



DH-PFM Wireless Equipment

User's Manual

V1.0.0

ZHEJIANG DAHUA VISION TECHNOLOGY CO.,LTD.

Legal Statement

Copyrights

© 2017 ZHEJIANG DAHUA VISION TECHNOLOGY CO.,LTD.. All rights reserved.

Any or full contents of the user's manual cannot be copied, transmitted, distributed or stored, partially or wholly, by any means, without the prior written approval of ZHEJIANG DAHUA VISION TECHNOLOGY CO.,LTD. (hereinafter "Dahua").

Dahua or a third party may reserve the right of the product described in this user's manual. Without the prior written approval of the corresponding party, any person cannot copy, distribute, amend, abstract, reverse compile, disassemble, decode, reverse engineering, rent, transfer or sub-license the software.

Trademark

 and **HDCVI** are trademarks or registered trademarks of the Dahua in various jurisdictions. Other trademarks and company names mentioned herein are the properties of their respective owners.

Update and Revision

In order to enhance the product safety and provide you with better user experience, Dahua may improve the product via software auto update, but Dahua doesn't need to inform in advance and isn't liable to any responsibility.

Dahua reserves the right to revise any information in this document at any time; the revised contents will be added into the new version without further notice. There may be minor differences in some product functions after it is updated.

Cybersecurity Statement

- You are responsible for the risks resulting from connecting your product to the internet, including but not limited to, cyber-attacks, hacking attacks, computer viruses and malware, etc. Please protect your data and personal information by taking necessary actions, such as changing the default password and using a strong combination, changing your password periodically, keeping your firmware up-to-date, etc. Dahua is not responsible for any dysfunction, information leakage or other problems caused by failure to take necessary precautions to secure your devices. We will provide product maintenance services.
- To the extent not prohibited by applicable laws, Dahua and its employees, licensees, and affiliates are not liable for personal injury, or any incidental, special, indirect, or consequential damages whatsoever, including, without limitation, damages for loss of profits, corruption or loss of data, failure to transmit or receive any data, business interruption, or any other commercial damages or losses arising out of or related to the use or inability to use its products or services, however caused, regardless of the theory of liability (contract, tort or otherwise), even if it has been advised of the possibility of such damages. Some jurisdictions do not allow the exclusion or limitation of liability for personal injury, or of incidental or consequential damages, so this limitation may not apply to you.
- In no event shall liability for all damages (other than as may be required by applicable laws in cases involving personal injury) exceed the amount paid for products or services.

Cybersecurity Recommendations

Mandatory actions to be taken towards cybersecurity

1. Change Passwords and Use Strong Passwords:

The number one reason systems get “hacked” is due to having weak or default passwords. Dahua recommends changing default passwords immediately and choosing a strong password whenever possible. A strong password should be made up of at least 8 characters and a combination of special characters, numbers, and upper and lower case letters.

2. Update Firmware

As is standard procedure in the tech-industry, we recommend keeping NVR, DVR, and IP camera firmware up-to-date to ensure the system is current with the latest security patches and fixes.

Check the firmware release of your running devices. If the firmware release date is over 18 months old, please contact a Dahua authorized local distributor or Dahua technical support for available update releases.

“Nice to have” recommendations to improve your network security

1. Change Passwords Regularly

Regularly change the credentials to your devices to help ensure that only authorized users are able to access the system.

2. Change Default HTTP and TCP Ports:

- Change default HTTP and TCP ports for Dahua systems. These are the two ports used to communicate and to view video feeds remotely.
- These ports can be changed to any set of numbers between 1025-65535. Avoiding the default ports reduces the risk of outsiders being able to guess which ports you are using.

3. Enable HTTPS/SSL:

Set up an SSL Certificate to enable HTTPS. This will encrypt all communication between your devices and recorder.

4. Enable IP Filter:

Enabling your IP filter will prevent everyone, except those with specified IP addresses, from accessing the system.

5. Change ONVIF Password:

On older IP Camera firmware, the ONVIF password does not change when you change the system's credentials. You will need to either update the camera's firmware to the latest revision or manually change the ONVIF password.

6. Forward Only Ports You Need:

- Only forward the HTTP and TCP ports that you need to use. Do not forward a huge range of numbers to the device. Do not DMZ the device's IP address.
- You do not need to forward any ports for individual cameras if they are all connected to a recorder on site; just the NVR is needed.

7. Disable Auto-Login on SmartPSS:

Those using SmartPSS to view their system and on a computer that is used by multiple people should disable auto-login. This adds a layer of security to prevent users without the appropriate credentials from accessing the system.

8. Use a Different Username and Password for SmartPSS:

In the event that your social media, bank, email, etc. account is compromised, you would not want someone collecting those passwords and trying them out on your video surveillance system. Using a different username and password for your security system will make it more difficult for someone to guess their way into your system.

9. Limit Features of Guest Accounts:

If your system is set up for multiple users, ensure that each user only has rights to features and functions they need to use to perform their job.

10. UPnP:

- UPnP will automatically try to forward ports in your router or modem. Normally this would be a good thing. However, if your system automatically forwards the ports and you leave the credentials defaulted, you may end up with unwanted visitors.
- If you manually forwarded the HTTP and TCP ports in your router/modem, this feature should be turned off regardless. Disabling UPnP is recommended when the function is not used in real applications.

11. SNMP:

Disable SNMP if you are not using it. If you are using SNMP, you should do so only temporarily, for tracing and testing purposes only.

12. Multicast:

Multicast is used to share video streams between two recorders. Currently there are no known issues involving Multicast, but if you are not using this feature, deactivation can enhance your network security.

13. Check the Log:

If you suspect that someone has gained unauthorized access to your system, you can check the system log. The system log will show you which IP addresses were used to login to your system and what was accessed.

14. Physically Lock Down the Device:

Ideally, you want to prevent any unauthorized physical access to your system. The best way to achieve this is to install the recorder in a lockbox, locking server rack, or in a room that is behind a lock and key.

15. Connect IP Cameras to the PoE Ports on the Back of an NVR:

Cameras connected to the PoE ports on the back of an NVR are isolated from the outside world and cannot be accessed directly.

16. Isolate NVR and IP Camera Network

The network your NVR and IP camera resides on should not be the same network as your public computer network. This will prevent any visitors or unwanted guests from getting access to the same network the security system needs in order to function properly.






For latest information about Dahua cybersecurity statement and recommendations, please visit www.dahuasecurity.com.

Overview

This document elaborates installation, configuration and use of DH-PFM wireless equipment.

Symbol Definition

The following symbols may appear in the document. Please refer to the table below for the respective definition.

Symbol	Note
 Danger	It means highly potential danger. It will cause severe injury or casualties if it fails to avoid.
 Warning	It means moderate or low potential danger. It may cause slight or moderate injury if it fails to avoid.
 Caution	It means potential risk. It may cause device damage, data loss, weaker performance or other unpredictable consequences if it fails to avoid.
 Tip	It means that it can help you to solve a problem or save your time.
 Note	It means the additional information, which is the emphasis and supplement of the main body.

Important Safeguards and Warnings

Before use, please read the following requirements carefully and conform to them strictly, in order to prevent danger and property loss.



Caution

- Please transport, use and store this product under allowed temperature and humidity.
- Please don't expose the product to direct sunlight or close to a heating source.
- Please don't place the product at humid, dusty or fuliginous places.
- Please install the product at well-ventilated places. Prohibit blocking its air vent.
- Please install the product at flat and stable places.
- Please don't drip or splash liquids onto the product.
- Please don't put other things onto the product.
- Please don't dismantle the product arbitrarily.



Warning

- Please use recommended power line within rated specifications.

Special Announcement

- This manual is for reference only. Please refer to the actual product for more details.
- This manual will be regularly updated according to product changes, and the updated contents will be added into the new version without prior announcement.
- Please contact Customer Service Department of this company for the latest program and supplementary instructions.
- The user shall undertake any losses resulting from violation of guidance in the manual.
- Regarding possible doubts or disputes in the manual, final explanations of the company shall prevail.

Table of Contents

Legal Statement	I
Cybersecurity Statement and Recommendations	II
Preface	V
Important Safeguards and Warnings	VI
Description	VIII
1 Product Overview	1
1.1 Product Overview.....	1
1.2 Overview of TDMA Technology.....	3
1.3 Technical Features.....	4
1.4 Equipment Kit.....	5
1.5 Application Range.....	5
1.6 Hardware Profile.....	6
2 Product Installation	7
2.1 Equipment Installation.....	7
2.2 Description of Equipment Line Connection.....	9
2.3 Restore Factory Defaults.....	9
3 Common Networking	11
3.1 Wireless Point-to-point.....	11
3.2 Wireless Point-to-multipoint.....	12
3.3 Adjustment of Wireless Coverage Dead Angle.....	13
4 Status Display	14
5 Setting Wizard	17
6 Wireless Settings	23
7 Network Settings	26
8 Advanced Settings	29
9 System Settings	31
10 Tool Application	33
Appendix 1 Industry Application	35
Appendix 1.1 Wireless Surveillance of Safe Site.....	35
Appendix 1.2 Wireless Surveillance of Safe Town.....	38
Appendix 2 Troubleshooting	40
Appendix 3 Points for Attention	42
Appendix 4 Test Report	44
Appendix 5 Technical Specification	50

Description



Table 1 Release Note

Version	Release Date	Revised Chapter	Author
1.0	2014-05-12	Create	cl

Aim of Manual

This manual mainly enables users to get familiar with DH-PFM88X, helps users to use it and solve some common problems when necessary. This manual mainly involves DH-PFM88X hardware information, WEB page parameters, configuration mode, networking mode and fault analysis, so as to effectively help users to know and use the equipment quickly, and shorten the time for users to know DH-PFM series products.

Table 2 Definition of Nouns and Description of Abbreviations

No.	Definition or Abbreviation	Description
1	DH-PFM880	AP local side
2	DH-PFM881	CPE client
3	DH-S4200-24T	Indoor switch without fan
4	DH-S4000-7X	Outdoor quasi-industrial switch with wide temperature range

1 Product Overview

DH-PFM88X series equipment owns unique built-in TDMA wireless technology. This technology combines advanced core technologies in the industry, and boasts features such as long transmission distance, high throughput and strong anti-interference performance.

TDMA technology includes TDMA, flexible configuration of 5M/10M/20M/40MHz bandwidth, rate control and ACK overtime automatic adjustment technologies. TDMA effectively solves hidden node problem that perplexes large point-to-multipoint WLAN. Flexible configuration of 5M/10M/20M/40MHz bandwidth realizes balance between scarce wireless bandwidth resource and complicated working scenes. With advanced rate control algorithm, adapt to channel quality changes quickly while keeping stable rate as far as possible. ACK overtime automatic adjustment technology detects the distance between access point and client automatically, adjusts wireless parameters and optimizes the equipment performance.

DH-PFM881 maximum point-to-point transmission distance reaches 3km and maximum transmission rate reaches 300Mbps. With excellent remote transmission performance, its throughput rate reaches 40Mbps (open space) at 3km and multi-channel HD video can be transmitted. AP equipment supports point-to-point and point-to-multipoint remote access wireless mode; CPE supports point-to-point remote access mode.

1.1 Product Overview

With a small body, DH-PFM88X boasts the most advanced design technology in the industry, wireless transmission effect comparable to base station, and high cost performance advantage.

The equipment adopts unique TDMA wireless technology, integrates advanced TDMA, MIMO and Multi-hop technologies, innovative compatibility and improved 802.11n protocol, and thus guarantees long distance, throughput rate and anti-interference performance of wireless transmission. Compared to products of other manufacturers, DH-PFM88X series wireless equipment owns the following advantages:

1. Integrate TDMA Technology

DH-PFM88X owns TDMA operating system and integrates with TDMA technology, which effectively solves hidden node problem that perplexes large point-to-multipoint WLAN. With advanced rate control algorithm, adapt to channel quality changes quickly while keeping stable rate as far as possible, so it is very suitable for remote wireless transmission. By solving remote point-to-multipoint access issue, access quantity increases, rate allocation becomes more uniform, and it can be applied to operator and wireless surveillance fields.



As a wireless equipment operating system redeveloped on the basis of kernel, TDMA is more suitable for wireless video surveillance data transmission.

2. Integrate Watchdog

DH-PFM88X integrates hardware watchdog to monitor system operation all the time. In case of abnormal system operation, watchdog resets and reboots the system, so as to ensure its stability effectively and reduce manual operation.

3. Ping Watchdog Function Carries out Real-time Detection of Link

Ping Watchdog function detects whether the link fails or not, and reboots the equipment immediately when the link fails, so as to ensure link stability.

4. A Lot of Frequency is Provided to the User

At present, most wireless products work at standard 802.11 5.8G frequency, but standard 5.8G frequency band is relatively scarce. When 5.8G equipment is used a lot, it is easily interfered. DH-PFM88X increases support for frequency near 5.8G and expands working frequency to 4920MHz-6100MHz within allowed range. Since some frequencies face less interference, clients and access points in these frequency bands work better than other frequency bands. DH-PFM88X supports for non-standard frequency band has reduced external interference to wireless product, enhanced its throughput rate effectively and satisfied users' requirements for relatively high bandwidth.



Before using these non-standard frequency bands, please confirm whether they conform to local laws, regulations and radio management stipulations.

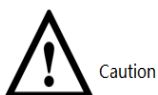
5. Adapt to Complicated and Changing Working Environment

DH-PFM88X is able to work in complicated and changing environment: working temperature ranges from -30°C to 70°C, while working humidity ranges from 5% to 95%. DH-PFM88X keeps relatively high throughput rate in all kinds of harsh environment for a long time, such as thunderstorm, high temperature and high humidity, low temperature and low humidity.

1.2 Overview of TDMA Technology

At present, most remote Wi-Fi network bridge products have developed from 802.11 WLAN technology. Built-in TDMA operating system integrates TDMA, flexible configuration of 5M/10M/20M/40MHz bandwidth, rate control and ACK overtime automatic adjustment technologies, and it is known as an ideal remote Wi-Fi access product. TDMA effectively solves hidden node problem that perplexes large point-to-multipoint WLAN. Flexible configuration of 5M/10M/20M/40MHz bandwidth realizes balance between scarce wireless bandwidth resource and complicated working scenes: narrow wireless bandwidth configuration is used when there are less idle wireless channels and single user doesn't place a high requirement on wireless access rate; wide wireless bandwidth configuration is used when there are many idle wireless channels and single user places a high requirement on wireless access rate. Moreover, narrow wireless bandwidth configuration is more effective in sheltered environment. With advanced rate control algorithm, adapt to channel quality changes quickly while keeping stable rate as far as possible, so it is very suitable for remote wireless transmission. ACK overtime automatic adjustment technology detects the distance between access point and client automatically, adjusts wireless parameters and optimizes the equipment performance.

Before AP enables TDMA, client shall set a priority. When one AP connects multiple clients and different clients place different requirements on bandwidth, priority shall be set according to bandwidth requirements of client on present equipment. In case of high bandwidth requirements, it is suggested that the priority should be set to be high; on the contrary, the priority should be set to be low. Of course, if all clients place the same requirements on bandwidth, priority of all clients can be the same



TDMA function can be enabled by AP; client can set its own priority. Other manufacturers' TDMA cannot intercommunicate with our TDMA.

1.3 Technical Features

- 1) Integrate TDMA and effectively enhance “point-to-multipoint” overall performance.
- 2) Support client priority setting and better deploy every client in case of point-to-multipoint.
- 3) Support Ping Watchdog and real-time monitoring of wireless link; reboot the equipment automatically when wireless link disconnects, and thus ensure its stability.
- 4) Support outdoor high temperature and low temperature: -30-70°; quasi-industrial design, waterproof IP66 grade.
- 5) Recommended wireless coverage range is 3km.
- 6) Lightning protection of radio frequency port reaches 15KV ESD.
- 7) Support automatic distance measurement function; display straight-line distance between client and base station in a real-time way.
- 8) Support automatic rebooting and restoration function of the equipment.
- 9) Full-band support: frequency spreading supports 4920~6100Mhz.
- 10) Support flow control; control input/output flow of base station/client effectively.
- 11) Support VLAN division, realize VLAN function and control broadcast storm.
- 12) Support 802.1x authentication method, ensure client access control effectively and provide access security.
- 13) Support multi-channel selection (5M/10M/20M/40M); promote anti-interference and penetrating power effectively.
- 14) Support 4 working modes: AP, Station, AP-WDS and Station-WDS.
- 15) Unique design of antenna radio-frequency amplifier and low-noise receiver guarantees remote video, audio and data transmission.
- 16) Human-oriented working mode wizard configuration is convenient for those who are not wireless professionals.
- 17) POE power supply supports international 802.3af standard, and becomes more convenient and

reliable.

18) Support IP login, carry out remote control and management via webpage, and thus facilitate configuration.

19) Waterproof ultraviolet-proof shell ensures that the equipment works stably outdoors.

1.4 Equipment Kit



No.	DH-PFM880	DH-PFM881
1	Host*1	Host*1
2	Antenna*1	N/A
3	Feeder*2	Cable tie *2
4	POE power supplier (24V/0.5A)*1	POE power supplier (24V/0.5A)*1
5	Instruction book	Instruction book
6	Other installation packages	Other installation packages

Table 1-1 Packing List

1.5 Application Range

- ◆ **First-choice recommendation:** safe town, safe construction site, safe scenic area, elevator IP HD wireless video surveillance.
- ◆ **Secondary recommendation:** unblocked scenes such as playground, pasture and suburb crossroad.

