H3C

H3C WX5002V2 Access Controller

Installation Manual

Hangzhou H3C Technologies Co., Ltd.

Manual Version: APW100-20091125

All Rights Reserved

Trademarks

Notice

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied.

About This Manual

Organization

H3C WX5002V2 Access Controller Installation Manual is organized as follows:

Chapter	Contents
1 Access Controller Overview	Introduces the appearance and features of the H3C WX5002V2 access controller.
2 Installation Preparation	Introduces the installation environment of the H3C WX5002V2 access controller, the precautions before and during the installation, and the tools required for the installation.
3 Installation	Introduces the installation method for the WX5002V2, connection method for the power cord, console cable and Ethernet cable, and the checking items after the installation.
4 Initial Startup	Introduces the startup and configuration of the WX5002V2, including the establishment of a configuration environment, connection of a configuration terminal, terminal parameter settings, and the access controller startup.
5 Software Maintenance	Introduces the software maintenance methods for the WX5002V2, including the BootWare menu introduction, software upgrade, and how to deal with password loss.
6 Troubleshooting	Introduces problems that may occur during the installation and startup of the WX5002V2 and the solutions to the problems.
Appendix A Installation of Lightning Arrester for Network Interfaces	Introduces the tools, installation procedure, and precautions for installing a lightning arrester for network interfaces.
Appendix B Installation of Lightning Arrester for AC Power	Introduces how to install a lightning arrester for the AC power and the installation precautions.
Appendix C Regulatory Compliance Information	Introduces the regulatory compliance standards, European directives compliance, USA regulatory compliance, Canada regulatory compliance, Japan regulatory compliance, and CISPR 22 compliance.
Appendix D Safety Information Sicherheits	Introduces the safety precautions that should be followed during the installation and maintenance of the access controller.

Conventions

The manual uses the following conventions:

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window appears; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Convention	Description
< >	Button names are inside angle brackets. For example, click <OK>.
[ ]	Window names, menu items, data table and field names are inside square brackets. For example, pop up the [New User] window.
/	Multi-level menus are separated by forward slashes. For example, [File/Create/Folder].

Symbols

Convention	Description
⚠ **Warning**	Means reader be extremely careful. Improper operation may cause bodily injury.
⚠ **Caution**	Means reader be careful. Improper operation may cause data loss or damage to equipment.
💡 **Highlight**	Means an action or information that needs special attention to ensure successful configuration or good performance.
📝 **Note**	Means a complementary description.

Related Documentation

In addition to this manual, each H3C WX5002V2 access controller documentation set includes the following:

Manual	Description
H3C WX Series Access Controller Products User Manual	Provides a guide to the configuration of the WX series access controllers. The manual covers command line interface, VLAN, system maintenance and debugging, wireless LAN, IPv4, IPv6, basic port configurations, multicast protocols, 802.1x, AAA, SSH, ACL, QoS, and description of the acronyms used throughout the manual.
H3C WX Series Access Controller Products Web-Based Configuration Manual	Introduces the Web based management function of the WX series access controllers.

Obtaining Documentation and Technical Support

To obtain up-to-date documentation and technical support, go to **http://www.h3c.com** and select your country or region. Depending on your selection, you will be redirected to either of the following websites:

At http://www.h3c.com

Documentation

Go to the following columns for different categories of product documentation:

[Technical Support & Document > Technical Documents]: Provides several categories of product documentation, such as installation and configuration.

[Technical Support & Document > Software Download]: Provides the documentation released with the software version.

Technical Support

customer_service@h3c.com

http://www.h3c.com

At http://www.h3cnetworks.com

Documentation

1) Select **Drivers & Downloads** in the **Support** area.
2) Select **Documentation** for **Type of File** and select **Product Category**.

Technical Support

Register Your Product

Warranty and other service benefits start from the date of purchase, so it is important to register your product quickly to ensure you get full use of the warranty and other service benefits available to you.

Warranty and other service benefits are enabled through product registration. Register your product at **http://www.h3cnetworks.com**, go to **Support**, **Product Registration**. Support services are based on accounts that you create or have authorization to access. First time users must apply for a user name and password that provides access to a number of eSupport features including Product Registration, Repair Services, and Service Request. If you have trouble registering your product, please contact 3Com Global Services for assistance.

Purchase Value-Added Services

To enhance response times or extend warranty benefits, contact 3Com or your authorized reseller. Value-added services like Express^{SM} and Guardian^{SM} can include 24x7 telephone technical support, software upgrades, onsite assistance or advance hardware replacement. Experienced engineers are available to manage your installation with minimal disruption to your network. Expert assessment and implementation services are offered to fill resource gaps and ensure the success of your networking projects. More information on 3Com maintenance and Professional Services is available at **http://www.h3cnetworks.com**.

Contact your authorized reseller or 3Com for a complete list of the value-added services available in your area.

Troubleshoot Online

You will find support tools posted on the web site at **http://www.h3cnetworks.com/** under **Support**, **Knowledgebase**. **The Knowledgebase** helps you troubleshoot H3C products. This query-based interactive tool contains thousands of technical solutions.

Access Software Downloads

Software Updates are the bug fix / maintenance releases for the version of software initially purchased with the product. In order to access these Software Updates you must first register your product on the web site at **http://www.h3cnetworks.com,** go to **Support**, **Product Registration.**

First time users will need to apply for a user name and password. A link to software downloads can be found at **http://www.h3cnetworks.com**, under **Support, Drivers and downloads**.

Software Upgrades are the software releases that follow the software version included with your original product. In order to access upgrades and related documentation you must first purchase a service contract from 3Com or your reseller.

Telephone Technical Support and Repair

To enable telephone support and other service benefits, you must first register your product at **http://www.h3cnetworks.com/**

Warranty and other service benefits start from the date of purchase, so it is important to register your product quickly to ensure you get full use of the warranty and other service benefits available to you.

When you contact 3Com for assistance, please have the following information ready:

- Product model name, part number, and serial number
- Proof of purchase, if you have not pre-registered your product

- A list of system hardware and software, including revision level
- Diagnostic error messages
- Details about recent configuration changes, if applicable

To send a product directly to 3Com for repair, you must first obtain a return authorization number (RMA). Products sent to 3Com, without authorization numbers clearly marked on the outside of the package, will be returned to the sender unopened, at the sender's expense. If your product is registered and under warranty, you can obtain an RMA number online at **http://www.h3cnetworks.com** under **support, Repair & Replacement Request**. First time users will need to apply for a user name and password.

Contact Us

3Com offers telephone, e-mail and internet access to technical support and repair services. To access these services for your region, use the appropriate telephone number, URL or e-mail address.

Find a current directory of contact information posted on the web site at **http://www.h3cnetworks.com** under **Support**, **Technical Support Contact**..

Documentation Feedback

You can e-mail your comments about product documentation to info@h3c.com.

We appreciate your comments.

Environmental Protection

This product has been designed to comply with the requirements on environmental protection. For the proper storage, use and disposal of this product, national laws and regulations must be observed.

Table of Contents

1 Access Controller Overview

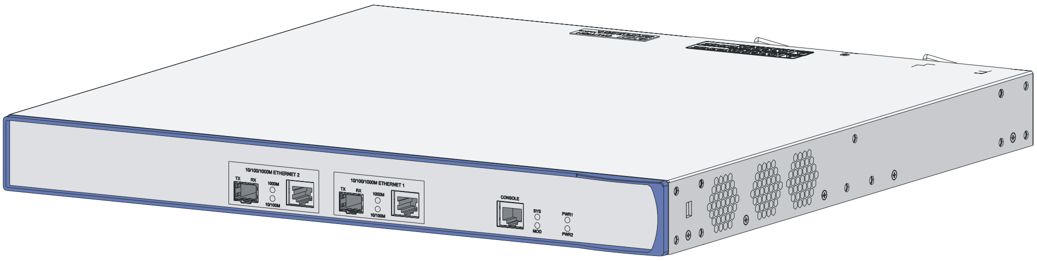
Introduction

The H3C WX5002V2 Access Controller is a new-generation wireless access controller product developed by Hangzhou H3C Technologies Co., Ltd. (referred to as H3C hereinafter). The WX5002V2 provides two groups of Combo ports. Besides, the WX5002V2 also provides an expansion slot, where you can insert a card of a different type as needed in the future. This provides not only strong processing capability but also flexible system configuration schemes. In terms of reliability, the WX5002V2 uses pluggable power supply units (PSU). Thus, you can choose to use double PSUs for high reliability or use a single PSU for economical sake.

Appearance

Figure 1-1 shows the appearance of the WX5002V2.

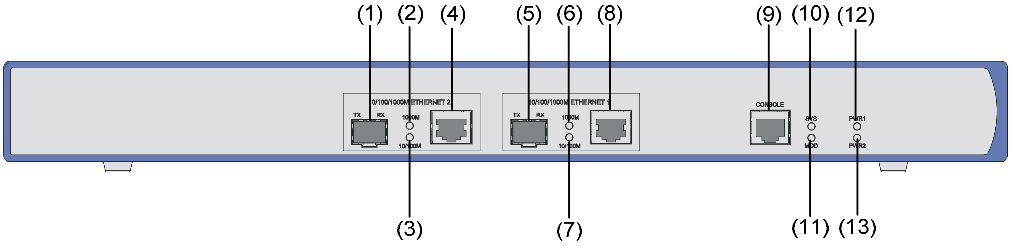
Figure 1-1 Appearance of the WX5002V2



Front Panel

The WX5002V2 provides two 10/100/1000 Base-T Ethernet electrical interfaces, two 1000 Base-X Ethernet optical interfaces (Combo ports) and one console port on its front panel, as shown in Figure 1-2.

Figure 1-2 Front panel of the WX5002V2

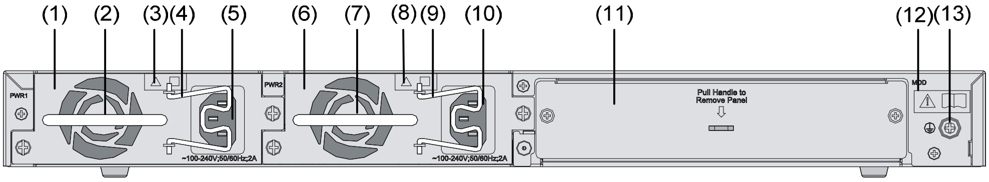


(1) Gigabit Ethernet interface 2—SFP optical interface	
(2) 1000 Mbps LED of gigabit Ethernet interface 2	
(3) 10/100 Mbps LED of gigabit Ethernet interface 2	
(4) 10/100/1000 Base-T auto-sensing Ethernet electrical interface 2	
(5) Gigabit Ethernet interface 1—SFP optical interface	
(6) 1000 Mbps LED of gigabit Ethernet interface 1	
(7) 10/100 Mbps LED of gigabit Ethernet interface 1	
(8) 10/100/1000 Base-T auto-sensing Ethernet electrical interface 1	
(9) Console port	(10) System LED
(11) LED of the expansion card	(12) LED of power supply 1
(12) LED of power supply 2	

Rear Panel

The WX5002V2 provides two power supply module slots and one expansion card slot, as shown in Figure 1-3.

Figure 1-3 Rear panel of the WX5002V2



(1) PSU 1 (AC/DC)	(2) Handle of PSU 1
(3) OPEN BOOK sign	(4) Power cord retainer for PSU 1
(5) AC power socket of PSU 1	(6) PSU 2 (AC/DC)
(7) Handle of PSU 2	(8) OPEN BOOK sign
(9) Power cord retainer for PSU 2	(10) AC power socket of PSU 2
(11) Expansion card slot	(12) OPEN BOOK sign
(13) Grounding screw	

OPEN BOOK and CAUTION signs: Refer to related sections when performing the following operations:

Table 1-1 OPEN BOOK sign description

Operation	Related section
Connect the power cord	Connecting the AC Power Cord
Ground the device	Connecting the Ground Wire

Specifications

Processor and Storages

Table 1-2 Processor and storages of the WX5002V2

Item	Description
Processor	XLR716 (800 MHz)
CF card	Built in, 256 MB
Memory type and capacity	Memory: DDR2 SDRAM Capacity: 1024 MB

Dimensions and Weight

Table 1-3 Dimensions and weight

Item	Description
Dimensions (H × W × D)	43.6 × 440 × 430 mm (1.72 × 17.32 × 16.93 in.)
Weight	7.4 kg (16.31 lb.) (with two PSUs installed)

Fixed Interfaces and Slots

Table 1-4 Fixed interfaces and slots

Item	Description
Console port	1 console port, 9600 bps (the default) to 115200 bps.
Ethernet interfaces	2 × 10/100/1000 Base-T autosensing Layer 2 Ethernet interfaces; support MDI/MDIX
SFP interfaces	2 × 1000 Base-X SFP optical interfaces, forming Combo ports together with the corresponding Ethernet electrical interfaces
Slots	• 1 expansion card slot • 2 PSU slots

Power Input

The WX5002V2 uses two AC/DC PSUs, which provide 1+1 redundancy backup for the WX5002V2 to enhance the system reliability.

Table 1-5 AC/DC power input

Item	Description
Rated voltage range	For AC power input: 100 VAC to 240 VAC, 50 Hz or 60 Hz For DC power input: –48 VDC to –60 VDC

Item	Description
Max input voltage range	For AC power input: 90 VAC to 264 VAC, 47 Hz to 63 Hz For DC power input: –36 VDC to –72 VDC
Power consumption	53.4 W to 67.7 W

Note

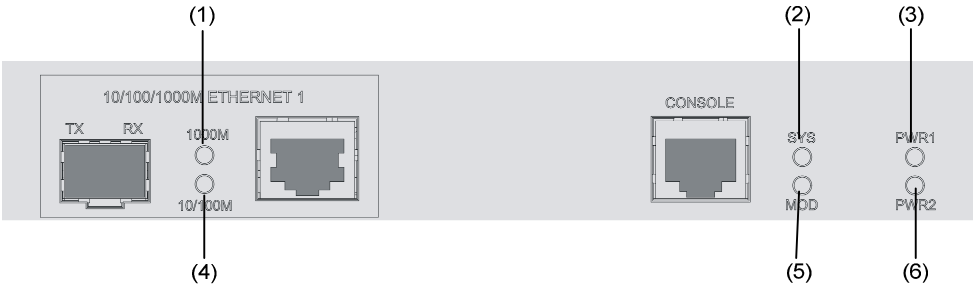
- You are not recommended to use an AC power module with a DC power module on the device.
- No AC or DC power module is provided with the access controller. You need to prepare them yourself.

Components

LEDs

The WX5002V2 provides LEDs on the front panel, as shown in Figure 1-4.

Figure 1-4 LEDs of the WX5002V2



(1) 1000 Mbps LED of gigabit Ethernet interface (1000M)	
(2) System status LED (SYS)	(3) Status LED of PSU 1 (PWR1)
(4) 10/100 Mbps LED of gigabit Ethernet interface (10/100M)	
(5) LED of the expansion card (MOD)	(6) Status LED of PSU 2 (PWR2)

Table 1-6 Description of LEDs

LEDs	Silkscreen	Status	Description
LED of PSU 1 (green/yellow)	PWR1	Solid green	PSU 1 supplies power to the system normally.
		Solid yellow	PSU 1 is faulty.
		Off	No PSU is installed in the slot.
LED of PSU 2 (green/yellow)	PWR2	Solid green	PSU 2 supplies power to the system normally.
		Solid yellow	PSU 2 is faulty.
		Off	No PSU is installed in the slot.

LEDs	Silkscreen	Status	Description
System LED (green/yellow)	SYS	Solid green	The system is performing POST or downloading software.
		Green, slow blinking (1 Hz)	The system works normally.
		Solid yellow	The POST has failed or another fatal error has been detected in the system.
		Off	No power input
LED of the expansion card (green)	MOD	Solid green	The expansion card is present in the slot.
		Off	The expansion card is not present in the slot
Gigabit Combo port LED	1000M	Solid green	The interface is connected at 1000 Mbps.
		Blinking green (6 Hz)	The port is receiving or sending data at 1000 Mbps
		Off	The interface is not connected at 1000 Mbps.
	10/100M	Solid yellow	The interface is connected at 10/100 Mbps.
		Blinking yellow (6 Hz)	The interface is receiving or sending data at 10/100 Mbps.
		Off	The interface is not connected at 10/100 Mbps.

Fixed Interfaces

Console port

The WX5002V2 provides an RS232 asynchronous serial port (console port) that can be connected to a computer for system debugging, configuration, maintenance, management, and host software loading.

The console cable is an 8-core cable. One end of the cable is a crimped RJ-45 connector and is connected to the console port of the WX5002V2. The other end is a DB-9 female connector and is connected to the 9-pin serial port on the configuration terminal. Figure 1-5 illustrates a console cable:

Figure 1-5 Console cable

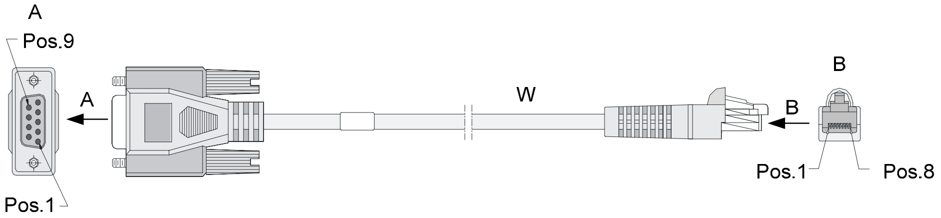


Table 1-7 Console cable pinouts

RJ-45	Signal	Direction	DB-9
1	RTS	←	7
2	DTR	←	4

RJ-45	Signal	Direction	DB-9
3	TXD	←	3
4	CD	→	1
5	GND	—	5
6	RXD	→	2
7	DSR	→	6
8	CTS	→	8

Ethernet interfaces

1) Introduction

The WX5002V2 provides two 10/100/1000 Base-T autosensing Ethernet electrical interfaces and two 1000 Base-X SFP optical interfaces. One electrical interface and one optical interface form a Combo port, which is marked in a white box on the front panel. Only one interface (either electrical or optical) of a Combo port can be used at a time.

- Ethernet electrical interfaces support 10/100/1000 Mbps autosensing. Table 1-8 describes the working mode of the interfaces in each speed.

Table 1-8 Speed and working mode of an electrical Ethernet interface

Speed	Working mode
10 Mbps (autosensing)	Half/full duplex, auto-negotiation
100 Mbps (autosensing)	Half/full duplex, auto-negotiation
1000 Mbps (autosensing)	Full duplex, auto-negotiation

- Ethernet optical interfaces support 1000 Mbps full duplex. The optical interface and the electrical interface of a Combo port share the same LED.

Note

- A Combo port can work in either the electrical interface mode or the optical interface mode, that is, either the electrical interface or the optical interface of a Combo port can be used at a time.
- A Combo port supports optical-electrical automatic switching, however, when both the optical and electrical interfaces are connected, the electrical interface will be used in precedence.

2) SFP interface modules

The WX5002V2 provides four SFP GE optical interfaces. The following SFP modules are available:

- 1000 Base-SX SFP module
- 1000 Base-LX SFP module

Table 1-9 Technical specifications for the GE optical interface modules

Item		Description				
		Short-haul multimode (850 nm) **SFP module**	**Medium-haul single-mode (1310 nm)** **SFP module**	**Long-haul single-mode (1310 nm)** **SFP module**	**Long-haul single-mode (1550 nm)** **SFP module**	**Ultra-long-haul single-mode (1550 nm)** **SFP module**
Connector		SFP/LC				
Optical fiber		62.5 µm/125 µm multimode	9 µm /125 µm single-mode	9 µm /125 µm single-mode	9 µm /125 µm single-mode	9 µm /125 µm single-mode
Max. transmission distance		0.55 km (0.34 mi)	10 km (6.21 mi)	40 km (24.86 mi)	40 km (24.86 mi)	70 km (43.50 mi)
Central wavelength		850 nm	1310 nm	1310 nm	1550 nm	1550 nm
Optical transmit power	Min.	-9.5 dBm	-9 dBm	-2 dBm	-4 dBm	-4 dBm
	Max.	0 dBm	-3 dBm	5 dBm	1 dBm	2 dBm
Receive sensitivity		-17 dBm	-20 dBm	-23 dBm	-21 dBm	-22 dBm
Working mode		1000 Mbps Full duplex				

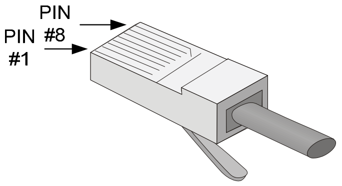
Note

No SFP module is shipped with the WX5002V2. You need to purchase SFP modules as needed and are recommended to use H3C SFP modules.

