Dahua Single, 4, 8-Port Fiber Transceiver

User's Manual

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

V1.0.3

Important Safeguards and Warnings

Please read the following safeguards and warnings carefully before using the product in order to avoid damages and losses.

Attention:

- Do not expose the device to lampblack, steam or dust. Otherwise it may cause fire or electric shock.
- Do not install the device at position exposed to sunlight or in high temperature. Temperature rise in device may cause fire.
- Do not expose the device to humid environment. Otherwise it may cause fire.
- The device must be installed on solid and flat surface in order to guarantee safety under load and earthquake. Otherwise, it may cause device to fall off or turnover.
- Do not place the device on carpet or quilt.
- Do not block air vent of the device or ventilation around the device. Otherwise, temperature in
- device will rise and may cause fire.
- Do not place any object on the device.
- Do not disassemble the device without professional instruction.

Warning:

- Please use battery properly to avoid fire, explosion and other dangers.
- Please replace used battery with battery of the same type.
- Do not use power line other than the one specified. Please use it properly. Otherwise, it may cause fire or electric shock.

Special Announcement:

- This manual is for reference only.
- All the designs and software here are subject to change without prior written notice.
- All trademarks and registered trademarks are the properties of their respective owners.
- If there is any uncertainty or controversy, please refer to the final explanation of us.
- Please visit our website for more information.

Table of Contents

1 Product Overview

1.1 Features

Common Features:

- 2-layer industrial level switch.
- Conform IEEE802.3, IEEE802.3u, IEEE802.3ab/z and IEEE802.3X standards
- MAC automatic learning and aging, MAC address list capacity is up to 8K.
- All ports automatic adapt to MDI/MDIX mode.
- Industrial level wide temperature design.
- Adopt metal structure.
- Support 12 VDC power supply.

Individual Features:

- Single-port fiber switch supports 1 100/1000 Mbps self-adaptive SFP fiber port and 1 10/100/1000 Mbps self-adaptive RJ 45 port.
- 4-port fiber switch supports 1 100/1000 Mbps self-adaptive SFP fiber port, 1 10/100/1000 Mbps self-adaptive RJ 45 port and 4 10/100 Mbps self-adaptive RJ 45 ports.
- 8-port fiber switch supports 1 100/1000 Mbps self-adaptive SFP fiber port, 1 10/100/1000 Mbps self-adaptive RJ 45 port and 8 10/100 Mbps self-adaptive RJ 45 ports.

1.2 Typical Application

See Figure 1-1 for the typical networking scene.

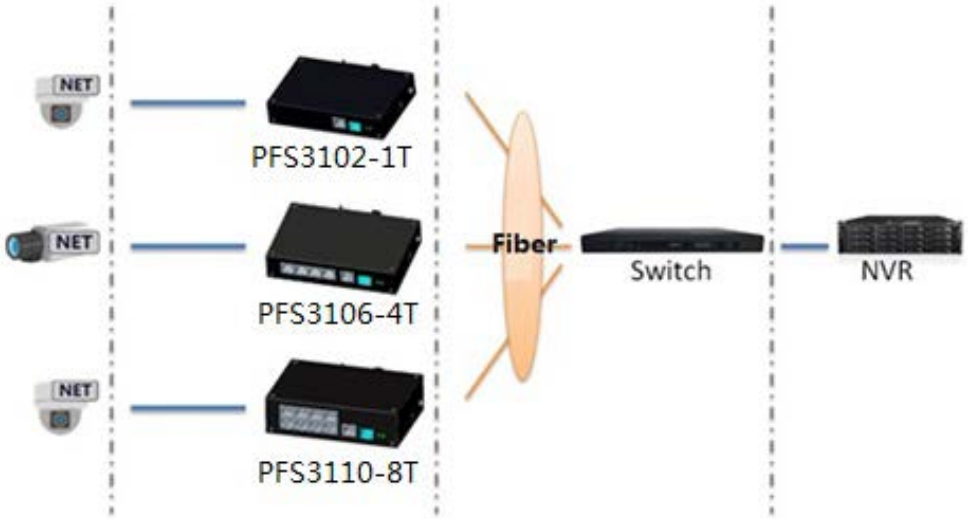

Figure 1-1

2 Device Structure

2.1 Single-port 1000 Mbps Fiber Transceiver

2.1.1 Front panel

The front panel is shown in Figure 2- 1.

