PoE+ Series Switches Technical White Paper

NETWORK SOLUTION

Models: S3150-8T2FP
S3260-8T2FP
S3260-16T4FP
S3400-24T4FP
S3400-48T4SP
S5500-48T8SP

TECHNICAL WHITE PAPER

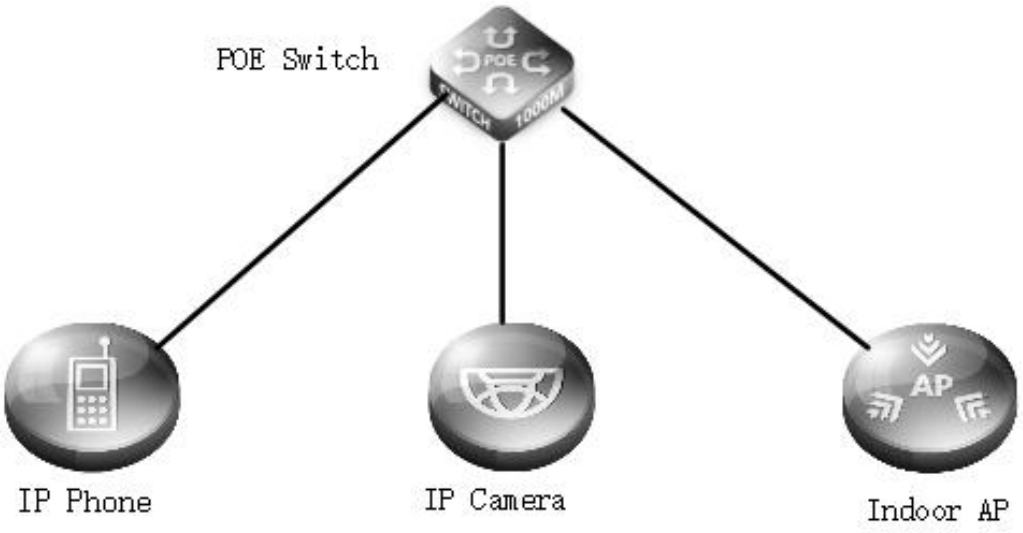
Contents

1. PoE Power Supply Principle

1.1 PoE Power Supply Principle Introduction

PoE (Power over Ethernet) refers to the technology that can transmit data signals for some IP based terminals (such as IP phone, Wireless LAN access point AP, webcam, etc.) while provides DC power supply technology for such equipment under the circumstances that the existing Ethernet Cat.5 cabling infrastructure has no changes. PoE technology can ensure the security of the existing structured cabling while the operation of the existing network is normal and the cost is minimum.

In PoE system, the equipment providing power is called Power Supply Equipment (PSE), and the equipment using power is called Powered Device (PD). As shown in the figure below, PoE switch is PSE, other IP phones, indoor AP, cameras, etc. are PD.



PoE technology is widely used in home applications, wireless networking, security protection, retail, entertainment and other scenes because of its easy installation, easy management, security and stability. Currently, PoE based on 802.3af standard can provide up to 15.4W power, and PoE+ based on 802.3at standard can provide up to 30W power.

Category	PoE	PoE+
Standard	802.3af	802.3at
Power Supply Distance	100m	100m
Classification	0 ~ 3	0 ~ 4
Maximum Current	350mA	600mA
PSE Output Voltage	44 ~ 57VDC	50 ~ 57VDC

Category	PoE	PoE+
PSE Output Power	<=15.4W	<=30W
Cable Requirements	Unstructured	CAT-5e or better
PD Input Voltage	36 ~ 57VDC	42.5 ~ 57VDC
PD Maximum Power	12.95W	25.5W
Power Supply Cable Pair	2	2

PoE Advantages:

Reliability: centralized power supply, convenient backup.

Simple connection: the network terminal does not need external power supply, only needs a network cable.

Standard: it conforms to IEEE 802.3af standard and IEEE 802.3at standard, and uses a global unified power interface, which can ensure the interaction with PD of different manufacturers.

1.2 Power Supply Process on PoE Equipment

The steps to achieve PoE power supply are as follows:

1. Detection of PD: the small voltage limited by the periodic output current of PSE at the port is used to detect the presence of PD equipment. If a resistance with a specific resistance value is detected, the cable terminal is connected to the receiving terminal equipment supporting IEEE 802.3af standard or IEEE 802.3at standard.

