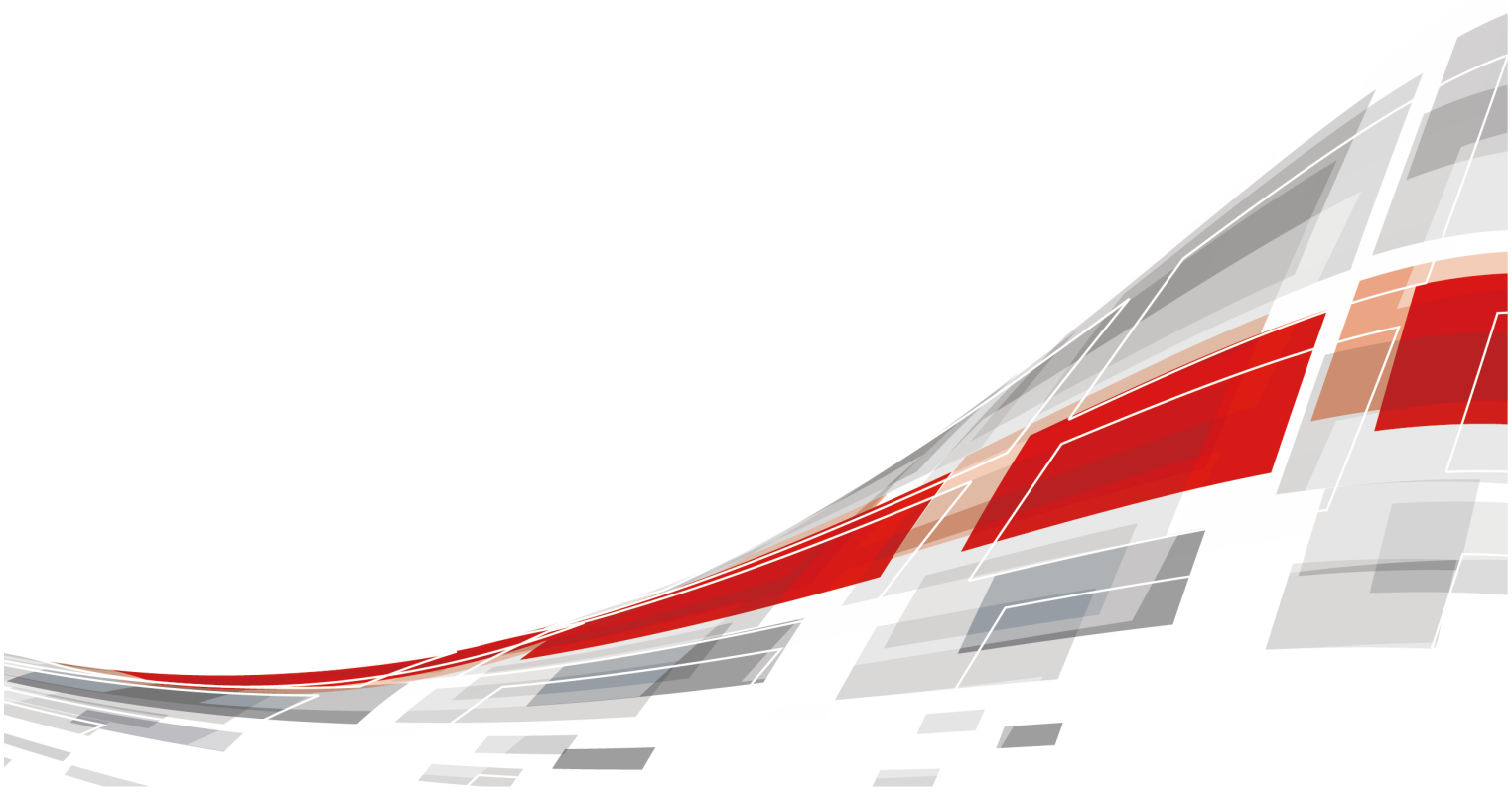
## Server

# Deployment Guide

**Issue** 03

**Date** 2025-03-30



**XFUSION INTERNATIONAL PTE. LTD.**

### Trademarks and Permissions



### Notice

The purchased products, services and features are stipulated by the contract made between xFusion and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

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 a warranty of any kind, express or implied.

## XFUSION INTERNATIONAL PTE. LTD.

Website: https://www.xfusion.com

# About This Document

## Purpose

This document describes how to deploy a server.

## Intended Audience

This document is intended for operators who perform the deployment. Operators must:

- Be familiar with the product networking and related network element (NE) versions.
- Have device maintenance experience and be familiar with device operation and maintenance.

## Symbol Conventions

The symbols that may be found in this document are defined as follows:

| Symbol | Description |
| --- | --- |
| DANGER | Indicates a hazard with a high level of risk which, if not avoided, will result in death or serious injury. |
| WARNING | Indicates a hazard with a medium level of risk which, if not avoided, will result in death or serious injury. |
| CAUTION | Indicates a hazard with a low level of risk which, if not avoided, will result in minor or moderate injury. |
| NOTICE | Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance degradation, or unpredictable results.<br>NOTICE is used to address practices not related to personal injury. |
| NOTE | Calls attention to important information, best practices and tips.<br>NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration. |

# Change History

| Issue | Date | Description |
| --- | --- | --- |
| 03 | 2025-03-30 | Optimized some description. |
| 02 | 2023-12-07 | This issue is the second official release. |
| 01 | 2021-12-17 | This issue is the first official release. |

# Contents

**About This Document** ..... ii

**1 Basic Knowledge Preparations** ..... 1

**2 Preparations for the Deployment** ..... 2

2.1 Environmental Requirements for Operation ..... 2
2.1.1 Requirements for the TR ..... 2
2.1.1.1 Site Selection Requirements ..... 2
2.1.1.2 Layout Requirements ..... 3
2.1.1.3 Construction Requirements ..... 4
2.1.1.4 Illumination Requirements ..... 5
2.1.1.5 Fire Control Requirements ..... 5
2.1.1.6 Shock Resistance Requirements ..... 5
2.1.1.7 Surge Protection Requirements ..... 6
2.1.2 Environment Requirements for the Proper Running of the Server ..... 6
2.1.2.1 Climate ..... 6
2.1.2.2 Organisms ..... 7
2.1.2.3 Corrosive Airborne Contaminants ..... 7
2.1.2.4 Mechanically Active Materials ..... 9
2.1.3 Lightning Protection and Grounding Requirements ..... 10
2.1.3.1 Generic Grounding Requirements ..... 10
2.1.3.2 Grounding Requirements for the TR Building ..... 11
2.1.3.3 Grounding Requirements for Power Supplies ..... 11
2.1.3.4 Grounding Requirements Inside the Cabinet ..... 11
2.1.3.5 Grounding Requirements for the Server ..... 11
2.1.3.6 Grounding Requirements for Signal Cables ..... 14
2.1.3.7 Wiring Requirements ..... 14
2.1.3.8 Grounding Requirements for Maintenance Terminals ..... 15
2.1.3.9 Lightning Protection Requirements ..... 15
2.1.4 Power Supply Requirements ..... 15
2.1.4.1 AC Power Supply ..... 16
2.1.4.2 DC Power Supply ..... 17
2.1.4.3 High-Voltage DC Power Supply ..... 21
2.1.5 Electromagnetic Compatibility and ESD Protection Requirements ..... 23

2.1.5.1 Electromagnetic Compatibility Requirements....23
2.1.5.2 ESD Protection Requirements....23
2.2 Checking the Equipment Room Environment....24
2.3 Planning Network Resources....39
2.4 Downloading Software and Documents....40
2.5 Tools....42
**3 Deployment....44**
3.1 Overall process....45
3.2 Unpacking and Checking Devices....46
3.2.1 Checking Before Unpacking....46
3.2.2 Unpacking Devices....48
3.2.3 Inspecting Devices....48
3.3 Installing Hardware....49
3.4 Powering On....49
3.5 Performing Initial Configuration....50
3.5.1 Default Data....50
3.5.2 Batch Deployment....51
3.5.3 Single-Node Deployment....53
3.5.3.1 Single-Node Deployment Process....53
3.5.3.2 Configuring the IP Address for the Management Network Port....54
3.5.3.2.1 Setting the IP Address for the Management Network Port Using the LCD....55
3.5.3.3 Logging In to the iBMC WebUI....55
3.5.3.4 Checking the Server....58
3.5.3.5 Changing Initial Passwords....61
3.5.3.6 Updating Firmware....65
3.5.3.7 Configuring RAID....66
3.5.3.8 Configuring the BIOS....66
3.5.3.9 Installing an OS....66
3.5.3.10 Installing drivers....66
3.6 Backing Up Configuration Files....66
3.6.1 Batch Backup....66
3.6.2 Single-Node Backup....66
3.7 Accepting Products....68
**4 Engineering Documents to Be Handed Over....69**
**5 Common Operations....70**
5.1 Logging In to the Server Over a Network Port by Using PuTTY....70
5.2 Logging In to a Server Over a Serial Port by Using PuTTY....72
5.3 Logging In to the Server Using the Remote Virtual Console....74
5.4 Enabling and Configuring IPv6 on the Client....74
**6 More Information....76**
6.1 Obtaining Technical Support....76

6.2 Product Information Resources ..... 77
6.3 Product Configuration Resources ..... 77
6.4 Maintenance Tools ..... 78

# 1 Basic Knowledge Preparations

The deployment personnel must master the following basic knowledge:

- For details about the server, see the user guide of each product. **Table 2-15** lists the paths where you can obtain the user guides.
- Basic knowledge of data communications

# 2 Preparations for the Deployment

2.1 Environmental Requirements for Operation

2.2 Checking the Equipment Room Environment

2.3 Planning Network Resources

2.4 Downloading Software and Documents

2.5 Tools

## 2.1 Environmental Requirements for Operation

### 2.1.1 Requirements for the TR

#### 2.1.1.1 Site Selection Requirements

The construction, structure, heating, ventilation, power supply, illumination, and fire control for the telecommunications room (TR) must be designed and engineered according to the environment design requirements for telecom equipment, local and national standards and specifications, as well as the specifications and requirements for construction design in process simulation.

During engineering design, a suitable site should be selected for the TR according to the telecom network plan and technical requirements for telecom equipment by considering hydrographic, geographic, seismic, power supply, and transportation factors.

To ensure that the server works in a favorable environment, locate the TR at a site away from high temperature, dust, toxic gases, explosive materials, unstable voltage, shock, strong noises, and substations.

The TR site should meet the following requirements:

- The TR should be
  - At least 5 kilometers away from heavy pollution sources such as smelteries and coal mines.

  - At least 3.7 kilometers away from medium pollution sources such as chemical, rubber, and galvanization industries.
  - At least 2 kilometers away from light pollution sources such as packinghouses and tanyards.

NOTE

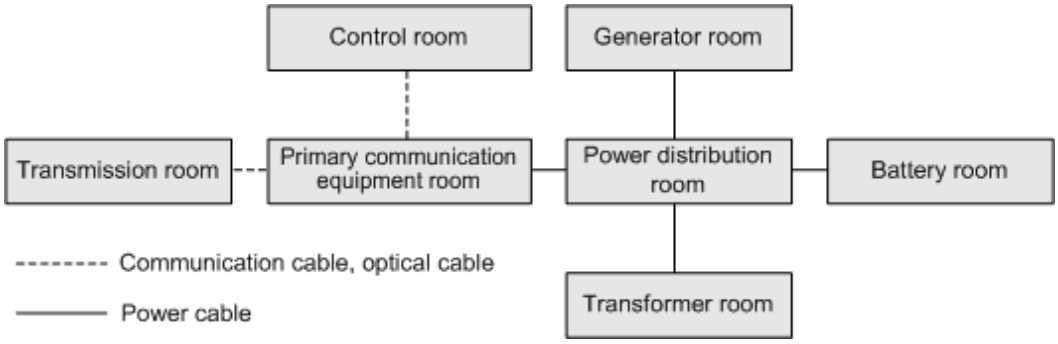
If one or more of these requirements cannot be met, ensure that the TR is situated in the upwind direction of the pollution sources.

- The air vents of the TR should be located far away from the exhaust of city waste pipes, large cesspools, and sewage treatment tanks. The TR should be in the positive pressure state. Otherwise corrosive gases will enter the TR and corrode components and circuit boards.
- The TR should be away from industrial and heating boilers.
- The TR should be away from dusty roads or sand fields. If this situation is unavoidable, the doors and windows of the TR should not be facing the pollution sources.
- The TR should be at least 3.7 kilometers away from the seaside or salt lakes. If this situation is unavoidable, the TR should be airtight and equipped with air conditioners. In addition, the salt-affected soil cannot be used as construction materials.
- The TR should be kept away from livestock farms. If this requirement cannot be satisfied, the equipment room should be located in the perennial upwind direction of the livestock farms.
- The TR cannot be a place that has been used for livestock raising or a warehouse that has been used to store fertilizer.
- It is recommended that the TR be on or above the second floor. If this is impossible, the ground for equipment installation in the TR should be at least 600 millimeters above the highest local flood record.

### 2.1.1.2 Layout Requirements

The TR mainly houses communication equipment, transmission equipment, and supporting equipment such as power supplies. For ease of maintenance and management, the equipment should be arranged in a compact manner and installed in different rooms depending on the service type. **Figure 2-1** shows the layout of a TR.

**Figure 2-1** TR layout



The layout should meet the requirements for easy wiring of communication cables and power cables and for easy maintenance of equipment.

### 2.1.1.3 Construction Requirements

Table 2-1 lists the construction requirements for the TR.

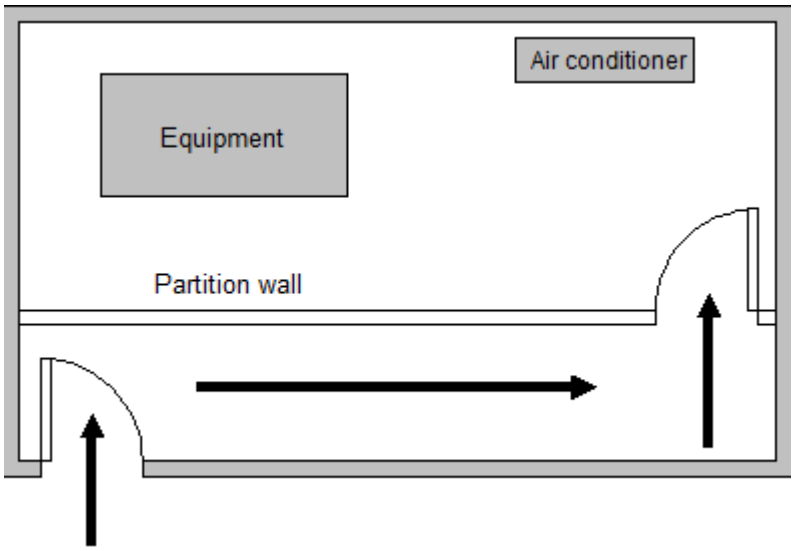
**Table 2-1** Construction requirements for the TR

| Item | Requirement |
| --- | --- |
| Area | The TR should be able to house all the planned equipment. |
| Indoor height | The indoor height indicates the distance between the floor and the beam or ventilation pipe of the TR. The height cannot be less than 3 meters. |
| Floor | It is recommended that the TR also have a movable raised floor properly. The horizontal tolerance in each square meter must be less than 2 meters. If a movable raised floor is not available, static electricity conductive floor materials with the volume resistivity of 1.0 x $10^7$ ohms to 1.0 x $10^{10}$ ohms should be used instead. The static electricity conductive floor materials or the movable raised floor must be connected to a ground point through a current limiting resistor and a connection line. The resistance of the current limiting resistor should be 1 megohm. |
| Load-bearing capacity | The floor bearing capacity varies according to devices. For details, see the physical specifications in the related user guide. |
| Doors and windows | The doors and windows must be sealed with dust-proof plastic tapes. It is recommended that windows be constructed with double-layer glass and be sealed properly. |
| Wall surface | The walls can be pasted with wallpapers or daubed with flat paint. Note that the paint that can be easily pulverized must not be used. |
| Water pipe | It is recommended that water supply pipes, drainpipes, and storm sewers should not be routed across the TR. Fire hydrants must be installed in a corridor or near a staircase where convenient access is possible. |
| Internal partition wall | The area where the server is installed should be isolated from the door of the TR by an internal partition wall, because an internal partition wall can prevent dust from entering, as shown in Figure 2-2. |
| Installation position of air conditioners | Air conditioners should be installed in a proper position where the air does not blow directly at the server. |

| Item | Requirement |
| --- | --- |
| Other requirements | Measures should be taken to prevent micro-organisms such as fungi and molds and rodents such as rats from entering the TR. |

**Figure 2-2** Internal partition wall in the TR




### 2.1.1.4 Illumination Requirements

The TR should be equipped with the following illumination systems:

- Active illumination system, which is powered by the mains supply.
- Backup illumination system, which is powered by the backup power supply (such as the diesel electric generator) in an office.
- Emergency illumination system, which is powered by storage batteries when the mains supply has been interrupted but the backup power supply has not yet started to supply power.

### 2.1.1.5 Fire Control Requirements

For small TRs, a certain number of portable fire extinguishers should be prepared in each room for initial fire control. The number and positions of fire extinguishers depend on their dimensions and the area of the TR. In large TRs, fire extinguishing facilities should be prepared. In addition, an automatic fire alarm system is also required, and fire emergency illumination systems and evacuation instruction marks should be configured at important places, paths, and gateways.

### 2.1.1.6 Shock Resistance Requirements

Shock resistance of the TR must be one degree (Richter scale) higher than that of local common buildings. The TR that does not meet the requirement should be reinforced. When the electronic equipment stops running, the vibration acceleration

of the equipment room floor surface in horizontal and vertical directions should not exceed 500 mm/s$^2$.

