100/1000 Mbps Unmanaged Desktop Switch

Quick Start Guide

V1.0.0

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Foreword

General

This manual introduces the structure and installation of the 100/1000 Mbps Unmanaged Desktop Switch.

Models

DH-PFS3005-5ET-L

DH-PFS3008-8ET-L

DH-PFS3005-5GT-L

DH-PFS3008-8GT-L

Safety Instructions

The following categorized signal words with defined meaning 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, lower performance, or unpredictable result.
TIPS	Indicates dangerous high voltage. Take care to avoid coming into contact with electricity.
NOTE	Indicates a laser radiation hazard. Take care to avoid exposure to a laser beam.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	November 2019

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related

regions. For detailed information, see the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.

- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our 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 the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Important Safeguards and Warnings

The manual helps you to use the product properly. To avoid danger and property damage, read the manual carefully before using the product, and keep it well for future reference.

Operating 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 that 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 operation.

Table of Contents

1 Device Structure

This manual is for multiple models of the switch. Here take DH-PFS3005-5ET-L model as an example. If there is inconsistency between the manual and the actual product, the actual product shall prevail.

1.1 Front Panel and Left Panel

There are serials of indicators on the front panel and 1 DC power port on the left panel. See Figure 1-1.

Figure 1-1 Front panel

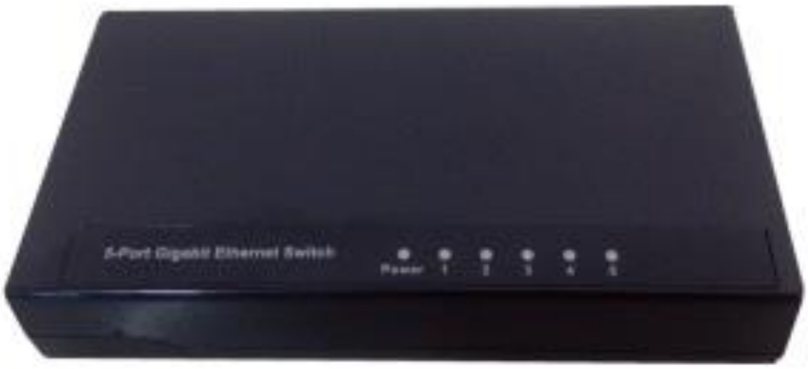


Table 1-1 Front panel description

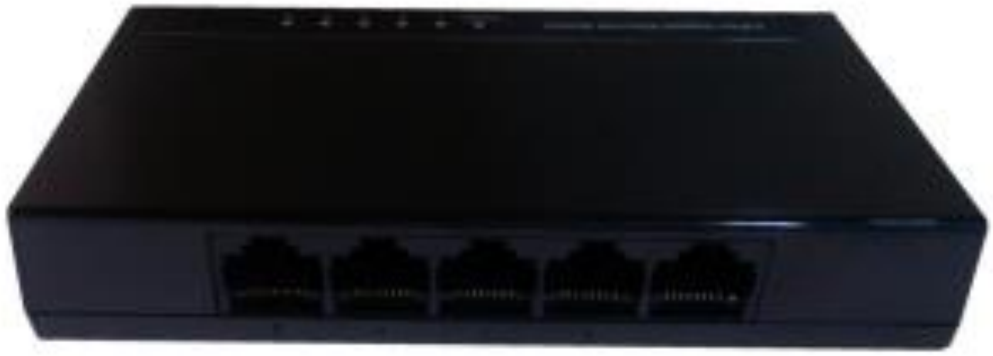
Indicator	Color	Status	Description
Power	Green	On	Switch is powered on.
		Off	Switch is powered off.
1–5/8	Green 10/100/1000 Mbps	Glows green	A device is connected to a port of the switch.
		Off	A device is disconnected from a port of the switch.
		Flashes green	Sending or receiving data.

DC power port: The power is supplied by an external DC power adapter. For information about the input voltage of DC power, refer to the specification section.

1.2 Rear Panel

There are 10/100/1000 Mbps RJ-45 ports on the rear panel. See Figure 1-2.

Figure 1-2 Rear Panel



10/100/1000 Mbps RJ-45 port: Support device connection with 10/100/1000 Mbps bandwidth, each port corresponds to a Link/Act/Speed indicator.

2 Installation and Connection

This chapter describes how to install and connect a 10 Gigabit Ethernet switch.

2.1 Installation

Step 1 Place the switch on a flat table.

Step 2 Make sure that the power adapter is connected to the power supply.