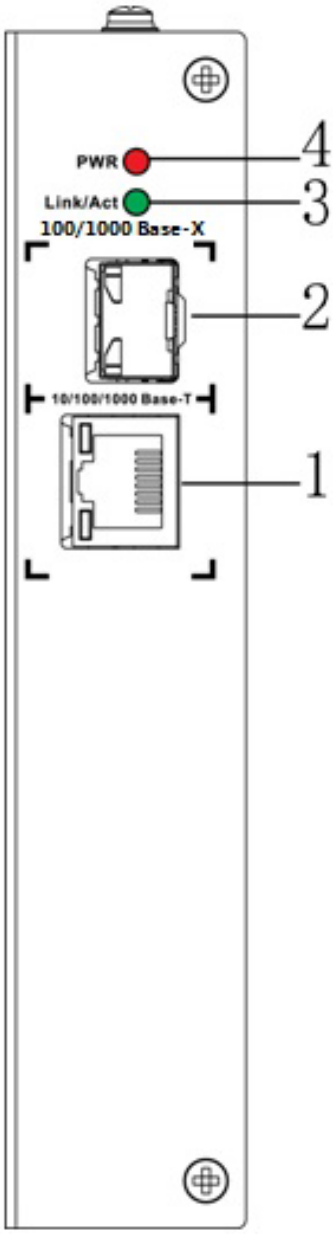

Figure 2- 1

Refer to Sheet 2-1 for more details.

SN	Name	Note
1	10/100/1000 Base-T	10/100/1000 Mbps self-adaptive RJ 45 port.
2	100/1000 Base-X	100/1000 Mbps self-adaptive SFP fiber port.
3	Link/Act	Fiber port status indicator light.

SN	Name	Note
4	PWR	Power indicator light

Sheet 2-1

2.1.2 Upper Cover

See Figure 2-2 for the device power port, which supports 12 VDC power supply.

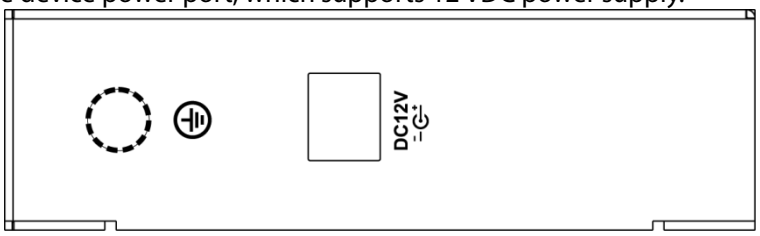

Figure 2-2

2.2 4-Port 1000 Mbps Fiber Transceiver

2.2.1 Front panel

The front panel is shown in Figure 2-3.

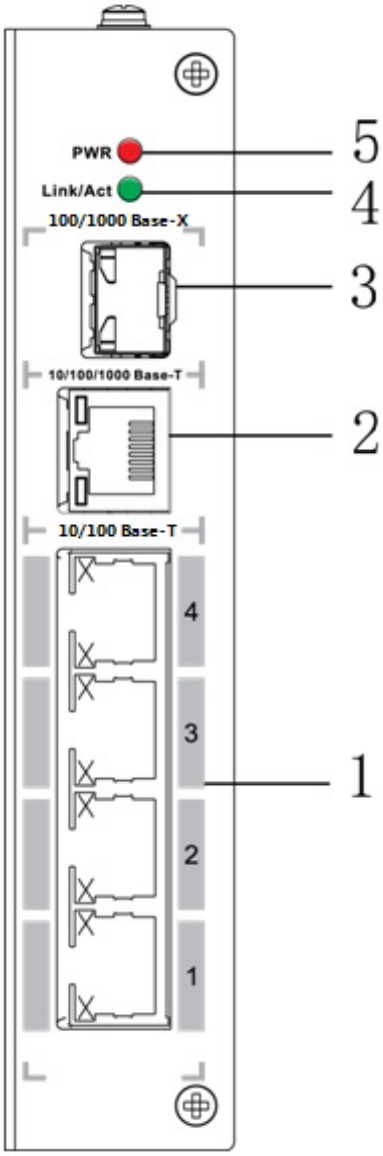

Figure 2- 3

Refer to Sheet 2-2 for more details.

SN	Name	Note
1	10/100 Base-T	4 10/100 Mbps self-adaptive RJ 45 ports
2	10/100/1000 Base-T	10/100/1000 Mbps self-adaptive RJ 45 port
3	100/1000 Base-X	100/1000 Mbps self-adaptive SFP fiber port
4	Link/Act	Fiber port status indicator light
5	PWR	Power indicator

Sheet 2-2

2.2.2 Upper Cover

See Figure 2-4 for the device power port, which supports 12 VDC power supply.

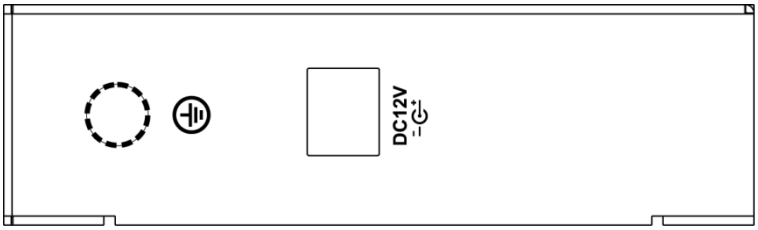

Figure 2-4

2.3 8-Port 1000 Mbps Fiber Transceiver

2.3.1 Front panel

The front panel is shown in Figure 2-5.