### 2.1.1.7 Surge Protection Requirements

Chimneys, antennas, or any other objects that are over 15 meters high on the top of the TR should be designed according to the surge protection requirements for civil buildings.

Measures should be taken against direct flash and intrusion of lightning current. In areas of frequent lightning occurrences, measures against lightning strikes from the side are also required.

The measures against direct flash and intrusion of lightning current are as follows:

- Install surge protector nets or bands at the positions susceptible to lightning strikes. Install surge protection wires or lightning rods on the top of chimneys and antennas that are on top of buildings. Ensure that the cross-sectional area of each down conductor of a surge protector is not smaller than 2 mm$^2$ and the space between the conductors is not greater than 30 meters.
- Use a surge protector with the ground resistance of less than 10 ohms.
- Ground outdoor cables and metal pipes before they enter the TR, and install surge protectors at the inlet of the TR when outdoor overhead cables are brought to the TR.
- Use roof plates, beams, and pillars made of reinforced concrete and reinforcement bars as the down conductor of lightening arresters if possible.

The measures against lightning strikes from the side are as follows:

- Connect the external metal window frame to the down conductor of surge protectors.
- Place surge protection metal bands horizontally at a definite spacing on the outside wall along the height of the building.

It is recommended that a joint ground system be used for the lightening protection of the TR building. A joint ground system connects the telecom power grounding, protection grounding, surge protection grounding of the TR building, and grounding of the power-frequency AC power supply system. The ground resistance of a joint ground system should not exceed 10 ohms.

It is recommended that reinforcement bars in the walls and pillars of the TR building be used as down conductors for lightening protection. These conductors should be electrically connected so as to equalize the electric potential in the building.

## 2.1.2 Environment Requirements for the Proper Running of the Server

### 2.1.2.1 Climate

Ensure that the temperature and humidity in the equipment room meet the requirements for normal device operating. For details about the requirements of each server, see the technical specifications in the corresponding server user guide.

### 2.1.2.2 Organisms

Plants and animals are not allowed in the TR.

To meet these requirements, take the following measures in the TR:

- Keep the atmosphere dry.
- Prevent molds on everything.
- Block cable holes and antenna holes.
- Clean and sterilize the TR periodically.

### 2.1.2.3 Corrosive Airborne Contaminants

Corrosive airborne contaminants and other negative environmental factors (such as abnormal temperature and humidity) may expose equipment to higher risks of corrosive failure. This article specifies the limitation on corrosive airborne contaminants with an aim to avoid such risks.

Table 2-2 lists common corrosive airborne contaminants and their sources.

**Table 2-2** Common corrosive airborne contaminants and their sources

| Symbol | Sources |
|---|---|
| $H_2S$ | Geothermal emissions, microbiological activities, fossil fuel processing, wood rot, sewage treatment |
| $SO_2$, $SO_3$ | Coal combustion, petroleum products, automobile emissions, ore smelting, sulfuric acid manufacture |
| S | Foundries, sulfur manufacture, volcanoes |
| HF | Fertilizer manufacture, aluminum manufacture, ceramics manufacture, steel manufacture, electronics device manufacture |
| $NO_x$ | Automobile emissions, fossil fuel combustion, chemical industry |
| $NH_3$ | Microbiological activities, sewage, fertilizer manufacture, geothermal emissions, refrigeration equipment |
| C | Incomplete combustion (aerosol constituent), foundry |
| CO | Combustion, automobile emissions, microbiological activities, tree rot |
| $Cl_2$, $ClO_2$ | Chlorine manufacture, aluminum manufacture, zinc manufacture, refuse decomposition |
| HCl | Automobile emissions, combustion, forest fire, oceanic processes, polymer combustion |
| HBr, HI | Automobile emissions |

| Symbol | Sources |
| --- | --- |
| $O_3$ | Atmospheric photochemical processes mainly involving nitrogen oxides and oxygenated hydrocarbons |
| $C_NH_N$ | Automobile emissions, animal waste, sewage, tree rot |

The concentration level of corrosive airborne contaminants in a data center shall meet the requirements listed in the white paper entitled Gaseous and *Particulate Contamination Guidelines for Data Centers published in 2011* by American Society of Heating Refrigerating and Air-conditioning Engineers (ASHRAE) Technical Committee (TC) 9.9.

According to the Guidelines, corrosive airborne contaminants in a data center shall meet the following requirements:

- Copper corrosion rate

  Less than 300 Å/month per ANSI/ISA-71.04-2013 severity level G1
- Silver corrosion rate

  Less than 200 Å/month.

NOTE

Å is a unit of length. One Å is equal to 1/10,000,000,000 meter.

According to ANSI/ISA-71.04-2013 Environmental Conditions for Process Measurement and Control Systems: Airborne Contaminants, the gaseous corrosivity levels are G1 (mild), G2 (moderate), G3 (harsh), and GX (severe), as described in **Table 2-3**.

**Table 2-3** Gaseous corrosivity levels per ANSI/ISA-71.04-2013

| Severity Level | Copper Reactivity Level | Silver Reactivity Level | Description |
| --- | --- | --- | --- |
| G1 (mild) | < 300 Å/ month | < 200 Å/ month | An environment sufficiently well-controlled such that corrosion is not a factor in determining equipment reliability. |
| G2 (moderate ) | < 1000 Å/ month | < 1000 Å/ month | An environment in which the effects of corrosion are measurable and may be a factor in determining equipment reliability. |
| G3 (Harsh) | < 2000 Å/ month | < 2000 Å/ month | An environment in which there is high probability that corrosive attack will occur. |

| Severity Level | Copper Reactivity Level | Silver Reactivity Level | Description |
|---|---|---|---|
| GX (severe) | ≥ 2000 Å/month | ≥ 2000 Å/month | An environment in which only specially designed and packaged equipment would be expected to survive. |

See **Table 2-4** for the requirements on the copper and silver corrosion rates.

**Table 2-4** Concentration limitation on corrosive airborne contaminants in a data center

| Group | Gas | Unit | Concentration |
|---|---|---|---|
| Group A | $H_2S$ | ppb[a] | < 3 |
| | $SO_2$ | ppb | < 10 |
| | $Cl_2$ | ppb | < 1 |
| | $NO_2$ | ppb | < 50 |
| Group B | HF | ppb | < 1 |
| | $NH_3$ | ppb | < 500 |
| | $O_3$ | ppb | < 2 |
| a: Parts per billion (ppb) is the number of units of mass of a contaminant per 1000 million units of total mass. | | | |

Group A and group B are common gas groups in a data center. Group A's or group B's concentration limitation values that correspond to copper reactivity level G1 are calculated based on the condition that relative humidity in a data center is lower than 50% and that the gases in the group interacts. A 10% of increase in the relative humidity will heighten the gaseous corrosivity level by 1.

Corrosion is not determined by a single factor, but by comprehensive environmental factors such as temperature, relative humidity, corrosive airborne contaminants, and ventilation. Any of the environmental factors may affect the gaseous corrosivity level. Therefore, the concentration limitation values specified in the previous table are for reference only.

### 2.1.2.4 Mechanically Active Materials

The TR should be free from explosive, conductive, magnetism-permeable, and corrosive dust. **Table 2-5** lists the requirements for concentration of the mechanically active materials in the TR.

**Table 2-5** Requirements for concentration of mechanically active materials

| Mechanically Active Materials | Unit | Concentration |
|---|---|---|
| Sand | $mg/m^3$ | ≤ 30 |
| Suspending dust | $mg/m^3$ | ≤ 0.2 |
| Dust deposit | $mg/(m^2h)$ | ≤ 1.5 |

To meet these requirements, take the following measures in the TR:

- Use dustproof materials on the ground, wall, and ceiling of the TR.
- Install screens for outdoor doors and windows, and use dustproof materials for outer windows.
- Clean the TR, especially the air filters once every three months.
- In areas with heavy dust, you are advised to clean the equipment once a year. (Be sure to ask professional companies to do so.)
- Wear shoe covers and ESD clothing before entering the TR.

## 2.1.3 Lightning Protection and Grounding Requirements

### 2.1.3.1 Generic Grounding Requirements

- The design for grounding should follow the principles of equal voltage and equal potential. In other words, the working grounding and protection grounding, including the shielded grounding and the surge protection grounding of the cable distribution frame are jointly grounded at the same grounding body set.
- Any uncharged metal objects in the TR, such as cable troughs, cable trays, cabinets, racks, shells, metal ventilation pipes, and metal doors and windows, should be grounded.
- The ground cable must be directly connected to the protection ground bar of the TR.
- The PGND cable should be a green-and-yellow insulated cable.

NOTE

In North America, the PGND cable should be a green insulated cable.

- To decrease high-frequency impedance, copper, rather than aluminum, should be used as the conductor of the ground cable and the ground cable should be thick and short as much as possible.
- Ground connection should meet the following requirements:
  - The joint face is conductive and cannot be painted.
  - The joint face is clean.
  - Surface contact should be used in connection and the connection area should meet the requirement for through-current capability.
  - Connecting parts should be fixed securely.

  - It is recommended that the same metal be used as connecting parts, because this prevents electrochemical corrosion.
- The PGND cable does not have any joint and no switch or fuse is installed on it.
- The AC neutral wire must not be used as a PGND cable. The cabinet shell and PGND cable must be insulated from the neutral wire of the AC power supply.

### 2.1.3.2 Grounding Requirements for the TR Building

- It is recommended that reinforced concrete be applied to the construction of the TR.

  The TR should be equipped with surge protectors, such as lightning rods.
- The surge protection grounding of the TR should share the same grounding body as the protection grounding of the TR.
- The grounding resistance of the TR or communication office should not be greater than 10 ohms and should comply with local and national industry standards.

  The grounding resistance should be measured periodically to ensure effective grounding.

### 2.1.3.3 Grounding Requirements for Power Supplies

- The protection grounding for the power supply should share the same grounding body set as the protection grounding for communication equipment.

  The power supply should share the same protection ground bar as the equipment in the same TR.
- The -48 V DC output positive terminal of the power supply must be connected to the nearest ground terminal.

  If only one protection ground bar is provided in the TR, the PGND cable and working ground cable of the power supply must be connected to this ground bar.

  If two ground bars are provided in the TR, namely, a protection ground bar and a working ground bar, then the PGND cable and working ground cable of the power supply must be connected to the corresponding ground bar. The protection ground bar and working ground bar must share one grounding body set.

### 2.1.3.4 Grounding Requirements Inside the Cabinet

- At least one ground terminal at the front door, rear door, and side panel of the cabinet should be properly connected to the ground terminal of the cabinet.
- At least one ground terminal at the shell of the shelf and power box (or power distribution box) should be properly connected to the ground terminal of the cabinet.

### 2.1.3.5 Grounding Requirements for the Server

- The server and supporting equipment (such as mobile base stations, switches, and power supplies) in the TR should be grounded. The protection ground (PGND) cables of the equipment in the communication office should be finally connected to the total ground bar.

PGND cables of the equipment in a line should be connected to the ground bar of the first cabinet. PGND cables of the equipment not in a line but in the same TR should be connected to the protection ground bar of the TR.

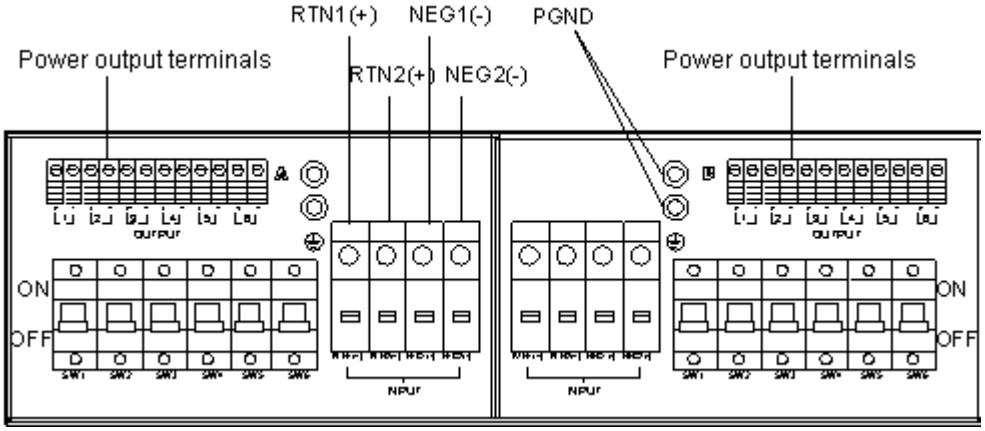
- The -48 V power cable that is led out from the -48 V power input terminal of the server should be connected to the -48 V bus bar of the power cabinet or power distribution cabinet that is provided and used by the customer. Similarly, the RTN cable that is led out from the RTN power input terminal should be connected to the RTN bus bar. See **Figure 2-3**.

  The PGND cable that is led out from the total ground terminal of the server should be connected to the nearest protection ground bar that is provided and used by the customer. See **Figure 2-4**.

NOTE

- If the server is powered by a power distribution cabinet, the PGND cable that is led out from the total ground terminal of the cabinet should be connected to the protection ground bar of the power distribution cabinet.
- If the server is powered by a power cabinet, the PGND cable that is led out from the total ground terminal of the cabinet should be connected to the nearest protection ground bar of the power cabinet or that of the TR.

**Figure 2-3** Output terminals of a power box



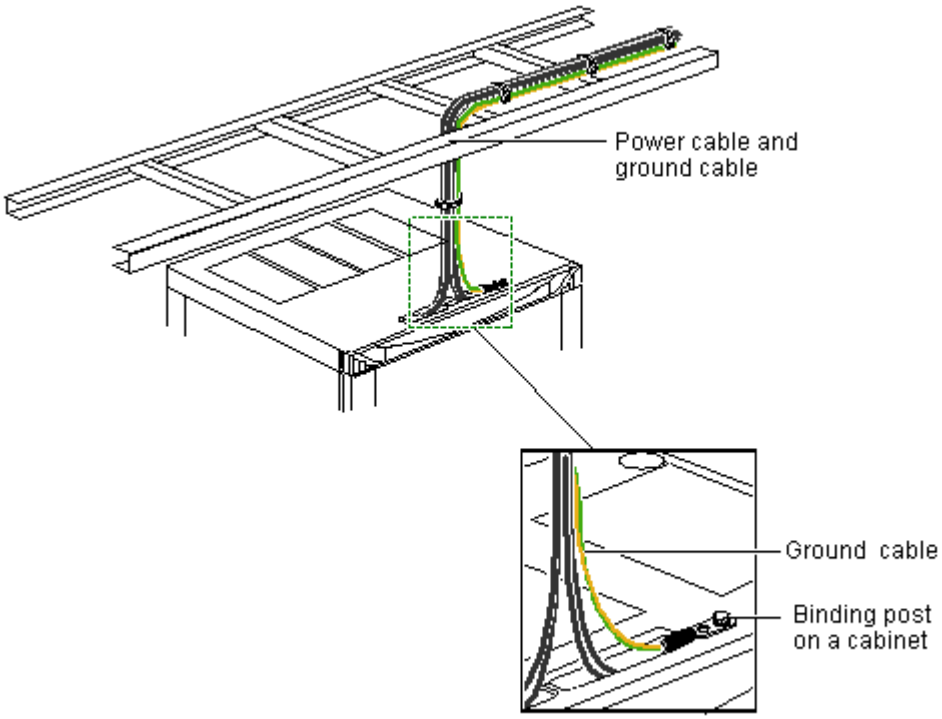

Description:

The protection ground terminal on the power box of a cabinet is used to ground the power box. The PGND cable that is led out from the protection ground terminal should be connected to the protection ground bar of the cabinet.

The -48 V power cable that is led out from the -48 V power input terminal of the power box in a cabinet should be connected to the -48 V bus bar of the power cabinet or power distribution cabinet that is provided and used by the customer. Similarly, the RTN cable that is led out from the RTN power input terminal should be connected to the RTN bus bar.

**Figure 2-4** Total ground terminal of a cabinet




Description:

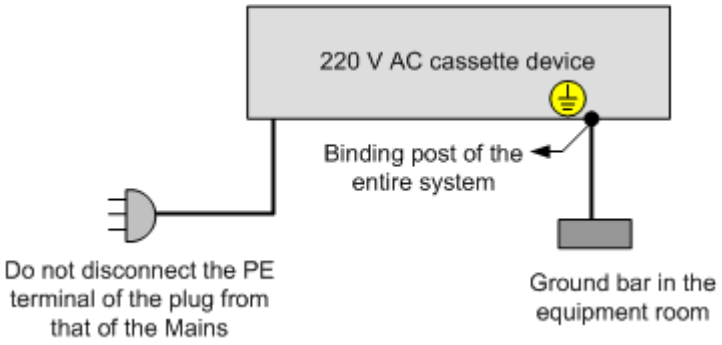
The total ground terminal of a cabinet is used for the grounding of the entire cabinet. The PGND cable that is led out from the total protection ground terminal should be connected to the protection ground bar that is provided and used by the customer.

- If a box device is not installed in a cabinet,
  - the -48 V power cable that is led out from the -48 V power input terminal of the device should be connected to the -48 V bus bar of the power cabinet or power distribution cabinet that is provided and used by the customer. Similarly, the RTN cable that is led out from the RTN power input terminal should be connected to the RTN bus bar.
  - The PGND cable that is led out from the total ground terminal of the device should be connected to the nearest protection ground bar that is provided and used by the customer.
- If a box device is installed in a cabinet provided by the customer,
  - The -48 V power cable that is led out from the -48 V power input terminal of the device should be connected to the -48 V ground terminal or ground bar of the cabinet that is provided and used by the customer. Similarly, the RTN cable that is led out from the RTN power input terminal should be connected to the RTN ground terminal or ground bar.
  - The PGND cable that is led out from the ground terminal of the device should be connected to the nearest protection ground terminal or ground bar that is provided and used by the customer.
- If there is no protection ground bar in the TR, an AC-powered box device can be grounded by properly connecting the PE cable of its three-core cord to the PE

end of the mains supply. See **Figure 2-5**. In this case, you need to check the electrical connectivity and reliability of grounding by using a multimeter after the installation.

