



Dahua 16/24-Port PoE Gigabit Managed Switch

Quick Start Guide



Foreword

General






This Quick Start Guide (hereinafter referred to be "the Guide") introduces the features and the structure of 16/24-Port PoE Gigabit Managed Switch. Read carefully before using the device, and keep the manual safe for future reference.

Models

Name	Model
16-Port PoE Gigabit Managed Switch (190 W)	DH-PFS4218-16GT-190
16-Port PoE Gigabit Managed Switch (240 W)	DH-PFS4218-16GT-240
24-Port PoE Gigabit Managed Switch (240 W)	DH-PFS4226-24GT-240
24-Port PoE Gigabit Managed Switch (360 W)	DH-PFS4226-24GT-360

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
 DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
 WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
 CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
 TIPS	Provides methods to help you solve a problem or save time.
 NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.5	Modified address.	August 2023
V1.0.4	Add iLinksView information.	June 2020
V1.0.3	Optimize description.	August 2019
V1.0.2	Delete specifications	June 2019
V1.0.4	First release.	May 2018

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the device, hazard prevention, and prevention of property damage. Read carefully before using the device, and comply with the guidelines when using it.

Operation Requirements



- Do not expose the device directly to the sunlight, and keep it away from heat.
- Do not install the device in the damp environment, and avoid dust and soot.
- Make sure the device is in horizontal installation, and install the device on solid and flat surface to avoid falling down.
- Avoid liquid spattering on the device. Do not place object full of liquid on the device to avoid liquid flowing into the device.
- Install the device in the well-ventilated environment. Do not block the air vent of the device.
- Use the device at rated input and output voltage.
- Do not disassemble the device without professional instruction.
- Transport, use, and store the device in allowed ranges of humidity and temperature.

Power Supply Requirements



- Use the battery properly to avoid fire, explosion, and other dangers.
- Replace the battery with battery of the same type.
- Use locally recommended power cord in the limit of rated specifications.
- Use the standard power adapter. We will assume no responsibility for any problems caused by nonstandard power adapter.
- The power supply shall meet the SELV requirement. Use the power supply that conforms to Limited Power Source, according to IEC60950-1. Refer to the device label.
- Adopt GND protection for I-type device.
- The coupler is the disconnecting apparatus. Keep it at the angle for easy to operate.

Table of Contents

Foreword	I
Important Safeguards and Warnings	错误!未定义书签。
1 Product Information	5
Appendix 1 Cybersecurity Recommendations	错误!未定义书签。

1 Product Overview

1.1 Product Introduction

The 16/24-Port Gigabit Managed PoE Switch is designed and developed for field transmission application of high definition video. The product is equipped with high performance switching engine and large buffer, which features low transmission delay and high reliability. Advantages of solid and sealed all-metal case design, low power consumption, fanless and efficient surface heat dissipation makes it work in the environment from -10 °C to 55 °C. And power input end overcurrent, overvoltage, and EMC protection can effectively resist the interference from static electricity, lightning, and pulse.