1.6 Hardware Profile

Hardware Index	
CPU/Baseband Radio	Atheros AR9344
Memory	64MB DRAM, 8MB Flash
Physical Interface	2×10/100M Base-TX (Cat. 5/5E, RJ-45) network interface
LED Indicator Light	Power, LAN, WLAN, 3×Link Quality
Power Supply	POE, Power Adapter 24V/0.5A

Table 1-2 Hardware Information

Description of LED Mechanism

DH-PFM88X adopts LED to display present working status and connecting quality, so users know its present working condition visually without logging onto the webpage. LED mainly consists of two parts, equipment status and connecting quality. The first LED in the left is power indicator light, the second one in the left is network indicator light and the third one is connection indicator light. The first one to the third one in the right is signal strength indicator light.



Figure 1-1 LED Indicator Light on DH-PFM881 Shell

LED	Color	Status
POWER	Green	When this light turns on, it means that DH-PFM88X is connected with power supply.
LAN	Green	When this light turns on, it means that DH-PFM88X LAN port is connected with external equipment.
WLAN	Green	When this light turns on, it means that DH-PFM88X wireless is enabled. When this light flickers, it means that equipment wireless is enabled, and data is wirelessly transmitted.
Signal Strength	Red	Indicator light shows signal strength.
	Yellow	Green light means high signal strength.
	Green	Yellow light means medium signal strength. Red light means very weak signal or no signal.

Table 1-3 LED Information

2 Product Installation

2.1 Equipment Installation

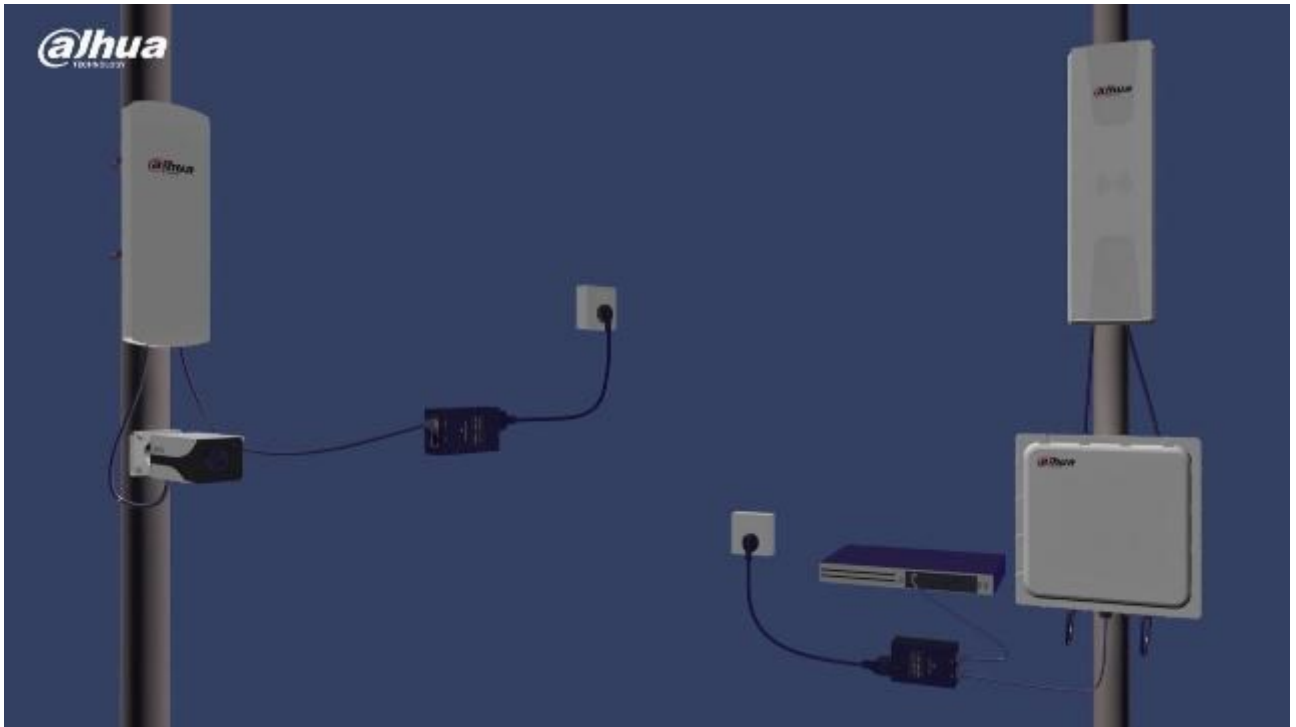


Figure 2-1 DH-PFM88X Overall Installation Diagram



Caution

DH-PFM88X line connection type differs under different network modes. Since its default setting is network bridge mode, this chapter mainly describes line connection type of network bridge mode. For connection type of route mode, please refer to Chapter 7 Route Mode of Network Setting.

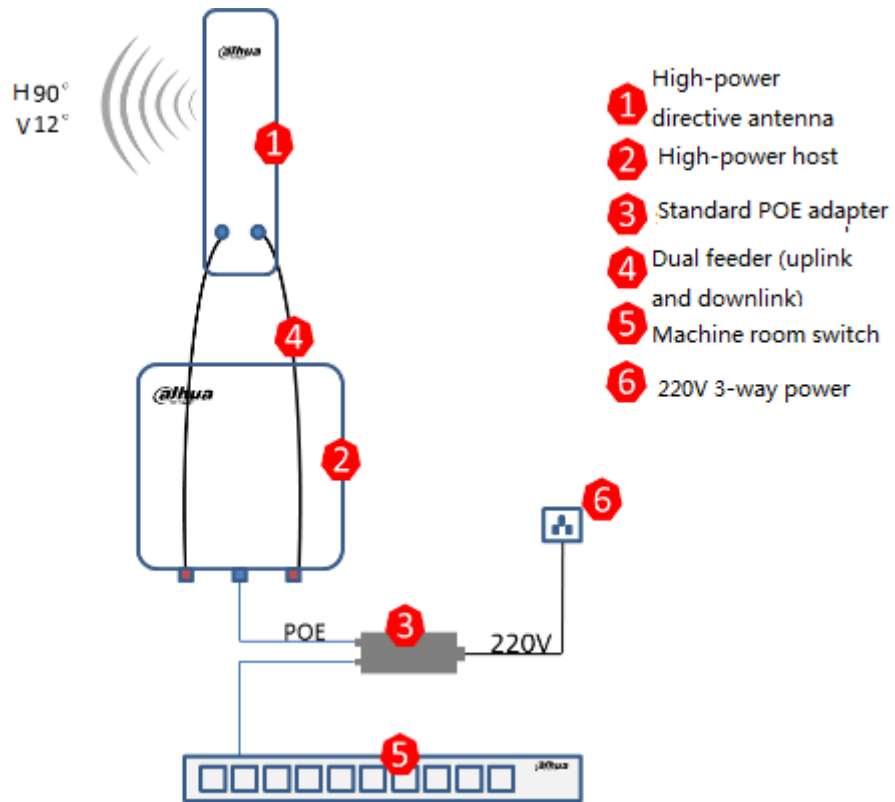


Figure 2-2 DH-PFM880 Installation Diagram

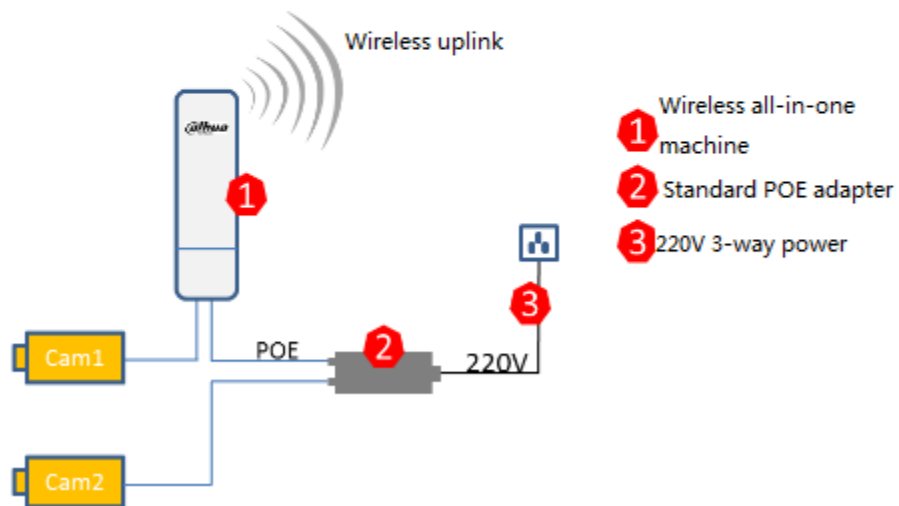


Figure 2-3 DH-PFM881 Installation Diagram

2.2 Description of Equipment Line Connection

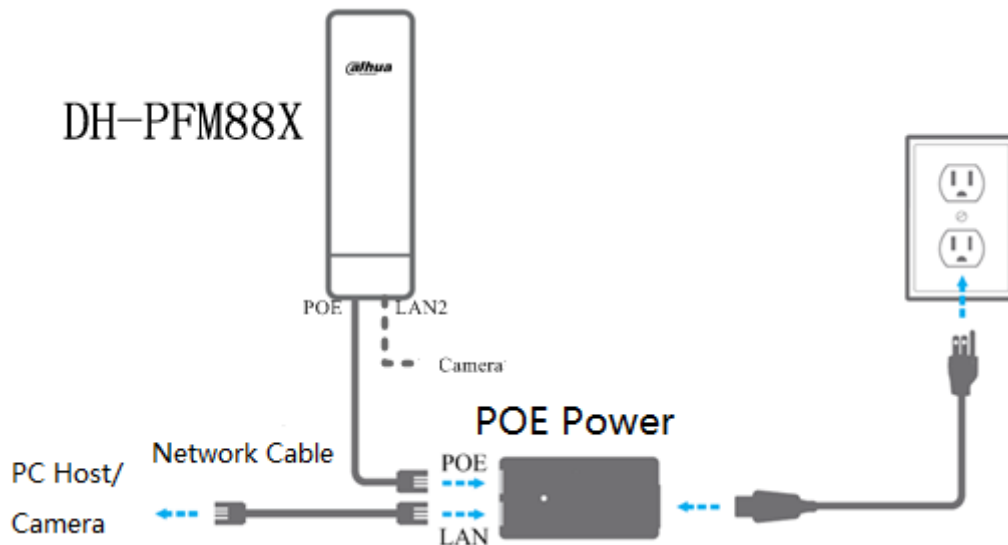


Figure 2-4 DH-PFM88X Interface Connection Diagram

Type	Interface	Interface Name	Connection and Function
DH-PFM881	Two RJ45 interfaces	POE	Connect "POE" on POE power supply with twisted pair cable; provide DH-PFM881 equipment with 24V power supply and data transmission.
		LAN2	As "LAN" interface, it can connect IP Camera. Any LAN port can be used for equipment debugging.
DH-PFM880	One RJ45 interface	None	Connect "POE" interface on POE power supply with network cable; provide DH-PFM880 equipment with 24V power supply and data transmission. "LAN" interface on POE power supply connects a switch or other equipment, and serves as a debugging interface.

Table 2-1 Description of Port Connection

2.3 Restore Factory Defaults

If the user forgets DH-PFM88X IP, choose manual operation: press Reset key for 5-10s and release it after all LED turn on, when the equipment has restored factory defaults. Meanwhile, the network interface, which owns a direct connection with DH-PFM88X host, displays 2 continuous connections and disconnections.

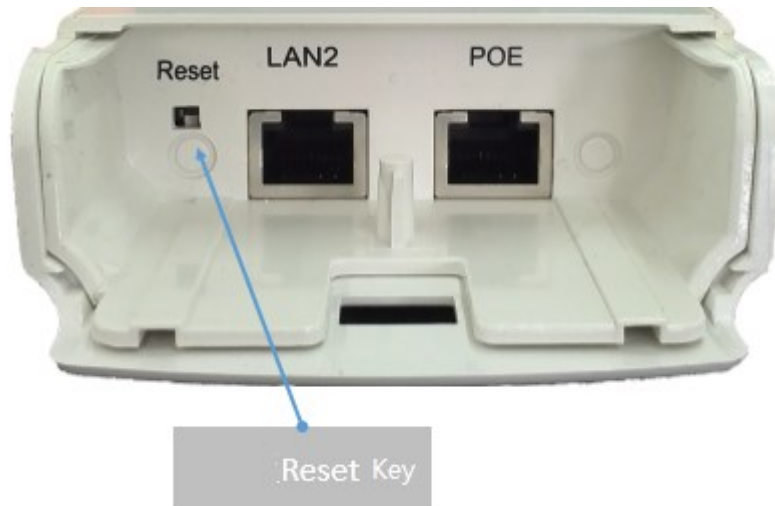


Figure 2-5 Restore Factory Defaults

Item	Factory Defaults
IP Address	192.168.1.36
User Name	admin
Password	admin
Wireless Mode	Client
Encryption Type	WPA->WPA2->CCMP->secret key: 1234567890abc
Network Mode	Network bridge mode

Table 2-2 Factory Defaults of Main Parameters



At network management page of the equipment (System Settings), click “Restore” and restore factory defaults. Factory parameters are shown in Table 2-2 Factory Defaults of Main Parameters.

3 Common Networking

3.1 Wireless Point-to-point

During point-to-point communications, one DH-PFM881 is usually set to be an access point, while the other DH-PFM881 equipment is the client. Actual connection diagram is as follows.

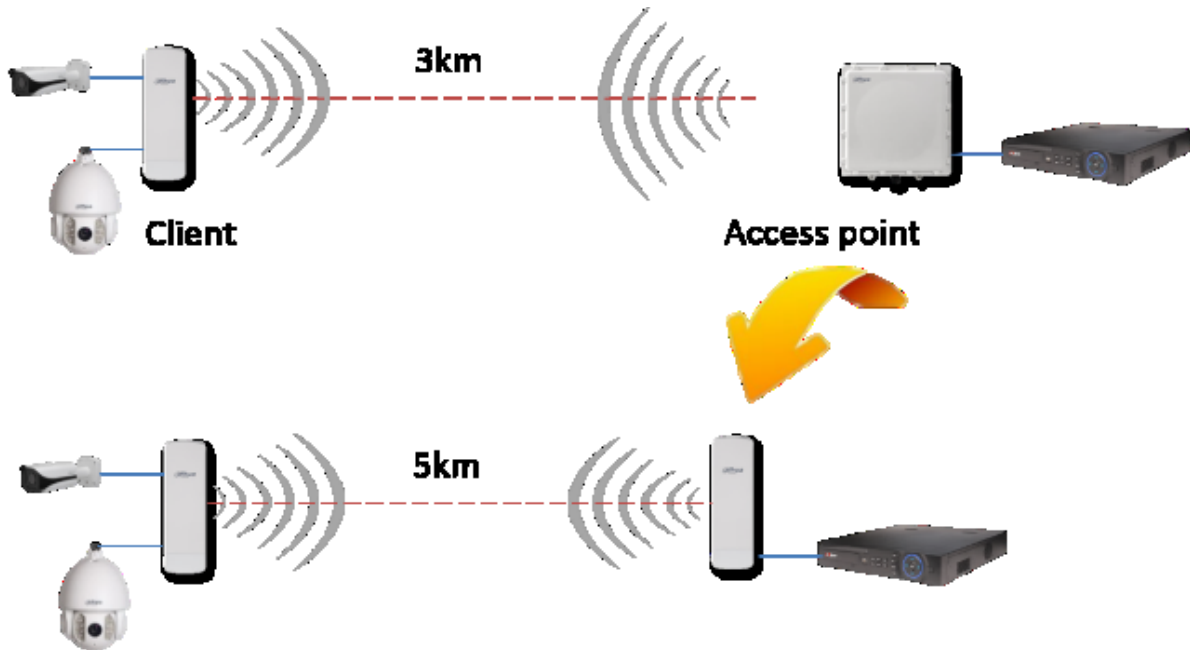


Figure 3-1 Networking Diagram of Access Point and Client

1. At Network Settings Page->Network Mode, both DH-PFM88X equipment shall be set to network bridge mode; firewall is prohibited in both equipment; they have different LAN IP.
2. At Wireless Page, wireless mode shall be set to be access point and client respectively. AP and client have the same SSID, the same encryption way and password. For example, WPA->WPA2->CCMP->1234567890. Output power is set to be 13dBm, AP frequency is 5.785GHz, whereas channel width of AP and client is 20MHZ.
3. **Caution:** directions of AP and client shall be opposite.
4. One computer pings the other computer. That is to say, input ping xxx.xxx.xxx.xxx (IP of the other computer) on one computer.

Expected result: after AP and client are connected, computers of AP and client can ping with each other. Meanwhile, connection quantity is 1 on AP status display page.

3.2 Wireless Point-to-multipoint

During point-to-multipoint communications, DH-PFM880 is usually set to be an access point (single AP covers 90 degrees and 4 AP cover 360 degrees), while other DH-PFM881 equipment shall be client. Actual connection diagram is as follows.