**Figure 2-5** Grounding of an AC-powered box device




## 2.1.3.6 Grounding Requirements for Signal Cables

- It is recommended that shielded cables or the cables with metal jackets be used as the signal cables that are led into or led out from an office.

  The shielded layer, metal jacket, or metal tube of a cable that is led into the TR must be connected to the nearest protection ground bar of the TR.
- Both ends of the shield layer of a shielded cable should have good electrical contact with the metal shell of the server they connect to.
- Grounding of the external conductors of coaxial cables to the digital distribution frame (DDF) should meet customer requirements.

  The DDF must be grounded. The DDF and the server in the same TR should share one protection ground bar.
- The incoming and outgoing signal cables to and from an office and the idle line pairs inside the cables should be grounded for protection.
- The metal reinforcing ribs of the incoming and outgoing signal cables to and from an office should be grounded to the optical distribution frame (ODF) or optical fiber box in the TR.

## 2.1.3.7 Wiring Requirements

- Ground cables must not be bound or entwined with signal cables. If they are parallel, the distance between them cannot be shorter than 3 centimeters.
- The incoming and outgoing signal cables, power cables, and optical cables to and from an office must not twine around the signal cables and power cables in the TR. If they are parallel, the distance between them cannot be shorter than 5 centimeters.
- Ground cables must not be led in from above. They must be underground or arranged indoors.
- PGND cables should be routed straight and as short as possible, and must not spiral.
- A PGND cable should not be longer than 30 meters, and should be as short as possible. The protection ground bar should be installed at a place less than 30 meters away from the server.

### 2.1.3.8 Grounding Requirements for Maintenance Terminals

- If an AC-powered maintenance terminal communicates with the monitored server only over an Ethernet port, the maintenance terminal can be grounded by connecting the PE cable in its three-core cord to the PE end of the mains supply.

  After grounding a maintenance terminal, use a multimeter to check the voltage or current at the connection between the maintenance terminal and the PE end of the AC power supply, ensuring a reliable electrical connection.
- If an AC-powered maintenance terminal communicates with the monitored DC-powered server over a non-Ethernet ports, for example, an RS232 port or RS422 port, the maintenance terminal should be grounded by connecting its PGND cable to any of the following ground devices:
  - Protection ground bar of the TR
  - Power distribution cabinet that supplies power to the server
  - Protection ground bar in the cabinet provided by the customer

    To disconnect the grounding connection between the three-core cord and the mains supply, break the PE prong of the plug and then insert the plug into an AC socket.
- If the server monitored by an AC-powered maintenance terminal is powered by an AC power supply, the maintenance terminal can be grounded by connecting the PE cable in its three-core cord to the PE end of the mains supply.

  After grounding a maintenance terminal, use a multimeter to check the voltage or current at the connection between the maintenance terminal and the PE end of the AC power supply, ensuring a reliable electrical connection.
- If a maintenance terminal is powered by an uninterruptible power supply (UPS) or an inverter, the shell of the UPS or inverter should be directly connected to the protection ground bar of the TR or the power distribution cabinet. The maintenance terminal can be grounded by connecting the PE cable of the three-core cord of the UPS or inverter to the PE end of the mains supply.
- If the maintenance terminal is powered by a DC power supply, the shell of the maintenance terminal should be connected to the protection ground bar of the TR, the power distribution cabinet, or the cabinet provided by the customer, or be connected to the ground terminal of the server, over a PGND cable.

### 2.1.3.9 Lightning Protection Requirements

- Power cables must not be led into the TR from above.

  After a power cable is led into the TR, an industry-standard power surge protector should be installed at the entrance near the power cable and be connected to the nearest ground terminal. The ground cable should be as short as possible.
- Signal cables must not be led into the TR from above.

  After a signal cable is led into the TR, an industry-standard signal surge protector should be installed at the entrance near the signal cable and be connected to the nearest ground terminal. The ground cable should also be as short as possible.

## 2.1.4 Power Supply Requirements

### 2.1.4.1 AC Power Supply

## Requirements for the AC Power Supply

The AC power supply comprised of the mains supply, UPS, and electric generator set is suitable for integrated power supply. Such an AC power supply should provide the features of simple connection, safe operation, flexible scheduling, and easy maintenance, and meet the load requirement in the office. A low voltage power supply system should be three-phase, five-wire, or single-phase, three-wire. **Table 2-6** lists the nominal voltage and rated frequency of a low voltage AC power supply.

**Table 2-6** Nominal voltage and rated frequency of a low voltage AC power supply

| Nominal Voltage | Rated Frequency |
| --- | --- |
| 110 V, 127 V, 220 V, and 380 V | 50 Hz |

A UPS is typically used as an AC potential power of network products. A UPS should be in the same phase as the mains supply. The time used for switching between the UPS and the mains supply should be less than 10 ms. Otherwise, the server will reboot or reset.

When determining the AC distribution capacity in the TR, consider the working current and fault current. An independent device must have an independent AC distribution protection apparatus. The maximum capacity of the current over the configuration protection switch should be greater than the maximum capacity of the current over the protection switch of each device. When designing the capacity of an AC power supply system, consider the maximum load of the system in dynamic mode and static mode and reserve a certain margin. The cabling on the power distribution panel must be figured out based on the maximum power supply load. This helps you determine the type and size of the conducting wire.

Voltages of an AC-powered server and power equipment should meet the following requirements:

- For an AC-powered server, the voltage fluctuates from -10% of the rated voltage to 5% of the rated voltage.
- For AC-powered power equipment and important buildings, the voltage fluctuates from -15% of the rated voltage to 10% of the rated voltage.
- The AC frequency fluctuates from -4% to 4%. The sinusoidal distortion rate of the voltage waveform is smaller than or equal to 5%.

The electric generator set should perform automatic power-on/off, automatic recruitment, remote communication, remote control, and remote detection, and provide standard interfaces that comply with communication protocols.

The power cable used for AC/DC power distribution should meet the following requirements:

- The conductor in the neutral wire must have the same cross-sectional area as the conductor in the live wire.
- The DC power feeder should be selected based on the long-term load. If the cross-sectional area exceeds 95 $mm^2$, a hard bus cable should be used. If there

is a great difference between the short-term load and the long-term load, cables can be routed by stage.

- AC/DC conducting wires should be flame-retardant and be routed according to the *Code for fire protection design of tall buildings* (GB50045-95). Low voltage power distribution rooms should be designed and configured according to the *Code for low voltage distribution and circuit design* (GBJ54-83).

## Recommendations on the AC Power Supply

Recommendations on the AC power supply are as follows:

- Use a voltage stabilizer or voltage-regulator to respond to unstable voltages. Use a voltage-regulator in the following situations:
  - The server is directly powered by the mains supply, and the power supply voltage exceeds the rated voltage by -10% to +5% or the voltage range allowed for the server.
  - The server is not directly powered by the mains supply, and the mains voltage exceeds the rated voltage by -15% to +10% or the AC input voltage range allowed for the DC power equipment.
- To ensure the continuity of power supplies, use the UPS or inverter.
- Install an electric generator set for an office to ensure the normal communication and power load in case of mains failure. The capacity of the electric generator set should be greater than or equal to 1.5 to 2 times the capacity of the server with uninterrupted power.
- Connect two storage battery strings in parallel. If UPSs are used as storage batteries, only one UPS battery string is required in general. The UPSs need to work in backup mode and can be connected in parallel or serial.

## 2.1.4.2 DC Power Supply

The DC power supply should be stable and reliable. The power equipment should be deployed near the server to make the DC feeder as short as possible. To reduce the power consumption and installation cost, the loop voltage drop from the battery port to the equipment port should be less than 3.2 V. A diesel generator can be configured as a standby AC power supply to reply to long-time outages.

A DC power supply system consists of storage batteries, primary power supplies (rectifiers), and DC power distribution control panels.

## Storage Battery

A storage battery, as an essential component of a DC power distribution system, performs the following functions:

- Stabilizes the voltage so that the server can run properly.
- Stores energy. In the case of mains outage, a storage battery can supply power for a period of time according to its capacity. This prevents communication from being disrupted immediately.
- Filters large capacitors. A storage battery can absorb surge voltages from the rectifier, preventing noise and power frequency interference from getting into the server.

- Shuts down automatically. When the voltage of a storage battery drops to lower than -43 V, the control circuit can automatically shut down the output.

A storage battery is charged or discharges under a low and constant voltage. **Table 2-7** lists the relevant requirements.

**Table 2-7** Requirements for the DC charge/discharge state and voltage

| Power Supply Category | Mains Supply State | Storage Battery Charge / Discharge | DC Voltage | Terminal Voltage of Each Storage Battery | Number of Storage Batteries in Each String |
|---|---|---|---|---|---|
| -48 V DC | Normal | Floating charge by the rectifier | The floating charge voltage reaches 53.5 V. | 2.23 V | 24 |
| | Failed | Discharge | The discharge voltage reaches 43.2 V. | 1.8 V | |
| | Resumed | With the presence of loading, the storage battery is automatically charged with the current 0.1 to 0.15 times the storage battery capacity. | When the charge voltage reaches 56.4 V, modified constant-voltage charge is enabled automatically. That is, the charging state changes to floating charge automatically. | 2.35 V | |

## Primary Power Supply (Rectifier)

Requirements for a primary power supply are as follows:

- Multiple primary power supplies can operate in a parallel connection, and a current equalizer should be configured between them.

- A primary power supply should be equipped with a current limiter.
- The output voltage of a primary power supply should satisfy the requirement for initial charging of a battery, that is, 2.35 x 24 = 56.4 V DC (when the power supply is -48 V DC).
- A DC voltmeter and an ammeter should be installed on a primary power supply.
- The efficiency of a primary power supply should be higher than 85% and its power factor must be greater than 0.8.
- A primary power supply is cooled in a natural manner. It can work continuously with full load at an ambient temperature of 0ºC to 40ºC.
- The output noise voltage (measured with a psophometer, plus the weighing factor) of a primary power supply should meet the requirements listed in **Table 2-8**.
- A primary power supply can automatically shut down the output at a low voltage.

**Table 2-8** Specifications for the DC power voltage

| Item | | DC Power Supply | |
|---|---|---|---|
| Nominal voltage (V) | | -48 V to -60 V | |
| Voltage fluctuation range | | -38.4 V to -72 V | |
| Noise voltage | 0 Hz to 300 Hz | ≤ 400 mV (peak value) | |
| | 300 Hz to 3400 Hz | ≤ 2 mV (weighted noise of the psophometer) | |
| | 3.4 kHz to 150 kHz | Single frequency: ≤ 5 mV effective value | Broadband: ≤ 100 mV effective value |
| | 150 kHz to 200 kHz | Single frequency: ≤ 3 mV effective value | Broadband: 150 kHz to 30 MHz<br>≤ 30 mV effective value |
| | 200 kHz to 500 kHz | Single frequency: ≤ 2 mV effective value | |
| | 500 kHz to 30 MHz | Single frequency: ≤ 1 mV effective value | |

## DC Power Distribution Control Panel

Requirements for the DC power distribution control panel are as follows:

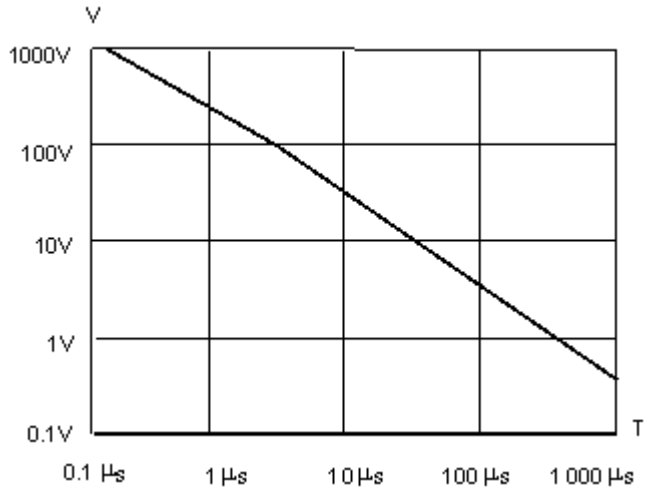
- The capacity of a primary power supply should be designed according to the total power consumption of an office. A certain margin should be reserved. Typically, a high-frequency switch power supply that has high conversion efficiency and works in N+1 hot backup mode should be used. An output current equalizer should be provided for each power module. The failure of a single power module does not affect the proper running of the entire DC power distribution system.

- Each control panel allows the access of a minimum of two storage battery strings. When one storage battery string fails, the other can supply power.
- Each control panel allows the access of a minimum of five primary power supplies.
- The AC power supply system can work in unattended mode.
- When a primary power supply charges storage batteries in floating charge mode, the number of operating primary power supplies depends on the load. When one primary power supply fails, it drops out automatically, and the standby primary power supply automatically starts to operate.
- In the case of mains outage, the storage battery discharges. When the mains supply resumes, the storage battery is recharged with a current 0.1 to 0.15 times the storage battery capacity. When the charge voltage reaches 56.4 V, modified constant-voltage charge is enabled automatically.
- After a storage battery is fully charged, the charging state is changed to floating charge automatically.
- When power equipment fails or works improperly, audible and visible alarms should be raised, and the alarm information should be transmitted to the operation and maintenance center.
- If a short circuit occurs on a branch of the power supply system, the entire power distribution system should not be affected by the sharp voltage reduction. The peak striking voltage should not cause any fault to the server.

The server also has strict restrictions on random transient noises, including the noises caused by external magnetic interference and the interference from the server and ground cables. The shorter the duration of a transient pulse, the higher the allowable transient noise. For the allowable transient noises, see **Figure 2-6**.

**Figure 2-6** Mapping between voltages and pulses




## Recommendations on the DC Power Supply

Recommendations on the DC power supply are as follows:

- Provide power supply in decentralized mode by using multiple DC power supply systems and setting power equipment on multiple sites.

- Use a standard DC power supply system. Set the output voltage of the power supply to a value in the specified range.
- Enhance the reliability of the AC power supply system and decrease the capacity of the storage battery to a proper extent. When the reliability of the AC power supply system at a small communication office fails to be enhanced, increase the capacity of storage batteries accordingly.
- Ensure that the total capacity of high-frequency switch rectifiers meets the requirements for the load power of the server and the charge power of storage batteries. When not more than 10 primary rectifiers are available, configure one secondary rectifier. When more than 10 primary rectifiers are available, configure one secondary rectifier for each 10 rectifiers and one secondary rectifier for the remaining primary rectifiers (less than 10).
- Install two or more storage battery strings. The total capacity of storage battery strings depends on the sum of the duration within which a storage battery string can supply power to loads. In most communication offices, one storage battery string should supply power for at least one hour.

### 2.1.4.3 High-Voltage DC Power Supply

The requirements for safe power supplies to IT equipment increase with the development of IT equipment and growing business demands. The conventional AC uninterruptible power system (UPS), however, has risks of single points of failure (SPOFs). The high-voltage direct current (HVDC) system can eliminate the problems, such as reliability risks, large number of voltage conversion levels, huge line loss, and high maintenance costs, existing in conventional AC and low-voltage DC power supplies.

At present, China Telecom 240 V HVDC standards and China Mobile 336 V HVDC standards are the mainstream HVDC standards used in China.

#### HVDC Power Supply Requirements

- Temperature
  - Operating range: 5°C to 45°C (41°F to +113°F)
  - Storage range: -40°C to + 65°C (-40°F to +149°F)
- Relative humidity
  - Operating range: ≤ 90% RH (40 ± 2°C, 104±35.6°F)
  - Storage range: ≤ 95% RH (40 ± 2°C, 104±35.6°F)
- Vibration performance: ability to withstand sinusoidal frequencies between 10 Hz to 55 Hz and amplitude of 0.35 mm.
- Battery capacity configuration: ensures continuous operation of servers at full loads when the power supplies are unavailable.

  The minimum battery backup time should be 60 minutes for a common system and 120 minutes for an important system.
- Battery cell voltage: 2 V (recommended), 6 V, and 12 V
- The insulation monitoring device acts properly if a ground fault occurs or the insulation resistance is 28 kΩ lower than the set value. The HVDC system is protected against overcurrent and short circuits and can be manually or automatically restored after overcurrent or short circuits are rectified.

- Over- and under-voltage protection for AC power supplies: The power supply system can monitor the input voltage changes. When detecting that the AC input voltage is higher or lower than the specified threshold, the system automatically shuts down. The system automatically restores when the input voltage is normal.
- The site is free from explosive materials, conductive media and hazardous gases that erode metals and affect insulation, and mold.
- Protection against high temperature: When the temperature in the power supply system reaches the specified threshold, the power supply system automatically reduces the power or shuts down the power amplifier. When the temperature falls below the threshold, the power supply system restores the normal power output.
- The system provides alarm records and query, and the alarm display can be updated on a real-time basis. The alarm information is protected against loss when the system is out of power.

