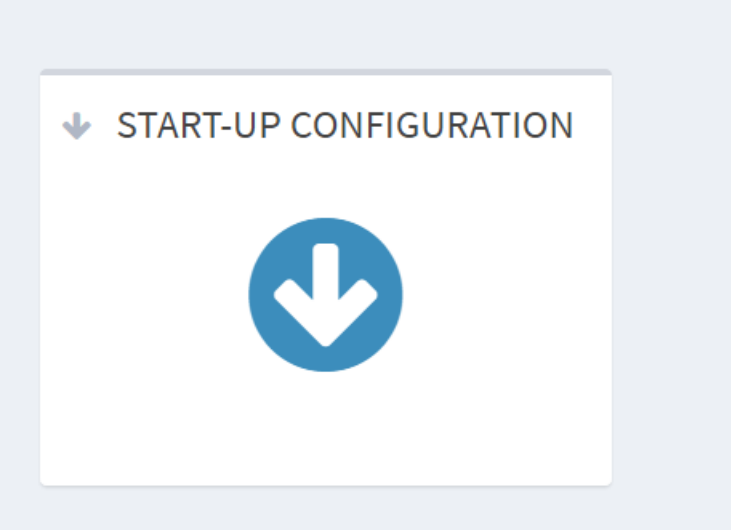


Figure 25 mib file download page

4.4.2 Configuration File Download

Click button in the START-UP CONFIGURATION, pop up the below window, click OK to download the startup_config.conf file to the specified path. As shown in below figure;



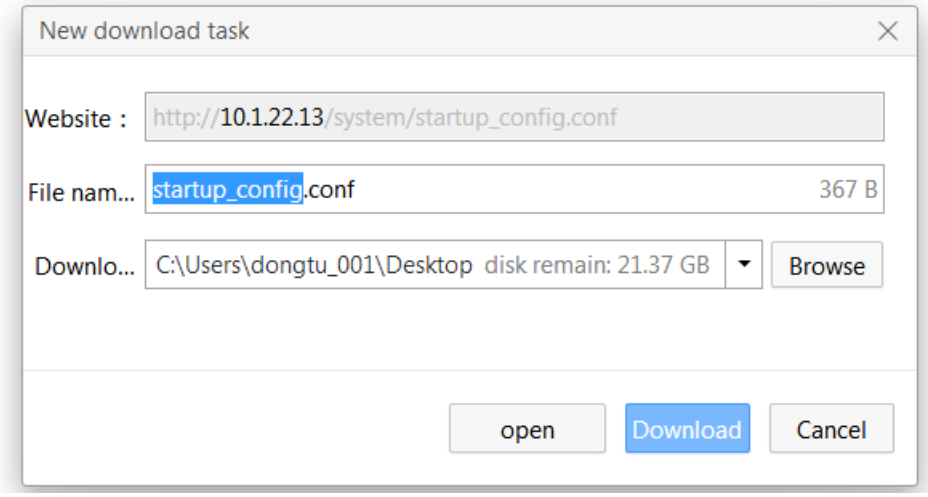


Figure 26 Configuration File Dwonload page

4.5 Firmware Upgrade

By upgrading the firmware to improve the performance of switch, it supports FTP/SFTP server upgrade and local upgrade.

4.5.1 Local Upgrade

Click the gear wheel iron in the top right corner of the main web page, select [**Firmware**] and enter into device upgrade page, as shown in below figure;

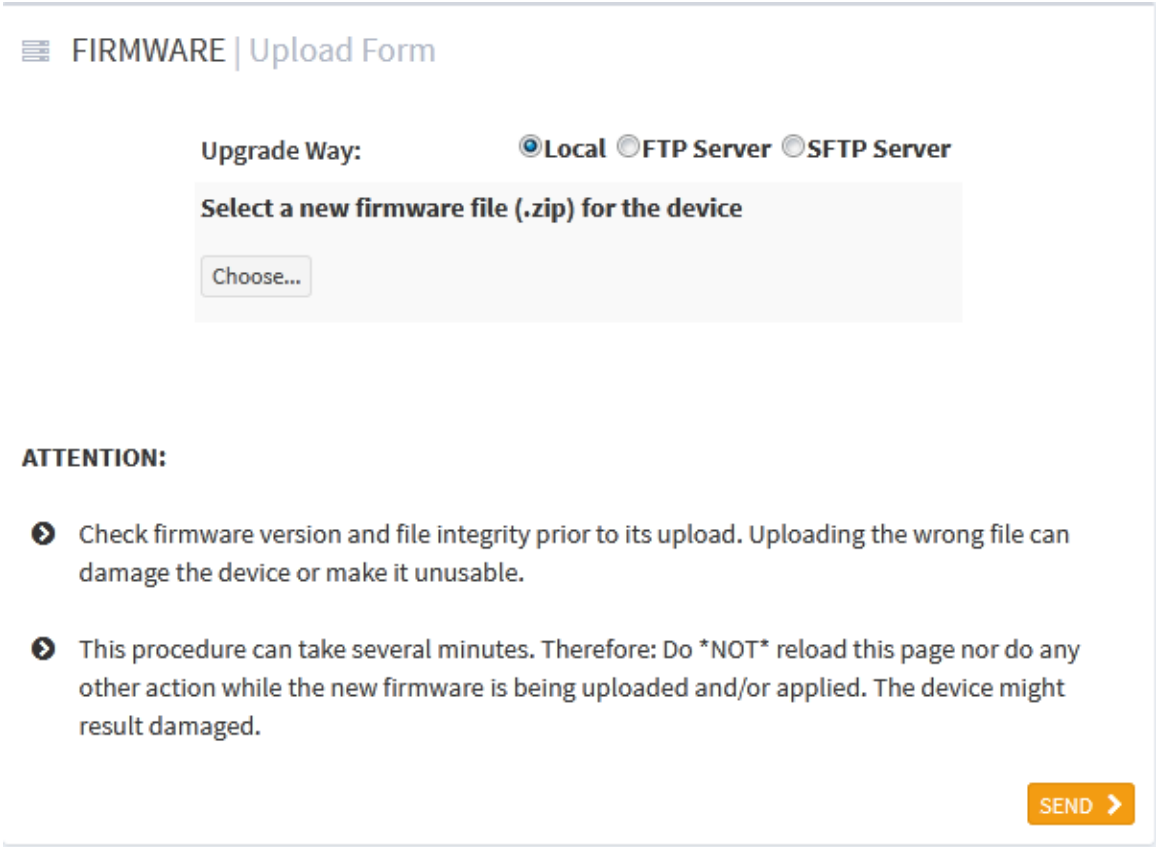


Figure 27 Local upgrade page

Upgrade Way

Configuration options: Local/FTP server/SFTP server

Local

Click Choose botton to select correct upgrading file, then click [SEND] botton to upgrade.

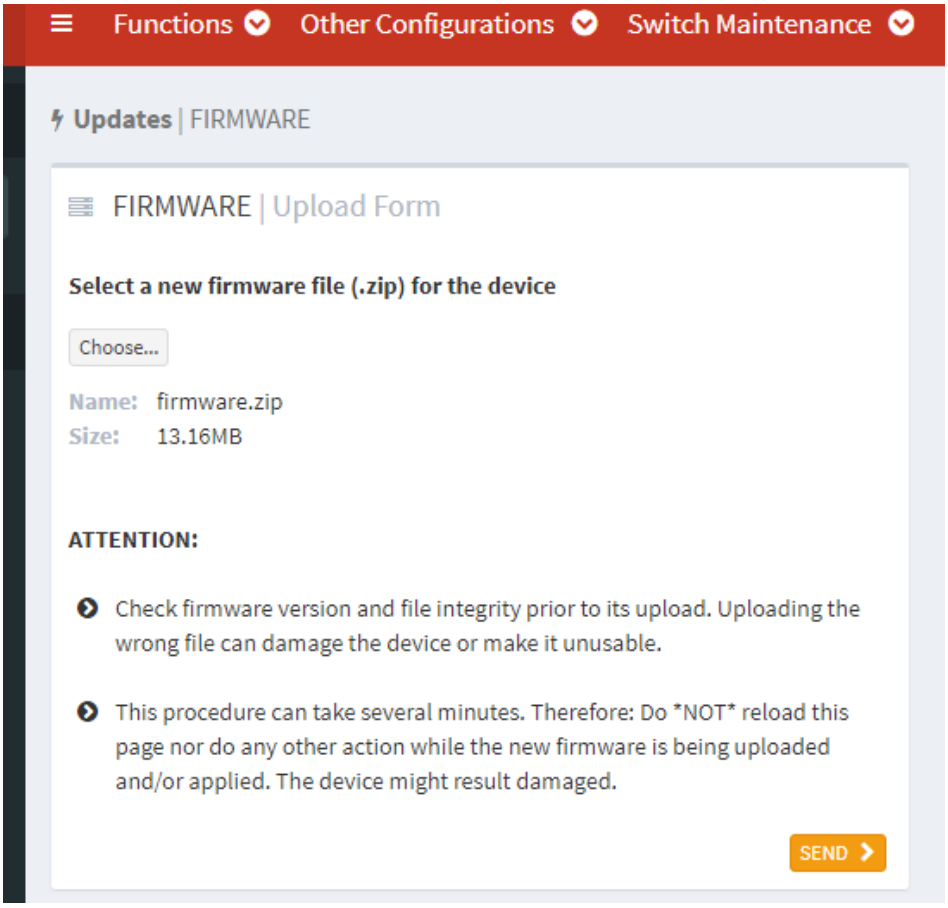


Figure 28 Local upgrade/select upgrade file

After selecting, click <**send**> button to start upgrading, the waiting page as shown in below figure;

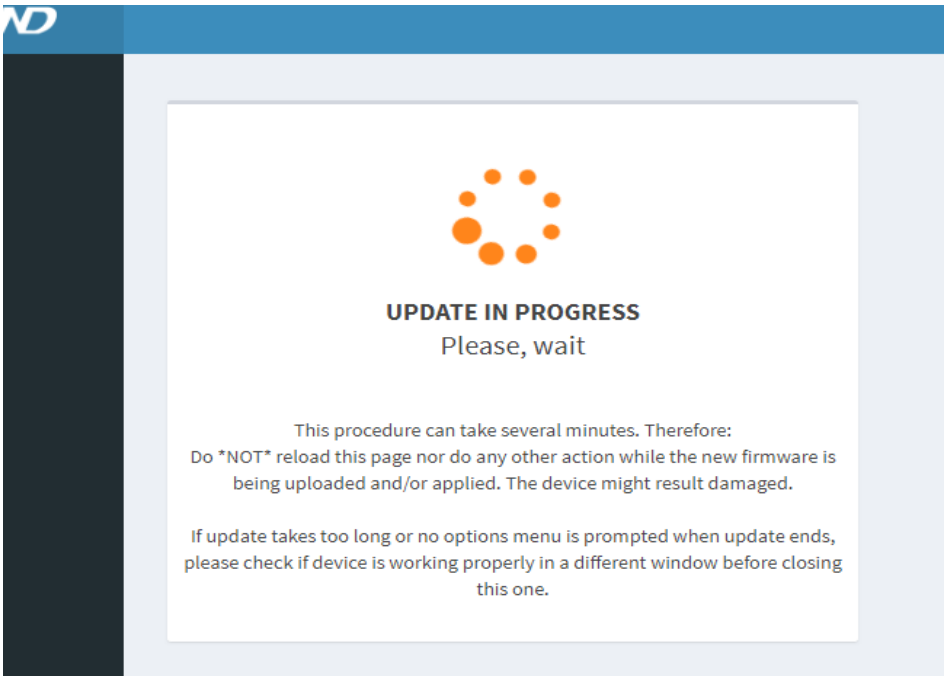


Figure 29 Local upgrade/firmware upgrading

Attention:

Do not do any other operation, especially shut down the power, it is easy to cause upgrade fail even can't start, the upgrade is successful till the below page appears, as shown in below figure.

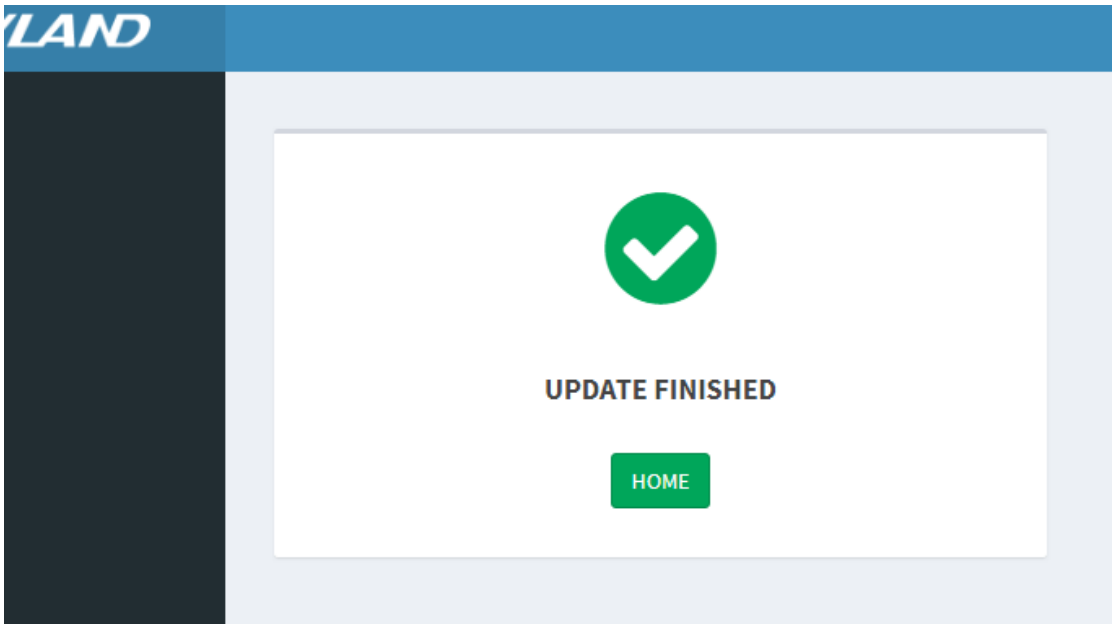


Figure 30 Local upgrade/ Upgrade success

Reboot the device, click the gear wheel iron in the top right corner, select **reboot**.

4.5.2 FTP Upgrade

Install an FTP server. The following uses WFTPD software as an example to introduce FTP server configuration and software update.

1. Click [Security] → [Users/Rights]. The "Users/Rights Security Dialog" dialog box is displayed. Click <New User> to create a new FTP user, as shown in Figure 31. Create a user name and password, for example, user name "admin" and password "123". Click <OK>.

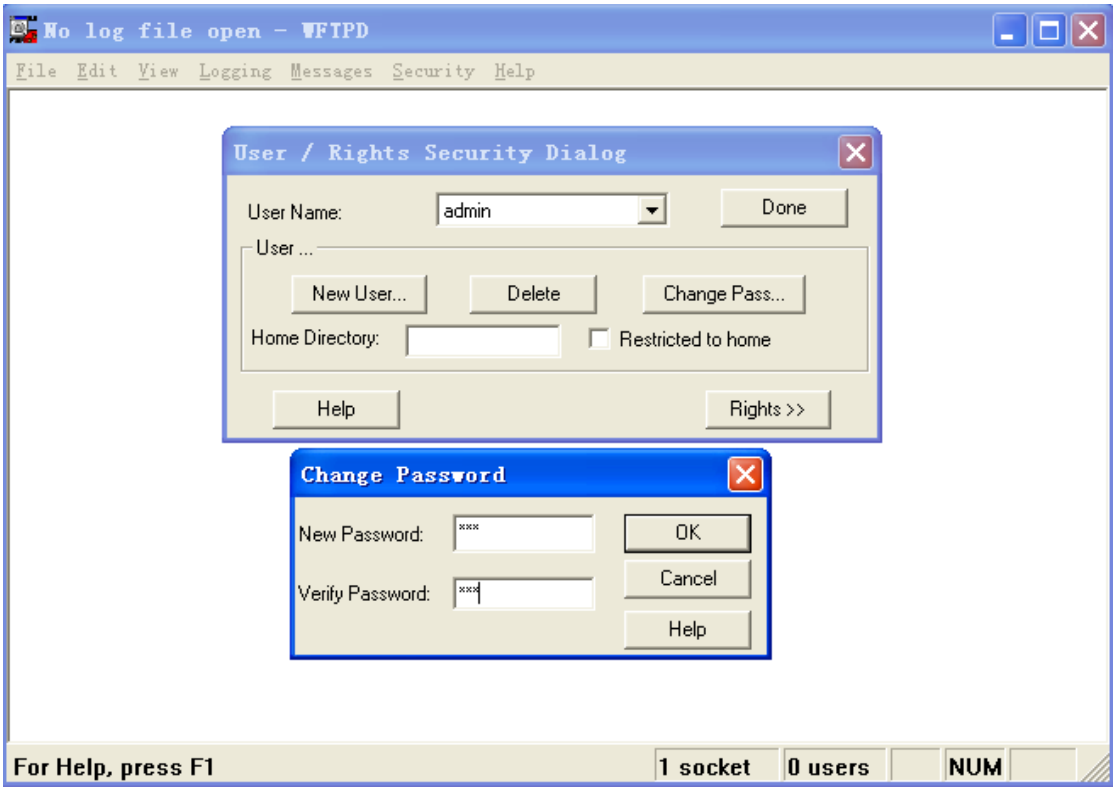


Figure 31 Creating a New FTP User

2. Input the storage path of the update file in "Home Directory", as shown below. Click <Done>.

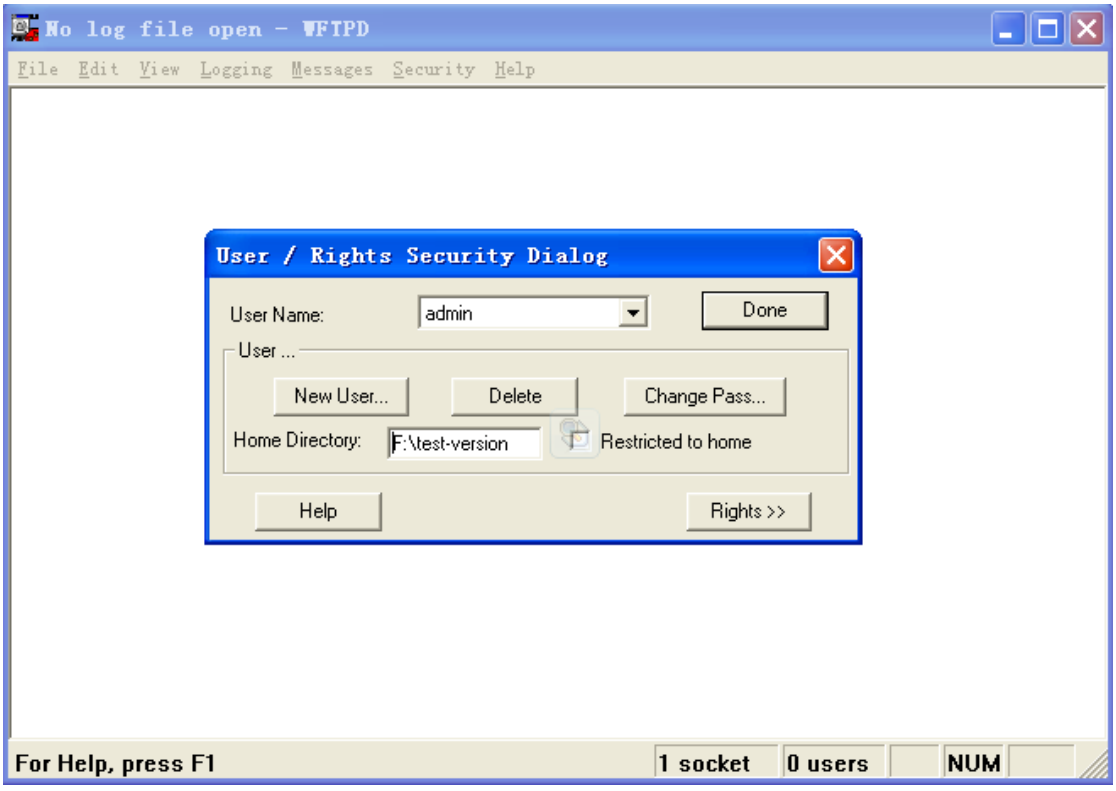


Figure 32 File Location

3. Click the gear wheel iron in the top right corner, select [Firmware] and enter into the devcie upgrade page, then select **FTP server** as shown in below figure, input the IP address of FTP, username, password and filename in the server, click <**SEND**>botton;

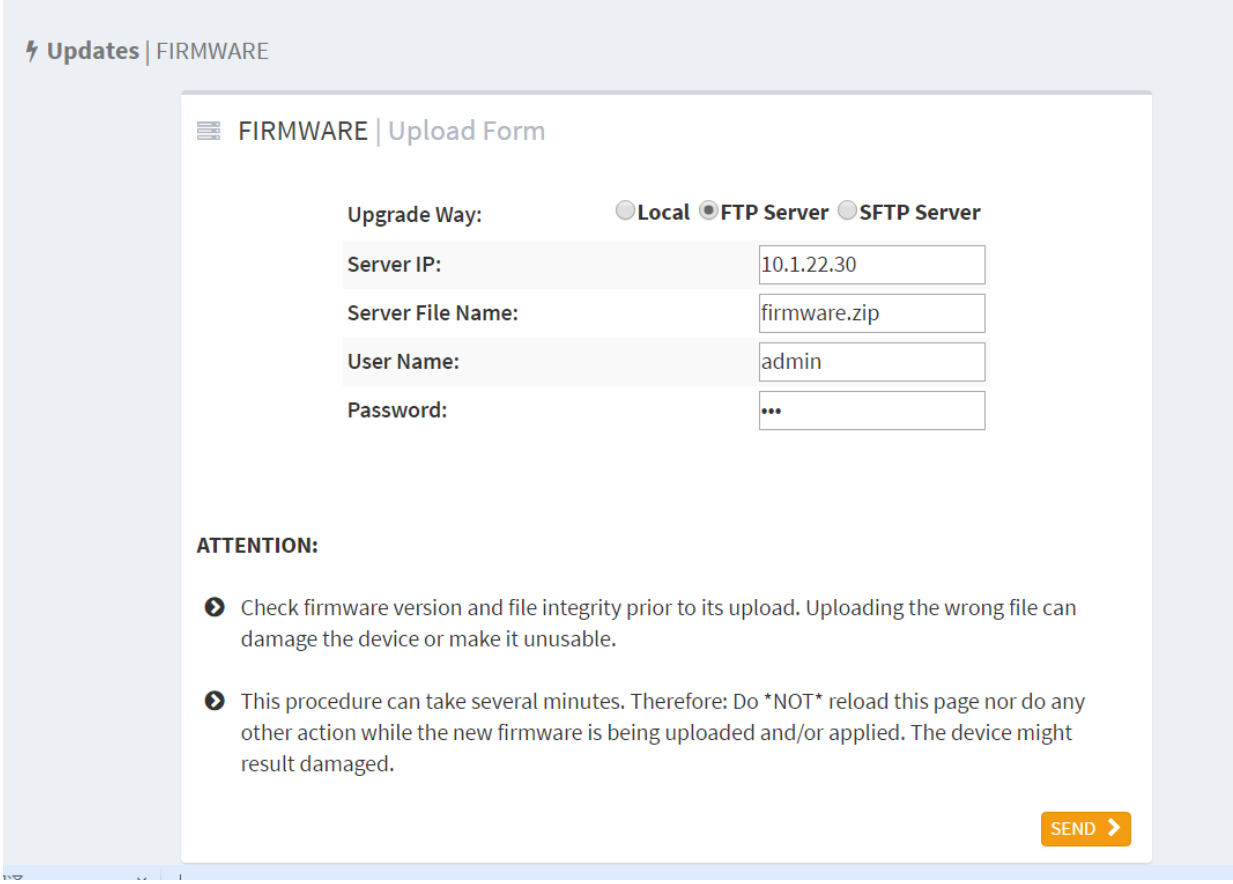


Figure 33 FTP server upgrade

Warning:

- Default upgrade filename is firmware.zip，the filename can be changed but suffix name must be zip, otherwise it cause the upgrade fails.

4. Make sure the normal communication between the FTP server and the switch, as shown in below figure;

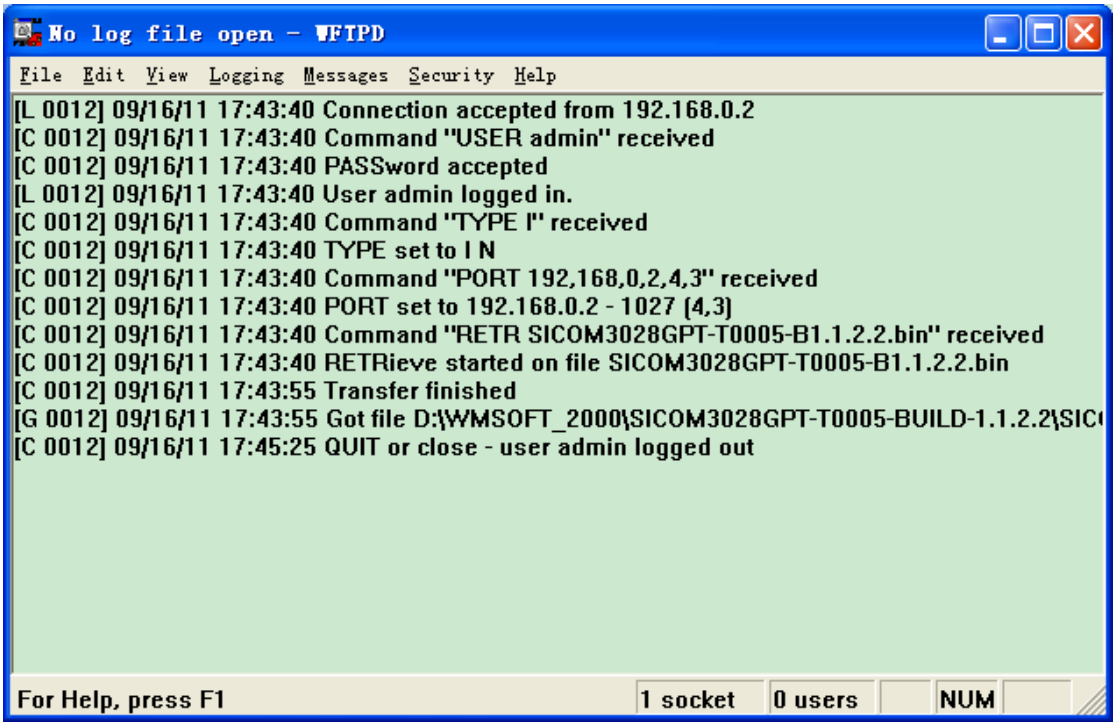


Figure 34 Normal Communication between FTP Server and Switch

Caution：

To display update log information as shown in Figure 34, you need to click [Logging] → [Log Options] in WFTPD and select Enable Logging and the log information to be displayed.