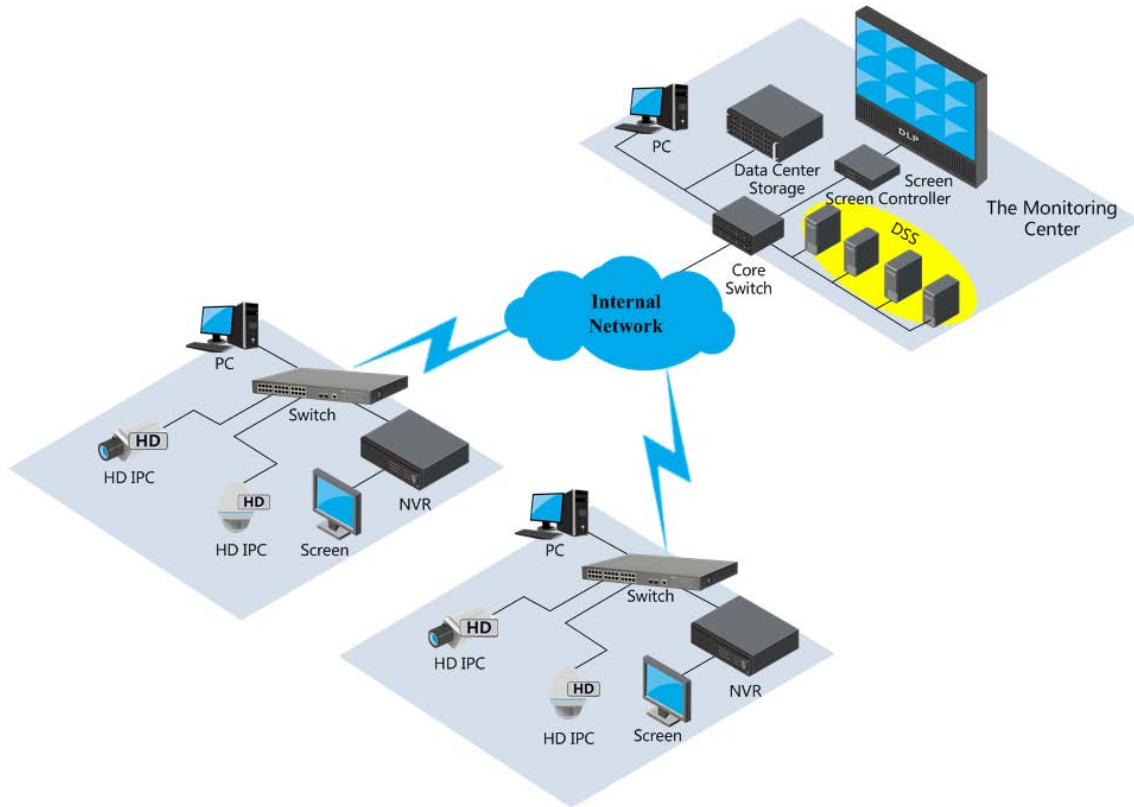
The product owns powerful network management function. Network management system supports iLinksView, CLI, Telnet, web, and network management software based on SNMP.

1.2 Product Features

- Layer 2 network management PoE switch.
- Support IEEE802.3af, IEEE802.3at standard.
- Support Hi-PoE 60 W.
- Network redundancy: STP/RSTP/MSTP.
- Support IPv4/IPv6, and DHCP.
- Network management based on SNMP.
- Configuration: web console, Telnet, CLI command.
- QoS (IEEE802.1p/1Q), CoS/ToS to increase determinism.
- Enhanced network security with IEEE802.1X, SNMP v1/v2c/v3, HTTPS, and SSH.
- Large data buffer up to 4 MB, realtime transmission.
- MAC auto study and aging, MAC address list capacity is 8K.
- EMC high protection design.

1.3 Typical Application

Figure 1-1 Networking



2 Product Overview

2.1 Front Panel

2.1.1 DH-PFS4218-16GT-190/240

Figure 2-1 Front panel

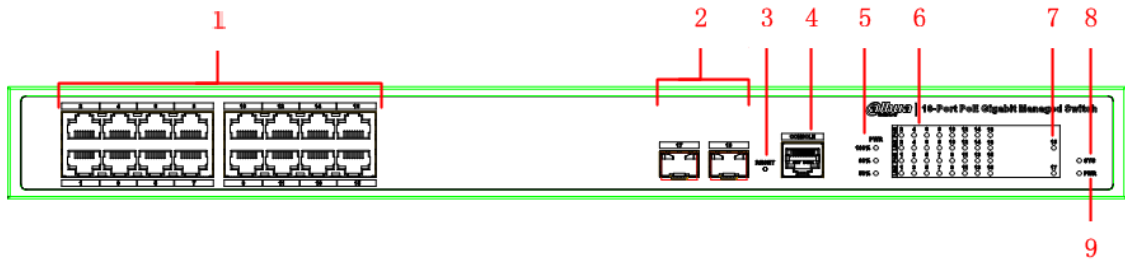


Table 2-1 Front panel description

No.	Name	Description
1	RJ-45 port	Ethernet port, support 10/100/1000 Mbps self-adaptive.
2	SFP port	Fiber port supports 1000 Mbps.
3	Reset button	Long press the button for 5 s to reset the device and recover default configuration.
4	Console serial port	Device debugging port.
5	PoE power usage indicator	Current power consumption display.
6	Downlink indicator	Current port link status and PoE status.
7	SFP port indicator	SFP port indicate link/act.
8	System indicator	System status: <ul style="list-style-type: none"> When device is booting up, the light is flashing quickly. When device is working properly, the light is flashing slowly.
9	Power indicator	Device current power status.