The voltage range of a China Telecom 240 V HVDC system is as follows:

| Nominal Voltage (V) | Output Voltage Range (V) | Powered Terminal Voltage Range (V) | Maximum Voltage Drop Allowed (V) |
|---|---|---|---|
| 240 | 204 to 288 | 192 to 288 | 12 |

The voltage range of a China Mobile 336 V HVDC system is as follows:

| Nominal Voltage (V) | Output Voltage Range (V) | Powered Device Voltage Range (V) | Output Voltage Error (V) | Overvoltage Protection Threshold (V) |
|---|---|---|---|---|
| 336 | 300 to 400 | 260 to 400 | ≤ ±1 | 410 |

## HVDC Power Supply Suggestions

- Terminal equipment can be connected to power sockets or wiring terminals. Wiring terminals are recommended.
- Do not use a shunt circuit breaker to connect or control multiple power modules through a multi-purpose power socket.
- Choose DC circuit breakers based on the rated current of the equipment. The 10 A or 16 A dual-pole DC breakers are recommended.
- Connect the DC output positive pole to terminal N of the equipment power cable. Connect the DC output negative pole to terminal L of the equipment power cable. Securely connect the ground terminal of the equipment power cable to the system PGND.
- The upstream input terminal of the power supply system is equipped with a surge protection device to protect the system against a minimal voltage surge of 10/700 us, 5 kV and a minimal current surge of 8/20 us, 20 kA.

- All cables in the power distribution frame (PDF) comply with YD/T 1173-2001 specifications, and the diameters of all power cables meet the requirements for wire ampacity.
- The other technical specifications of the PDF meet YD/T 585-1999 specifications.

# 2.1.5 Electromagnetic Compatibility and ESD Protection Requirements

## 2.1.5.1 Electromagnetic Compatibility Requirements

Table 2-9 lists the electromagnetic compatibility requirements for the proper running of the server.

**Table 2-9** Electromagnetic compatibility requirements

| Electromagnetic Phenomenon | | Specifications |
|---|---|---|
| Low frequency magnetic field | Frequency (Hz) | 50-20,000 |
| | Ampl. A/m (rms) | 0.025-10 |
| Amplitude modulation RF electric field | Frequency (MHz) | 0.009-18,000 |
| | Ampl. V/m (rms) | < 3 |
| Pulse modulation RF electric field | Frequency (GHz) | 1-18 |
| | Ampl. V/m (peak) | < 3 |

To meet the previous requirements, take the following measures:

- Locate the TR away from transformers, high-voltage wires, and high-current equipment, for example, at least 20 meters away from the AC transformer with the capacity greater than 10 kVA and at least 50 meters away from high-voltage wires.
- Locate the TR away from high-power broadcasting transmitter, for example, at least 100 meters away from the broadcasting transmitter with the power greater than 1500 W.
- If there is a mobile communication transmitter in the TR building, its interference effect must comply with local and national standards and regulations. If necessary, take measures to screen and isolate the interference.
- Do not use portable wireless devices when you are near the server.

## 2.1.5.2 ESD Protection Requirements

Static electricity may damage the chips on integrated circuit boards and cause faults in software and electronic switches. Statistics show that 60 percent of damaged circuit boards are caused by static electricity. Therefore, it is essential to take effective ESD protection measures.

The absolute value of electrostatic voltage must be less than 1000 V.

To meet ESD protection requirements, take the following measures:

- Popularize the importance of ESD prevention.
- Wear ESD shoes and ESD clothing before entering the TR. Use ESD tools such as ESD wrist straps, ESD tweezers, and extraction tools when operating on the server.
- Install an ESD floor in the equipment room.
- Ground all conducting materials in the TR, including computers, and set up ESD worktables.
- Keep non-ESD materials (such as common bags, foams, and rubbers) at least 30 centimeters away from ESD-sensitive components.
- Ground the server properly. Although laying the raised floor covered with semiconductive materials, use copper foil for grounding at a number of points on the floor (the copper foil should be placed between the concrete floor and the semiconductive floor and should be connected to a ground cable).
- Take dust prevention measures. Dust or other particles in the TR may cause poor connections between connectors or between metal connecting points.
- Maintain proper humidity. Too high humidity may make metal components rusty, while too low humidity may induce static electricity.

# 2.2 Checking the Equipment Room Environment

Before deployment, check the device operating environment in the customer equipment room. The check items include the layout, load-bearing capacity, shock resistance, surge protection, temperature, humidity, power supply, electromagnetic conditions, electrostatic discharge (ESD), and device installation space in the equipment room. Ensure that the equipment room environment meets the product deployment and construction requirements for a successful project delivery. For details about the requirements for the server running environment, see the *Environmental Requirements for Operation* of corresponding server model.

## Equipment Room Environment

Check the equipment room environment based on the site requirements and low level design (LLD) and fill in the following table. (The following table is for reference only.)

**Table 2-10** Equipment room environment checklist

| No. | Item | Description | Check Result | Remarks | Risk Statement |
|---|---|---|---|---|---|
| 1 | Special configuration in the contract | Fill in the temporary BOM numbers that are not provided by the configuration generator. | None/BOM *XXXXX* | Confirmation from the product manager | To avoid the risk that the temporary BOM numbers do not match with the OS or customers' services. |
| 2 | Unloading tool | Determine the available transportation tools in the customer equipment room and the transportation tools to be provided. | | | |
| 3 | Unloading field environment | The unloading field depth and width are greater than or equal to the length of the truck plus 5 m (16.40 ft) for ease of unloading. | | | |
| 4 | Transportation with packaging materials | The recommended ramp of the road for transportation is less than or equal to five degrees. | | | |

| No. | Item | Description | Check Result | Remarks | Risk Statement |
|---|---|---|---|---|---|
| 5 | Headroom | The headroom is at least 2.15 m (7.05 ft) for devices without packages for fire-proof and elevator doors. (At least 2.35 m (7.71 ft) for devices with packages for fire-proof and elevator doors.) | | | |
| 6 | Transportation road conditions | The roads in the equipment room are level without any step or ramp. If there are steps or ramps, check the height of steps and degree of ramps. | | | |
| 7 | Transportation space | The width of aisles is at least 1.5 m (4.92 ft), and that of elevator or fire-proof doors is at least 1.2 m (3.94 ft). The depth of an elevator is at least 2.2 m (7.22 ft). | | | |

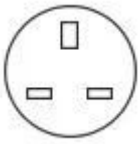
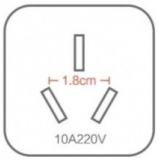
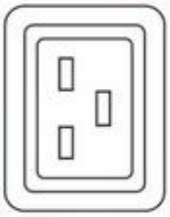
  

| No. | Item | Description | Check Result | Remarks | Risk Statement |
|---|---|---|---|---|---|
| 8 | Positions of all devices | Check whether all devices are placed in the same equipment room. | | If all devices are not in the same equipment room, record devices by equipment rooms. | |
| 9 | Ambient temperature and humidity | Check whether the temperature and humidity in the equipment room are controllable. And record the temperature and humidity. | Temperature (°C):<br>Humidity (RH) : | For details, see the environmental specifications of the specific product model. | |
| 10 | Floor type | Check whether the ESD floor or concrete floor is used in the equipment room. | | | |

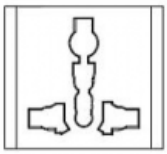
  

| No. | Item | Description | Check Result | Remarks | Risk Statement |
|---|---|---|---|---|---|
| 11 | Floor bearing capacity | Check whether the floor bearing capacity meets requirements of the cabinets to be deployed.<br>The floor bearing capacity must be greater than 450 $kg/m^2$. | | 1. Maximum weight: See the physical specifications in the user guide of a product. For details about how to obtain the user guide, see **2.4 Downloading Software and Documents**.<br>**NOTE**<br>Note: If other devices are to be deployed in the same cabinet as the server, add the weight of the devices.<br>2. Ask the customers to consider the safety coefficient. | |

| No. | Item | Description | Check Result | Remarks | Risk Statement |
|---|---|---|---|---|---|
| 12 | Cabinet type | Check whether the cabinet type meets the installation requirements of each server. For details, see the user guide of each server. | | | |
| 13 | Number of cabinets | Determine the number of cabinets required. | | | |
| 14 | Power cable connector types of a cabinet (with pictures) | Provide pictures of the power cable connectors in the survey results to ensure correct power cable types. |  <br>U.K. socket<br>  <br>10 A socket<br>  <br>16 A socket<br>  <br>Socket for C19 connectors | Confirm before written to the contract using the configuration generator. | To avoid the risk that the power cable configured in the contract is incompatible with the jack. |

| No. | Item | Description | Check Result | Remarks | Risk Statement |
|---|---|---|---|---|---|
| | | |  <br>Socket for C13 connectors | | |
| | | |  <br>European socket | | |
| | | |  <br>10 A universal socket | | |
| | | | Others (Provide pictures and specifications) | | |

| No. | Item | Description | Check Result | Remarks | Risk Statement |
|---|---|---|---|---|---|
| 15 | Cabinet dimensions (D x W x H) | 1. The cabinet installation space meets the following requirements: Height × Width × Depth = 2050 mm x 606 mm x 1118 mm (80.71 in. x 23.86 in. x 44.02 in.). This is for reference only. Reserve space based on the actual cabinet dimensions.<br>2. Check whether there is sufficient maintenance space in front of and behind the cabinet. It is recommended that 1.8 m (5.91 ft) be reserved in front of the cabinet and 1.2 m (3.94 ft) be reserved behind the cabinet. | | | |
| 16 | Cabinet height (U) | Enter the cabinet height in the unit of U, for example, 42U or 46U. | | | |

| No. | Item | Description | Check Result | Remarks | Risk Statement |
|---|---|---|---|---|---|
| 17 | Cabinet installation requirement | Check whether the cabinets need to be secured on the floor, raised floor, or supports of the raised floor. | | | |
| | | Check whether the cabinets need to be combined. | | | |
| 18 | Distance between the four columns in a cabinet | Enter the distance between the front and rear columns and that between the left and right columns. | Distance between the front and rear columns: | For details about the installation dimensions, see rack dimensions in the installation guide or user guide. | To avoid the risk that the guide rails configured in the contract cannot be installed onsite. |
| | | | Distance between the left and right columns: | | |
| 19 | Number of power inputs for a cabinet | Enter the number of external power inputs of a cabinet, for example, two, one, or others. | | | To avoid the risk that the power supply reliability does not meet requirements. |
| 20 | Input power type of a cabinet | Check whether the input power is three-phase, single-phase, or high-voltage (HV) DC. | | For high-voltage DC, specify the voltage range, such as 192 V DC to 288 V DC. | To avoid the risk that the PSUs are incompatible with the current power source. |

| No. | Item | Description | Check Result | Remarks | Risk Statement |
|---|---|---|---|---|---|
| 21 | Power supply capacity of a cabinet | Check the current and voltage that a cabinet provides. | | If the power supply capacity of the equipment room cannot support the power of a cabinet that is fully configured, a cabinet that is half-configured can be delivered. | |
| 22 | Circuit breaker model of PDUs | Enter the circuit breaker vendors and models (for example, C10, C16, C25, and C32). | Vendor:<br>Model: | The circuit breaker and PSU fuse may disconnect at the same time. Greater specifications indicate lower probability of false triggering. | To minimize the probability of circuit breaker tripping due to a circuit breaker with low specifications, at least C32 is recommended. |
| 23 | Check whether the PDU sockets include a fuse or circuit breaker. | If yes, enter the model, for example, x A. | | | |
| 24 | Guide rail | Check whether guide rails are required. | L-shape slide rails<br>Adjustable guide rails<br>Not required | Confirm before written to the contract using the configuration generator. | To avoid the risk that guide rails are incorrectly configured. |

| No. | Item | Description | Check Result | Remarks | Risk Statement |
|---|---|---|---|---|---|
| 25 | Cabling in the equipment room | Check whether the uplink network cables and optical cables use overhead or underfloor cabling. | | | |
| | | Check whether sufficient uplink optical cables have been reserved, that is, reserve each optical cable to the middle in a rack and with additional space. The recommended additional space is 1.2 m (3.94 ft). | | | |
| | | Check the optical cable routing requirements. | | Optical fibers are routed on the top of a cabinet or along a cable ladder. | |
| | | Check whether power cables use overhead or underfloor cabling. | | | |

| No. | Item | Description | Check Result | Remarks | Risk Statement |
|---|---|---|---|---|---|
| | | Check the distance between the power input socket and the bottom of a cabinet or the power output port. | It is recommended that the AC input socket in the equipment room be located in a place that is not more than 0.5 m (1.64 ft) away from bottom on the rear of a cabinet. | | |
| | | Check whether ground cables use overhead or underfloor cabling. | | | |
| | | Check the distance between the device to be grounded and the ground point on a cabinet. | | | |

| No. | Item | Description | Check Result | Remarks | Risk Statement |
|---|---|---|---|---|---|
| 26 | Electromagnetic environment | The following requirements must be met:<br>Low-frequency magnetic field:<br>50 Hz to 20,000 Hz<br>0.025 rms to 10 rms<br>Amplitude-modulation radio-frequency electric field<br>0.009 MHz to 18,000 MHz<br><3rms<br>Pulse-modulation radio-frequency electric field<br>1 GHz to 18 GHz<br>< 3 V/m (peak) | | You are advised to take the following measures to suppress interference signals:<br>● Keep the equipment room away from transformers, high-voltage electricity transmission lines, and high-current devices. For example, there should be no AC transformer of higher than 10 kVA within 20 m (65.62 ft) and no high power voltage electricity transmission line within 50 m (164.04 ft).<br>● Keep the equipment room far | |

| No. | Item | Description | Check Result | Remarks | Risk Statement |
|---|---|---|---|---|---|
| | | | | away from high power broadcast transmitters. For example, there should be no transmitter of higher than 1500 W within 100 m (328.08 ft).<br>● If a mobile communication transmitter is installed in a communication building, its interference degree must comply with the relevant standards and regulations. If necessary, take measures to screen and isolate the | |

| No. | Item | Description | Check Result | Remarks | Risk Statement |
|---|---|---|---|---|---|
| | | | | interference.<br>● Do not use hand-held wireless communication devices when you are close to the devices. | |
| 27 | Types and models of the connected storage devices and switches | Select FC SAN, IP SAN, or specific types of the storage device and switch to be connected, and confirm the optical module model and transmission distance. | FC SAN<br>IP SAN<br>Others | Check the type on the Compatibility Checker. If the device is not in the compatibility list, submit an RM requirement e-flow to evaluate the feasibility. | To ensure that the configured server can be interconnected. |

## Cabinet layout

Determine the cabinet layout based on the site requirements and LLD and complete the following table. (The following table is for reference only.)

**Table 2-11** Cabinet layout

| Row/ Column No. | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| A | | | | | | |
| | N610E-22 | N610E-22 | | | | |
| Row spacing | 1m | | | | | |
| B | | | | | | |
| | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Row spacing | 1m | | | | | |
| C | | | | | | |
| Remarks | | | | | | |
| Note: Specify the position, model (such as N610E-22), and usage (such as CSS) of the cabinets. If the cabinet has its capacity expanded or is closely near to other cabinets, mark the original cabinet in italic and the new cabinet in bold. If you encounter any special situation when checking the installation environment, describe it in the **Remarks** column. | | | | | | |

# 2.3 Planning Network Resources

## Network Topology

Attach the network topology of the network devices connected to the onsite servers.

## IP Address Planning

Before the deployment, plan IP addresses based on the LLD and network topology, and fill in **Table 2-12** and **Table 2-13**.

**Table 2-12** Server management plane (iBMC) IP address planning

| No. | Type | Document | Model | Usage Planning | Equipment Serial Number | iBMC Address (Provided by the Customer) | iBMC MAC Address[1] | iBMC User Name and Password | Management VLAN |
|---|---|---|---|---|---|---|---|---|---|
| Example | Rack server | Cabinet No._Product Model_No. | 1288H V5 | Controller01_DC01 | XXXXXXXX | 10.30.2.1/24 | fa:16:3e:0f:ff:ff | Administrator/Admin@9000 | 3002 |
| | | | | | | | | | |
| | | | | | | | | | |

| No. | Type | Document | Model | Usage Planning | Equipment Serial Number | iBMC Address (Provided by the Customer) | iBMC MAC Address[1] | iBMC User Name and Password | Management VLAN |
|---|---|---|---|---|---|---|---|---|---|
| 1: You can query the iBMC MAC address of a single server in the BIOS or iBMC. For details, see the *BIOS Parameter Reference* and *iBMC User Guide* of corresponding server model. To obtain the iBMC MAC addresses of multiple servers, contact product managers. | | | | | | | | | |

**Table 2-13** Server service plane IP address planning

| No. | Server Name | Network Port ID | IP Address | Service VLAN |
|---|---|---|---|---|
| Example | Cabinet No._Product Model_No. | GE_01 | 10.30.2.1/24 | 3002 |
| | | | | |

# 2.4 Downloading Software and Documents

Before deployment, download the software and documents listed in **Table 2-14** and **Table 2-15** to your PC.

Before deployment, check whether the OS to be installed is compatible, including the OS vendor, OS version, and 32-bit or 64-bit by using the Compatibility Checker. If the OS is not in the compatibility list, submit an RM request for research and development (R&D) tests in advance to ensure that the OS is compatible and can be quickly installed.