5. Upgrade in progress as shown in below figure;

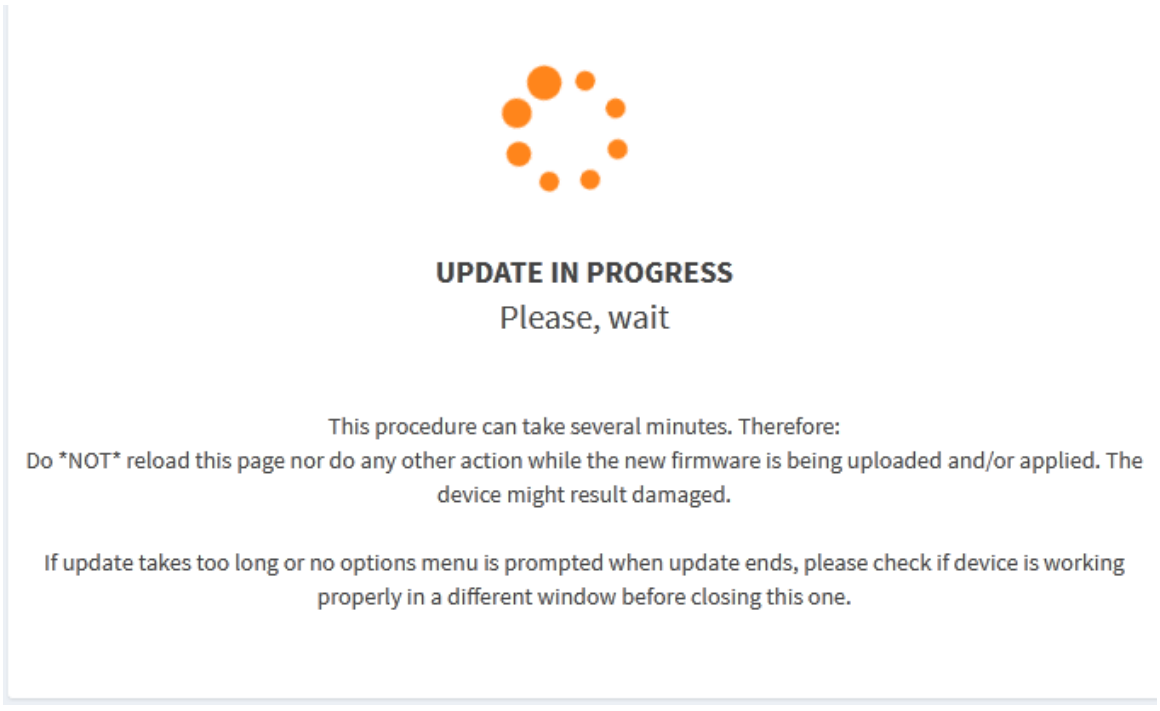


Figure 35 FTP upgrading

6. Update finished as shown in below figure;

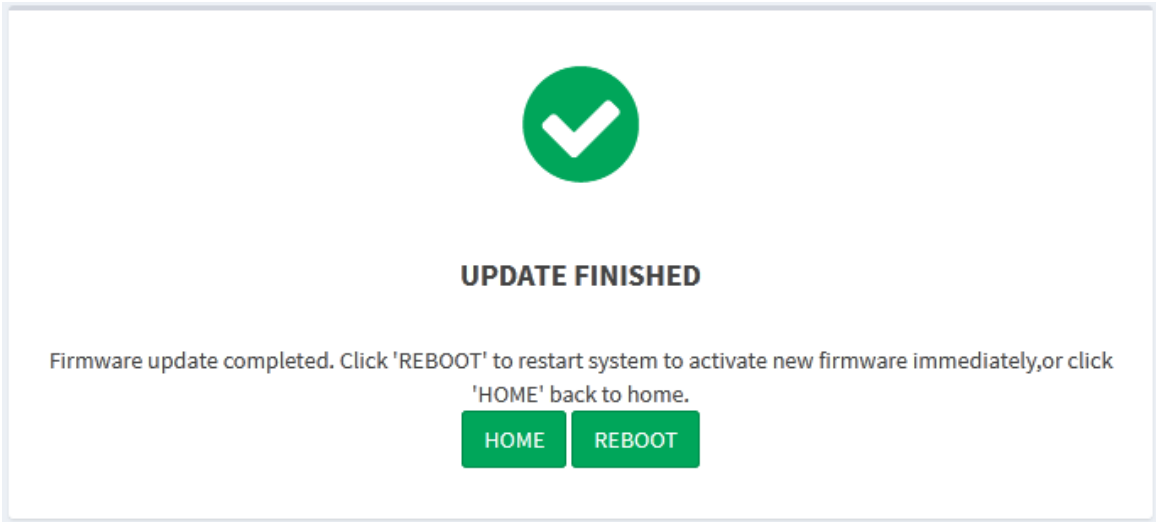


Figure 36 FTP Update finished

After update finished, [HOME] and [REBOOT] can be selected, only when the device restarts, the new version is avild, and check whether the firmware version is the latest.

Warning:

- During firmware upgrade, the FTP server should be kept running.
- After firmware upgrade is successful, it is necessary to restart the switch to make the new firmware work.
- Do not restart the switch if upgrading fails to avoid loss of the file to cause the switch can't start.

4.5.3 SFTP upgrade

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 37. 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.

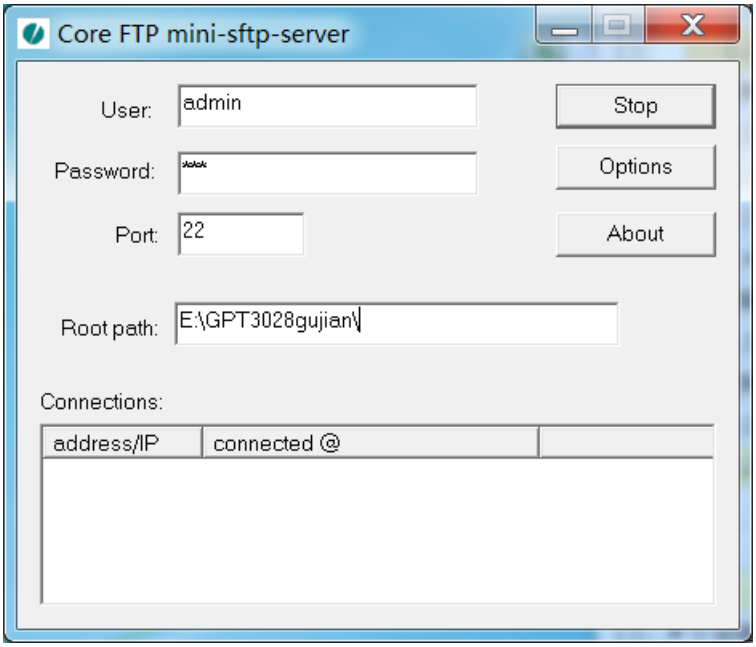


Figure 37 Adding an SFTP User

2. Click the gear wheel iron in the top right corner, select [Firmware] and enter into the devcie upgrade page, then select SFTP server as shown in below figure, input the IP address of SFTP, username, password and filename in the server, click <**SEND**>botton;

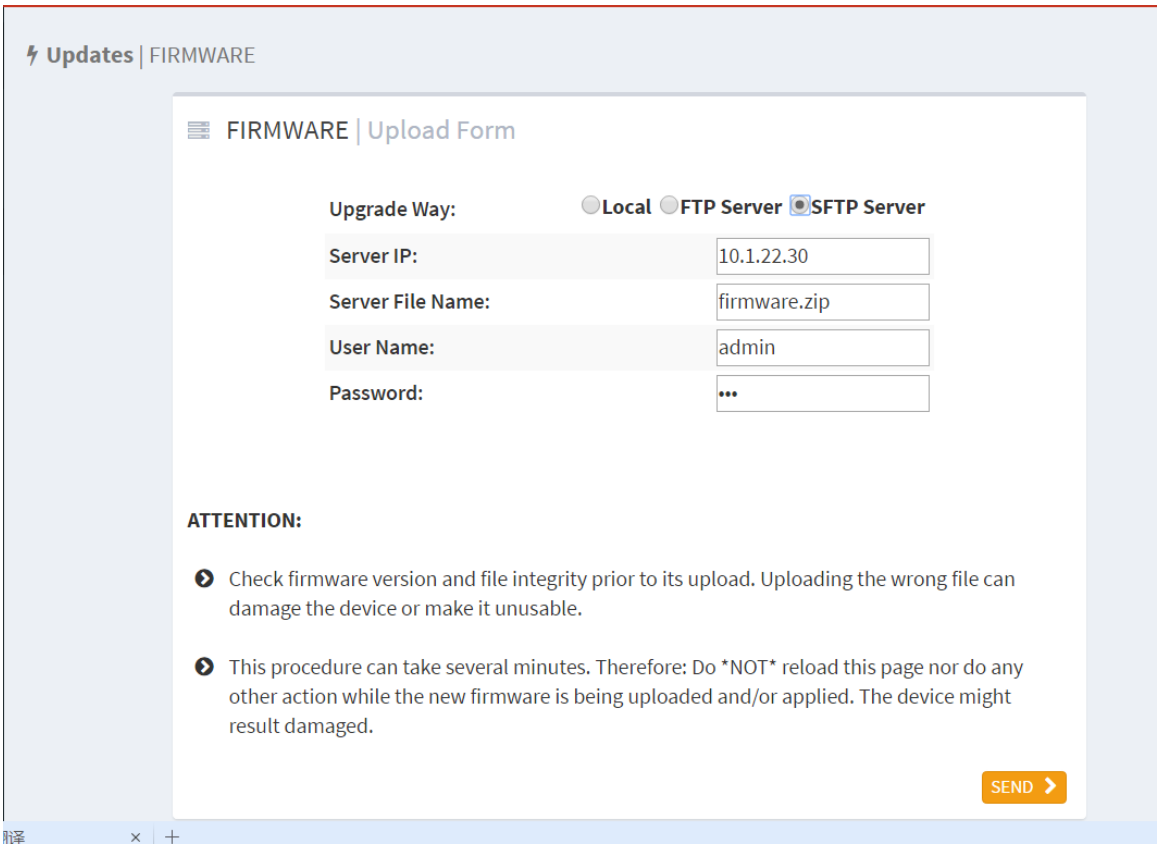


Figure 38 SFTP server upgrade

Warning：

- Default upgrade filename is firmware.zip，the filename can be changed but suffix name must be zip, otherwise it cause the upgrade fails.

3. Upgrade in progress as shown in below figure;

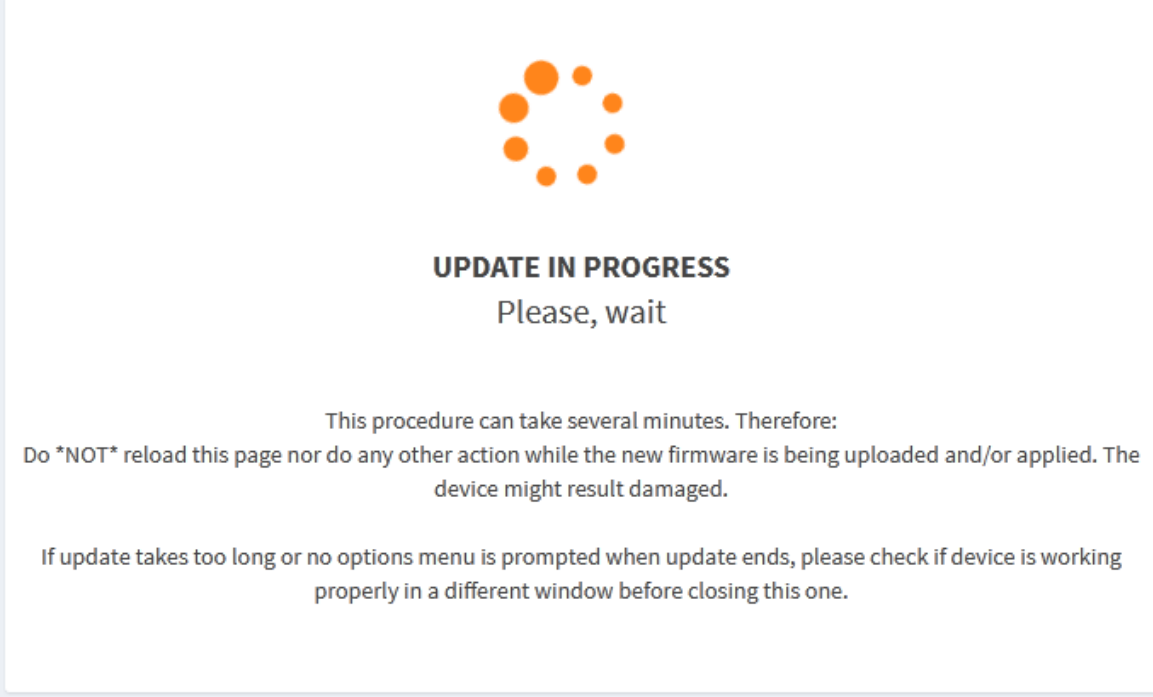


Figure 39 SFTP upgrading

4. Update finished as shown in below figure;

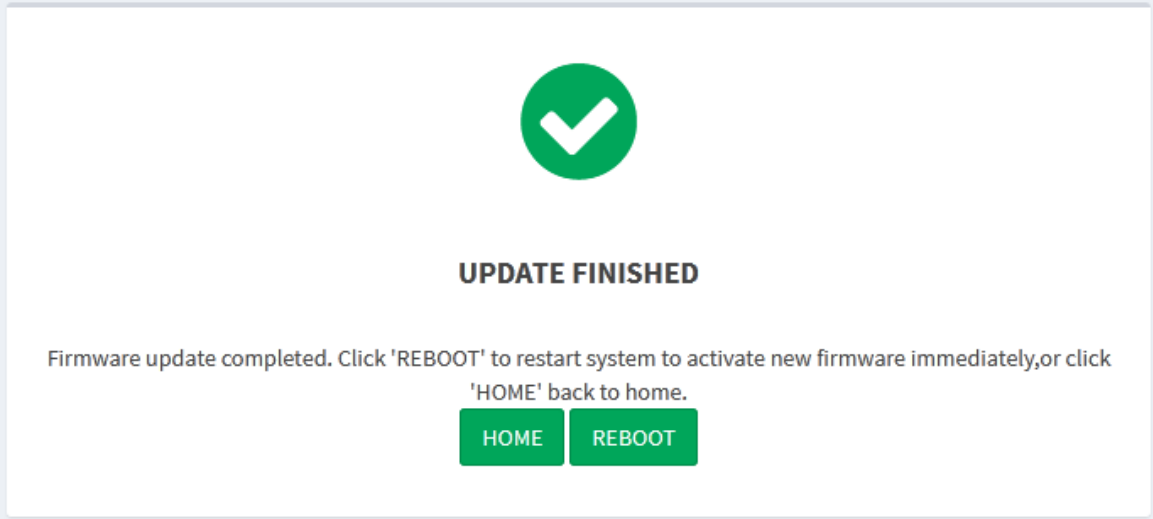


Figure 40 SFTP Update finished

5. After update finished, [HOME] and [REBOOT] can be selected, only when the device

restarts, the new version is avild, and check whether the firmware version is the latest.

Warning:

- During firmware upgrade, the FTP server should be kept running.
- After firmware upgrade is successful, it is necessary to restart the switch to make the new firmware work.
- Do not restart the switch if upgrading fails to avoid loss of the file to cause the switch can't start.

4.6 File Upload

Click the gear wheel iron in the top right corner of web main page, select [Configuration] under the [UPDATES] to upload the local server configuration file to the switch as the switch start file, as shown below;

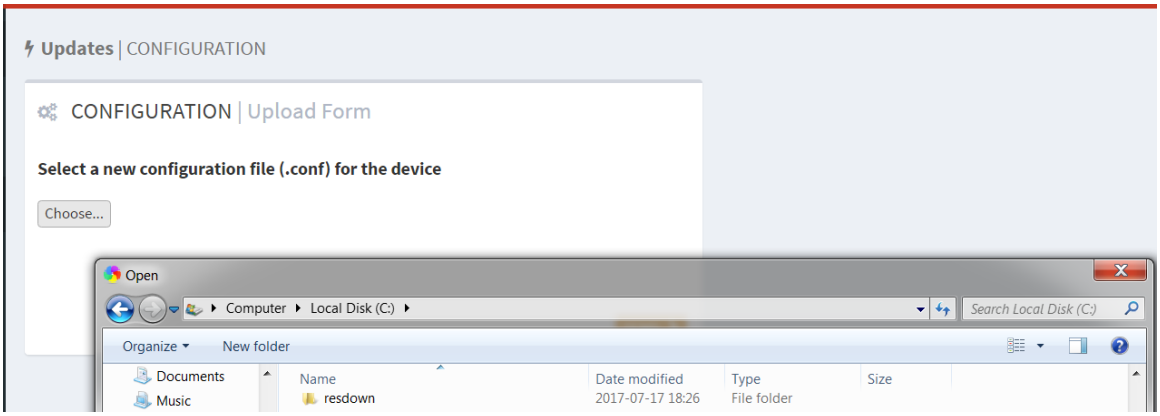


Figure 41 Configuration file upload

The uploaded configuration file is stored in the switch directory as /etc/switch_service, and the device starts with the startup.conf as startup file includeing all the configuration information of the switch.

WARNING:

Uploaded configuration file must be the text file with .conf as suffix.

4.7 Reboot

When the device need to reboot, click the gear wheel iron in the top right corner of web main page, select **reboot**, device will reboot as shown in below figure.

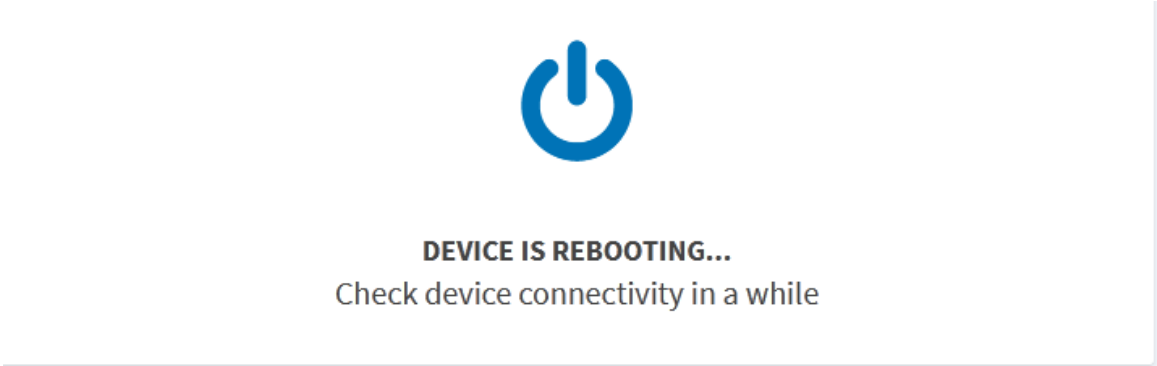


Figure 42 Reboot

5 FUNCTIONS

5.1 Redundancy

5.1.1 Principle

- Paraphrase

SAN: singly attached node;

RedBox: Redundancy box, it is the redundant switch that can connect PRP networks and other networks.

DANH: The doubly attached node with HSR.

DANP: The doubly attached node with PRP.

- PRP

The basic idea of the PRP is to provide redundancy for the system through the network nodes supporting the prp, and its basic working principle is shown in the following figure;

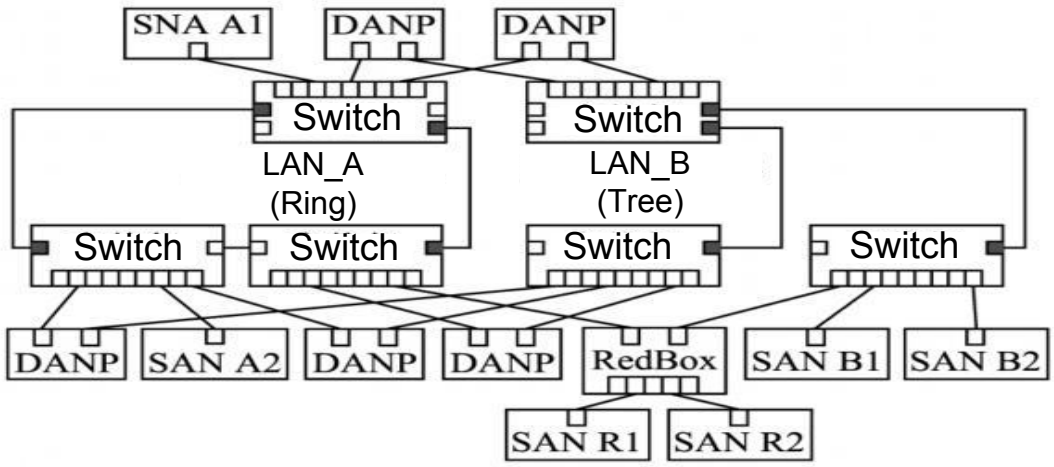


Figure 43 PRP protocol working principle Schematic

SAN: Abbreviations for singly attached node. RedBox is the redundant switch that can connect PRP networks and other networks. In the schematic of the working principle of the PRP protocol, each DANP is connected to two separate parallel working LAN A and B simultaneously, and the message is copied into 2 copies, sent separately through two full duplex communication ports, and then forwarded to the destination DANP by LAN A and B respectively. Meanwhile, each independent LAN with different communication structures (such as tree structure LAN B、 bus structure, ring structure LAN A and RSTP etc.) to

improve system redundancy. And for the node SAN that do not support PRP, it can be directly connected to a LAN (for example the SANA1 node of Figure 43) without configuration, or connected to a special RedBox, it can also provide a little redundancy. PRP port principle as shown in Figure 44. Two parallel working ports (port A and port B) are simultaneously connected to the link redundant entity. when it receives network frames from the upper user datagram protocol (UDP) or the transfer control protocol (TCP), the frames are copied into 2 copies and sent simultaneously from the 2 transmit ports (T), the receiver link redundant entity send the first-to-come frames of these 2 frames from the receiving ports (Rx) to the UDP or TCP, the later-to-come frames are discarded. Obviously, this mechanism makes the parallel redundancy of the physical layer transparent to the protocol above the link layer, so the PRP is compatible with other upper layer protocols, such as RSTP, VLAN. In addition, the link redundant entity also sends the network monitoring message regularly, which is used to detect the network break and other faults.

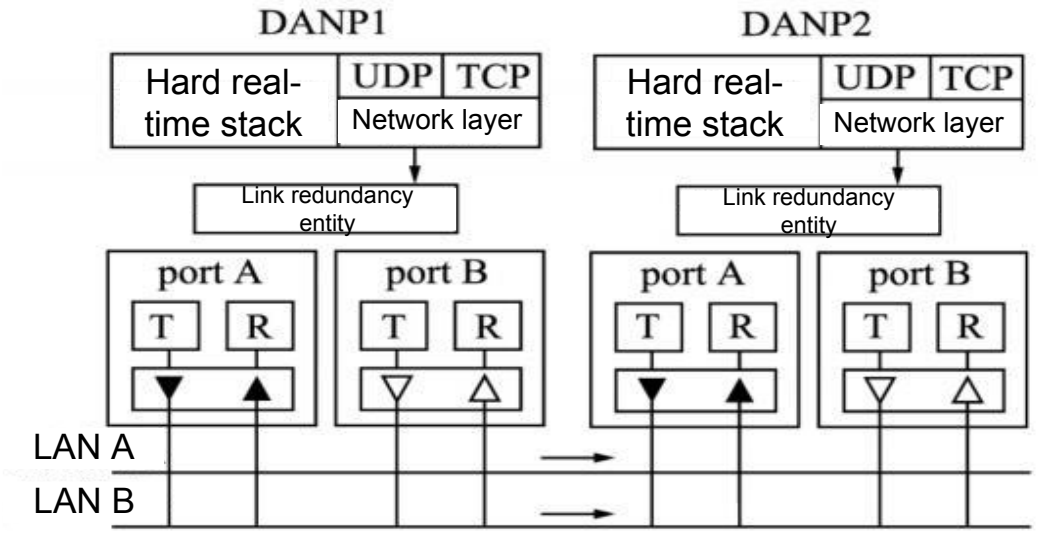


Figure 44 PRP port working principle Schematic

- **HSR**

HSR is the same as the basic idea of PRP, it also provides redundancy for the system by two independent physical ports, but the network structure is ring, and its working principle is shown below.

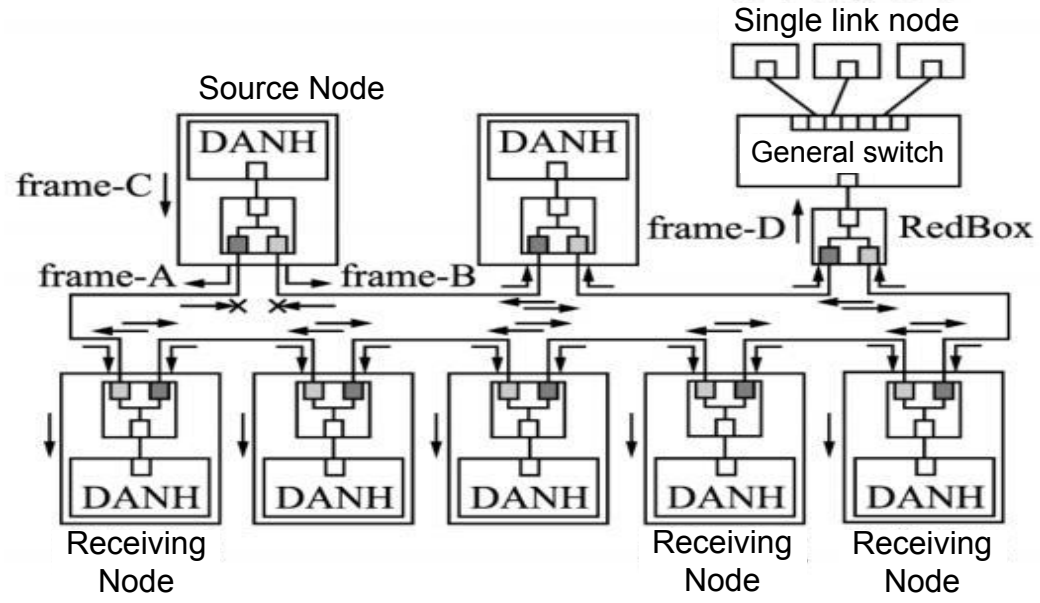


Figure 45 HSR working principle schematic

DANH: Support HSR, abbreviations for doubly attached node with PRP; Frame A, Frame B, and Frame C are frame number.