3) RJ-45 connector

The 10/100/1000 Mbps electrical Ethernet interfaces of the WX5002V2 use RJ-45 connectors to connect with the category 5 twisted pair cables. Figure 1-6 shows the appearance of an RJ-45 connector.

Figure 1-6 RJ-45 connector

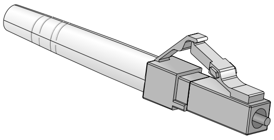


4) LC connector

Optical fiber connectors are indispensable passive components in optical fiber communication systems. Their application enables the removable connection between optical channels, which makes the optical system debugging and maintenance more convenient and the transit dispatching of the system more flexible.

The Ethernet optical interfaces of the WX5002V2 support LC connectors only.

Figure 1-7 LC connector



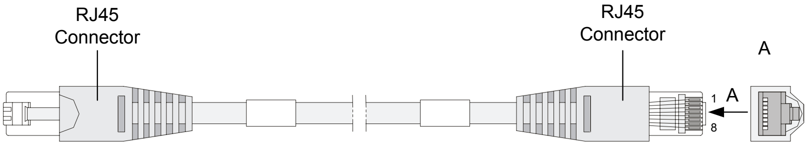
Note

- Before using an optical fiber to connect a network device, make sure that the optical fiber connector matches the optical module.
- Before connecting the fiber, make sure that the receiving-end optical power does not exceed the upper threshold of the receiving optical power. Excessive receiving optical power is very likely to burn the optical module. For optical power values of the optical modules, refer to Table 1-9.

5) Ethernet electrical interface cables

Usually, you can use a category-5 twisted pair cable to connect an electrical interface to an Ethernet. Figure 1-8 shows an Ethernet cable.

Figure 1-8 Ethernet cable



Ethernet cables fall into the following two categories:

- Standard cable: Also called straight-through cable. At both ends of a standard cable, wires are crimped in the RJ-45 connectors in the same sequence. A straight-through cable is used to connect a terminal (for example, PC or router) to a Hub or LAN Switch.
- Crossover cable: At both ends of a crossover cable, wires are crimped in the RJ-45 connectors in different sequences. A crossover cable is used to connect a terminal (for example, a PC or router) to another terminal. You can make crossover cables by yourself as needed.

Table 1-10 Straight-through cable pinouts

RJ-45	Signal	Category-5 twisted pair	Signal direction	RJ-45
1	TX+	White (Orange)	→	1
2	TX-	Orange	→	2
3	RX+	White (Green)	←	3
4	—	Blue	—	4
5	—	White (Blue)	—	5
6	RX-	Green	←	6

RJ-45	Signal	Category-5 twisted pair	Signal direction	RJ-45
7	—	White (Brown)	—	7
8	—	Brown	—	8

Table 1-11 Crossover cable pinouts

RJ-45	Signal	Category-5 twisted pair	Signal direction	RJ-45
1	TX+	White (Orange)	→	3
2	TX-	Orange	→	6
3	RX+	White (Green)	←	1
4	—	Blue	—	4
5	—	White (Blue)	—	5
6	RX-	Green	←	2
7	—	White (Brown)	—	7
8	—	Brown	—	8

Note

- You can refer to the table above when distinguishing between or preparing these two types of Ethernet cables.
- When preparing Ethernet cables, please follow the chromatogram given in the table to arrange the wires. Otherwise communication quality will be affected even if the devices at both ends are connected.

Fans

The WX5002V2 is equipped with five fans: three fans for heat dissipation of the main board and two fans for heat dissipation of the expansion card. If no expansion card is installed, these two fans do not work.

Interface Numbering

The WX5002V2 provides four fixed GE interfaces numbered GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2, with the last part of the port numbers indicated on the front panel.

2 Installation Preparation

Safety Precautions

Warning

Installation and removal of the unit and its accessories must be carried out by qualified personnel. You must read all of the Safety Instructions supplied with your device before installation and operation.

Warnung

Installation und Ausbau der Anlage und ihrer Zubehörteile müssen von qualifiziertem Personal realisiert werden. Sie müssen vor der Installation oder Bedienung allen beiliegenden Sicherheitshinweise lesen.

警告

负责安装和日常维护本设备的人员必须具备安全操作基本技能。在操作本设备前，请务必认真阅读和执行产品手册规定的安全规范。

To avoid any device impairment and bodily injury caused by improper use, observe these rules:

- Pull the power plug(s) out of the access controller before cleaning it. Do not clean the access controller using wet cloth or liquid.
- Keep the access controller away from water or dampness. Prevent water or moisture from entering the chassis of the access controller.
- Do not place the access controller on an unstable case or desk. The access controller might be damaged severely in case of a fall.
- Ensure proper ventilation of the equipment room and keep the ventilation vents of the access controller free of obstruction.
- Make sure that the operating voltage is the same one labeled on the access controller.
- Do not open the chassis when the access controller is operating or when electrical hazards are present to avoid electrical shocks.
- When replacing interface modules, wear the ESD-preventive wrist strap to avoid damaging the interface modules.

Installation Site Checking

The WX5002V2 must be used indoors. You can mount the WX5002V2 in a cabinet or on a workbench, but make sure that:

- Adequate clearance is reserved at the air inlet/exhaust vents for heat dissipation.
- The cabinet or workbench is in the environment that has a good ventilation system.
- The cabinet is sturdy enough to support the access controller and its accessories.
- The cabinet or workbench is well earthed.

To ensure normal operation and long service life of your access controller, install it in an environment that meets the requirements described in the following subsections.

Requirements on Temperature and Humidity

To ensure the normal operation and service lifetime of the access controller, proper temperature and humidity should be maintained in the equipment room.

- A long term of high humidity may lead to bad insulation, electricity leakage, mechanical property changes, and metal components corrosion.
- If the relative humidity is too low, captive screws may become loose as a result of contraction of insulation washers and static electricity may be produced in a dry environment to endanger the circuits on the access controller.
- A high temperature is the most undesirable condition, because it accelerates the aging of insulation materials and thus significantly lowers the reliability and service life of the access controller.

The following table lists temperature and humidity requirements for the WX5002V2.

Table 2-1 Operating environment

Item	Description
Operating temperature	0°C to 45°C (32°F to 113°F)
Relative humidity (noncondensing)	5% to 95%

Requirements on Cleanness

Dust is a hazard to the operating safety of the access controller. The dust accumulated on the chassis can be adsorbed by static electricity and result in poor contact of metal connectors or metal contact points. Especially, when the relative indoor humidity is low, electrostatic adsorption is more likely to happen. This can not only shorten the service life of the access controller but also cause communications failures. The following table lists the dust concentration limit.

Table 2-2 Dust concentration limit in the equipment room

Physical active substance	Concentration limit (particles/m^3)
Dust	≤ 3 × 10^4 (No visible dust on the tabletop over three days)
Note: The dust particle diameter is ≥ 5 μm	

Besides the dust specifications, the equipment room of the access controller also needs to strictly meet the requirements on the concentration of salt, acid and sulfide. These harmful gases can accelerate the metallic corrosion and the aging process of some parts. The specific limits of the harmful gases such as are given in the following table.

Table 2-3 Limit on harmful gases in the equipment room

Gas	Maximum concentration (mg/m^3)
SO_2	0.2
H_2S	0.006
NH_3	0.05
Cl_2	0.01

Anti-Static Requirements

Generation and damage of static electricity

In the communication network to which the WX5002V2 is connected, static induction of the access controller mainly comes from the following sources:

- External electric fields, such as outdoor high-voltage transmission lines or thunderbolts.
- Internal environment like flooring materials or the structure of the overall system.

Although the WX5002V2 is designed to be Electrostatic Discharge (ESD) preventive, excessive static electricity may enormously damage the card circuits or even the whole device.

Protection measures

To prevent electrostatic damage, observe the following:

- Ensure that the access controller and the floor is well grounded.
- Keep the equipment room clean.
- Maintain suitable temperature and humidity;
- Wear ESD-preventive gloves or an ESD-preventive wrist strap and uniform when handling the circuit board.
- Hold the interface module only by its edge when installing, observing or removing it. Do not touch the components on it.
- Place the removed interface module on an ESD-preventive workbench with the component-side facing upward or place it in an antistatic bag.

Wearing ESD-Preventive Wrist Strap

Note

No ESD-preventive wrist strap is shipped with the access controller. You need to purchase one if needed.

Follow these steps to use an ESD-preventive wrist strap:

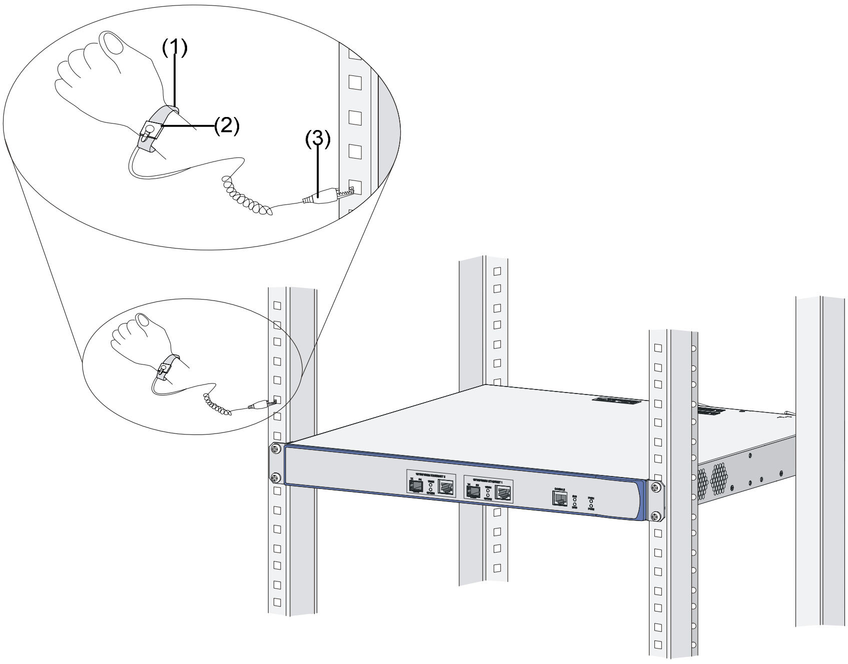
1) Put on the ESD-preventive wrist strap.
2) Fasten the ESD-preventive wrist strap and verify that it makes good skin contact.

3) Lock the terminal of the alligator clip to the ESD-preventive wrist strap.

4) Attach the alligator clip to the rack where the access controller is installed.

5) Make sure that the rack has been well-grounded.

Figure 2-1 Use ESD-preventive wrist strap



(1) ESD-preventive wrist strap	(2) Locker	(3) Alligator clip

Electromagnetic Environment Requirements

The operation of your access controller may be affected by external interferences, such as capacitance coupling, inductance coupling, electromagnetic wave radiation, common impedance (including the grounding system) coupling, and the conducted interference of leads (power cords, signaling cables and output wires). To eliminate the interferences,

- Use the TN power system as the AC power supply system. A TN power system is called zero connection protection system. It is a power distribution system with one point connected directly to earth (ground). The exposed conductive parts and the neutral metal parts of the installation are connected to that point by protective earth conductors. Use a single-phase three-wire power socket with a protection earth (PE) to effectively filter interference from the power grid.
- Keep the access controller far from high-power radio transmitters, radars, and high-frequency heavy-current devices.
- Use electromagnetic shielding measures when necessary. For example, use shielded interface cables.
- Route interface cables only indoors to prevent signal ports from getting damaged by over-voltage or over-current caused by lightning strikes.

Laser Safety

The WX5002V2 is a Class 1 laser device.

When the optional optical ports on the WX5002V2 are operating, avoid staring into the optical interfaces because the high-energy laser beam emitted from the optical fiber may hurt your retina.

Warning

Do not stare the laser beam of an optical fiber. Otherwise, your eyes may be hurt.

Installation Tools

- Flat-blade screwdriver
- Phillips screwdriver: P2-150mm
- ESD-preventive wrist strap

Note

No installation tool or ESD-preventive wrist strap is provided with the access controller. You need to prepare them yourself.

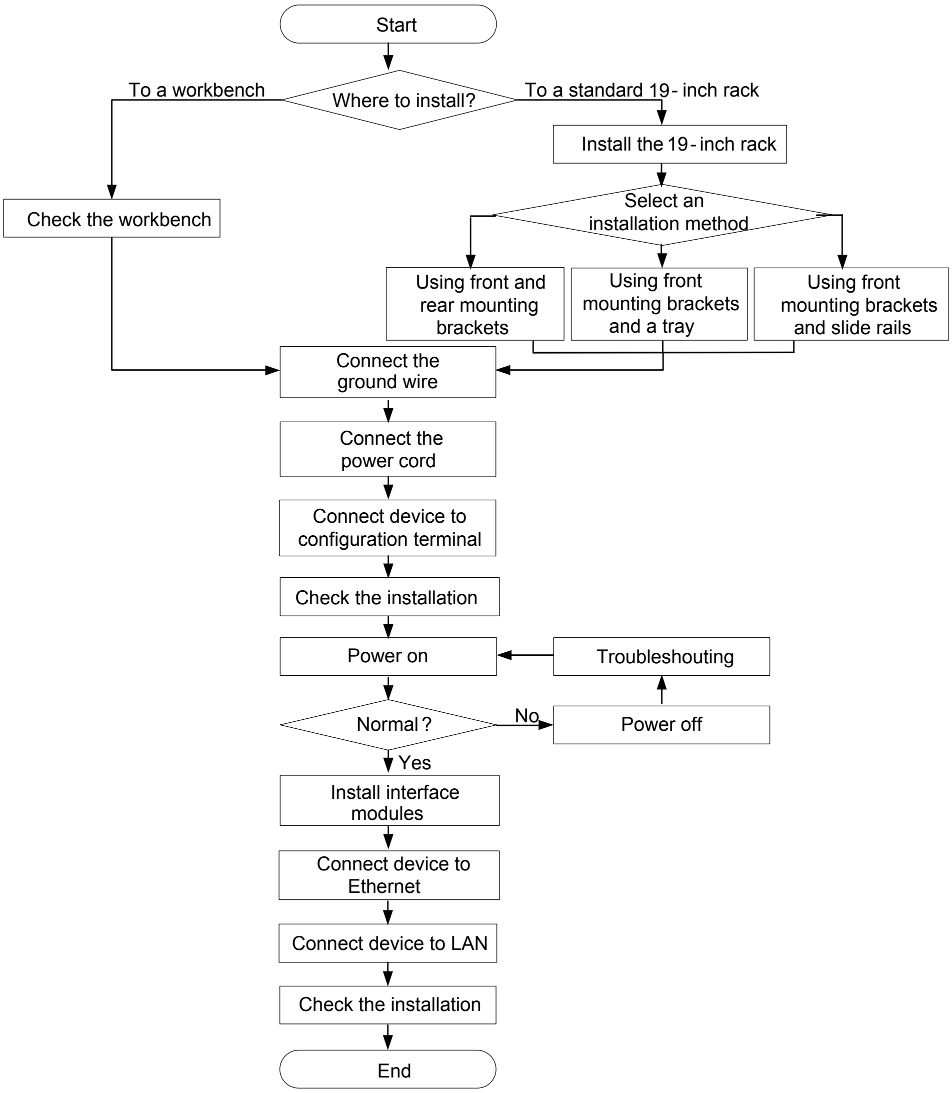
3 Installation

Warning

When you ask your sales agent to maintain your access controller, you must ensure that the dismantlement-preventive seal on a mounting screw of the access controller chassis is intact. If you want to open the chassis, you should contact the agent for permission. Otherwise, you will bear any consequence resulting from your actions.

Installation Procedure

Figure 3-1 Installation procedure


Start
Where to install?
To a workbench
To a standard 19- inch rack
Install the 19- inch rack
Check the workbench
Select an installation method
Using front and rear mounting brackets
Using front mounting brackets and a tray
Using front mounting brackets and slide rails
Connect the ground wire
Connect the power cord
Connect device to configuration terminal
Check the installation
Power on
Troubleshouting
Normal ?
No
Power off
Yes
Install interface modules
Connect device to Ethernet
Connect device to LAN
Check the installation
End

The WX5002V2 can be installed in either a standard 19-inch rack or a workbench as needed.

Installing the Access Controller onto a 19-Inch Rack

The access controller can be installed onto a 19-inch standard rack in one of the following approaches:

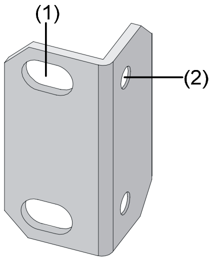
- Installing the access controller with front and rear mounting brackets
- Installing the access controller with front mounting brackets and a tray
- Installing the access controller with front mounting brackets and slide rails

Installing the Access Controller with Front and Rear Mounting Brackets

Mounting bracket structure

1) Appearance of a front mounting bracket

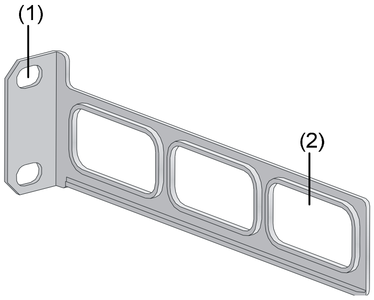
Figure 3-2 Front mounting bracket appearance



(1) Screw hole for fixing the front mounting bracket to the rack (use M6 screws)
(2) Screw hole for fixing the front mounting bracket to the access controller

2) Appearance of a rear mounting bracket

Figure 3-3 Rear mounting bracket appearance



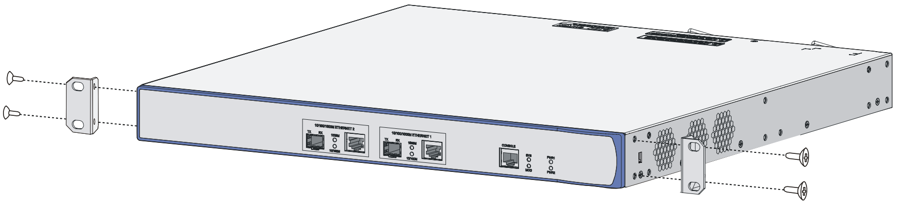
(1) Screw hole for fixing the rear mounting bracket to the rack (use M6 screws)
(2) Heat dissipation hole

Installation procedure

1) Put on the EAD-preventive wrist strap and check that the rack is sturdy and properly earthed.

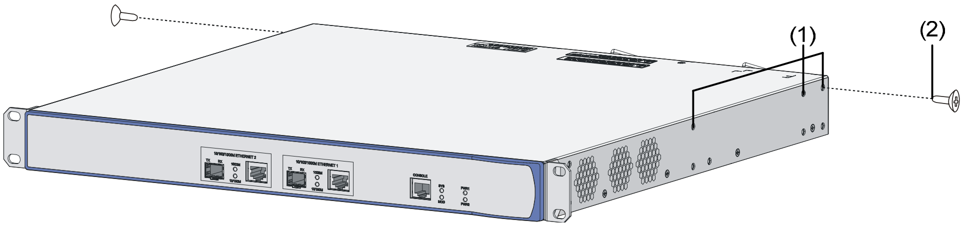
2) Take out the screws, which are packaged with the front mounting brackets. Attach the front mounting brackets to the access controller with the screws, as shown in Figure 3-4.