Step 3 Make sure that there is sufficient ventilation around the switch to dissipate heat and air.

- Avoid placing any heavy objects on the switch.
- To ensure a stable cable connection, place the switch horizontally on the desktop.

2.2 Connection to Switch

Switches can be connected to computers or other devices through UTP or twisted pairs of CAT3, CAT4 and CAT5. UTP of CAT5 or CAT5e is required for 100 Mbps operation. Twisted pair of CAT5e or CAT6 is required for 1000 Mbps operation. You can connect to RJ-45 ports with 10/100/1000 Mbps on a computer or other devices from any port on the switch.

Connect the switch and power on, the switch initializes automatically, and the LED indicator is on.

If the LED indicator is off, check the power supply and its connection.

Appendix 1 Technical Specification

Appendix table 1-1 Specification

Hardware					
Model		DH-PFS3005-5ET-L	DH-PFS3008-8ET-L	DH-PFS3005-5GT-L	DH-PFS3008-8GT-L
Standards Compliance		IEEE 802.3, IEEE 802.3u, IEEE 802.3x, IEEE802.3az		IEEE 802.3i, IEEE 802.3u, IEEE 802.3ab, IEEE802.3x	
Network Medium		● 10Base-T: UTP of CAT3, CAT4 or CAT5 (Maximum 100 M) ● 100Base-TX: UTP of CAT5 or CAT5e (Maximum 100 M)		● 10Base-T: UTP of CAT3, CAT4 or CAT5 (Maximum 100 M) ● 100Base-TX: UTP of CAT5 or CAT5e (Maximum 100 M) ● 1000Base-TX: UTP of CAT5e or CAT6 (Maximum 100 M)	
Port		5 adaptive RJ-45 ports with 10/100 Mbps	8 adaptive RJ-45 ports with 10/100 Mbps	5 adaptive RJ-45 ports with 10/100/1000 Mbps	8 adaptive RJ-45 ports with 10/100/1000 Mbps
LED Indicator	Link/Act	Green, 10/100 Mbps RJ-45 port		Green, 10/100/1000 Mbps RJ-45 port	
	PowerSYS	Green		Green	
Transmission Mode		Store-and-Forward			
Switching Capacity		1 Gbps	1.6 Gbps	10 Gbps	16 Gbps
Packet Buffer Memory		448 KB	448 KB	1.5 MB	1.5 MB
Dimensions (L × W × H)		77 mm × 46 mm × 21 mm (3.03” × 1.81” × 0.83”)	132 mm × 70 mm × 26 mm (5.20” × 2.76” × 1.02”)	77 mm × 46 mm × 21 mm (3.03” × 1.81” × 0.83”)	125 mm × 65 mm × 22 mm (4.92” × 2.56” × 0.87”)
Application environment		● Operating Temperature: 0℃ to 40℃ (32℉ to 104℉) ● Storage Temperature: -40℃ to 70℃ (-40℉ to 158℉) ● Operating Humidity: 10% – 90% ● Storage humidity: 5% –90%			
Power Supply and Consumption		● Input: 5V/500mA DC ● Power consumption: 1.3W	● Input: 5V/500mA DC ● Power consumption: 1.5W	● Input: 5V/1A DC ● Power consumption: 1.6W	● Input: 5V/1A DC ● Power consumption: 4W

Appendix 2 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 on how to create a more secured security system.

Mandatory actions to be taken for basic equipment 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 equipment (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 equipment 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 equipment network security:

1. **Physical Protection**

   We suggest that you perform physical protection to equipment, especially storage devices. For example, place the equipment 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 equipment (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 equipment 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. **Enable Whitelist**
   We suggest you to enable whitelist function to prevent everyone, except those with specified IP addresses, from accessing the system. Therefore, please be sure to add your computer's IP address and the accompanying equipment's IP address to the whitelist.
8. **MAC Address Binding**
   We recommend you to bind the IP and MAC address of the gateway to the equipment, thus reducing the risk of ARP spoofing.
9. **Assign Accounts and Privileges Reasonably**
   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.
10. **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.
11. **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.
12. **Secure Auditing**
    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check equipment log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.
13. **Network Log**
    Due to the limited storage capacity of the equipment, 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.
14. **Construct a Safe Network Environment**
    In order to better ensure the safety of equipment 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.

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address: No.1199, Bin'an Road, Binjiang District, Hangzhou, P.R. China
Postcode: 310053
Tel: +86-571-87688883
Fax: +86-571-87688815
Email: overseas@dahuatech.com
Website: www.dahuasecurity.com