



24-Port 10/100 Mbps + 1-Port Gigabit Combo Base-T SFP multi-mode PoE Switch

User's Manual



Foreword

General

This user's manual introduces the functions and operations of 24-Port 10/100 Mbps + 1-Port Gigabit Combo Base-T SFP multi-mode PoE Switch devices. Read carefully before using the device, and keep the manual safe for future reference.

Models

DH-PFS3125-24ET-190

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
V1.0.2	Modified address.	August 2023
V1.0.1	Delete specifications	June 2019
V1.0.0	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.

Electrical safety



- All installation and operation here should conform to your local electrical safety codes.
- The product must be grounded to reduce the risk of electric shock.
- We assume no liability or responsibility for all the fires or electrical shock caused by improper handling or installation.

Transportation security

Heavy stress, violent vibration or water splash are not allowed during transportation, storage and installation

Installation

- Keep upwards. Handle with care.
- Do not apply power to the Device before completing installation.
- Do not place objects on the Device.

Qualified engineers needed

All the examination and repair work should be done by the qualified service engineers. We are not liable for any problems caused by unauthorized modifications or attempted repair.

Environment

The Device should be installed in a cool, dry place away from conditions such as direct sunlight, inflammable substances, and explosive substances.

Accessories

- Be sure to use all the accessories recommended by manufacturer.
- Before installation, please open the package and check all the components are included.
- Contact your local retailer ASAP if something is broken in your package.

Battery

- Improper battery use might result in fire, explosion, or personal injury.
- When replacing the battery, please make sure you are using the same type. Risk of explosion if battery is replaced by an incorrect type.
- Dispose of used batteries according to the instructions.

- Please make sure to use the same battery model if possible.
- We recommend replace battery regularly (such as one-year) to guarantee system time accuracy. Before replacement, please save the system setup, otherwise, you may lose the data completely.

Table of Contents

Foreword	I
Important Safeguards and Warnings	III
1 Introduction	1
1.1 Overview	1
1.2 Product Features	1
1.3 External Component Description	1
1.3.1 Front Panel	1
1.3.2 Rear Panel	3
1.4 Package Contents	3
2 Installation and Connection	5
2.1 Installation	5
2.1.1 Desktop Installation	5
2.1.2 Rack-mountable Installation in 13-inch Cabinet	5
2.1.3 Powering on the Switch	6
2.2 Connecting Computer (NIC) to the Switch	6
2.3 Switch connection to the PD	6
Appendix 1 Cybersecurity Recommendations	7

1 Introduction

1.1 Overview

The Switch is a high performance multi-mode PoE switch. Provides twenty-four 10/100 Mbps Auto-Negotiation RJ-45 ports, plus one gigabit Combo ports, it can be used to link bandwidth higher upstream equipment. These PoE ports can automatically detect and supply power with those IEEE 802.3at compliant Powered Devices (PD) such as AP, IP Cameras or IP Phones, etc. The switch port1 and port2 can support the 802.3bt standard, and the maximum output power can reach 60W. The switch on the panel to stir, can be configured to automatically switch the normal working mode, port isolation (VLAN) mode, monitoring mode, network extend mode, flexible and extensible family, office network without power line layout restrictions; meet the small and medium-sized enterprises, intelligent community, hotels, parks and office network network networking and access requirements.

1.2 Product Features

- Comply with IEEE802.3, IEEE802.3u, IEEE802.3ab, IEEE802.3x, IEEE802.3az, IEEE802.3at, IEEE802.3af, IEEE802.3bt standards.
- 24 x 10/100 Mbps Auto Negotiation Ethernet port, 1 x 1000 Mbps Combo ports. All port auto MDI/MDIX.
- The switch 1 and 2 ports support IEEE802.3bt standard 60 W high power output, the total power consumption of up to 190 W.
- Supports IEEE802.3x flow control for Full-duplex and backpressure for Half-duplex.
- Supports MAC address auto-learning and auto-aging.
- Store and forward mode operates.
- Free switching of multiple working modes.
- LED indicators for monitoring PSE, Link/Activity.
- Built in 210 W high performance switching power supply.

1.3 External Component Description

1.3.1 Front Panel

The front panel of the Switch consists of a series of LED indicators, one Mode Switch, 24 x 10/100 Mbps RJ-45 ports, one Combo (RJ-45/SFP) port.