2. Power Supply Capacity Negotiation: PSE classifies PD and negotiates power supply. There are two ways to negotiate the power supply capacity: analyzing the specific resistance detected and negotiating the power supply capacity through lldp protocol.

3. Start Power Supply: during the start-up period (generally less than 15 μs), PSE equipment starts to supply power from low voltage to PD equipment until providing 48V DC voltage.

4. Normal Power Supply: after the voltage reaches 48V, PSE provides stable and reliable 48V DC power for PD equipment. When PSE equipment only supports PoE and PoE+, the power consumption of PD equipment shall not exceed 30W.

5. Power Off: during the power supply process, PSE will continuously monitor the PD current input. When the PD current consumption drops below the minimum value, or the current surges, such as unplugging the equipment or encountering PD equipment power consumption overload, short circuit, power supply load exceeding PSE, PSE will disconnect the power supply and repeat the test process.

1.3 Power Management Description of PoE Equipment

PoE switch provides real-time power management function, which will be managed according to PD real-time power. For example, the customer selects S3400-48T4SP PoE device, which has 48 ports PoE/PoE+ power supply capacity, providing 370W PoE power supply capacity, and can calculate how many ports can be provided through the table below. The switch is powered according to the power consumption management port of PD, not 30W for each port.

PD Power Waste	Cable Transmission Loss	Number of Power Supply Ports Available
12.95W	2.45W	24
25.5W	4.5W	12

2. Fallible Scene Process

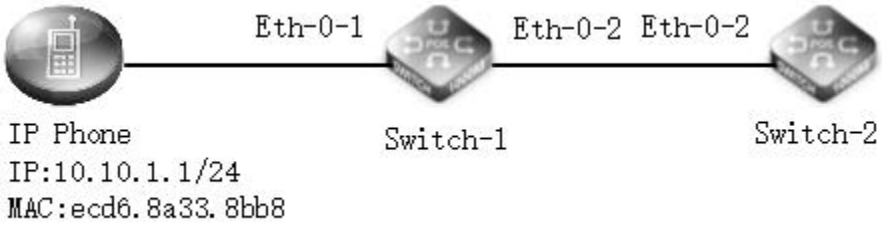
2.1 Application Scene of Voice VLAN

2.1.1 Issue Description

Before configuring Voice VLAN, you must create corresponding VLAN. VLAN1 is the default VLAN, so it cannot be set as Voice VLAN.

IP phone does not support the protocol to obtain the Voice VLAN information configured on the switch. The voice VLAN based on MAC address can be configured.

2.1.2 Topology Information



2.1.3 Handling Process

Voice VLAN function can divide voice data flow into specified VLAN. Users can add the port connecting voice equipment to voice VLAN by creating Voice VLAN, which can make voice data centralized in voice VLAN for transmission, facilitate targeted QoS configuration of voice flow, improve the transmission priority of voice traffic, and ensure voice quality.

1) The data sent by the IP phone is added to the Voice vlan, and the packet priority is set to 7.

