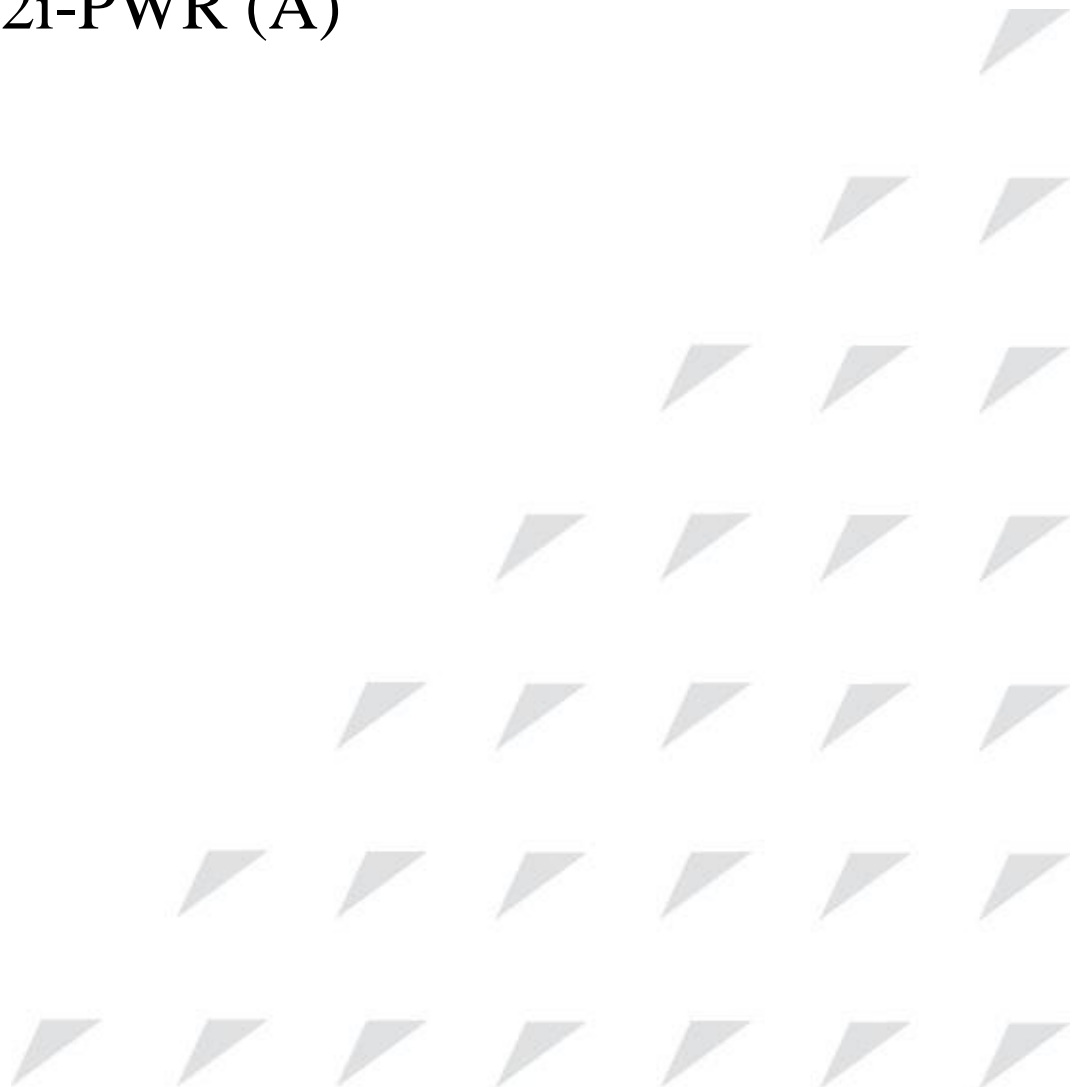


[www.raisecom.com](http://www.raisecom.com)

**Gazelle S1512i-PWR (A)**  
**User Manual**  
**(Rel\_02)**



Raisecom Technology Co., Ltd. provides customers with comprehensive technical support and services. For any assistance, please contact our local office or company headquarters.