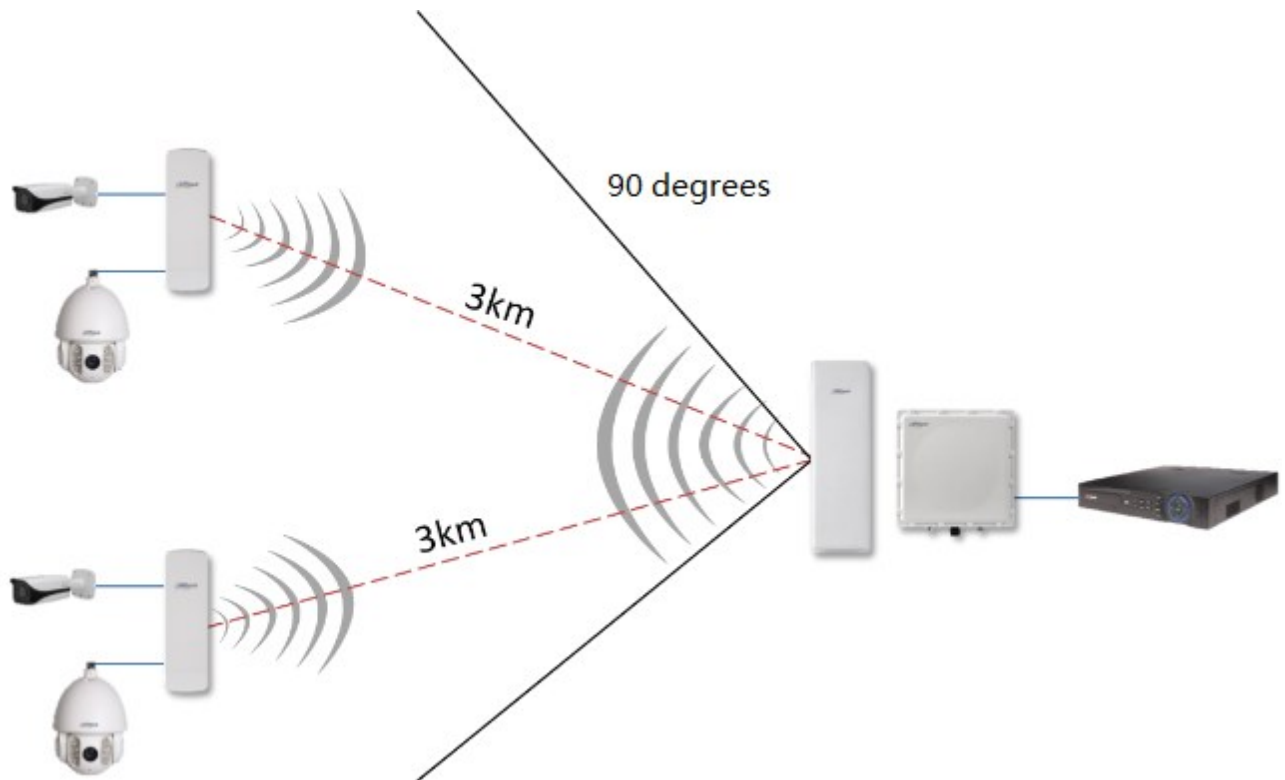


Figure 3-2 Point-to-multipoint Networking Diagram

1. At Network Settings Page->Network Mode, all DH-PFM88X equipment shall be set to network bridge mode; firewall is prohibited (which is disabled by default) in all equipment; they have different LAN IP.
2. At Wireless Page, wireless mode shall be set to be access point and client respectively. AP and client have the same SSID, the same encryption way and password. For example, WPA->WPA2->CCMP->1234567890. It is suggested that configuration should be completed according to equipment wizard.
3. **Caution:** directions of AP and client shall be opposite.
4. One computer pings the other computer. That is to say, input ping xxx.xxx.xxx.xxx (IP of the other computer) on one computer.

Expected result: after AP and client are connected, computers of AP and client can ping with each other.

Meanwhile, connection quantity is N (representing the quantity of connected clients) on AP status display page.

3.3 Adjustment of Wireless Coverage Dead Angle

When client adopts direct wireless communications with central AP (access point) because surveillance point is blocked seriously, two sets of CPE realize back-to-back connection and carry out angle adjustment. Actual connection diagram is as follows.

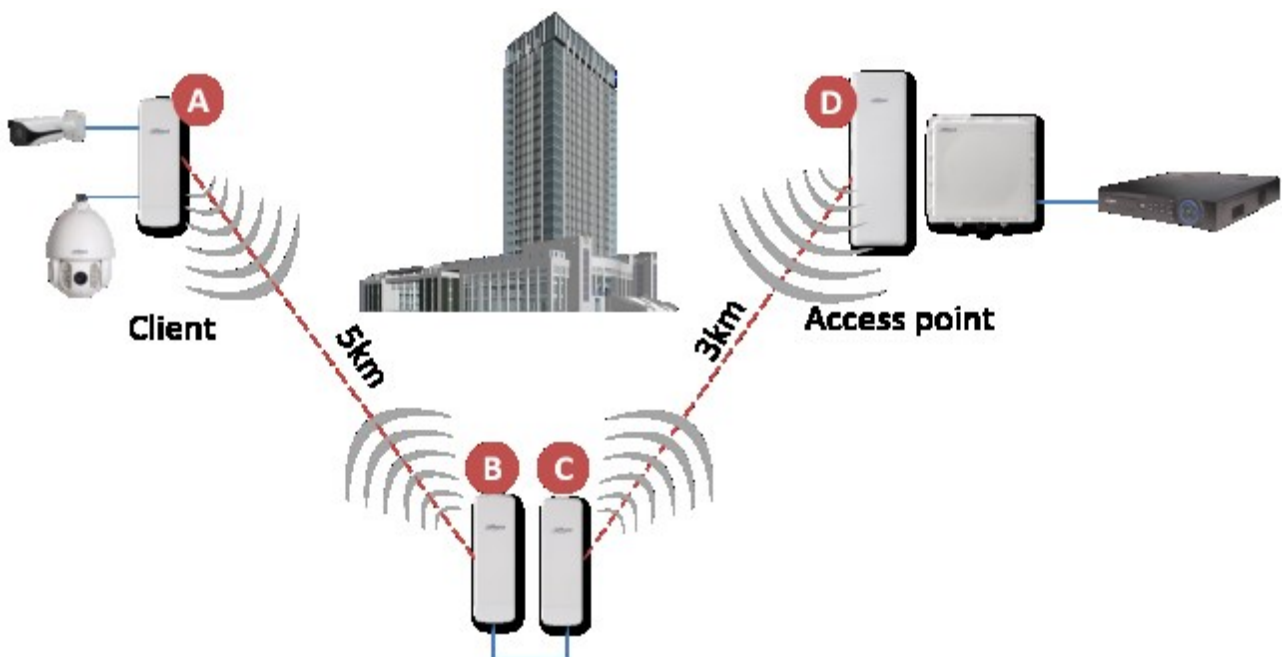


Figure 3-3 Networking Diagram of Coverage Dead Angle Adjustment

1. Two back-to-back equipment shall adopt wired connection.
2. Downlink client equipment is set to be access point; uplink central AP equipment is set to be client.
3. For specific configuration of single equipment, please refer to setting wizard configuration.

Network Bridge	Equipment	Mode	Frequency (MHz)	Network Name	Password
A&B Pairing	A	Client	Default	Dahua1	Dahautech1
	B	AP	5745MHz(149)	Dahua1	Dahautech1
C&D Pairing	C	Client	Default	Dahua2	Dahautech2
	D	AP	5825MHz(165)	Dahua2	Dahautech2

Corresponding Table of Pairing Across Network



Caution

By default, client doesn't need to set equipment frequency, but differentiates by network name and password. High-end user can set client input frequency at wireless setting page.

4 Status Display

As the first page after the user logs on, status display page shows present configuration of the equipment and real-time monitoring of present working status. It is the 2nd item of menu bar.

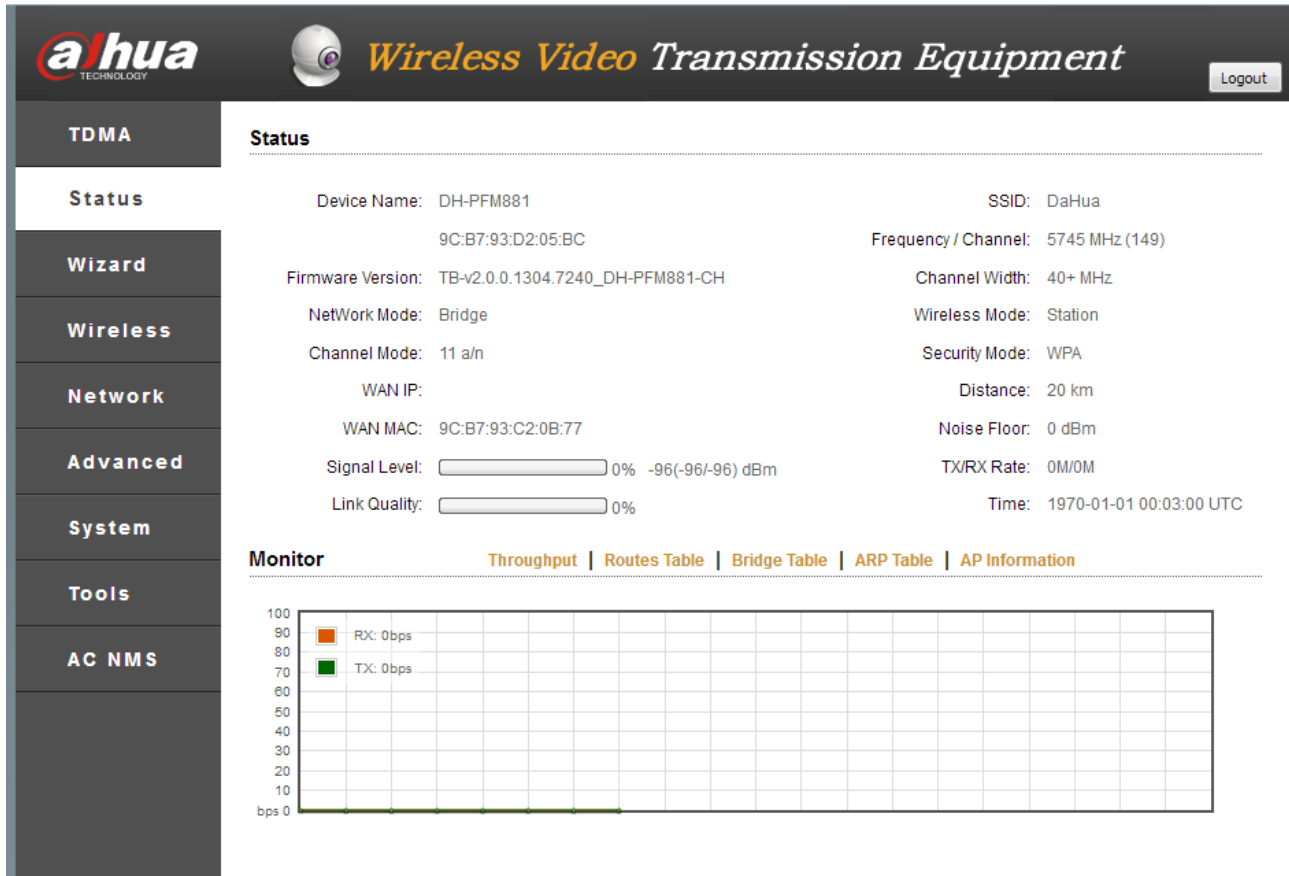


Figure 4-1 Status Display

Item	Function	Item	Function
Name	DH-PFM88X	Kernel Version	V2.1.0.2681.9344
Firmware Version	Software version number	802.11 Mode	Conform to 802.11 protocol at present
WAN IP	IP address of WAN port in route mode	WAN MAC	MAC address of WAN port in route mode
Network Mode	Operation mode, route mode or network bridge mode	Network Name	Name of wireless network
Frequency/ Channel	Communications channel	Channel Width	There are 4 types, including 5M, 10M, 20M and 20/40M AUTO.
Wireless Mode	Client, AP, WDS client, WDS AP and WDS repeater	Encryption	Several encryption methods of wireless network
Distance	Distance between interconnected client and AP	Noise Floor	Interference from external environment
Signal	As a parameter for client, WDS	Link	Link connection quality

Level	client and WDS repeater, it shows overall signal level of client, as well as uplink and downlink signal level of client.	Quality	
TX/RX Rate	As a parameter for client, WDS client and WDS repeater, it shows momentary rate of transmitting/receiving data of present equipment.	Time	It displays time. When NTP client function is enabled, NTP server is set correctly and the equipment is online, the time item will be automatically updated to calibration time on NTP server. If it cannot go online, it has a default value.

Table 4-1 Parameters on Status Display Page

Real-time Monitoring

Throughput rate: also known as throughput capacity, it refers to data size passing every section within unit time. Throughput rate on status display page refers to data size transmitted on the network within unit time. This is a main index to measure network performance. With this index, the user can monitor data transmission speed of the equipment.

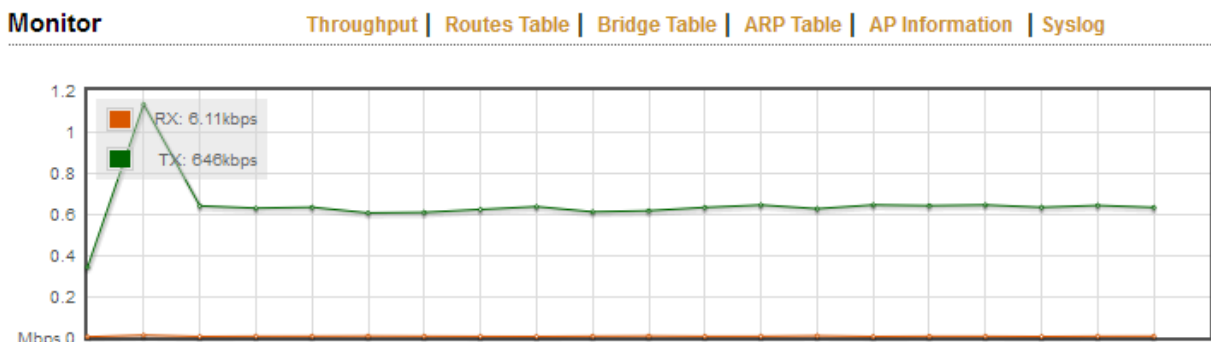


Figure 4-2 Throughput Rate

Routes table: it stores the path pointing to network of DH-PFM88X equipment.

Monitor			
Throughput Routes Table Bridge Table ARP Table AP Information Syslog			
Destination	Gateway	Netmask	Interface
192.168.1.0	*	255.255.255.0	br0

Figure 4-3 Routes Table

Bridge table: corresponding relation of MAC address and aging time of equipment whose communication has gone through DH-PFM88X in the past certain period, obtained by DH-PFM88X.

MAC Address	Ageing Timer
08:9e:01:bb:a2:8b	0.50
9c:b7:93:de:d9:2b	0.00
9c:b7:93:e0:d9:2b	0.00

Figure 4-4 Bridge Table

ARP table: corresponding relation of IP address and MAC address used by LAN port, whose communication has gone through DH-PFM88X in the past certain period, obtained by the equipment.

IP Address	MAC Address	Interface
192.168.1.11	08:9e:01:bb:a2:8b	br0

Figure 4-5 ARP Table

AP/Client Information Table

When the equipment connects a client in AP mode, it shows client information.

MAC Address	TX/RX Rate	RSSI
9c:b7:93:e0:40:69	216M/240M	65

Figure 4-6 Client Information

When the equipment connects an AP in client mode, it shows AP information.

MAC Address	TX/RX	Signal Level	Noise Floor	RX Packets	TX Packets	RX Bytes	TX Bytes
9c:b7:93:d2:05:bc	240M/240M	-27	-96	4877	1063943	3131930	39917838

Figure 4-7 AP Information

5 Setting Wizard

Precondition

Connect the equipment with configuration host and turn on power by reference to Figure 2-4 DH-PFM88X Interface Connection Diagram.

Operating Steps

Step 1 Configure static IP address of “192.168.1.x” segment of host IP address (for example, 192.168.1.180).

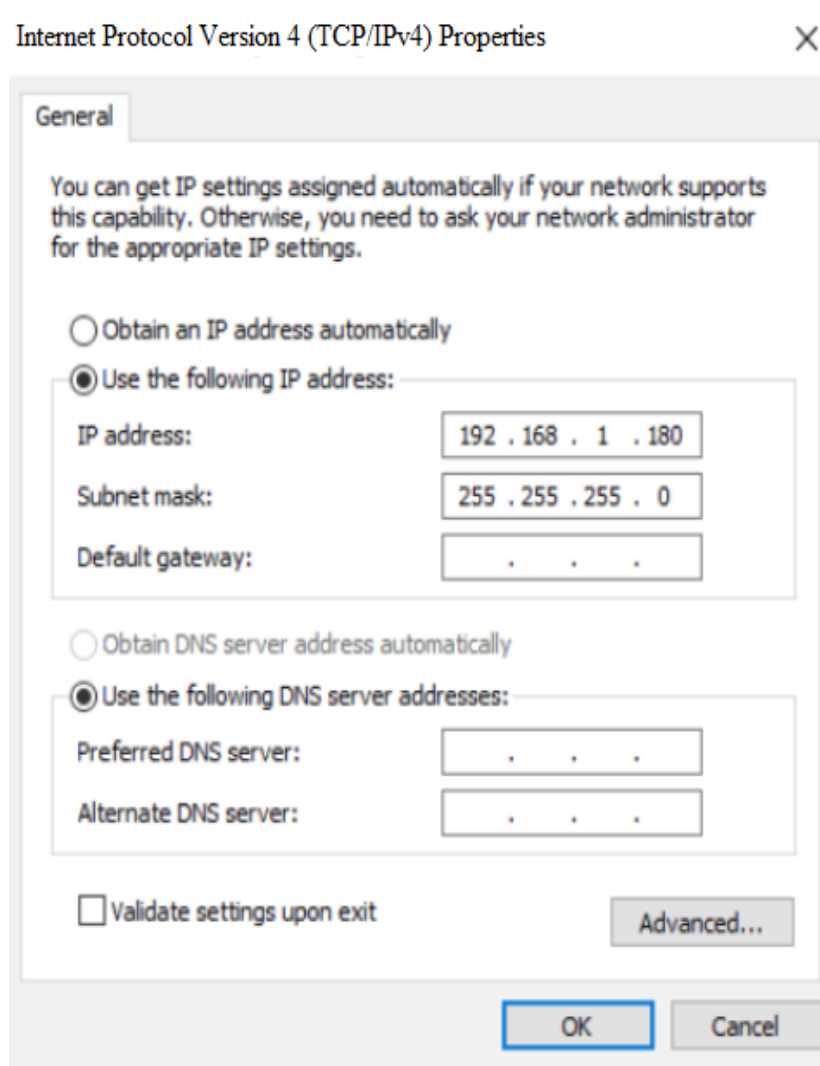


Figure 5-1 Host IP

Step 2 In the browser, input default IP address of DH-PFM88X: **192.168.1.36**. The system shows login page.