Figure 3-4 Install front mounting brackets to both sides of the access controller



3) Take out the bearing screws, which are packaged with rear mounting brackets. Attach a bearing screw into the proper installation hole on the rear, upper right and left sides of the access controller respectively, as shown in Figure 3-5.

Figure 3-5 Install bearing screws into the access controller



(1) Three installation holes for bearing screws (choose one as needed)

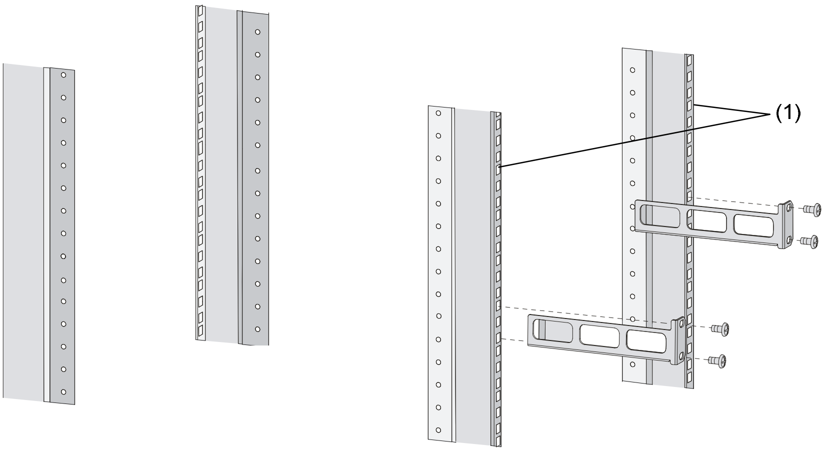
(2) Bearing screw

Note

There are three screw holes on both the right and left sides of the rear, and upper part of the access controller for installing the bearing screws. You need to choose a proper hole to install a bearing screw to each side. The rear mounting brackets can support the weight of the access controller through firm contact with the bearing screws.

4) Determine the position for installing the access controller on the rack. Use screws and the corresponding cage nuts to fix the rear mounting brackets to the rear square-hole rack rails, as shown in Figure 3-6.

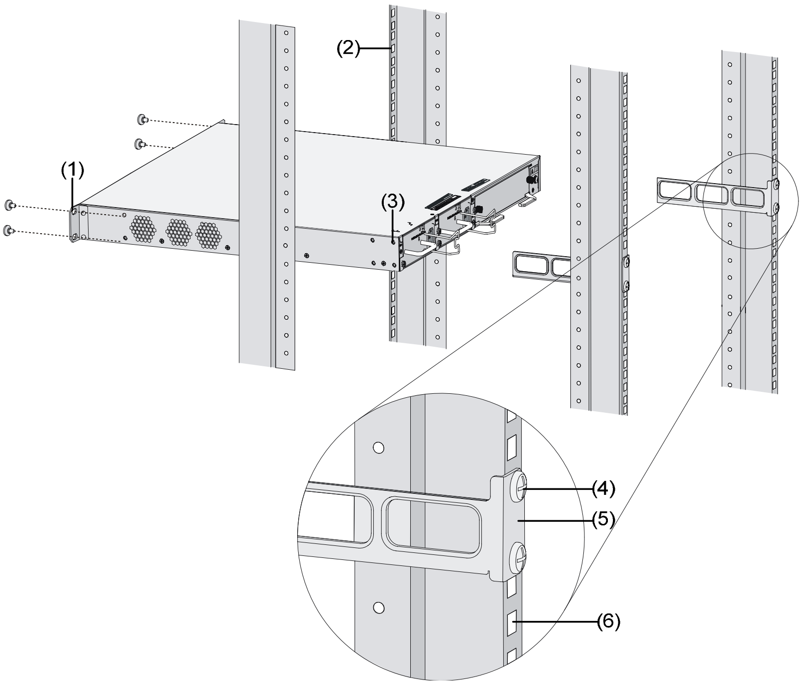
Figure 3-6 Install rear mounting brackets to the rack



(1) Rear square-hole rack rails

5) Support the bottom of your access controller with one hand and hold the front part of the access controller with the other hand, and then gently push the access controller into the rack, as shown in Figure 3-7.

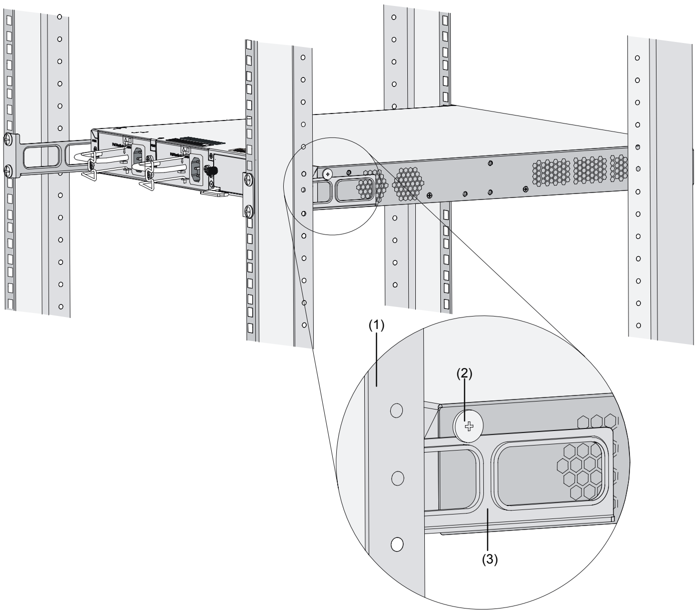
Figure 3-7 Installation with front and rear mounting brackets



(1) Front mounting bracket	(2) Front square-hole rack rail	(3) Bearing screw
(4) Screw for fixing the rear mounting bracket to the rear square-hole rack rail		
(5) Rear mounting bracket	(6) Rear square-hole rack rail	

6) After the access controller is pushed in, make sure that the upper side of the rear mounting brackets and the bearing screws are closely touched, as shown in Figure 3-8.

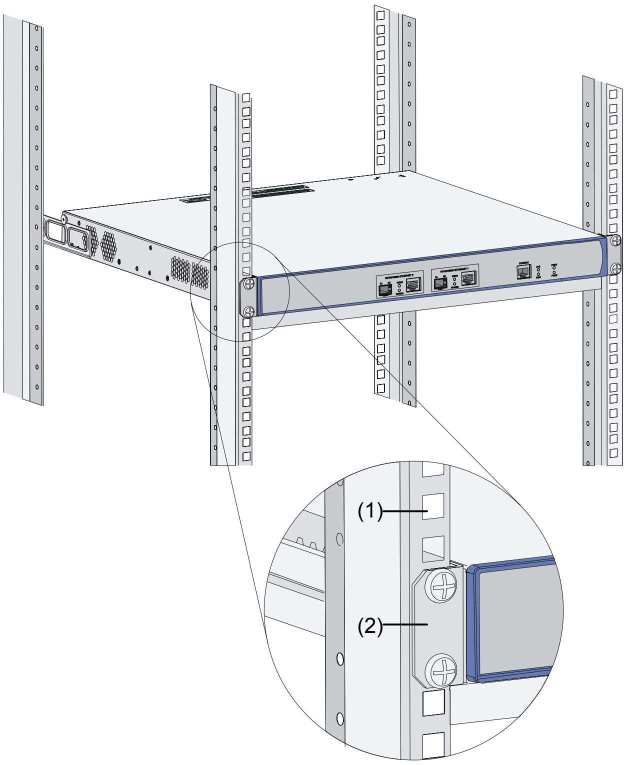
Figure 3-8 Installation with front and rear mounting brackets



(1) Rear square-hole rack rail	(2) Bearing screw
(3) Rear mounting bracket	

7) Use screws and the corresponding cage nuts to fix the front mounting brackets to the front square-hole rack rails, so that the front and rear mounting brackets can fix the access controller on the rack horizontally and steadily, as shown in Figure 3-9.

Figure 3-9 Installation with front and rear mounting brackets



(1) Front square-hole rack rail	(2) Front mounting bracket

Installing the Access Controller with Front Mounting Brackets and a Tray

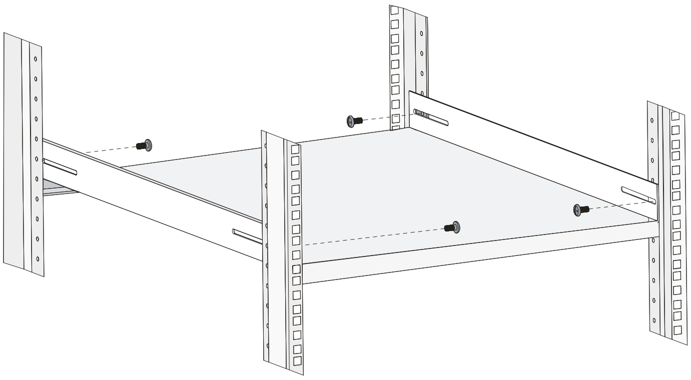
Note

The tray is an optional component, which needs to be separately ordered if needed.

Installation procedure with front mounting brackets and a tray:

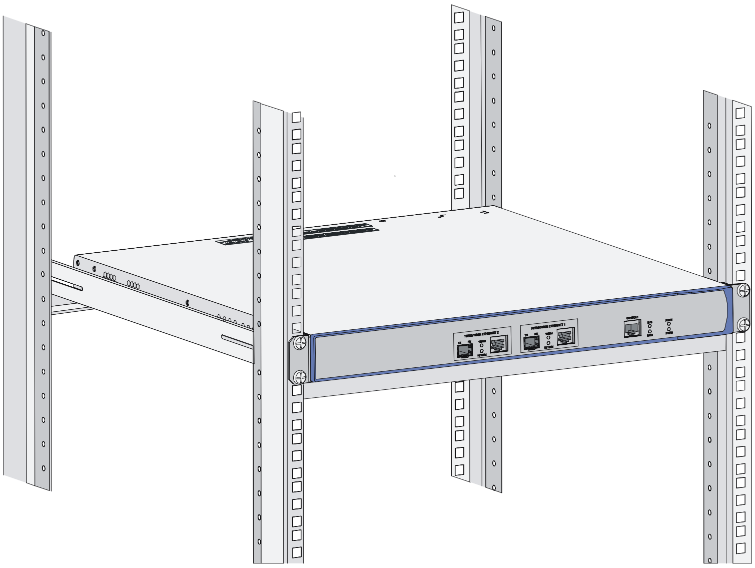
1) Put on the EAD-preventive wrist strap and check that the rack is sturdy and properly earthed.
2) Take out the screws, which are packaged with the front mounting brackets. Attach the front mounting brackets to the access controller with the screws, as shown in Figure 3-4.
3) Fix the tray horizontally to a proper poison on the rack, as shown in Figure 3-10. (This figure is just for your reference. The installation may differ on a different rack.)

Figure 3-10 Install a tray



4) Place the access controller on the tray horizontally, gently push the access controller into the rack along the tray, and then use screws and the corresponding cage nuts to fix the front mounting brackets to the front square-hole rack rails of the rack, as shown in Figure 3-11.

Figure 3-11 Installation with front mounting brackets and a tray



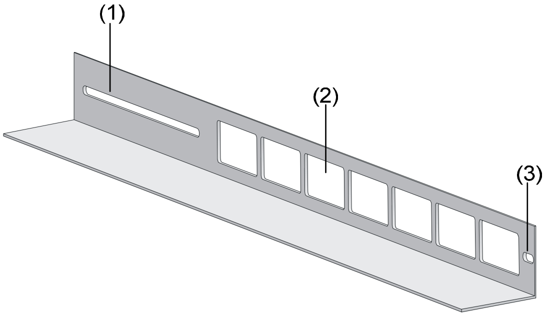
Installing the Access Controller with Mounting Brackets and Slide Rails

Note

- Slide rails are optional components, which need to be separately ordered if needed.
- H3C slide rails are suitable for only the H3C standard racks with a depth of 1000 mm (39.37 in.). If the depth of your rack is different, substitute other supports for the slide rails.

Slide rail appearance

Figure 3-12 Appearance of a slide rail



(1) Slotted hole, a screw hole for fixing the slide rail to the rear round-hole rack rail of the rack. You can adjust the screw position within the screw hole according to the device position.

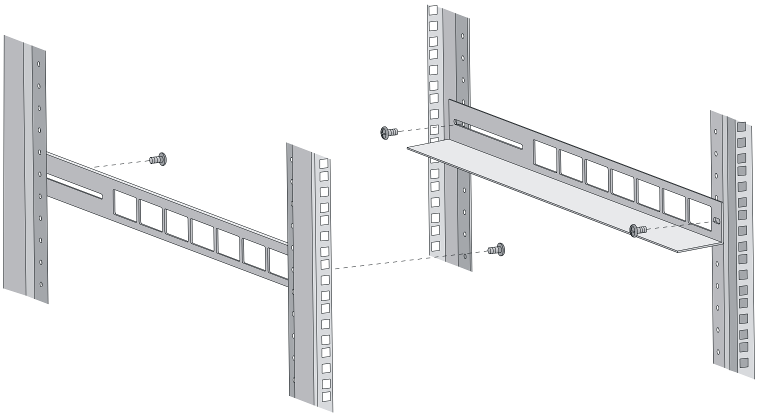
(2) Heat dissipation hole. It is for heat dissipation between the device and rack.

(3) Slotted hole, a screw hole for fixing the slide rail to the front round-hole rack rail of the rack.

Installation procedure

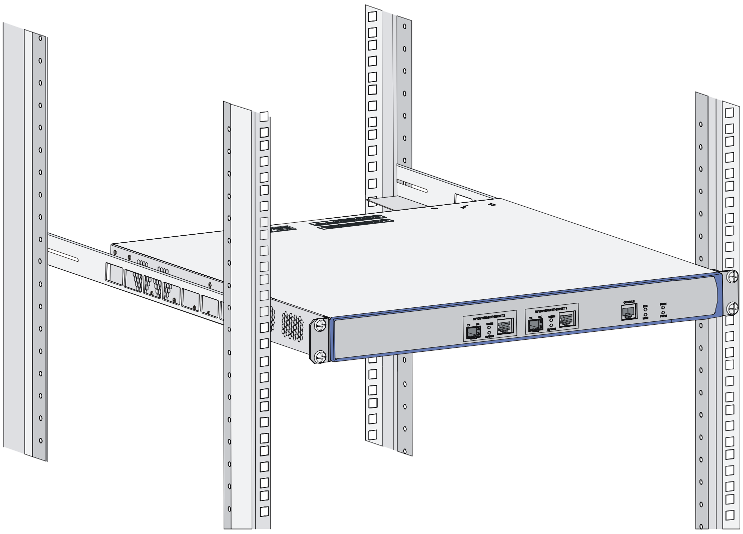
1) Put on the EAD-preventive wrist strap and check that the rack is sturdy and properly earthed.
2) Take out the screws, which are packaged with the front mounting brackets. Attach one end of the front mounting brackets to the access controller with the screws, as shown in Figure 3-4.
3) Install the slide rails to the round-hole rack rails at both sides of the rack using M5 tapping screws, as shown in Figure 3-13. (This figure is just for your reference. The installation may differ on a different rack.)

Figure 3-13 Install slide rails



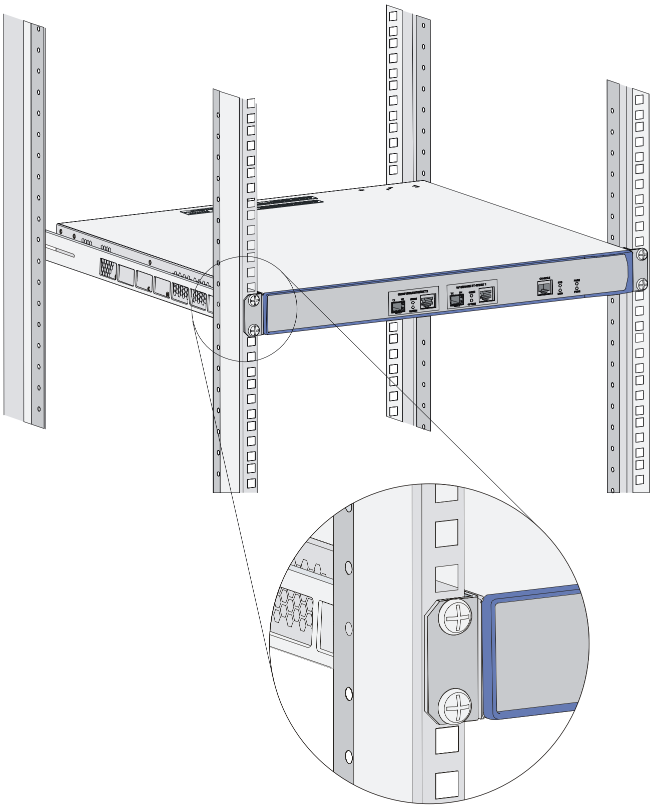
4) Hold the two sides of the access controller with both hands, and then slightly slide the access controller into a proper position of the rack, as shown in Figure 3-14. Make sure that the bottom of the access controller is closely touched with the slide rails.

Figure 3-14 Installation with front mounting brackets and slide rails



5) Use M6 screws and cage nuts to fix the front mounting brackets to the front square-hole rack rails, so that the front mounting brackets and the slide rails can fix the access controller on the rack steadily, as shown in Figure 3-15.

Figure 3-15 Installation with front mounting brackets and slide rails (diagram 2)



Note

Make sure that there is at least 1 U (44.45 mm, 1.75 in.) height away from neighbor devices for heat dissipation.

Installing the Access Controller on a Workbench

In case the standard 19-inch rack is not available, you can install the access controller on a clean workbench. When installing the access controller on a workbench,

- Make sure that the workbench is flat, sturdy and well earthed.
- Keep the environment well ventilated and reserve a clearance of 10 cm (3.9 in.) around the chassis for heat dissipation.
- Place no heavy objects on the access controller.
- Keep at least a vertical distance of 1.5 cm (0.59 in.) between access controllers when they are placed one above the other.

Connecting the Ground Wire

Warning

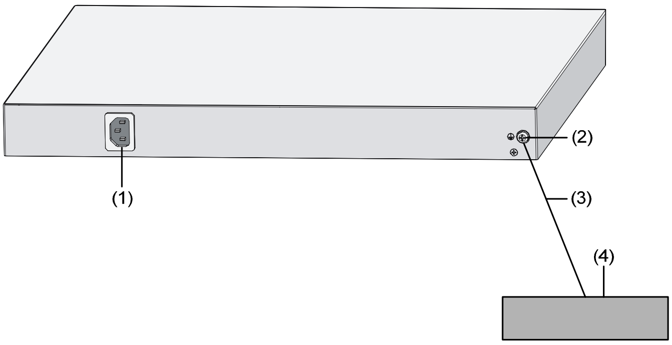
The correct connection of the protection ground (PGND) wire of the access controller is an essential safeguard against lightning strokes and electromagnetic susceptibility (EMS) interference. You must first correctly connect the PGND wire when installing the access controller.

The power input end of the access controller is connected with a noise filter, whose central ground is directly connected to the chassis, forming the chassis ground (also known as PGND). This chassis ground must be securely grounded so that induced and leaked electricity can be safely discharged to the ground, enhancing the anti-EMS capability of the access controller. Ground the access controller as follows:

When a grounding strip is available

1) Remove the grounding terminal screw located at the right back of the chassis, as shown in Figure 3-16.
2) Fasten the wiring terminal of the yellow-green PGND wire of the access controller to the grounding terminal screw you removed in step 1.
3) Put the grounding terminal screw back to the grounding hole on the chassis and fasten it.
4) Fasten the other end of the yellow-green PGND wire to the grounding stud for the access controller on the grounding strip.
5) On the grounding strip, use a nut to fasten the grounding stud that is attached with the PGND wire.