Suppose that the source node DANH receive one frame from the upper protocol as frame C, copy it to 2 copies, add tag as frame A and frame B, and are sent separately. The DANH on the loop receives the frame A from the port, checks whether it is a broadcast frame, if yes then receives and forwards, otherwise checks whether its destination link mac address is the address of this node; if not then it is forwarded from the other port to the next node, if yes then checks whether the frame B has arrived first; if frame B arrives then discards frame A, otherwise packages the frame A sends to the upper protocol for processing. When the frame A returns to the source node port, the node determines that this is the frame sent by itself and discards it, thus avoiding the loop storm. Frame B transmission principle is exactly the same as frame A. in this way, each upper layer protocol frame is copied into 2 copies, transmitted in different directions in the loop, any one single point breaks, only affects the transmission in one direction, the other direction is not affected, no network recovery time is required, this mechanism is also completely transparent to the upper layer protocol. HSR will also send a network monitoring message, once a port has not received the monitoring message for a long time, it is determined that the network connected is broken. HSR

network can be accessed via RedBox for devices that do not support HSR.

5.1.2 Web Configuration

Click navigation tree [Functions]→[Redundancy], enter into the redundancy configuration page as shown in below figure;

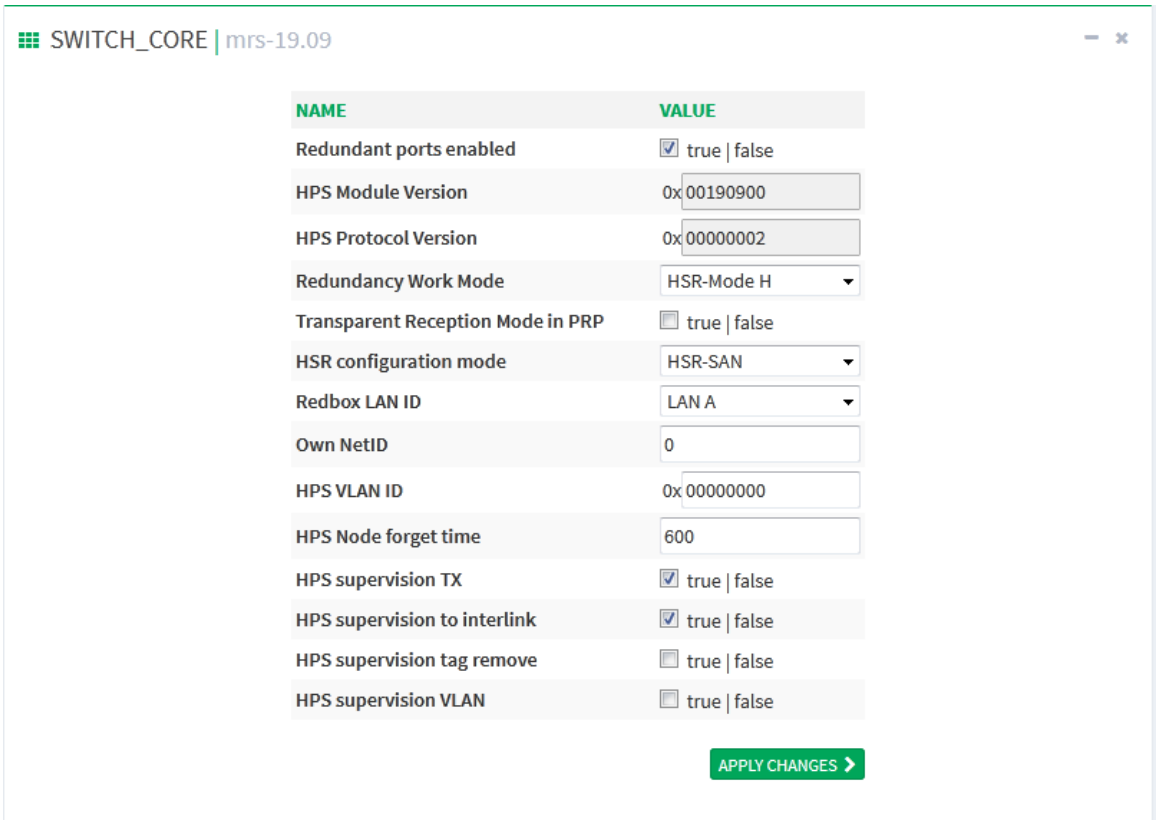


Figure 46 Redundancy configuration page

Redundant ports enabled

Configuration options: true/false

Default configuration: true

Function: When the enable port acts as a redundant port, the port is not a common Ethernet port.

HPS Module Version

Function: show the current HPS module version.

HPS Protocol Version

Function: show the current HSR-PRP redundancy protocol version.

Redundancy Work Mode

Configuration options: PRP-Duplicate discard mode/PRP-Duplicate accept mode/HSR-Mode H/HSR-Mode N/HSR-Mode T/HSR-Mode U/HSR-Mode X

Default configuration: HSR-Mode H

Function: PRP-Duplicate discard mode: receiver can detect duplicate items in this mode, the transmitter LRE attaches a six-byte field after the two frames, it contains a serial number, which is the redundancy control tail (RCT). The receiver LRE uses RCT serial number and source mac address to detect duplicate items. It only forwards the first frame in a pair to its upper layer. All devices in the PRP network must be set to prp-duplicate-discard mode as shown in figure 5 PRP configuration schematic.

PRP-Duplicate accept mode: this mode is used for testing purposes to verify that duplicate items are indeed discarded by the link layer rather than the high-level protocol. in this mode, the transmitter is configured to send two frames without RCT. the receiver is configured to accept two frames and forward them (if both arrive) to its upper layer.

HSR-Mode H: this mode is required option and is the default mode, mainly the forwarding of data frames with HSR tag. In this mode, except the frames sent by the node itself, the DANH will insert the HSR tag and forward the loop network traffic. The duplicate frame and the frame that the node is unicast destination will not be forwarded. all devices in the HSR network must be set to HSR-H mode, as shown in Figure 49 typical HSR network schematic;

HSR-Mode N: This mode is optional, no forwarding. In this mode, the behavior of the node is similar to the mode H, the difference is that the node must not forward loop network traffic between ports.

HSR-Mode T: This mode is optional; it is transparent forwarding. In this mode, DANH must first remove the HSR tag and then forward the frame to another port and send the frame from the host to both ports without the tag and without dropping the duplicate items.

HSR-Mode U: This mode is optional; it is unicast forwarding. In this mode, the behavior of the node is similar to the mode H, the different is that the node must forward unicast traffic as destination like multicast.

Transparent Reception Mode in PRP

Configuration options: true/false

Default configuration: false

Function: After the mode is enabled, the duplicate frame is not discarded and the RTC is not erased.

HSR configuration mode

Configuration options: HSR-SAN/HSR-HSR/HSR-PRP

Default configuration: HSR-SAN

Function: in HSR, it identifies whether the Redbox is configured in HSR-SAN，HSR-PRP or HSR-HSR mode.

Redbox LAN ID

Configuration options: LAN A/LAN B

Default configuration: LAN A

Function: it identifies Redbox LAN ID "A" or "B" used in HSR-PRP mode.

Own NetID

Configuration range: 3 bits [0-7]

Default configuration: 0

Function: It is the identification number of the ring network connected by the node.

HPS VLAN ID

Configuration range: 12 bits [00-FFF]

Default configuration：00000000

Function: it is used to determine the VLAN ID of the Redbox nodes.

HPS Node forget time

Configuration range: 10 bits [0-1023] unit is s

Default configuration: 600s

Function: forget time of node. By default, it is set to 600s.

HPS supervision TX

Configuration options: true/false

Default configuration: true

Function: enable or disable the transmission of supervisory frames.

HPS supervision to interlink

Configuration options: true/false

Default configuration: true

Function: transfer the supervision frame to the interlink port.

HPS supervision tag remove

Configuration options: true/false

Default configuration: false

Function: Remove the HSR head or PRP tail to the supervision frame when transfer to the interlink port.

HPS supervision VLAN

Configuration options: true/false

Default configuration: false

Function: Processing supervision frame with VLAN.

5.1.3 Typical Configuration Example

Three typical configurations: PRP network, HSR network and QUADBOX network.

- **PRP typical network**

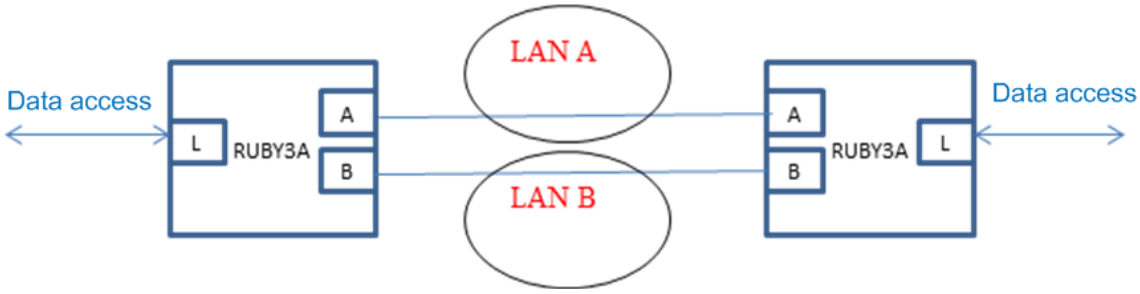


Figure 47 PRP typical network schematic

Networking Notes:

All devices in the PRP network must be set to prp-duplicate-discard mode, it is recommended that A port connect to A port of the other end, B port connect to B port of the

other end. Where A—A can pass through a LAN A, B—B can pass through a LAN B, but note that it must independent between LAN A and LAN B.

In PRP networking way, data between port A and B will not be added to other headers, so all devices between LAN A and LAN B can be managed by Ruby3a (different with HSR). Web configuration is shown below;

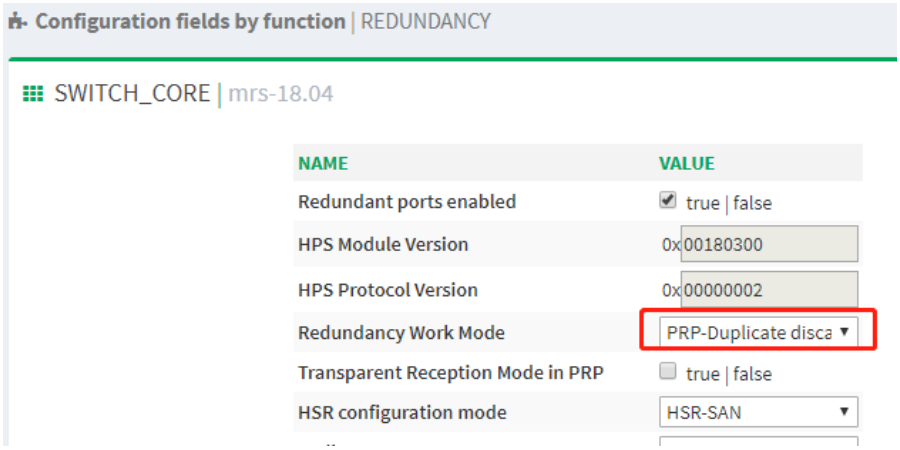


Figure 48 PRP configuration schematic

- **HSR typical network**

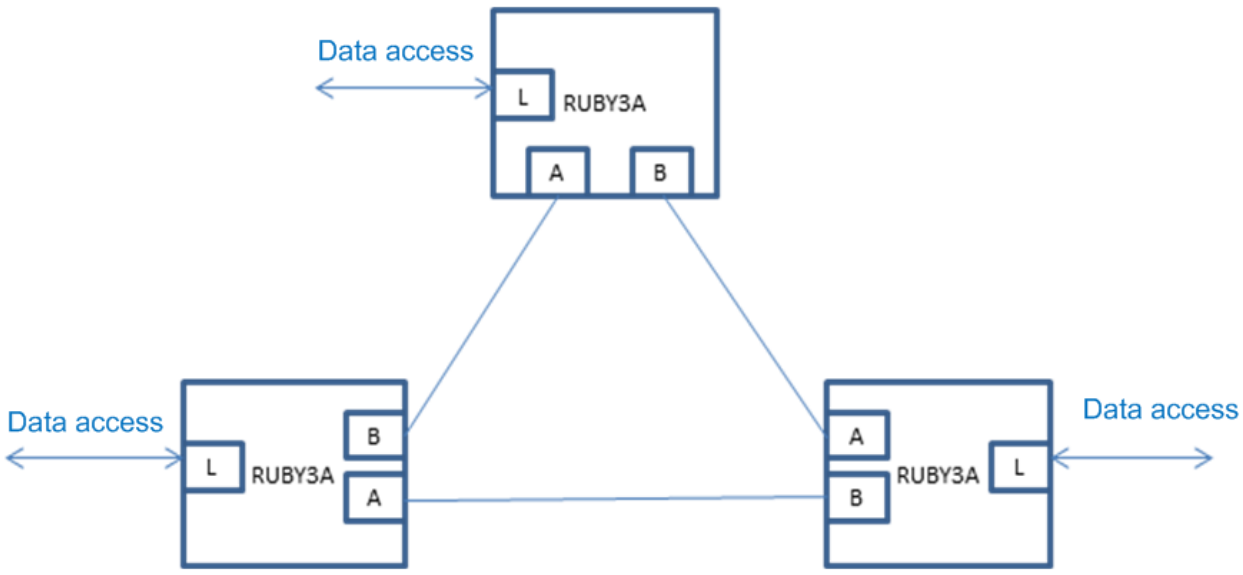


Figure 49 HSR typical network schematic

Networking Notes:

All devices in the HSR network must be set to HSR-H mode, it is recommended that A port connect to B port of the other end and B port connect to A port of the other end as a ring.

Note: the connection points between devices can be transparent transmission using other devices, but note that since the data between HSR devices are all added with HSR heads, it can not be remotely managed if the transparent transmission devices are added between devices. Web configuration is shown below;

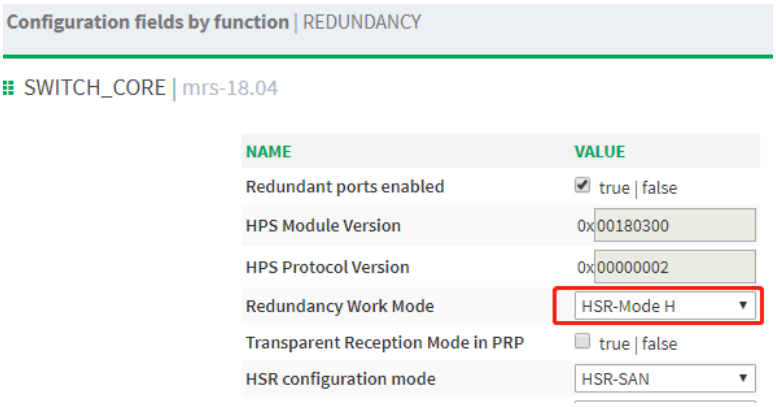


Figure 50 HSR configuration schematic

- QUADBOX typical network

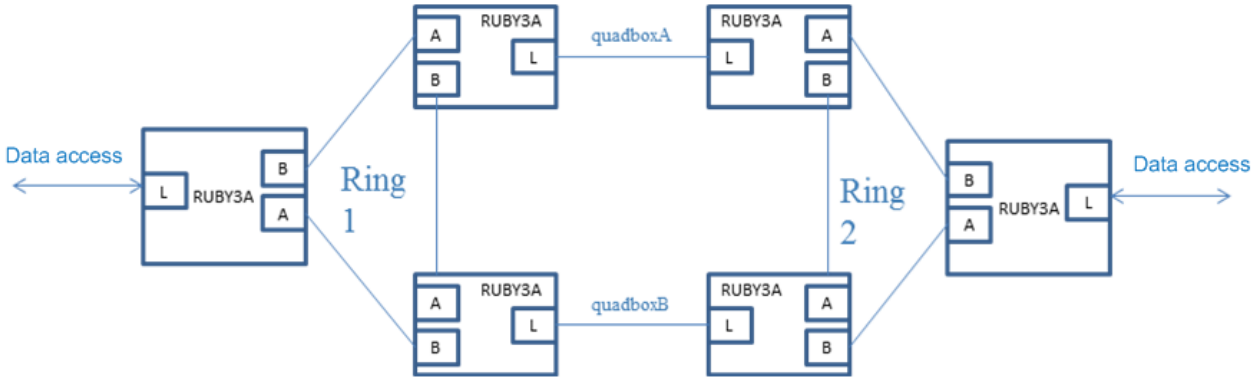


Figure 51 QUADBOX typical network schematic

Networking Notes:

The advantage of Quadbox network is that the two HSR rings can be protected each other, that is ,1 to 1 protection upgraded to 4 to 1 protection. Where the connection of quadboxA and quadboxB is set to need to run HSR protocol, so that the 3 ports of the 4 devices that make up the quadboxA and quadboxB become the HSR redundant ports.

All devices in the quadbox network must be set to HSR-H mode (default mode), the interlink port which is used to connect quadboxA and quadboxB is configured to be in HSR-HSR mode. Web configuration is shown below;

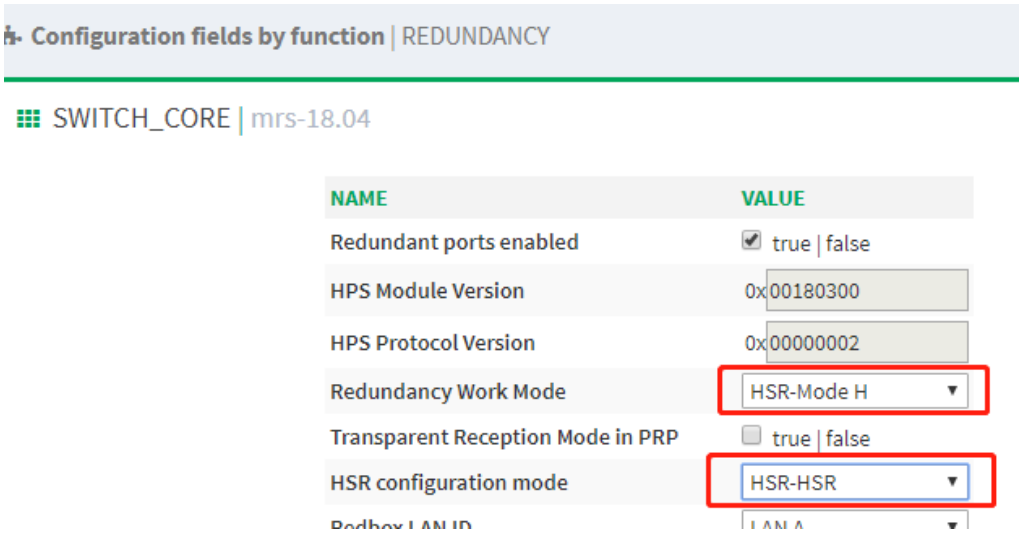


Figure 52 QUADBOX configuration schematic

5.2 PTP

5.2.1 Introduce

PTP (precision time protocol) synchronizes the clock running independently on separate nodes within the measurement and control system to a protocol of high accuracy and accuracy. The synchronization protocol includes both phase synchronization and frequency synchronization, and the synchronization accuracy can reach ±100 ns.

5.2.2 Concept

1. PTP domain

The network applying the PTP protocol is the PTP domain. PTP domain has only one most advanced clock, and the other devices in the domain keep synchronized with that clock.

2. PTP port

The port that enables the PTP protocol is the PTP port.

3. Clock node

The node in the PTP domain is clock node, PTP protocol defines the following basic clock nodes:

- OC (Ordinary Clock)

  This clock node has only one PTP port in the PTP domain involved in clock

synchronization, and synchronizes the time from the upstream clock node or publishes the time to the downstream clock node through this port.

- BC (Boundary Clock)

This clock node has one or more PTP ports in the PTP domain involved in clock synchronization.

When only one PTP port is involved in clock synchronization, the time is synchronized from the upstream clock node or published to the downstream clock node through this port; When multiple PTP ports are involved in clock synchronization, the time is synchronized from the upstream clock node through one of the ports, and time is published to the downstream clock node through the remaining ports. when the boundary clock is used as a clock source, time can be published to the downstream clock node through multiple PTP ports.

- TC (Transparent Clock)

This clock node does not need to keep clock synchronization with other clock nodes. there are multiple PTP ports on the TC, but these ports only forward PTP protocol message and forward delay correction for them without synchronizing the clock through either port. The transparent clock has two types:

E2ETC (End-to-End Transparent Clock): Directly forwarding non-P2P types protocol message in the network, and calculating the whole link delay.

P2PTC (Peer-to-Peer Transparent Clock): Directly forwarding Sync meassage, Follow_Up message and Announce message, terminate other protocol messages, and calculating the delay of each link on the whole link.

4. For a pair of synchronous clock nodes, there are the following master-slave relationships:
The node that publishes the synchronous clock is the master node, and the node that receives the synchronous clock is the slave node.
The clock of the master node is the master clock, and the clock of the slave node is the slave clock.
The port that publishes the synchronous clock is the master port, and the port that receives

the synchronous clock is the slave port.

5.2.3 Synchronization principle

1. Select Optimal Clock

Through interactive the clock level, clock ID and other information in the Announce message, each clock node finally selects a clock node as the optimal clock for the PTP domain. At this time, the master-slave relationship between each node and the master-slave port on each node are also determined. By this process, a spanning tree based on the optimal clock as root is established in the PTP domain. Since then, the master clock will send announce message to the slave clock regularly. If the slave clock does not receive the Announce message sent by the master clock for a period of time, the master clock will be considered invalid, so the optimal clock selection is resumed.

Announce message contains enough information to ensure the selection of the optimal clock, which contains several important information, such as master clock priority 1, clock level, clock accuracy, master clock priority 2, clock ID. This information is compared in turn when selecting optimal clock. Clock with smaller clock priority 1 is selected as optimal clock; clock with smaller clock level is selected as optimal clock when primary clock priority 1 is same; similarly, clock with smaller clock is selected as optimal clock when all previous information is the same.

2. Synchronization principle

The message is interacted and synchronized between the master and slave clocks and the sending and receiving time of the message are recorded. The total delay between master and slave clocks is calculated by calculating the time difference of the round-trip of message. If the network is symmetrical, the one-way delay is half of the total round-trip delay. The slave clock can synchronize with the master clock by adjusting the local time according to the master-slave clock deviation and one-way delay.

PTP has two delay measurement mechanisms:

request_response mechanisms: Time delay measurement for end-to-end of the whole

link;

peer-to-peer delay mechanisms: Time delay measurement for point-to-point, compared with the request_response mechanism, the peer-to-peer delay mechanism measures the delay of each link on the whole link;

5.2.4 Web Configuration

Click navigation tree [Functions]→[PTP], enter into the PTP configuration page, as shown below;

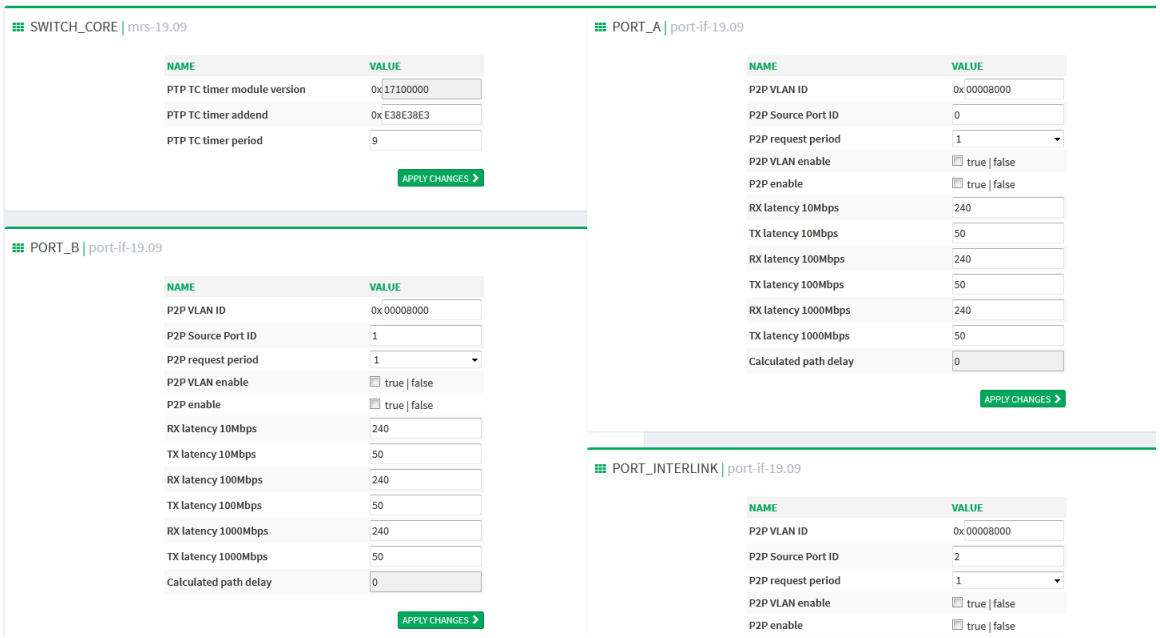


Figure 53 PTP configuration page

From Figure 53, the PTP configuration page is divided into 4 parts, which are the PTP TC configuration page and the ptp configuration page of three ports (port_a/port_b/port_interlin).

1. PTP TC configuration

PTP TC configuration page as shown in below;

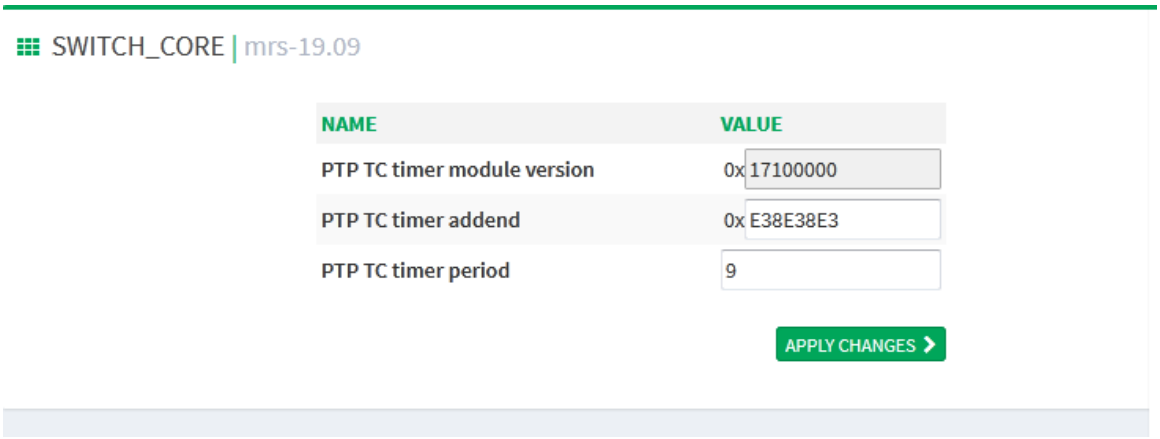


Figure 54 PTP TC configuration page

PTP TC timer module version

Description: IEEE1588 TC timer module version.