Figure 5-2 Login Page

Step 3 Input username and password (whose default values are **admin**), and click “Confirm”. The system shows status display page, including basic information, such as working status, present settings and software version of DH-PFM88X equipment.

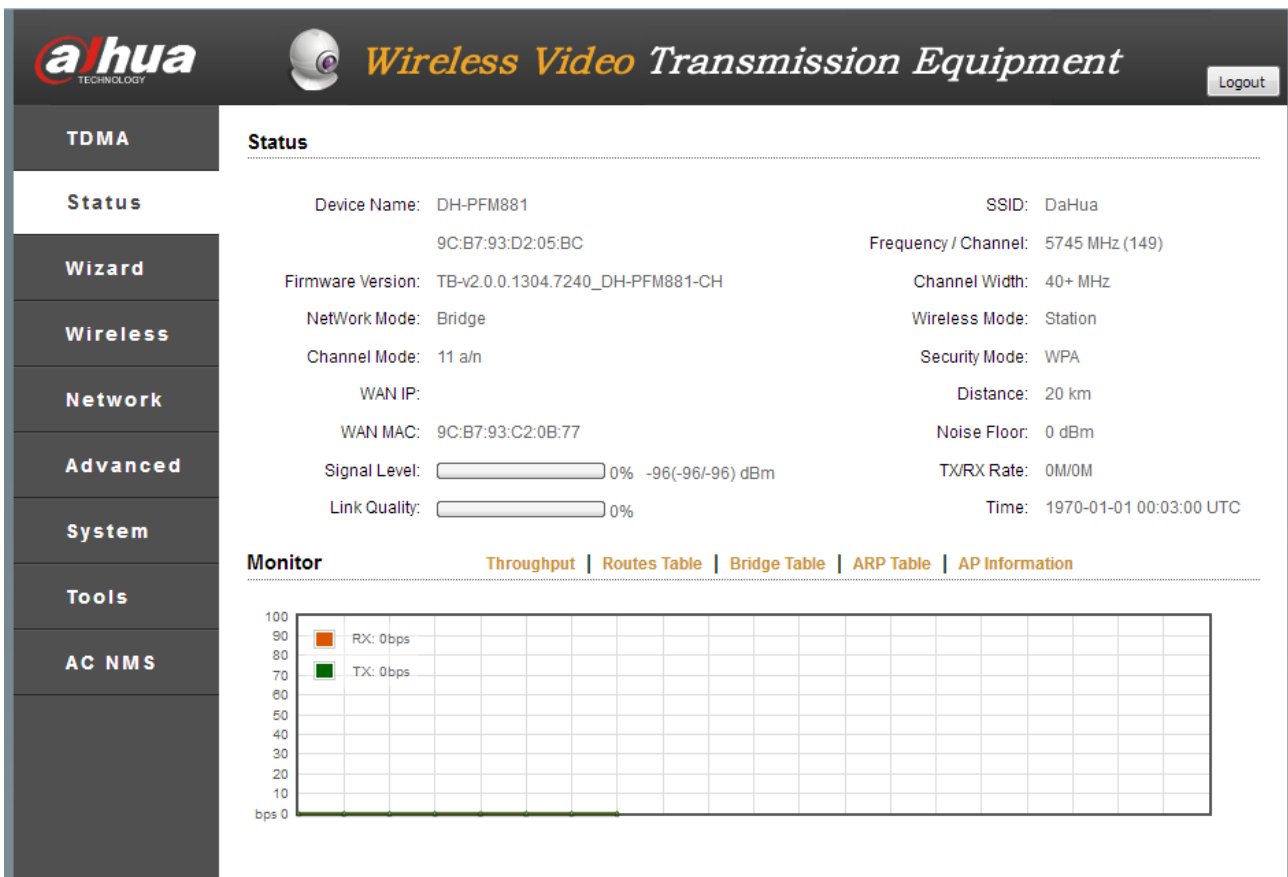
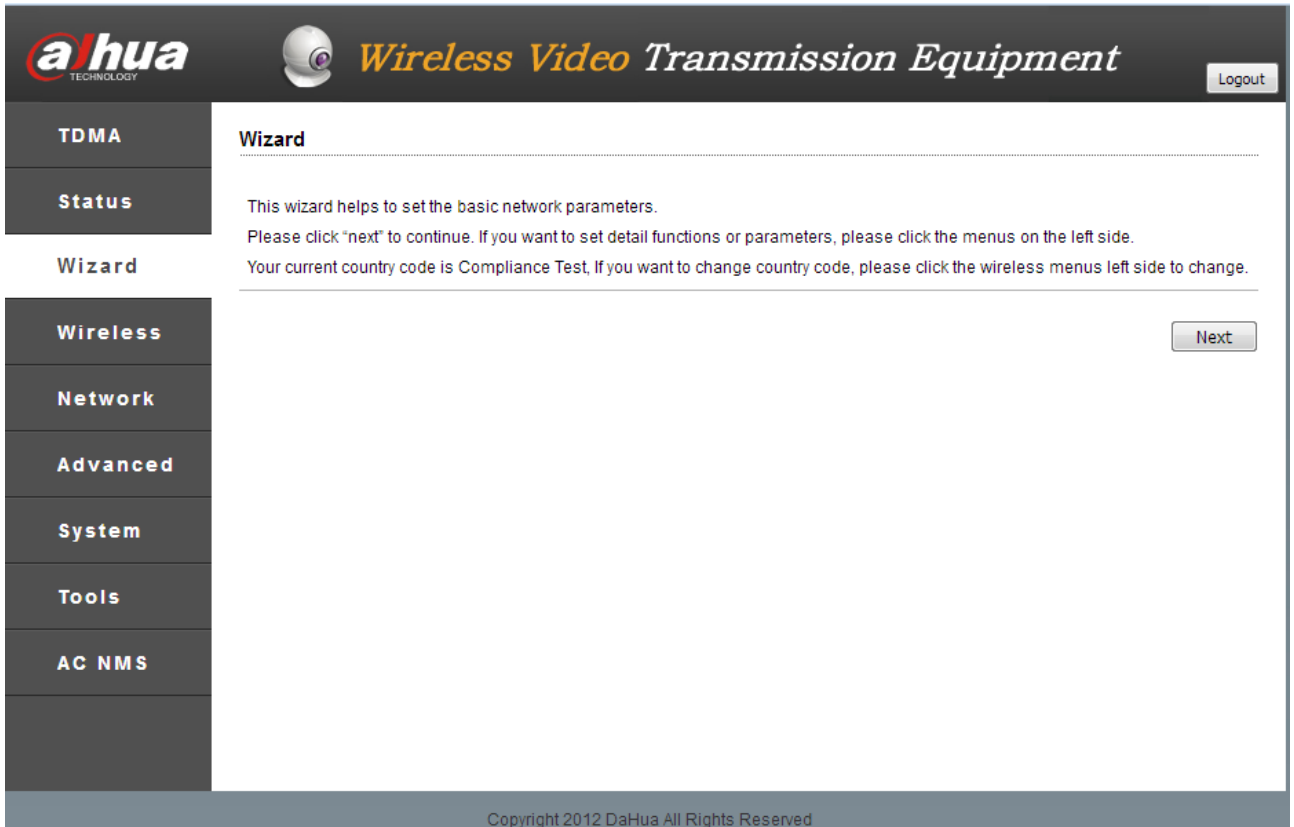


Figure 5-3 Status Display

Step 4 Click “Wizard” in the left, which helps the user to configure the equipment quickly, such as network configuration and wireless mode and so on.

You can click menu in the left of the page, to enter corresponding configuration page.



Copyright 2012 DaHua All Rights Reserved

Figure 5-4 Wizard

Step 5 Click “Next” to show basic network parameters. Default configuration is “Network Bridge Mode”; IP address of LAN port is “192.168.1.36”. It is suggested that the user should modify its IP address immediately after logging onto the equipment.



Note

Equipment IP is unique in the same LAN. Pay attention to modify equipment IP according to design, and ensure that IP in the same LAN doesn't conflict.



Copyright 2012 DaHua All Rights Reserved

Figure 5-5 Network Setting

Step 6 Click “Next” to show basic wireless parameters and wireless encryption options. The most common two wireless modes of DH-PFM88X equipment are “client” and “access point”. In the same LAN, local end and client wireless equipment have the same needs for wireless encryption option, network name option and password option.

 Note

- In “client” mode, equipment connecting video camera is usually set as client mode.
- In “access point” mode, local DH-PFM88X equipment is usually set as access point mode, connecting surveillance room.
- In case of multiple access points in the same region, pay attention to set different frequencies for different DH-PFM880 equipment; choose one from 8 defined frequencies.



Figure 5-6 Wireless Setting

Step 7 Click “Next” to show working scenario option. This wizard provides custom scenarios for the user, as is shown in the following figure. It is suggested that default settings should be used.

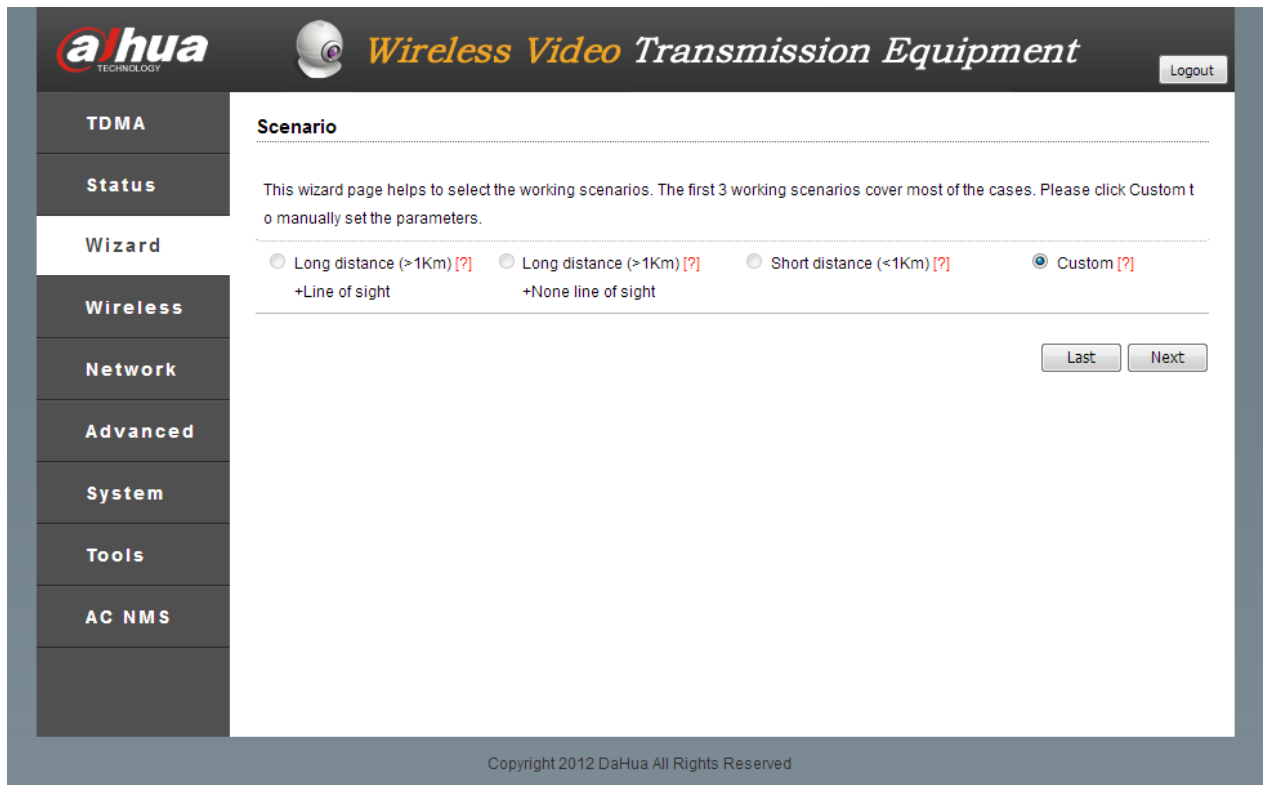


Figure 5-7 Working Scenario

Step 8 Click “Next” to show custom scenarios.

- When wireless mode is access point, the user only needs to change channel width to be 40+MHz or 40-MHz, set output power at 27dBm and tick “ACK-Timeout Adjustment”. Other options remain unchanged.
- When wireless mode is client, the user shall set channel at 20/40M, output power at 27dBm and tick “ACK-Timeout Adjustment”. Other options remain unchanged.

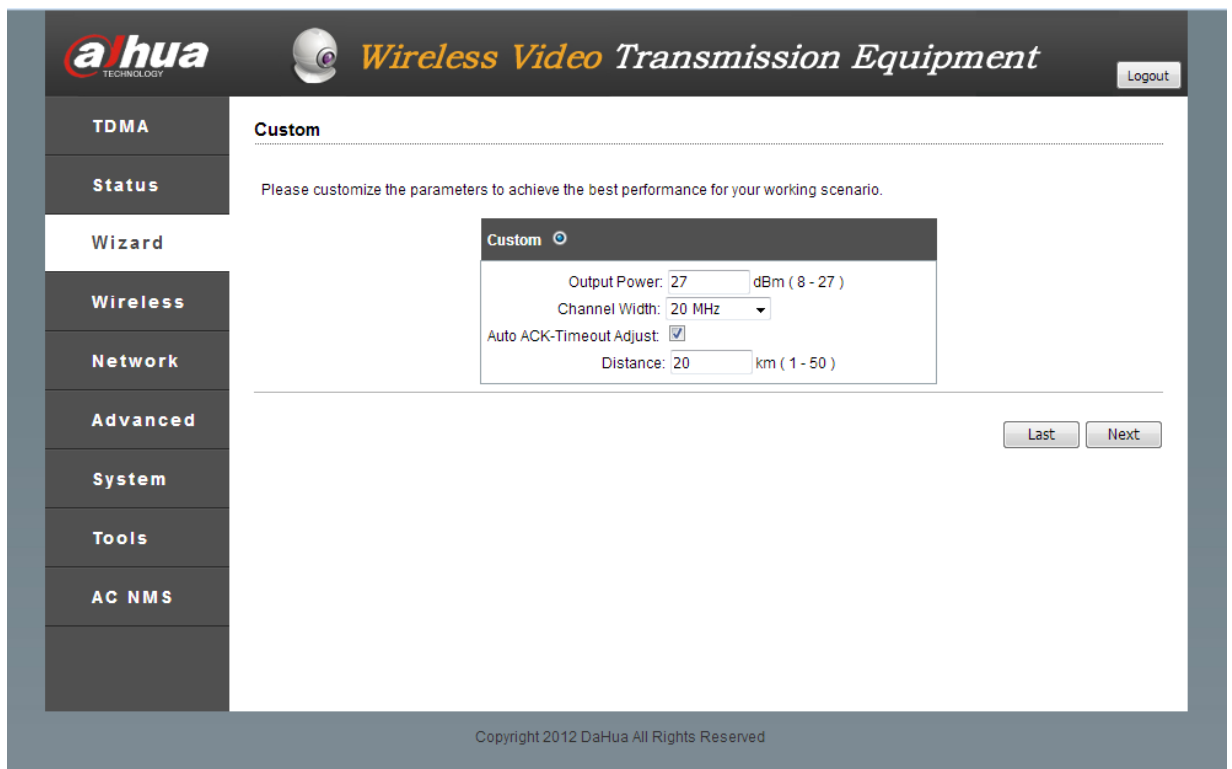


Figure 5-8 Custom Scenario

Parameter Name	Parameter Description
Output Power	The user configures output power of the equipment according to actual working conditions and local laws. The larger the output power is, the farther the wireless transmission distance will be (maximum output power available to the system is 27dBm).
Channel Width	Default value is 20MHz, so as to reach the optimal wireless transmission rate. It is suggested that channel width should be 40+MHz or 40-MHz, so as to enhance wireless transmission quality.
ACK-Timeout Adjustment	It is suggested that the user should enable "ACK-Timeout Adjustment". This option tests the distance between two equipment automatically, sets parameters according to this distance and thus optimizes wireless connection quality.
Distance	If "ACK-Timeout Adjustment" is enabled, this distance setting becomes invalid; the system will test equipment distance automatically and optimize connection quality. "ACK-Timeout Adjustment" shall be disabled, so that the distance set by the user takes effect.

Table 5-1 Parameter Description

Step 9 Click "Next" to show "Wizard-Finish" page.