**Table 2-14** Software list

| Software | How to Obtain | Operation Instructions |
|---|---|---|
| Smart Provisioning | Visit the **Technical Support Website** > **Software Download** > **Smart Provisioning**. | For details, see the *Smart Provisioning User Guide* of corresponding version. |

| Software | How to Obtain | Operation Instructions |
| --- | --- | --- |
| Drivers and firmware packages of server components | 1. Visit the **Technical Support Website** > **Software Download** > **FusionServer iDriver**.<br>2. Click **Software**, select the required version, and download the driver and software package.<br>**NOTICE**<br>If the card driver or firmware is not released on iDriver, download the driver or firmware package and guide from the official website of the card vendor and manually install and upgrade the driver or firmware according to the guide. | For details, see the *Upgrade Guide* of corresponding server model. |
| ISO image file of the OS to be installed | Prepared by the customer. | For details, see the *Server OS Installation Guide*. |
| Independent remote console | From the support website, search for "kvm_client" and download the required software. | For details, see the *FusionServer Tools User Guide* of corresponding version. |

**Table 2-15** Documentation list

| Document Name | How to Obtain |
| --- | --- |
| Server user guide | 1. Visit the technical support website.<br>2. Go to the corresponding page, for example, **Rack Servers > 1288H V5**.<br>3. On the **Documentation** tab page, choose Installation & Upgrade > Servers to download the required user guide. |
| Server Product Acceptance Manual | 1. Visit the technical support website.<br>2. Go to the corresponding page, for example, **Rack Servers > 1288H V5**.<br>3. On the **Documentation** tab page, choose Maintenance & Services > Acceptance Tests to download the required acceptance guide. |
| BIOS parameter reference | For details, see the *BIOS Reference Document* of corresponding server model. |
| iBMC User Guide | For details, see the *iBMC User Guide* of corresponding server model. |

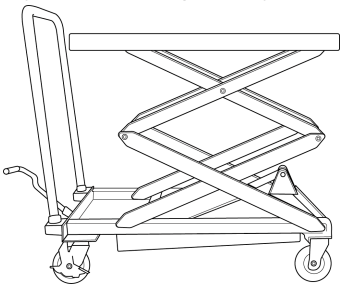
| Document Name | How to Obtain |
| --- | --- |
| iBMC alarm handling | For details, see the *iBMC Alarm Handling* of corresponding server model. |
| RAID controller card user guide | For details, see *RAID Controller Card User Guide* of corresponding server model. |
| OS installation guide | For details, see the corresponding server OS installation guide cases. |
| Release notes | 1. Visit the technical support website.<br>2. Go to the corresponding page, for example, **Rack Servers > 1288H V5**.<br>3. On the **Software Download** tab page, click the required version, and download the required version release notes from the version documentation. |
| Site LLD | Prepared by the customer. |

# 2.5 Tools

**Table 2-16** describes the tools to be prepared.

**Table 2-16** Tools

| Tools for Deployment Except GPU Modules | Tools for Replacing the GPU Module |
| --- | --- |
| ● Hydraulic lifting trolley<br>  <br>The load must be greater than 200 kg (440.92 lb) and the lifting height must be greater than 1.0 m (3.28 ft).<br>● ESD wrist strap or ESD gloves<br>● Protective gloves<br>● ESD bags<br>● Box cutter<br>● Flat-head screwdriver<br>● Socket screwdriver<br>● No.2 Phillips screwdriver<br>● M2.5 Phillips screwdriver<br>● Die-casting pliers<br>(Used to remove LC optical fibers, pluggable optical modules, and unshielded network cables.)<br>  | ● ESD wrist strap<br>● Protective gloves<br>● ESD bags<br>● M3 Phillips screwdriver<br>● T15 x 150 mm (5.91 in.) extended hex screwdriver<br>● M4 x 150 mm (5.91 in.) extended Phillips screwdriver<br>● Vacuum pen |

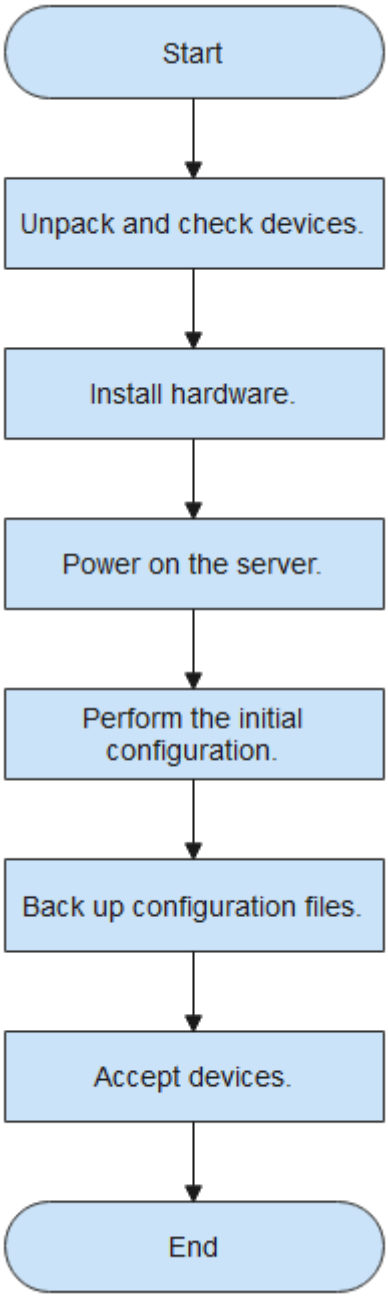
# 3 Deployment

3.1 Overall process
3.2 Unpacking and Checking Devices
3.3 Installing Hardware
3.4 Powering On
3.5 Performing Initial Configuration
3.6 Backing Up Configuration Files
3.7 Accepting Products

# 3.1 Overall process

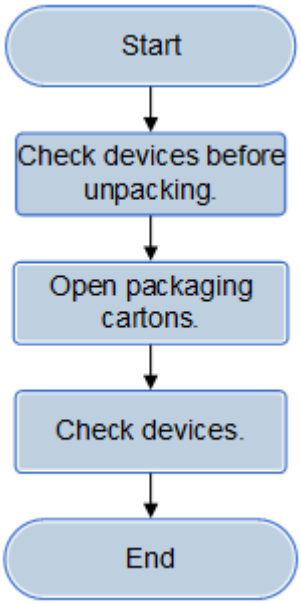
**Figure 3-1** Overall process



# 3.2 Unpacking and Checking Devices

**Figure 3-2** Device acceptance process




## 3.2.1 Checking Before Unpacking

After a project is started, the project supervisor works with the customer to check the received devices.

### Prerequisites

- The devices have been delivered to the site.

  NOTE

  Do not stack servers after unpacking them. If you need to transport the servers, pack them again respectively before transport.

- The project supervisor and the customer representatives have arrived on the site.

### Background

- The bag storing the *Packing List* is attached to the outside of the box.
- Check the number of devices against the *Packing List*.
- If an item in the *Packing List* is marked **Out of Stock**, contact the local office of the device vendor and sign the *Packing List*. If short, wrong, or excessive shipment of goods occurs or goods are damaged, the project supervisor and the customer representative sign the *Memo for Unpacking and Checking Goods* and *Packing List*. The project supervisor fills out the *Cargo Problems Feedback Form*, submits it to the local office of the device vendor within three days, and stores the goods with all the internal and external packages for further investigation.

NOTE

Contact technical support to obtain the *Cargo Problems Feedback Form*.

- After confirming that all devices are intact, both parties sign the *Packing List*. Then the devices are handed over to the customer.

## Procedure

**Step 1** Check the appearance and number of the packages before unpacking the devices.

**Step 2** After a project is started, the project supervisor should work with the customer to check and accept the received devices before unpacking the devices. For details about the check items, see **Table 3-1**.

**Table 3-1** Checklist

| Type | Check Items |
|---|---|
| Carton<br>(skip over this item if no carton is used) | All cartons have no scratch or crack on the surface. |
| | All cartons have no stain or soak mark on the surface. |
| | The cartons, especially the eight angles and twelve edges on each carton, are not misshapen, such as bulges, dents, or creases. |
| | The packing tapes are not abnormally cut open. |
| | Each carton has two or more layers of tamper labels, and the labels are not abnormally cut open. |
| Palletized packaging<br>(skip over this item if no pallet is used) | The stacked cartons are not misshapen, such as bulges or dents. |
| | No strapping band is broken. |
| | The bottom of each pallet does not split, and no wooden leg tilts or is missing. |
| | Paper edge protectors are not pressed crease on cartons and have no obvious dirt, or wear mark or impact on the surface. |
| Delivery labels | The writings on the label are clear and complete, and the labels do not tilt, or have no loss or alteration. |
| | Monitoring labels (if any) on devices are properly displayed. |
| Others | The packages are not damaged, and materials are not exposed. |

**Step 3** Take actions as follows according to the check results:

- If the number of packages is correct, unpack and inspect the devices.
- If the number of packages is incorrect or any carton is damaged or soaked, find the causes and contact the local office of the device vendor. If the equipment is damaged or faulty after unpacking because the carton is severely damaged or soaked, delivery engineers should contact the local product manager or sales personnel and the logistics company to return or replace the goods according to the actual situation, or initiate a dead on arrival (DOA) process.

NOTICE

To protect the devices, store unpacked devices indoors. Take photos of the storage site, rusty or corroded devices, packaging cases, and packaging materials, and archive the photos. Store the unpacked packing cases and packaging materials properly.

**----End**

## 3.2.2 Unpacking Devices

### Procedure

**Step 1** Learn the device types and quantity from the label on the carton.

**Step 2** Cut off the strapping bands using diagonal pliers.

**Step 3** Use a box cutter to cut the tapes along the seams of the carton cover.

NOTICE

Use the box cutter with care, ensuring that the knife edge is not completely inserted into the packing case to avoid injury to your hands or damage to the device.

- Unpack the packaging cartons, and take out foaming boards.
- Check the number and types of objects in each carton against the Packing List and sign the Packing List.

**----End**

## 3.2.3 Inspecting Devices

### Procedure

**Step 1** Open the carton labeled with "Packing List Inside", take out the packing list, and check devices against the packing list.

- If shortage or miscarriage is found, fill in the *Cargo Problems Feedback Form* and send it to the local office.

- If goods are found damaged during the unpacking, fill in the *Cargo Problems Feedback Form* and send it to the local office within three days.
- If the quantity or model of any device does not conform to the packing list, store the unpacked devices, unpacked packages, and packing materials indoors properly, take photos of the storage site, rusty or corroded equipment, packing cases, and packaging materials, and archive the photos.

**Step 2** After checking that all devices and components in one carton are intact, unpack and check the other cartons one by one to avoid misoperations. After checking all devices, sign the Packing List with the customer and affix the customer's official seal.

**----End**

NOTE

Check the air tightness of the 2288E V6 server when it is unpacked. For details, see "Installation and Configuration" > "Installing the Hardware" > "Checking the Air Tightness of a Server" in the *User Guide* of the corresponding server model.

# 3.3 Installing Hardware

For details about how to install the server, see "Installation and Configuration" in the user guide of each product. For details about how to obtain the user guide, see **Table 2-15**.

# 3.4 Powering On

**Powering On a Single Server**

Check that the active and standby PSUs are powered on, the PSU indicators are on, and no PSU alarm is generated on the iBMC. Power on the server using one of the following methods based on the actual situation:

- If PSUs are properly installed but are not yet powered on, power on the PSUs.

  The server will be powered on along with the PSUs.

  NOTE

  By default, **System State Upon Power Supply** is set to **Power On**, which allows the server to power on after the PSUs are applied with power. You can change the option on the iBMC WebUI or BIOS.

- If the PSUs are powered on and the server is in standby state (the power indicator is steady yellow), you can use any of the following methods to power on the server:
  - Press the power button  on the front panel to power on the server.

    If the power indicator is steady green, the device is powered on.
  - Power on the server using the iBMC WebUI.
    i. Log in to the iBMC WebUI. For details, see **3.5.3.3 Logging In to the iBMC WebUI**.
    ii. Choose **System** > **Power** > **Power Control**. The **Power Control** page is displayed.

iii. Click **Power On**. In the displayed dialog box, click **Yes** to power on the server.

– Power on the servers using the Remote Virtual Console.

i. Log in to the Remote Virtual Console. For details, see the *iBMC User Guide* of corresponding server model.

ii. On the KVM screen, click  on the toolbar, and choose **Power On**.

The server is being powered on.

NOTE

Here, the HTML5 integrated remote console is used as an example, and the operation of Java integrated remote console is similar.

– Power on the server using the iBMC CLI.

i. Log in to the iBMC CLI. For details, see the *iBMC User Guide* of corresponding server model.

ii. On the iBMC CLI, run the **ipmcset -d powerstate -v 1** command.

iii. Enter **y** or **Y** to remotely power on the server.

**Power On Servers in Batches**

For details about how to power on servers in batches, see "Performing Server Power Control Operations" in the *FusionServer Tools User Guide* of corresponding version.

NOTE

You are advised to power on servers in several small batches to prevent unstable power supply due to the sharp increase of loads on the power grid when too many servers are powered on at a time.

# 3.5 Performing Initial Configuration

## 3.5.1 Default Data

**Table 3-2** Default data

| Type | Document | Default Value |
| --- | --- | --- |
| iBMC management network port data | IP address and subnet mask of the management network port | • Default IP address: **192.168.2.100**<br>• Default subnet mask: **255.255.255.0** |
| iBMC login data | User name and password | • Default username: **Administrator**<br>• Default password: **Admin@9000** |
| BIOS data | Default Password | Admin@9000 |

| Type | Document | Default Value |
| --- | --- | --- |
| iBMC U-Boot data<br>**NOTE**<br>V6 and later servers do not support iBMC U-Boot. | Default Password | Admin@9000 |

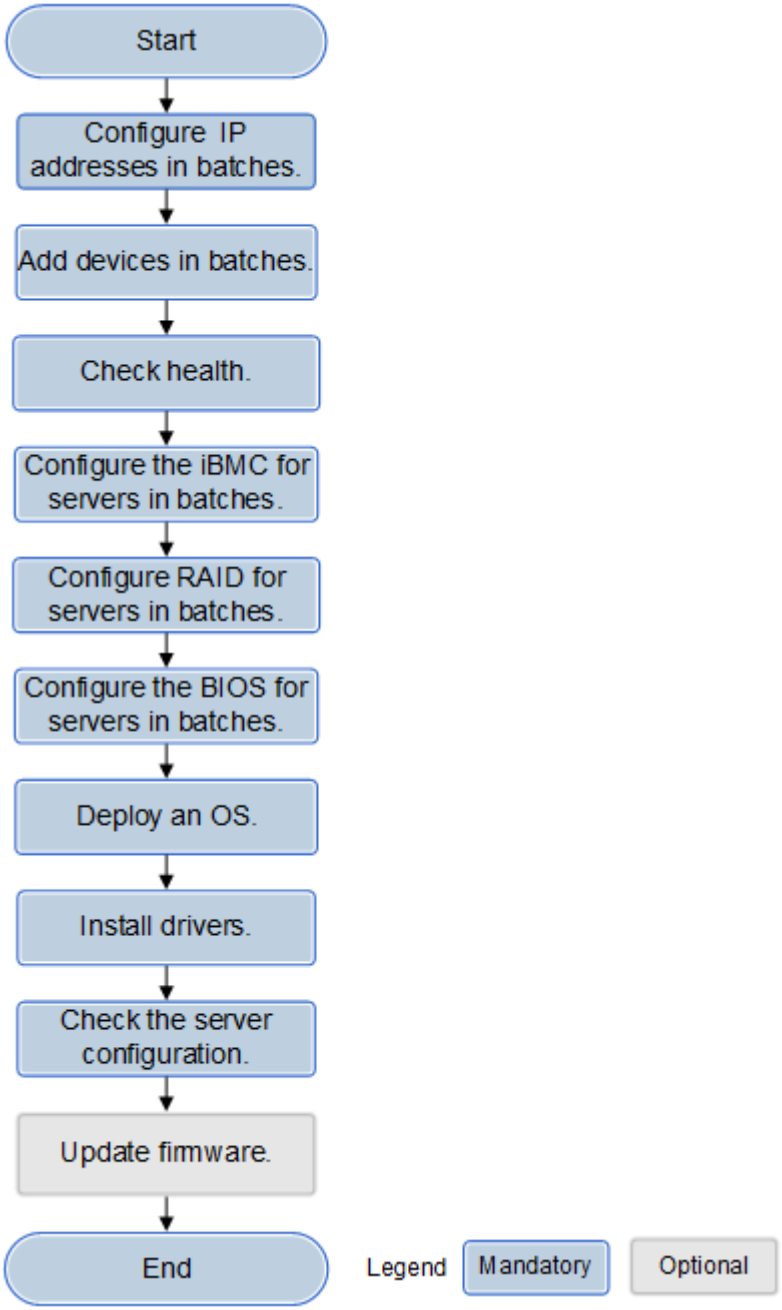
## 3.5.2 Batch Deployment

NOTE

Use FusionServer Tools for one-click deployment. For details, see "Using FusionServer Tools > One-Click Deployment" in the *FusionServer Tools User Guide* of corresponding version.

**Figure 3-3** Batch deployment process




For details about batch deployment, see the *FusionServer Tools User Guide* of corresponding version. **Table 3-3** lists the reference path of each step.

**Table 3-3** Reference paths

| Procedure | Reference Path |
| --- | --- |
| Configure IP address in batches. | Using FusionServer Tools > Configuring IP Address Information |

| Procedure | Reference Path |
| --- | --- |
| Add devices in batches. | Using FusionServer Tools > Health Check > Selecting Devices |
| Check system health. | Using FusionServer Tools > Health Check |
| Configure the iBMC for servers in batches. | Using FusionServer Tools > Hardware Configuration > Configuring the iBMC |
| Configure RAID for servers in batches. | Using FusionServer Tools > Hardware Configuration > Configuring the RAID |
| Configure the BIOS for servers in batches. | Using FusionServer Tools > Hardware Configuration > Configuring the BIOS |
| Deploying an OS. | Using FusionServer Tools > Fusion Deployment > OS Deployment |
| Installing drivers | For details about how to install drivers, visit the **Technical Support Website** > **Software Download** > **FusionServer iDriver** to access the **Readme** file in the driver package.<br>**NOTICE**<br>If the card driver is not released on iDriver, download the driver package and guide from the official website of the card vendor and manually install and upgrade the driver according to the guide. |
| Check the server configuration. | Using FusionServer Tools > Configuration Check |
| Update firmware. | Using FusionServer Tools > Bundle Upgrade |
| Update the PCIe card or drive firmware. | Using FusionServer Tools > Bundle Upgrade |

## 3.5.3 Single-Node Deployment

This section uses the 1288H V5 server as an example.