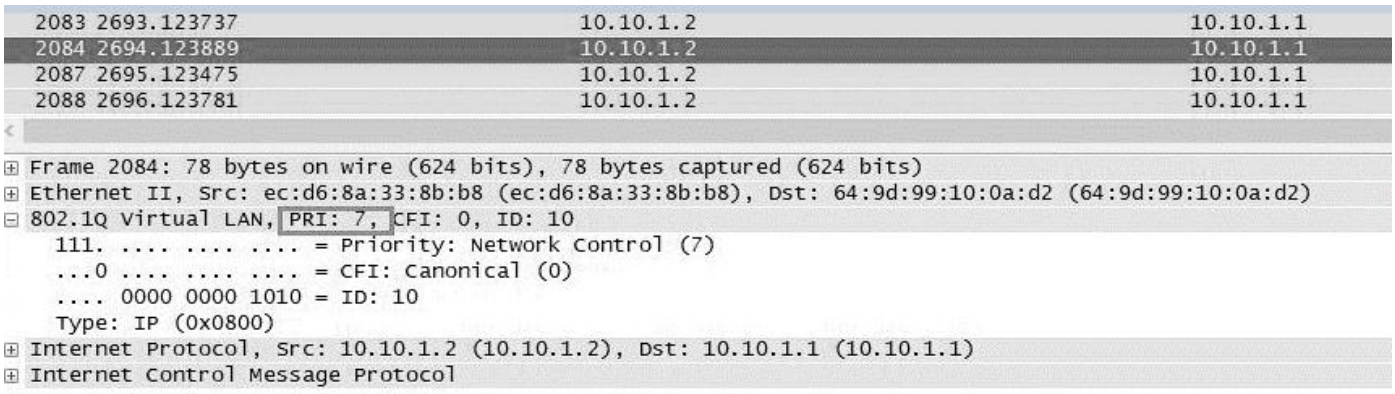
Switch-1: Config

```
48PoE_config#vlan 10
48PoE_config_vlan10#exit
48PoE_config#int gigaEthernet 0/1
48PoE_config_g0/1#switchport mode trunk
48PoE_config_g0/1#switchport voice-vlan 10 cos 7  (Voice VLAN default priority 6)
48PoE_config_g0/1#int gigaEthernet 0/2
48PoE_config_g0/2#switchport mode trunk
48PoE_config_g0/2#exit
48PoE_config#voice-vlan mac-address ecd6.8a33.8bb8 mask ffff.ffff.ffff (The MAC address here is the Mac address of the IP phone)
```

Switch-2: Config

```
48PoE_config#vlan 10

48PoE_config_vlan10#exit

48PoE_config#int vlan 10

48PoE_config_v20#ip add 10.10.1.2 255.255.255.0

48PoE_config_vlan20#exit

48PoE_config#int gigaEthernet 0/2

48PoE_config_g0/2#switchport mode trunk

48PoE_config_g0/2#switchport trunk allowed vlan all
```

2) Send ping packet to IP phone with Switch-2, grab packet on Switch-2, and check that the priority of Voice VLAN configuration is 7 on the package of 802.1Q.



2.1.4 Root Cause

When configuring voice VLAN, you need to create corresponding VLAN (not vlan1).

When IP phone sends voice data without VLAN Tag, you need to configure Voice VLAN based on MAC address matching on the PoE switch.

2.1.5 Solution

1. When configuring voice VLAN, you need to create a new VLAN. Vlan1 cannot be configured as voice VLAN.

2. When the IP phone does not support lldp protocol to obtain voice VLAN information, the voice VLAN based on MAC address can be configured.

2.1.6 Suggestions and Conclusions

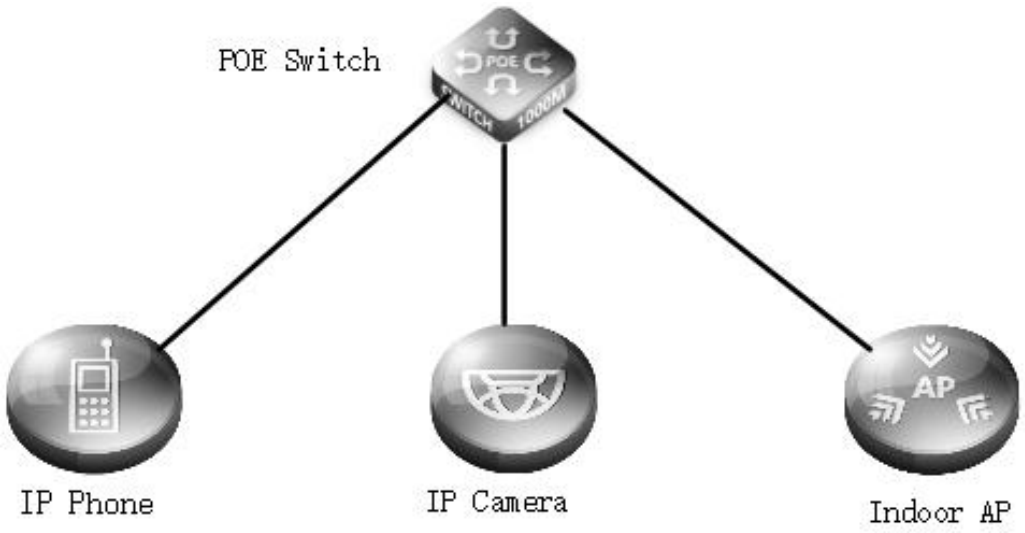
When configuring the voice VLAN function, you need to pay attention to creating a new VLAN; when accessing the IP phone, you can configure Voice VLAN based on MAC address matching as required.