Website: <http://www.raisecom.com>

Tel: 8610-82883305

Fax: 8610-82883056

Email: [export@raisecom.com](mailto:export@raisecom.com)

Address: Raisecom Building, No. 11, East Area, No. 10 Block, East Xibeiwang Road, Haidian District, Beijing, P.R.China

Postal code: 100094

---

## Notice

Copyright © 2018

Raisecom

All rights reserved.

No part of this publication may be excerpted, reproduced, translated or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in Writing from **Raisecom Technology Co., Ltd.**

**RAISECOM** is the trademark of Raisecom Technology Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

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

# Preface

---

## Objectives

This document describes overview, hardware structure, technical specifications, serial server features, hardware installation, networking application, and management and maintenance of the Gazelle S1512i-PWR. The appendix lists terms, acronyms, and abbreviations involved in this document.

## Versions




The following table lists the product versions related to this document.


Product name	Product version	Software version	Hardware version
Gazelle S1512i-4GF-8GE-PWR	P100R001	V3.41 or later	A.00 or later

## Conventions

### Symbol conventions

The symbols that may be found in this document are defined as below.

Symbol	Description
 <b>Warning</b>	Indicate a hazard with a medium or low level of risk which, if not avoided, could result in minor or moderate injury.
 <b>Caution</b>	Indicate a potentially hazardous situation that, if not avoided, could cause equipment damage, data loss, and performance degradation, or unexpected results.
 <b>Note</b>	Provide additional information to emphasize or supplement important points of the main text.

Symbol	Description
	Indicate a tip that may help you solve a problem or save time.

## General conventions

Convention	Description
Times New Roman	Normal paragraphs are in Times New Roman.
Arial	Paragraphs in Warning, Caution, Notes, and Tip are in Arial.
<b>Boldface</b>	Buttons and navigation path are in <b>Boldface</b> .
<i>Italic</i>	Book titles are in <i>italics</i> .
Lucida Console	Terminal display is in Lucida Console.
Book Antiqua	Heading 1, Heading 2, Heading 3, and Block are in Book Antiqua.

## Change history

Updates between document versions are cumulative. Therefore, the latest document version contains all updates made to previous versions.

### Issue 02 (2018-05-31)

Second commercial release

- Fixed known bugs.

### Issue 01 (2018-02-26)

Initial commercial release

---

# Contents

---

<b>1 Overview.....</b>	<b>1</b>
1.1 Introduction.....	1
1.2 Characteristics.....	2
1.2.1 High reliability.....	2
1.2.2 Various interface types.....	2
1.2.3 Powerful PoE power supply.....	3
1.2.4 Flexible networking performance.....	3
1.2.5 Strict QoS.....	3
1.2.6 Complete security guarantee.....	3
1.2.7 Comprehensive management modes.....	4
1.3 Models.....	4
1.4 Software features.....	4
1.5 Networking applications.....	6
<b>2 Hardware structure.....</b>	<b>8</b>
2.1 Appearance.....	8
2.1.1 Front appearance.....	8
2.1.2 Top appearance.....	9
2.1.3 Rear appearance.....	10
2.2 Interfaces.....	11
2.2.1 Service interfaces.....	11
2.2.2 RJ45 Console interface.....	11
2.2.3 Management and auxiliary interfaces.....	12
2.3 Button.....	12
2.4 LEDs.....	13
2.5 Power supply.....	14
2.5.1 Introduction.....	14
2.5.2 Appearance and interfaces.....	14
<b>3 Interfaces and modules.....</b>	<b>15</b>
3.1 Interfaces.....	15
3.1.1 1000BASE-X SFP optical interface.....	15
3.1.2 1000BASE-T electrical interface.....	15
3.1.3 RJ45 Console interface.....	16