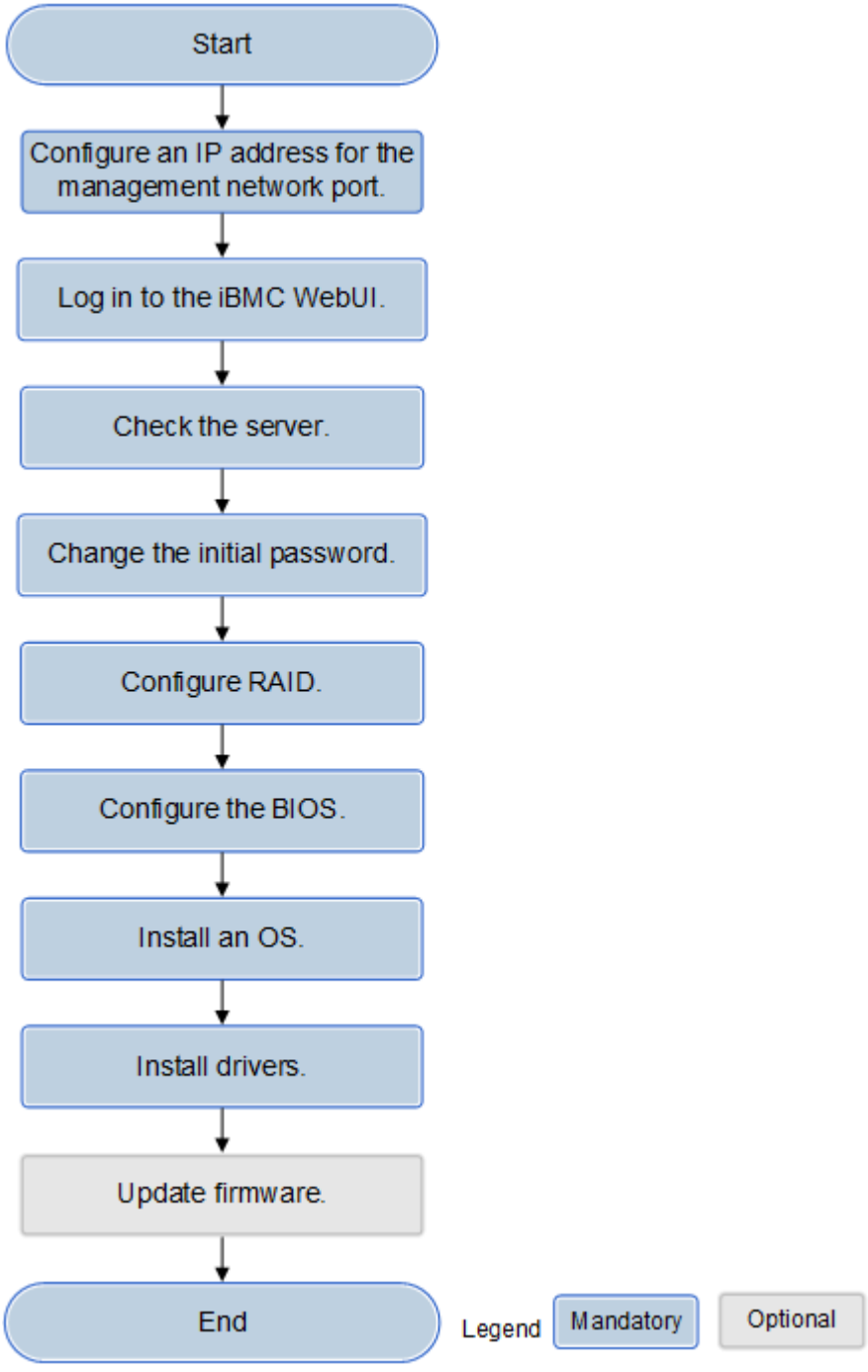
### 3.5.3.1 Single-Node Deployment Process

NOTE

Use FusionServer Tools for one-click deployment. For details, see "Using FusionServer Tools > One-Click Deployment" in the *FusionServer Tools User Guide* of corresponding version.

**Figure 3-4** Single-node deployment process




### 3.5.3.2 Configuring the IP Address for the Management Network Port

You can set the IP address using any of the following methods:

- Use the iBMC WebUI. For details, see the *iBMC User Guide* of corresponding server model.
- Use the iBMC CLI. Run the ipmcset -d ipaddr command to configure the IP address of the management network port. For details, see the *iBMC User Guide* of corresponding server model.

- Use the BIOS. For details, see the *BIOS Parameter Reference* of corresponding server model.
- Use the FusionServer Tools. For details, see the *FusionServer Tools User Guide* of corresponding version.
- Use the LCD (applicable only to the servers configured with LCD). For details, see **3.5.3.2.1 Setting the IP Address for the Management Network Port Using the LCD**.

### 3.5.3.2.1 Setting the IP Address for the Management Network Port Using the LCD

This section applies only to the servers configured with LCD.

**Step 1** On the LCD, tap the **Setting** tab.

The Setting screen is displayed, as shown in **Figure 3-5**.

**Figure 3-5** Setting screen


**Step 2** Click the **Mgmtport** tab.

The **Mgmtport** screen is displayed.

**Step 3** Set an IP address for the management network port.

NOTE

The soft keyboard is displayed when you tap the text box. Use the soft keyboard to set IP address information or tap **Cancel** to return to the **Mgmtport** screen.

**----End**

## 3.5.3.3 Logging In to the iBMC WebUI

For details about the system configuration requirements of the local PC, see "Before You Start > Login Precautions" in the *iBMC User Guide* of corresponding server model.

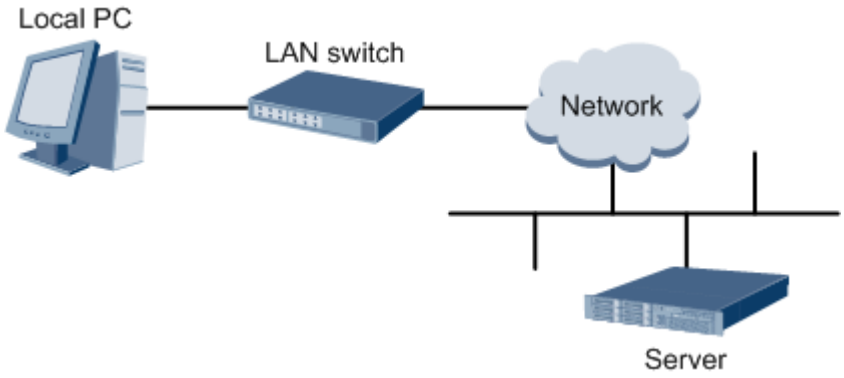
NOTE

This section describes how to log in to the iBMC WebUI by connecting the local PC to the iBMC management network port of the server using a network cable. For details about how to log in to the iBMC WebUI in other modes, see the *User Guide* of corresponding server.

**Step 1** Configure the IP address of the local PC so that the PC can communicate with the iBMC management network port.

**Figure 3-6** shows the network diagram.

**Figure 3-6** Network diagram




**Step 2** Open Internet Explorer on the local PC.

**Step 3** In the address box, enter the IP address of iBMC in the format of **https://***IP address of the server iBMC management network port*, for example, **https://192.168.2.100**.

**Step 4** Press **Enter**.

The iBMC login page is displayed, as shown in **Figure 3-7** and **Figure 3-8**.

NOTE

- If the message "There is a problem with this website's security certificate" is displayed, click **Continue to this website (not recommended)**.
- If the **Security Alert** dialog box indicating a certificate error is displayed, click **Yes**.

**Figure 3-7** iBMC login page (earlier than V561)

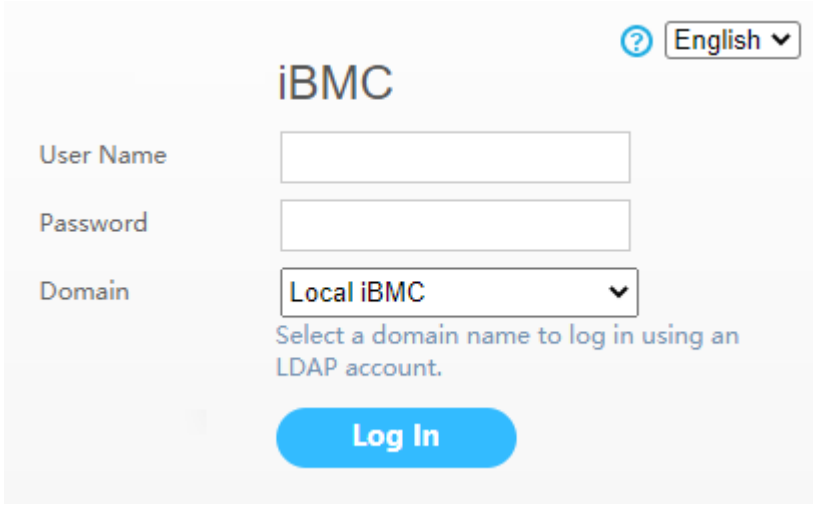


**Figure 3-8** iBMC login page (V561 or later, or V3.01.00.00 or later)


**Step 5** On the iBMC login page, enter the user name and password.

NOTE

The user account will be locked after five consecutive login failures with wrong passwords. If your user account is locked, log in again 5 minutes later.

**Step 6** Select **This iBMC** from the **Domain** drop-down list.

**Step 7** Click **Log In**.

**----End**

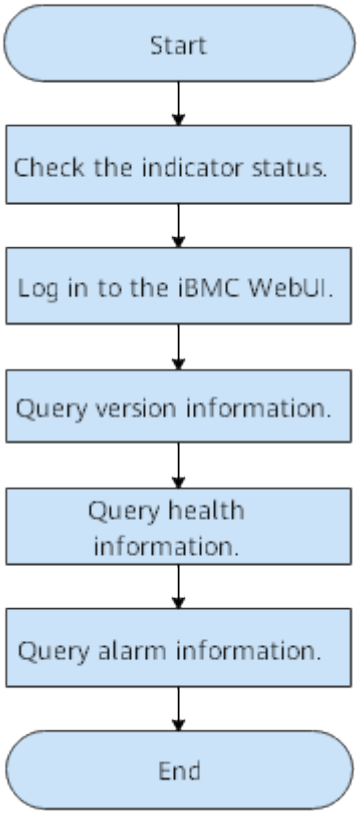
### 3.5.3.4 Checking the Server

## Operation Process

Check the server in the sequence shown in **Figure 3-9**.

For details about the commands involved in the operations, see the *iBMC User Guide* of corresponding server model.

**Figure 3-9** Check process




## Procedure

**Step 1** Check indicator status.

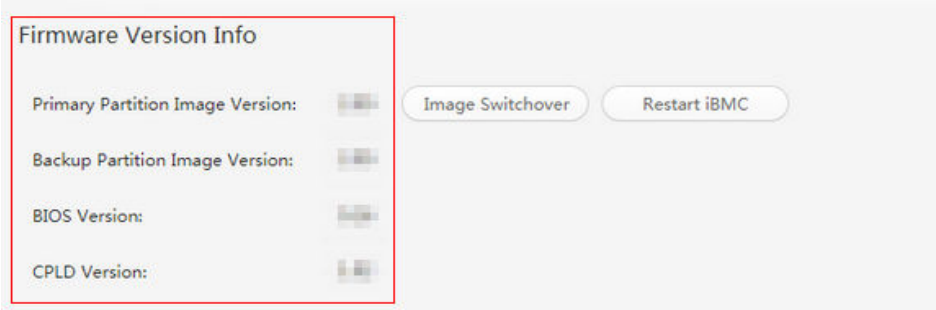
Observe the indicator status of the server. For details, see the indicator description in the *User Guide* of corresponding server model..

**Step 2** Check the server using the iBMC WebUI.

1. Log in to the iBMC WebUI. For details, see **3.5.3.3 Logging In to the iBMC WebUI**.
2. Check the server firmware version and ensure that the server firmware version meets site requirements.
   - If the iBMC version is earlier than V561, choose **System** > **Firmware Upgrade**. The window shown in **Figure 3-10** is displayed.

**Figure 3-10** Querying firmware information (iBMC earlier than V561)



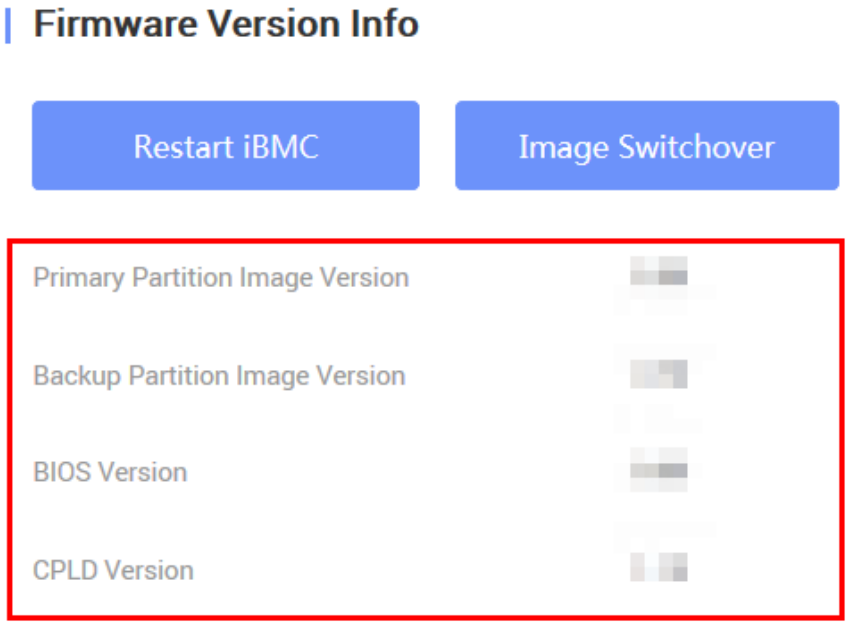

NOTE

The iBMC, BIOS, and CPLD version information is displayed.

- **Primary Partition Image Version** is the current iBMC version.
- **BIOS Version** is the current BIOS version.
- **CPLD Version** is the current CPLD version.

– If the iBMC version is V561 or later, choose **iBMC Settings** > **Firmware Upgrade**. The page shown in **Figure 3-11** is displayed.

**Figure 3-11** Querying version information (iBMC V561 or later)



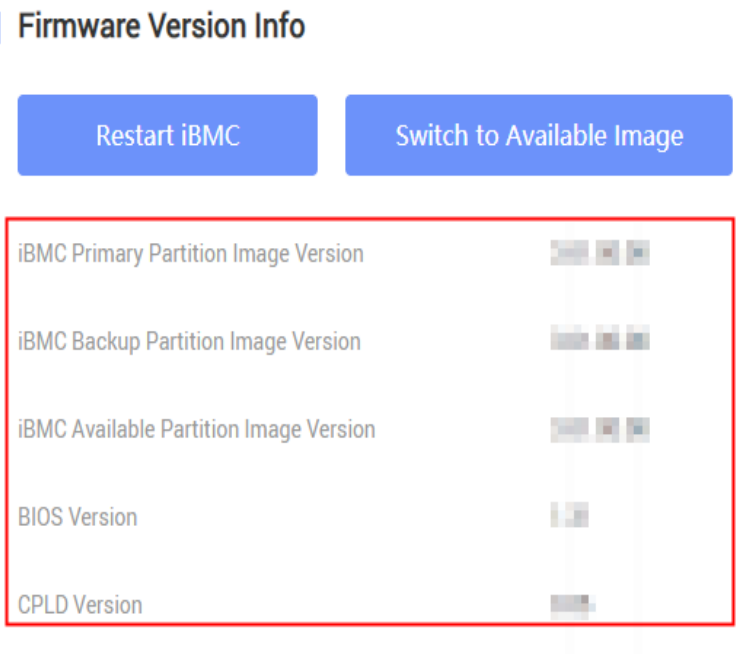
NOTE

The iBMC, BIOS, and CPLD version information is displayed.

- **Primary Partition Image Version** is the current iBMC version.
- **BIOS Version** is the current BIOS version.
- **CPLD Version** is the current CPLD version.

– If the iBMC version is V3.01.00.00 or later, choose iBMC Settings > Firmware Upgrade. The page shown in **Figure 3-12** is displayed.

**Figure 3-12** Querying version information (iBMC V3.01.00.00 or later)




NOTE

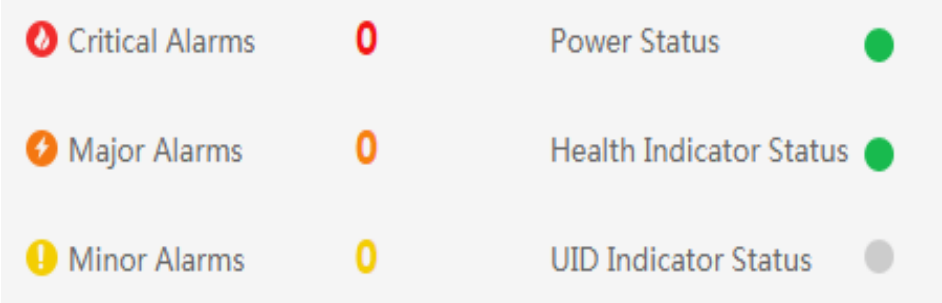
The iBMC, BIOS, and CPLD version information is displayed.

- **Primary Partition Image Version** is the current iBMC version.
- **BIOS Version** is the current BIOS version.
- **CPLD Version** is the current CPLD version.

3. Check the health status of the server.
   – If the iBMC version is V561 or earlier, choose **Information** > **Overview**. The page shown in **Figure 3-13** is displayed.