2.1.2 DH-PFS4226-24GT-240/360

Figure 2-2 Front panel

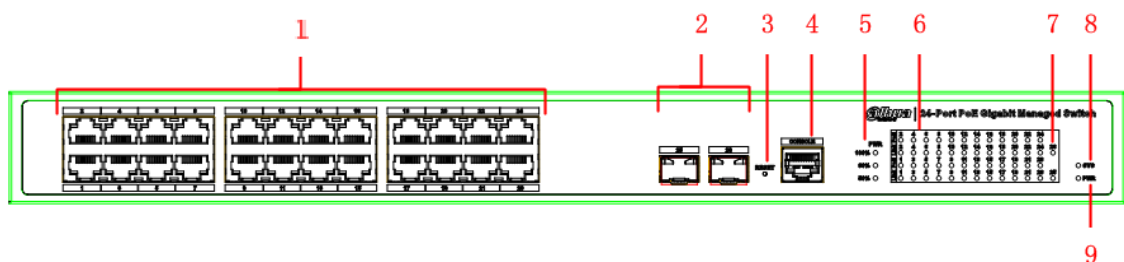


Table 2-2 Front panel description

No.	Name	Description
1	RJ-45 port	Ethernet port, support 10/100/1000 Mbps self-adaptive.
2	SFP port	Fiber port supports 1000 Mbps.
3	Reset button	Long press the button for 5 s to reset the device and recover default configuration.
4	Console serial port	Device debugging port.
5	PoE power usage indicator	Current power consumption display.
6	Downlink indicator	Current port link status and PoE status.
7	SFP port indicator	SFP port indicate link/act.
8	System indicator	System status: <ul style="list-style-type: none"> ● When device is booting up, the light is flashing quickly. ● When device is working properly, the light is flashing slowly.
9	Power indicator	Device current power status.

2.2 Rear Panel

Figure 2-3 Rear panel



Table 2-3 Rear panel description

No.	Name	Description
1	Power switch	Control device power on and off.
2	Power socket	Support 100 VAC to 240 VAC.
3	Ground terminal	GND

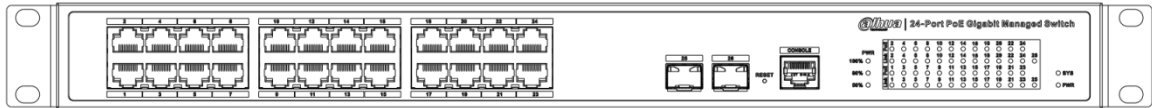
3 Installation

3.1 Installing the Device

The device supports standard rack-mount.

Install the rackmount kit on both sides of the switch.

