Dahua 10-Port Gigabit Unmanaged Desktop Switch with 8 PoE Ports

User's Manual

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V1.0.0

Foreword

General

This manual introduces the features and structure of the 10-port gigabit unmanaged desktop switch with 8 PoE ports device (hereinafter referred to as "the device").

Models

DH-PFS3010-8GT-96

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	Provides methods to help you solve a problem or save you time.
NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	Modify the front panel image.	April 2020

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.

Table of Contents

Foreword ..... **I**
1 Product Overview **1**
1.1 Introduction 1
1.2 Features 1
1.3 Typical Application 1
2 Device Structure **2**
2.1 Front Panel 2
2.2 Rear Panel 2
2.3 Side Panel 3
2.4 PoE Power Supply 3
Appendix 1 Cybersecurity Recommendations **4**

1 Product Overview

1.1 Introduction

10-port gigabit unmanaged desktop switch with 8 PoE ports is a type of layer two commercial switch. It provides eight 10/100/1000 Mbps Ethernet ports and two 10/100/1000 Mbps uplink ports.

1.2 Features

General Features

- Layer two commercial switch.
- Supports IEEE802.3, IEEE802.3u and IEEE802.3X standards.
- MAC auto learning, aging, MAC address capacity 4K.
- Supports MDI/MDIX self-adaptation.
- RJ-45 port supports 10/100/1000 Mbps self-adaptation, supports IEEE802.3af and IEEE803.3at power supply standards.
- Adopts metal enclosure.
- Supports DC 48V–57V power supply.
- Supports wall-mount installation.
- Supports the anti-theft lock hole.

Individual Features

Port 1 supports Hi-PoE 60W power supply.

1.3 Typical Application

Figure 1-1 Typical networking scene

2 Device Structure

2.1 Front Panel

Figure 2-1 Front panel

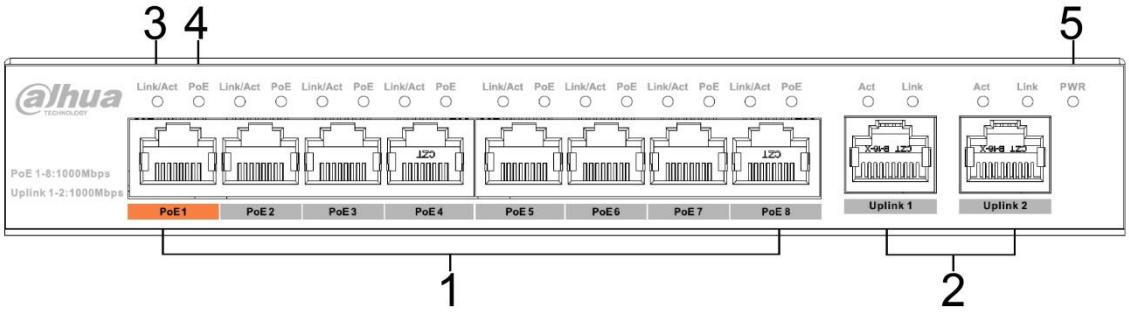

Table 2-1 The description of front panel

No.	Name	Description
1	10/100/1000 Base-T	8 × 10/100/1000 Mbps self-adaptive PoE power supply ports.
2	10/100/1000 Base-T	2 × 10/100/1000 Mbps self-adaptive uplink ports.
3	Link/Act	Single port Link status indicator light.
4	PoE	Single port PoE status indicator light.
5	PWR	Power indicator light, meanwhile it is the PoE power supply status indicator light.

2.2 Rear Panel

Figure 2-2 Back panel

Table 2-2 The description of back panel

No.	Name	Description
1	Ground terminal	GND.
2	Lock hole	Locks the switch.
3	Power port	Supports DC 48V–57V.

2.3 Side Panel

Figure 2-3 Side panel

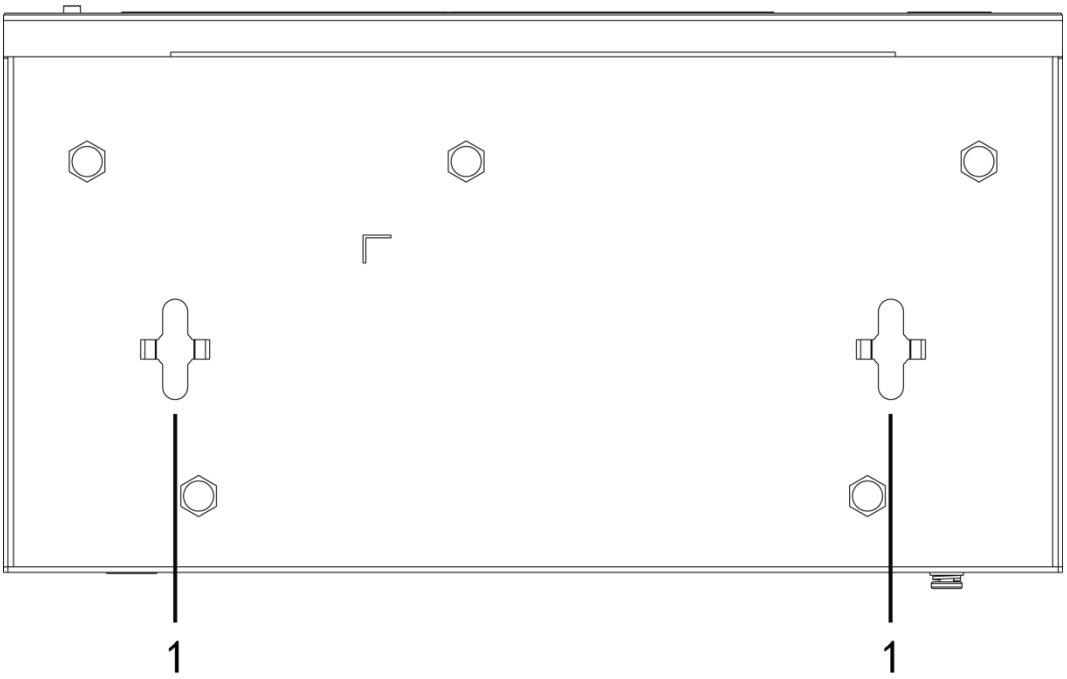

Table 2-3 The description of side panel

No.	Name	Description
1	Wall-mount hole	Supports the wall-mount installation.

2.4 PoE Power Supply

- One 1000M RJ-45 port supports IEEE802.3af, IEEE802.3at standards and Hi-PoE 60W power supply.
- Seven 1000M RJ-45 ports support IEEE802.3af, IEEE802.3at standard power supply.

Appendix 1 Cybersecurity Recommendations

1 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.

2 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.

3 "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.
- It is recommended that you enable your device's firewall or blacklist and whitelist feature to reduce the risk that your device might be attacked.

ENABLING A SAFER SOCIETY AND SMARTER LIVING

Zhejiang Dahua Vision Technology Co., Ltd | Address: No.1199 Bin an Road, Binjiang District, Hangzhou, PRC. | Tel: +86-571-87688883
Website: www.dahuasecurity.com | Fax: +86-571-87688815 | Email: overseas@dahuatech.com | Postcode: 310053