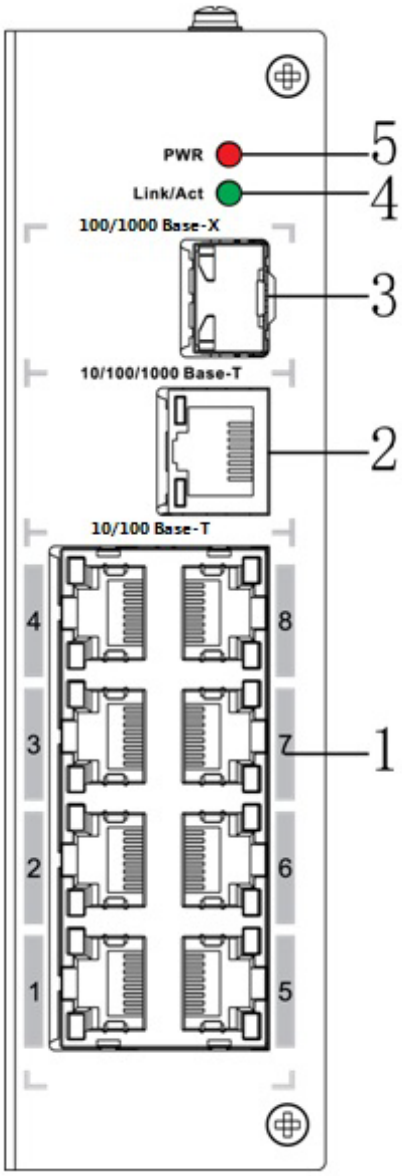

Figure 2-5

See Sheet 2-3 for more details.

SN	Name	Note
1	10/100 Base-T	8 10/100 Mbps self-adaptive RJ 45 ports
2	10/100/1000 Base-T	10/100/1000 Mbps self-adaptive RJ 45 port
3	100/1000 Base-X	100/1000 Mbps self-adaptive SFP fiber port
4	Link/Act	Fiber port status indicator light
5	PWR	Power indicator light

Sheet 2-3

2.3.2 Upper Cover

See Figure 2-6 for the device power port, which supports 12 VDC power supply.

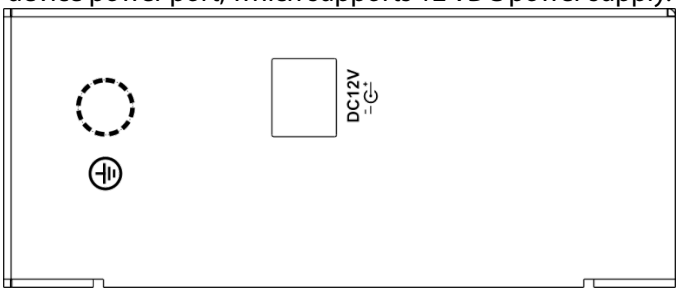

Figure 2-6

3 Installation Guide

The fiber transceiver supports guide rail installation.
Hang the hook of fiber transceiver on the slider, press the fiber transceiver to make the buckle stuck into the slider, see Figure 3-1 for more details.
Note:

- Both single-port 1000 Mbps fiber transceiver and 4-port 1000 Mbps fiber transceiver support the slider with the width of 28 mm.
- 8-port 1000 Mbps fiber transceiver supports the slider with the width of 38 mm.

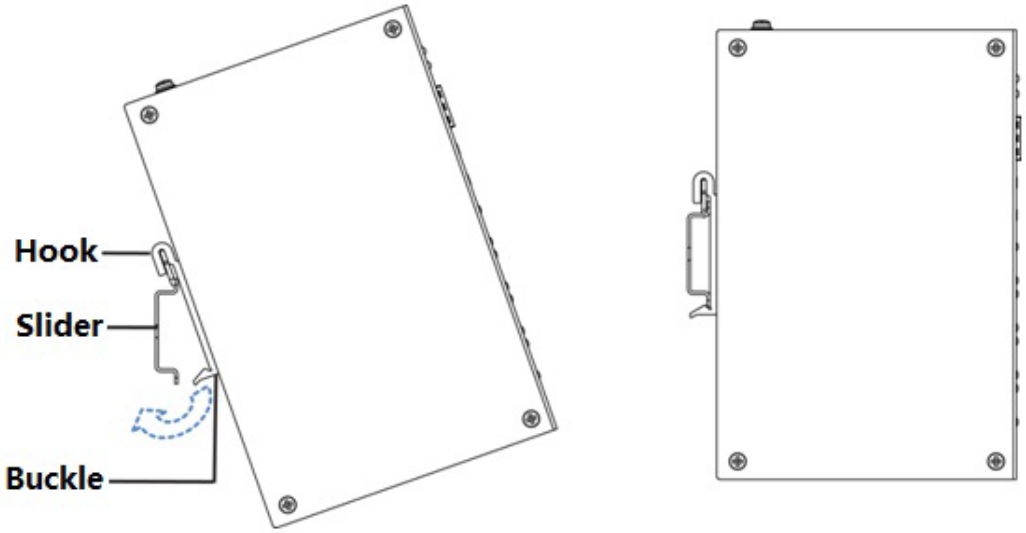

Figure 3-1

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