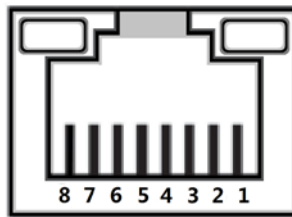
Figure 3-1 Rack-mount



3.2 Wiring

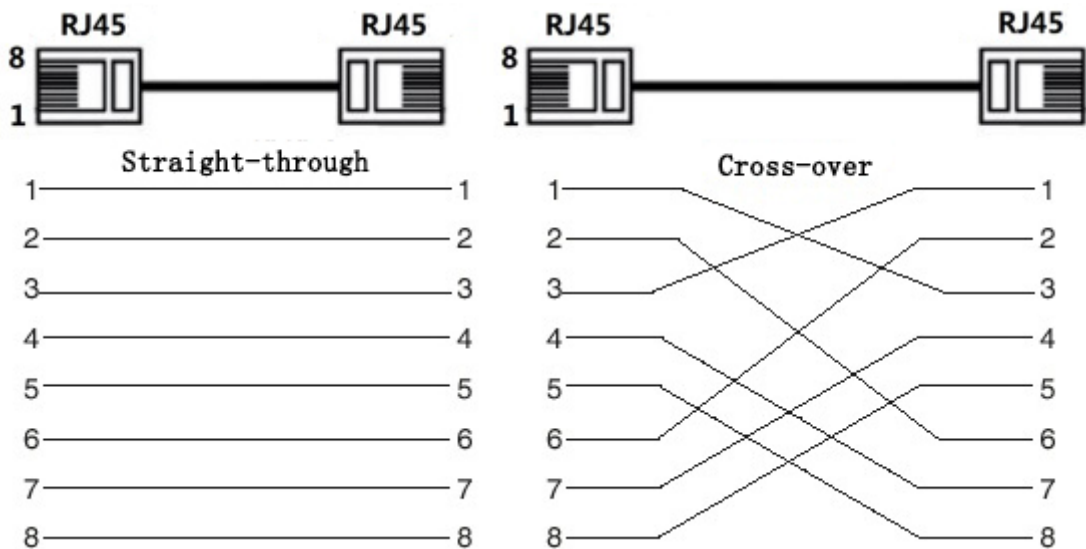
3.2.1 Ethernet Port

Figure 3-2 Ethernet port pin No.



10/100/1000 Base-T Ethernet port adopts standard RJ-45 port. Equipped with self-adaptation function, it can be automatically configured to full duplex/half-duplex operation mode, and supports MDI/MDI-X self-recognition function of the cable, which means it can use cross-over cable or straight-through cable to connect terminal device to network device.

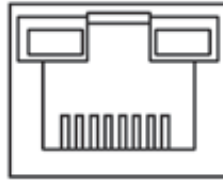
Figure 3-3 Pin description



The cable connection of RJ-45 connector conforms to the standard 568B (1-orange white, 2-orange, 3-green white, 4-blue, 5-blue white, 6-green, 7-brown white, 8-brown).

3.2.2 Console Port

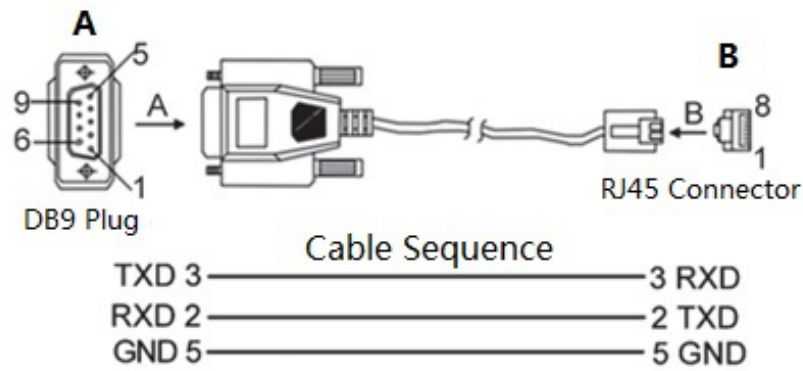
Figure 3-4 Console port



See Figure 3-4 for console port. The switch console port and computer controlling 9-pin serial port are connected with RJ-45-DB9 cable. You can call the console software of the device by operating the superterminal software of the Windows system for device configuration, maintenance, and management.

See Figure 3-5 for cable sequence of RJ-45-DB9.

Figure 3-5 Cable sequence of RJ-45-DB9



One end of RJ-45-DB9 cable is RJ-45 connector, which needs to be inserted into the console port of the device. And the other end is DB9 plug, which needs to be inserted into the computer controlling 9-pin serial port.

See Table 3-1 for pin description.

Table 3-1 Pin description

DB9 pin	RJ-45 pin	Signal	Description
2	3	RXD	Receiving data.
3	2	TXD	Sending data.
5	5	GND	GND

3.2.3 SFP Port



The signal is transmitted through laser by optical fiber cable. The laser conforms to the requirement of level 1 laser products. To avoid injury upon eyes, do not look at the 1000 Base-X optical port directly when the device is powered on.