---

3.1.4 Alarm output interface .....	16
3.1.5 DI interface .....	17
3.2 SFP modules.....	18
3.2.1 Dual-fiber bidirectional (LC/PC) .....	19
3.2.2 Single-fiber bidirectional (LC/PC).....	19
<b>4 Cables .....</b>	<b>20</b>
4.1 Ground cable .....	20
4.1.1 Introduction.....	20
4.1.2 Appearance.....	20
4.1.3 Technical specifications .....	21
4.2 DC power cable .....	22
4.2.1 Introduction.....	22
4.2.2 Appearance.....	22
4.2.3 Technical specifications .....	23
4.3 Ethernet cable.....	23
4.3.1 Introduction.....	23
4.3.2 Appearance.....	24
4.3.3 Technical specifications .....	24
4.4 Fiber .....	27
4.4.1 Introduction.....	27
4.4.2 Appearance.....	27
4.4.3 Wiring .....	28
4.5 Digital input cable .....	28
4.5.1 Introduction.....	28
4.5.2 Appearance.....	29
4.5.3 Technical specifications .....	29
4.6 Alarm cable .....	30
4.6.1 Introduction.....	30
4.6.2 Appearance.....	30
4.6.3 Technical specifications .....	30
<b>5 Technical specifications.....</b>	<b>31</b>
5.1 Overall parameters .....	31
5.2 Protocols and standards .....	32
5.2.1 Compliant communication protocols and standard .....	32
5.2.2 Laser safety class .....	32
5.2.3 Reliability indexes .....	32
5.2.4 EMC standards.....	33
5.2.5 Environmental standards.....	33
<b>6 Hardware installation.....</b>	<b>34</b>
6.1 Preparing for installation .....	34
6.1.1 Enviromental conditions .....	34

---

---

6.1.2 Power conditions .....	34
6.1.3 Electrostatic conditions .....	35
6.1.4 Grounding conditions .....	35
6.1.5 Other conditions .....	35
6.1.6 Precautions for unpacking .....	35
6.2 Installing device .....	35
6.2.1 Installing device on guide rail .....	35
6.2.2 Installing device on wall .....	37
6.3 Grounding device .....	38
6.4 Connecting cables .....	39
6.4.1 Connecting LC/PC fiber .....	39
6.4.2 Connecting Ethernet cable .....	40
6.4.3 Connecting power cable .....	40
6.5 Powering on device .....	41
6.6 Checking installation .....	41
<b>7 Management and maintenance .....</b>	<b>43</b>
7.1 Management modes .....	43
7.1.1 CLI .....	43
7.1.2 Web .....	44
7.1.3 SNMP .....	44
7.2 Maintenance methods .....	44
7.2.1 Ping .....	44
7.2.2 Traceroute .....	45
7.2.3 Enviromental monitoring .....	45
7.2.4 RMON management .....	45
7.2.5 System log .....	45
7.2.6 Watchdog .....	45
7.2.7 Port mirroring .....	45
7.3 Troubleshooting strategy .....	46
7.4 NView NNM system .....	46
7.4.1 Functions .....	46
7.4.2 Features .....	47
<b>8 Appendix .....</b>	<b>49</b>
8.1 Terms .....	49
8.2 Acronyms and abbreviations .....	54