Figure 3-16 Ground the access controller through a grounding strip



(1) AC power socket	(2) Grounding terminal
(3) PGND wire	(4) Grounding strip

Warning

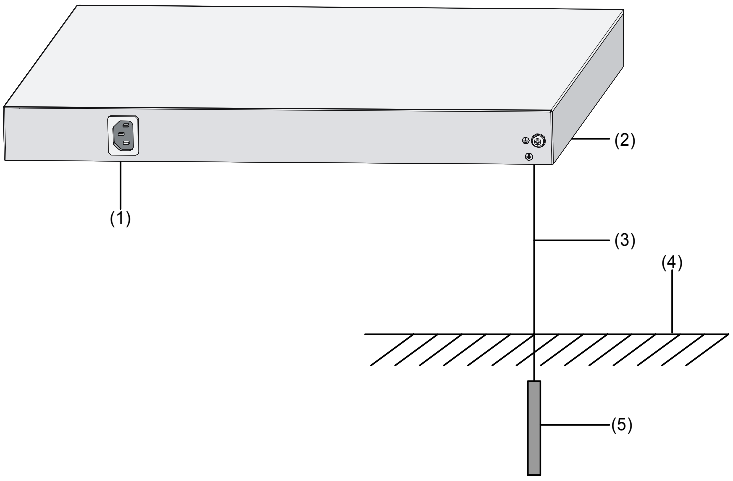
The fire main and lightning rod of a building are not good grounding options. The ground wire of the access controller should be connected to the grounding system in the equipment room.

When a grounding strip is unavailable

1) If earth is available nearby and allows a grounding body to be buried

Hammer an angle steel or steel pipe longer than 0.5 m (1.64 ft) into the earth. In this case, weld the yellow-green PGND wire of the access controller onto the angle steel or steel pipe, and treat the joint for corrosion protection.

Figure 3-17 Ground the access controller through a grounding body



(1) AC power socket	(2) Grounding terminal	(3) PGND wire
(4) Earth	(5) Angle steel	

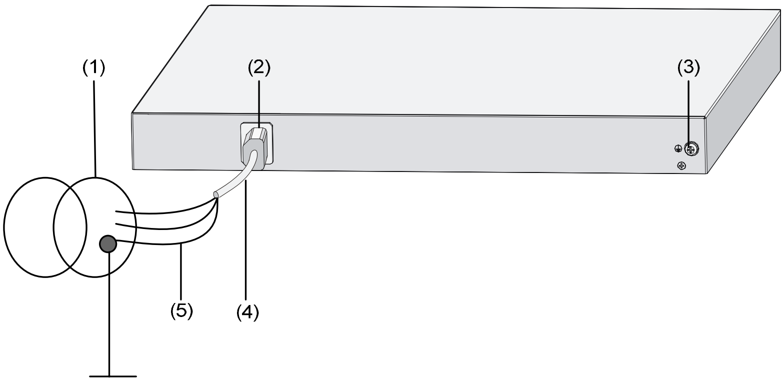
2) If no grounding body is allowed to be buried

Caution

This method applies to the device using AC power input.

If the access controller is AC powered, you can ground the access controller through a PE wire of the AC power supply. In this case, make sure the PE wire is well connected to the ground in the power distribution room or on the AC transformer side.

Figure 3-18 Ground the access controller through an AC PE wire



(1) Power transformer	(2) AC power socket	(3) Grounding terminal
(4) Three-core AC power cord	(5) PE wire	

Connecting the Power Cord

Warning

Make sure that the ground wire is properly connected before powering on the access controller.

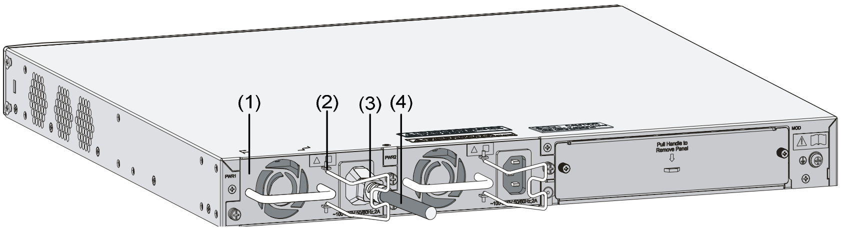
If the device is AC-powered, connect the device with an external AC power system through an AC power cord; if the device is DC-powered, connect the device with an external DC power system through a DC power cord.

Connecting the AC Power Cord

Follow the steps below to connect the AC power cord:

1) Make sure that the PGND of the access controller is correctly connected.
2) Install the AC power cord retainer to the access controller, and turn the retainer left.
3) Connect one end of the power cord to either power socket on the rear panel of the chassis, and the other end to the AC power supply.
4) Turn the power cord retainer right to lock the power cord plug.

Figure 3-19 Install the AC power cord retainer



(1) Rear panel	(2) Power cord retainer slot
(3) AC power cord retainer	(4) AC power cord

5) Check the corresponding PWR LED on the front panel of the access controller. If the LED is solid green, the AC power input is normal.

Note

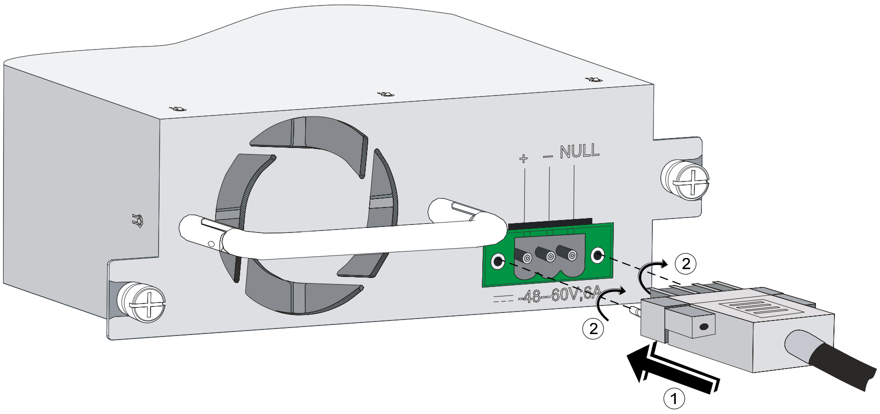
- The AC power cord retainer can prevent the AC power cord from accidentally falling off.
- Whether a power cord retainer is needed depends on the power supply system of the country.

Connecting the DC Power Cord

Follow the steps below to connect the DC power cord:

1) Make sure that the PGND of the access controller is correctly connected.
2) Insert the DC connector with upside on top into the DC power receptacle of the power module, as shown in callout 1 of Figure 3-20. (If the connector is inserted with the upside down, the insertion is not smooth due to the specific design of the receptacle and connector.)
3) Fix the screws on the two sides of the DC connector using a flat-blade screwdriver until the connector is secured to the DC power receptacle, as shown in callout 2 of Figure 3-20.
4) Connect the other end of the power cord to the external DC power supply.
5) Check the corresponding PWR LED on the front panel of the access controller. If the LED is solid green, the DC power input is normal.

Figure 3-20 Connect the DC power cord



Connecting Interface Cables

Connecting the Console Cable

1) Select a terminal for configuration.

The terminal can be a character terminal with a standard RS232 serial port or a PC. A PC is used in this example.

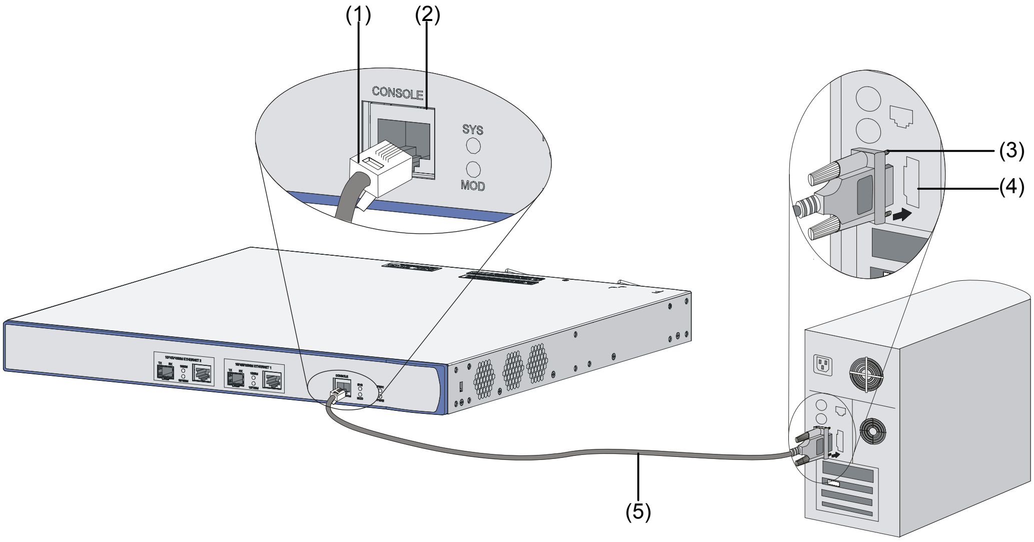
2) Connect the console cable

Power off the access controller, connect the DB-9 female connector of the console cable to the serial interface of the PC, and connect the RJ-45 connector of the console cable to the console port of the access controller.

Warning

Pay attention to the interface mark and plug the connector to the right interface.

Figure 3-21 Connect the console cable



(1) RJ-45 connector	(2) Console port	(3) DB-9 (female) connector
(4) Serial interface of the configuration terminal		(5) Console cable

Note

For a powered-on access controller:

- When connecting a PC to the access controller, you are recommended to first connect the DB-9 connector of the console cable to the PC, and then the RJ-45 connector to the console port of the access controller.
- When disconnecting a PC from the access controller, you are recommended to first disconnect the RJ-45 connector, and then the DB-9 connector.

Connecting the Ethernet Cable

To an the Ethernet electrical interface

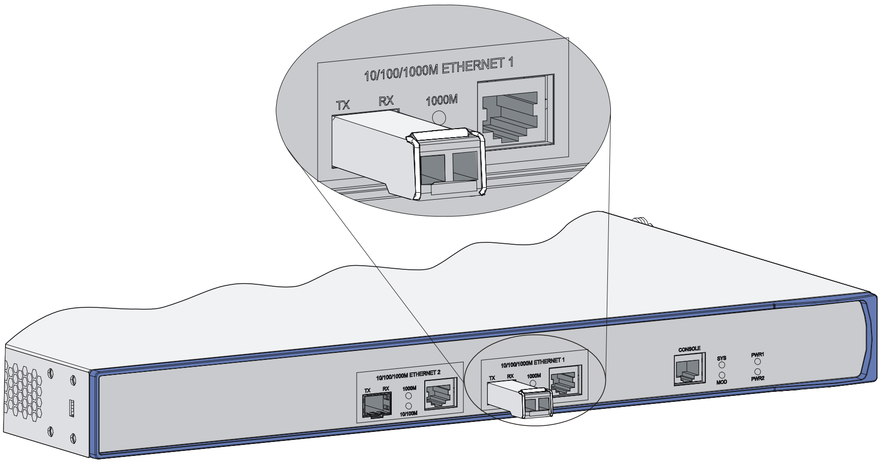
1) Connect one end of the Ethernet cable to an Ethernet electrical interface of the access controller and the other end to an Ethernet interface of the peer device.
2) After powering on the access controller, check the LED of the Ethernet electrical interface. For description on the LED status, refer to section “LEDs” on page 1-4.

To an the Ethernet optical interface

To connect a 1000 Mbps optical interface, follow these steps:

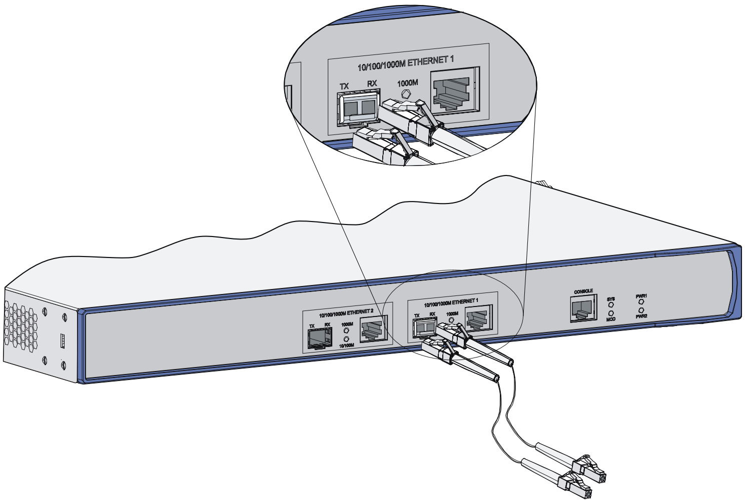
1) Align the end without handle of an SFP module with an SFP interface and insert the SFP module into the SFP interface carefully.

Figure 3-22 Insert an SFP module



2) Distinguish between the Rx and Tx interfaces on the SFP module. Connect the LC connector at one end of an optical fiber to the Rx interface of the access controller and the LC connector at the other end of the optical fiber to the Tx interface of the peer device. Use another fiber to connect the access controller and the peer device in the opposite way.

Figure 3-23 Plug LC connectors



3) Power on the access controller and check the SFP interface LEDs. For description on SFP LED status, refer to section “LEDs” on page 1-4.

⚠ **Warning**

When connecting optical fibers, make sure that:

- The curvature radius of fibers is no less than 10 cm (3.9 in.).
- The Tx and Rx connectors are correctly connected.
- The fiber ends are clean.

Checking the Installation

After installation, make sure that:

- The correct power supply is used.
- The ground wire is properly connected.
- Both the console cable and power cord are correctly connected.
- All interface cables are routed indoors. If there are cables outdoors, check that lightning arresters for the AC power strip and network interfaces have been correctly connected. For how to connect the lightning arresters for the AC power supply and network interfaces, refer to Appendix A and B.

4 Initial Startup

Setting up the Configuration Environment

Connecting a Configuration Terminal to the Access Controller

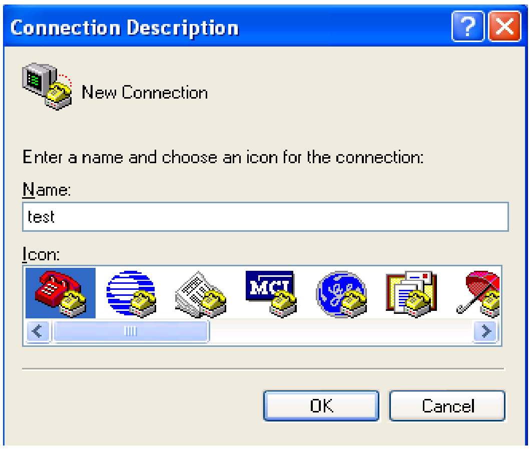
For how to connect a configuration terminal to the access controller, refer to section “Connecting Interface Cables” on page 3-13.

Setting Terminal Parameters

Step1 Start the PC and run the terminal emulation program such as the Terminal of Windows 3.1 or the HyperTerminal of Windows 95/98/NT/2000/XP.

Step2 Select **Start** > **Program** > **Accessories** > **Communications** > **HyperTerminal**. On the **Connection Description** interface, type the name of the new connection and click **OK**, as shown in Figure 4-1.

Figure 4-1 Connection description interface



Connection Description

New Connection

Enter a name and choose an icon for the connection:

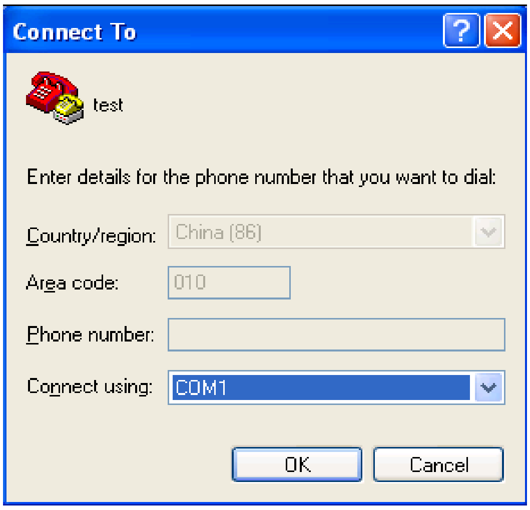
Name:

test

Icon:

Step3 The system displays the **Connect To** interface, as shown in Figure 4-2. From the **Connect using** drop-down list, select the serial interface to be used. (Be sure to select the serial interface to which the console cable is actually connected.)

Figure 4-2 Select the serial interface used for HyperTerminal connection



Connect To

test

Enter details for the phone number that you want to dial:

Country/region: China (86)

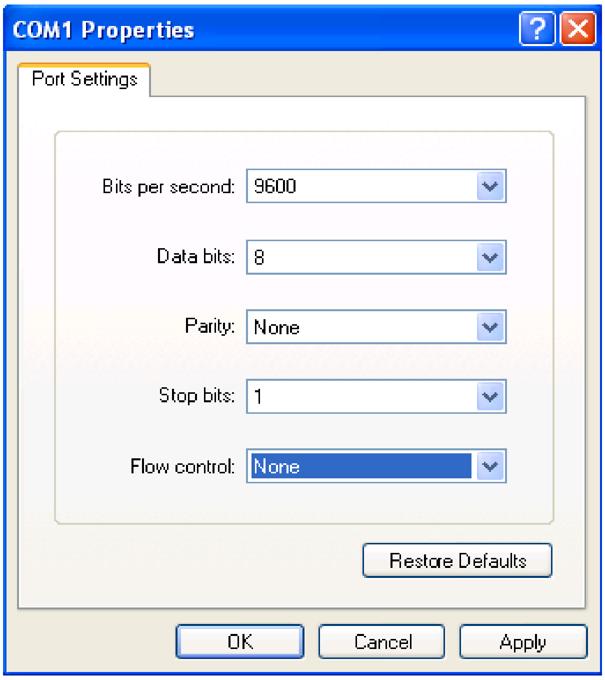
Area code: 010

Phone number:

Connect using: COM1

Step4 Click **OK** and the system displays the following interface, as shown in Figure 4-3. On the interface, set **Bits per second** to **9600**, **Data bits** to **8**, **Parity** to **None**, **Stop bits** to **1**, and **Flow control** to **None**.

Figure 4-3 Set serial port parameters



COM1 Properties

Port Settings

Bits per second: 9600

Data bits: 8

Parity: None

Stop bits: 1

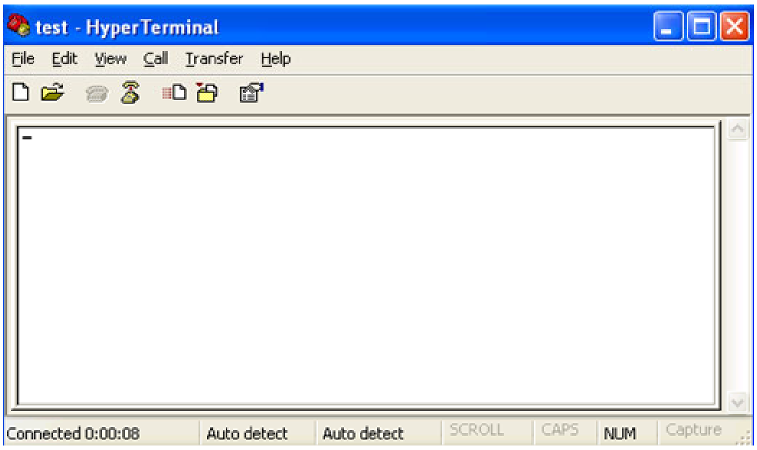
Flow control: None

Note

To use the default settings, click **Restore Defaults**.