**Figure 3-13** Querying alarm information (iBMC earlier than V561)

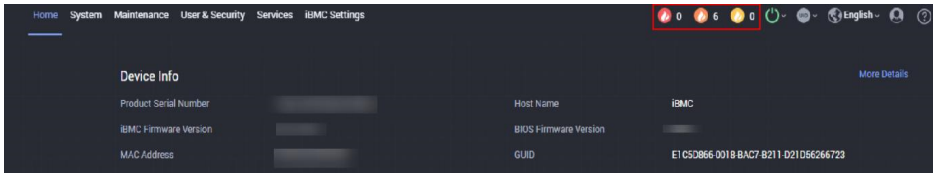



– If the iBMC version is V561 or later, view **Alarm Statistics** on the **Home** page, as shown in **Figure 3-14**.

**Figure 3-14** Querying alarm information (iBMC V561 or later)


– If the iBMC version is V3.01.00.00 or later, view alarm information in the upper right corner of the **Home** page, as shown in **Figure 3-15**.

**Figure 3-15** Querying alarm information (iBMC V3.01.00.00 or later)




4. Clear alarms. For details, see the *iBMC Alarm Handling* of corresponding server model.

**----End**

## 3.5.3.5 Changing Initial Passwords

Change the following initial user passwords:

- Initial password of the default iBMC user
- Initial password for the iBMC U-Boot

NOTE

- The default user name for logging in to the iBMC system is **Administrator**, and the default password is **Admin@9000**.
- U-Boot is a piece of underlying software used to configure basic settings, for example, initialize hardware devices and set up memory space mapping, to prepare for commissioning the iBMC. V6 and later servers do not support U-Boot.
- To ensure system security, change the default password upon the first login, and change the password periodically.
- You are advised to use a password that meets complexity requirements or to enable the password complexity check function.
- The password complexity check function is enabled by default.

The following describes how to change the user password on the iBMC WebUI. To change the user password on the iBMC CLI, see the *iBMC User Guide* of corresponding server model.

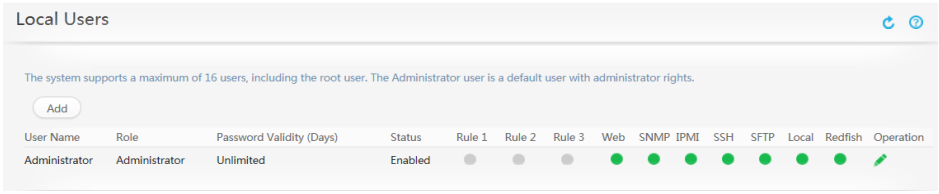
## Procedure

### Changing the Initial Password of the Default iBMC User

**Step 1** Log in to the iBMC WebUI and open the **Local User** page.

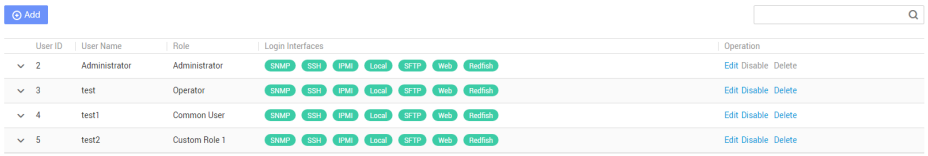
- If the iBMC version is earlier than V561, choose **Configuration** > **Local Users**. The page shown in **Figure 3-16** is displayed.

**Figure 3-16** Local Users page (iBMC earlier than V561)




- If the iBMC version is V561 or later, or V3.01.00.00 or later, choose **User & Security** > **Local Users**. The page shown in **Figure 3-17** is displayed.

**Figure 3-17** Local User page (iBMC V561 or later, or V3.01.00.00 or later)

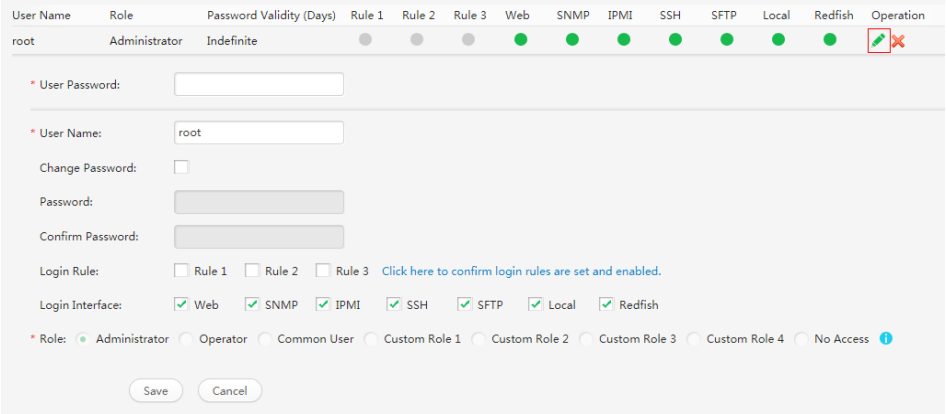



**Step 2** Modify user information.

- If the iBMC version is earlier than V561, locate the user and click . The page shown in **Figure 3-18** is displayed.

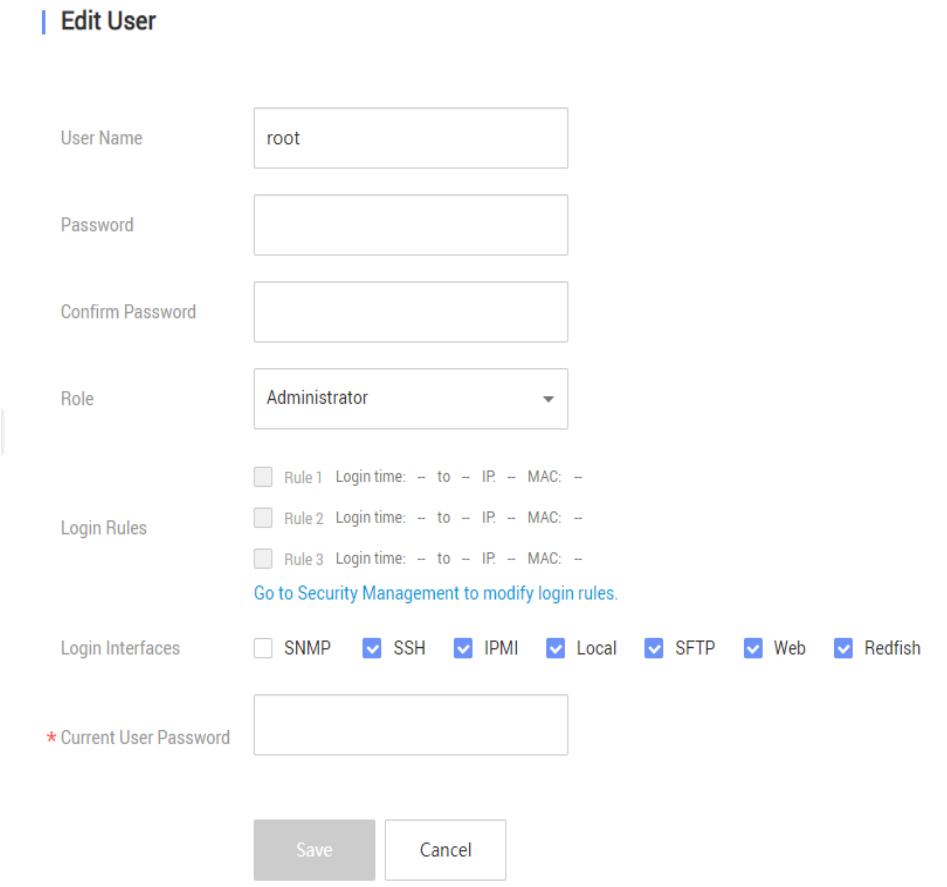
  

**Figure 3-18** Modifying user information (iBMC earlier than V561)




- If the iBMC version is V561 or later, or V3.01.00.00 or later, locate the user and click **Edit**. The page shown in **Figure 3-19** is displayed.

**Figure 3-19** Modifying user information (iBMC V561 or later, or V3.01.00.00 or later)




**Step 3** Change the user password by following on-screen instructions.

The password must meet the following complexity requirements:

- Contain 8 to 20 characters.

- Contain at least one space or one of the following special characters:
  `~!@#$%^&*()-_=+\|[{}];:'",<.>/?
- Contain at least two of the following character types:
  – Lowercase letters a to z
  – Uppercase letters A to Z
  – Digits 0 to 9
- Cannot be the same as the user name or user name in reverse order.

**----End**

**Changing the Initial Password of the iBMC U-Boot**

**Step 1** Log in to the iBMC CLI over the serial port. For details, see "Accessing the CLI" in the *iBMC User Guide* of corresponding server model.

**Step 2** Run the following command to restart the iBMC:

**iBMC:/->ipmcset -d reset**

The command output is as follows:

```
This operation will reboot IPMC system. Continue? [Y/N]:
```

**Step 3** Type **y** and press **Enter**.

The system restarts.

**Step 4** Press **Ctrl+B** immediately when the following information is displayed:

```
Hit 'ctrl + b' to stop autoboot: 1
```

**Step 5** Enter the default password for the iBMC U-Boot.

The following command output indicates that you have logged in to the U-Boot.

```
u-boot>
```

**Step 6** Run the following command to change the U-Boot password:

**u-boot> passwd**

The following information is displayed:

```
Enter old password:
```

**Step 7** Enter the old password.

The following information is displayed:

```
Enter new password:
```

**Step 8** Enter a new password. For details about password complexity requirements, see "Changing the User Password" in the *iBMC User Guide* of corresponding server model.

The following information is displayed:

```
Enter the new password again:
```

**Step 9** Enter the new password again.

If the command output is as follows, the password has been changed:

```
. done
Un-Protected 1 sectors
Erasing Flash...
. done
Erased 1 sectors
Writing to Flash... done
. done
Protected 1 sectors

password be changed successfully.
```

**Step 10** Run the following command to exit the U-Boot:

**boot**

**----End**

## 3.5.3.6 Updating Firmware

Determine whether to perform the upgrade based on the firmware version requirements. For details, see the Upgrade Guide of corresponding server model.

Before the upgrade, use **Table 3-4** to list all firmware versions and fill in the source and target versions by referring to the version mapping of each product. For details about how to obtain the version mapping, see **Table 2-15**.

NOTE

Since the servers involve a lot of components, **Table 3-4** does not list all the components. Check the components whose firmware needs to be upgraded as required.

**Table 3-4** Confirming versions before an upgrade

| Module Name | To Be Updated or Not | Source Version | Target Version |
|---|---|---|---|
| RAID controller card | Yes□ No□ | | |
| iBMC | Yes□ No□ | | |
| BIOS | Yes□ No□ | | |
| CPLD (iBMC) | Yes□ No□ | | |
| Drive backplane firmware | Yes□ No□ | | |
| PSU firmware (iBMC) | Yes□ No□ | | |
| Drive backplane CPLD (iBMC) | Yes□ No□ | | |
| ..... | | | |

#### 3.5.3.7 Configuring RAID

The RAID configuration method varies according to the RAID controller card model. For details, see *RAID Controller Card User Guide* of corresponding server model.

#### 3.5.3.8 Configuring the BIOS

For details about how to set the BIOS, see the *BIOS Parameter Reference* of corresponding server model.

#### 3.5.3.9 Installing an OS

Operating Systems Compatible with this product please visit the compatibility list on the technical support website.

For details about how to install other OSs, see the corresponding server *OS Installation Guide Cases*.

#### 3.5.3.10 Installing drivers

For details about how to install drivers, visit the **Technical Support Website** > **Software Download** > **FusionServer iDriver** to access the **Readme** file in the driver package.

NOTICE

If the card driver is not released on iDriver, download the driver package and guide from the official website of the card vendor and manually install and upgrade the driver according to the guide.

## 3.6 Backing Up Configuration Files

For details about the server models that support batch configuration backup, see the *FusionServer Tools User Guide* of corresponding version.

### 3.6.1 Batch Backup

For details, see **Configuration Check > Checking the Server Configuration > Checking the Configuration** in the *FusionServer Tools User Guide* of corresponding version.

NOTE

By default, the obtained server configuration file is stored in **C:\ProgramFiles\FusionServer Tools\tools\ServerMain\work\ConfigCheck**.

### 3.6.2 Single-Node Backup

- For iBMC earlier than V561, you can export the iBMC, BIOS, and RAID controller configuration files on the **Import/Export** page of the iBMC WebUI.

- For iBMC V561 and later, or V3.01.00.00 and later, you can export the iBMC, BIOS, and RAID controller configuration files on the **Configuration Update** page of the iBMC WebUI.

NOTE

- Only the administrator can import, export, and update configuration files.
- RAID controller card configurations take effect only after the system power-on self test (POST) is complete (the RAID controller card must support out-of-band management).
- In the configuration file exported, passwords are not displayed in plain text. If you want to import the configuration file to another server, you need to configure user passwords before importing the file.
- In the configuration file exported, the iBMC management network port IP address is commented out.

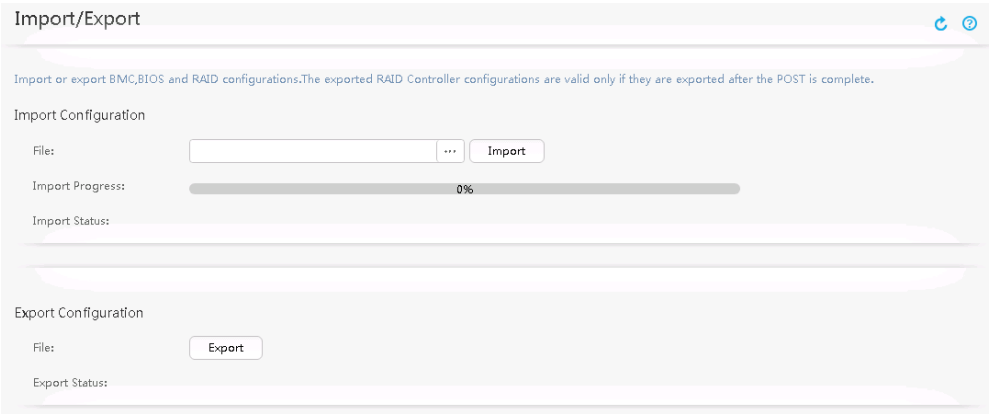
## Procedure

**Step 1** Log in to the iBMC WebUI of the server node. For details, see **3.5.3.3 Logging In to the iBMC WebUI**.

**Step 2** Open the **Import/Export** page.

- If the iBMC version is earlier than V561, choose **Configuration** > **Import/Export**. The page shown in **Figure 3-20** is displayed.

**Figure 3-20** Import/Export (iBMC earlier than V561)




- If the iBMC version is V561 or later, or V3.01.00.00 or later, choose **iBMC Settings** > **Configuration Upgrade**. The page shown in **Figure 3-21** is displayed.

**Figure 3-21** Configuration Upgrade (iBMC V561 or later, or V3.01.00.00 or later)


**Step 3** Click **Export Configuration** > **Export**.

**Step 4** Set the path for exporting the configuration file and start the export.

After the export is complete, a message is displayed, indicating that the export is successful.

**----End**

# 3.7 Accepting Products

See the acceptance guide of each product to perform acceptance tests. For details about how to obtain acceptance guides, see **Table 2-15**.

# 4 Engineering Documents to Be Handed Over

| List of Engineering Documents to Be Handed Over |
| --- |
| **Equipment Room Layout** |
| Attach the onsite equipment room layout diagram. |
| **Networking Diagram** |
| Attach the network topology of the network devices connected to the onsite servers. |
| **IP Addresses** |
| Provide the detailed IP address information after the onsite servers are configured. |
| **Backup Files** |
| Hand over the backup files to the equipment room administrator of the customer. |

# 5 Common Operations

5.1 Logging In to the Server Over a Network Port by Using PuTTY

5.2 Logging In to a Server Over a Serial Port by Using PuTTY

5.3 Logging In to the Server Using the Remote Virtual Console

5.4 Enabling and Configuring IPv6 on the Client

## 5.1 Logging In to the Server Over a Network Port by Using PuTTY

### Scenarios

You can use PuTTY to remotely log in to the server over a local area network (LAN) and to configure and maintain the server.

### Prerequisites

**Conditions**

The PC is connected to the management network port of the server using a network cable.

**Data**

The following data is required:

- IP address of the server
- Username and password for logging in to the server

**Software**

PuTTY.exe (free software)

### Procedure

1. Set an IP address and a subnet mask or add route information for the PC, and ensure that the PC can properly communicate with the server.