# Figures

---

Figure 1-1 Appearance .....	2
Figure 1-2 Security protection and monitoring application with the device .....	7
Figure 2-1 Front appearance .....	9
Figure 2-2 Top appearance .....	10
Figure 2-3 Rear appearance.....	11
Figure 2-4 Appearance of the DC power interface.....	14
Figure 3-1 Alarm output interface on the DC power model.....	17
Figure 3-2 DI interface.....	17
Figure 4-1 Ground cable .....	21
Figure 4-2 OT terminal .....	21
Figure 4-3 DC power cable .....	23
Figure 4-4 Ethernet cable.....	24
Figure 4-5 Wiring of the straight-through cable.....	25
Figure 4-6 Wiring of the 100 Mbit/s crossover cable.....	26
Figure 4-7 Wiring of the 1000 Mbit/s crossover cable.....	26
Figure 4-8 LC/PC fiber connector.....	28
Figure 4-9 Alarm interface .....	29
Figure 4-10 Alarm output interface.....	30
Figure 6-1 Connecting the rail clip to the guide rail.....	36
Figure 6-2 Installing the rail clip to the guide rail.....	36
Figure 6-3 Installing the device on the guide rail.....	37
Figure 6-4 Removing the rail clip .....	37
Figure 6-5 Installing the wall-mount bracket to the rear panel of the device .....	38
Figure 6-6 Installing the wall-mount bracket on the wall .....	38
Figure 6-7 Unfastening the screw of the ground terminal.....	39
Figure 6-8 Connecting the ground cable .....	39



---

Figure 6-9 Connecting the Ethernet cable .....	40
Figure 6-10 Connecting the connector of the DC power cable .....	41
Figure 6-11 Fastening screws of the DC power cable .....	41
Figure 7-1 Orientation of the NView NNM system .....	48

# Tables

---

Table 1-1 Model .....	4
Table 1-2 Software features.....	5
Table 2-1 Interfaces .....	11
Table 2-2 Parameters of the RJ45 Console interface.....	12
Table 2-3 Management and auxiliary interfaces.....	12
Table 2-4 Button.....	12
Table 2-5 LEDs .....	13
Table 2-6 DC power interface .....	14
Table 3-1 Parameters of the 1000BASE-X SFP optical interface .....	15
Table 3-2 Parameters of the 1000BASE-T electrical interface.....	15
Table 3-3 Parameters of the RJ45 Console interface.....	16
Table 3-4 Parameters of the alarm output interface.....	17
Table 3-5 PINs of the DI interface .....	17
Table 3-6 Configuring triggering condition .....	18
Table 3-7 Parameters of the DI interface.....	18
Table 3-8 Parameters of GE (1250 Mbit/s) dual-fiber bidirectional optical modules .....	19
Table 3-9 Parameters of GE (1250 Mbit/s) single-fiber bidirectional optical modules.....	19
Table 4-1 Technical specifications of the ground cable.....	21
Table 4-2 Technical specifications of the OT terminal.....	22
Table 4-3 Technical specifications of the DC power cable .....	23
Table 4-4 Wiring of EIA/TIA 568A and EIA/TIA 568B standards .....	24
Table 4-5 Technical specifications of the Ethernet cable .....	24
Table 4-6 Type and usage of the fiber .....	27
Table 4-7 Wiring of the fiber.....	28
Table 4-8 Digital input interface .....	29
Table 4-9 Technical specifications of the digital input cable.....	29

---

Table 4-10 Technical specifications of the alarm cable .....	30
Table 5-1 Overall parameters .....	31
Table 5-2 Reliability indexes.....	32
Table 5-3 Environmental requirements .....	33
Table 6-1 Power conditions .....	34
Table 6-2 Items to be checked after installation .....	42
Table 7-1 Troubleshooting strategy .....	46

# 1 Overview

---

This chapter describes basic information about the Gazelle S1512i-PWR, including the following sections:

- Introduction
- Characteristics
- Models
- Software features
- Networking applications

## 1.1 Introduction

The all-1000 Mbit/s guide-rail Power over Ethernet (PoE) industrial Ethernet switch Gazelle S1512i-4GF-8GE-PWR (hereinafter referred to as the Gazelle S1512i-PWR) is characterized by all-1000 Mbit/s interfaces, guide-rail chassis, all-metal shell, fanless design for heat dissipation (with cooling fins), small size, low power consumption, and easy installation. It can meet requirements for guide-rail switches in scenarios, such as the smart city and places with high-electromagnetic interference and difficulty in taking power.