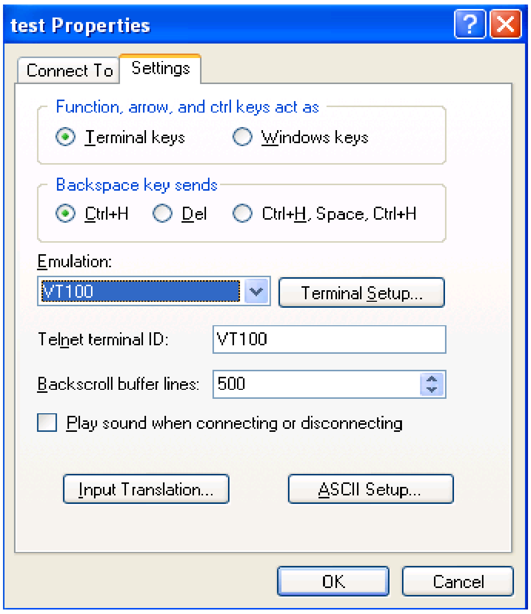
Step5 Click **OK** and the system displays the HyperTerminal interface.

Figure 4-4 HyperTerminal window



Step6 Set HyperTerminal properties. Select **File** > **Properties** > **Settings** in the HyperTerminal to enter the properties setting window, as shown in Figure 4-5. Select **VT100** as the terminal emulation, and click **OK**.

Figure 4-5 Set terminal emulation



Function, arrow, and ctrl keys act as

● Terminal keys ○ Windows keys

Backspace key sends

● Ctrl+H ○ Del ○ Ctrl+H, Space, Ctrl+H

Emulation: VT100

Telnet terminal ID: VT100

Backscroll buffer lines: 500

□ Play sound when connecting or disconnecting

Powering On the Access Controller

Checking Before Power-On

Before powering on the access controller, verify that:

- The power cord and the ground wire are properly connected.
- The power supply voltage is within the range that required by the access controller.
- The console cable is properly connected; the terminal (for example, a PC) used for configuration has been started; the configuration parameters have been set.

Powering on the Access Controller

After the access controller is powered on, the system first initializes memory. After the initiation, the system runs the extended BootWare, and the following information is displayed on the terminal:

```
System is starting...
Booting Normal Extend BootWare....
The Extend BootWare is self-decompressing.................
Done!

**************************************************************************
*                                                                        *
*                 H3C WX5002 BootWare, Version 1.06                      *
*                                                                        *
**************************************************************************
Copyright (c) 2004-2009 Hangzhou H3C Technologies Co., Ltd.

Compiled Date       : Nov  9 2009
CPU Type            : XLR716
CPU L1 Cache        : 32KB
CPU Clock Speed     : 800MHz
Memory Type         : DDR2 SDRAM
Memory Size         : 1024MB
Memory Speed        : 533MHz
BootWare Size       : 512KB
Flash Size          : 4MB
cfa0 Size           : 259MB
CPLD Version        : 008
PCB Version         : Ver.A


BootWare Validating...
Press Ctrl+B to enter extended boot menu...
```

Press **Ctrl+B** to enter the extended boot menu; otherwise, the system will start loading and decompressing the application file.

Note

- You must press **Ctrl+B** in four seconds when "Press Ctrl+B to enter extended boot menu" appears. Otherwise, the system will not enter the extended boot menu but start loading and decompressing the application file.
- You need to reboot the access controller if you want to enter the extended boot menu after the application file is decompressed.
- The extended BootWare menu is referred to as the BootWare main menu in this manual unless otherwise specified.

```
Starting to get the main application file--cfa0:/main.bin!..............................
.........................................
The main application file is self-decompressing.........................................
........................................................................................
........................................................................................
........................................................................................
.................................................
Done!
System is starting...
Startup configuration file does not exist.
User interface con0 is available.

Press ENTER to get started.
```

Press **Enter**. The following prompt is displayed:

```
<H3C>
```

The prompt indicates that the system has entered user view and you can configure the access controller now.

5 Software Maintenance

Overview

Files Managed by the Access Controller

The WX5002V2 manages the following three types of files:

- BootWare program file
- Application file
- Configuration file

BootWare Program File

The BootWare program file is used to boot the applications when the access controller is started up. The complete BootWare program file consists of two segments: basic and extended.

- Basic BootWare implements the basic system initialization.
- Extended BootWare provides abundant human-computer interaction (HCI) functions. It is used for interface initialization for upgrading applications and booting the system.
- The full BootWare refers to the combination of the two segments. After the basic BootWare is booted, you can load or upgrade the extended BootWare on the menu of the basic BootWare.

Warning

Do not power off or restart the access controller during BootWare upgrade process; otherwise, the BootWare program may be damaged and the access controller may fail to operate normally.

Application Files

The WX5002V2 supports the Dual Image function. By default, three application files are defined for system boot:

- Main application file (main file)
- Backup application file (backup file)
- Secure application file (secure file)

These files are stored on the built-in CF card, with the extension **.bin**.

Typically, the default application file is written into the built-in CF card of an access controller before it is delivered.

If you have loaded the three application files to the CF card, the system uses these three files to boot the access controller in the sequence of main.bin, backup.bin, and secure.bin. For how to set the application file types, refer to section “Maintaining Application and Configuration Files” on page 5-22.

The default names and types of the application files and their loading priorities for booting are as follows.

- Main application file. The default name is main.bin, and the file type is M. It is the default application file used for booting.
- Backup application file. The default name is backup.bin, and the file type is B. When the boot using the main application file fails, the system boots using the backup application file.
- Secure application file. The default name is secure.bin, and the file type is S. When boot using the backup application file fails, the system tries the secure application file. If the boot using the secure application file fails, the system prompts a boot failure.

Note that:

- The application files for system boot can be type M, B and S, but not type N/A.
- After the application program is loaded, you can rename the application files through the command line interface (CLI) or change the file type (M, B or N/A) through the BootWare menu or the CLI. However, you cannot change the file type of the S-type application file.
- As the secure application file is the last resort for system boot, you cannot change the type of the secure application file, or change other types of files to the secure application file. You can only download it by selecting the “Update Secure Application File” option on the BootWare menu.
- Only one file of the same type (M, B, or S) can exist on the CF card. For instance, if an application file of type M+B exists on the CF card, another file of type M or B cannot exist. If the type of another file is changed to B, the existing type M+B file changes to a file of type M.

Configuration Files

Configuration files store configuration information of the access controller, with the extension of **.cfg**. Typically, the access controller has no configuration file when it is delivered.

The configuration files generated by users are saved in the built-in CF card, with the default name **startup.cfg**.

Warning

- The length of a configuration file name must no exceed 64 characters (including the drive name and the string terminator). For example, if the drive name is **cfa0:/**, the maximum length of a file name is [64–1–6] = 57 characters.
- If the length of a file name exceeds 57 characters, error will occur in file operations on that file. Generally, it is recommended to keep the file name within 16 characters.
- There is a limitation on the length of file name that can be displayed in BootWare. If a file name is shorter than 30 characters, all the characters of the file name can be displayed; if a file name has or exceeds 30 characters, only the first 26 characters of the file name can be displayed, followed by a tilde (~) and a serial number. The serial number identifies position in sequence of the file. For example, if three files, file A, file B and file C, have a file name longer than 30 characters, the name of file A will appear as the first 26 characters plus ~001, that of file B will appear as the first 26 characters plus ~002, and that of file C will appear as the first 26 characters plus ~003.

Approaches for Software Maintenance

You can maintain the access controller in one of the following three ways:

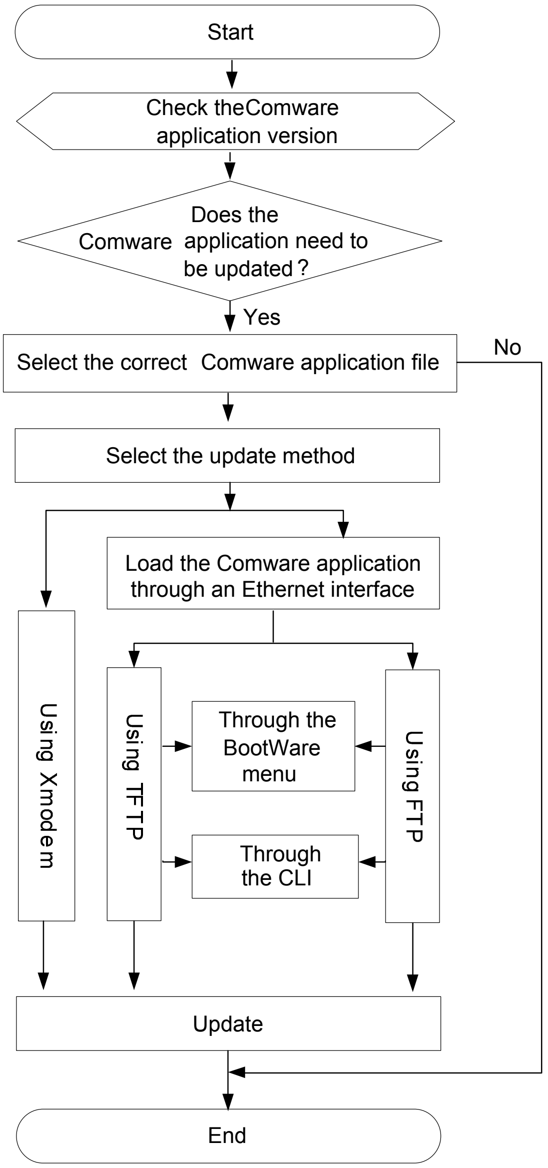
- Upgrade BootWare and application files using the XMODEM protocol through a serial interface.
- Upgrade application files using TFTP/FTP through an Ethernet interface on the BootWare menu.
- Upload/download application files and configuration files using TFTP/FTP through command lines.

Note

- The BootWare program is upgraded together with the host software program version. That is, the system automatically upgrades the BootWare program when you upgrade the host software program.
- Before upgrading the software of your access controller, check the current BootWare version and application program version to make sure that the correct file is used for the upgrade. For the association between the host software version and the BootWare version, refer to the version compatibility matrix in *Release Notes*.

BootWare and Application File Upgrade Flow

Figure 5-1 BootWare and application file upgrade flow



Start
Check theComware application version
Does the Comware application need to be updated ?
Yes
No
Select the correct Comware application file
Select the update method
Load the Comware application through an Ethernet interface
Using Xmodem
Using TFTP
Through the BootWare menu
Through the CLI
Using FTP
Update
End

BootWare Menus

BootWare Main Menu

When a device is powered on or restated, the terminal first displays the following information:

```
System is starting...
```

Then, the system displays the following:

```
Booting Normal Extend BootWare....
The Extend BootWare is self-decompressing.................
Done!
****************************************************************************
*                                                                          *
*                  H3C WX5002 BootWare, Version 1.06                       *
*                                                                          *
```

```
****************************************************************************
Copyright (c) 2004-2009 Hangzhou H3C Technologies Co., Ltd.

Compiled Date       : Nov  9 2009
CPU Type            : XLR716
CPU L1 Cache        : 32KB
CPU Clock Speed     : 800MHz
Memory Type         : DDR2 SDRAM
Memory Size         : 1024MB
Memory Speed        : 533MHz
BootWare Size       : 512KB
Flash Size          : 4MB
cfa0 Size           : 259MB
CPLD Version        : 008
PCB Version         : Ver.A

BootWare Validating...
Press Ctrl+B to enter extended boot menu...
```

Note

The extended boot menu is referred to as the BootWare main menu in this manual unless otherwise specified.

Press **Ctrl + B** when the system prompts “Press Ctrl+B to enter extended boot menu”. Then, the system prompts you to enter the BootWare password:

```
Please input BootWare password:
```

You have three chances to enter the BootWare password (the initial password is null). If you fail to enter the correct password three times in a row, the system will be halted and you can only restart the system. After you provide the correct password, the system enters the BootWare main menu:

```
Note: The current operating device is cfa0
Enter < Storage Device Operation > to select device.

=============================<EXTEND-BOOTWARE MENU>=============================
|<1> Boot System                                                               |
|<2> Enter Serial SubMenu                                                      |
|<3> Enter Ethernet SubMenu                                                    |
|<4> File Control                                                              |
|<5> Modify BootWare Password                                                  |
|<6> Skip Current System Configuration                                         |
|<7> BootWare Operation Menu                                                   |
|<8> Clear Super Password                                                      |
|<9> Storage Device Operation                                                  |
|<0> Reboot                                                                    |
================================================================================
Enter your choice(0-9):
```

BootWare Submenus

Serial submenu

You can upgrade application files, change the serial interface baud rate, and so on through the serial submenu.

Enter **2** on the BootWare main menu to enter the serial submenu. The system displays:

```
=============================<Enter Serial SubMenu>=============================
|Note:the operating device is cfa0                                             |
|<1> Download Application Program To SDRAM And Run                             |
|<2> Update Main Application File                                              |
|<3> Update Backup Application File                                            |
|<4> Update Secure Application File                                            |
|<5> Modify Serial Interface Parameter                                         |
|<0> Exit To Main Menu                                                         |
================================================================================
Enter your choice(0-5):
```

Ethernet submenu

Enter **3** on the BootWare main menu to enter the Ethernet submenu. The system displays:

```
============================<Enter Ethernet SubMenu>============================
|Note:the operating device is cfa0                                             |
|<1> Download Application Program To SDRAM And Run                             |
|<2> Update Main Application File                                              |
|<3> Update Backup Application File                                            |
|<4> Update Secure Application File                                            |
|<5> Modify Ethernet Parameter                                                 |
|<0> Exit To Main Menu                                                         |
|<Ensure The Parameter Be Modified Before Downloading!>                        |
================================================================================
Enter your choice(0-5):
```

Items in this submenu are described in the following table.

File control submenu

Enter **4** on the BootWare main menu to enter the file control submenu. The following information is displayed:

```
=================================<File CONTROL>=================================
|Note:the operating device is cfa0                                             |
|<1> Display All File(s)                                                       |
|<2> Set Application File type                                                 |
|<3> Delete File                                                               |
|<0> Exit To Main Menu                                                         |
================================================================================
Enter your choice(0-3):
```

BootWare operation submenu

Enter **7** on the BootWare main menu to enter the BootWare operation submenu. The system displays:

```
===========================<BootWare Operation Menu>============================
|Note:the operating device is cfa0                                             |
|<1> Backup Full BootWare                                                      |
|<2> Restore Full BootWare                                                     |
|<3> Update BootWare By Serial                                                 |
|<4> Update BootWare By Ethernet                                               |
|<0> Exit To Main Menu                                                         |
================================================================================
Enter your choice(0-4):
```

Storage device operation submenu

Enter **9** on the BootWare main menu to enter the storage device operation submenu. The system displays:

```
================================<DEVICE CONTROL>================================
|<1> Display All Available Nonvolatile Storage Device(s)                       |
|<2> Set The Operating Device                                                  |
|<3> Set The Default Boot Device                                               |
|<0> Exit To Main Menu                                                         |
================================================================================
Enter your choice(0-3):
```

Upgrading the BootWare Through a Ethernet/Serial Interface

To upgrade the BootWare through a serial interface, use the XMODEM protocol.

XMODEM is a file transfer protocol that is widely used due to its simplicity and good performance. XMODEM transfers files through serial interfaces. It supports two types of data packets (128 bytes and 1 KB), two check methods (checksum and CRC), and error packet retransmission mechanism (generally the maximum number of retransmission attempts is ten).

The XMODEM transmission procedure is completed by the cooperation of a receiving program and a sending program. The receiving program sends a negotiation character to negotiate a packet check method. After the negotiation, the sending program starts to send data packets. Upon receiving a complete packet, the receiving program checks the packet using the agreed check method.

- If the check succeeds, the receiving program sends an acknowledgement character and the sending program proceeds to send another packet.
- If the check fails, the receiving program sends a negative acknowledgement character and then the sending program retransmits the packet.

Note

- The BootWare program is upgraded together with the Comware application. When you upgrade the Comware application program, the system automatically checks whether the current BootWare version is compliant with that included the updated Comware application and upgrades the current BootWare if needed.
- Before upgrading the software of your access controller, check the current BootWare version and Comware application version to make sure that the correct file is used for the upgrade. For the association between the Comware application version and the BootWare version, refer to the version compatibility matrix in *Release Notes*.

Modifying Serial Interface Parameters

Sometimes, we need a high serial interface baud rate to save the update time, or a low baud rate to ensure transmission reliability. This section introduces how to adjust the serial interface baud rate.

Enter the BootWare main menu and enter **2** to go to the serial submenu, and then enter **5** on the submenu to modify the baud rate. The system displays the following:

```
=================================<BAUDRATE SET>=============================
|Note:'*'indicates the current baudrate                                    |
|     Change The HyperTerminal's Baudrate Accordingly                      |
|---------------------------<Baudrate Available>------------------------  |
|<1> 9600(Default)*                                                        |
|<2> 19200                                                                 |
|<3> 38400                                                                 |
|<4> 57600                                                                 |
|<5> 115200                                                                |
|<0> Exit                                                                  |
============================================================================
Enter your choice(0-5):
```

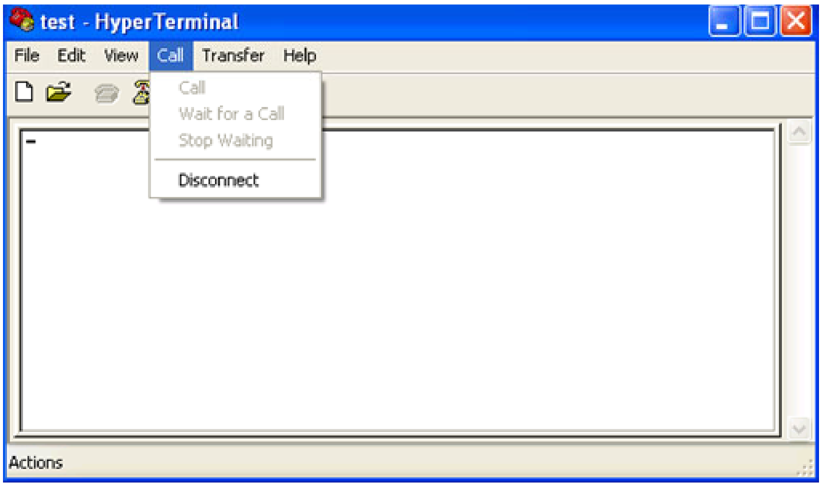
Select a proper baud rate. For example, enter **5** for a baud rate of 115200 bps and the system displays the following information:

```
Baudrate has been changed to 115200 bps.
Please change the terminal's baudrate to 115200 bps, press ENTER when ready.
```

At this time, the serial interface baud rate of the access controller is modified to 115200 bps, while that of the terminal is still 9600 bps. The access controller and the terminal cannot communicate with each other. Change the baud rate to 115200 bps on the terminal.

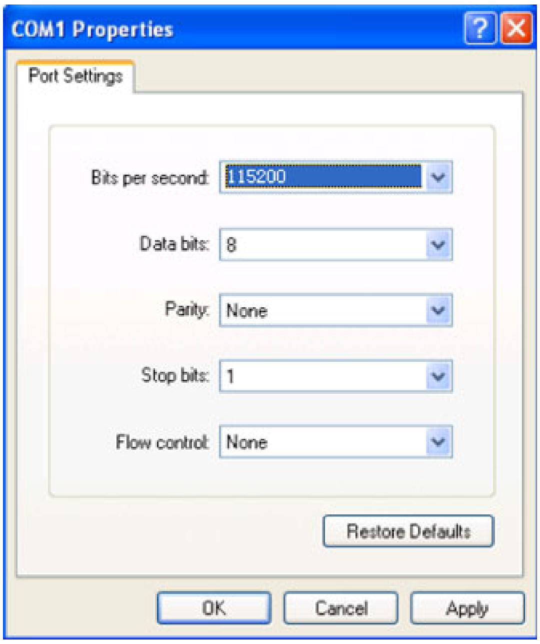
Perform the following operations on the terminal:

Figure 5-2 Disconnect the terminal



Select **File** > **Properties**, In the **Properties** dialog box, click **Configure…** and then Set the **Bits per second** to 115200.