2.2 Access Scene of PD (AP, IP phone, camera, etc.)

2.2.1 Issue Description

When S3400-48T4SP switch is connected to AP, camera, IP phone and other devices, it is necessary to check whether the powered equipment supports 802.3af/at standard. If yes, use RJ45 network cable to connect the powered device and make it work normally. If not, check the operating instructions of powered device and supply power in the correct way.

2.2.2 Topology Information



2.2.3 Handling Process

1) Access to non-standard (not support 802.3af/at standard) power receiving equipment of PoE switch

PoE switch is connected to non-standard power receiving equipment. You can view PoE power supply information at the corresponding port of PoE device, and connect to non-standard power receiving equipment. After the port is tested, this port will not turn on PoE power supply function.

```
48PoE#show PoE interface gigaEthernet 0/36 (view power supply details of specified port)
```

2) Access to standard (support 802.3af/at standard) power receiving equipment of PoE switch

PoE switch is connected to standard power receiving equipment. After inspection, it will classify the power receiving equipment and provide corresponding power to ensure that the power receiving equipment can work normally.

```
48PoE#show PoE interface gigaEthernet 0/36 (view power supply details of specified port)
```

Turn down port PoE power supply

```
48PoE#_config_g0/36#PoE disable (Turn down port PoE power supply)
```

2.2.4 Root Cause

When S3400-48T4SP switch is connected to non-standard power receiving equipment, in order to prevent excessive power supply voltage from damaging the power receiving equipment, PoE power supply function of corresponding port will be closed.

2.2.5 Solution

Before connecting the PoE switch to the power receiving equipment, first check the product introduction of the power receiving equipment to see whether the product supports the PoE power supply standard (802.3af / at). If not, please use the power supply method supported by the product manual to avoid damage to the power receiving equipment.

2.2.6 Suggestions and Conclusions

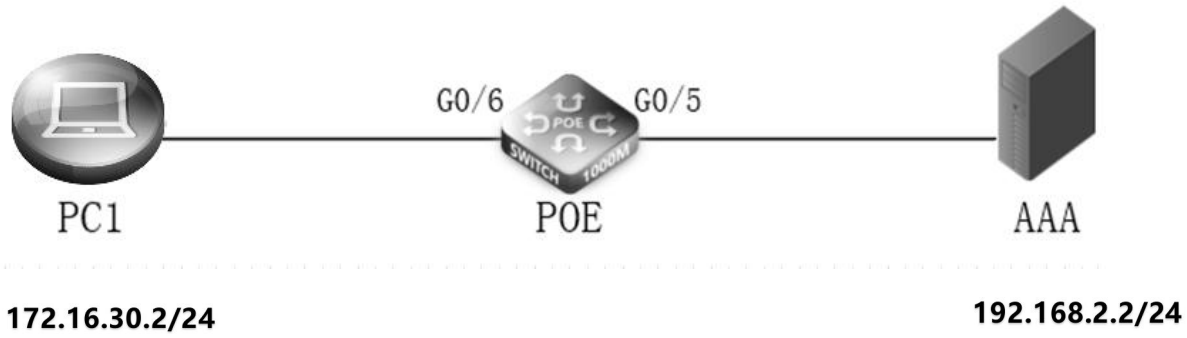
Before supplying power to the standard PoE receiving equipment, it is recommended to check the product introduction first and carry out relevant operations according to the product operation guide.

2.3 TACACS + Authentication Scene

2.3.1Issue Description

When S3400-48T4SP switch is used to configure TACACS + authentication for user side devices, the authentication key must be consistent with the TACACS + server, otherwise the login will fail.

2.3.2 Topology Information



2.3.3 Handling Process

TACACS + protocol is mainly used for PPP and VPDN (Virtual Private Dial-up Network, Virtual Private Dialup Networks) to access AAA of users and end users. It provides authentication, authorization and billing these three security functions.

1) Set up the the scene building according to the Topo to ensure that the PoE switch can reach the network with PC and Tacacs+ server respectively.