PTP TC timer addend

Configuration range: 32 bits [00-FFFFFFFF]

Default configuration：E38E38E3

Function: adjust the timer in subsecond level (please refer to Freescale AN3423)

PTP TC timer period

Configuration range: 32 bits [0-4294967295]

Default configuration：9

Function: please refer to Freescale AN3423.

2. PTP port configuration

Take port port_a as an example, the port_a PTP configuration page is shown in below.

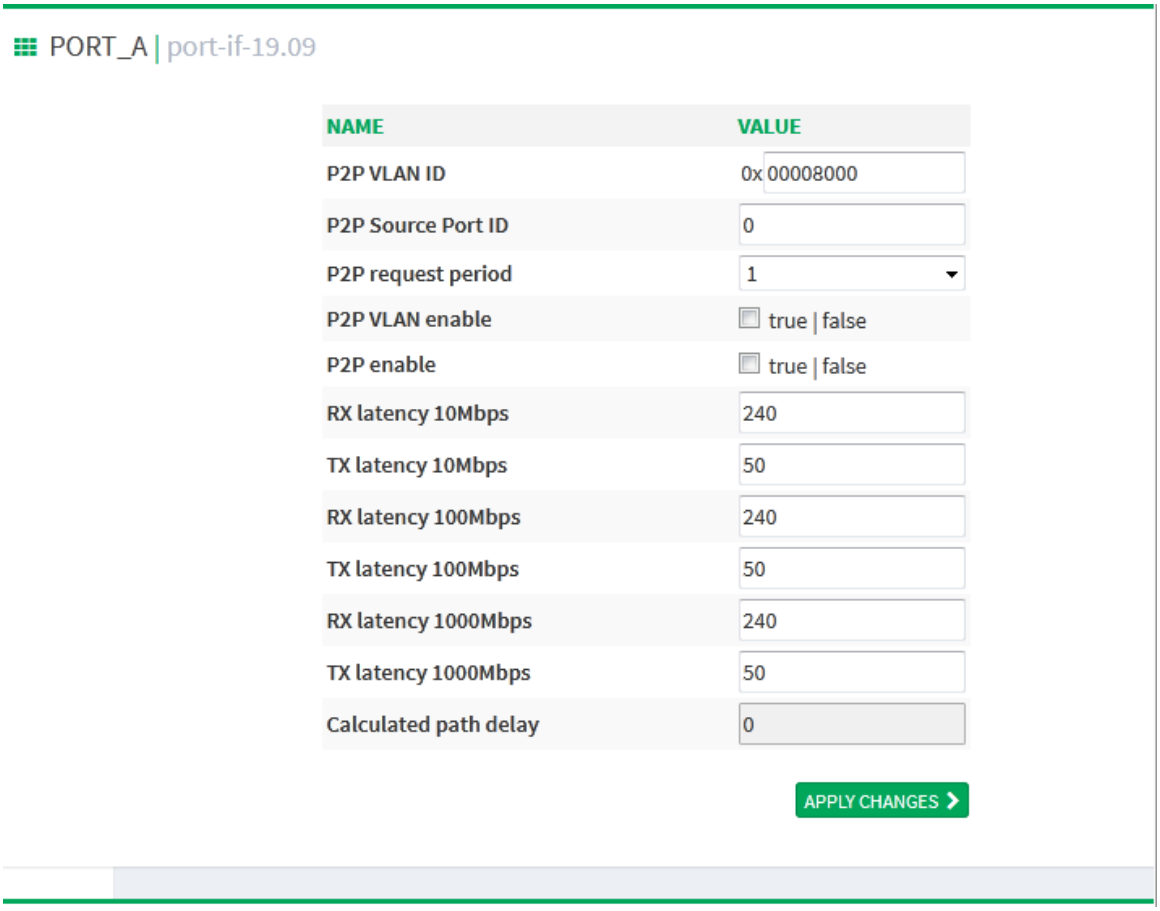


Figure 55 PTP port configuration page

P2P VLAN ID

Configuration range: 16 bits [00-FFFF]

Default configuration: 00008000

Function: configure VLAN tage of PTP.

P2P Source Port ID

Configuration range: 8 bits [00-255]

Default configuration: 0

Function: configure source port ID of PTP.

P2P request period

Configuration options: 1/2/4/8

Default configuration: 1

Function: Pdelay number of requests per second.

P2P VLAN enable

Configuration options: true/false

Default configuration: false

Function: add VLAN tag to the PTP message

P2P enable

Configuration options: true/false

Default configuration: false

Function: enable or disable PTP delay mechanism.

RX latency 10Mbps

Configuration range: 16 bits [0-65535]

Default configuration: 240

Function: RX logical delay (ns (10Mbps) as unit).

TX latency 10Mbps

Configuration range: 16 bits [0-65535]

Default configuration: 50

Function: TX logical delay (ns (10Mbps) as unit).

RX latency 100Mbps

Configuration range: 16 bits [0-65535]

Default configuration: 240

Function: RX logical delay (ns (100Mbps) as unit).

TX latency 100Mbps

Configuration range: 16 bits [0-65535]

Default configuration: 50

Function: TX logical delay (ns (100Mbps) as unit).

RX latency 1000Mbps

Configuration range: 16 bits [0-65535]

Default configuration: 240

Function: RX logical delay (ns (1000Mbps) as unit).

TX latency 1000Mbps

Configuration range: 16 bits [0-65535]

Default configuration: 50

Function: TX logical delay (ns (1000Mbps) as unit).

Calculated path delay

Function: a path delay (ns as unit) calculated using peer-to-peer mechanism of PTP transparent clock.

5.3 Statistics

Click navigation tree [Functions]→[Statistics], enter into statistics configuration page, take port_a as an example as shown in below;

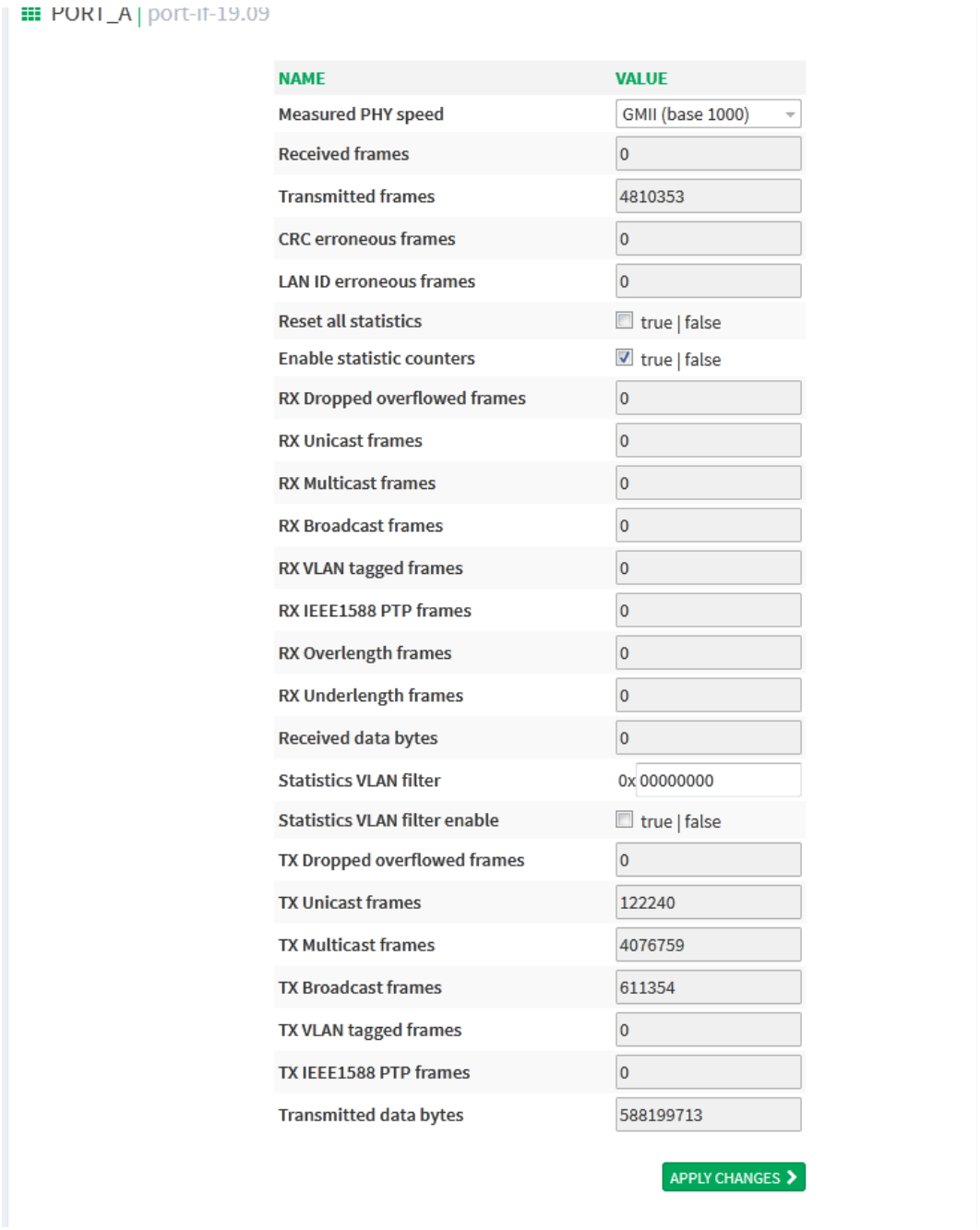


Figure 56 statistics configuration page

Measured PHY speed

Description: PHY speed measured using the speed measurement module: "11" at 1000 Mbps, "10" at 100Mbps and "01" at 10 Mbps.

Received frames

Description: Number of received frames. Range: 32 bits [0-4294967295]

Transmitted frames

Description: Number of transmitted frames. Range: 32 bits [0-4294967295]

CRC erroneous frames

Description: Number of CRC erroneous frames. Range: 32 bits [0-4294967295]

LAN ID erroneous frames

Description: Number of LAN ID erroneous frames. Range: 32 bits [0-4294967295]

Reset all statistics

Description: Reset all statistics counters.

Enable statistic counters

Description: Enable/disable statistic counters.

RX Dropped overflowed frames

Description: Number of RX dropped overflowed frames (in the receiving path). Range: 32 bits [0-4294967295]。

RX Unicast frames

Description: Number of RX unicast frames. Range: 32 bits [0-4294967295]

RX Multicast frames

Description: Number of RX multicast frames. Range: 32 bits [0-4294967295]

RX Broadcast frames

Description: Number of RX broadcast frames. Range: 32 bits [0-4294967295]

RX VLAN tagged frames

Description: Number of RX VLAN tagged frames. Range: 32 bits [0-4294967295]

RX IEEE1588 PTP frames

Description: Number of RX IEEE1588 PTP frames. Range: 32 bits [0-4294967295]

RX Overlength frames

Description: Number of RX overlength frames. (It is valid when jumbo frame is disabled) Range: 32 bits [0-4294967295]

RX Underlength frames

Description: Number of underlength (less than length of min frame) frames. Range: 32 bits [0-4294967295]

Received data bytes

Description: Number of received data bytes (do not include lead byte) Range: 32 bits [0-4294967295]

Statistics VLAN filter

Description: Specified VLAN filter conuter. Range: 12 bits 0X[0-00000FFF]。

Statistics VLAN filter enable

Description: Whether enable specified VLAN filter conuter.

TX Dropped overflowed frames

Description: Number of Tx dropped overflowed frames (in the receiving path). Range: 32 bits [0-4294967295]。

TX Unicast frames

Description: Number of Tx unicast frames. Range: 32 bits [0-4294967295]

TX Multicast frames

Description: Number of Tx multicast frames. Range: 32 bits [0-4294967295]

TX Broadcast frames

Description: Number of Tx broadcast frames. Range: 32 bits [0-4294967295]

TX VLAN tagged frames

Description: Number of Tx VLAN tagged frames. Range: 32 bits [0-4294967295]

TX IEEE1588 PTP frames

Description: Number of Tx IEEE1588 PTP frames. Range: 32 bits [0-4294967295]

Transmitted data bytes

Description: Number of transmitted data types (do not include lead type). Range: 32 bits [0-4294967295]

6 Other Configurations

There are multiple functional modules with switch configuration except HSR/PTP in the configuration page, including modules such as alarm、sntp、snmp、radius、tacacs.

6.1 Alarm

6.1.1 Introduce

This series switches support the following types of alarms:

- Memory / CPU usage alarm: If this function is enabled, an alarm is generated when the CPU / memory usage exceeds the specified threshold.
- Port alarm: If this function is enabled, an alarm is triggered when the port is in link down state.

When the alarm function is enabled, alarm modes include logging, front alarm LED blinking, alarm terminal block triggering, and SNMP trap packet sending.

6.1.2 Web Configuration

1. Configure and display memory/ CPU usage alarm.

Click navigation tree [Other Configurations]→[Alarm], enter into Alarm configuration and display page as shown in below;

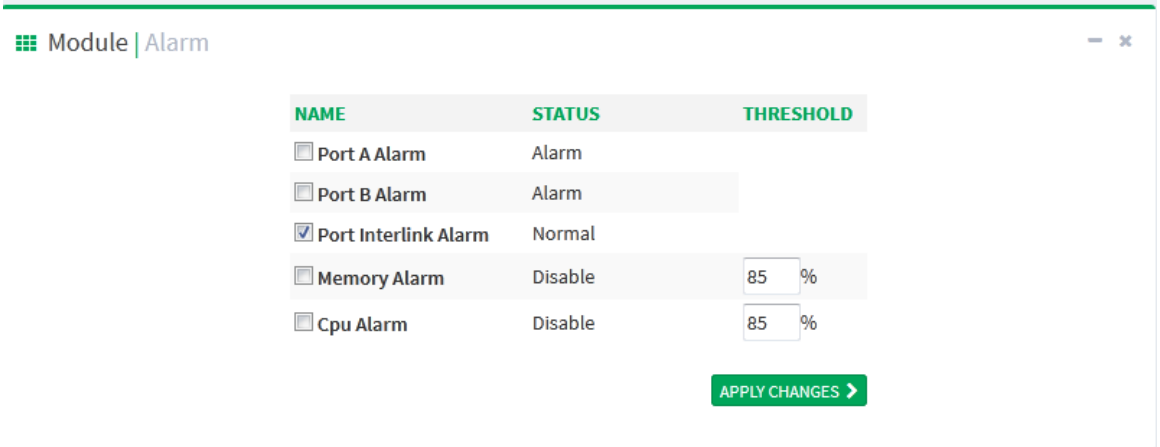


Figure 57 Memory and CPU utilization alarm configuration page

Memory Alarm/CPU Alarm

Configuration options: enable/disable

Default configuration: disable

Function: enable or disable Memery alarm/CPU alarm.

Threshold（%）

Configuration range: 50~100

Default configuration: 85

Function: configures the switch Memory/CPU alarm threshold. When the Memory/CPU utilization of this switch is greater than this value, Memory/CPU alarm is generated.

Explanation: When the Memory/CPU alarm is generated, in order to prevent the Memory/CPU utilization fluctuates near the threshold to cause frequent alarm and alarm release, the alarm will be released only when the Memory/CPU utilization ratio is one floating value lower than the threshold.

Alarm status

Display options: Normal/Alarm

Function: Display switch Memory/CPU utilization status. Alerm indicates Memory/CPU utilization is more than threshold.

CAUTION:

The CPU utilization rate in this text refers to the average CPU utilization rate of 5 seconds.

2. Configure and display port alarm.

Click navigation tree [Other Configurations]→[Alarm], enter into alarm configuration and dispaly page as shown in below;

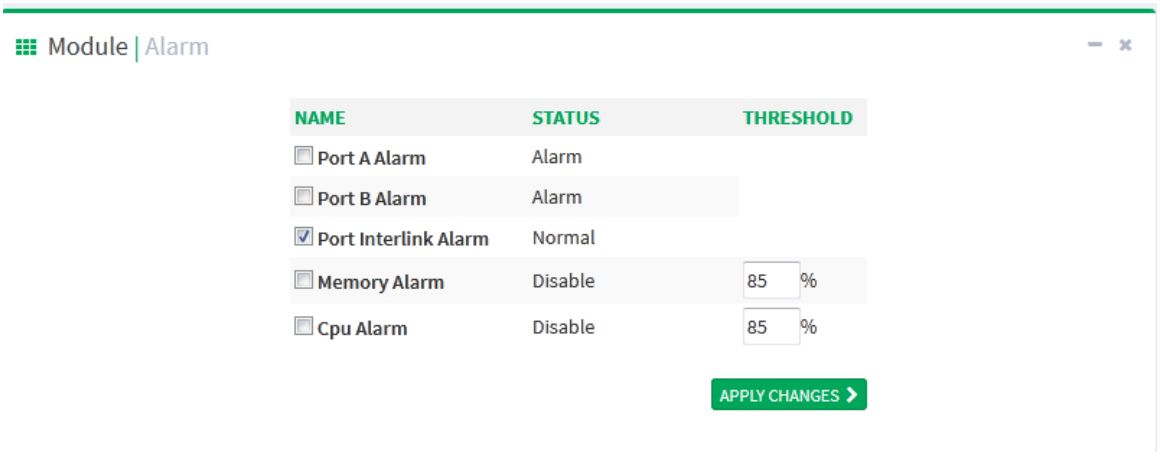


Figure 58 Port alarm configuration page

Port

Configuration options: disable/enable.

Default configuration: enable.

Function: enable or disable port alarm.

Alarm status

Display options: LinkDown/LinkUp

Function: Display port connection status. LinkUp indicates that the port is connected and can communicate normally; LinkDown indicates that the port is disconnected or abnormal, an alarm will be generated.

6.2 Port Configuration

Click navigation tree [Other Configurations]→[Port configuration], enter into port configuration page, the port link state, speed, type can be configured in the page, as shown in below;

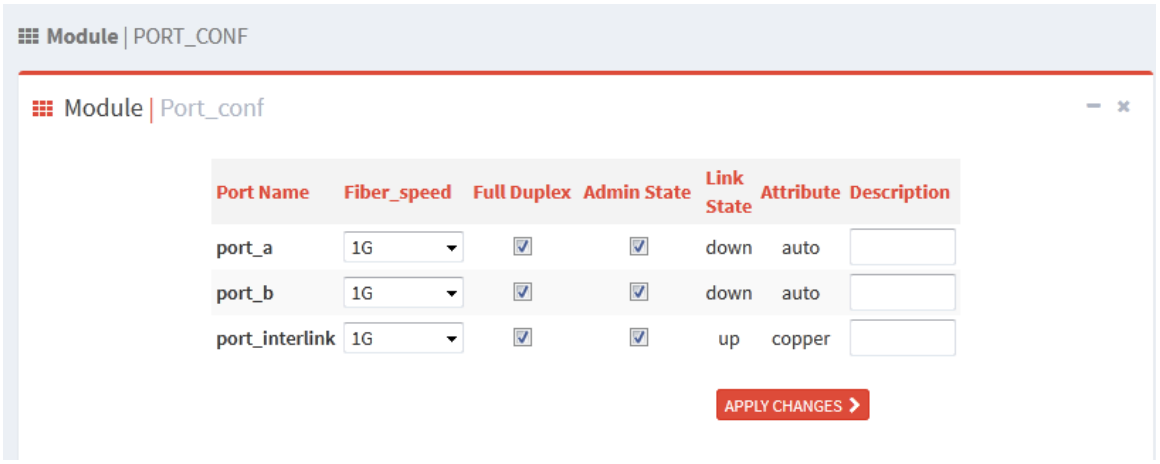


Figure 59 Port configuration

Port Name

There are three prots, port_a, port_b and port_interlink

Fiber_speed

Configuration options: 100M/1G

Function: configure port autonegotiation speed.

Description: Configuring port mode to auto, the port default speed is determined by auto-negotiation with the other end, and the negotiated speed can be either within the port speed range. By configuring the speed, the port can negotiate only part of the speed, thus controlling the speed negotiation. Only the optical port can set 100M.

CAUTION:

- Duplex and speed configuration are avlid only in auto mode.
- The port_interlink of the SM6.6-HSR/PRP subcard is used internally, do not configure or close it.

Full Duplex

Configuration options: Fdx/Hdx

Function: Configure port auto-negotiation duplex mode.

Description: Fdx full duplex refers to the port can receive data while transmitting data; Hdx half duplex refers to the port can only transmit or receive data at the same time.

When the port mode is configured to auto, the port default duplex mode is determined by auto-negotiation with the other end, and duplex mode can be either of the Fdx and Hdx.

By configuring the duplex, the port can negotiate only one duplex mode, thus controlling the duplex mode negotiation.

Admin Status

Configuration options: shutdown/no shutdown

Default configuration: no shutdown

Function: Whether the port is allowed to transmit data.

Description: no shutdown indicates that enable port and allow data transmission; shutdown indicates that disable port and do not allow data transmission. This option can directly affect the hardware status of the port and trigger port alarm information.

Link Status

Display the connection status of the current port.

up indicates that the port is in LinkUp state and can communicate normally;

down indicates that the port is in LinkDown state and can't communicate normally;

Attribute

Configuration options: auto/copper

Default configuration: auto

Function: Ethernet port media type.

Description: Auto port detect the cables automatically to determine media type

Copper: The port media type is copper

Description

Configuration range: 1~200 characters

Function: configure the port alias to describe the port.

6.3 Mac Configuration

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

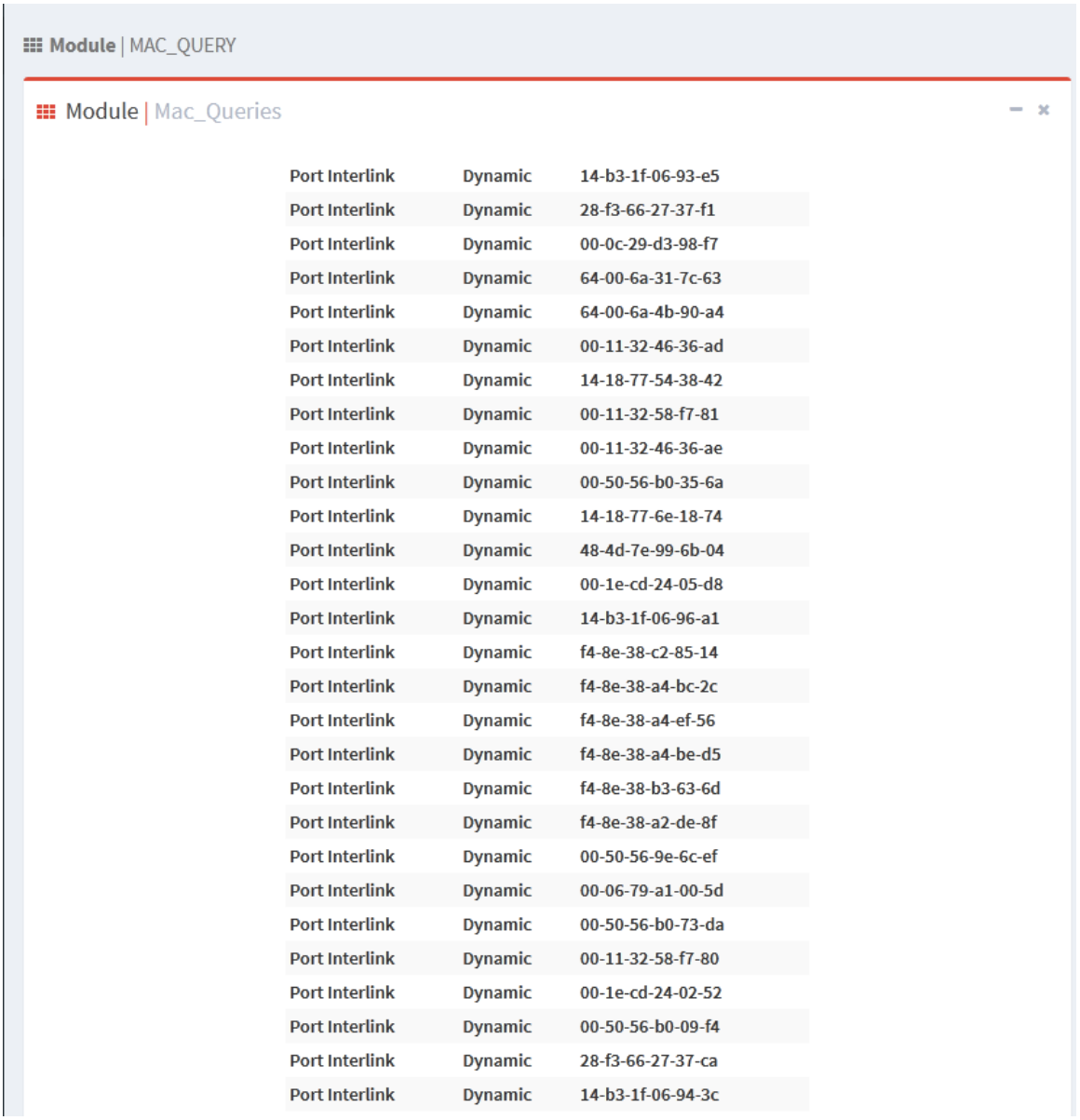
dynamic MAC addresses) and is permanently valid.

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.