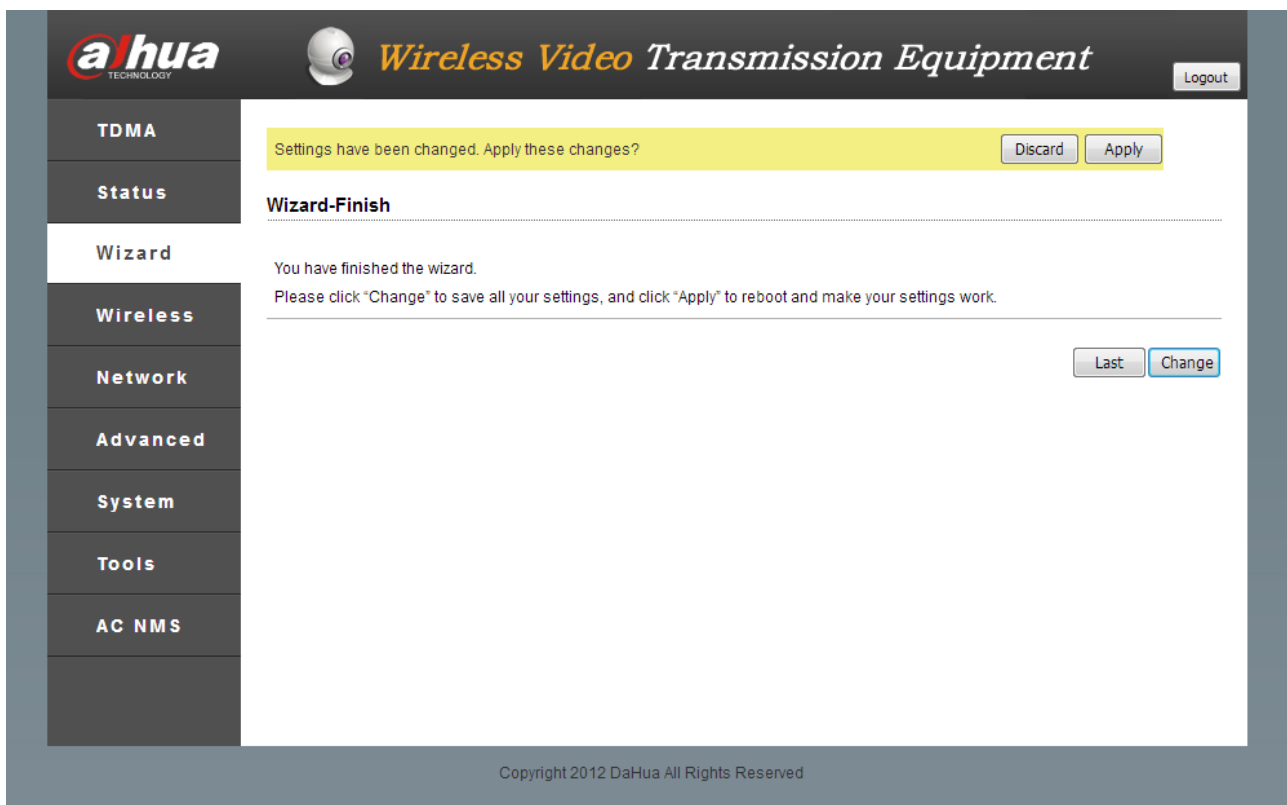


Figure 5-9 Finish Page

Step 10 Click "Change" button to save all settings, and then click "Apply" button, so as to make them take effect.

You can click "Last" to change previous settings.

6 Wireless Settings

Page of wireless settings is shown as follows:

The screenshot displays the DaHua web interface for wireless settings. The top header includes the DaHua logo, a camera icon, the text "Wireless Video Transmission Equipment", and a "Logout" button. A left sidebar contains navigation tabs: TDMA, Status, Wizard, Wireless (selected), Network, Advanced, System, Tools, and AC NMS. The main content area is divided into two sections: "Basic Wireless Settings" and "Wireless Security Settings".

Basic Wireless Settings:

- Wireless Mode[?]: Station
- SSID: DaHua (with a "Select" button)
- Frequency Scan List[?]: Enable
- Output Power: 27 dBm (with a slider)
- IEEE 802.11 Mode: A/N mixed
- Country Code: Compliance Test (with a "Select" button)
- Channel Width[?]: 20/40 MHz
- Max TX Rate, Mbps[?]: MCS 15-300

Wireless Security Settings:

- Security: WPA
- Mode: WPA 2
- Cypher: CCMP
- Authentication Mode: PSK
- WPA Key: [masked] (with a "Show" button)

A "Change" button is located at the bottom right of the settings area. The footer contains the text "Copyright 2012 DaHua All Rights Reserved".

Figure 6-1 Wireless Settings

There are 5 wireless modes, including AP mode, CPE/client mode, WDS client mode, WDS AP mode and WDS repeater.

Access Point (AP) mode: a wireless access node can be connected with client equipment, such as computer, mobile phone and wireless bridge etc.. One AP is able to connect with multiple clients.

CPE/Client: it is used with AP. One client only connects with one AP.

WDS Client: equivalent to client, it only connects with WDS AP or WDS repeater. One WDS client only connects with one WDS AP or WDS repeater.

WDS AP: it can only be connected with WDS repeater or WDS client. One WDS AP can connect with multiple WDS clients or WDS repeaters.

SSID: this value is used to control access to wireless network. When other equipment connects with this equipment, only those with the same SSID can communicate with each other and build LAN. Click “Select” key in the right of SSID, search nearby wireless network and connect corresponding wireless network according to your needs.

Frequency: it is center frequency of carrier wave; left and right offset of center frequency is bandwidth. This parameter shall be set in AP mode, while several frequencies are available in client mode. If AP frequency is not the frequency selected by client, client cannot connect with AP. They can connect with each other only if AP frequency is one frequency selected by client.

Output Power: it refers to output power of wireless signal transmitted by the equipment, to be adjusted according to equipment distance. When output power is increased, the transmitted signal distance and signal strength will be enhanced.

Country Code: different countries or regions have different standard channels, which can be differentiated by country code.

Channel Width: it refers to maximum data transmission rate of channel.

Max. TX Rate: it refers to maximum transmitting and receiving rate of the equipment. By limiting maximum transmitting and receiving rate of the equipment, keep stability of equipment performance.


MAC Address of Root AP: by setting it, client, WDS repeater or WDS client limits the connecting object.

Wireless Encryption: encrypt the wireless connection. The user chooses corresponding encryption type according to safety requirement. Equipment to be associated shall have the same wireless encryption; otherwise, they cannot be associated.

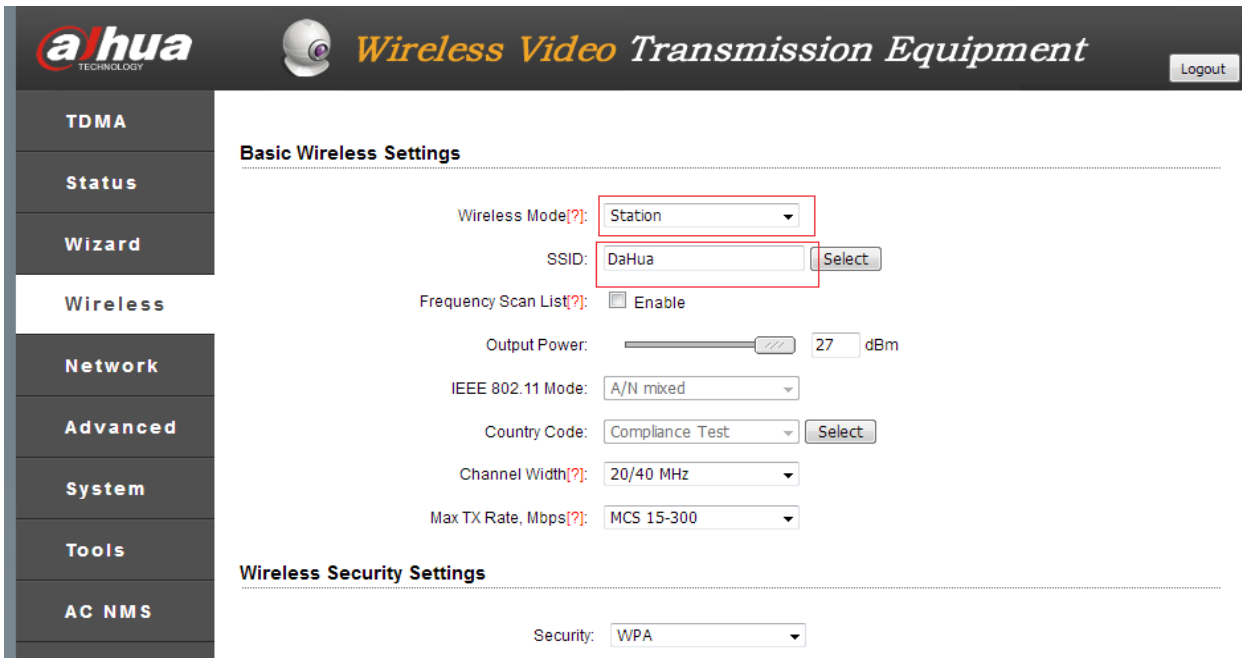
WEP: wired equivalent privacy, a data encryption technique.

WPA: this standard specification strengthens interoperable safety, and enhances data protection and access control level greatly within existing and future WLAN. It operates on existing hardware in the form of software upgrading. Wi-Fi Protected Access originates from and is compatible with future IEEE 802.11i standard. After correct installation, WPA provides Wi-Fi users with high-level protection, always

keeps their data under protection and ensures that only authorized network users can visit the network. WPA makes up all defects of wired equivalent privacy (WEP).

 Tips

In client mode, DH-PFM88X searches for surrounding 5.8G wireless band, provides basis for setting, avoids interference source effectively and searches for those equipment with access port mode. One client only connects one access port.



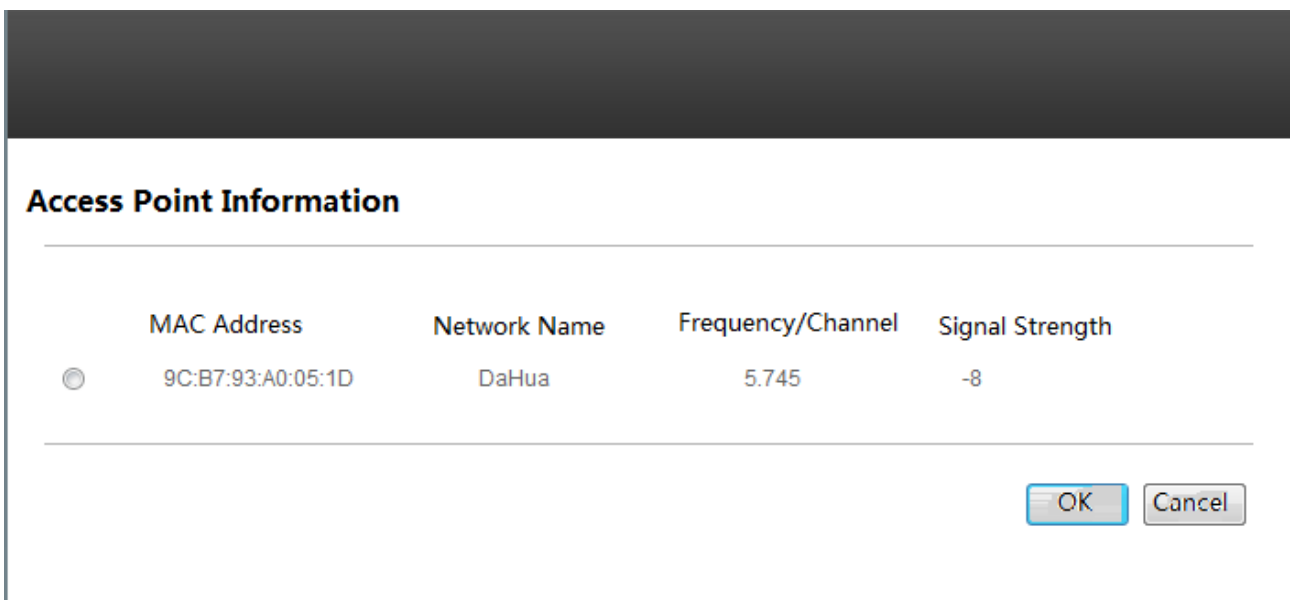
The screenshot shows the web interface for DaHua Wireless Video Transmission Equipment. The page is titled "Basic Wireless Settings" and "Wireless Security Settings". The "Basic Wireless Settings" section includes the following fields:

- Wireless Mode[?]: Station (dropdown menu)
- SSID: DaHua (text input field) with a "Select" button
- Frequency Scan List[?]: Enable
- Output Power: 27 dBm (slider control)
- IEEE 802.11 Mode: A/N mixed (dropdown menu)
- Country Code: Compliance Test (dropdown menu) with a "Select" button
- Channel Width[?]: 20/40 MHz (dropdown menu)
- Max TX Rate, Mbps[?]: MCS 15-300 (dropdown menu)

The "Wireless Security Settings" section includes the following field:

- Security: WPA (dropdown menu)

Figure 6-2 Wireless 5.8G Band Searching Page of Client



The screenshot shows the "Access Point Information" dialog box. It contains a table with the following data:

MAC Address	Network Name	Frequency/Channel	Signal Strength
9C:B7:93:A0:05:1D	DaHua	5.745	-8

At the bottom right of the dialog box, there are "OK" and "Cancel" buttons.

Figure 6-3 Searching Result

7 Network Settings

Route mode

In route mode, DH-PFM88X with WAN port and LAN port is equivalent to a router. LAN2 port of DH-PFM88X is equivalent to LAN port of router, whereas LAN port of POE power supply is equivalent to WAN port of router. In route mode, connection diagram is shown as follows:

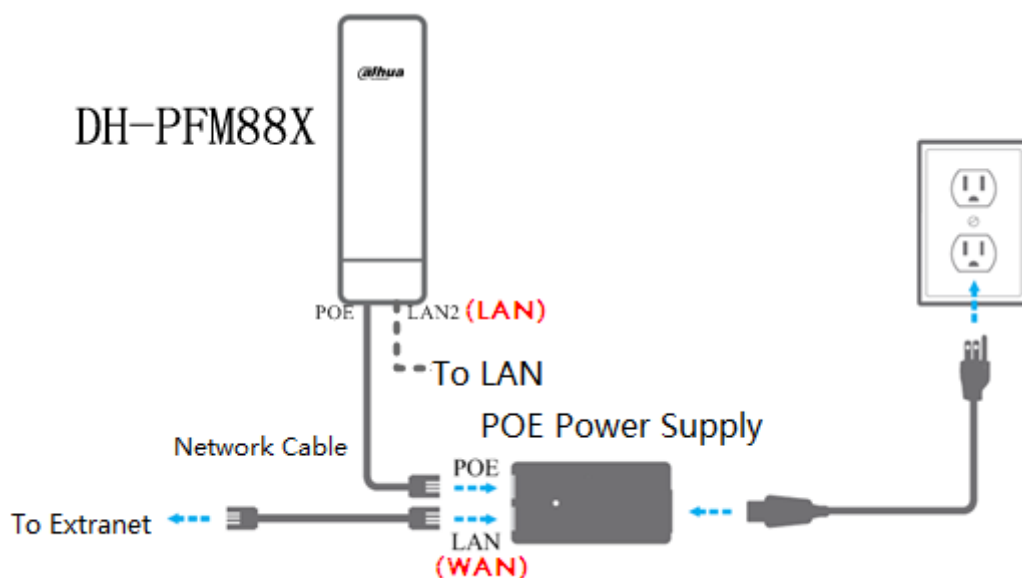


Figure 7-1 Connection Diagram of Route Mode

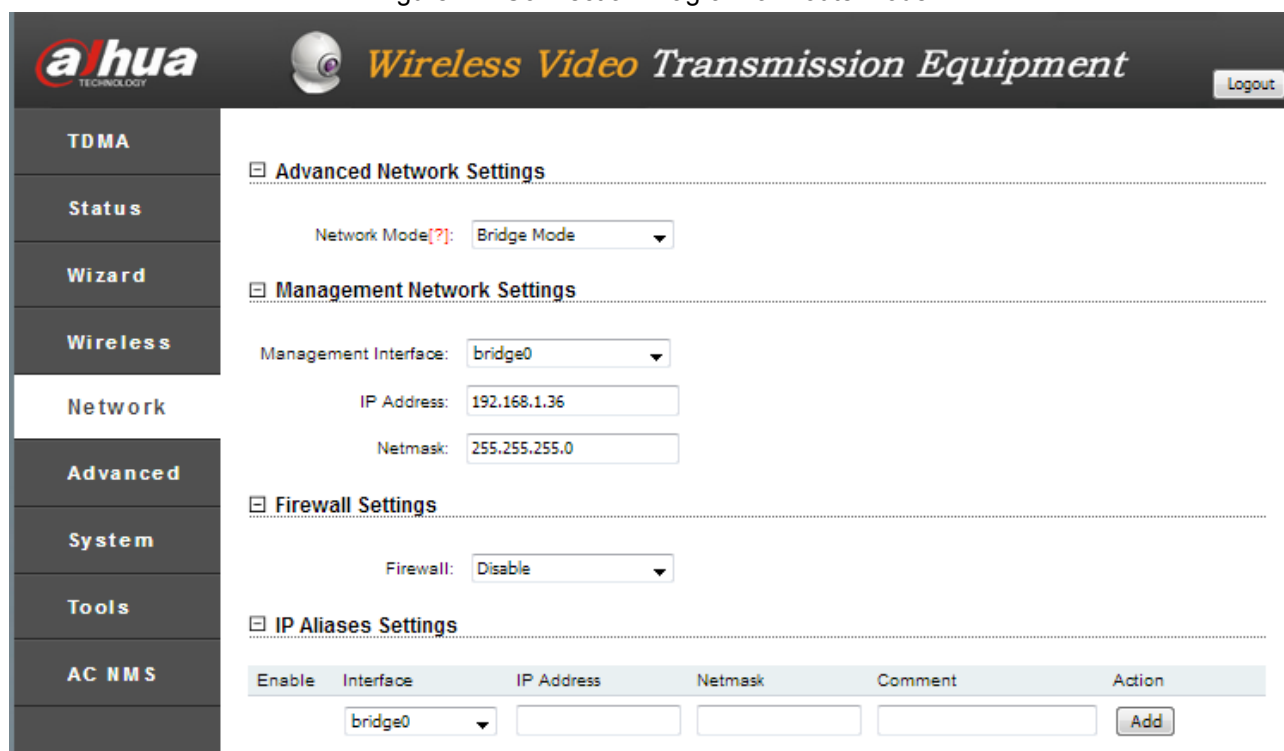


Figure 7-2 Route Mode

WAN Mode: WAN mode is to set WAN port to be static IP address and dynamic acquisition (DHCP). When it is static IP, the user shall manually set IP and subnet mask; when it is DHCP, the equipment can acquire IP address from DHCP server automatically.