The Gazelle S1512i-PWR provides four 1000 Mbit/s SFP optical interfaces and eight 1000 Mbit/s PoE RJ45 electrical interfaces. These PoE interfaces can supply 15 W or 30 W power. The Gazelle S1512i-PWR adopts guide-rail installation, or can be installed on a wall.

Figure 1-1 shows appearance of the Gazelle S1512i-PWR

Figure 1-1 Appearance



## 1.2 Characteristics

### 1.2.1 High reliability

The Gazelle S1512i-PWR is characterized by high reliability:

- Possess a guide-rail chassis, all-metal shell, and fanless heat dissipation design.
- Support IP30 protection level.
- Support wide-temperature working environment with the operating temperature in the range of -40 to +75 °C (altitude: 0–1800 m) and storage temperature in the range of -40 to +85 °C.
- Be dampproof and corrosion-resisting, and work at 5%–95% relative humidity (non-condensing).
- Pass IEC 61000-4 industrial-grade electromagnetic compatibility test with good anti-electromagnetic interference performance.
- Support Mean Time Between Failure (MTBF) of 35 years.



#### Note

When the altitude increases by 220 m between 1800 m and 5000 m, the highest operating temperature of the device decreases by 1°C.

### 1.2.2 Various interface types

The Gazelle S1512i-PWR meets special on-site environment requirements with flexible interface configurations, including:

- Provide eight 1000 Mbit/s RJ45 electrical interfaces and four 1000 Mbit/s SFP optical interfaces.
- The SFP optical interface supports the 1000 Mbit/s optical module.
- Provide the RJ45 Console interface.
- Provide the external alarm output interface in form of a Phoenix connector.

### 1.2.3 Powerful PoE power supply

The Gazelle S1218i-PWR supports PoE, with the following characteristics:

- Support Endpoint PSE (PoE integrated in the Gazelle S1512i-PWR).
- Support IEEE 802.3af standard (PoE).
- Support IEEE 802.3at standard (PoE+).
- Support the standard PD and non-standard PD.
- Support supplying 15 W or 30 W power from 8 RJ45 PoE interfaces. All these interfaces can supply up to 240 W power.
- Support enabling/disabling PoE and configuring maximum Tx power, power supply mode, and power supply priority of a power supply interface through software.
- Support overtemperature protection.

### 1.2.4 Flexible networking performance

The Gazelle S1512i-PWR possesses flexible networking performance:

- Support chain, star, double-star, single ring, intersecting ring, and tangent ring networking schemes.
- Support Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP), which enhance the link redundant backup and fault-tolerant performance to ensure stable operation of the network.

### 1.2.5 Strict QoS

The Gazelle S1112i-PWR supports the following QoS characteristics:

- Support IEEE 802.1p QoS, thus providing the customer with reliable and effective methods for optimizing services.
- Support interface trust modes, trusted Class of Service (CoS) priority, and trusted Differentiated Services Code Point (DSCP) priority.
- Support interface-based priority mapping, mapping from CoS to local priority, and mapping from DSCP to local priority.
- Support 2 scheduling queues on the interface, with Strict Priority (SP) and Weight Round Robin (WRR) scheduling modes.

### 1.2.6 Complete security guarantee

The Gazelle S1512i-PWR provides complete security guarantee:

- Support user management at different levels and password protection to avoid unauthorized access.
- Support Remote Authentication Dial In User Service (RADIUS) authentication and Terminal Access Controller Access Control System (TACACS+) authentication, and provide integrated password management.
- Support static Address Resolution Protocol (ARP), that is, bind the MAC address with the interface to protect the network from ARP attacks.
- Support storm control (including broadcast, unknown multicast, and unknown unicast packets), which effectively ensures the Gazelle S1512i-PWR to work normally in bad network conditions.