6.3.1 Mac Queries

Click navigation tree [Other Configurations]→[Mac Queries], enter into MAC address query page, as shown in below;



Port Interlink	Dynamic	14-b3-1f-06-93-e5
Port Interlink	Dynamic	28-f3-66-27-37-f1
Port Interlink	Dynamic	00-0c-29-d3-98-f7
Port Interlink	Dynamic	64-00-6a-31-7c-63
Port Interlink	Dynamic	64-00-6a-4b-90-a4
Port Interlink	Dynamic	00-11-32-46-36-ad
Port Interlink	Dynamic	14-18-77-54-38-42
Port Interlink	Dynamic	00-11-32-58-f7-81
Port Interlink	Dynamic	00-11-32-46-36-ae
Port Interlink	Dynamic	00-50-56-b0-35-6a
Port Interlink	Dynamic	14-18-77-6e-18-74
Port Interlink	Dynamic	48-4d-7e-99-6b-04
Port Interlink	Dynamic	00-1e-cd-24-05-d8
Port Interlink	Dynamic	14-b3-1f-06-96-a1
Port Interlink	Dynamic	f4-8e-38-c2-85-14
Port Interlink	Dynamic	f4-8e-38-a4-bc-2c
Port Interlink	Dynamic	f4-8e-38-a4-ef-56
Port Interlink	Dynamic	f4-8e-38-a4-be-d5
Port Interlink	Dynamic	f4-8e-38-b3-63-6d
Port Interlink	Dynamic	f4-8e-38-a2-de-8f
Port Interlink	Dynamic	00-50-56-9e-6c-ef
Port Interlink	Dynamic	00-06-79-a1-00-5d
Port Interlink	Dynamic	00-50-56-b0-73-da
Port Interlink	Dynamic	00-11-32-58-f7-80
Port Interlink	Dynamic	00-1e-cd-24-02-52
Port Interlink	Dynamic	00-50-56-b0-09-f4
Port Interlink	Dynamic	28-f3-66-27-37-ca
Port Interlink	Dynamic	14-b3-1f-06-94-3c

Figure 60 MAC address query

Caution:

- In switching mode, port_a, port_b, port_interlink correspond to three real ports respectively;
- In redundancy mode, the port_b represents two redundant ports that do not distinguish A and B, port_a is not used.

6.3.2 Mac Address Control

Click navigation tree [Other Configurations]→[Mac Address Control], enter into MAC address control page, as shown in below;

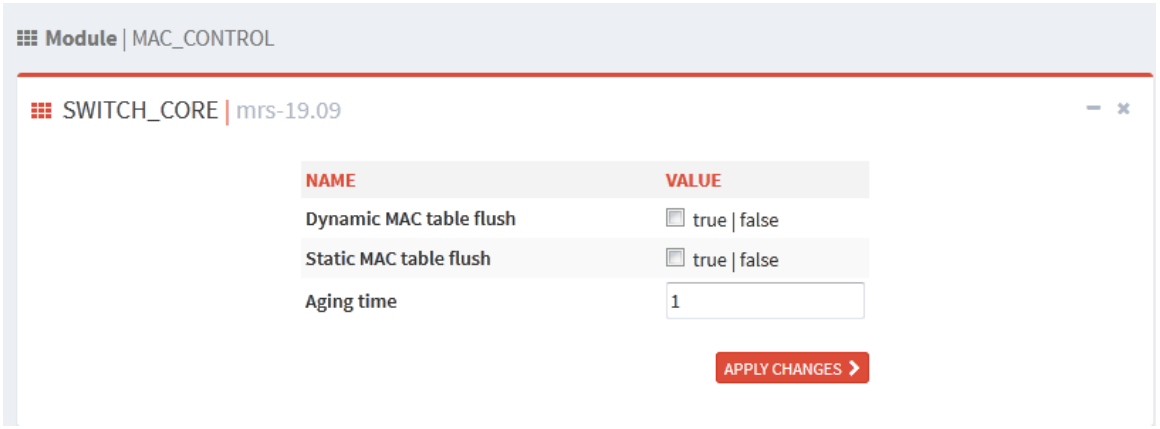


Figure 61 mac address control page

Dynamic MAC table flush

Configuration options: true/false

Default configuration: false

Configure whether refresh the dynamic mac address.

Static MAC table flush

Configuration options: true/false

Default configuration: false

Configure whether refresh the static mac address.

Aging time

Configuration options: 0-15min

Default configuration: 1

Configurate mac table aging time.

6.3.3 Mac Address Configuration

Click navigation tree [Other Configurations]→[Mac Address Configuration], enter into mac address configuration page, as shown in below;

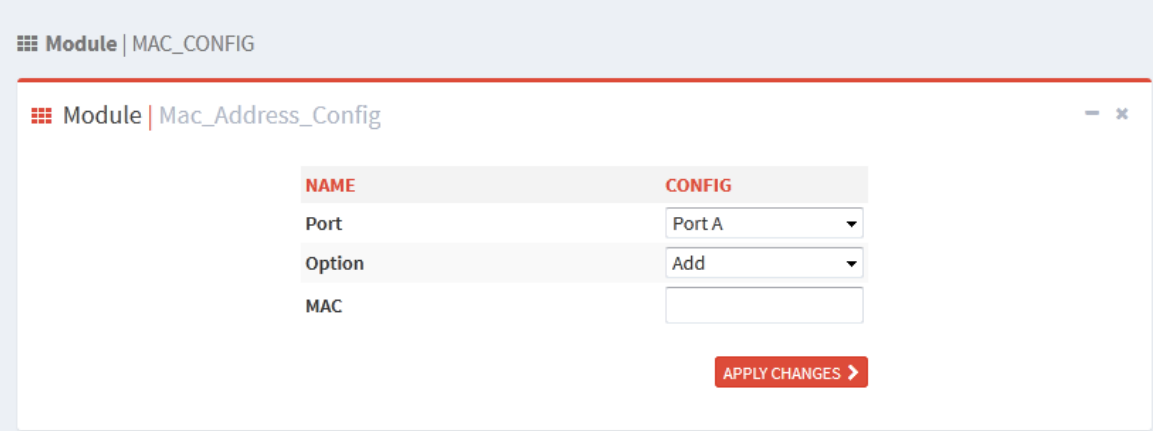


Figure 62 mac configuration page

Port

Configuration options: port_a/port_b/port_interlink

Default option: port_a

Option

Configuration options: add/delete

Default option: add

Delete or add mac address of port.

MAC

Configuration format: HH-HH-HH-HH-HH-HH (H is a hexadecimal number)

Function: Configure unicast mac address with the lowest bit of the highest byte is 0.

6.4 Sntp

6.4.1 Introducation

SNTP (Simple Network Time Protocol) protocol calibrates the time by requesting and responding between the server and the client. The switch acts as a client to calibrate the time based on the server's message.

The request of the SNTP client is sent to the server one by one in unicast form, the server responds to the message.

CAUTION:

- When the switch uses SNTP, the SNTP server must be active;

➢ SNTP time information in the protocol is the standard time information of time zone 0.

6.4.2 Web Configuration

1. Enable SNTP protocol

Click navigation tree [Other Configurations]→[SNTP], enter into SNTP configuration page, as shown in below;

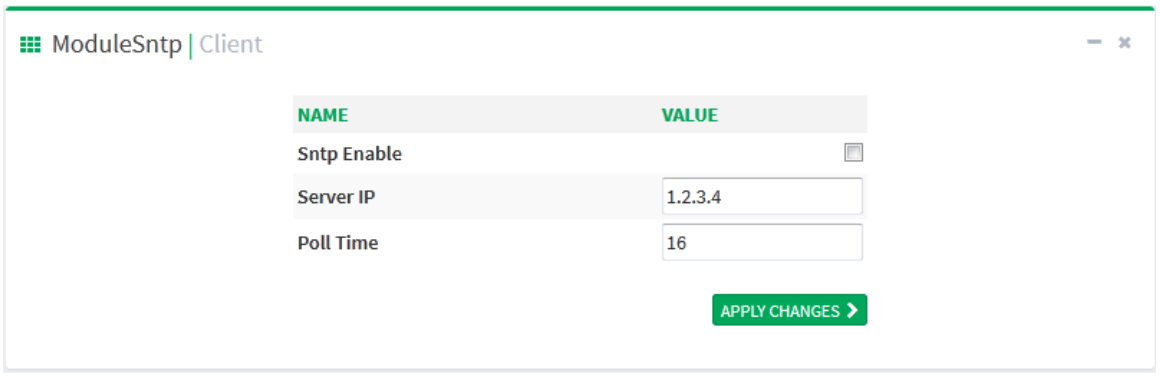


Figure 63 Enable SNTP protocol

SNTP Enable

Configuration options: enable/disable

Default configuration: disable

Function: enable or disable SNTP protocol

Caution:

Since NTP and SNTP use the same udp port number, both can not be enabled at the same time.

2. SNTP Server IP Configuration

Server IP

Configuration format: A.B.C.D

Function: Configure SNTP server IP, the client will calibrate the time according to the message of this server.

3. Configure time interval of SNTP client send synchronization request

Poll Time

Configuration options: 16~16284s

Function: Configure time interval of SNTP client send synchronization requests to SNTP server.

4. View if the clock synchronizes with server time

Click navigation tree [Network Nodes], enter into clock viewing page, as shown in below;

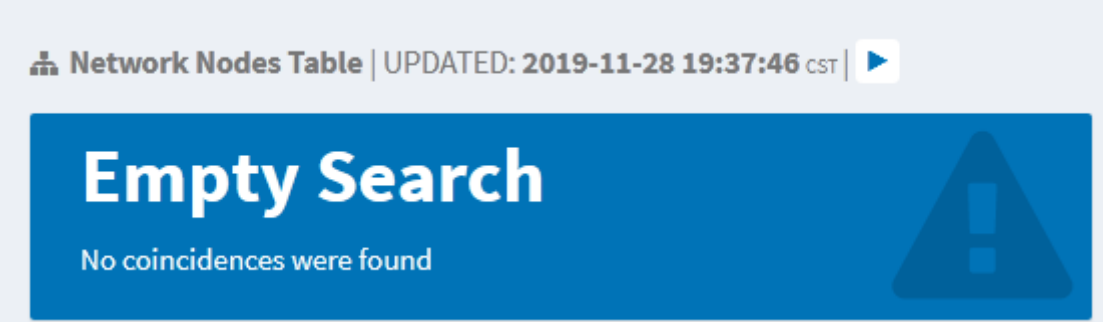


Figure 64 View synchronized clock page

Click <display clock> button, the clock is displayed in the window after SNTP client synchronizes time with the server.

6.5 Ntp

6.5.1 Introduction

The Network Time Protocol (NTP) synchronizes time between distributed servers and clients. NTP synchronizes the clocks of all network devices, ensuring time consistency among all devices. This enables devices to provide multiple applications based on the same time. NTP-enabled local system cannot only synchronize its clock from other clock sources, but also serve as the clock source for other devices.

As shown in Figure 65, the round-trip delay "(T4-T1)-(T3-T2)" and clock offset "((T2-T1) + (T3-T4))/2" can be calculated based on the exchange of NTP packets, thereby achieving high-precision clock synchronization among devices.

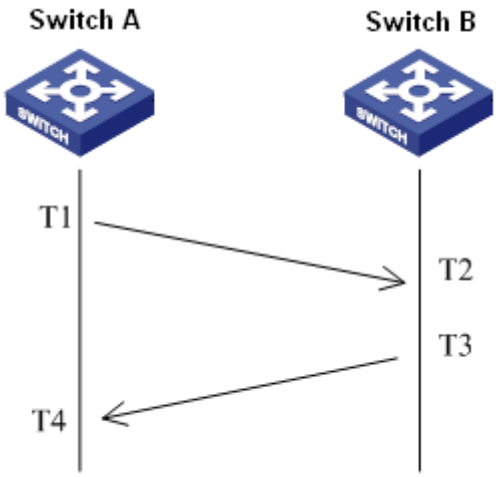


Figure 65 NTP

6.5.2 NTP Working Modes

NTP can adopt the following working modes for time synchronization. You can select the appropriate working mode as required.

Client/Server mode: In this mode, the client sends clock synchronization packets (client mode) to the server. After receiving the packets, the server automatically works in server mode and sends response packets (server mode). After receiving response packets, the client synchronizes from the optimal server clock.

Peer mode: In this mode, the active peer sends clock synchronization packets (active peer mode) to the passive peer. After receiving the packets, the passive peer automatically works in passive peer mode and sends response packets (passive peer mode). Based on the exchange of packets, the devices set up the peer mode. The active peer and passive peer can synchronize time from each other. If both peers have synchronized time from other devices, the peer with greater clock stratum synchronizes time from the peer with smaller clock stratum.

Broadcast mode: In this mode, the broadcast server periodically broadcasts clock synchronization packets (broadcast mode). After receiving the packets, the broadcast client sends clock synchronization packets (client mode) to the server. After receiving the request packets, the server sends response packets (server mode). The server and the client

accomplish clock synchronization by exchanging eight request and response packets.

Multicast mode: The multicast client periodically sends multicast synchronization request packets (client mode) to the multicast server. After receiving the packets, the server sends unicast response packets (server mode). Then the server and the client accomplish clock synchronization by exchanging unicast clock synchronization request and response packets.

6.5.3 Web Configuration

1. Enable NTP protocol

Click navigation tree [Other Configurations]→[NTP], enter into NTP global configuration Interface, as shown in below;

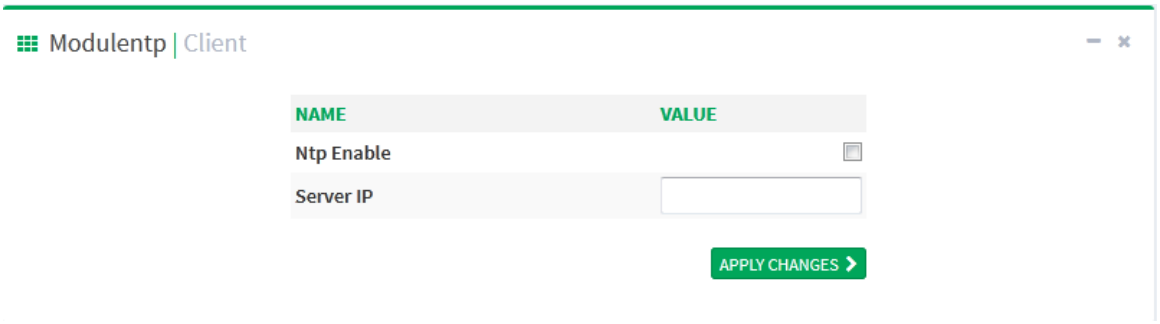


Figure 66 Enable NTP protocol

NTP Enable

Configuration options: enable/disable

Default configuration: disable

Function: enable or disable global NTP service.

Caution:

- Since NTP and SNTP use the same udp port number, both can not be enabled at the same time.
- When the NTP service is not enabled, the NTP service can be configured and saved, that is, whether the NTP service is enabled or not does not affect the configuration of the ntp service.

2. NTP Server configuration

Server IP

Configuration format: A.B.C.D

Function: Configure IP address of NTP server, and the client will calibrate the time according to the message of that server.

6.6 IEC61850 MMS

6.6.1 Introduction

At present, the switch is transparent by the function of the transformer substation in the transformer substation network. The tools (protocols) other than IEC61850 are required for monitoring, such as EMS, WEB, CLI and OPC etc.. it causes the knowledge point and the configuration point disperse, inconsistent, and inconvenient. To solve these problems, the switch is modeled according to the IEC61850 protocol and incorporated into the substation automatic system (IEC61850) as an intelligent electronic device (IED，Intelligent Electronic Device). It unifies substation automatic monitor viewing, convenient user integrated management planning, save construction costs, save maintenance costs.

Caution:

Default modeling files switch.cid provided by our company have been imported in this switch, if customers need to import other modeling files refer to the section "4.6 file upload "to import files.

6.6.2 Web Configuration

1. Enable IEC 61850 function

Click navigation tree [Other Configurations]→[Iec61850mms], enter into NTP global configuration page, as shown in below;

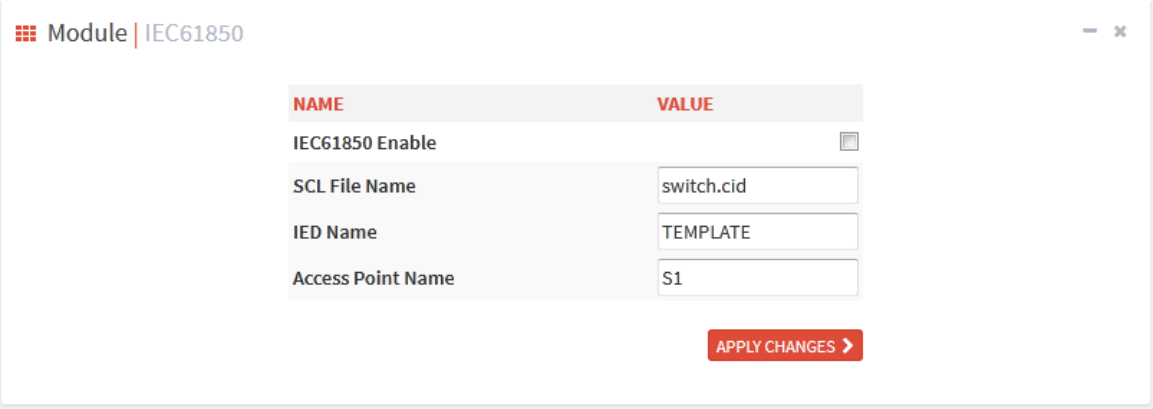


Figure 67 IEC 61850 configuration page

IEC61850 Enable

Configuration options: enable/disable

Default configuration: disable

Function: enable or disable IEC61850.

SCL File Name

Configuration range: 1~25 characters

Default configuration: switch.cid

Function: Specify the modeling file that takes effect when the IEC61850 function is initialized.

IED Name

Configuration range: 1~25 characters

Default configuration: TEMPLATE

Function: Configure logical device name for this IED in the modeling file.

Access Point Name

Configuration range: 1~25 characters

Default configuration: S1

Function: Configure access point name for this IED in the modeling file.

Caution:

Access Point and IED name configuration shall be consistent with the Access Point and IED names in the specified modeling file, otherwise cause the IEC 61850 function startup fails.

6.7 SNMPv2c

6.7.1 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.

6.7.2 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.

6.7.3 Explanation

This series switches support SNMPv2 and SNMPv3. SNMPv2 is compatible with SNMPv1. SNMPv1 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.

SNMPv2 also uses community name for authentication. It is compatible with SNMPv1, and extends the functions of SNMPv1.

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.

6.7.4 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 68 shows the relationships among the NMS, agent, and MIB.

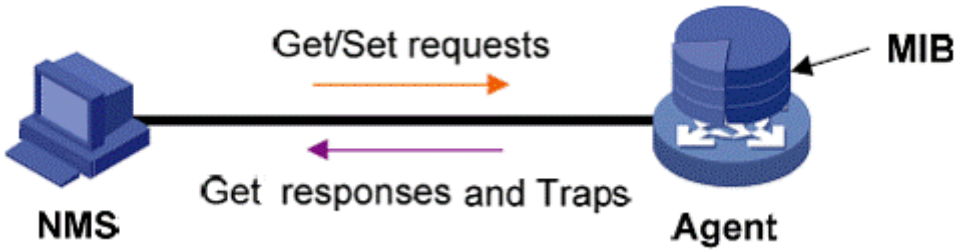


Figure 68 Relationship among NMS, Agent, and MIB

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 69, the OID of object A is 1.2.1.1.

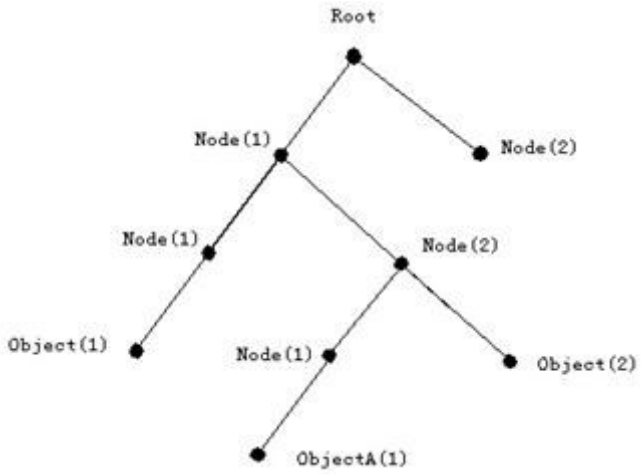


Figure 69 MIB Structure

6.7.5 Web Configuration

1. Enable SNMP protocol, as shown below;

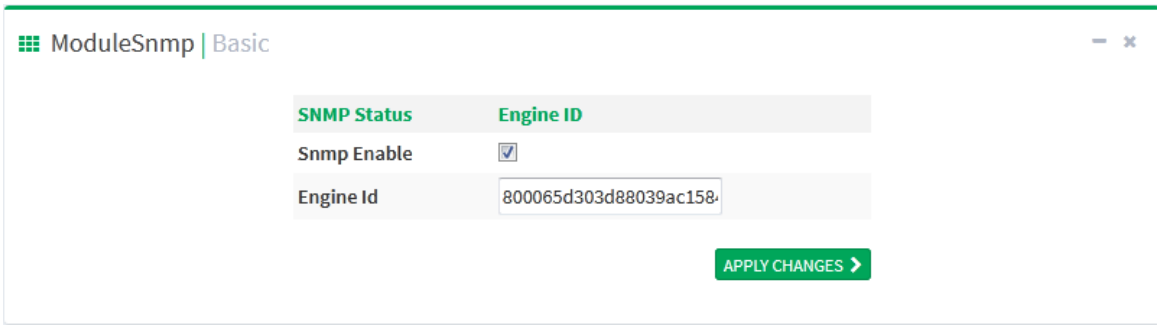


Figure 70 Enable SNMP protocol

SNMP Enable

Configuration options: enable/disable

Default configuration: enable.

Function: enable or disable SNMP protocol.

Engine ID

Configuration range: even number of hexadecimal numbers, can not be full 0 or full F, even number of values range 10~64.

Function: Configure SNMP v3 system engine ID, the device ID corresponding user in the table is deleted when modifying the engine ID.

2. Configure community name, as shown below;

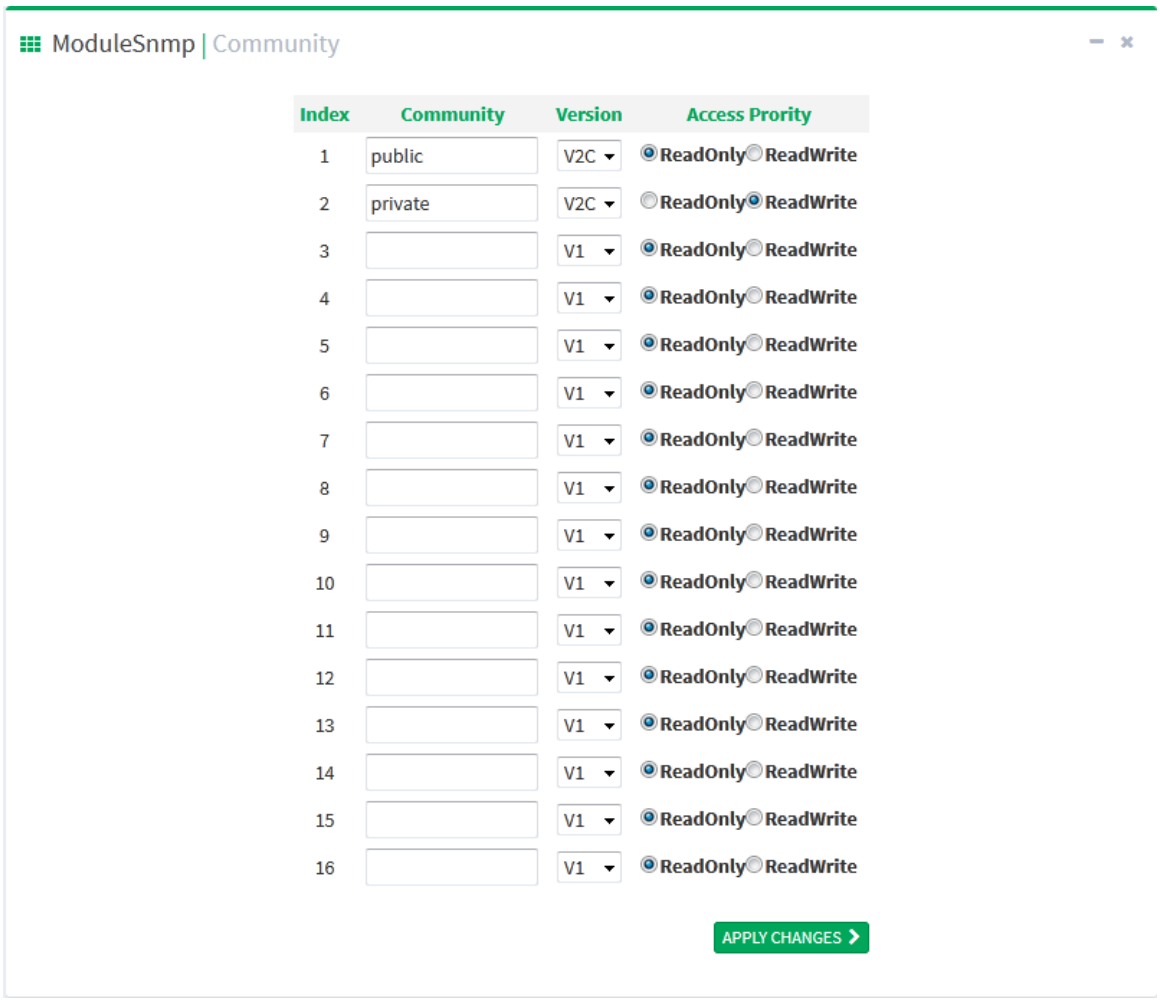


Figure 71 Configure community name

Community

Configuration range: 1~32 characters

Function: Configure community name of switch.

Description: The MIB library information of the switch can be accessed only for the community name in the SNMP message is consistent with the strings of this community.

Expaination: Up to 16 community strings can be configured.

Version

Configuration options: V1/V2C

Function: Select version number of SNMP.

Access Prority

Configuration options: Readonly/ReadWrite

Default configuration: Readonly

Function: Configure the access mode of the MIB library.

Description: ReadOnly permission can only read MIB library information; ReadWrite permissions can read and write mib library information.

3. Configure trap, as shown below;

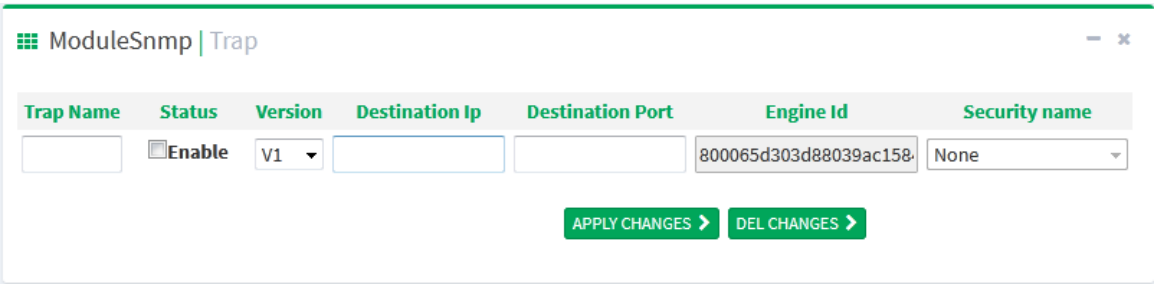


Figure 72 Configure trap

Trap name

Configuration range: 1~32 characters

Function: Configure trap name.