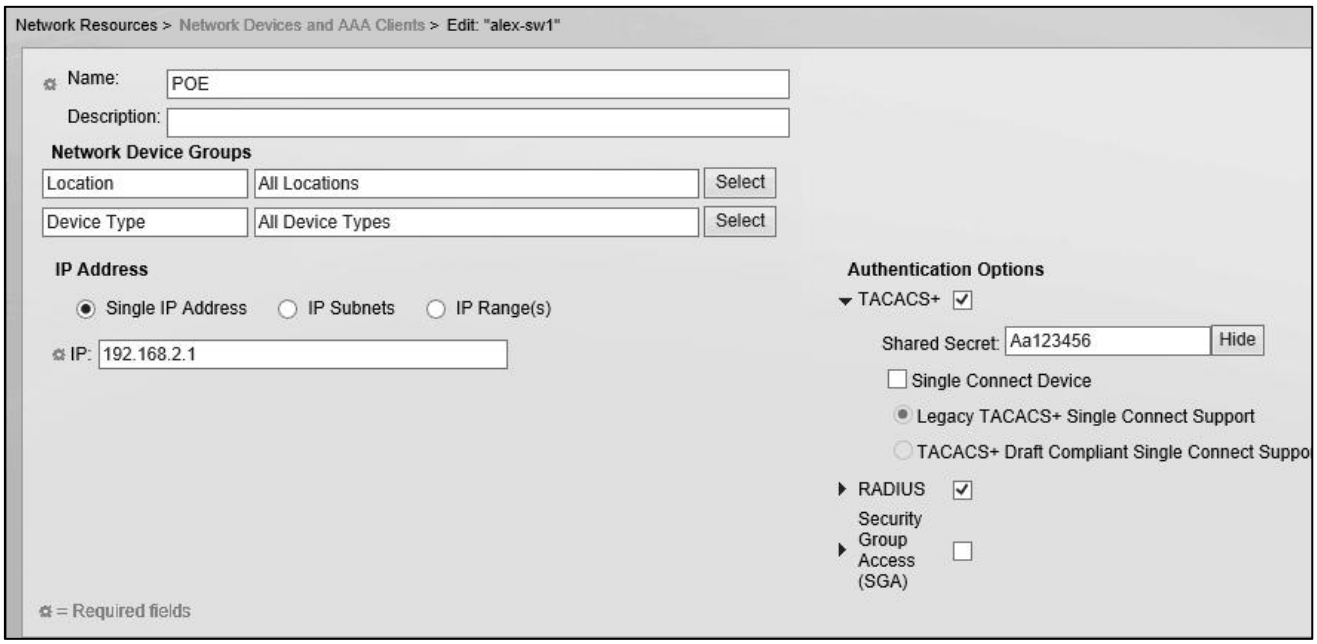
```
#48PoE_config#VLAN 20
48PoE_config_vlan20#exit
48PoE_config#VLAN 30
48PoE_config_vlan30#exit
48PoE_config#int vlan 20
48PoE_config_v20#ip add 172.16.30.1 255.255.255.0
48PoE_config_v20#int vlan 30
48PoE_config_v30#ip add 192.168.2.1 255.255.255.0
48PoE_config#int gigaEthernet 0/5
48PoE_config_g0/5#switchport mode access
48PoE_config_g0/5#switchport pvid 30
48PoE_config_g0/5#int gigaEthernet 0/6
48PoE_config_g0/6#switchport mode access
48PoE_config_g0/6#switchport pvid 20
```

2) Turn on the telnet function on the 48PoE switch, and use the default user and password for remote login on the PC side. (Default is on, and remote login cannot be supported after closing)