- Support VLAN partition based on the IEEE 802.1Q to isolate physical interfaces.
- Support interface protection to realize data isolation in the interface protection group and further complete the protection mechanism of the user data.
- Support encrypted authentication and access security provided by SNMPv3.

## 1.2.7 Comprehensive management modes

The Gazelle S1512i-PWR supports the following management modes:

- Web mode: it employs the graphic management interface, which reduces the difficulty of Human-Computer Interaction (HCI) and facilitates management and maintenance of the device.
- SNMP/RMON mode: the Gazelle S1512i-PWR can be managed through the NView NNM platform, which can realize alarm management of a single device or multiple devices to achieve the goal of managing all devices comprehensively.
- Support Telnet and SSH remote login to implement remote management and maintenance.
- Support multiple software upgrading modes, such as TFTP, FTP, SFTP, Network Management System (NMS), and Web.

## 1.3 Models

Table 1-1 lists the model of the Gazelle S1512i-PWR.

Table 1-1 Model

Model	Description
Gazelle S1512i-4GF-8GE-PWR	<ul style="list-style-type: none"><li>• Support eight 10/100/1000 Mbit/s Ethernet electrical interfaces, which can supply 8 ways of power compliant with IEEE 802.3af and IEEE 802.3at standards. Support non-standard PDs. Each PoE interface supports 15/30 W power. The Gazelle S1512i-PWR can supply up to 240 W power.</li><li>• Support four 1000BASE-X SFP optical interfaces.</li><li>• Support 48 VDC power input.</li></ul>

## 1.4 Software features

Table 1-2 lists software features of the Gazelle S1512i-PWR.

Table 1-2 Software features

Feature	Description
Basic features	<ul style="list-style-type: none"> <li>• Logging in to the device through Console/Telnet/SSH/Web</li> <li>• Hierarchical command management</li> <li>• User management in login authentication, privilege allocation, and commands</li> <li>• File management (BootROM/system files/configuration files)</li> <li>• Upgrading system (in BootROM through FTP/FTPv6/SFTP/TFTP/TFTPv6)</li> <li>• Two system software sets which can be switched</li> <li>• Time management (time zone, DST, NTP, and SNTP)</li> <li>• Interface management (Jumbo frame, duplex, flow control, and rate)</li> <li>• Basic information about the device (device name, language mode, saving/deleting configurations, and restart)</li> <li>• Task scheduling</li> </ul>
Ethernet	<ul style="list-style-type: none"> <li>• MAC address (16K)</li> <li>• Basic VLAN (up to 4094 concurrent VLANs), Access and Trunk interface modes for VLAN</li> <li>• Basic QinQ and selective QinQ</li> <li>• STP/RSTP/MSTP</li> <li>• Loop detection for eliminating the self-loop, inner loop, and outer loop</li> <li>• Line detection</li> <li>• Interface protection for isolating Layer 2 data</li> <li>• Port mirroring</li> <li>• Layer 2 protocol transparent transmission (Dot1x packets, BPDU packets, LACP packets, CDP packets, PVST packets, and VTP packets)</li> </ul>
PoE	<ul style="list-style-type: none"> <li>• IEEE 802.3af and IEEE 802.3at PoE</li> <li>• Non-standard PDs</li> <li>• Up to 240 W power supplied by all PoE interfaces</li> </ul>
Ring protection switching	ERPS (ITU-T G.8032)
IP services	<ul style="list-style-type: none"> <li>• Layer 3 interface (IPv4/IPv6 address)</li> <li>• ARP</li> <li>• NDP</li> <li>• DHCP Client</li> <li>• DHCP Relay</li> <li>• DHCP Server</li> <li>• DHCP Snooping</li> <li>• DHCP Option 82</li> </ul>
IP route	<ul style="list-style-type: none"> <li>• Static route</li> <li>• Route management</li> <li>• RIP (v1 and v2)</li> <li>• OSPFv2</li> <li>• Route policy (matching ACL, address prefix list, and routing mapping table rule)</li> </ul>
QoS	<ul style="list-style-type: none"> <li>• ACL rules</li> <li>• Priority trust (DSCP and CoS)</li> <li>• Traffic classification and traffic policy (rate limiting, redirection, and remarking based on traffic policy)</li> <li>• Local priority mapping and queue scheduling (SP, WRR, DRR, SP+DRR, and SP+WRR)</li> <li>• Interface-based rate limiting</li> </ul>