WAN IP: IP address of WAN port, which can be IP address of the same segment of network to be connected.

WAN Subnet Mask: subnet mask of WAN port, which can be IP address of the same segment of network to be connected.

Caution: IP address of WAN port cannot be the same as existing IP in the network, so as to prevent IP address conflict.

LAN IP: IP address of LAN port, to be set by the user according to needs. However, LAN IP shall not be the same as IP of other equipment in the same network, so as to prevent IP address conflict.

LAN Subnet Mask: subnet mask of LAN port, which is set by the user according to IP of LAN port.

Main DNS and Supplemental DNS: DNS server, which is set to be value of local DNS server.

Gateway: gateway address is usually set to be IP address of LAN port.

Firewall

Firewall is used to shield DH-PFM88X from some equipment, as is shown in the following figure.

There are 4 types of firewall filtering:

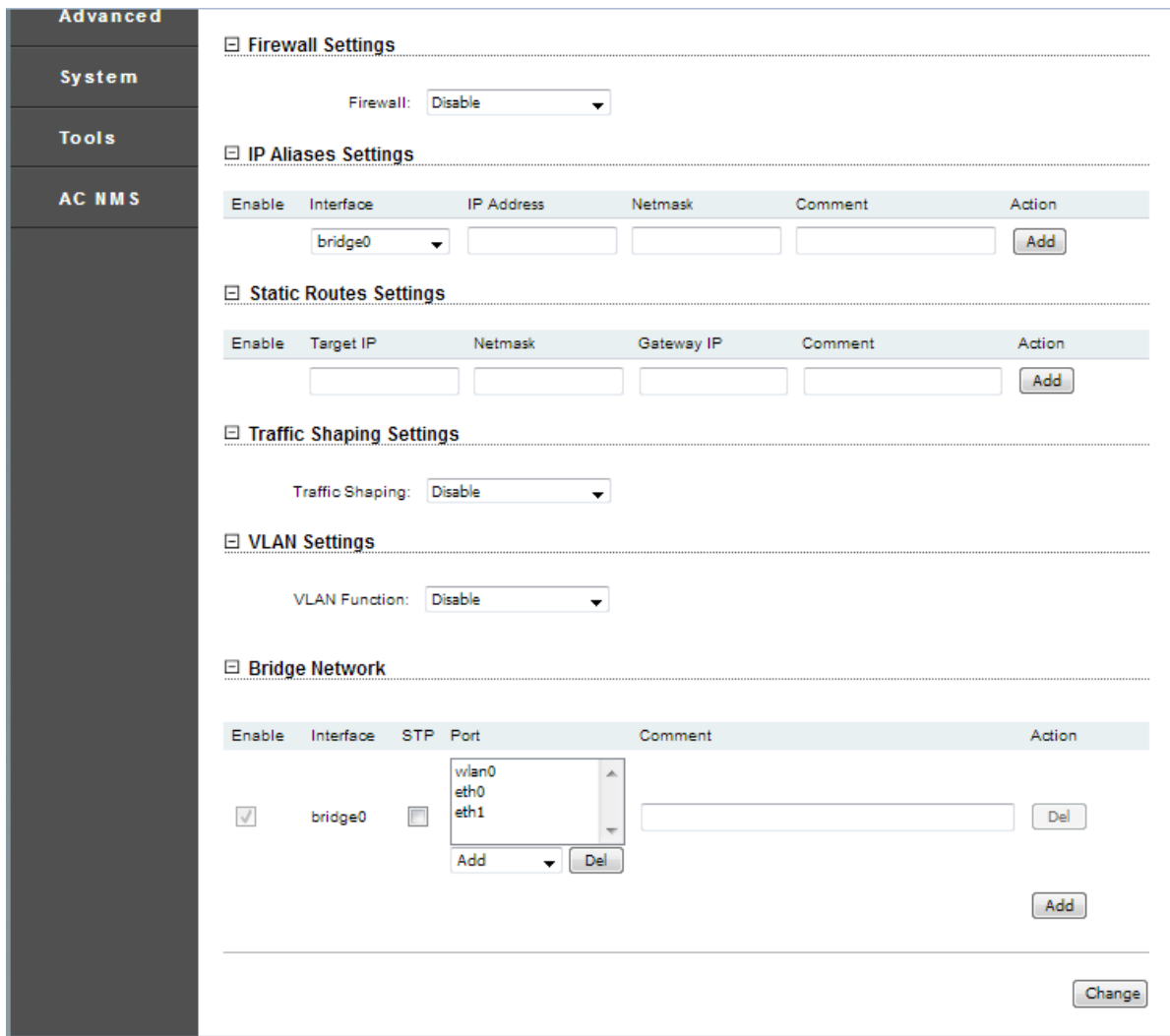


Figure 7-3 Firewall

Filter one equipment whose IP address is xxx.xxx.xxx.xxx

Firewall is enabled, IP filtering mode is set to be “Refuse”, and any one item in IP1~IP10 is set to be IP that shall be filtered.

Filter one equipment

Firewall is enabled, MAC filtering mode is set to be “Refuse”, and any one item in Mac1~Mac10 is set to be MAC address of the equipment to be filtered.

Except the equipment whose IP address is xxx.xxx.xxx.xxx, others are filtered.

Choose to “Accept” IP filtering. Any one item in IP1~IP10 is set to be the IP that shall be accepted.

Accept only one equipment

Firewall is enabled, MAC filtering mode is set to be “Accept”, and any one item in Mac1~Mac10 is set to be MAC address of the equipment to be accepted.

8 Advanced Settings

Page of advanced settings:

The screenshot displays the 'Advanced Wireless Settings' and 'Advanced Ethernet Settings' sections of the DaHua web interface. The 'Advanced Wireless Settings' section includes options for 'Auto ACK-Timeout Adjust' (checked), 'Distance' (20 km), 'Aggregation' (checked, 32 Frames, 50000 Bytes), 'RTS Threshold' (2346, off), 'Fragmentation Threshold' (2346, off), and 'Multicast Data' (Allow All). The 'Advanced Ethernet Settings' section includes 'Enable Autonegotiation' (checked), 'Enable Full Duplex' (unchecked), and 'LAN Speed' (10). The 'Signal LED' section shows 'LED Configure, dB' settings for LED1 (-86), LED2 (-71), and LED3 (-56). A 'Change' button is located at the bottom right of the settings area. The footer of the interface reads 'Copyright 2012 DaHua All Rights Reserved'.

Figure 8-1 Advanced Settings

Auto ACK-Timeout Adjustment: it is suggested that “Auto ACK-Timeout Adjustment” should be enabled. This option can test the distance between two devices automatically, and set parameters according to this distance, in order to optimize wireless connection quality.

Distance: if “Auto ACK-Timeout Adjustment” is enabled, this distance setting becomes invalid; the system will test device distance automatically and optimize connection quality. “Auto ACK-Timeout Adjustment” shall be disabled, so distance set by the user will take effect.

Aggregation: different frames are aggregated and sent out. This function enhances throughput rate and

it is enabled by default.

RTS Threshold: when packet length is over or equivalent to the set value, RTS/CTS mechanism will be started. To send data, the station will send a RTS to AP, and notify AP that it will send data. After receiving the request, AP notifies all other stations in its coverage through CTS, and requires them delaying sending. Meanwhile, AP notifies requesting station to send data.

Fragmentation Threshold: when packet length is over the set value, the packet will be divided into multiple data fragments, which shall be even number.

Multicast Data: if this function is enabled, DH-PFM88X allows multicast packets to pass DH-PFM88X.

Enable Autonegotiation: when enabled, according to connecting speed and duplex mode of device on the other end, LAN port automatically adjusts its speed to the highest public level, so both ends of the line own the highest speed and duplex mode. It is enabled by default, so the user doesn't need to set.

Enable Full Duplex: it determines whether LAN port of DH-PFM88X allows the data to transmit in two directions simultaneously.

LAN Speed: LAN port of DH-PFM88X owns two speeds: 10Mbps and 100Mbps.

Signal LED Configure: LED1, LED2 and LED3 settings refer to signal strength value of the device to turn on 3 LED lights. LED3 signal strength value is the largest (LED3>LED2>LED1); default settings are LED1:-86dB, LED2:-71dB and LED3:-56dB. LED1 turns on when signal strength is higher than LED1 and lower than LED2. LED1 and LED2 turn on when signal strength is higher than LED2 and lower than LED3. LED1, LED2 and LED3 turn on when signal strength is higher than LED3.

9 System Settings

System settings interface consists of configuration management, firmware configuration, device settings and account information.

The screenshot shows the Dahua system settings interface. On the left is a navigation menu with options: TDMA, Status, Wizard, Wireless, Network, Advanced, System, Tools, and AC NMS. The main content area is titled 'Wireless Video Transmission BaseStation' and includes a 'Logout' button. It is divided into four sections: 'Configuration Management' (Backup Configuration: Download; Upload Configuration: Browse... Upload), 'Firmware Configuration' (Firmware Update: Browse... Update; Firmware Reboot: Reboot; Restore Factory Settings: Reset), 'Device Settings' (Device Name: DH-PFM881; Login Timeout: Unlimited Minutes; Interface Language: English), and 'Accounts Information' (Modify User Password: ; Read-Only Account:). A 'Change' button is at the bottom right.

Figure 9-1 System Settings

Accounts Information

The Accounts Information section shows the 'Modify User Password' checkbox checked. Below it are input fields for 'Old Password', 'New Username', 'New Password', and 'New Password Verification', each with a 'Show' button. At the bottom is a 'Read-Only Account' checkbox.

Figure 9-2 Accounts Information

Backup Configuration: click “Download” to backup present webpage configurations. Note that configuration file contents cannot be modified manually.

Upload Configuration: click “Browse” to select previously downloaded configuration file; click “Upload”.

Device configuration will be restored to the device configuration when backup of configuration file is carried out.

Firmware Update: click “Browse” to select the version to be updated; click “Update” and the device starts to update.

Firmware Reboot: click “Reboot” and the device starts to reboot.

Restore Factory Settings: click “Reset” on the webpage. After a while, device configurations are restored to factory settings.

Device Name: the user can set the device name according to needs.

Login Timeout: when login timeout is set to a value and the webpage doesn’t respond after the time period, the system will skip to login interface.

Interface Language: the user chooses language of the webpage according to needs.

Account Information: when “Modify User Password” is enabled, the user can modify account information according to needs.

10 Tool Application

Tool application page consists of testing tool and Telnet:

The screenshot displays the configuration interface for a Wireless Video Transmission BaseStation. The left sidebar contains navigation tabs: TDMA, Status, Wizard, Wireless, Network, Advanced, System, Tools, and AC NMS. The main content area is titled 'Tools' and includes several sections:

- Ping IP:** A form with a 'Ping IP:' text input field and a 'Ping' button.
- Time To Restart:** Settings for 'Time to Restart' (checkbox), 'Restart Minutes' (input), 'Restart Hours' (input), 'Time Zone' (dropdown), and 'Restart Date' (checkboxes for Mon, Tues, Wed, Thur, Fri, Sat, Sun).
- Ping Watchdog:** Settings for 'Ping Watchdog' (checkbox), 'Ping Interval' (input, 300 sec), 'Startup Delay' (input, 300 sec), 'Ping IP Address' (input, 192.168.1.1), and 'Ping Failure' (input, 3) to Reboot System.
- Telnet / Syslog:** Settings for 'Telnet' (checkbox, checked), 'Syslog' (checkbox), 'Server IP' (input), and 'Server Port' (input, 514).
- NTP / SNMP:** Settings for 'NTP Client' (checkbox), 'NTP Server' (input), 'SNMP Agent' (checkbox), 'SNMP Group' (input), 'Contact Mailbox' (input), and 'Location' (input).
- IPERF:** A dropdown menu for 'IPERF Type' set to 'Disable'.

Figure 10-1 Tools

ping IP: when the user sets IP address of a device in ping IP bar and clicks “Ping”, if this device is connected with DH-PFM88X, ping result will be “Alive”; otherwise, it will be “Not Alive”.

Ping Watchdog: it is used to monitor the operation of Wireless Bridge continuously. In particular, Ping tool is used when connecting remote host. Wireless Bridge is able to ping the target host for a long time. If Wireless Bridge doesn’t receive certain defined quantity of replies, this tool will reboot Wireless Bridge.

Ping IP Address: IP address of target host.

Ping Interval: time interval between two pings.

Ping Failure: when continuous Ping failure reaches the set value, the device will reboot WIFI.

Startup Delay: it will start to ping the target host, after Wireless Bridge system is started and delayed for the set time period.

Telnet: when Telnet is enabled, in command prompt window of Windows XP or Windows 7, Telnet xxx.xxx.xxx.xxx(DH-PFM88XIP) can be used to login DH-PFM88X. When Telnet is disabled, it cannot be used to login the system.

Syslog: enable Syslog function, set PC IP of Syslog server and set server port to be 514. Then, relevant log information will be seen on Syslog server.

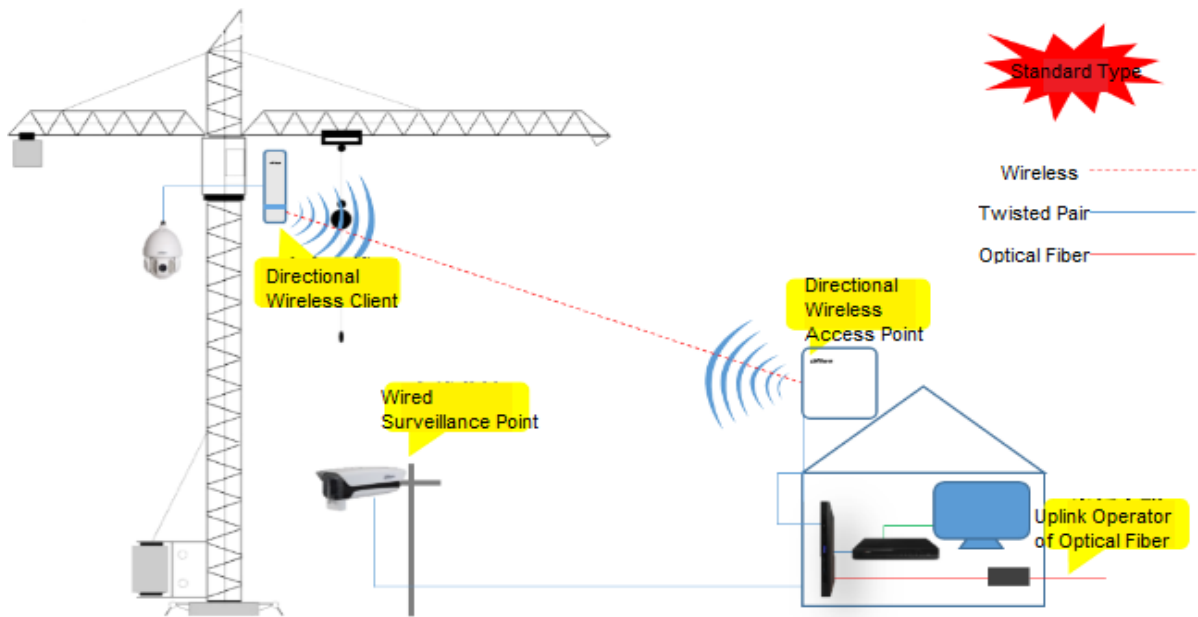
NTP Client: if DH-PFM88X can go online, NTP client function is enabled and URL of NTP server is set, DH-PFM88X will calibrate device time according to NTP server, and display it on status display page.

SNMP Proxy: with SNMP proxy, network administrator can monitor network performance, search and solve network problems. For example, enable SNMP proxy, fill in a user name in SNMP community, such as creatcomm, fill in the mailbox such as jerry@creatcomm.com and write creatcomm in location information. Then, save and apply. Install mrtg on the host, and open mrtg webpage to observe traffic and other information about DH-PFM88X.

Appendix 1 Industry Application

Appendix 1.1 Wireless Surveillance of Safe Site

System Diagram (Standard Proposal)



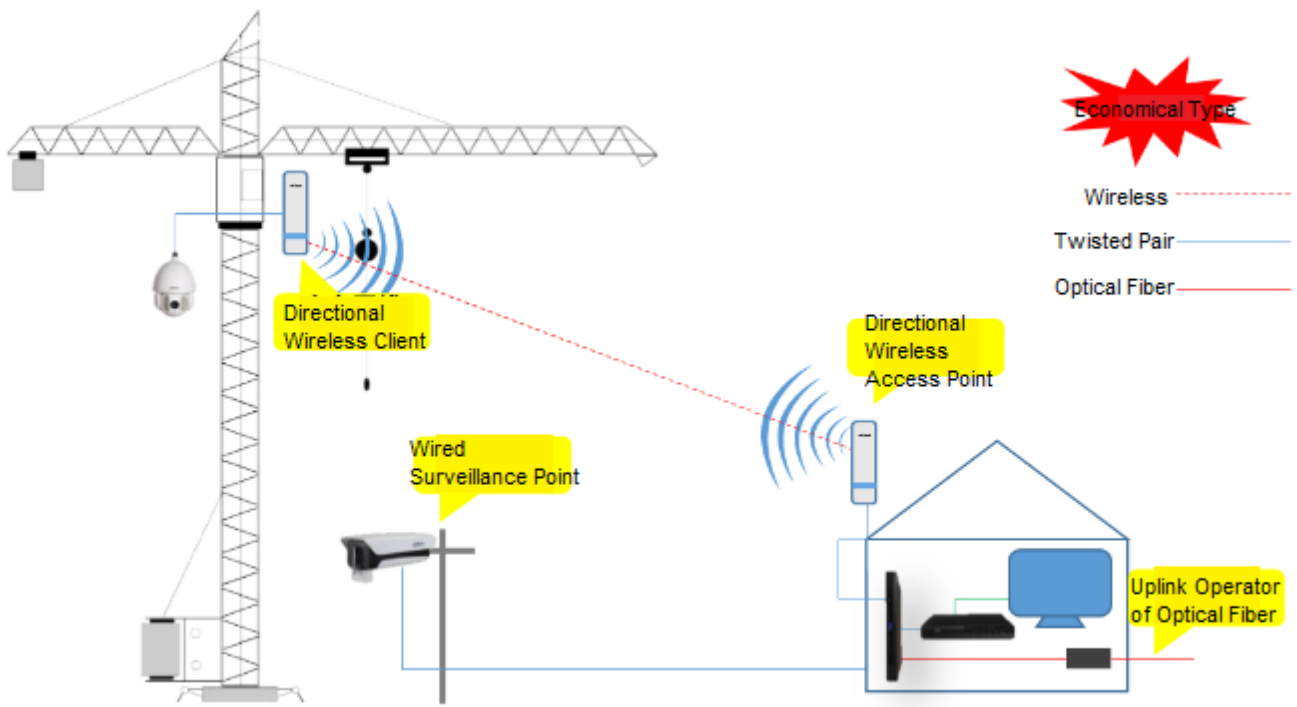
Appendix Figure 1-1

The recommended standard wireless surveillance proposal of construction site adopts point-to-point transmission. Receiving end adopts DH-PFM880 device, which provides necessary technical support for future expansion.