Figure 3-6 SFP module structure

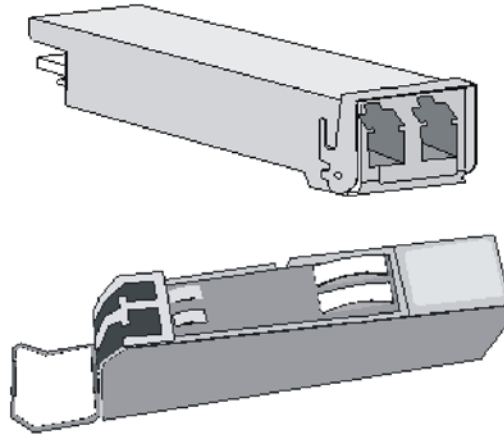
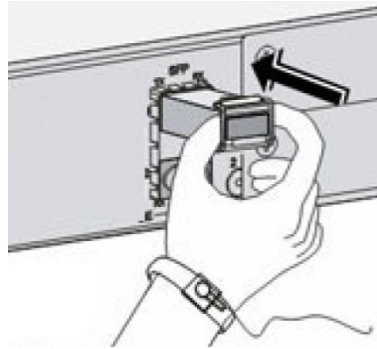


Figure 3-7 SFP module installation

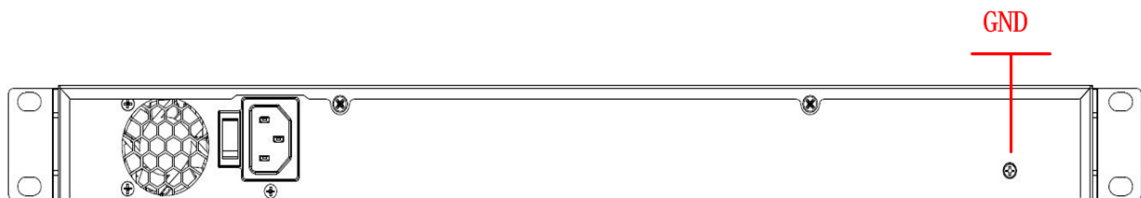


Installing SFP Port

- Step 1** It is recommended that before installing SFP module, you should wear antistatic gloves, and then wear antistatic wrist. Make sure that the antistatic gloves and the antistatic wrist are in good contact.
- Step 2** Lift the handle of SFP module upward vertically, and stuck it to the top hook. Hold the SFP module by both sides, and push it gently into the SFP slot till the SFP module is firmly connected to the slot (you can feel that both the top and bottom spring strip of the SFP module are firmly stuck with the SFP slot).

3.2.4 GND

Figure 3-8 GND terminal



Normal GND of the device is the important guarantee for device lightning protection and anti-interference. You should connect the GND cable before powering on the device, and power off the device before disconnecting the GND cable.

There is a GND screw on the device cover board for the GND cable, which is called enclosure GND. Connect one end of the GND cable with the cold-pressed terminal, and fix it on the enclosure GND with the GND screw. The other end of the GND cable should be reliably connected to the ground.



The sectional area of the GND cable shall be more than 2.5 mm², and the GND resistance shall be less than 5 Ω.

4 Quick Operation

We will introduce VLAN configuration briefly in this section. See the corresponding command line manual for detailed configuration.

4.1 First Login by Console Port

Login by console port is the most basic way to log in the local interface, and it is also the method to configure other ways to log in the device.

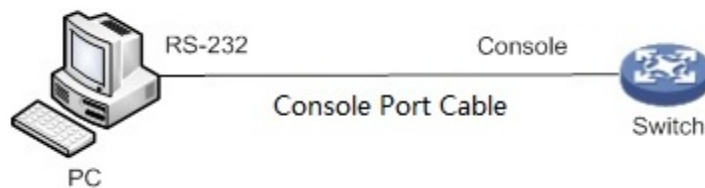
Step 1 Power off the PC.

Step 2 Connect the PC and the device with the default console port cable. Insert the DB-9 (hole) plug of console port cable into the 9-pin serial port of PC, and then insert the RJ-45 plug into the console port of the device.

 **NOTE**

- Check the mark on the port before you insert the plug and make sure you insert the plug into the correct port.
- Plug out RJ-45 first and then DB-9 when dismantling console port cable.

Figure 4-1 Connection with console port cable



Step 3 Power on the PC.

Step 4 Run terminal simulation program on the PC. Select the serial port connected with the device, and configure the terminal communication parameters. The parameter values should match with the values of the device. By default:

- Baud rate: 115200
- Data bit: 8
- Stop bit: 1
- Parity: none
- Flow control: none

 **NOTE**

If the PC adopts Windows Server 2003 operating system, add the super terminal program in the Windows component and then login and manage the device according to this Guide. If the PC adopts Windows Server 2008, Windows Vista, Windows 7, or other operating systems, use the third-party terminal control software and refer to the software operation guide or online help for operation method.