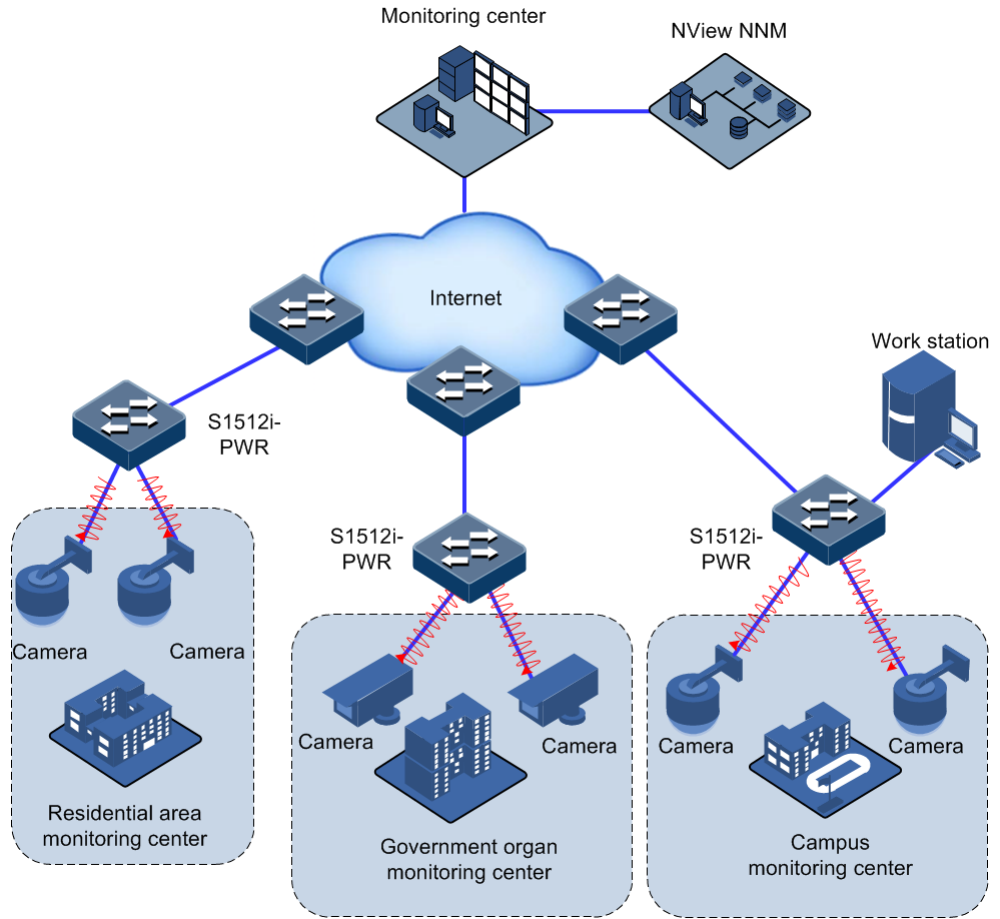
Feature	Description
Multicast	<ul style="list-style-type: none"> <li>• Static multicast</li> <li>• Filtering multicast packets and discarding unknown multicast packets</li> <li>• IGMP Snooping (v1/v2)</li> <li>• IGMP MVR</li> <li>• Multicast VLAN copy</li> <li>• IGMP Proxy</li> <li>• IGMP filtering</li> </ul>
Security	<ul style="list-style-type: none"> <li>• Port security MAC (static, dynamic, and sticky secure MAC addresses)</li> <li>• Dynamic ARP inspection (static binding and dynamic binding)</li> <li>• RADIUS authentication</li> <li>• TACACS+ authentication</li> <li>• Interface-based storm control</li> <li>• IP Source Guard</li> <li>• PPPoE+ (static binding and dynamic binding)</li> </ul>
Reliability	<ul style="list-style-type: none"> <li>• Manual and static link aggregation</li> <li>• Interface backup</li> <li>• Link-state tracking</li> </ul>
System management	<ul style="list-style-type: none"> <li>• SNMP (v1/v2/v3)</li> <li>• KeepAlive</li> <li>• RMON (statistical group, historical statistical group, alarm group, and event group)</li> <li>• LLDP</li> <li>• Optical module DDM</li> <li>• System log</li> <li>• Alarm management</li> <li>• Hardware environment monitoring</li> <li>• CPU monitoring</li> <li>• CPU protection</li> <li>• Ping and Traceroute</li> </ul>