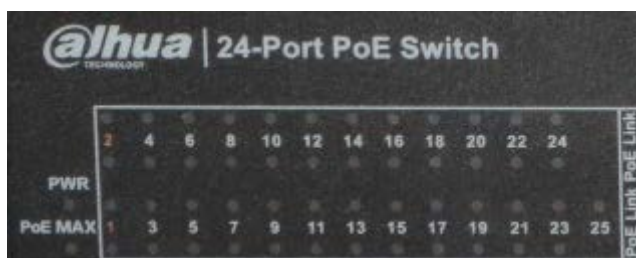
Figure 1-1 Front panel



LED indicators:

The LED Indicators will allow you to monitor, diagnose and troubleshoot any potential problem with the Switch, connection or attached devices.

Figure 1-2 LED indicator



The following chart shows the LED indicators of the Switch along with explanation of each indicator.

Table 1-1 Description of the indicator

LED Indicator	Faceplate Marker	Status	Indication
Power Indicator	PWR	Off	Power Off
		Solid green	Power On
MAX indicator	PoE MAX	Off	PoE load value is normal
		Solid red	The PoE load value reaches the set limit value which is 190 W, and the load quota can no longer be increased.
10/100 BASE-T adaptive Ethernet port indicators (1-24, 25)	Link	Off	The port is NOT connected.
		Solid green	The port is connected, but no data is transmitting or receiving.
		Blinking	The port is transmitting or receiving data.
PoE status indicators (1-24)	PoE	Off	No PD is connected to the corresponding port, or there is a breakdown.
		Solid yellow	A Powered Device is connected to the port, which supply power successfully.

Mode Control:

You can select the switch mode.

Normal mode (NORMAL): Switch all ports can communicate with each other

Port isolation mode (VLAN): 1 to 24 cannot communicate with each other, but can communicate with the uplink Combo port 17.

Monitoring mode (MONITOR): 1 to 8 ports support port priority, optimize port cache, switch all ports can communicate with each other.

Network extend mode(EXTEND): 1 to 8 port rate down to 10 Mbps, the farthest transmission distance of up to 250 meters, all ports can communicate with each other.

10/100 Mbps RJ-45 ports (1 to 24):

Designed to connect to the device with a bandwidth of 10 Mbps, 100 Mbps. Each has a corresponding Link/Act and PoE indicator.

10/100/1000Mbps RJ-45 port 25:

Designed to connect to the device with a bandwidth of 10 Mbps, 100 Mbps or 1000 Mbps. Each has a corresponding Link/Act LED.

1000Mbps SFP port 25:

Designed to install the SFP module. The Switch features one SFP transceiver slots that are shared with one associated RJ-45 ports. A SFP port and an associated RJ-45 port are referred to as "Combo" port, which means they cannot be used simultaneously, and only SFP port work or only RJ-45 port work at the same time.

1.3.2 Rear Panel

The rear panel of the Switch contains one Grounding Terminal, Heat vent and AC power connector shown as below.

Figure 1-3 Rear panel



Grounding Terminal:

Located on the left side of the power supply connector, use wire grounding to lightning protection.

Heat vent:

The Heat vent is located in the middle position of the rear panel of the switch. It is used for heat dissipation and ventilation. Do not cover it.

AC Power Connector:

Power is supplied through an external AC power adapter. It supports 100–240 VAC, 50/60 Hz.

1.4 Package Contents

Before installing the Switch, make sure that the following the "packing list" listed OK. If any part is lost and damaged, please contact your local agent immediately. In addition, make sure that you have the tools install switches and cables by your hands.

- One 24-Port 10/100 Mbps + 1-Port Gigabit Combo Base-T SFP multi-mode PoE Switch.

- One Installation Component.
- One AC power cord.
- One User's Manual.

2 Installation and Connection

This part describes how to install your PoE Ethernet Switch and make connections to it. Please read the following topics and perform the procedures in the order being presented.

2.1 Installation

Please follow the following instructions in avoid of incorrect installation causing device damage and security threat.