Step 5 Power on the device, and the device self-check information is displayed on the terminal. There will be the prompt for you to press Enter key after device self-check. And you can enter the user name and password.

Step 6 Enter the user name, and then press Enter key.

Step 7 The command line prompt (SWITCH#) is displayed after you press Enter key, as shown in the following. And you login the device successfully.

```
+M25PXX : Init device with JEDEC ID 0xC22018.
Luton10 board detected (VSC7428 Rev. D).

RedBoot (tm) bootstrap and debug environment [ROMRAM]
Non-certified release, version 1_31-4752 - built 17:29:35, Jul 29 2017

Copyright (C) 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009
Free Software Foundation, Inc.
RedBoot is free software, covered by the eCos license, derived from the
GNU General Public License. You are welcome to change it and/or distribute
copies of it under certain conditions. Under the license terms, RedBoot's
source code and full license terms must have been made available to you.
Redboot comes with ABSOLUTELY NO WARRANTY.

Platform: VCore-III (MIPS32 24KEc) LUTON26
RAM: 0x80000000-0x88000000 [0x80028f20-0x87fdfffc available]
FLASH: 0x40000000-0x40ffffff, 256 x 0x10000 blocks
== Executing boot script in 3.000 seconds - enter ^C to abort
RedBoot> diag -p
RedBoot> fis load -x linux
MD5 signature validated
Stage1: 0x80100000, length 4641272 bytes
Initrd: 0x80600000, length 188416 bytes
Kernel command line: init=/usr/bin/stage2-loader loglevel=4
RedBoot> exec
Now booting linux kernel:
Base address 0x80080000 Entry 0x80100000
Cmdline : init=/usr/bin/stage2-loader loglevel=4
Active fis: linux
[ 0.374113] vcfw_uio vcfw_uio: UIO driver loading
[ 0.378957] vcfw_uio vcfw_uio: Invalid memory resource
[ 0.384141] iounmap: bad address (null)
00:00:00 Stage 1 booted
00:00:00 Using device: /dev/mtd7
00:00:01 Mounted /dev/mtd7
00:00:01 Loading stage2 from NAND file 'n6G5Xw'
00:00:05 Overall: 4195 ms, ubifs = 748 ms, rootfs 3422 ms of which xz = 0 ms of which untar =
0 ms
Starting application...wuxuwuxu
Using existing mount point for /switch/
system time:2017-10-14 17:59:53
W icfg 18:00:22 71/icfg_commit_tftp_load_and_trigger#2695: Warning: TFTP get bringup-
config: Operation timed out.
```

Press ENTER to get started

Username: admin

Password:

SWITCH#

Enter the command, and you can configure the device and view the device operating status.

You can enter ? anytime if you need help.

4.2 Restore to the Factory Default

You can log in the web interface of the device via the following IP address.

Login the web interface of the device or login by console port with the user name and the password.

Table 4-1 Factory default

Parameter	Description
IP address	192.168.1.110/255.255.255.0
User name	admin
Password	admin (hidden)

NOTE

- iLinksView is enabled by default, and the default username is admin, the default password is lt_91_il_02_nmp.
- When using the iLinksView to manage the device, note that the username and password must be the same as that you have set in the iLinksView, otherwise the iLinksView cannot discover the device.

4.3 VLAN Configuration

Virtual Local Area Network (VLAN) is frequently and widely applied. It is the basic to divide the network. VLAN is the network that multiple devices are logically organized as one network, regardless of the physical location of the devices. Every VLAN is a logical network with all functions and attributes of traditional physical network. Every VLAN is a broadcast domain, and the broadcast packet can only be forwarded within one VLAN. The broadcast packet cannot be forwarded across different VLANs.

VLAN Based on Port

VLAN based on port is that one switch can divide the logical working groups by controlling interoperability between two and several ports. Dividing the port VLAN reasonably can enhance network security, improve bandwidth availability, and reduce the probability of broadcast storm. This series of products support 4094 VLANs. When you create the VLAN, you need to select a VLAN ID which ranges from 2 through 4094. By default, VLAN 1 is created, and it cannot be deleted.