Status

Configuration options: enable/disable

Default configuration: disable

Function: enable or disable trap, the switch sends the corresponding trap message to the server if enable.

Version

Configuration options: SNMP v1/SNMP v2c/SNMP v3

Default configuration: SNMP v1

Function: Configure the trap message version number that the switch sends to the server.

Destination IP

Configuration format: A.B.C.D

Function: Configure the server address to receive trap messages.

Destination Port

Configuration range: 1~65535

Default configuration: 162

Function: Configure the port number for sending trap messages.

6.7.6 Typical Configuration Example

SNMP management station is connected to switch via Ethernet, management station IP address is 192.168.0.23 and switch IP address is 192.168.0.2. NMS monitor Agent through SNMPv2c, read and write the MIB node information of Agent, and send trap message report to the NMS when Agent is failure or error, as shown in the below figure.

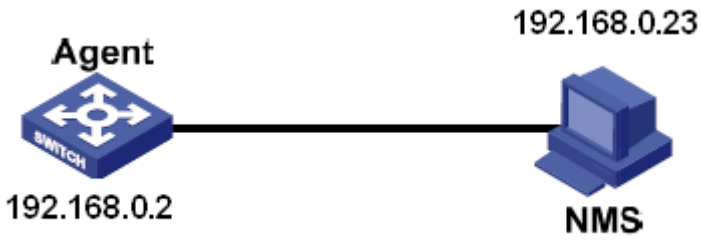


Figure 73 SNMPv2c configuration example

Agent configuration process:

1. Enable SNMP protocol and V2C status, see the Figure 70；

Configure access prority, ReadOnly community name is public, ReadWrite community name is private; see the Figure 71；

2. Enable Trap status, select version to V2C, server IP address is 192.168.0.23, see the Figure 71；

To monitor and manage the status of Agent device, it is necessary to run the corresponding management software at NMS, such as the Kyvision network management software of Kyland.

Kyvision operation of NMS please refer to “Kyvision network management software operation manual”.

6.8 SNMP v3

6.8.1 Introduce

SNMPv3 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.

6.8.2 Implementation

SNMPv3 provides five 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 context table identifies the strings that can be read by users, irrespective of security models.

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, context name, security model, and security level.

6.8.3 Web Configuration

1. Enable SNMP protocol, as shown in below figure;

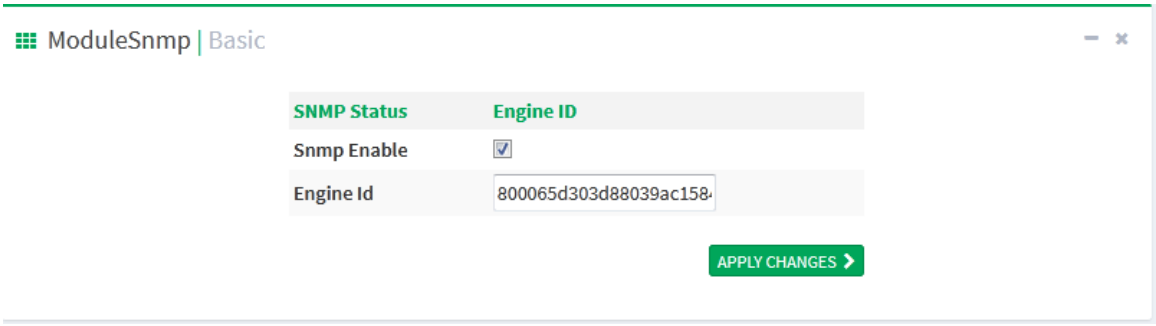


Figure 74 Enabl SNMP protocol

SNMP Enable

Configuration options: Enable/disable

Default configuration: enable

Function: enable or disable SNMP protocol.

Engine ID

Configuration range: Even number of hexadecimal numbers, can not be full 0 or full F, even number of values range 10~64.

Function: Configure SNMP v3 system engine ID, the device ID corresponding user in the table is deleted when modifying the engine ID.

2. Configure trap, as shown below;

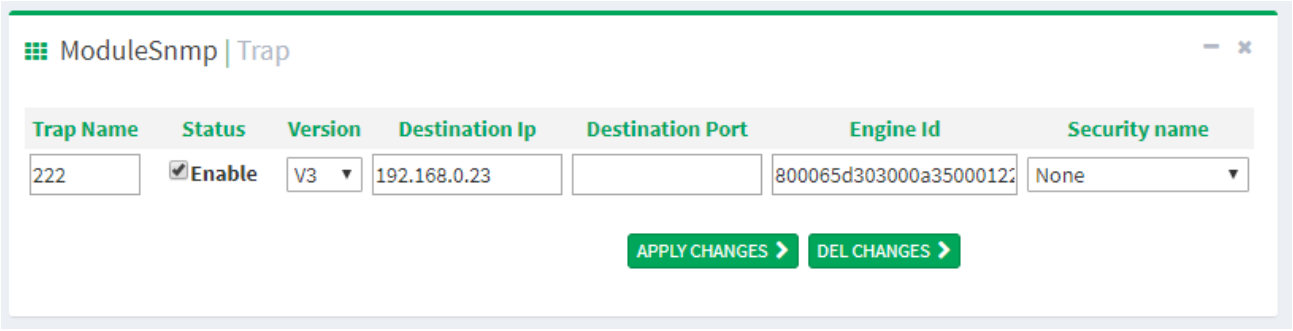


Figure 75 Confgure trap

Trap Name

Configuration range: 1~32 characters

Function: Configure trap name.

Status

Configuration options: enable/disable

Default configuration: disable

Function: enable or disable trap, the switch sends the corresponding trap message to the server if enable.

Version

Configuration options: SNMP v1/SNMP v2c/SNMP v3

Default configuration: SNMP v1

Function: Configure the trap message version number that the switch sends to the server.

Destination IP

Configuration format: A.B.C.D

Function: Configure the server address to receive trap messages.

Destination Port

Configuration range: 1~65535

Default configuration: 162

Function: Configure the port number for sending trap messages.

3. Configure user table, as shown below;

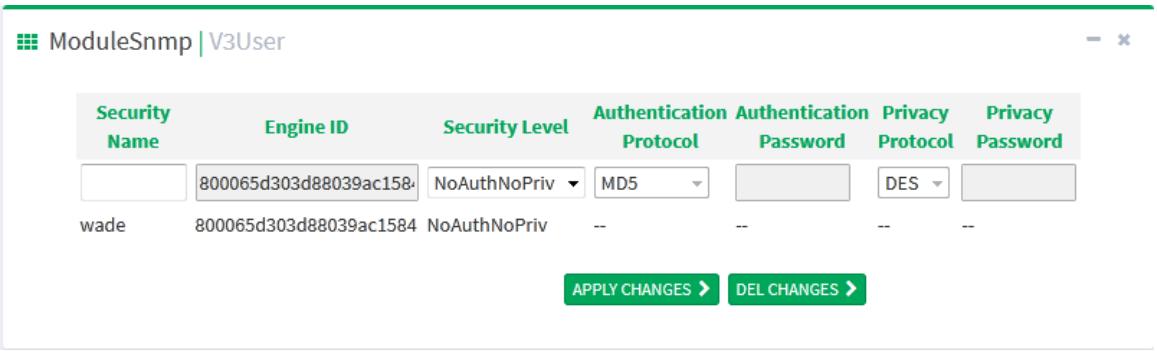


Figure 76 Configure SNMPv3 user table

Security Name

Configuration range: 1~32 characters

Function: Create user name.

Engine ID

Configuration range: Even number of hexadecimal numbers, can not be full 0 or full F, even number of values range 10~64.

Function: Configure security engine ID in SNMP v3 trap message.

Security Level

Configuration options: NoAuthNoPriv/AuthNoPriv/AuthPriv

Function: Configure the security level of the current user.

Description: NoAuthNoPriv need neither authentication nor privacy; AuthNoPriv need authentication but no privacy; AuthPriv need both authentication and privacy.

Authentication Protocol

Configuration options: MD5/SHA

Function: Select an authentication protocol. The authentication protocol and password need to be configured when AuthNoPriv/AuthPriv is selected in security level.

Authentication password

Configuration range: 8~40 characters (MD5 protocol) 8~32 characters (SHA protocol)

Function: Create authentication password.

Privacy Protocol

Configuration options: DES/AES

Function: Select a privacy protocol. The privacy protocol and password need to be configured when AuthPriv is selected.

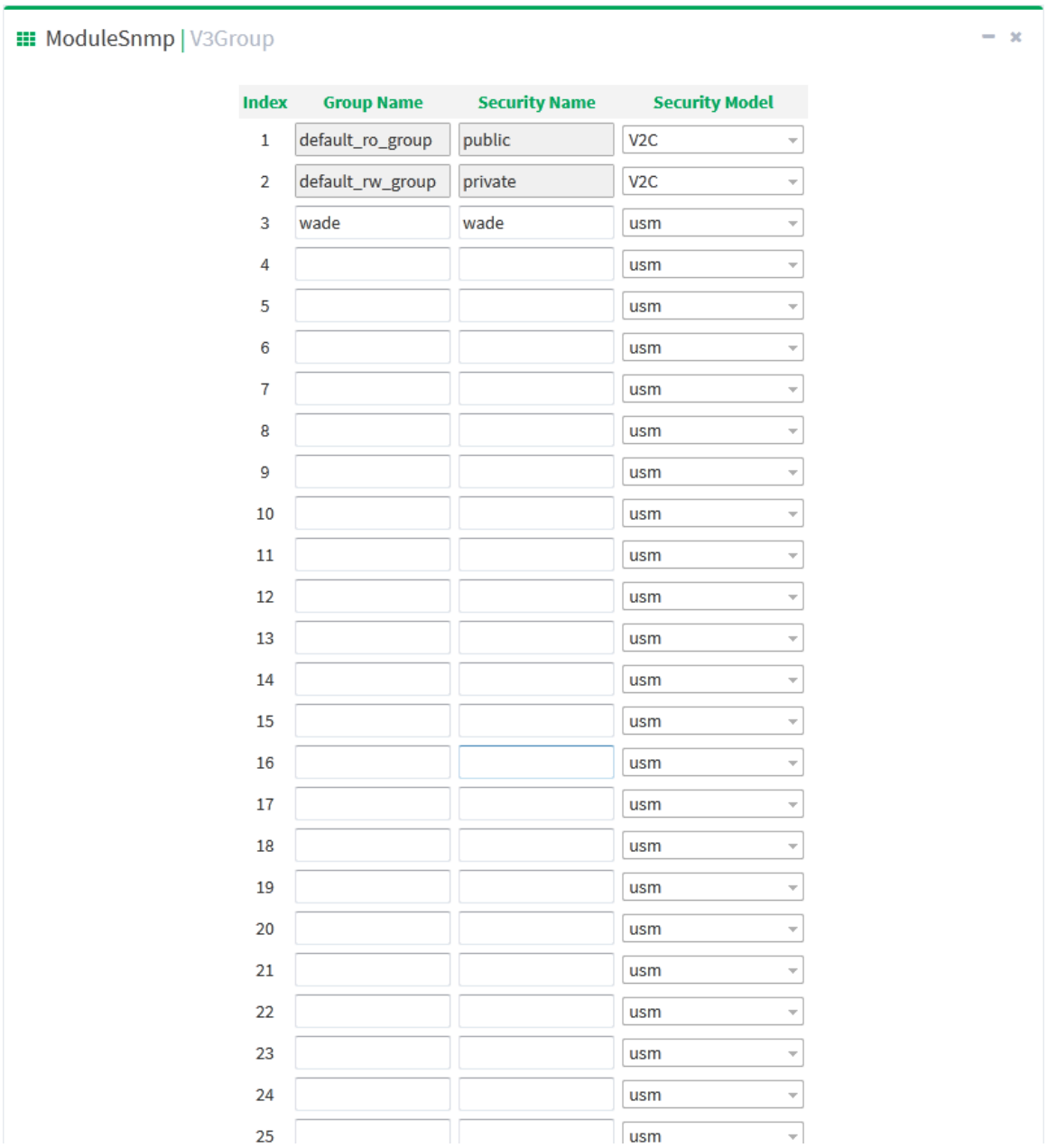
Privacy Password

Configuration range: 8~32 characters

Function: Create privacy password.

Up to 16 users can be configured.

4. Configure group table, as shown below;



Index	Group Name	Security Name	Security Model
1	default_ro_group	public	V2C
2	default_rw_group	private	V2C
3	wade	wade	usm
4			usm
5			usm
6			usm
7			usm
8			usm
9			usm
10			usm
11			usm
12			usm
13			usm
14			usm
15			usm
16			usm
17			usm
18			usm
19			usm
20			usm
21			usm
22			usm
23			usm
24			usm
25			usm

Figure 77 Configure SNMPv3 group table

Group Name

Configuration range: 1~32 characters

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

Security Name

Configuration range: Created username ,1~32 characters

Function: Configure security name, the security name should be consistent with the

user name in the user table. Users with the same group name belong to the same group.

Up to 32 groups can be configured.

Security model

Default configuration: SNMP v3

Function: Select security model of current group (SNMP version number), SNMPv3 uses USM (user-based security model) technology, which is forced to SNMP v3 model.

5. Configure view table, as shown below;

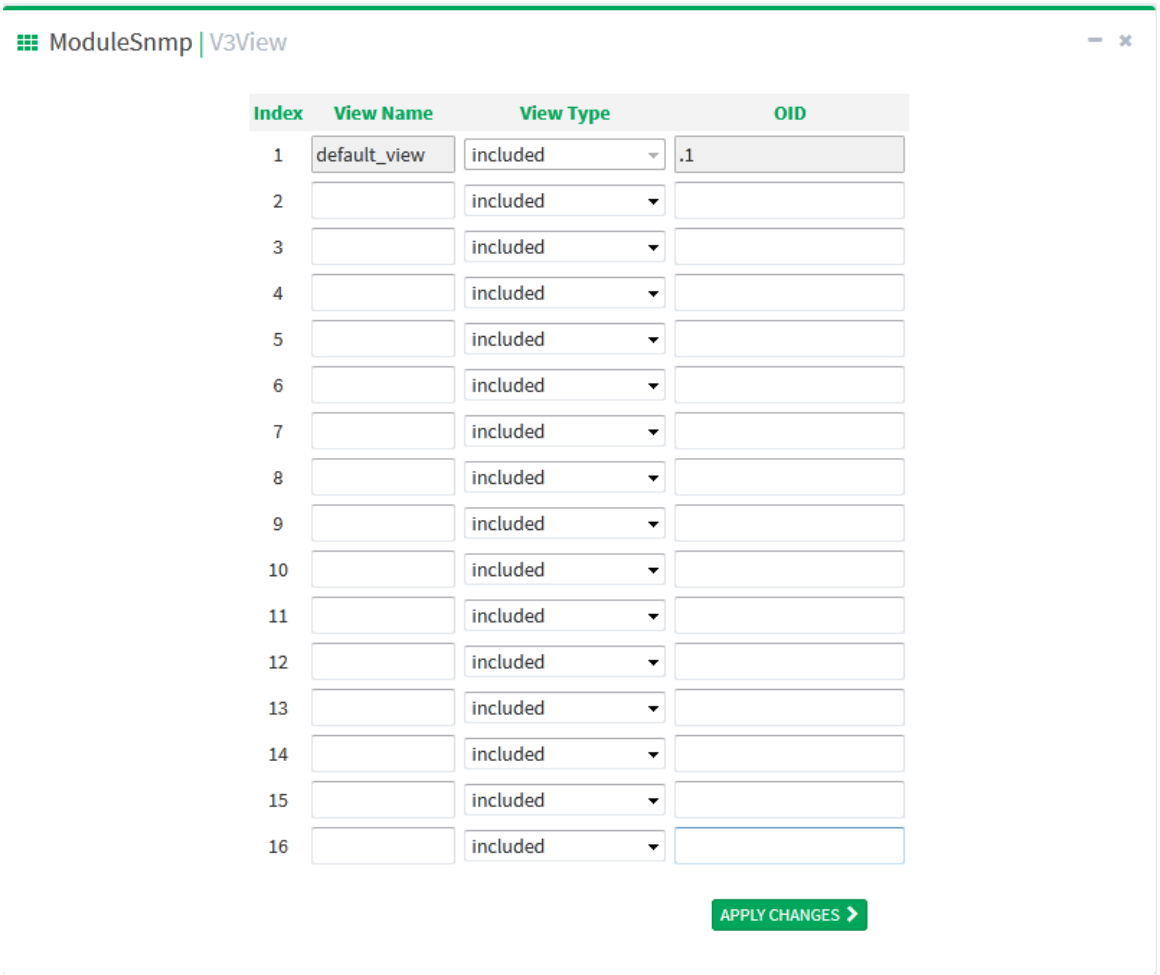


Figure 78 Configure SNMPv3 view table

View Name

Configuration range: 1~32 characters

Function: Configure view name.

View Type

Configuration options: included/excluded

Function: Included represents that the current view includes all nodes of the MIB subtree; excluded represents that the current view does not include any node of the MIB subtree.

OID

Function: Configure MIB subtree, epresented by the OID of the subroot node.

Up to 16 views can be configured.

Note:

The default view table default_view contains all nodes of 1 subtree in the switch.

6. Configure access table, as shown below;

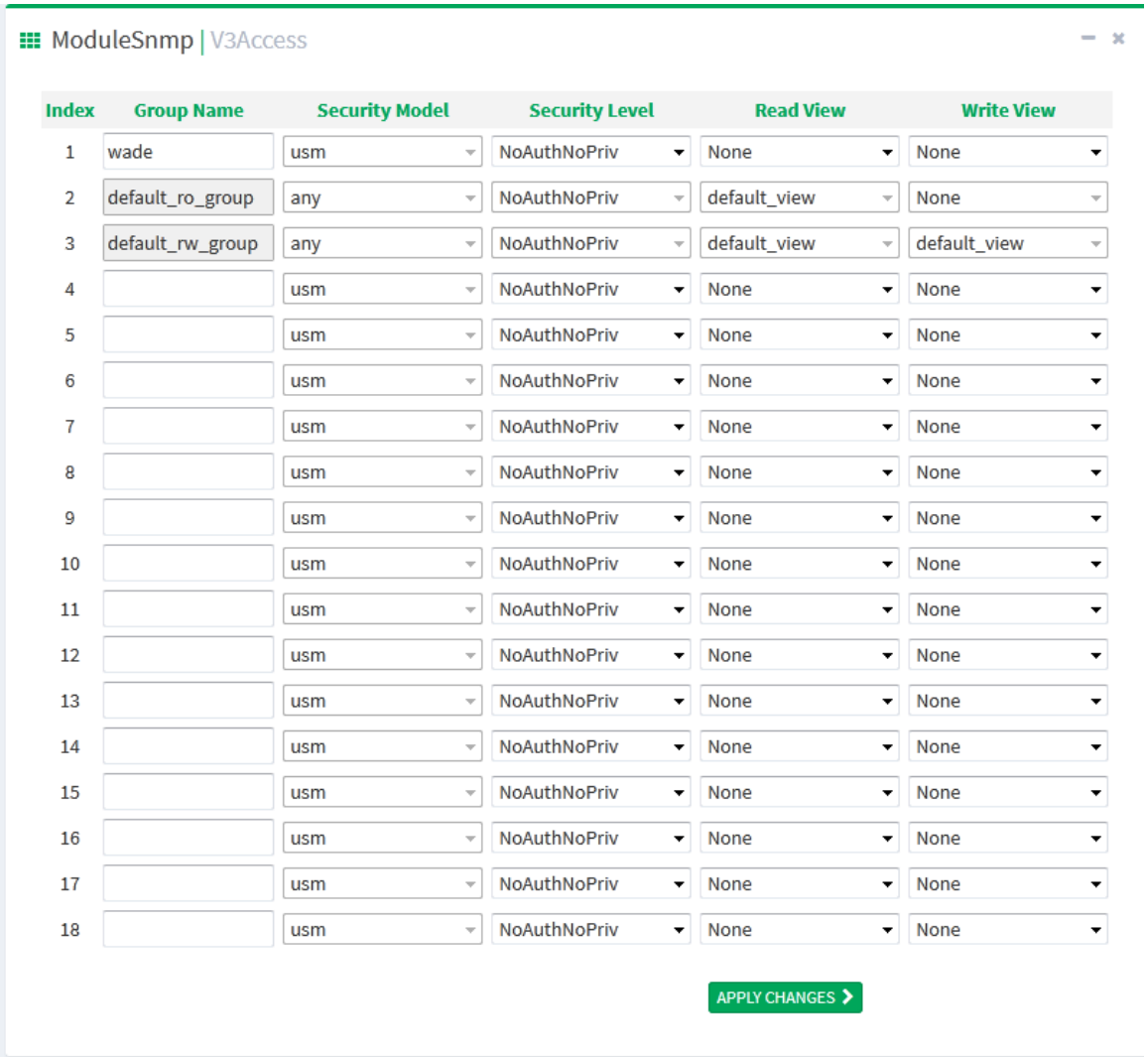


Figure 79 Configure SNMPv3 access table

Group Name

Configuration range: Created group name, 1~32 characters

Description: All users in a group have the same access authority.

Security Model

Default configuration: any/v1/v2/usm

Function: Select security model used when current group access switch (SNMP version number), SNMPv3 uses USM (user-based security model) technology, any means that any security model can be used. Group name, security model should be consistent with group name, security model in group table.

Security Level

Configuration options: NoAuthNoPriv/AuthNoPriv/AuthPriv

Function: Configure security level of current group.

Description: NoAuthNoPriv need neither authentication nor privacy; AuthNoPriv need authentication but no privacy; AuthPriv need both authentication and privacy. If encryption is required, the authentication/privacy protocol, authentication/privacy password on the NMS side should be consistent with the configuration in the user table in order to successfully access the corresponding node information of the switch.

The security of NoAuthNoPriv, AuthNoPriv, AuthPriv Increase in order, Low security level is allowed to access by high security level. For example, the security level of a group is configured to AuthNoPriv, the Users with security levels of AuthNoPriv and AuthPriv in the group can access the switch successfully if both the authentication/privacy protocol and the authentication/privacy password are correct; but users with a security level of NoAuth,NoPriv can not access it.

Read View

Configuration options: default_view/None/Created view name

Function: Select ReadOnly view name.

Write View

Configuration options: default_view/None/Created view name

Function: Select ReadWrite view name.

Up to 16 access tables can be configured.

Note:

Default access tables in the switch {default_ro_group, any, NoAuth,NoPriv, default_view, None}、{default_rw_group, any, NoAuth,NoPriv, default_view, default_view}。

6.8.4 Typical Configuration Example

SNMP management station is connected to switch via Ethernet, management station IP address is 192.168.0.23 and switch IP address is 192.168.0.2. User 1111 and user 2222 monitor and manage the Agent through the SNMPv3, the security level uses authnopriv, all nodes information in Agent can be read only; Agent sends actively the trap v3 message to the NMS when there's an alarm, as shown in the below figure.

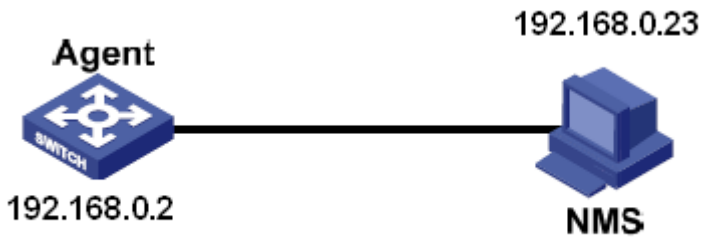


Figure 80 SNMPv3 Configuration example

Agent configuration as below:

1. Enable SNMP protocol, see Figure 70；

2. Configure SNMP v3 user table

User name: 1111, security level: Auth,Priv, authentication protocol: MD5, authentication password: aaaaaaaa, privacy protocol: DES, privacy password: xxxxxxxx；

User name: 2222, security level: Auth,Priv, authentication protocol: SHA, authentication password: bbbbbbbb, privacy protocol: AES, privacy password: yyyyyyyy； see the Figure 76；

3. Create group, security model: usm, include user 1111 and 2222, see the Figure 77；

4. Configure SNMP v3 access table

Group name: group, security model: USM, security level: Auth,NoPriv, read view name: default_view, write view name: None, see the Figure 78;

5. Enable trap model, see the Figure 75;

6. Create trap table item 222, and enable trap model, select version to SNMP v3, destination IP address is 192.168.0.23，select trap event to all event of system, interface, authentication and switch, the others use default configuration;

To monitor and manage the status of agent device, it is necessary to run the corresponding management software at the NMS end.

6.9 File Server

File transfer service can make the file information in client and server backup each other, when the file information of client (server) changes, the backup file can be obtained from server (client) through file transfer based on FTP/SFTP protocol.

The switch can be used either as client or as server to upload and download files through FTP/SFTP protocol.