No.	Type	Model No.	Qty.	Description	Feature
1	Wireless receiving end	DH-PFM880	1	IP66, wide temperature: -30~70°, wireless bandwidth: 300M, coverage area: 3km, standard power supply, high-power antenna and dual feeder	It applies to outdoor high temperature and low temperature environment.
2	Wireless client	DH-PFM881	1	Outdoor waterproof, wide temperature: -30~70°, wireless bandwidth: 300M, coverage area: 3km, standard power supply	It applies to outdoor high temperature and low temperature environment.
3	Switch of machine room (optional)	DH-S4200-24T	1	Gigabit management switch, 24*10/100/1000Base-T, 4*SFP (Combo) light, natural heat dissipation without fan, dustproof design	It applies to non-standard machine room environment.

Appendix Table 1-1 Recommended Model Selection List of Standard Proposal

System Diagram (Economical Proposal)



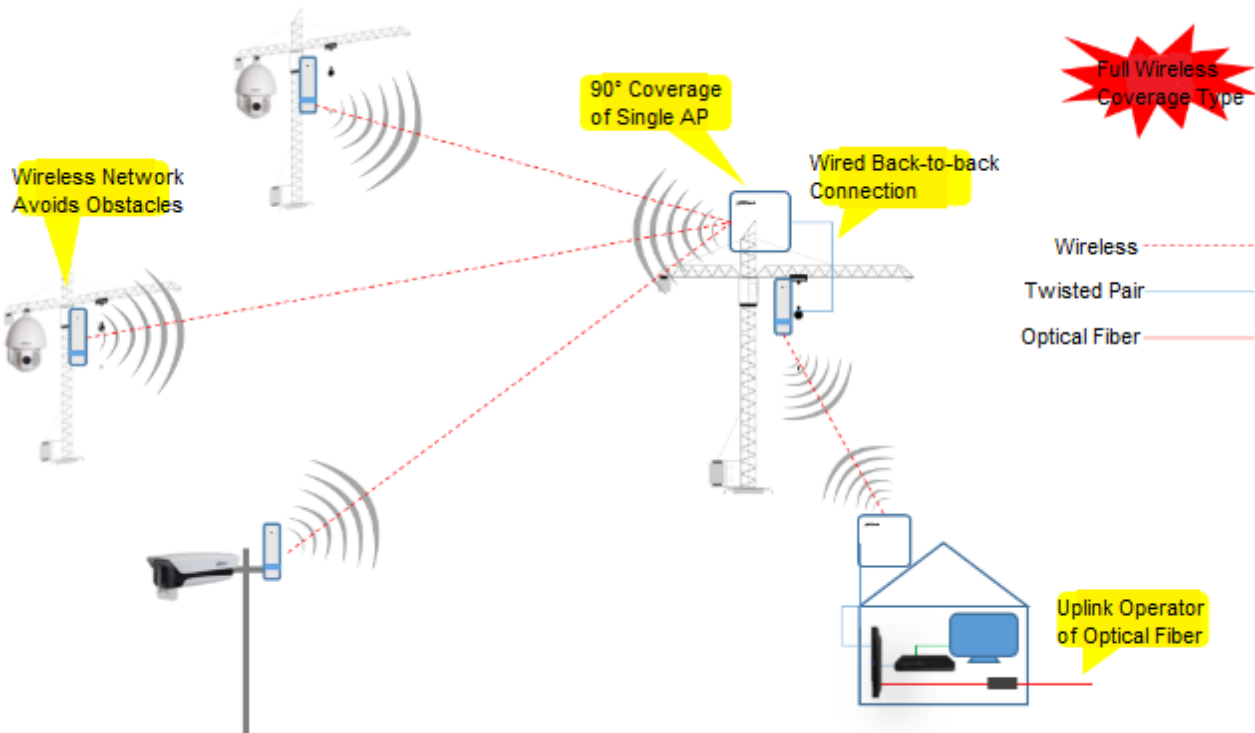
Appendix Figure 1-2

With point-to-point transmission, receiving end adopts DH-PFM881 device.

No.	Type	Model No.	Quantity	Description	Feature
1	Wireless receiving end	DH-PFM881	1	Outdoor waterproof, wide temperature: -30~70°, wireless bandwidth: 300M, coverage area: 3km, standard power supply	It applies to outdoor high temperature and low temperature environment.
2	Wireless client	DH-PFM881	1	Outdoor waterproof, wide temperature: -30~70°, wireless bandwidth: 300M, coverage area: 3km, standard power supply	It applies to outdoor high temperature and low temperature environment.
3	Switch of machine room (optional)	DH-S4200-24 T	1	Gigabit management switch, 24*10/100/1000Base-T, 4*SFP(Combo) light, natural heat dissipation without fan, dustproof design	It applies to non-standard machine room environment.

Appendix Table 1-2 Recommended Model Selection List of Economical Proposal

System Diagram (Full Wireless Coverage Proposal)



Appendix Figure 1-3

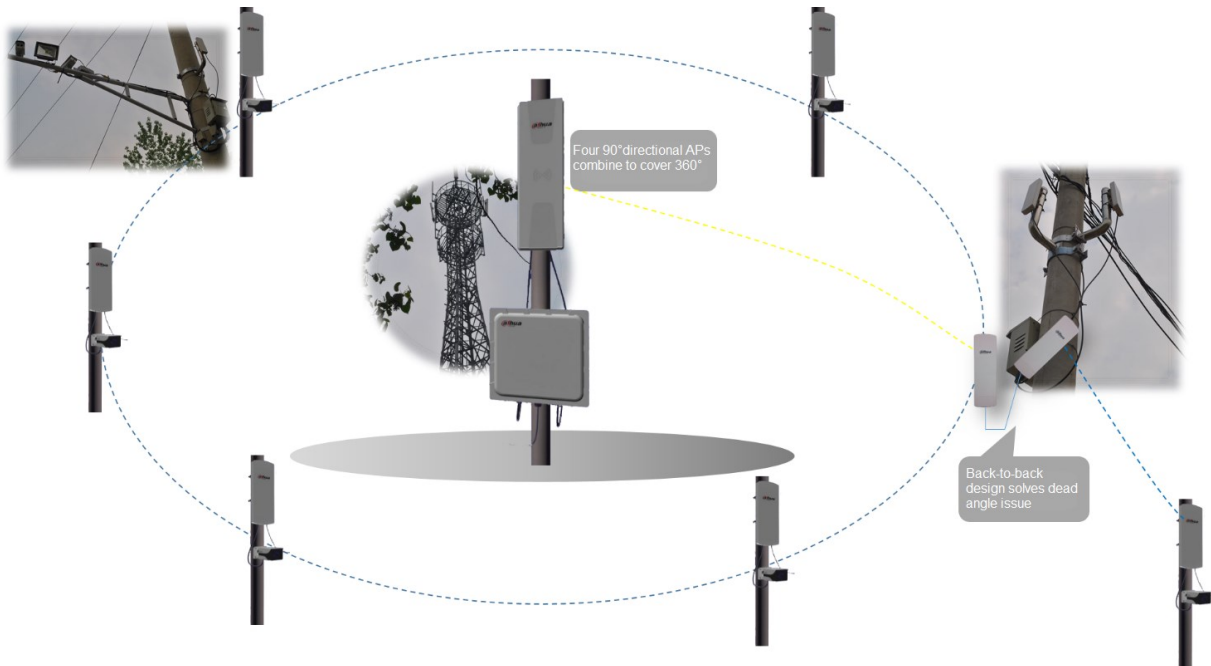
This proposal is highly comprehensive. Generally speaking, required device quantity shall be confirmed according to actual needs.

No.	Type	Model No.	Qty.	Description	Feature
1	Wireless receiving end	DH-PFM880	X	IP66, wide temperature: -30~70°, wireless bandwidth: 300M, coverage area: 3km, standard power supply, high-power antenna and dual feeder	It applies to large construction site projects, to be adjusted according to actual needs.
2	Wireless client	DH-PFM881	X	Outdoor waterproof, wide temperature: -30~70°, wireless bandwidth: 300M, coverage area: 3km, standard power supply	It applies to large construction site projects, to be adjusted according to actual needs.
3	Outdoor switch	DH-S4000-7X	X	4* 10/100M, 1*10/100/1000M, 2*1000MSFP optical port, 1 Console port, support STP ring network protocol	It applies to large construction site projects, to be adjusted according to actual needs.
4	Switch of machine room (optional)	DH-S4200-24 T	1	Gigabit management switch, 24*10/100/1000Base-T, 4*SFP(Combo) light, natural heat dissipation without fan, dustproof design	It applies to non-standard machine room environment.

Appendix Table 1-3 Recommended Model Selection List of Full Wireless Coverage Proposal

Appendix 1.2 Wireless Surveillance of Safe Town

System Diagram (Full Wireless Coverage Proposal)



Appendix Figure 1-4

Rural scene is relatively fixed, so it is easiest to design wireless proposals. The proposal for every village is almost the same: it centers on village committee, and video data is wirelessly converged and saved in NVR device in machine room. Through operator network, town and county surveillance center can carry out data debugging, backup and save crucial videos.

No.	Type	Model No.	Qty.	Description	Feature
1	Wireless receiving end	DH-PFM880	4	IP66, wide temperature: -30~70°, wireless bandwidth: 300M, coverage area: 3km, standard power supply, high-power antenna and dual feeder	Four APs combine to cover 360° for 3 km area
2	Wireless client	DH-PFM881	X	Outdoor waterproof, wide temperature: -30~70°, wireless bandwidth: 300M, coverage area: 3km, standard power supply	There are about 15 generally, to be adjusted according to actual needs.
3	Outdoor switch	DH-S4000-7X	1	4* 10/100M, 1*10/100/1000M, 2*1000MSFP optical port, 1 Console port, support STP ring network protocol	It applies to outdoor high and low temperature environment, and converges with four APs.

4	Switch of machine room (optional)	DH-S4200-24T	1	Gigabit management switch, 24*10/100/1000Base-T, 4*SFP (Combo) light, natural heat dissipation without fan, dustproof design	It applies to non-standard rural machine room.
---	-----------------------------------	--------------	---	--	--

Appendix Table 1-4 Recommended Model Selection List of Wireless Rural Surveillance

Appendix 2 Troubleshooting

1. The device fails to start normally:

- (1) Network line from the device to POE module exceeds 40 meters.
- (2) Network line has poor quality and materials.
- (3) Crystal plug of network line isn't connected firmly or line sequence is wrong (crystal plug shall be remade).

2. IP address is forgotten and factory settings cannot be restored.

Please manually press Reset key for 5-10 seconds. After all LED lights of the device turn on, input IP:192.168.1.36 to log onto the device.

3. My computer cannot find wireless AP. Why?

Solution: wireless system will connect at the maximum working rate, and specific rate will depend on distance and environment. To obtain maximum possible connecting rate, the following links shall be tested:

(1) Position of wireless AP

Try to adjust the position and direction of wireless AP.

(2) Wireless channel

Use other communication channels. Interference may be obviously improved.

(3) Wireless interference

Other devices may cause interference too. Turn off other devices and check whether it is improved. Interfering devices shall be shielded or relocated.

4. Too low signal strength is due to the following reasons:

- (1) Client fails to be visible for AP, because of large obstacles.
- (2) Surface plate of client doesn't align with AP; angle of pitch of AP and client is inappropriate.
- (3) Client is installed on a window, which easily leads to planar interference.

(4) Distance between AP and client is too long.

5. Why is signal quality high while throughput capacity is low?

Analyze reasons:

(1) Too much interference or multipath interference.

(2) Ethernet port of the device breaks down.

6. Frequent packet loss. Serious packet loss occurs when many devices are installed in the same region. It will be improved if channels are changed.

Same frequency interference occurs in case that multiple DH-PFM88X devices are used in the same region, and channels of every two devices are not isolated. It is suggested that the user should isolate their frequency, and make sure that their channels don't overlap. When channel width is 20M, frequency difference between two devices shall be over 20M.

7. Packet loss and large delay occur when the computer pings device address:

(1) APs connecting with the same POE switch shall carry out port isolation.

(2) Crystal plug of network line isn't connected well (crystal plug shall be remade).

8. The user suffers from frequent lost connection and low speed:

(1) Too many users connect with AP.

(2) AP signal is weak.

(3) There are many serious interference signals in surrounding environment; client and AP aren't bound.

(4) Check whether user quantity and upper network bandwidth are saturated or not.

Appendix 3 Points for Attention

1. Horizontal Direction and Angle of Pitch of Antenna

Since base station and wireless bridge adopt directional antenna, AP antenna on the base station shall tilt down for certain angle. Meanwhile, AP shall align with client antenna.

2. Erecting Height of Antenna

Since the earth is spherical, wireless communication between two actual points places certain requirements on the distance between two points and erecting height of antenna. For details, refer to the following table.

Transmission distance	3Km	5Km	10Km	15Km
5.8GHz	5m	7m	11m	16m

Appendix Table 3-1

3. Geographical Environment

The farthest communication distance is realized at sea level and clear open land; this is geographical condition used to evaluate communication distance of wireless communication equipment. It is followed by semi-clear and semi-open environment, such as suburb countryside, hills and riverbeds. The nearest communication distance is realized at urban buildings or mountains. In one word, closer obstacles exert greater effects on wireless communication distance; especially metal objects exert the greatest effects. Therefore, during actual construction, try to make sure that client and AP are visible to each other directly.

4. Electromagnetic Environment

DC motor, high-voltage grid, switching power supply, electric welding machine, high-frequency electronic equipment, computer and single-chip microcomputer exert effects on communication distance of wireless communication equipment to varying degrees.

5. Climatic Condition

Communication distance is relatively far in case of dry air and relatively near in case of moist air (especially rainy and snowy weather).

6. Transmitted Power

The larger the transmitted power is, the farther communication distance will be. During outdoor long-distance communication, output power is usually set at the maximum value.

7. Try to Avoid Same Frequency Interference and Adjacent Frequency Interference

When setting AP frequency, employ the client to search what frequencies are being used by other equipment nearby. AP frequency shall try to avoid these frequencies. To prevent adjacent frequency interference, AP frequency shall be away from those frequencies used nearby. For example, when channel width is 20M, it shall be at least 20M away from the frequency under use. Meanwhile, frequency between APs shall also be set in this way.

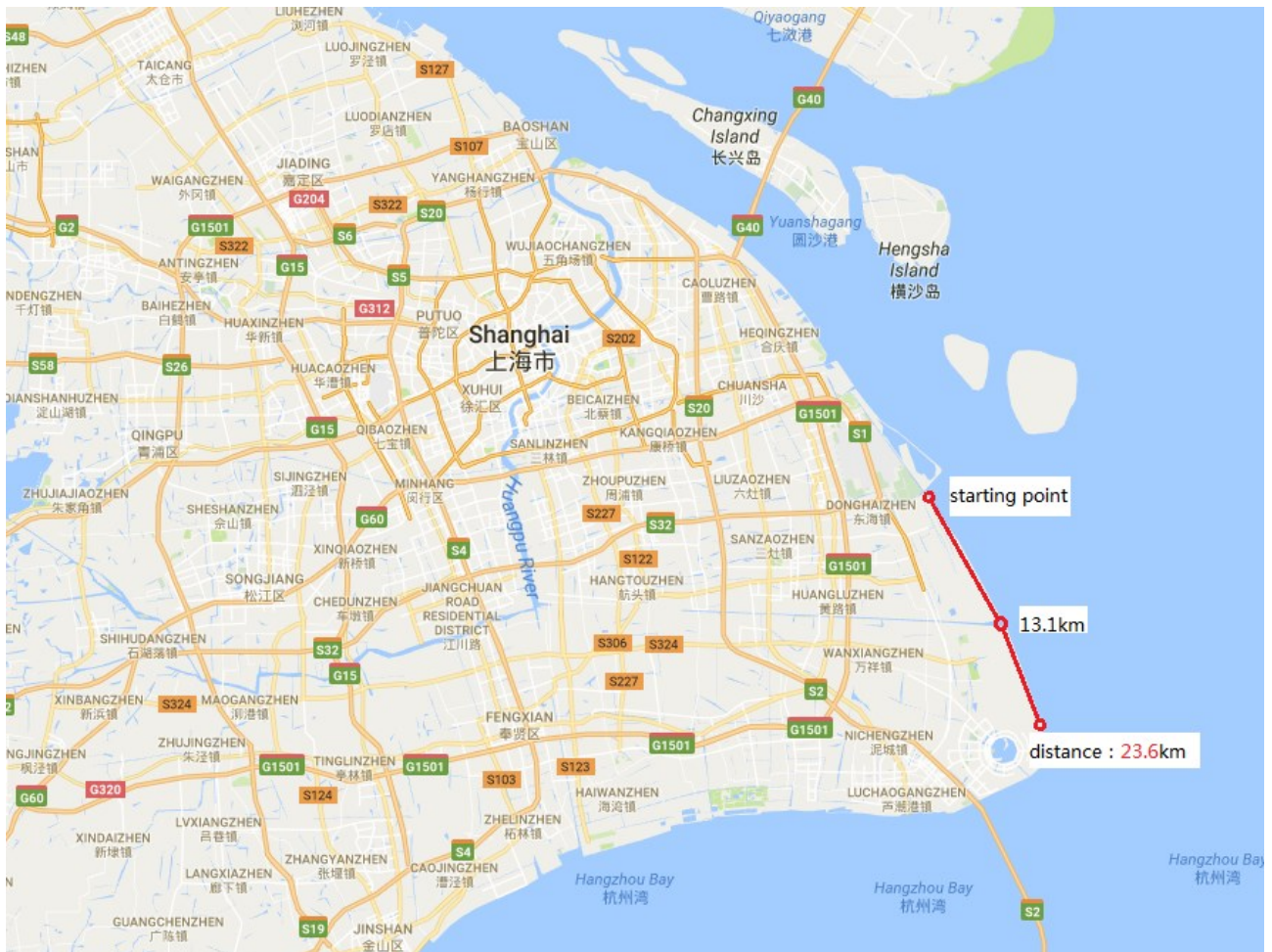
Appendix 4 Test Report

Test Description

This test report mainly tests ultimate wireless transmission performance of DH-PFM88X product under the condition of no occlusion and slight occlusion, including transmission distance and wireless throughput rate with certain transmission distance.