Figure 5-3 Modify the baud rate



Bits per second: 115200

Data bits: 8

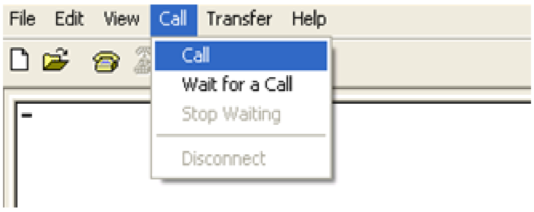
Parity: None

Stop bits: 1

Flow control: None

Select **Call** > **Call** to establish a new connection.

Figure 5-4 Re-establish a call connection



Then, press the **Enter** key, and the system will prompt the current baud rate.

```
The current baudrate is 115200 bps

==============================<BAUDRATE SET>=============================
|Note:'*'indicates the current baudrate                                  |
|     Change The HyperTerminal's Baudrate Accordingly                    |
|---------------------------<Baudrate Available>-------------------------|
|<1> 9600(Default)                                                       |
|<2> 19200                                                               |
|<3> 38400                                                               |
|<4> 57600                                                               |
|<5> 115200*                                                             |
|<0> Exit                                                                |
==========================================================================
Enter your choice(0-5):
```

Note

After downloading files with a changed baud rate, timely change the baud rate back to 9,600 bps in HyperTerminal to ensure the normal display on the console screen when the system boots or reboots.

Upgrading the BootWare Through an Ethernet Interface

Enter the BootWare main menu (refer to section “BootWare Main Menu” on page 5-4). On the BootWare main menu, enter **7**. The system will enter the BootWare operation submenu, where you can perform all BootWare operations. For details about this menu, refer to section “BootWare operation submenu” on page 5-7.

Enter **4** on the BootWare operation submenu to enter the BootWare operation Ethernet submenu:

```
=====================<BOOTWARE OPERATION ETHERNET SUB-MENU>=====================
|<1> Update Full BootWare                                                       |
|<2> Update Extend BootWare                                                     |
|<3> Update Basic BootWare                                                      |
|<4> Modify Ethernet Parameter                                                  |
|<0> Exit To Main Menu                                                          |
================================================================================
Enter your choice(0-4):
```

Enter **4** on the BootWare operation Ethernet submenu. The system prompts you to modify the network parameters.

```
============================<ETHERNET PARAMETER SET>============================
|Note:       '.' = Clear field.                                                 |
|            '-' = Go to previous field.                                        |
|          Ctrl+D = Quit.                                                       |
================================================================================
Protocol (FTP or TFTP) :tftp
```

```
Load File Name         :host
                       :main.bin
Target File Name       :target
                       :main.bin
Server IP Address      :192.168.0.1
Local IP Address       :192.168.0.10
Gateway IP Address     :0.0.0.0
```

Note

The load file name and the target file name must not exceed 50 bytes.

After modification of the parameters, the system display returns to the BootWare operation Ethernet submenu.

```
=====================<BOOTWARE OPERATION ETHERNET SUB-MENU>=====================
|<1> Update Full BootWare                                                      |
|<2> Update Extend BootWare                                                    |
|<3> Update Basic BootWare                                                     |
|<4> Modify Ethernet Parameter                                                 |
|<0> Exit To Main Menu                                                         |
================================================================================
Enter your choice(0-4):
```

Enter **1** on the BootWare operation Ethernet submenu.

The system displays:

```
Loading...................................................................
..........................................................................
.........................................................Done!
20710792 bytes downloaded!
Updating Basic BootWare? [Y/N]Y
Updating Basic BootWare................Done!
Updating Extend BootWare? [Y/N]Y
Updating Extend BootWare..............Done!
```

After download of the BootWare program file, the system display returns to the BootWare operation Ethernet submenu.

```
===================<BOOTWARE OPERATION ETHERNET SUB-MENU>===================
|<1> Update Full BootWare                                                  |
|<2> Update Extend BootWare                                                |
|<3> Update Basic BootWare                                                 |
|<4> Modify Ethernet Parameter                                             |
|<0> Exit To Main Menu                                                     |
============================================================================
Enter your choice(0-4):
```

Enter **0** on this menu to return to the BootWare operation submenu:

```
=========================<BootWare Operation Menu>==========================
|Note:the operating device is cfa0                                         |
|<1> Backup Full BootWare                                                  |
|<2> Restore Full BootWare                                                 |
|<3> Update BootWare By Serial                                             |
|<4> Update BootWare By Ethernet                                           |
|<0> Exit To Main Menu                                                     |
===========================================================================
Enter your choice(0-4):
```

Enter **0** on the BootWare operation submenu to return to the BootWare main menu:

```
===========================<EXTEND-BOOTWARE MENU>===========================
|<1> Boot System                                                           |
|<2> Enter Serial SubMenu                                                  |
|<3> Enter Ethernet SubMenu                                                |
|<4> File Control                                                          |
|<5> Modify BootWare Password                                              |
|<6> Skip Current System Configuration                                     |
|<7> BootWare Operation Menu                                               |
|<8> Clear Super Password                                                  |
|<9> Storage Device Operation                                              |
|<0> Reboot                                                                |
============================================================================
Enter your choice(0-9): 0
```

Enter **0** on the BootWare main menu to reboot the access controller.

Upgrading the BootWare Through a Serial Interface

Enter the BootWare main menu (refer to section “BootWare Main Menu” on page 5-4). On the BootWare main menu, enter **7**. The system will enter the BootWare operation submenu, where you can perform all BootWare operations. For detail description on this submenu, refer to section “BootWare operation submenu” on page 5-7.

Enter **3** on the BootWare operation submenu to enter the BootWare operation serial submenu:

```
======================<BOOTWARE OPERATION SERIAL SUB-MENU>======================
|<1> Update Full BootWare                                                      |
|<2> Update Extend BootWare                                                    |
|<3> Update Basic BootWare                                                     |
|<4> Modify Serial Interface Parameter                                         |
|<0> Exit To Main Menu                                                         |
================================================================================
Enter your choice(0-4):
```

Enter **4** on the BootWare operation serial submenu. The system prompts you to modify the baud rate:

```
=================================<BAUDRATE SET>=================================
|Note:'*'indicates the current baudrate                                        |
|     Change The HyperTerminal's Baudrate Accordingly                          |
|-----------------------------<Baudrate Available>-----------------------------|
|<1> 9600(Default)*                                                            |
|<2> 19200                                                                     |
|<3> 38400                                                                     |
|<4> 57600                                                                     |
|<5> 115200                                                                    |
|<0> Exit                                                                      |
================================================================================
Enter your choice(0-5):
```

Change the communication baud rate. For the detailed modification procedure, refer to section “Modifying Serial Interface Parameters” on page 5-8. After the modification, the system displays the following information:

```
Baudrate has been changed to 115200 bps.
Please change the terminal's baudrate to 115200 bps, press ENTER when ready.
The current baudrate is 115200 bps
=================================<BAUDRATE SET>=============================
|Note:'*'indicates the current baudrate                                     |
|     Change The HyperTerminal's Baudrate Accordingly                       |
|---------------------------<Baudrate Available>---------------------------|
|<1> 9600(Default)                                                          |
|<2> 19200                                                                  |
|<3> 38400                                                                  |
|<4> 57600                                                                  |
|<5> 115200*                                                                |
|<0> Exit                                                                   |
============================================================================
Enter your choice(0-5):
```

Enter **0** to return to the BootWare operation serial submenu.

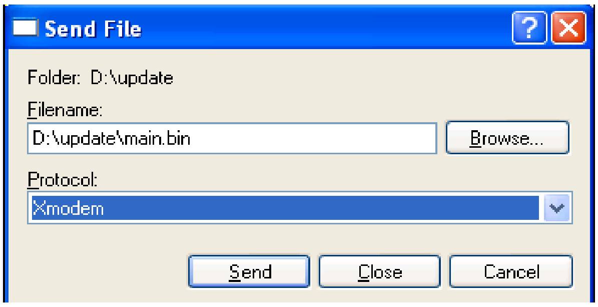
```
======================<BOOTWARE OPERATION SERIAL SUB-MENU>======================
|<1> Update Full BootWare                                                      |
|<2> Update Extend BootWare                                                    |
|<3> Update Basic BootWare                                                     |
|<4> Modify Serial Interface Parameter                                         |
|<0> Exit To Main Menu                                                         |
================================================================================
Enter your choice(0-4):
```

Enter **1** on the BootWare operation serial submenu. The system displays the following information:

```
Please Start To Transfer File, Press <Ctrl+C> To Exit.
Waiting ...CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
```

Select **Transfer** > **Send file…** on the terminal window. The following dialog box appears:

Figure 5-5 Send File dialog box



Send File

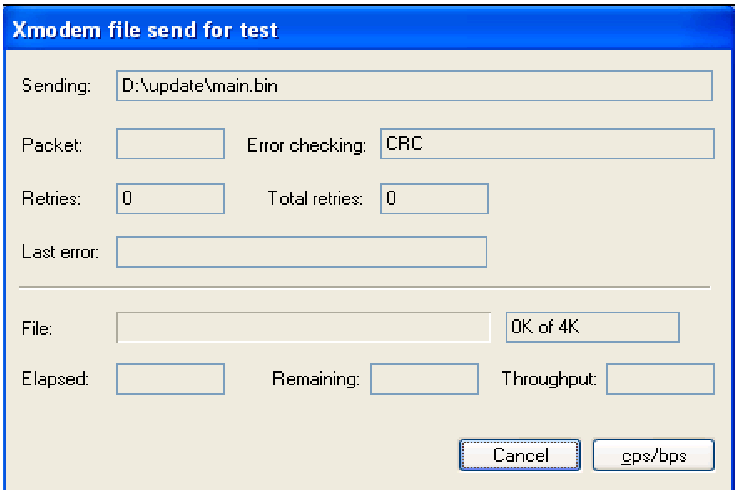
Folder: D:\update

Filename: D:\update\main.bin

Protocol: Xmodem

Click **Browse…** to select the application file to be downloaded, and select **Xmodem** from the **Protocol** drop-down list. Then click **Send**. The following dialog box appears:

Figure 5-6 Sending file dialog box



Xmodem file send for test

Sending: D:\update\main.bin

Packet:

Error checking: CRC

Retries: 0

Total retries: 0

Last error:

File: 0K of 4K

Elapsed:

Remaining:

Throughput:

Upon successful download, the system displays the following information:

```
Download successfully!
10323456 bytes downloaded!
Updating Basic BootWare? [Y/N]Y
Updating Basic BootWare................Done!
Updating Extend BootWare? [Y/N]Y
Updating Extend BootWare..........Done!
```

Change the baud rate on the configuration terminal from 115200 bps to 9600 bps, and then reboot the access controller.

Note

- The actual file name, size and path may differ from what are shown in the figure above. Before upgrading the software of your access controller, check the current BootWare version and the application program version to ensure that the correct file is used for the upgrade.
- After you download files with a changed baud rate, timely change the baud rate in the HyperTerminal to 9600 bps to ensure the normal display on the console screen when the system boots or reboots.

Upgrading Applications Through a Serial Interface on the BootWare Menu

The application file upgrade through a serial port is implemented on the serial submenu. Enter **2** on the BootWare main menu to enter the serial submenu. For detailed description on this submenu, refer to section "Serial submenu" on page 5-6.

The following example shows how to upgrade the main application file.

To improve the upgrading speed, you can modify the serial interface baud rate before upgrading the file. (refer to section "Modifying Serial Interface Parameters" on page 5-8). Enter **2** on the serial submenu. The system displays the following information:

```
Please Start To Transfer File, Press <Ctrl+C> To Exit.
Waiting ...CCCCCCCCCC
```

Select and send the application file. The procedure for upgrading an application file through a serial interface is the same as upgrading the BootWare. For details, refer to section "Upgrading the BootWare Through a Ethernet/Serial Interface" on page 5-7.

Note

The size of an application program is typically over 10 MB. Even at the maximum baud rate of 115200 bps, the upgrade will also take a long time. Therefore, it is not recommended to upgrade application files through a serial interface but through an Ethernet interface.

Upgrading Applications Through an Ethernet Interface on the BootWare Menu

Enter **3** on the BootWare main menu to enter the Ethernet submenu. For details, refer to section "Ethernet submenu" on page 5-6.

Configuring Ethernet Interface Parameters

Before upgrading an application program through an Ethernet interface, you need to configure the Ethernet interface of the access controller, as follows:

Enter **3** on the BootWare main menu to enter the Ethernet submenu. Then, enter **5** on the submenu to enter the Ethernet interface configuration interface:

```
============================<ETHERNET PARAMETER SET>============================
|Note:       '.' = Clear field.                                                |
|            '-' = Go to previous field.                                       |
|          Ctrl+D = Quit.                                                      |
================================================================================
Protocol (FTP or TFTP) :tftp
Load File Name         :host
                       :main.bin
Target File Name       :target
                       :main.bin
Server IP Address      :192.168.0.250
Server IP Address      :192.168.0.1
Local IP Address       :192.168.0.10
Gateway IP Address     :0.0.0.0
```

Note

- When configuring a parameter, you can enter a new value directly, or press **Enter** to accept the default value, which is after the colon. Type a dot (.) to clear the input, a hyphen (-) to return to the previous parameter field, and a combination of **^D** (namely, **Ctrl+D**) to exit the parameter configuration interface.
- The WX5002V2 supports only GigabitEthernet 1/0/1 for application upgrade.

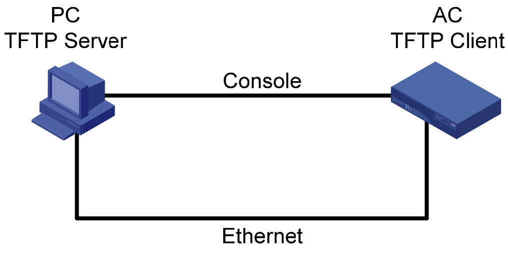
Upgrading Applications Through an Ethernet Interface

The Trivial File Transfer Protocol (TFTP) is a TCP/IP protocol used for file transfer between client and server. It provides a simple and low-cost file transfer service. TFTP provides unreliable data transfer over UDP and does not provide any access authorization and authentication mechanism. It employs the timeout retransmission method to implement best-effort delivery of data. Compared with FTP, TFTP has a much smaller software size.

Follow these steps to upgrade an application file through the management Ethernet interface (10/100 Base-TX):

Step1 Set up a software upgrade environment.

Figure 5-7 Set up a software upgrade environment



Connect GigabitEthernet 1/0/1 to a PC with an Ethernet cable. Run TFTP Server on the PC, and set the path of the application file to be downloaded.

Note

The TFTP Server software is not provided with the WX5002V2. You need to prepare it yourself.

Step2 Modify the Ethernet interface parameters. For details, refer to section “Configuring Ethernet Interface Parameters” on page 5-15.

Step3 Enter **3** on the BootWare main menu to enter the Ethernet submenu. The following example shows how to upgrade the main application file. Enter **2** on the Ethernet submenu. The following information appears:

```
Loading.....................................................................
............................................................................
............................Done!
10323352 bytes downloaded!
Updating File cfa0:/main.bin
The file is exist,will you overwrite it?
[Y/N]Y.............................................
............................................................................
............................................................................
............................................................................
............................................................................
............................................................................
............................................................ ... .....................
....Done!
```

Step4 Enter **0** to return to the BootWare main menu. Enter **1** on the BootWare main menu to reboot the access controller.

Caution

- If the downloaded file has the same name with an existing file on the CF card, the system prompts **The file is exist, will you overwrite it? [Y/N]**. If you choose **Y**, the existing file will be overwritten.
- Make sure that sufficient space is available on the CF card. In case of insufficient space, the system will give a prompt.
- The new application file directly replaces the existing file of the same type. In this example, the downloaded file main.bin replaces the existing application file of type M and becomes the only main application file.
- For details about the application file types, refer to section “Application Files” on page 5-1.

Maintaining the Application and Configuration Files Through the CLI

After the access controller is normally started, you can back up and restore the application and configuration files through the CLI.

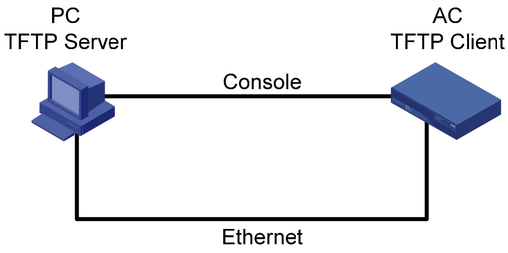
Maintaining the Access Controller Through TFTP

Use the WX5002V2 as a TFTP client and a file server as the TFTP server. You can use commands on the configuration terminal, which can be the same file server, to upload the application and configuration files from the access controller to the file server or download the files from the file server to the access controller.

Setting up a configuration environment

Set up a network environment (for the procedure, refer to section "Upgrading Applications Through an Ethernet Interface" on page 5-16). Run the TFTP Server on the file server and set the file path.

Figure 5-8 Network diagram for software maintenance through the CLI



Configure the IP addresses for both sides, which must be on the same subnet. For example, set the IP address of the TFTP server to 192.168.0.1, and that of the access controller's management interface to 192.168.0.2. Then use **ping** to verify the network connectivity.

Backing up and restoring application and configuration files

After setting up the environment, perform the following operations on the PC:

View the files in the current file system with the **dir** command.

```
<H3C>dir
Directory of cfa0:/

   0     -rw-  10295948  Sep 11 2053 02:17:14   main.bin
   1     -rw-        33  Aug 20 2008 09:58:44   system.xml
   2     -rw-       802  Aug 20 2008 09:58:44   startup.cfg
   3     -rw-     76960  Aug 15 2008 15:58:02   vmetest.vme

252434 KB total (243028 KB free)

File system type of cfa0: FAT32

<H3C>
```

For example, to back up the file **startup.cfg** on the access controller and save it as **config.bak** on the TFTP server, use the following command:

```
<H3C>tftp 192.168.0.1 put startup.cfg config.bak

  File will be transferred in binary mode
  Sending file to remote TFTP server. Please wait... \
  TFTP:      802 bytes sent in 10 second(s).
  File uploaded successfully.
```

To download **config.cfg** from the TFTP server to the access controller, use the following command:

```
<H3C>tftp 192.168.0.1 get config.bak startup.cfg

  File will be transferred in binary mode
  Downloading file from remote TFTP server, please wait...
  TFTP:      842 bytes received in 1 second(s)
  File downloaded successfully.
```

If a file with the same name already exists on the access controller, the system will ask you whether to replace the existing file. Enter **Y** to replace it, or **N** to abort.

Caution

- When you back up a file to the server and if a file with the same name already exists on the server, the existing file will be overwritten without a prompt.
- The above-mentioned operations are performed in user view.
- The backup configuration file can be modified by using a text editor. To update the system configuration of the access controller, you can modify the backup configuration file on the file server, and then download the modified configuration file to the access controller. Your update takes effect on the access controller after it is restarted. Likewise, you can download a new application file to the access controller to overwrite the existing main application file to update the application.

Maintaining the Access Controller Through FTP

The access controller as the FTP server

The File Transfer Protocol (FTP) is an application layer protocol in the TCP/IP suite. It is mainly used for file transfer between remote hosts. FTP provides a reliable, connection-oriented data transfer service over TCP.