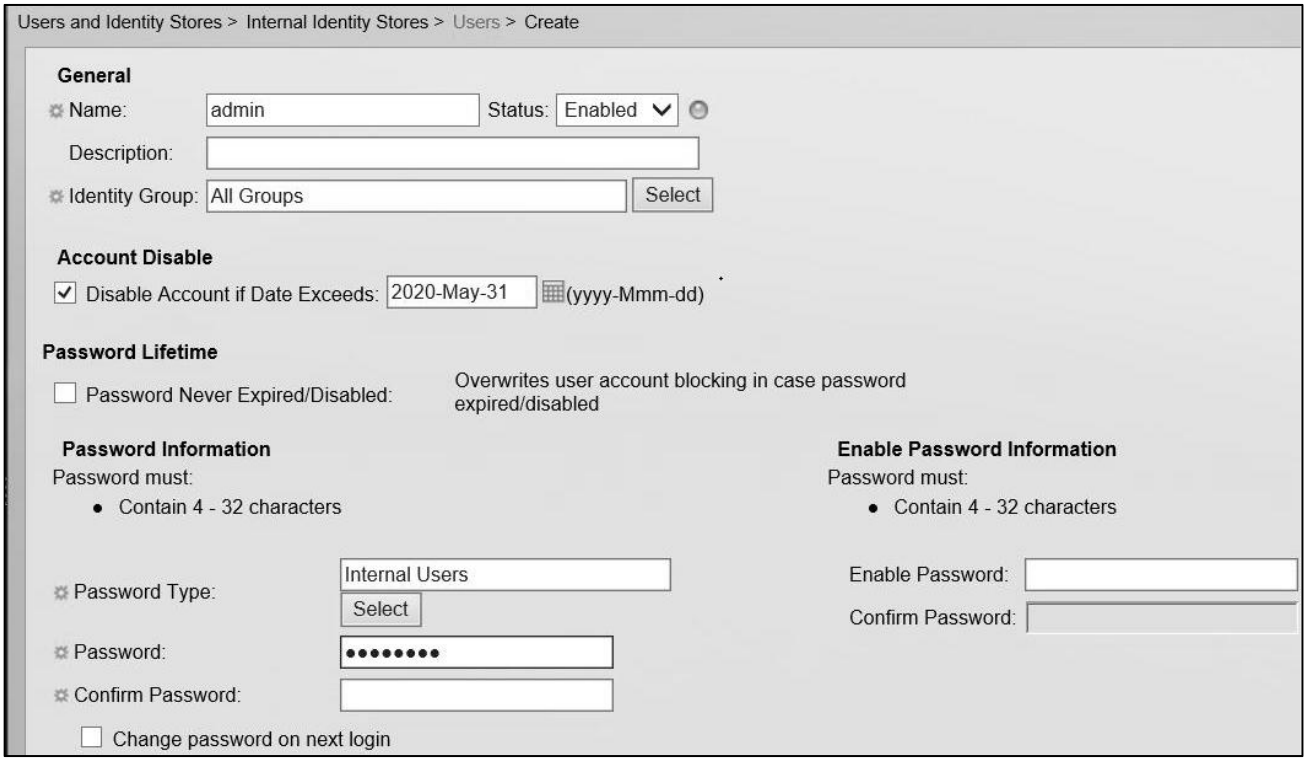
```
48PoE_config#ip telnet enable
```

3) Add the username and password which need to be authenticated on Tacacs+ server.

Add the key, and the key needs to be consistent with the switch key. Otherwise, the switch will fail to negotiate with the Tacacs server. (The key is **Aa123456**)



Create a username and password. The username is **admin** and the password is **admin123**.



4) Tacacs+ authentication, authorization and billing functions are configured on the PoE device. (The configured key must be consistent with the Tacacs+ server, otherwise the login will fail.)

Configure tacacs+ authentication

```
48PoE_config#aaa authentication login default group tacacs+ local

48PoE_config#tacacs-server host 192.168.2.206
```

```
48PoE_config#tacacs-server key Aa123456
```

Configure Tacacs+ authorization

```
48PoE_config#aaa authentication login default group tacacs+ local
48PoE_config#aaa authorization exec default group tacacs+
48PoE_config#tacacs-server host 192.168.2.206
48PoE_config#tacacs-server key Aa123456
```

Configure Tacacs+ billing

```
48PoE_config#aaa authentication login default group tacacs+ local
48PoE_config#aaa accounting exec default start-stop group tacacs+
48PoE_config#tacacs-server host 192.168.2.206
48PoE_config#tacacs-server key Aa123456
```

5) Log in to the 48 PoE switch via telnet on the PC and log in to the device with the username and password created on the Tacacs server. The username is **admin** and the password is **admin123**.

2.3.4 Root Cause

The Tacacs+ shared key configured by S3400-48T4SP switch is inconsistent with the shared key of Tacacs+ server, which leads to authentication failure.

2.3.5 Solution

Before configuring Tacacs+ authentication as a user side device, S3400-48T4SP switch needs to check whether the remote login function is enabled; when configuring the Tacacs+ shared key, it should be consistent with the Tacacs+ server.