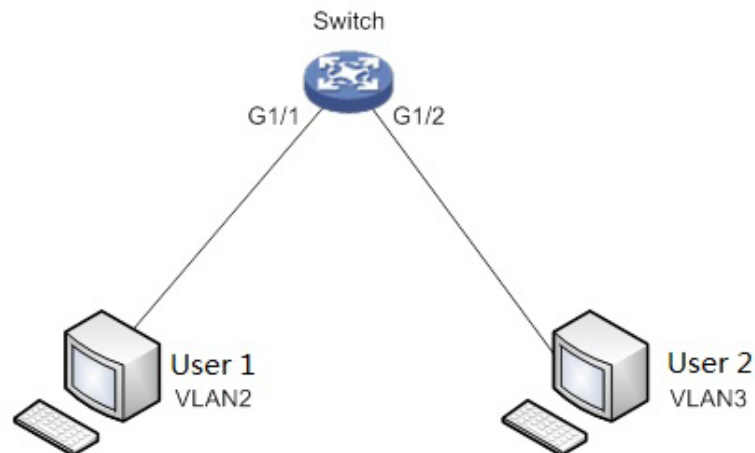
Application Example

Networking Requirement

There are two users, user 1 and user 2. They need to be in different VLANs because the network function and environment they use are different. User 1 belongs to VLAN 2, connected to the switch

port G1/1 (GigabitEthernet 1/1). User 2 belongs to VLAN 3, connected to switch port G1/2 (GigabitEthernet 1/2).

Figure 4-2 VLAN networking



Configuration Steps

To configure the switch, do the following:

Step 8 Create the VLAN.

```
SWITCH #configure terminal
SWITCH (config)#vlan 2
SWITCH (config-vlan)# exit
SWITCH (config)#vlan 3
SWITCH (config-vlan)# exit
```

Step 9 Allocate the ports into the VLAN.

```
SWITCH(config)# interface GigabitEthernet 1/1
SWITCH (config-if)# switchport access vlan 2
SWITCH (config-if)# exit
SWITCH (config)# interface GigabitEthernet 1/2
SWITCH (config-if)# switchport access vlan 3
SWITCH (config-if)# exit
```

Appendix 1 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations from Dahua on how to create a more secured security system.

Mandatory actions to be taken for basic device network security:

1. Use Strong Passwords

Please refer to the following suggestions to set passwords.

- The length should not be less than 8 characters.
- Include at least two types of characters; character types include upper and lower case letters, numbers and symbols.
- Do not contain the account name or the account name in reverse order.
- Do not use continuous characters, such as 123, abc, etc.
- Do not use overlapped characters, such as 111, aaa, etc.

2. Update Firmware and Client Software in Time

- According to the standard procedure in Tech-industry, we recommend to keep your device (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the device is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
- We suggest that you download and use the latest version of client software.

"Nice to have" recommendations to improve your device network security:

1. Physical Protection

We suggest that you perform physical protection to device, especially storage devices. For example, place the device in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable device (such as USB flash disk, serial port), etc.

2. Change Passwords Regularly

We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

3. Set and Update Passwords Reset Information Timely

The device supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

4. Enable Account Lock

The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

5. Change Default HTTP and Other Service Ports

We suggest you to change default HTTP and other service ports into any set of numbers between

1024–65535, reducing the risk of outsiders being able to guess which ports you are using.

6. Enable HTTPS

We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

7. MAC Address Binding

We recommend you to bind the IP and MAC address of the gateway to the device, thus reducing the risk of ARP spoofing.

8. Assign Accounts and Privileges Reasonably

According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

9. Disable Unnecessary Services and Choose Secure Modes

If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

- SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
- SMTP: Choose TLS to access mailbox server.
- FTP: Choose SFTP, and set up strong passwords.
- AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

10. Audio and Video Encrypted Transmission

If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

Reminder: encrypted transmission will cause some loss in transmission efficiency.

11. Secure Auditing

- Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
- Check device log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

12. Network Log

Due to the limited storage capacity of the device, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

13. Construct a Safe Network Environment

In order to better ensure the safety of device and reduce potential cyber risks, we recommend:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.

- Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.

More information

Please visit Dahua official website security emergency response center for security announcements and the latest security recommendations.

ENABLING A SAFER SOCIETY AND SMARTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053

Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188