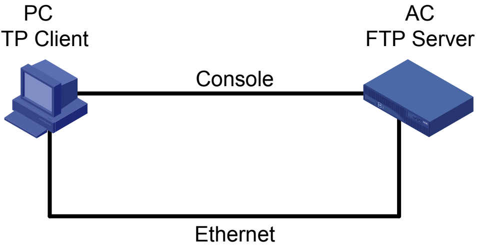
The access controller can serve as the FTP server. In this case, you can use your PC as an FTP client to log in to the access controller for file operations.

Before using FTP, you need to install the FTP client application on your PC. The FTP client software is not provided with the access controller. You must prepare it yourself. In the following example, the FTP client program is the one that comes with Microsoft Windows XP.

Follow these steps to maintain the software of your access controller through FTP with the access controller as the FTP server:

1) Set up a network environment as follows:

Figure 5-9 Set up a software maintenance environment (the access controller as the FTP server)



Configure the IP addresses for both sides, which must be on the same subnet. For example, set the IP address of the FTP client (PC) to 192.168.0.1, while that of the access controller's Ethernet interface to 192.168.0.2. Then use the **ping** command to verify the network connectivity.

2) Enable the FTP service.

Configure FTP server authentication and authorization and enable FTP. The FTP server supports multi-client access. When a remote FTP client sends a request to the FTP server, the FTP server executes an action accordingly and returns the execution result to the client. Use the following command to enable the FTP service.

```
[H3C]ftp server enable
```

Add an authorized FTP username and password:

```
[H3C]local-user guest                                 //Create user account guest.
[H3C-luser-guest]service-type ftp                     //Set user type to FTP.
[H3C-luser-guest]password simple 123456               //Set password to 123456 for the user.
[H3C-luser-guest]authorization-attribute level 3      //Set the user level to 3.
```

3) Maintain the access controller.

After enabling the FTP service and configuring the username and password, start the FTP client program on the PC.

Open a DOS window, and enter **ftp** at the DOS prompt:

```
C:\Documents and Settings\Administrator>ftp
ftp>                                                  //The system prompt changed to ftp>.
ftp> open 192.168.0.2                                 //Connect to the access controller.
Connected to 192.168.0.2.
220 FTP service ready.
User (192.168.0.2:(none)): guest                      //Enter the user name guest.
331 Password required for guest
Password:                                             //Enter the password 123456.
230 User logged in.                                   //Successfully connected to the server.
```

Now, use the following commands to maintain the access controller: To back up **main.bin** on the access controller to the PC, do the following:

```
ftp> binary                                           //Specify the transfer mode as binary.
200 Type set to I.
ftp> lcd c:\temp                                      //Change the local path.
Local directory now C:\temp.
ftp> get main.bin main.bin                            //Back up the file to the PC.
200 Port command okay.
150 Opening BINARY mode data connection for /main.bin.
```

```
226 Transfer complete.
ftp: 14323376 bytes received in 16.81Seconds 851.87Kbytes/sec.
```

To restore the backup file to the access controller, do the following:

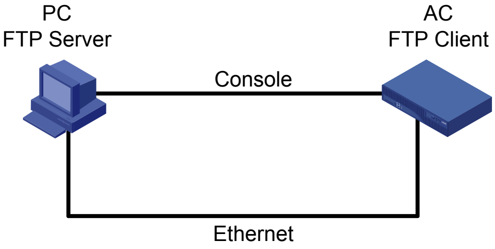
```
ftp> put main.bin main.bin                        //Download the backup file to the access controller.
200 Port command okay.
150 Opening BINARY mode data connection for /main.bin.
226 Transfer complete.
ftp: 14323376 bytes sent in 8.29Seconds 1727.37Kbytes/sec.
ftp> quit                                          //Quit FTP.
221 Server closing.
```

The access controller as an FTP client

You can also maintain the file system of your access controller through FTP with the access controller as an FTP client.

1) Set up a maintenance environment.

Figure 5-10 Set up a software maintenance environment (access controller as an FTP client)



Run the FTP server program on the PC, set the file path, and set the username and password for the access controller.

Configure the IP addresses for both sides, which must be on the same subnet. For example, set the IP address of the FTP server (PC) to 192.168.0.1, while that of the access controller's Ethernet interface to 192.168.0.2. Then use **ping** to verify the network connectivity.

2) Maintain the access controller using the terminal connected to the console port of the access controller.

```
<H3C>ftp 192.168.0.1
Trying 192.168.0.1 ...
Press CTRL+K to abort
Connected to 192.168.0.1.
220 3Com 3CDaemon FTP Server Version 2.0
User(192.168.0.1:(none)):guest                          //Enter the username set on the server.
331 User name ok, need password
Password:                                               //Enter the password.
230 User logged in                                      //Connection succeeded.
[ftp]
```

Use the following commands to maintain the access controller.

Download and back up files using the **get** and **put** commands.

```
[ftp]get main.bin main.bin                  //Download the file from the server to the access controller.
 cfa0:/main.bin has been existing. Overwrite it?[Y/N]:y      //Overwrite the existing file or not?
```

```
227 Entering passive mode (192,168,0,1,5,60)
125 Using existing data connection
226 Closing data connection; File transfer successful.
FTP: 10323352 byte(s) received in 13.234 second(s), 780.00K byte(s)/sec.
[ftp]put main.bin main.bin                    //Back up the file on the access controller to the server.
227 Entering passive mode (192,168,0,1,5,90)
125 Using existing data connection
226 Closing data connection; File transfer successful.
FTP: 10323352 byte(s) sent in 7.342 second(s), 1406.00Kbyte(s)/sec.
[ftp]quit                                      //Quit FTP.
221 Service closing control connection
```

Maintaining Application and Configuration Files

You can modify and display file types by using the file control submenu or the CLI.

Enter **4** on the BootWare main menu to enter the file control submenu. The system displays the following:

```
=================================<File CONTROL>==================================
|Note:the operating device is cfa0                                              |
|<1> Display All File(s)                                                        |
|<2> Set Application File type                                                  |
|<3> Delete File                                                                |
|<0> Exit To Main Menu                                                          |
=================================================================================
Enter your choice(0-3):
```

Displaying All Files

Displaying all files on BootWare menu

Enter **1** on the file control submenu, and the system displays the following information:

```
Display all file(s) in cfa0:
 'M' = MAIN      'B' = BACKUP      'S' = SECURE      'N/A' = NOT ASSIGNED
===========================================================================
|NO. Size(B)   Time                 Type   Name                           |
|1   10323352  Aug/20/2008 10:42:42 M      cfa0:/main.bin                 |
|2   33        Aug/20/2008 10:06:24 N/A    cfa0:/system.xml               |
|3   842       Aug/20/2008 10:23:56 N/A    cfa0:/startup.cfg              |
|4   76960     Aug/15/2008 15:58:02 N/A    cfa0:/vmetest.vme              |
===========================================================================
```

Displaying all files on the CLI

```
<H3C>dir
Directory of cfa0:/

   0     -rw-   10323352  Sep 11 2053 02:17:14   main.bin
   1     -rw-         33  Aug 28 2008 10:22:50   system.xml
   2     -rw-        802  Aug 28 2008 10:22:50   startup.cfg
   3     -rw-     76960  Aug 15 2008 15:58:02   vmetest.vme

252434 KB total (242996 KB free)

File system type of cfa0: FAT32
```

Setting an Application File Type

Using the BootWare menu

Enter **2** on the file control submenu, and the system displays the following information:

```
'M' = MAIN      'B' = BACKUP      'S' = SECURE      'N/A' = NOT ASSIGNED
==========================================================================
|NO. Size(B)   Time                 Type   Name                          |
|1   10323352  Aug/20/2008 10:42:42 M      cfa0:/main.bin                |
|0   Exit                                                                |
==========================================================================
Enter file No:
```

Enter the file sequence number at the prompt above. In this example, type **1** for file main.bin and press **Enter**. The system prompts you to modify the file type:

```
Modify the file attribute:
================================================================================
|<1> +Main                                                                     |
|<2> -Main                                                                     |
|<3> +Backup                                                                   |
|<4> -Backup                                                                   |
|<0> Exit                                                                      |
================================================================================
Enter your choice(0-4)
```

Enter **1** for +Main (set to type M), **2** for –Main (remove the M type), **3** for +Backup (set to type B), or **4** for –Backup (remove the B type). For details about the file types, refer to section “Application Files” on page xx.

Using the CLI

# Change the type of file main.bin from type B to type M+B.

```
<H3C> boot-loader file main.bin main
This command will set the boot file. Continue? [Y/N]:y
The specified file will be used as the main boot file at the next reboot on slot 1!
```

Now, the type of file main.bin is modified as M+B, and the file is specified as the main boot file to be used at the next startup of the access controller. If a file of type M already exists on the access controller, the type of the file will automatically change to N/A.

Specifying a Startup Configuration File

Using the CLI

You can use the **startup saved-configuration** *cfgfile* command to specify the configure file to be used for the next startup of the access controller. *cfgfile* represents the name of the configuration file to be specified.

# Specify the configuration file to be used for the next startup of the access controller.

```
<H3C> startup saved-configuration startup.cfg
Please wait ...
... Done!
```

# Display the configuration file used for the current startup and that to be used for the next startup of the access controller.

```
<H3C>display startup
 Current startup saved-configuration file: cfa0:/startup.cfg
 Next startup saved-configuration file: cfa0:/startup.cfg
```

# Cancel the configuration file specified for the next startup of the access controller.

```
<H3C>undo startup saved-configuration
 Please wait ...... Done!
<H3C>display startup
 Current startup saved-configuration file: cfa0:/startup.cfg
 Next startup saved-configuration file: NULL
```

Delete a File

Using the BootWare menu

Enter **3** on the file control submenu, and the system displays the following information:

```
Deleting the file in cfa0:
 'M' = MAIN      'B' = BACKUP      'S' = SECURE      'N/A' = NOT ASSIGNED
============================================================================
|NO. Size(B)   Time                 Type   Name                            |
|1   10323352  Aug/20/2008 10:42:42 M      cfa0:/main.bin                  |
|2   33        Aug/20/2008 10:06:24 N/A    cfa0:/system.xml                |
|3   842       Aug/20/2008 10:23:56 N/A    cfa0:/startup.cfg               |
|4   76960     Aug/15/2008 15:58:02 N/A    cfa0:/vmetest.vme               |
|0   Exit                                                                  |
============================================================================
Enter file No:
```

Type a file sequence number and press **Enter**. The system asks you to confirm your operation:

```
The file you selected is cfa0:/startup.cfg,Delete it? [Y/N]
```

Enter **Y** for confirmation. The following message appears, indicating the file was successfully deleted.

```
Deleting.........Done!
```

Using the CLI

Execute the **delete** [**/unreserved**] *file-url* command in user view to delete a file, where:

- ***/unreserved***: Permanently deletes the specified file, and the deleted file can never be restored.
- *file-url*: Name of the file to be deleted.

# Delete file **test.txt** in the root directory.

```
<H3C> delete test.txt
Delete cfa0:/test.txt?[Y/N]:y

%Delete file cfa0:/test.txt...Done.
```

At this time, file **test.txt** is removed to the recycle bin. If you want restore the file, you can use the **undelete** command.

# Restore file **test.txt** from the recycle bin.

```
<H3C> undelete test.txt
Undelete cfa0:/test.txt? [Y/N]:y
% Undeleted file cfa0:/test.txt.
```

Dealing With Password Loss

This section describes how to deal with password loss.

User Password Loss

Your login will be refused if you have forgotten the user password. In this case, set a new user password by following the steps below:

1) Enter the BootWare main menu, and enter **6** to bypass the current configuration in system startup.

The system prompts the following information, which indicates that your setting succeeds.

```
Flag Set Success.
```

2) When the BootWare main menu appears again, enter **0** to reboot the system.

```
System starts booting ...
```

3) Set a new password in system view.

```
[H3C]user-interface console 0
[H3C-ui-console0]authentication-mode password
[H3C-ui-console0]set authentication password simple 123456
```

The above output information indicates that password authentication is used for console port login, the password is set to **123456** in plain text.

Highlight

- After reboot, the system runs with the default configuration, while the original configuration file is still kept on the CF card. To restore the original configuration, use the **display saved-configuration** command to locate the configuration file, and then copy and run it.
- If the password is stored in plain text, you can use the **display current-configuration** command to view the password in the current configuration. If you use the **set authentication password cipher 123456** command to set your password, the password will be stored in cipher text.

4) Save the new password.

```
[H3C] save
```

Note

After modifying the user password, use the **save** command to save it.

BootWare Password Loss

Contact your local dealer if you forget the BootWare password. The technical support staff will help you log in to the access controller and set a new password.

To change the BootWare password, enter the BootWare main menu.

Enter **5** on the BootWare main menu, and follow the prompts:

```
please input old password:
Please input new password:
Please input new password again:
Password Set Successfully.
```

Note

- Once you enter a wrong old password or different new passwords, the password modification operation will fail and the system will exit this operation.
- The BootWare password can consist of a maximum of 32 printable characters, such as letters, numerals, and punctuations.

Super Password Loss

The super password enables you to switch between four super levels. Without a super password, you cannot perform higher privilege operations.

Enter **8** from the BootWare main menu to clear the super password. Then, reboot the access controller. You will directly enter system view after the access controller restarts.

This setting works only once. When the access controller is restarted for a second time, the super password is restored.

Backing Up and Restoring the BootWare

Using the BootWare Menu

You can back up and restore the BootWare on the BootWare operation submenu. After the BootWare is backed up on a storage device, if the normal BootWare is lost, you can restore it using the backup BootWare to boot the device. Enter **7** on the BootWare main menu to enter the BootWare operation submenu. For details of this submenu, refer to section “BootWare operation submenu” on page 5-7.

To back up the basic and extended BootWare to the CF card, enter **1** on the BootWare operation submenu and follow the prompts:

```
Will you backup the Basic BootWare? [Y/N]Y
Begin to backup the Basic BootWare...................Done!
Will you backup the Extend BootWare? [Y/N]Y
Begin to backup the Extend BootWare..................Done!
```

To restore the backup BootWare from the CF card, enter **2** on the BootWare operation submenu and follow the prompts:

```
Will you restore the Basic BootWare? [Y/N]Y
Begin to restore Normal Basic BootWare...Done!
Will you restore the Extend BootWare? [Y/N]Y
Begin to restore Normal Extend BootWare....Done!
```

Using the CLI

You can also use **bootrom** commands to back up and restore the BootWare.

Backing up the BootWare

- Back up the complete BootWare to the Flash:

```
<H3C>bootrom backup all
    Now backuping bootrom, please wait...

    Backup bootrom completed!
```

- Back up the extended BootWare to the Flash:

```
<H3C>bootrom backup part
    Now backuping bootrom, please wait...

    Backup bootrom completed!
```

Restoring the BootWare

- Restore the complete BootWare backed up on the Flash to the system:

```
<H3C>bootrom restore all
 This command will restore bootrom file, Continue? [Y/N]:y
 Now restoring bootrom, please wait...

 Restore bootrom completed!
```

- Restore the extended BootWare backed up on the Flash card to the system:

```
<H3C>bootrom restore part
 This command will restore bootrom file, Continue? [Y/N]:y
 Now restoring bootrom, please wait...

 Restore bootrom completed!
```

6 Troubleshooting

Software Loading Failure

If software loading fails, the system runs the old version of the software. The following information appears:

```
=========================<Enter Ethernet SubMenu>===========================
|Note:the operating device is cfa0                                         |
|<1> Download Application Program To SDRAM And Run                         |
|<2> Update Main Application File                                          |
|<3> Update Backup Application File                                        |
|<4> Update Secure Application File                                        |
|<5> Modify Ethernet Parameter                                             |
|<0> Exit To Main Menu                                                     |
|<Ensure The Parameter Be Modified Before Downloading!>                    |
============================================================================
Enter your choice(0-5): 2
Loading...Failed!
```

In this case, check whether the physical interfaces are properly connected.

- If the interfaces are not properly connected, reconnect them correctly and restart the loading process.
- If the interfaces are properly connected, check the loading process information displayed on the configuration terminal for input errors. In case of any input error, restart the loading process with correct inputs.

Input errors include:

- A baud rate other than 9600 bps selected for BootWare loading using XMODEM
- An improper baud rate setting in HyperTerminal
- A wrong IP address, file name, or TFTP Server work path specified for software loading using TFTP
- A wrong IP address, file name, username, or password specified for software loading using FTP

If the cause cannot be located, contact your local agent for help.

Power Supply Failure

You can check whether the power system of the access controller works normally by observing the PWR LED on the front panel. The PWR LED is solid green when the power system works normally. When the PWR LED is off, check whether:

- The power cord of the access controller is properly connected.
- The voltage of the power input is correct.

Configuration System Failure

If the access controller is operational upon power-on, the configuration terminal displays the boot information; otherwise, you may see nothing or illegible characters on the configuration terminal.

No Display on the Terminal

If there is no information display on the configuration terminal after the access controller is powered on, please check:

- Whether the power LED is solid green.
- Whether all LEDs are off or blinking. If so, the main control board is abnormal.
- Whether the console cable is connected to the console port of the main control board.

If the cause cannot be located in the steps above, the possible reasons are as follows:

- The serial interface to which the console cable is connected is not the one specified in the terminal emulation program.
- Terminal settings are incorrect. The required settings are as follows: 9600 bits per second, 8 data bits, no parity check, 1 stop bit, no flow control, and VT100 for terminal emulation type.
- The console cable is not in good condition.

Illegible Characters on the Terminal

- If illegible characters are displayed, check whether the connection of the console cable is loose.

Table of Contents

Appendix A Installation of Lightning Arrester for Network Interfaces

Note

- You can install a lightning arrester only for each 10/100 Mbps electrical Ethernet interface supporting RJ-45 connectors.
- No lightning arrester for network interface is supplied with the access controller.

If an outdoor network cable should be directly led to the access controller, to prevent possible damages to the access controller due to lightning strike, please serially connect the lightning arrester for the network interface before you plug the outdoor cable into the access controller.

Tools

- Philips or flat-blade screwdrivers
- Multimeter
- Diagonal cutting plier

Installation Procedure

Step1 Remove the protective paper on one side of the double-faced adhesive tape and stick it on the shell of the arrester; remove the protective paper on the other side and stick the arrester on the chassis of the access controller. Keep the arrester as close to the grounding screw of the access controller as possible.

Step2 Cut the ground cable of the arrester of a suitable length according to the distance between the arrester and the grounding screw and then fasten the cable on the grounding screw tightly.

Step3 Use the multimeter to verify whether the ground cable of the arrester has a close touch with the grounding screw and chassis of the access controller.

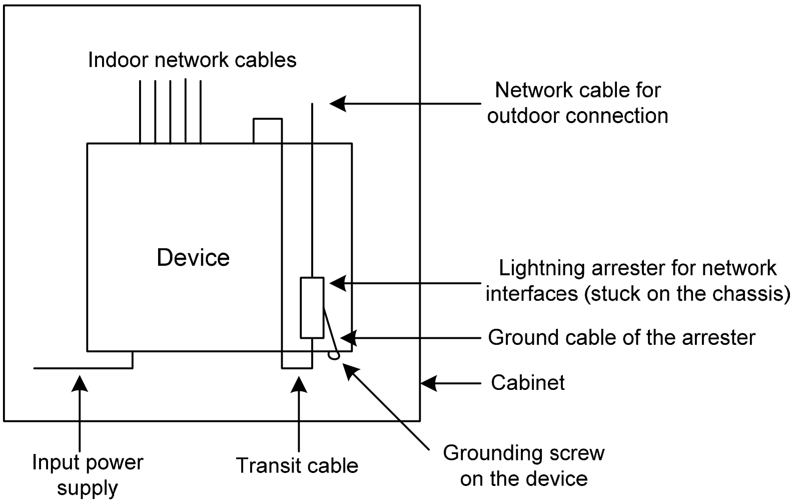
Step4 Follow the instruction of the arrester to connect the arrester for network interface with a transit cable. Pay attention to the direction: IN end of the cable is connected to the arrester while OUT end of the cable is connected to the access controller. After the connection, check whether the LEDs of the interface modules are normal.