2.3.6 Suggestions and Conclusions

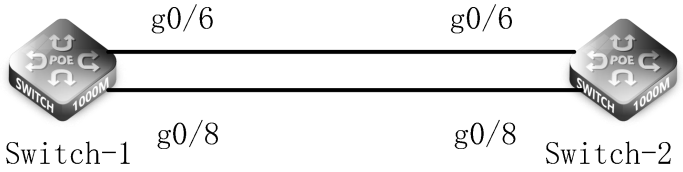
Before configuring Tacacs+ authentication, pay attention to check the accessibility of the underlying network, and whether related functions are enabled and the configuration steps are complete.

2.4 Application Scene of Link Aggregation

2.4.1Issue Description

When configuring the Link Aggregation, S3400-48T4SP switch cannot join the aggregation group directly under the port. You need to configure the aggregation group in advance under the global mode, otherwise you cannot join the aggregation group which is not created under the port configuration.

2.4.2 Topology Information



2.4.3 Handling Process

Link aggregation is to combine two or more data channels into a single channel. The channel appears as a single logical link with higher bandwidth, which can realize load balancing and provide redundant links.

1) Link Aggregation Configuration Failure Issue (Prompts that aggregation group 1 is not created)

```
48PoE_config#int g0/7
48PoE_config_g0/7#aggregator-group 2 mode lacp
```

2) Correctly configure the scene of Link Aggregation (The switch configuration at the other end is same)

```
48PoE_config#interface port-aggregator 1
48PoE_config_p1#exit
48PoE_config#int g0/6
```

```
48PoE_config_g0/6#aggregator-group 1 mode lacp active
48PoE_config_g0/6# int g0/8
48PoE_config_g0/8#aggregator-group 1 mode lacp active
```

3) View information of aggregation group

```
48PoE #show aggregator-group brief
```

2.4.4 Root Cause

When the S3400-48T4SP switch is configured with the link aggregation, it is unable to join the aggregation group that has not been created under the port configuration. Because of the logic problem of statement, the aggregation group must be created first before the port can be added to the aggregation group.

2.4.5 Solution

S3400-48T4SP switch should be in accordance with the configuration guide when configuring Link Aggregation.

2.4.6 Suggestions and Conclusions

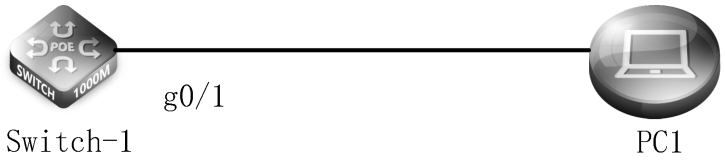
After the configuration fails, you should check the error message and related configuration information, and refer to the configuration guide for troubleshooting.

2.5 User Management Application Scene

2.5.1 Issue Description

Because the device has not been logged in for a long time, the user name and password are forgotten, and the device cannot be logged in for management operation.

2.5.2 Topology Information



2.5.3 Handling Process

1. Use the console cable to log in to the device and restart the switch. During the startup, use the Shortcut Ctrl + P to enter the monitor mode.

2. In monitor mode, view the file directory through dir, find the configuration file, use (more+file name) to view the configuration information, and find the (username **** password ****) command.

1) The user uses the method of plain text authentication, and can directly view the information of username and password.

```
fmonitor#show configuration (View configuration information)
!
aaa authentication login default local
aaa authentication enable default none
aaa authorization exec default local
!
username admin password 0 admin
!
```

2) The password authentication mode is used by the user, so the information of username and password cannot be viewed directly. The current configuration file can be deleted in the monitor mode, so as to restore the factory settings (Before executing this command, the configuration file can be copied to the txt file on the desktop for the convenience of subsequent configuration file import), and then exit the monitor mode. At this time, the default username and password (**admin/admin**) can log in to the device normally.

2.5.4 Root Cause

After changing the default username and password, the user information will lose if the user do not make a memo and do not log in to the device for a long time.

2.5.5 Solution

Restart the device, enter monitor mode, view the username and password information, or delete the current configuration file.

2.5.6 Suggestions and Conclusions

When changing the default username and password, please make a memo. When the password is lost, you can use Ctrl+P to enter the monitor mode during the device restart process and solve the problem of unabled device login.