Test (No Occlusion)

This test was carried out at East China Sea Dike in Pudong New District of Shanghai; the coastal dike has no occlusion, as shown in the map.



Appendix Figure 4-1

Actual environment and actual condition of this test is shown as follows:

- 1) The test was located at a coastal dike, about 5~10 meters higher than the sea in the left and

land in the right.

- 2) The whole dike was basically a straight line.
- 3) Test pole was about 8 meters higher than the dike. Point-to-point test was carried out between point A and point B.



Appendix Figure 4-2

Test Tool

- 1) Test tool: Chariot (professional network speed test software)
- 2) Test equipment: DH-PFM880 <->DH-PFM881; one DH-PFM880 and one DH-PFM881 were placed at both points respectively.

Test Result

- 1KM Test Result

<i>Equipment (AP/STA)</i>	<i>RSS (dBm)</i>	<i>Throughput (Mbps)</i>	<i>Channel</i>	<i>Bandwidth</i>
55/56	-51/-53	31.2/31.1 (uplink and downlink)	5785 MHz	20MHz
55/56	-50/-49	37/36.8(uplink and downlink)	5500 MHz	20MHz
55/56	-55/-57	36.2/36(uplink and downlink)	5785 MHz	40MHz
55/56	-54/-54	40.7/42.7(uplink and downlink)	5500 MHz	40MHz

- 2KM Test Result

<i>Equipment (AP/STA)</i>	<i>RSS (dBm)</i>	<i>Throughput (Mbps)</i>	<i>Channel</i>	<i>Bandwidth</i>
---------------------------	------------------	--------------------------	----------------	------------------

55/56	-62/-63	27.1/26.4 (uplink and downlink)	5785 MHz	20MHz
55/56	-60/-60	32.9/33.1 (uplink and downlink)	5500 MHz	20MHz
55/56	-66/-64	31.2/31.3 (uplink and downlink)	5785 MHz	40MHz
55/56	-63/-64	38.7/38.3 (uplink and downlink)	5500 MHz	40MHz

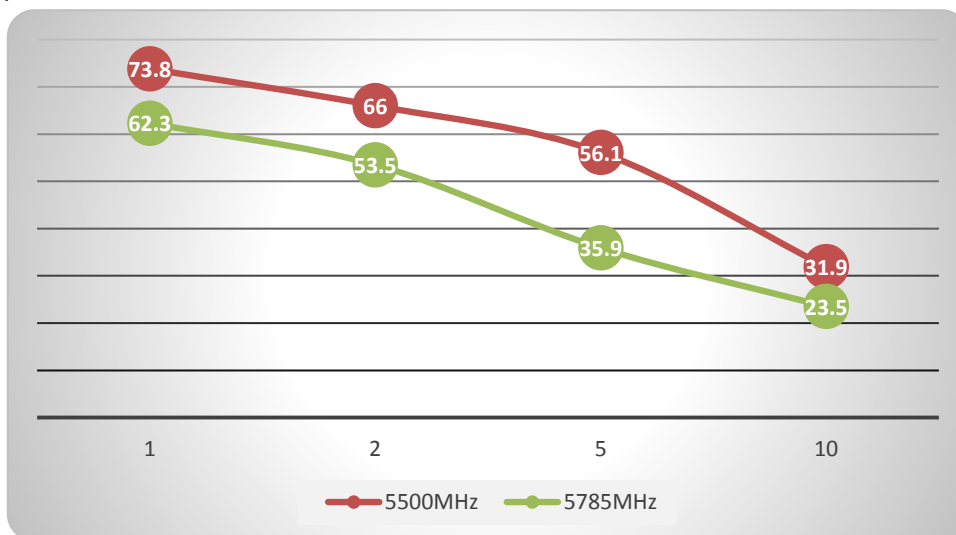
- 5KM Test Result

Equipment (AP/STA)	RSS (dBm)	Throughput (Mbps)	Channel	Bandwidth
55/56	-72/-73	17.8/18.1 (uplink and downlink)	5785 MHz	20MHz
55/56	-72/-69	28/28.1 (uplink and downlink)	5500 MHz	20MHz
55/56	-77/-77	26.2/25.9 (uplink and downlink)	5785 MHz	40MHz
55/56	-74/-74	34.4/34.7 (uplink and downlink)	5500 MHz	40MHz

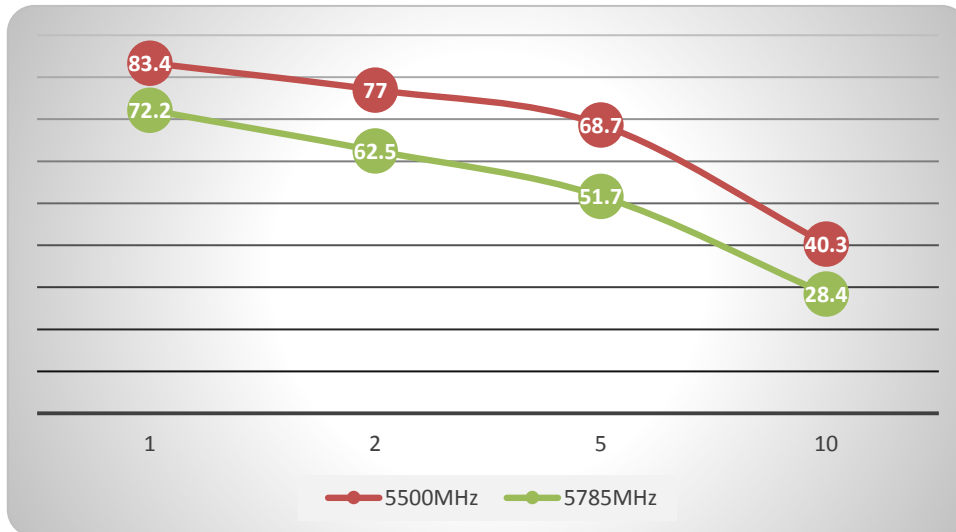
- 10KM Test Result

Equipment (AP/STA)	RSS (dBm)	Throughput (Mbps)	Channel	Bandwidth
55/56	-77/-79	11.8/11.7 (uplink and downlink)	5785 MHz	20MHz
55/56	-75/-72	16/15.9 (uplink and downlink)	5500 MHz	20MHz
55/56	-80/-81	14.8/13.6 (uplink and downlink)	5785 MHz	40MHz
55/56	-78/-74	19.3/21 (uplink and downlink)	5500 MHz	40MHz

- Throughput and Distance Curve



Appendix Figure 4-3 Throughput and Distance Curve at Suburb and 20M bandwidth

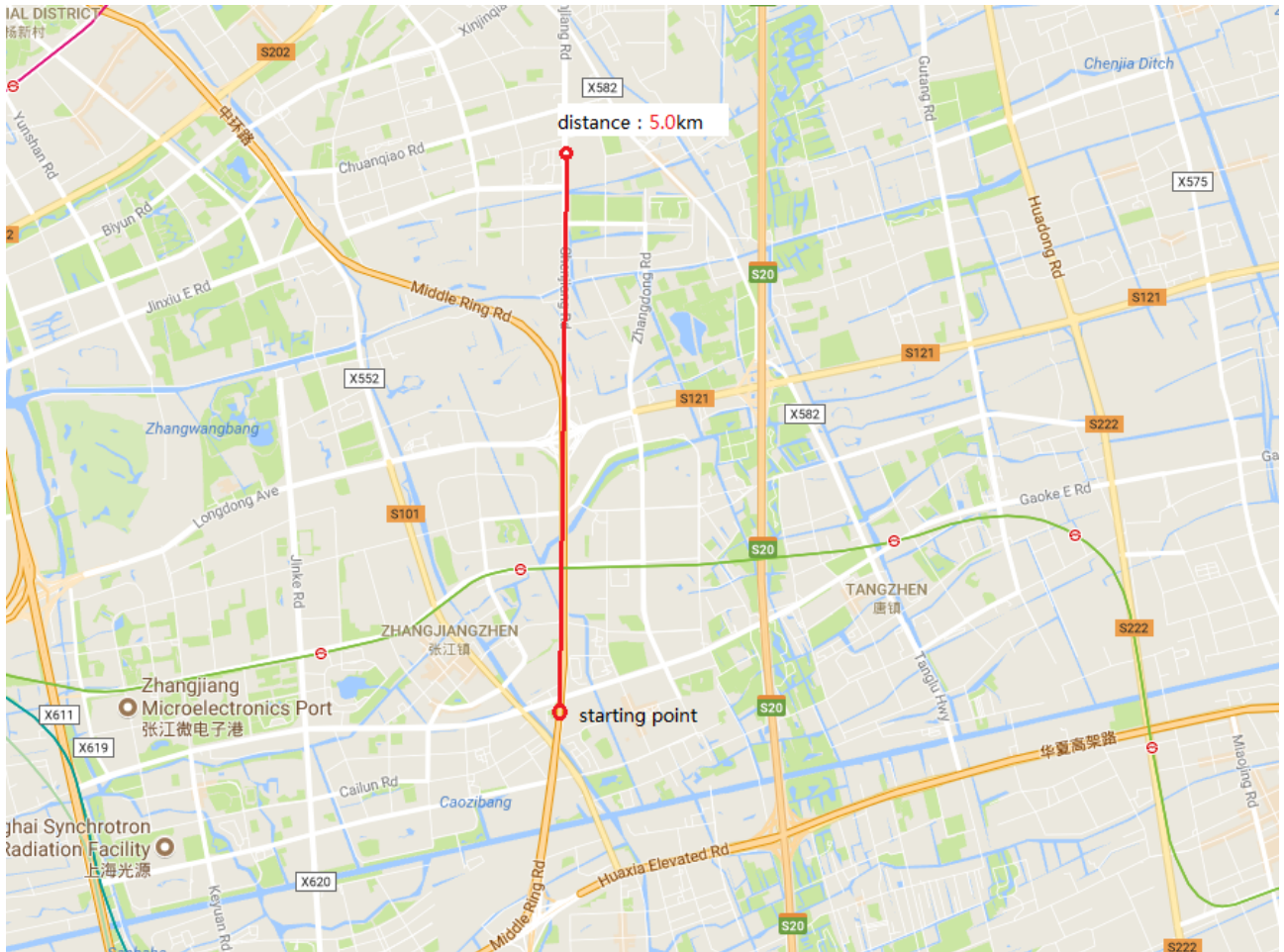


Appendix Figure 4-4 Throughput and Distance Curve at Suburb and 40M bandwidth

Test (Slight Occlusion)

This test was carried out at Shenjiang Road in Pudong New District of Shanghai (as shown in the following figure). Crucial features of this test are as follows:

- 1) Shenjiang Road is relatively straight, but with ups and downs (including bridges etc.), so it is slightly occluded environment.
- 2) There are buildings, many companies and hotels at both sides of Shenjiang Road. There is WIFI signal in many buildings, so wireless environment is relatively harsh.
- 3) Numerous trucks and cars on Shenjiang Road exert great effects on wireless signal.



Appendix Figure 4-5

Test Tool

- 1) Test tool: Chariot (professional network speed test software)
- 2) Test equipment: DH-PFM880 <->DH-PFM881; one DH-PFM880 and one DH-PFM881 were placed at both points respectively.

Test Result

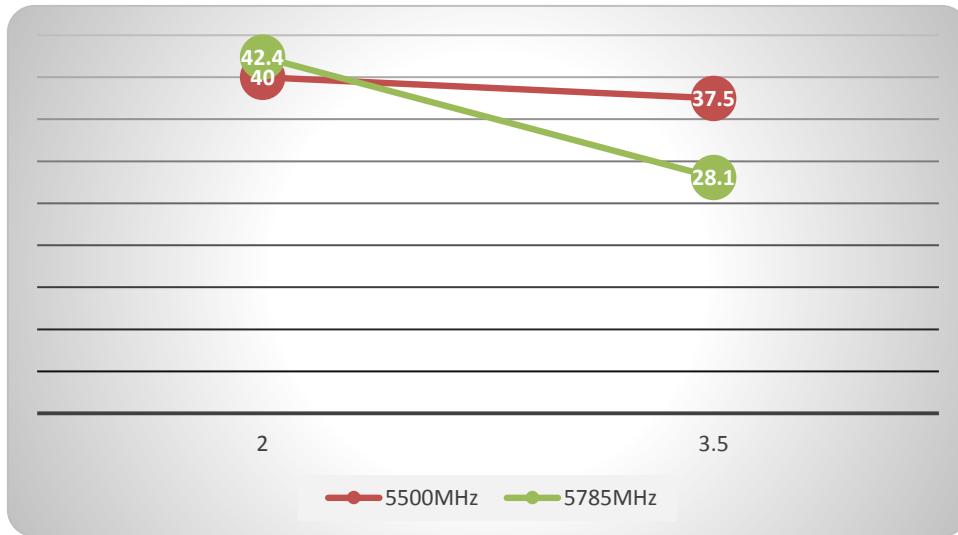
- 2KM Test Result

Equipment (AP/STA)	RSS (dBm)	Throughput (Mbps)	Channel	Bandwidth
55/56	-73/-75	33.5/8.9(uplink and downlink)	5785 MHz	20MHz
55/56	-71/-73	23.6/16.4(uplink and downlink)	5500 MHz	20MHz

- 3.5KM Test Result

Equipment (AP/STA)	RSS (dBm)	Throughput (Mbps)	Channel	Bandwidth
55/56	-77/-77	14.6/13.5(uplink and downlink)	5785 MHz	20MHz
55/56	-74/-73	17.7/19.8(uplink and downlink)	5500 MHz	20MHz

- Throughput and Distance Curve



Appendix Figure 4-6 Throughput and Distance Curve at Downtown Area and 20M bandwidth

Appendix 5 Technical Specification

Type	Item	DH-PFM880	DH-PFM881
Wireless technology	Standard	IEEE802.11a/n (2T2R 300Mbps)	
	Modulation	802.11 a/n:OFDM	
	Antenna	External antenna: gain 16dbi	Internal antenna: gain 15dbi
	Equivalent output power	+27dBm(@MCS0,11n)	+23dBm(@MCS0,11n) +15dBm(@300Mbps,11n)
	Receiving sensitivity	-74dBm @ 65Mbps, -96dBm@1Mbps	
	Optimal transmission distance	0-3km	
	Working frequency	5745-5825 MHz (support frequency extension, extension)	
	Wireless authentication	SRRC	
	Wireless direction angle	Horizontal 90°, angle of elevation 12°	Horizontal 40°, angle of elevation 15°
	Transmission rate	11n:13.5/15/27/30/40.5/45/54/60/81/90/108/120/121.5/135/150/162/180/211n:130/117/104/78/65/58.5/52/39/26/19.5/13/6.5Mbps (20MHz Channel) 11a: 54/48/36/24/18/12/9/6Mbps(self-adaption)	
Hardware	Working voltage	12~24V POE	
	Power consumption	MAX 10W	MAX 8W
	Interface	POE	
	Indicator light	Wi-Fi status indicator light /LAN interface indicator light /power indicator light /signal strength indicator light	
	Working temperature	-30℃~+70℃	
	Storage temperature	-30~+80℃	
	Working humidity	5%~95%RH non-condensing	
	Host machine dimension (mm)	233×233×45	270×50×80
	Antenna dimension (mm)	450×140×35	N/A
	Host machine weight	2.4Kg	0.45Kg
	Antenna weight	1.26Kg	N/A
	Protection level	IP66	N/A
Software	Way of encryption	WEP/WPA-PSK/WPA2/CCMP(AES)/TKIP	
	Network mode	Route/ network bridge	
	Working mode	AP/client /WDS AP/WDS client	
	Security mechanism	IP/MAC address filtering, hide network name and so on	
	Network protocol	TCP/UDP/ARP/ICMP/DHCP/HTTP/NTP	
	TDMA enhancement	Support (TDMA removes effects of hidden nodes and promotes one-to-many performance substantially)	
	Auto ACK timing adjustment	Support (optimize parameters automatically during long-distance communication, and optimize performance)	
	Management and log	NTP, SNMP, Syslog, Telnet	
	Webpage configuration management	Support webpage configuration	
	Firmware update	Support webpage update of firmware	
	Flexible configuration of bandwidth	5M/10M/20M/40MHz	



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