Note

Technical parameters, installation and maintenance methods of an arrester have been given in the arrester instruction. Read the instruction carefully before installing the lightning arrester for the network interface.

Step5 Tie the cables together with nylon clips.

Figure A-1 Installation of a lightning arrester for network interface


Indoor network cables
Network cable for outdoor connection
Device
Lightning arrester for network interfaces (stuck on the chassis)
Ground cable of the arrester
Cabinet
Input power supply
Transit cable
Grounding screw on the device

Precautions

To ensure performance of the lightning arrester for network interface during installation, observe the following rules:

- Properly connect the lightning arrester for network interface, with IN connecting to the lightning arrester while OUT connecting to the network interface of the access controller.
- Correctly ground the lightning arrester. When connecting the ground cable, make sure that the ground cable is of a proper length and has a good touch with the grounding screw of the access controller. Check the ground cable with a multimeter after connection.
- Install adequate lightning arresters for network interfaces. When there are more than one network interface connecting to outdoor cables, you should install a lightning arrester for each of the network interfaces to guard the interfaces against possible damages.

Table of Contents

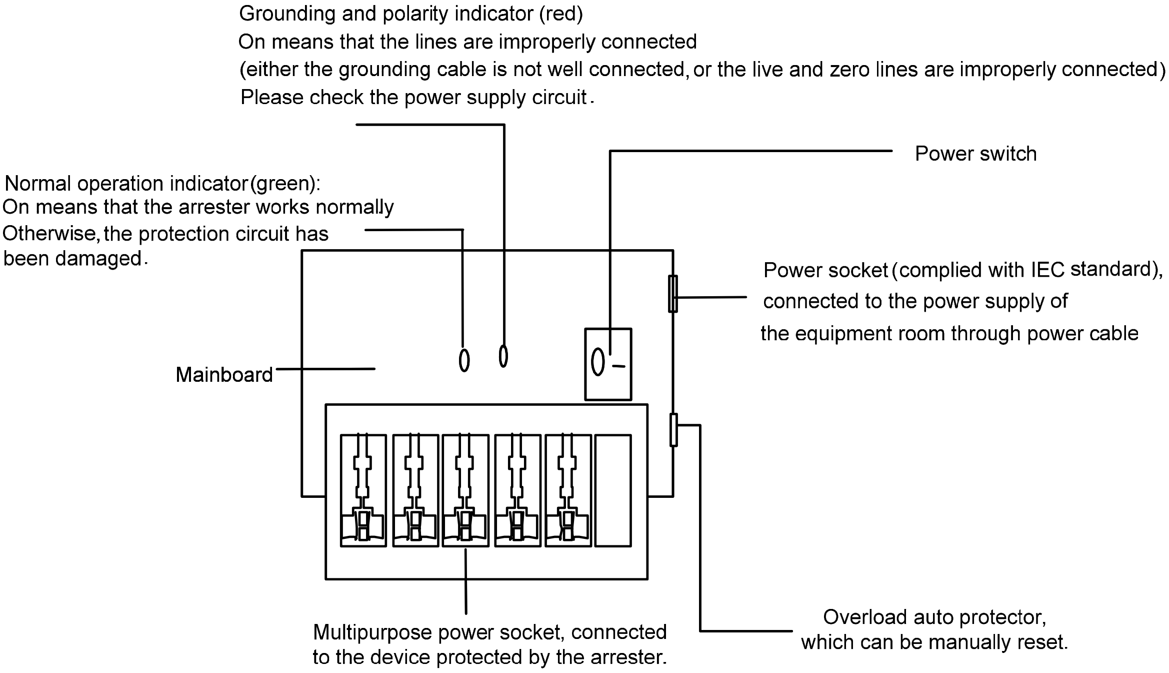
Appendix B Installation of Lightning Arrester for AC Power

Note

No lightning arrester (lightning protection grounding strip) is supplied with the access controller.

If an outdoor AC power cable should be directly led to the access controller, to prevent possible damages to the access controller due to lightning strike, please serially connect the lightning arrester for AC power (lightning protection grounding strip) before you plug AC power cable into the access controller. You can use cable clips and screws to fasten the lightning arrester for AC power on the cabinet, workbench or the wall of the equipment room. When you power on the access controller, the AC power flows through the lightning arrester and then into the access controller.

Figure B-1 Diagram of lightning arrester


Grounding and polarity indicator (red)
On means that the lines are improperly connected
(either the grounding cable is not well connected, or the live and zero lines are improperly connected)
Please check the power supply circuit.
Power switch
Normal operation indicator(green):
On means that the arrester works normally
Otherwise, the protection circuit has been damaged.
Power socket (complied with IEC standard), connected to the power supply of the equipment room through power cable
Mainboard
Multipurpose power socket, connected to the device protected by the arrester.
Overload auto protector, which can be manually reset.

Note the following points:

1) Make sure that the PE terminal of the arrester is well grounded before using the lightning arrester for power.
2) Upon plugging the AC power cable connector of the access controller into the receptacle of the lightning arrester, if the green LED is on while the red LED does not alarm, it means that the lightning arrester of power is running and the function of lightning protection has taken effect.

3) Pay adequate attention if the red LED is on. You should correctly locate the problem, whether it is caused because the ground cable of the arrester is not well grounded or because the live and zero wires are connected in reverse direction.

4) You may use a multimeter to examine the polarity at the power receptacle of the arrester:

- With the power receptacle facing you, if the multimeter displays that the left wire is the zero wire and the right is the live wire, it means that the PE terminal of the arrester is not well grounded.
- Otherwise, it means that the power receptacle of the arrester is set to the reverse polarity. In this case, open the power receptacle of the arrester and correct the polarity. After that, if the red LED still alarms, it means that the arrester is not well grounded yet.

Table of Contents

Appendix C Regulatory Compliance Information

Regulatory compliance standards

Table C-1 Regulatory compliance standards

Discipline	Standards
EMC	FCC Part 15 (CFR 47) CLASS A ICES-003 CLASS A VCCI-3 CLASS A VCCI-4 CLASS A CISPR 22 CLASS A EN 55022 CLASS A AS/NZS CISPR22 CLASS A CISPR 24 EN 55024 EN 61000-3-2 EN 61000-3-3 EN 60601-1-2
Safety	UL 60950-1 CAN/CSA C22.2 No 60950-1 IEC 60950-1 EN 60950-1/A11 AS/NZS 60950 EN 60825-1 EN 60825-2 FDA 21 CFR Subchapter J

European Directives compliance

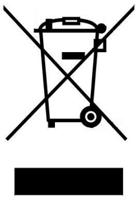
LVD/EMC Directive

These products comply with the European Low Voltage Directive 2006/95/EC and EMC Directive 2004/108/EC.

A copy of the signed Declaration of Conformity can be downloaded from:

http://www.h3c.com/portal/Technical_Documents

WEEE Directive–2002/96/EC



The products this manual refers to are covered by the Waste Electrical & Electronic Equipment (WEEE) Directive and must be disposed of in a responsible manner.

USA regulatory compliance

FCC Part 15

These products comply with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

If the customer modifies the equipment without the authorization of H3C and 3Com, which directly or indirectly contribute to the equipment incompliance with FCC requirements for Class A digital devices, H3C is not liable for such interference problem and the expenses incurred therefrom shall be covered by the customers.

⚠ **Note**

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FDA

These products conform to the applicable requirements of 21 CFR Subchapter J

Canada regulatory compliance

ICES-003

This Class A digital apparatus complies with Canadian ICES-003.

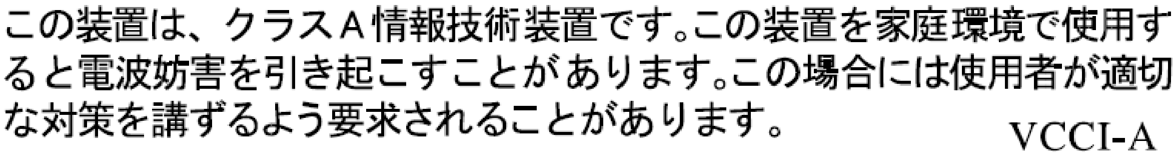
Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Japan regulatory compliance

VCCI

These products comply with the requirements of VCCI Class A Information Technology Equipment (ITE).

Warning: If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.



この装置は、クラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

VCCI-A

EN55022 / CISPR 22 Compliance

These products comply with the requirements of EN55022/CISPR 22 for Class A Information Technology Equipment (ITE).

Warning: If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

Table of Contents

Appendix D Safety Information Sicherheits informationen 安全信息

Overview Überblick 概述

This section introduces part of the safety precautions that should be followed during the installation and maintenance of the equipment. And for the safety statements and warnings, there followed the translations of both German and Chinese to comply with the national requirements.

Dieser Abschnitt macht Sie mit den Sicherheitsvorschriften vertraut, die Sie bei der Installation und Instandhaltung der Ausrüstung beachten müssen.

本章节介绍了在安装、日常维护本系列设备时，必须遵循的安全预防规范。

Note

Before any operation is performed, please read the operation instructions and precautions carefully to minimize the possibility of accidents. The **Note, Caution, Warning and Danger** items in other manuals do not cover all safety precautions that should be followed. They are only the supplements to the safety precautions for operations as a whole. Therefore, the personnel in charge of the installation and maintenance of the products are required to understand these basics of safety operation.

In performing various operations, please follow the local safety regulations. The safety precautions introduced in the product manuals are supplementary and subject to the local safety regulations.

When various operations are executed on the products, the precautions and special safety instructions provided with the products must be followed to the full.

Anmerkung

Lesen Sie bitte alle Arbeitsanweisungen und Sicherheitvorschriften sorgfältig durch, bevor Sie mit dem Arbeiten beginnen. Nur durch Beachtung dieser Hinweise lässt sich das Unfallrisiko minimieren. Die in anderen Handbüchern aufgeführten Symbole **Anmerkung**, **Achtung**, **Warnung** und **Gefahr** beinhalten nicht alle zu beachtenden Sicherheitvorschriften. Sie dienen lediglich der Ergänzung. Deshalb muss sich das für die Installation und Instandhaltung der Ausrüstung verantwortliche Personal mit allen Sicherheitshinweise vertraut machen.

Bei der Durchführung der verschiedenen Arbeitsschritte müssen außerdem die örtlichen Sicherheitsvorschriften beachtet werden. Die in den Handbüchern der einzelnen Produkte aufgeführten Sicherheitshinweise sind Ergänzungen und unterliegen den nationalen Sicherheitsvorschriften.

Während der Arbeit mit den Produkten sind deshalb grundsätzlich alle Sicherheitsvorschriften und spezifischen Sicherheitshinweise genau zu beachten.

说明

为了避免可能发生的事故，请在进行任何操作前，仔细阅读设备操作手册和本章节的安全规范。手册中 出现的**说明、注意、警告、危险，**不能涵盖所有的安全预防，仅仅是在整个操作过程中的安全提示和补充。因此，负责安装和日常维护本设备的人员必须具备安全操作基本技能。

操作人员要按照当地的安全规范进行操作。出现在产品手册中的安全预防措施仅仅是当地安全规范的补充。

在操作本设备时，请认真执行产品手册规定的安全规范。

Conventions Used Symbole Erläuterung 应用惯例

The symbols in this manual are shown in the following table. They are used to remind the reader of the safety precautions during equipment installation and maintenance.

Die Symbole in diesem Handbuch verwendeten sind in der folgenden Tabelle dargestellt. Diese Symbole sollen das Personal während der Installation und Instandhaltung der Ausrüstung an die Wichtigkeit der im Handbuch aufgeführten Sicherheitsvorschriften erinnern.

以下表格中的安全标识，是用来提示读者在进行设备安装和维护时的安全预防要求。

Table D-1 Safety symbol and description

Sicherheitssymbole und Beschreibung 安全标识和描述

Safety Symbol **Symbole** **安全标识**	**Description** **Erläuterung** **描述**
⚠	Generic alarm symbol: To suggest a general safety concern Alarm: Hinweis auf ein generelles Sicherheitsproblem 一般注意标识：用于一般安全提示
⚠	ESD protection symbol: To suggest electrostatic-sensitive equipment. ESD-Schutz: Hinweis auf Beschädigung infolge elektrostatischer Entladung 防静电标识：用于表示静电敏感的设备
⚡	Electric shock symbol: To suggest a danger of high voltage Elektrischer Schlag: Hinweis auf Gefährdung durch Hochspannung 电击防护标识：用于表示高压危险
✹	Laser symbol: To suggest a strong laser beam Laser: Hinweis auf starken Laser 激光辐射标识：用于表示强激光辐射

General Requirements Allgemeine Anforderungen 通用要求

In order to reduce the technically unavoidable residual risk to a minimum, it is imperative to follow the rules below:

Um das technisch bedingte Restrisiko auf ein Minimum zu begrenzen, ist es unbedingt erforderlich, die folgenden Regeln zu beachten:

为了避免对人和设备造成伤害，请认真执行下列要求：

- Read all the instructions before operation.
- Lesen Sie alle Anweisungen sorgfältig durch, bevor Sie mit dem Arbeiten beginnen.
- 在进行操作前仔细阅读手册内容。
- When installing the unit, always make the ground connection first and disconnect it last.
- Beachten Sie, dass bei der Installation des Systems stets zuerst die Erdverbindung angebracht wird und das die Erdverbindung stets als letztes getrennt wird.
- 进行设备安装时，必须确保接地连接是最先连接和最后断开。
- Do not block ventilation openings while the system is on, and keep at least 5 cm distance from ventilation openings and walls or other things which may block the openings.
- Sorgen Sie dafür, dass die Öffnungen der Ventilation zu keinem Zeitpunkt verschlossen, verstopft oder anderweitig blockiert sind. Zwischen den Ventilationsöffnungen und Wänden bzw. anderen Gegenständen muss stets ein Abstand von mindestens 5cm bestehen.
- 设备在工作时必须确保通风口的畅通，确保设备离墙壁或是其它的可能堵塞通风口的物体的间距至少 5cm。
- Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection.
- Betreiben Sie die Ausrüstung niemals ohne Erdung. Trennen Sie das System nicht von der Erdung.
- 不允许破坏设备的接地导线或是在无接地连接的情况下操作设备，要进行适当的电气检查。
- The unit/system must be connected to the protection ground before operation. And the cross-section of protective earthing conductor shall be at least 1.0 mm^2
- Das System muss vor der ständigen Inbetriebnahme geerdet werden. Der Querschnitt der Erdverbindung sollte mindestens 1.0mm^2 betragen.
- 进行设备/系统操作前，请确保永久接地，并且用于进行保护接地连接的接地线截面不小于 1.0mm^2。
- For AC supplied model: The device applies to TN power systems.
- Mit Wechselstrom betriebenes Modell: Das Gerät arbeitet mit einem Phase-Nullleiter-System.
- AC 电源输入：此设备用于 TN 电源系统。
- For AC supplied model: The plug-socket combination must be accessible at all times because it serves as the main disconnecting device.
- Mit Wechselstrom betriebenes Modell: Der Netzstecker muss jederzeit leicht zugänglich sein.
- AC 供电：插座必须随时可用，因为它是主要的切断电源装置。
- Because these products have several power supplies, disconnect all of them to switch off the device.
- Da das Gerät mehrere Energiequellen hat, ist es notwendig stets alle Verbindungen zu unterbrechen, um den energiefreien Zustand zu erreichen.
- 因为设备存在多种电源输入，在关闭设备时确保切断所有电源连接。
- To prevent laser radiation from hurting your eyes, never stare into the open optical port.
- Nehmen Sie das Gerät nicht in Betrieb, solange das optische Fenster nicht geschlossen ist. Der Laserstrahl kann zu Augenverletzungen führen.
- 为了避免光纤发出的高能量的激光光束伤害到视网膜，请不要直视光接口。
- For DC input, a disconnect device shall be provided by the building installation
- Mit Gleichstrom betriebenes Modell: die Gebaeudeinstallation liefert eine Trennung Vorrichtung
- DC 输入设备需要使用建筑物安装来提供短路保护
- For DC supplied model: Reinforced insulation must be provided to isolate 61-72V source from the AC mains supply.
- Mit Gleichstrom betriebenes Modell: Für das Gerät muss eine verstärkte Isolation bereitgestellt werden, um die 61-72V-Quelle gegen die Hauptversorgung zu isolieren.

- DC 电源输入：61-72V 电源和 AC 主输入之间的绝缘等级是加强绝缘。

Power Cable Zuleitung 电缆

Note

Installation and removal of live power cable is prohibited strictly. Transient contact between the core of power cable and conductor may generate electric arc or spark or electric arc, which may lead to fire or eye injury.

Anmerkung

Das Entfernen und Anbringen von Zuleitungen ist strengstens verboten. Kurzschlüsse zwischen innerem und äußerem Leiter können Lichtbögen oder Funkenflug verursachen, was zu Feuer oder einer Augenverletzung führen kann.

Note

禁止安装和移动带电的线缆。因为导电体和带电的线缆，即使短暂接触，也会引起电火花或电弧，从而导致失火或是伤害眼睛。

- Before the power cable is installed or removed, the power switch must be turned off.
- Das System muss stets abgeschaltet werden, bevor die Zuleitung angebracht oder entfernt wird.
- 在安装、移动线缆之前，请切断电源。
- Before the power cable is connected, it must be confirmed that the power cable and label comply with the requirements of the actual installation.
- Überprüfen Sie vor dem Anbringen der Zuleitung immer, ob das von Ihnen verwendete Kabel den Anforderungen entspricht.
- 在进行线缆连接前，请确认线缆和线缆的标识与实际安装要求是一致的。

Note

For DC power supplied equipment, please use 1.0 mm^2 or 16 AWG minimum power supply cord.
For AC power supplied equipment, please use 1.0 mm^2 or 16 AWG minimum power supply cord.

Anmerkung

Für mit Gleichstrom betriebene Ausrüstung benutzen Sie bitte eine 1.0 mm^2 oder 16 AWG Zuleitung. Für mit Wechselstrom betriebene Ausrüstung benutzen Sie bitte eine 1.0 mm^2 oder 16 AWG Zuleitung.

说明

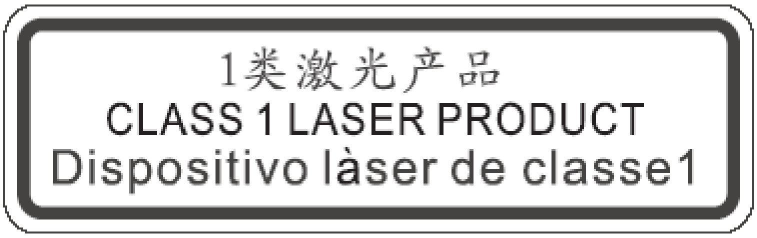
DC 电源设备，请使用 1.0mm^2 或 16AWG 电缆；
AC 电源设备，请使用 1.0mm^2 或 16AWG 电缆。

Laser Laser 激光辐射

The laser hazard level of this equipment is Class 1.

Die von diesem Laser ausgehende Gefahr entspricht der Kategorie 1.

本设备的激光防护等级是 1 类



1类激光产品
CLASS 1 LASER PRODUCT
Dispositivo làser de classe1

Warning

When performing installation and maintenance operations of optical fibers, you should not stand close to, or look into the optical fiber outlet directly with unaided eyes.

Warnung

Während der Installation und Instandhaltung der optischen Fasern dürfen Sie nicht zu nahe am Ausgang der optischen Fasern stehen und nicht ohne Augenschutz in die optischen Fasern sehen.

警告

在安装和维护设备的光纤接口时，请不要把眼睛靠近或是直视这些光接口。