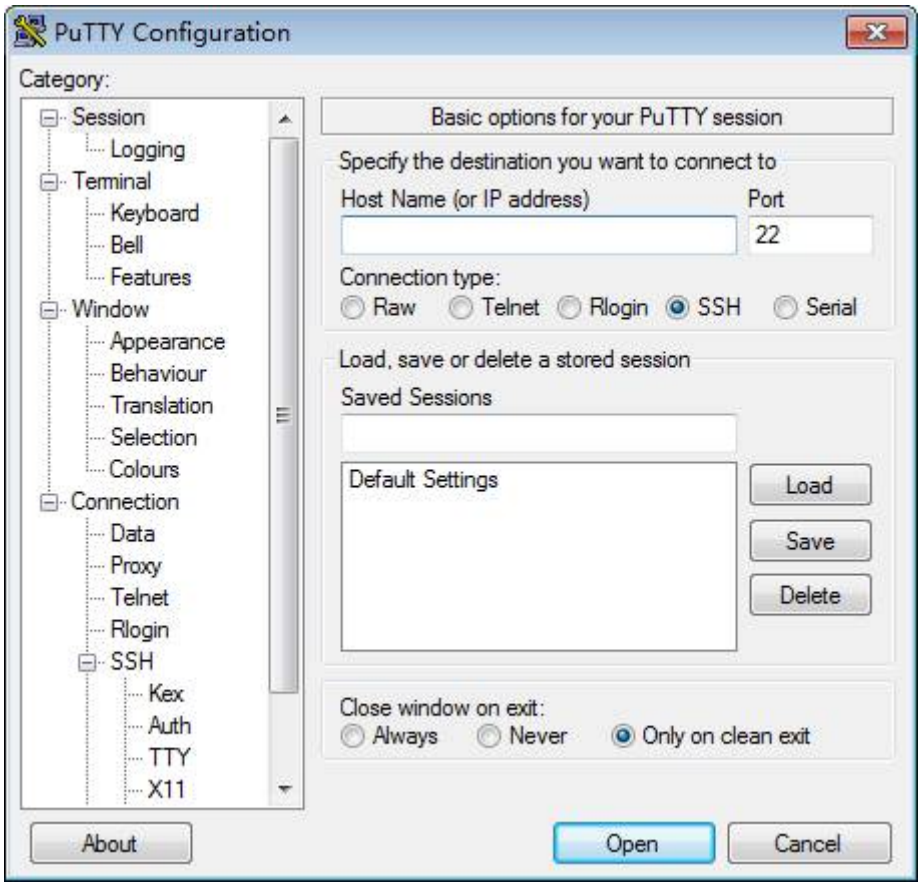
  

You can run the **Ping *server IP address*** command in the command window of the PC to check the communication between the PC and the server.

2. Double-click **PuTTY.exe**.

   The **PuTTY Configuration** window is displayed, as shown in **Figure 5-1**.

**Figure 5-1** PuTTY Configuration




3. Set login parameters.

   The command-line options are described as follows:

   – **Host Name (or IP address)**: Enter the IP address of the server, for example, **192.168.2.1**.
   – **Port**: Retain the default value **22**.
   – **Connection type**: Use the default value **SSH**.
   – **Close window on exit**: Retain the default value **Only on clean exit**.

   NOTE

   Configure **Host Name** and **Saved Sessions**, and click **Save**. In future use, you can directly double-click a saved record to log in to the serve.

4. Click **Open**.

   The **PuTTY** window is displayed.

NOTE

- If it is your first login, the **PuTTY Security Alert** window is displayed. Click **Yes**. Then the **PuTTY** window is displayed.
- If the entered user name is incorrect during server login, the PuTTY must be connected to again.

5. Enter the username and password.

   If the login is successful, the server host name is displayed on the left of the prompt.

# 5.2 Logging In to a Server Over a Serial Port by Using PuTTY

NOTE

By default, the server serial port is the OS serial port. For details about how to redirect the server serial port, see "Querying and Redirecting the Serial Port (serialdir)" in the *iBMC User Guide*.

## Scenarios

Use PuTTY to log in to the server over a serial port in either of the following scenarios:

- The server is configured for the first time at a new site. You need to use a local PC to log in to the server over a serial port to configure initialization.
- A remote connection to the server cannot be established. You can log in to the server over a serial port to locate faults.

NOTE

The server in this section can be a management module, compute node, or switching plane.

## Prerequisites

**Conditions**

- The PC is connected to the management network port of the server using a serial cable.
- PuTTY 0.60 or later has been installed.

**Data**

Username and password for logging in to the server.

**Software**

PuTTY.exe: This tool is third-party software. You need to obtain it by yourself. PuTTY 0.60 or later is required for login over a serial port.

## Procedure

**Step 1** Double-click **PuTTY.exe**.

The **PuTTY Configuration** window is displayed.

**Step 2** In the navigation tree, choose **Connection > Serial**.

**Step 3** Set the login parameters.

The command-line options are described as follows:

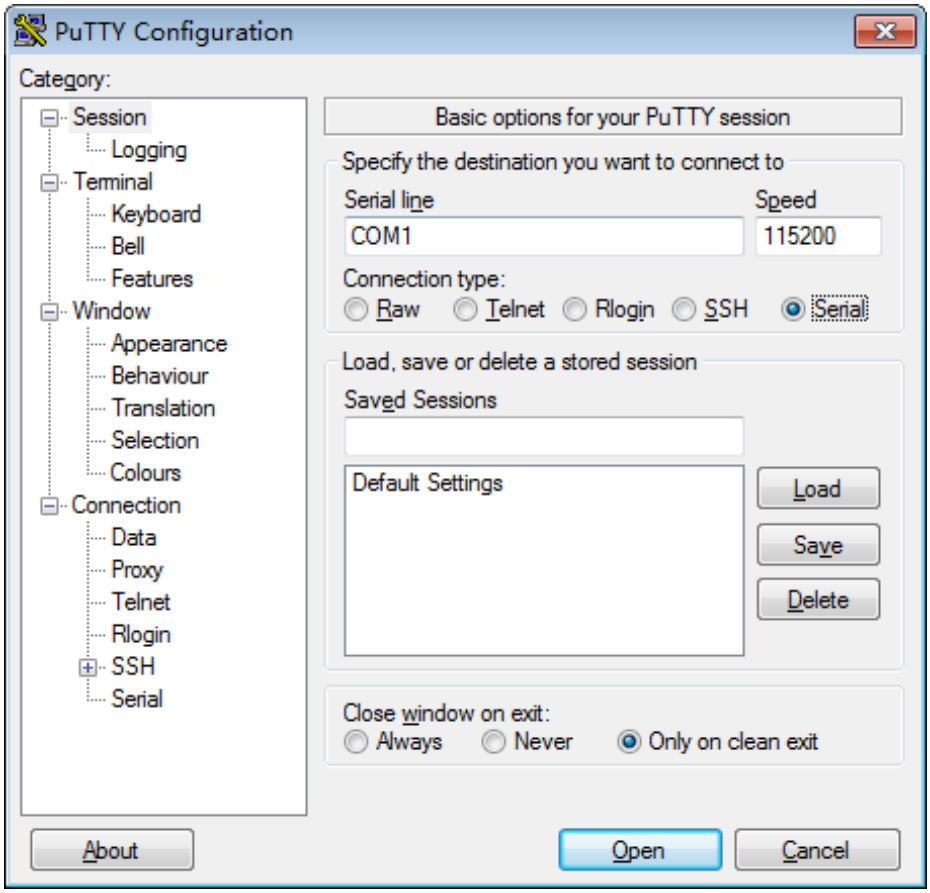
- Serial Line to connect to: COMn
- Speed (baud): 115200
- Data bits: 8
- Stop bits: 1
- Parity: None
- Flow control: None

*n* indicates the serial port number, which is an integer.

**Step 4** In the navigation tree, choose **Session**.

**Step 5** Choose **Connection type** to **Serial**, as shown in **Figure 5-2**.

**Figure 5-2** PuTTY Configuration




**Step 6** Click **Open**.

The **PuTTY** window is displayed.

**Step 7** Enter the username and password.

If the login is successful, the server host name is displayed on the left of the prompt.

**----End**

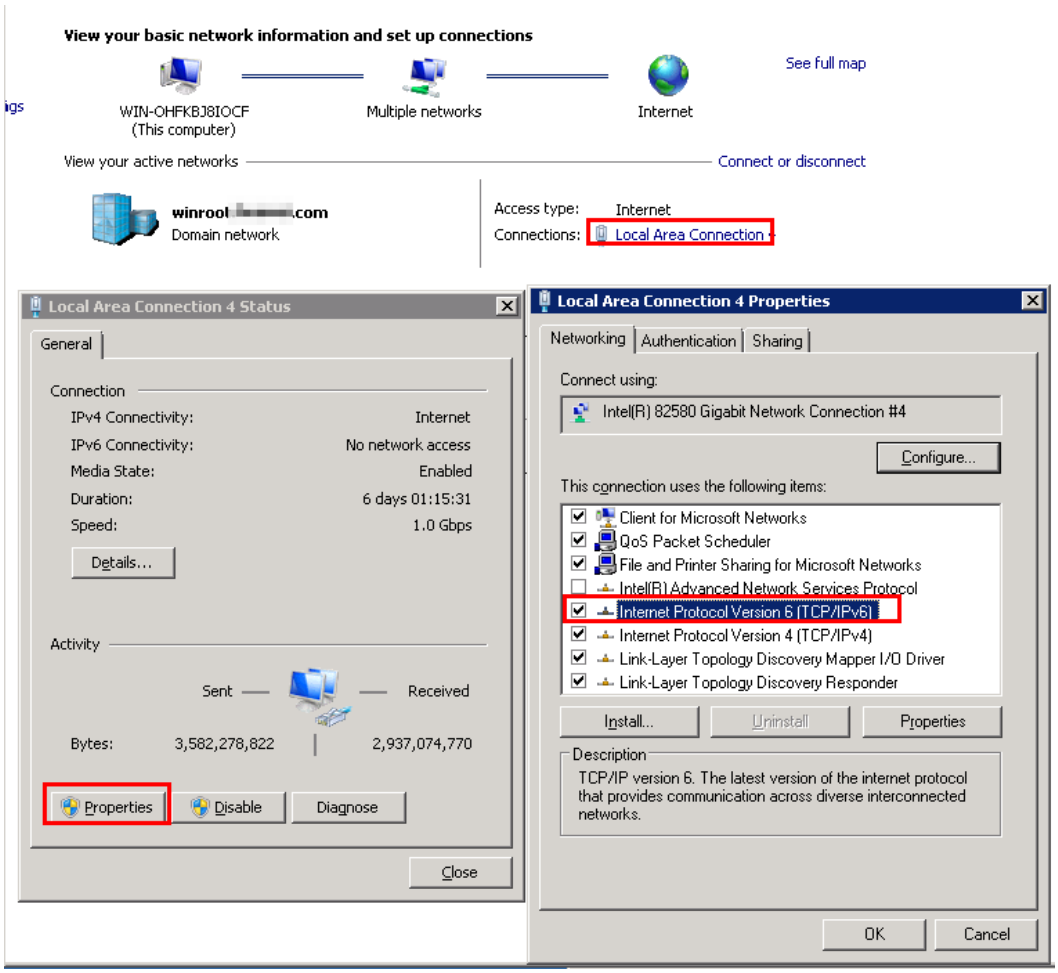
# 5.3 Logging In to the Server Using the Remote Virtual Console

For details, see section "Logging In to a Server Using the Remote Virtual Console" in the *Server User Guide*. For details about how to obtain the *Server User Guide*, see **Table 2-15**.

# 5.4 Enabling and Configuring IPv6 on the Client

In this section, Windows 7 is used as an example to describe how to enable and configure the IPv6 function.

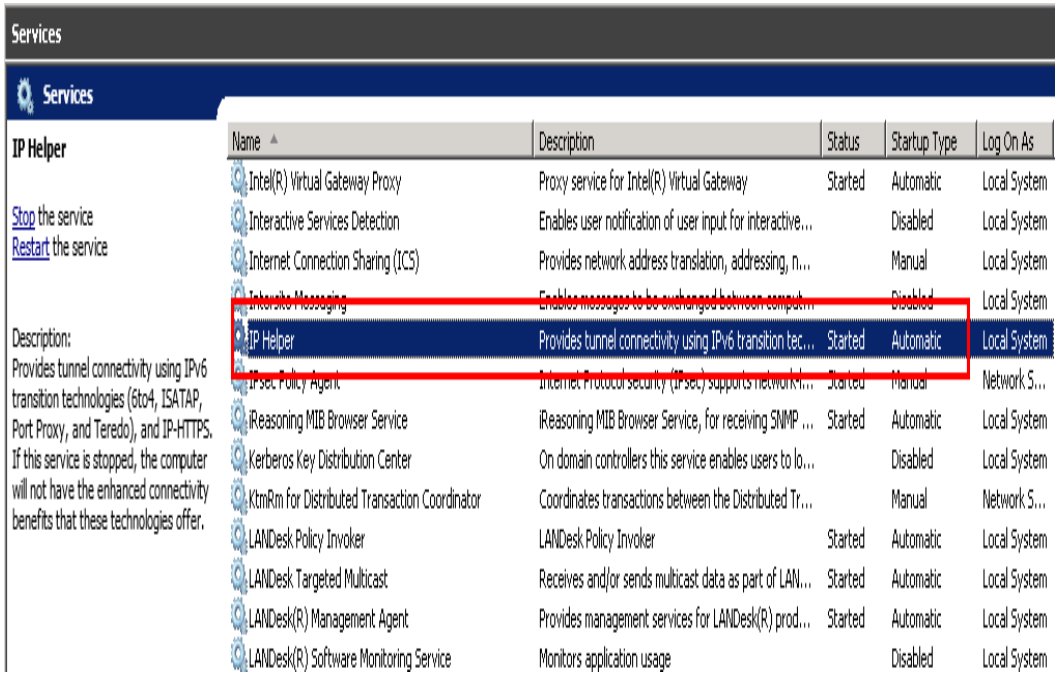
**Step 1** Open the Internet and sharing center, and select **Local Area Connection > Properties** to ensure that **Internet Protocol Version 6 (TCP/IPv6)** is selected.




**Step 2** On the cmd, run the **services.msc** command and set parameters of **IP Helper**: set **Status** to **Started** and **Startup Type** to **Automatic**.

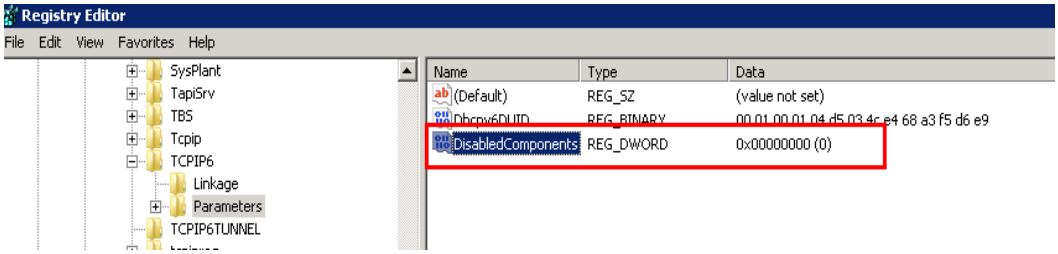
  

**Figure 5-3** IP Helper




**Step 3** On the cmd, run the **regedit** command and find **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\TCPIP6\Parameters**. Set **DisabledComponents** to **0**.

**Figure 5-4** DisabledComponents




**Step 4** Restart the PC.

**Step 5** On the cmd, run the **ipconfig** command to check whether an IPv6 address exists in the local connection. If the IPv6 address exists, the IPv6 function is successfully enabled.

NOTE

If the IP address configuration still fails and an error message is displayed indicating that the connection fails after the IPv6 function is enabled, disable irrelevant networks and configure the IP address again.

**Step 6** When the IPv6 function is successfully enabled, choose **Local Area Connection > Properties > Internet Protocol Version 6 (TCP/IPv6) > Properties** and configure the IPv6 function. If the PC communicates with the servers properly, the IPv6 function is configured successfully.

**----End**

# 6 More Information

6.1 Obtaining Technical Support

6.2 Product Information Resources

6.3 Product Configuration Resources

6.4 Maintenance Tools

## 6.1 Obtaining Technical Support

xFusion Digital Technologies Co., Ltd. provides timely and effective support for users through local branch offices, secondary technical support system, telephone technical support, remote and on-site technical services.

### Technical Support Website

Technical documents are available at **xFusion website**.

### Case Library

To obtain case study about servers, visit **Knowledge Base**.

### Technical Support

xFusion provides comprehensive technical support and services. To obtain assistance, contact xFusion technical support as follows:

- Contact Hyper-Fusion Digital Technologies Co., Ltd. Technical Support Center.
  - Customers in China can contact us on:
    - Telephone: 400-009-8999
    - Email: **support@xfusion.com**
  - Global customers can contact us on **Global Service Hotline**.
- Contact technical support personnel at your local xFusion branch office.

# 6.2 Product Information Resources

**Table 6-1** Product information resources

| Item | Description | How to Obtain |
| --- | --- | --- |
| Server product documentation | Documents that provide information about the structure, specifications, installation and removal of components, installation of software, and server configuration. | On the technical support website, click the product model to access the product page. On the Documentation tab, view the information. |
| Compatibility List | A tool used to query the OSs, components, and peripherals compatible with a server. | Visit the **Technical Support Website** > **Compatibility List**. |
| Warranty Query | A system used to query service information about servers. | Visit the **Technical Support Website** > **Maintenance Status**. |
| Power Calculator | A tool used to calculate server power consumption based on the server configuration. | Visit the **Technical Support Website** > **Power Calculator**. |
| 3D Model | View the server hardware 3D structure. | Visit the **Technical Support Website** > **3D Model**. |

# 6.3 Product Configuration Resources

**Table 6-2** Product configuration resources

| Tool | Description | How to Obtain |
| --- | --- | --- |
| Server removal and installation videos | Show how to remove and install server hardware. | Visit the **Technical Support Website** > **Service Support** > **Multimedia Portal**. |
| Memory Configuration Guide | Displays the DIMM installation sequence in a graphical manner after you select the server model, CPU quantity, and DIMM quantity. | Visit the **Technical Support Website** > **Online Tools** > **Server Assembly Guide**. |

# 6.4 Maintenance Tools

**Table 6-3** Software tools for routine maintenance

| Tool | Server Model and Software Version | Description |
| --- | --- | --- |
| FusionServer Tools | For details, see the *FusionServer Tools User Guide* of the corresponding version. | Used for new site deployment and delivery, troubleshooting, and firmware upgrade.<br>Visit the **Technical Support Website** > **Software Download** > **FusionServer Tools**. |
| Smart Provisioning | For details, see the *Smart Provisioning User Guide* of the corresponding version. | Used to install OSs without a physical DVD-ROM drive, configure RAID, upgrade firmware, and perform troubleshooting.<br>Visit the **Technical Support Website** > **Software Download** > **Smart Provisioning**. |