6.9.1 FTP

Switch as FTP client, first install FTP server, take WFTPD software as an example to introduce the process of uploading and downloading configuration files in FTP server;

1. Click [Security]→[users/rights], Click <New User> button and add FTP new user, as shown in below figure, input username and password, for example, username: admin, password: 123, click <OK>;

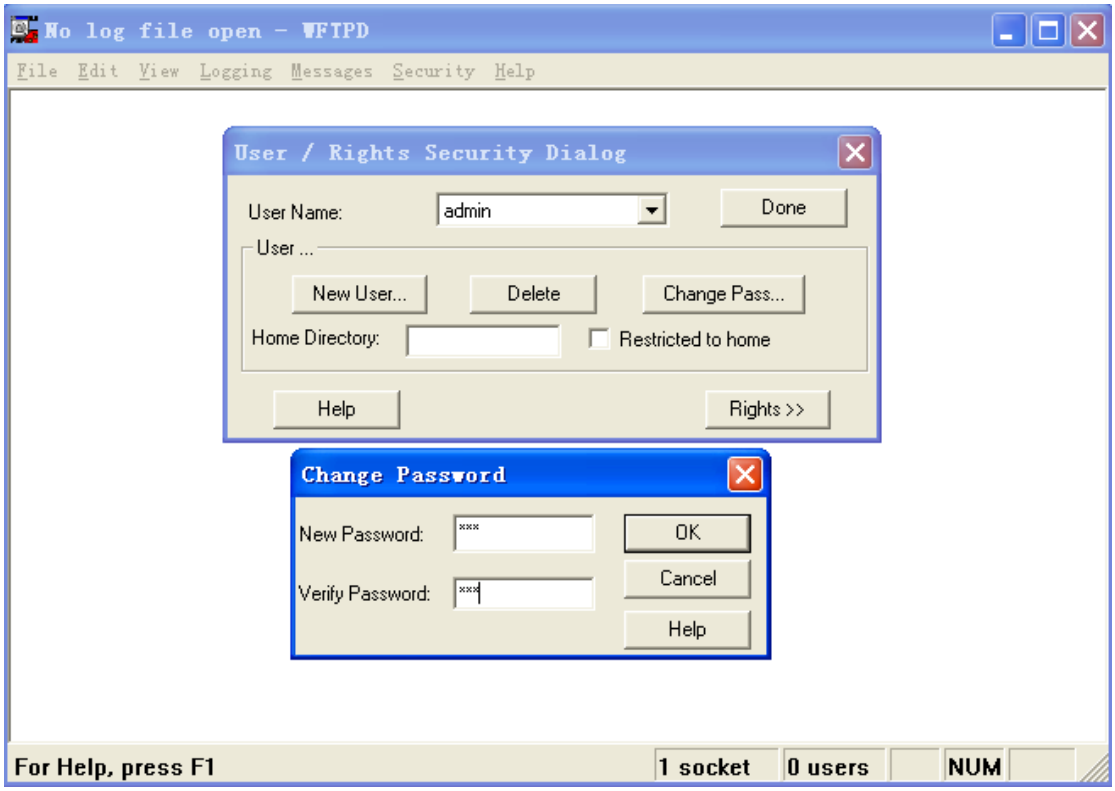


Figure 81 Add FTP new user

2. Enter the storage path of the software version file in the server in the Home Directory bar, as shown in below figure, Click <Done>;

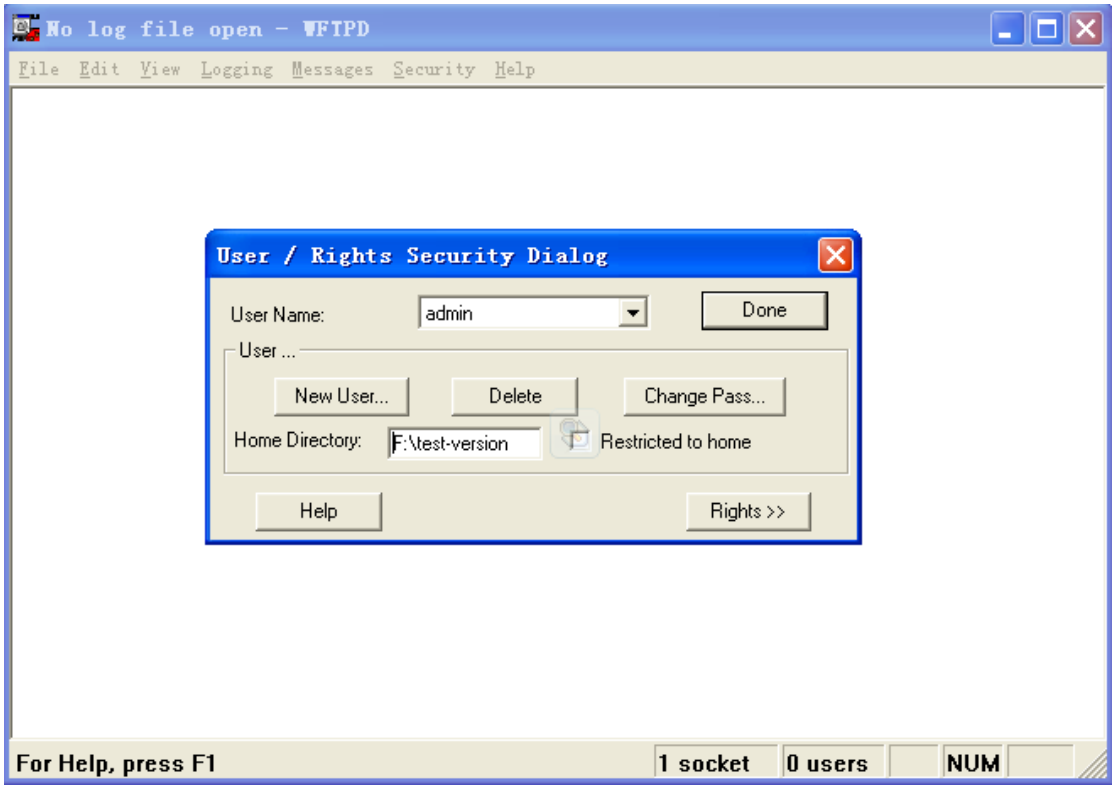


Figure 82 Change file path

3. Click navigation tree [Other Configurations]→[File Server], enter into file transfer service configuration page, as shown in below figure;

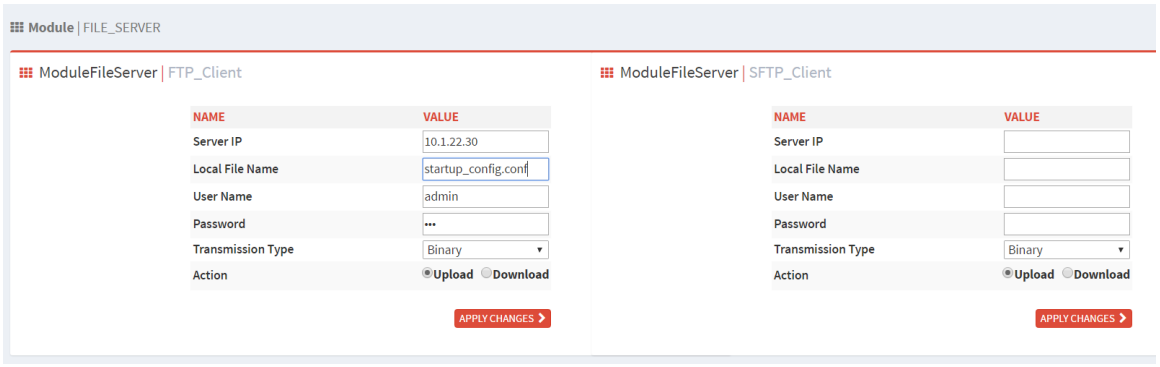


Figure 83 file transfer service configuration

You can configure items of FTP or SFTP protocol. Below is FTP configuration items as client;

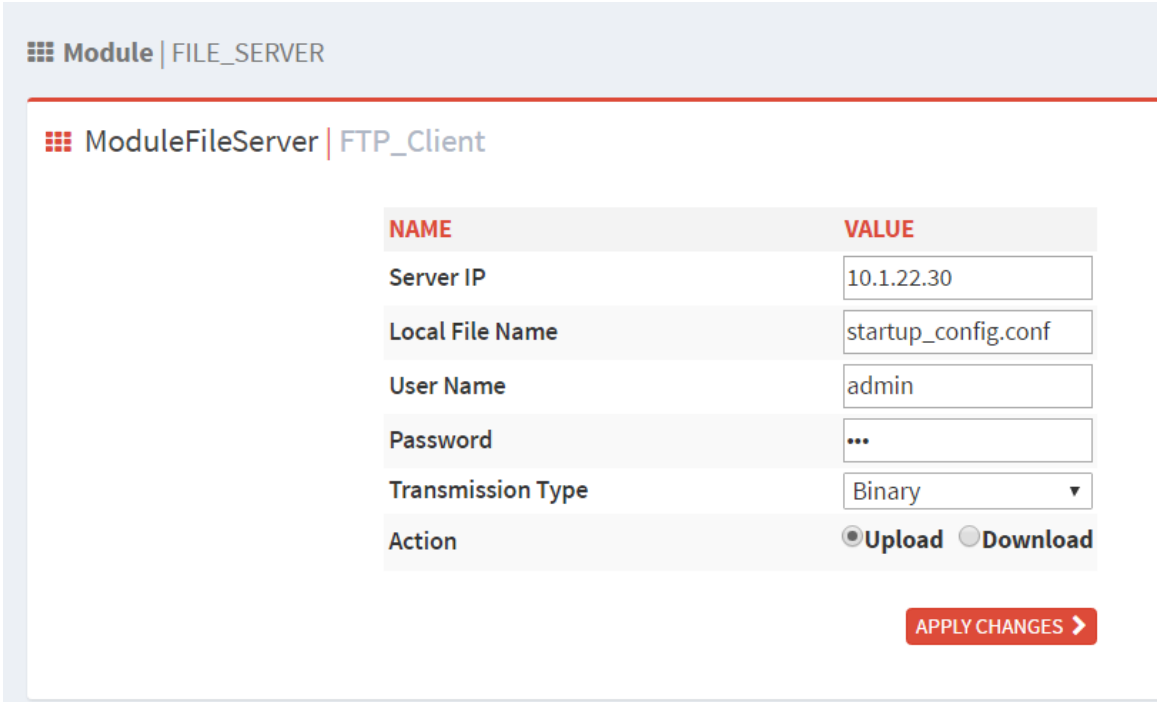


Figure 84 FTP configuration

Server IP

Configuration format: A.B.C.D

Description: Input IP address of server.

Server File Name

Configuration range: 1~100 characters

Description: file name in the server.

User Name

User name in the server

Password

User password

Transmission Type

Configuration options: binary/ascii

Default configuration: binary

Function: Select file transfer standard.

Description: ASCII indicates transfer file with ASCII standard; binary indicates transfer file with binary standard.

Action

Configuration options: update/download

Function: update: Upload the switch configuration file to the remote FTP server directory

Download: Download configuration file from remote FTP server to switch

6.9.2 SFTP

SFTP (Secure File Transfer Protocol) is a file transfer protocol based on SSH, which can encrypt the file and ensure the security of the transmission.

Switch as a SFTP client, first install SFTP server, take MSFTP software as an example to introduce the process of uploading and downloading configuration files in SFTP server;

1. Add SFTP user, as shown in below figure, input User and Password, such as: User: admin, Password: 123; Port is the protocol port number 22 of SFTP; input the server software version file storage path in the Root path bar, click <Start>;

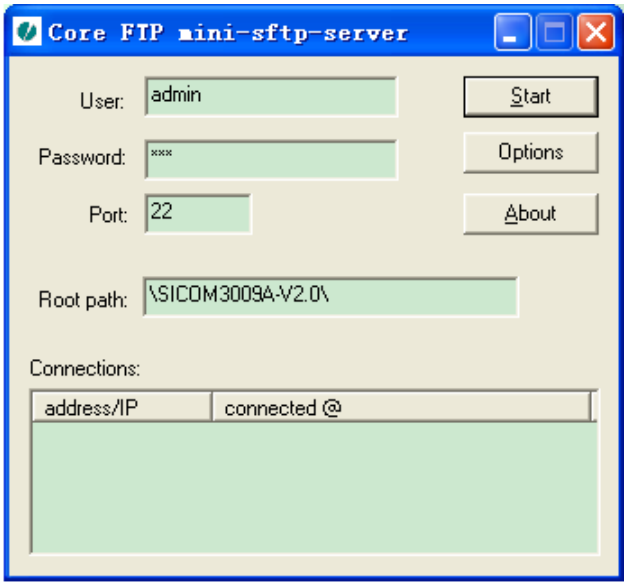


Figure 85 Add SFTP new user

2. Click navigation tree [Other Configurations]→[File Server], enter into file transfer service configuration page, as shown in below figure;

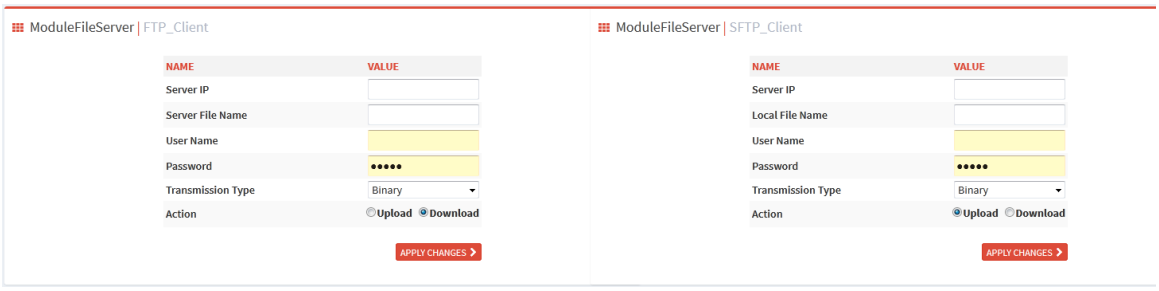


Figure 86 File transfer service configuration

You can configure items of FTP or SFTP protocol. Below is SFTP configuration items as client;

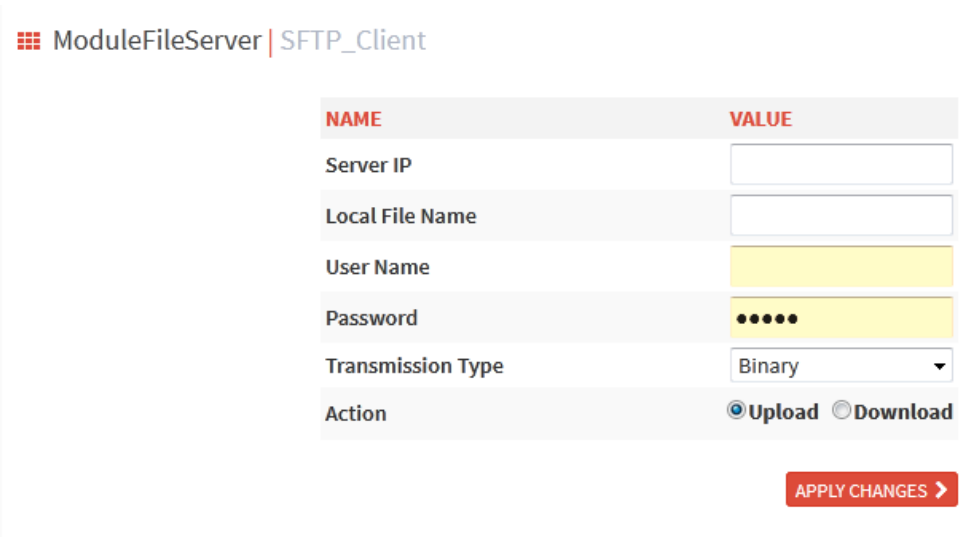


Figure 87 Sftp transfer configuration

Server IP

Configuration format: A.B.C.D

Description: Input IP address of server.

Local File Name

Configuration range: 1~100 characters

Description: file name in the switch.

User Name

User name corresponding to the FTP server

Password

User password

Transmission Type

Configuration options: binary/ascii

Default configuration: binary

Function: Select file transfer standard.

Description: ASCII indicates transfer file with ASCII standard; binary indicates transfer file with binary standard.

Action

Configuration options: update/download

Function: update: Upload the switch configuration file to the remote FTP server

Download: Download configuration file from remote FTP server to switch.

6.10 LLDP

6.10.1 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.

6.10.2 Web Configuration

1. Configure LLDP

Click navigation tree [Other Configurations]→[Lldp], enter into LLDP configuration page, as shown in below figure;

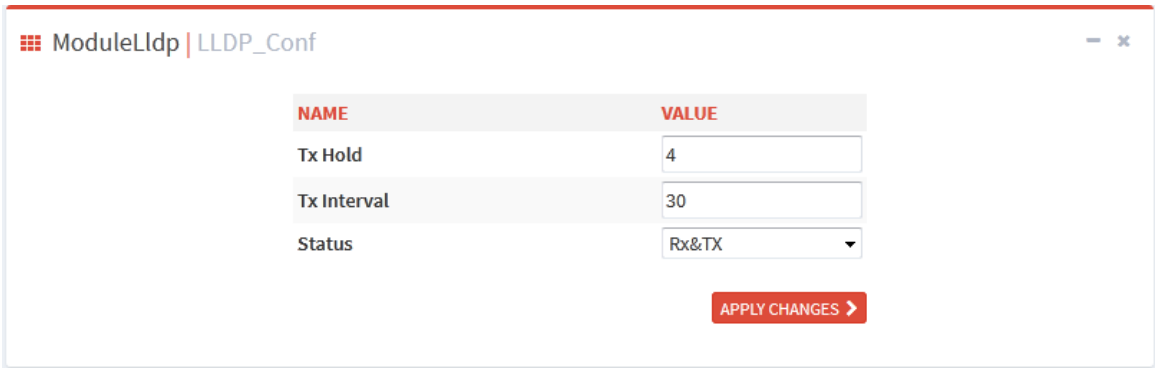


Figure 88 LLDP configuration

Tx Hold

Configuration range: 2~10 times

Default configuration: 4 times

Function: Configure Tx Hold number. Valid time of LLDP message = Tx interval × Tx hold.

Tx Interval

Configuration range: 5~32768s

Default configuration: 30s

Function: Configure the time interval for periodically sending LLDP messages.

Status

Configuration options: Rx&Tx/Disable/RxOnly/TxOnly

Default configuration: Rx&Tx

Function: Configure LLDP message status. Rx&Tx means that the switch not only sends LLDP messages, but also receives and recognizes LLDP messages. Disable means

that the switch neither sends LLDP messages nor receives LLDP messages; RxOnly means that the switch only receives and recognizes LLDP messages and does not send LLDP messages; TxOnly means that the switch only sends LLDP messages and does not receive LLDP messages.

2. View LLDP information, as shown in below figure;

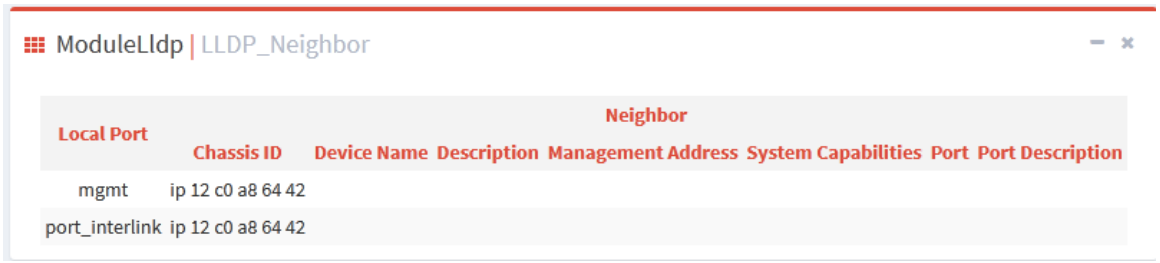


Figure 89 LLDP information

6.11 DDMI

6.11.1 Introduction

Digital Diagnostic Monitor Interface optical module (DDMI) is also called intelligent module, optical module by adding chip and auxiliary circuit design, network management unit can monitor the temperature of transceiver module, supply voltage, laser bias current and transmit and receive optical power in real time. These parameters can help the management unit to find out the location of the fault in the optical fiber link, simplify the maintenance work and improve the reliability of the system.

6.11.2 Web Configuration

Click navigation tree [Other Configurations]→[Ddmi], enter into DDMI configuration page, as shown in below figure;

Figure 90 L port optical module information

Take L port as an example, after inserting the optical module, we can read the basic information of the optical module. This information includes basic information such as vendor, part number, serial number, revision, transmission distance and transceiver. Some pluggable optical modules also support more advanced information queries, including temperature, voltage, Tx bias, Tx power and Rx power.

6.12 Virtual Cable Test

6.12.1 Introduction

VCT (Virtual Cable Tester) uses Time Domain Reflectometry (TDR) to detect Twisted-pair status. It transmits a pulse signal to the cable and detects the reflection of the pulse signal to detect the cable fault. If a failover occurs in the cable, parts of or all pulse energy will be reflected back to the sending source when the transmitted pulse signal reaches the end of the cable or the fault point, and VCT technology can measure the signal arrival time at the fault point and the time of getting back to the sending source, then calculates the distance according to the time.

VCT technology can detect the media of link connecting the Ethernet copper ports and send back the detection result. VCT can detect the following types of cable faults:

Short: it means short circuit. It is that two or more wires are shorted.

Open: it means open circuit. There might be broken wires on the cable.

Normal: it means normal cable connection.

Imped: it means impedance mismatch. For example, the impedance of the Cat.5 cable is 100 ohm, the impedance of the terminators at the both ends of the cable must be 100 ohm to avoid wave reflection and data error.

Fail: it means VCT test fails.

6.12.2 Web Configuration

Click navigation tree [Other Configurations]→[Virtual Cable Test], enter into VCT configuration page, as shown in below figure;

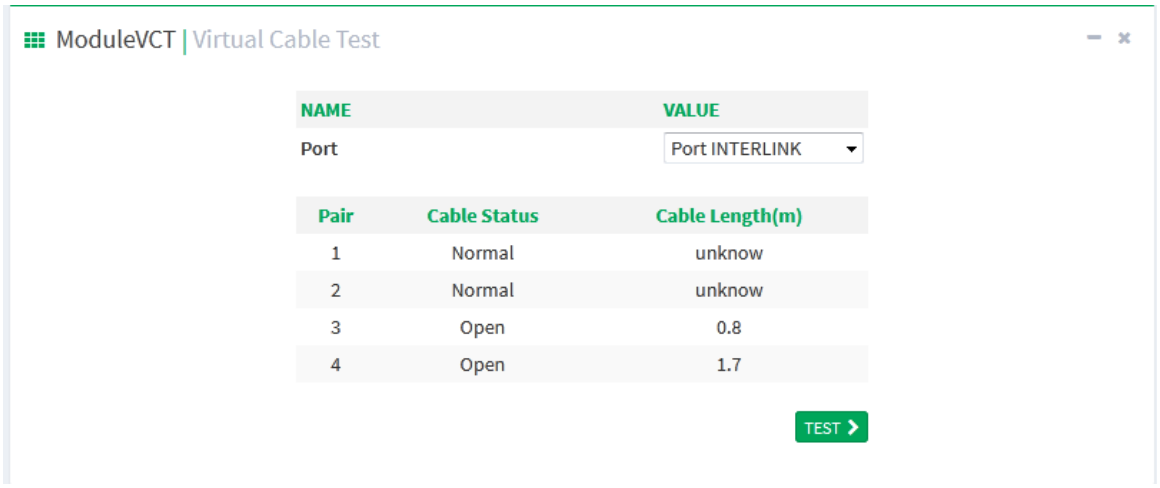


Figure 91 VCT configuration page

Port

Configuration range: port_a/port_b/port_interlink

Default configuration: port_a

Function: Select the corresponding port to detect the cable.

After selecting the port, click the [TEST] button to test cable connection, as shown above.

Pair

Number of cable pairs, a pair is two copper wires.

Cable Status

There is three status with Normal/Open/Short.

Normal: Cable connection is normal

Open: There may be broken lines in the cable.

Short: Two or more wires are short connected together.

Cable Length(m)

The approximate distance of the fault point from the switch port, the unit is meter. If the cable is normal, the cable length shows Unknown.

6.13 RADIUS

6.13.1 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 92 shows the structure.

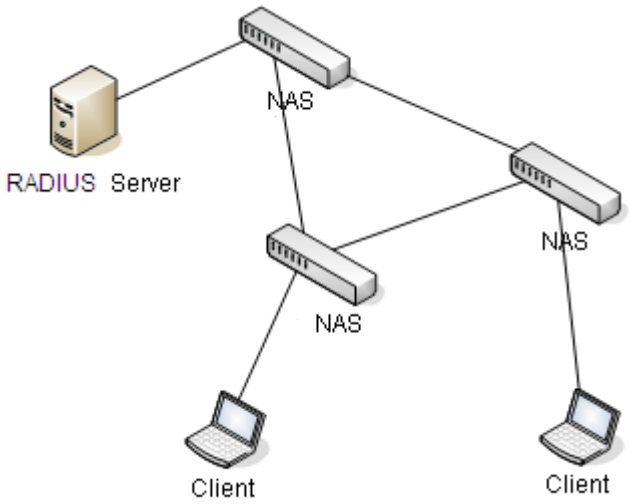


Figure 92 RADIUS Structure

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.

6.13.2 Web Configuration

1. Configure RADIUS authentication

Click navigation tree [Other Configurations]→[Radius], enter into RAIDUS configuration page, as shown in below figure;

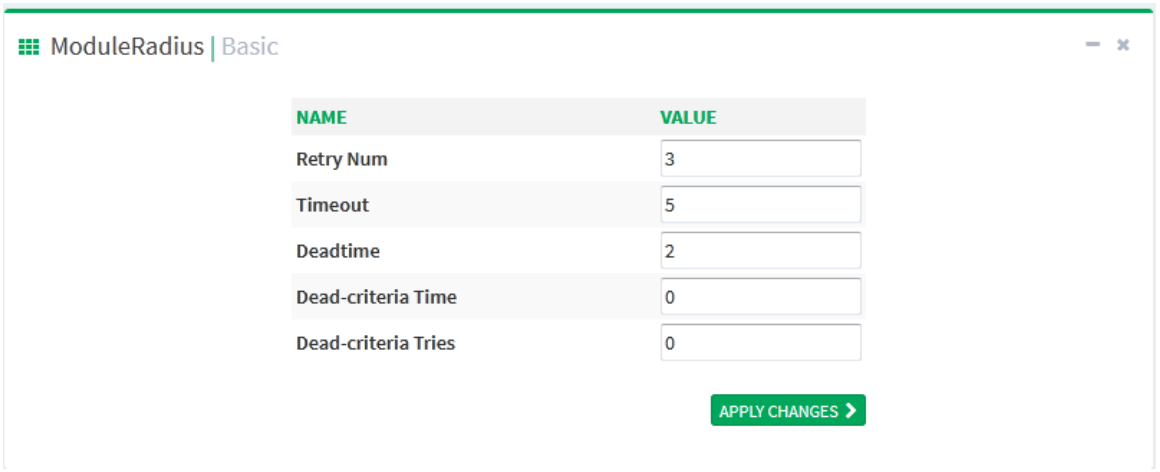


Figure 93 RADIUS authentication parameter configuration

Retry Num

Configuration range: 1~3

Default configuration: 3

Function: Configure RADIUS retry number for message timeout. If the total retry number exceeds configuration value and the RADIUS server still does not respond, the device will determine this authentication failure.

Timeout

Configuration range: 1~3s

Default configuration: 3s

Function: Configure RADIUS server reply timeout; after the device sends RADIUS

request message, if no response from the RADIUS server is received during this period, the request message is retried.