- Put the Switch on stable place or desktop in case of falling damage.
- Make sure the Switch works in the proper AC input range and matches the voltage labeled on the Switch.
- To keep the Switch free from lightning, do not open the Switch's shell even in power failure.
- Make sure that there is proper heat dissipation from and adequate ventilation around the Switch.
- Make sure the cabinet to enough back up the weight of the Switch and its accessories.

2.1.1 Desktop Installation

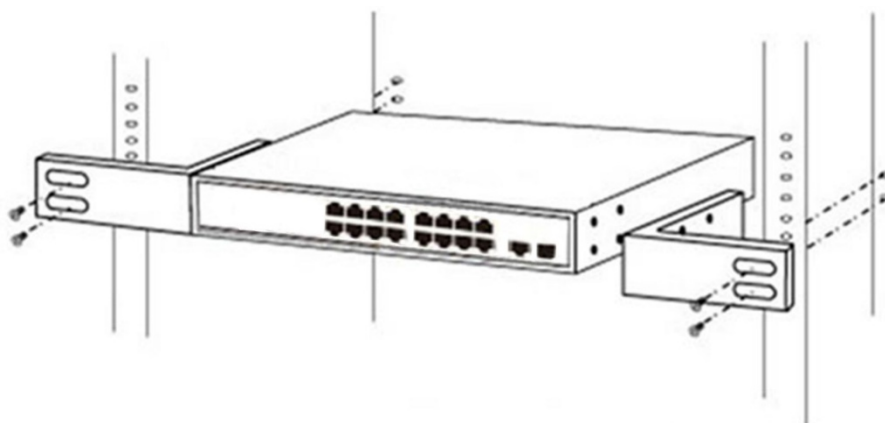
Sometimes users are not equipped with the 19-inch standard cabinet. So when installing the Switch on a desktop, please attach these cushioning rubber feet provided on the bottom at each corner of the Switch in case of the external vibration. Allow adequate space for ventilation between the device and the objects around it.

2.1.2 Rack-mountable Installation in 13-inch Cabinet

The Switch can be mounted in an EIA standard-sized, 19-inch rack, which can be placed in a wiring closet with other equipment. To install the Switch, please follow these steps:

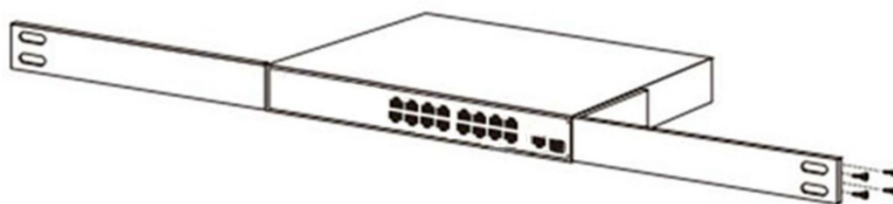
Step 1 Attach the mounting brackets on the Switch's side panels (one on each side) and secure them with the screws provided.

Figure 2-1 Bracket installation



Step 2 Use the screws provided with the equipment rack to mount the Switch on the rack and tighten it.

Figure 2-2 Rack installation



2.1.3 Powering on the Switch

The Switch is powered on by the 100-240 VAC 50/60 Hz internal high-performance power supply. Please follow the next tips to connect:

AC Electrical Outlet:

It is recommended to use single-phase three-wire receptacle with neutral outlet or multifunctional computer professional receptacle. Please make sure to connect the metal ground connector to the grounding source on the outlet.

AC Power Cord Connection:

Connect the AC power connector in the back panel of the Switch to external receptacle with the included power cord, and check the power indicator is ON or not. When it is ON, it indicates the power connection is OK.

2.2 Connecting Computer (NIC) to the Switch

Please insert the NIC into the computer, after installing network card driver, please connect one end of the twisted pair to RJ-45 jack of your computer, the other end will be connected to any RJ-45 port of the Switch, the distance between Switch and computer is around 100 meters. Once the connection is OK and the devices are power on normally, the LINK status indicator lights corresponding ports of the Switch.

2.3 Switch connection to the PD

1-16 ports of the Switch have PoE power supply function, the switch port 1 and port 2 support IEEE802.3bt standard 60W high power output, other PoE port power maximum support 30W, it can make PD devices, such as internet phone, network camera, wireless access point work. You only need to connect the Switch PoE port directly connected to the PD port by network cable.

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