Deadtime

Range: <1-1440>

Default: 2

The server needs to be set to close for some time when the Radius server is determined to be invalid. After the deadtime arrives, the Radius server returns to a valid state. This reduces the number of requests to an invalid server.

Dead-critecria Time

Range: <3-120>

Default: 0

Function: Number of timeout seconds.

Description: By setting the server's timeout limit to determine whether the server is invalid.

Dead-critecria Tries

Range: <1-100>

Default: 0

Function: Retry number

Description: By setting the server's retry number limit to determine whether the server is invalid.

2. RADIUS server configuration, as shown in below figure;

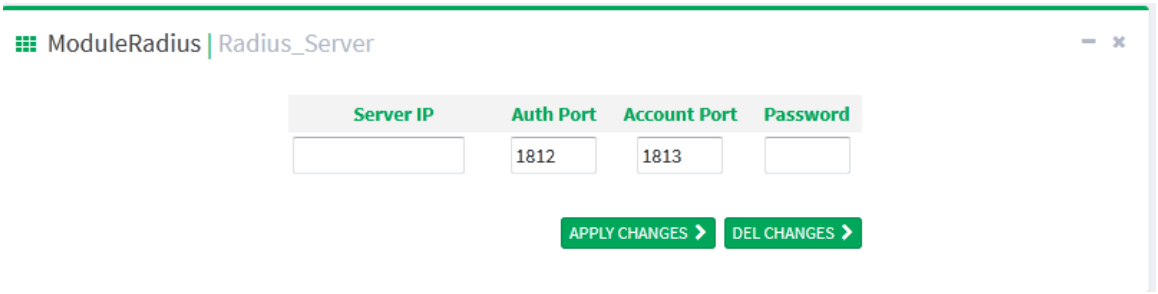


Figure 94 RADIUS server configuration

Server IP

Configuration format: A.B.C.D

Function: Configure IP address of RADIUS server, up to support 5 RADIUS server.

Auth Port

Configuration range: 1~65535

Default configuration: 1812

Function: Configure UDP port number of RADIUS server.

Account Port

Configuration range: 1~65535

Default configuration: 1813

Function: Configure UDP port number of RADIUS server.

Password

Configuration range: 1~32 characters

Function: Configure password of RADIUS server.

6.13.3 Typical Configuration Example

1. Topology graph

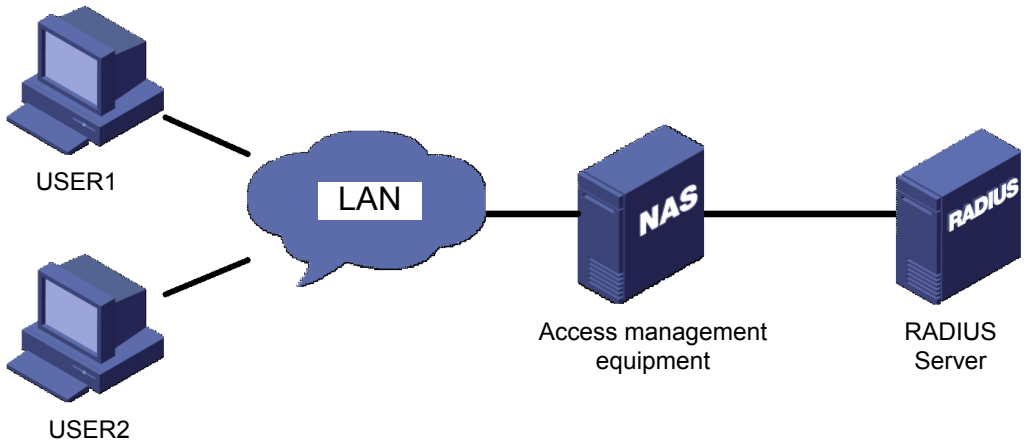


Figure 95 Typical network

2. Configuration requirements

a. User login to management device through line vty0 with AAA authentication;

b. Radius authentication and account server IP address is 192.168.1.1, authentication port is 1812, account port is 1813, authentication key is test;

3. Please refer to 6.13.2 web page configuration example.

6.14 TACACS Plus

6.14.1 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 96 shows the structure.

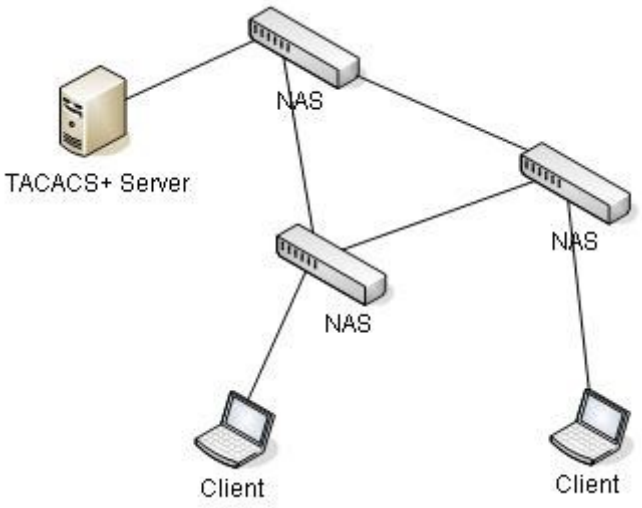


Figure 96 TACACS+ Structure

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.

6.14.2 Web Configuration

1. Enable TACACS+ protoccl

Click navigation tree [Other Configurations]→[Tacacs plus], enter into TACACS+ configuration page, as shown in below figure;

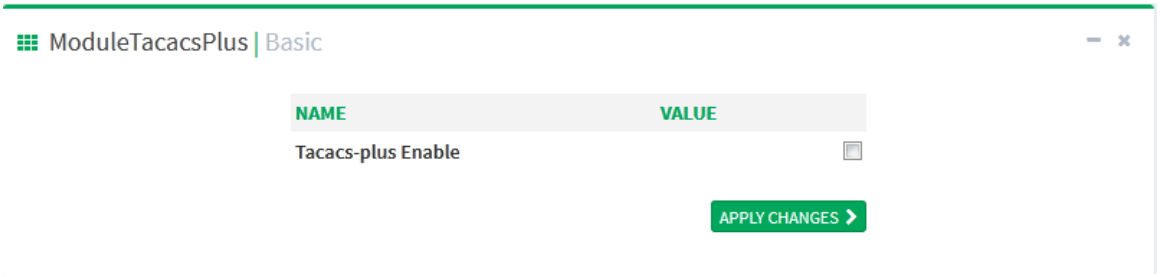


Figure 97 Enable TACACS+ protocol

Tacacs-plus Enable

Configuration options: Enable/disable

Default configuration: Disable

Function: Enable or disable TACACS+ protocol.

2. TACACS+ Server configuration, as shown in below figure;

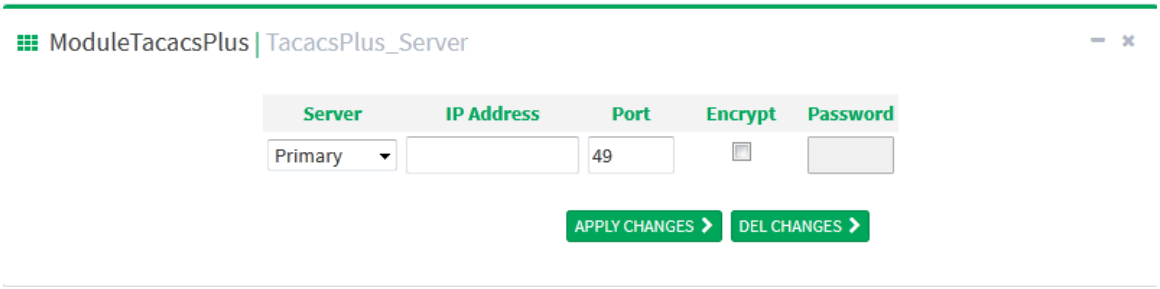


Figure 98 TACACS+ server configuration

Server

Configuration options: Master server/Slave server

Default configuration: Master server

Function: Select server type of current configuration.

IP address

Configuration format: A.B.C.D

Function: Input IP address of server.

Port

Configuration range: 1~65535

Default configuration: 49

Function: Port number of receiving NAS authentication request.

Encrypt

Configuration options: Enable/disable

Default configuration: Disable

Function: Enable or disable encryption, need to input encryption key if enable.

Password

Configuration range: 1~32 characters

Description: Configure the key to improve the security of the client's communication with the TACACS+ server. Both client and server can verify the legitimacy of the message by sharing the key of the device. Only when the key is consistent, both receive the message sent by the other and respond to each other, so it is necessary to ensure that the sharing key configured on the device is exactly the same as the key on the TACACS+ server.

After the configuration is complete, the server configuration information is displayed in the server list below, as shown below;

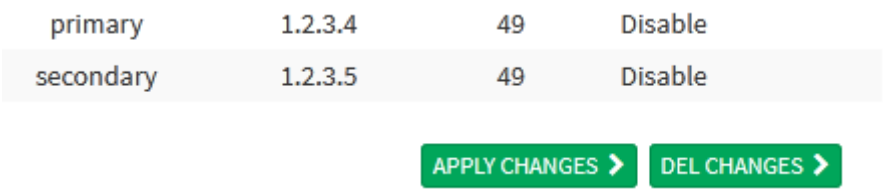


Figure 99 Server configuration list

6.14.3 Typical Configuration Example

As shown in below figure, TACACS+ authenticate and authorize to user through switch. Server IP address is 192.168.0.23, the sharing key is aaa when the switch interacts message with the server.

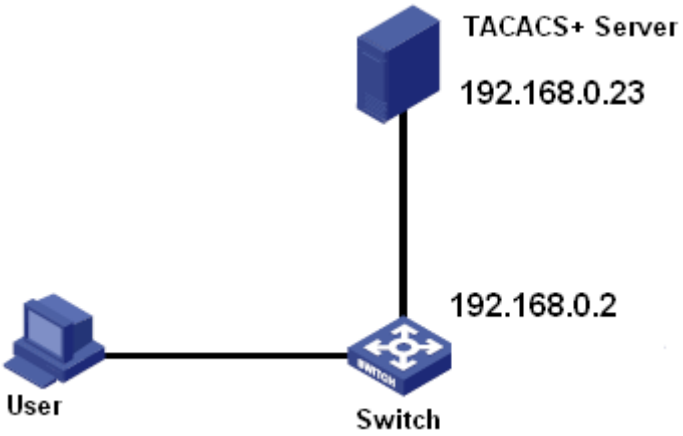


Figure 100 TACACS+ authentication example

Please refer to 6.14.2 tacacs+ web page configuration.

6.15 AAA

6.15.1 AAA Introducation

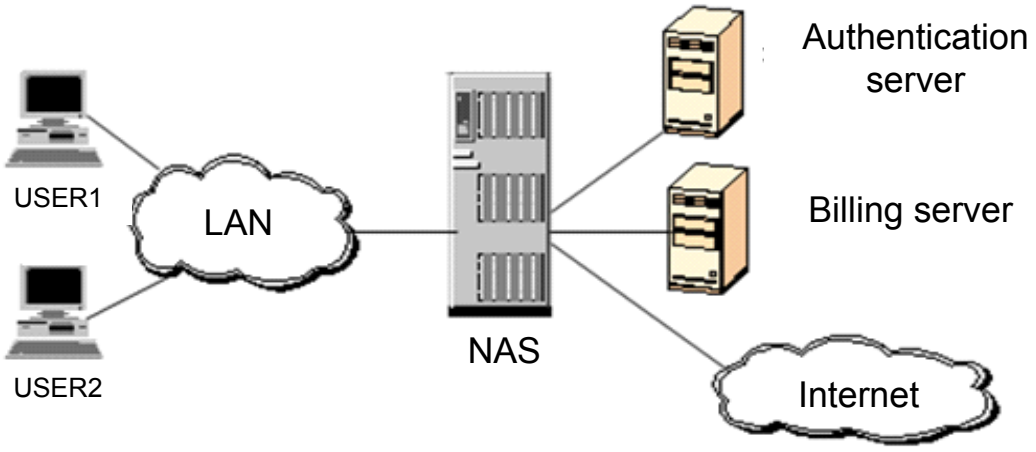


Figure 101 AAA Structure

In order to improve the security of the network, it is necessary to control the permissi onof the resources in the network. AAA protocol can provide authentication, authorizat ion and account services, to effectively solve network resources security and account problems.

AAA have 2 parts to implement services: AAA module for handling access requests o f user and RADIUS module for providing AAA services.

AAA have 2 parts to implement services: AAA management framework for handling a ccess requests of user and RADIUS client for handing AAA services.

AAA management framework: It interact directly with the user,manage the AAA services required by the user and the information of the requesting user; At the same time, sending the user's request to a specific AAA server (such as RADIUS).

AAA management framework in the process of providing AAA access, authentication is a necessary process to verify the legitimacy of users; Authorization services (optional)can be performed only after certification has been passed only after the authentication passed

authorization is AAA server provide the necessary information of user access to nas device, so that users can access the network successfully; account service (optional) register the successful authentication of users or count traffic.

RADIUS client: Realize the data interaction between AAA user and RADIUS server. RADIUS client converts the user's AAA request into RADIUS protocol message, which is sent to the RADIUS server; the RADIUS server sends the user's request result to the RADIUS client again, RADIUS client resolves the request result, feedbacks to the AAA management framework, and finally the user gets the request result.

6.15.2 Web Configuration

1. Enable AAA

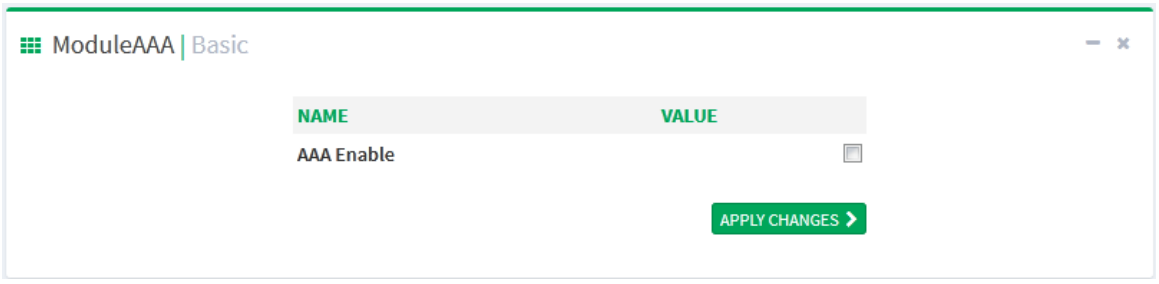


Figure 102 Enalbe AAA

The global switch of AAA, only enable AAA, the related services of AAA can the configured. AAA services previously applied will become invalid If disable AAA, Configure the login mode to access switch and the authentication mode and authentication sequence.

2. Authentication Configuration

Click navigation tree [Other Configurations]→[AAA], enter in the login authentication configuration page, as shown in below figure;

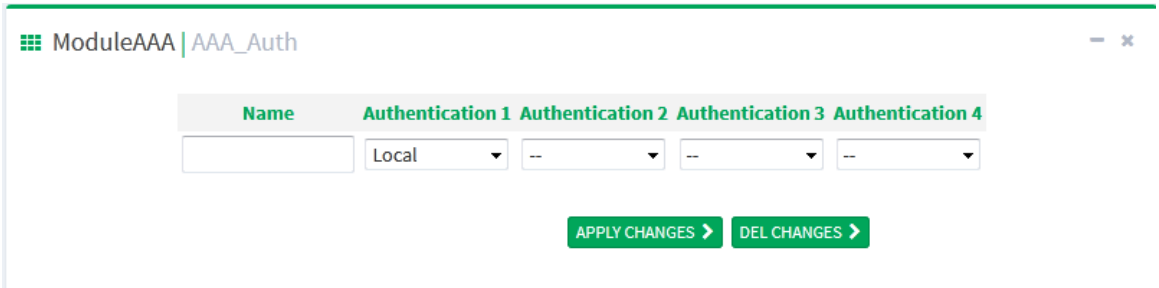


Figure 103 Login authentication configuration

Authentication Name

Configuration options: Telnet/Web/dot1x/SSH

Function: Select the login mode to access the switch.

Authentication 1/ Authentication 2/ Authentication 3/ Authentication 4

Configuration options: Local/Tacacs+/Radius/None

Default configuration: Local

Function: Select the order of login authentication, first use authentication 1 for authentication; if it does not pass, then use authentication 2; if the first two authentication does not pass, use authentication 3; if all previous authentication fail, use authentication mode 4.

Description: Local means using local created username and password for authentication; Tacacs+ means using created username and password in Tacacs+ server for authentication; Radius means using created username and password in Radius server for authentication.

6.16 LINE

6.16.1 Introducation

Line as the logical interface of terminal management, is divided into two types: line console and line vty. line console corresponds to console login, line vty corresponds to generic login protocols, including telnet. Both types line configurations are basically the same, both types are supported without special instructions.

6.16.2 Web Configuration

Click navigation tree [Other Configurations]→[Line], enter into login authentication configuration page, as shown in below figure;

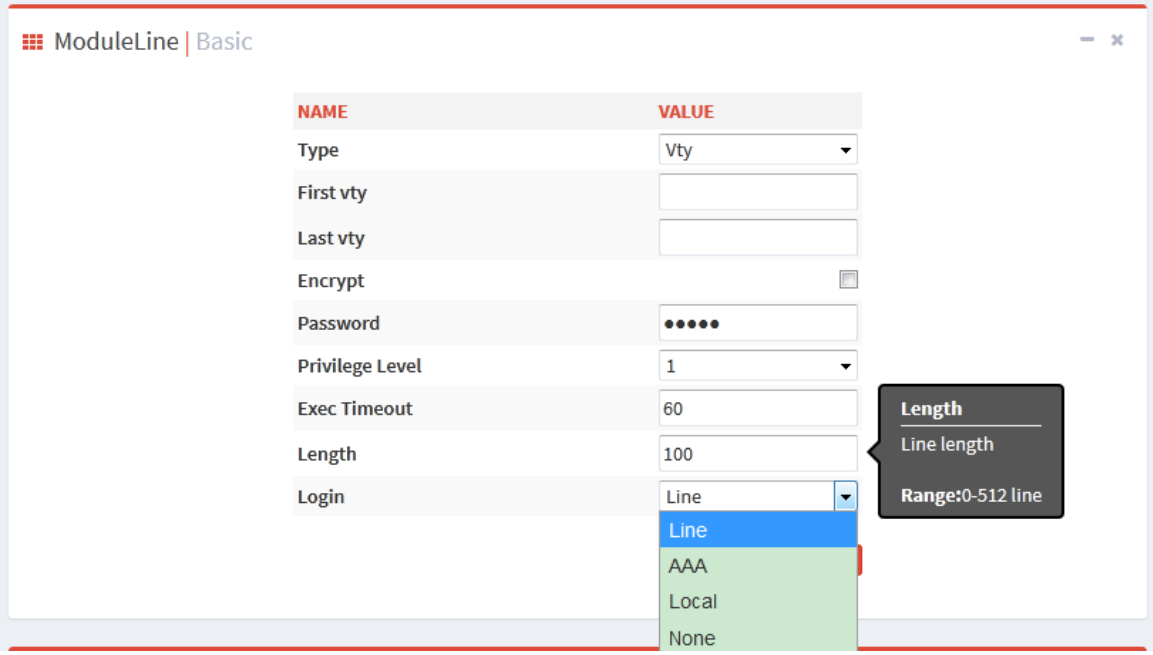


Figure 104 line configuration page

Type

Configuration options: console/vty

Function: Select login mode remotely of switch

Console: Console port login.

Vty corresponds to generic login protocols including telent.

Vty Id

Configuration options: 0-9

Default configuration: 0

Function:

1. Line type is console, vty value default as 0, configure to Console port.

2. Line type is vty, we need to configure first-vty or last-vty.

first-vty: The first line vty ID, Range: 0-9

last- vty: The last line vty ID, Range: 0-9

Only configure *first-vty* means only configure one line vty; Configure *last-vty* means configure all line from *first-vty to last-vty*.

Encrypt

Configuration options: Plaintext encryption/ ciphertext encryption

Default configuration: Plaintext encryption

Function: Default password is admin，uncheck Encrypt means plaintext encryption; check encrypt means ciphertext encryption. The private encryption algorithm tool is provided to generate ciphertext. The command is rypt 7.

Password

Configuration options: Plaintext password/ciphertext password

Plaintext password length is 1-64 characters, ciphertext password length range is 1-129 characters

Default configuration: plaintext password with admin

Privilege level

Configuration options: Range is 0-15

Default configuration: 1

Function: When configuring the line authentication mode, the console/telnet authentication permission is controlled by the line permission.

Exec timeout

Configuration options: Range: <0-86400>, unit is second

Default configuration: 60

Function: Configure time for idle timeout after login user terminal. Ternial no timeout if 0

Length

Configuration options: <0-512>

Default configuration: 100

Function: Configure the maximum number of output rows in screen.

Login

Configuration options: line/aaa/local/none

Line: Use the configuration of authentication with password in line interface to login.

Aaa: Use the configuration of authentication with user and password in AAA to login.

Local: Use the configuration of authentication with username and password in local user management configuration to login.

None: No authentication.

Default configuration: line

Function: Configure the authentication mode when the terminal login.

7 Switch Maintenance

Click navigation tree [Switch Maintenance]， select pop-up option to operate.

The following options allow the device save configuration and recovery the default factory configuration.

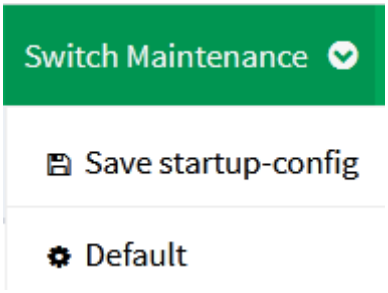


Figure 105 save startup-config and recovery default configuration

8 Network Nodes

Click navigation tree [Network Nodes] to view network node information of device, as shown in below figure;

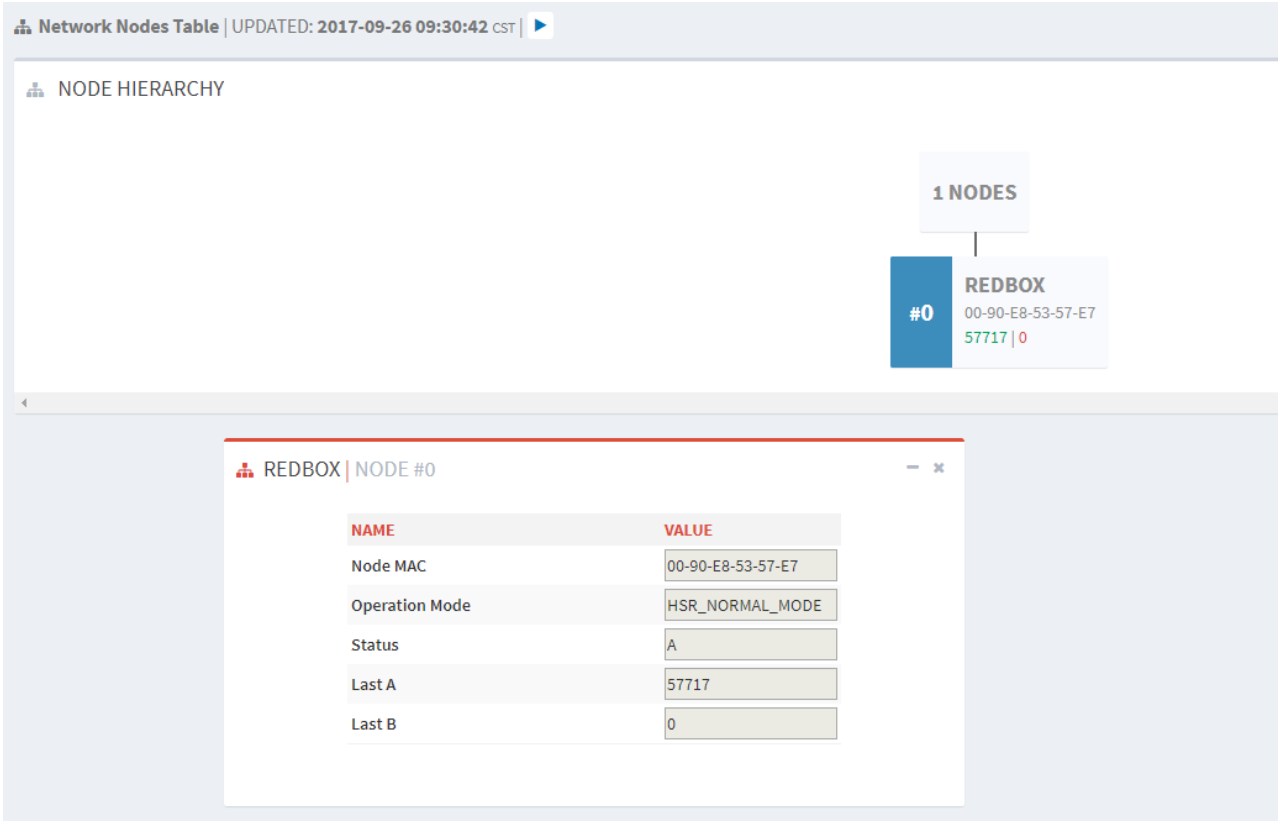


Figure 106 Network node

The top diagram shows the current device networking situation, NODES is the local device, REDBOX is remote device, connect to the local device through A port, the remote device's mac address and the statistics of received and transmitted message of port can be seen from the diagram.

It more clearly shows the device networking situation in REDBOX table as below.

Node MAC

Description: MAC address of remote device.

Operation Mode

Description: Operation mode of device.

Status

Description: the interface between the remote device and local device, option can be

A/B/A&B.

Last A

Description: Message statistics of A port

Last B

Description: Message statistics of B port.

Appendix List of abbreviations

Abbr.	Full
BC	Boundary Clock
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
DST	Daylight Saving Time
E2ETC	End-to-End Transparent Clock
FTP	File Transfer Protocol
GPS	Global Positioning System
HTTP	Hyper Text Transfer Protocol
IED	Intelligent Electronic Device
LLDP	Link Layer Discovery Protocol
LLDPDU	Link Layer Discovery Protocol Data Unit
MIB	Management Information Base
NTP	Network Time Protocol
OC	Ordinary Clock
OID	Object Identifier
P2PTC	Peer-to-Peer Transparent Clock
PTP	Precision Time Protocol
RADIUS	Remote Authentication Dial-In User Service
RTC	Real Time Clock
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SSL	Secure Sockets Layer
TACACS+	Terminal Access Controller Access Control System
TC	Transparent Clock