## 1.5 Networking applications

When the economy grows, security protection technologies play a vital role in maintaining public order and safeguarding people's lives and properties. More and more monitoring devices are deployed in public places, such as residential areas, schools, and enterprises. Most cameras are installed in places where power cables are difficult to be installed, such as corners, wayside, and doorway. By supplying power to cameras through the Ethernet, you can save cost of cabling and maintenance and reduce workload.

The Gazelle S1512i-PWR can supply power to PDs and their monitors and collect data, as shown in Figure 1-2.

Figure 1-2 Security protection and monitoring application with the device



# 2 Hardware structure

---

This chapter describes the hardware structure of the Gazelle S1512i-PWR, including the following sections:

- Appearance
- Interfaces
- Button
- LEDs
- Power supply

## 2.1 Appearance

Dimensions of the Gazelle S1512i-PWR chassis are as below:

- 80 mm (Width) × 121 mm (Depth) × 150 mm (Height) (without cooling fins)
- 105 mm (Width) × 121 mm (Depth) × 150 mm (Height) (with cooling fins)

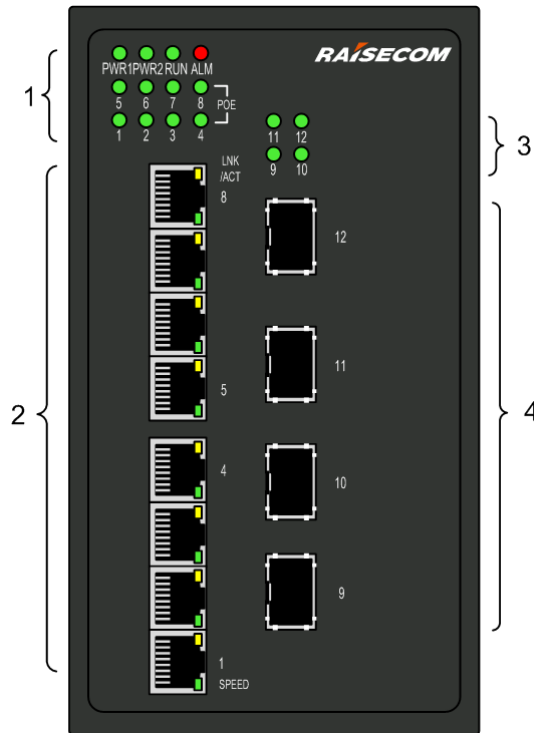
The Gazelle S1512i-PWR supports the following installation modes:

- Guide-rail installation
- Wall-mount installation

### 2.1.1 Front appearance

Figure 2-1 shows the front appearance of the Gazelle S1512i-PWR.

Figure 2-1 Front appearance

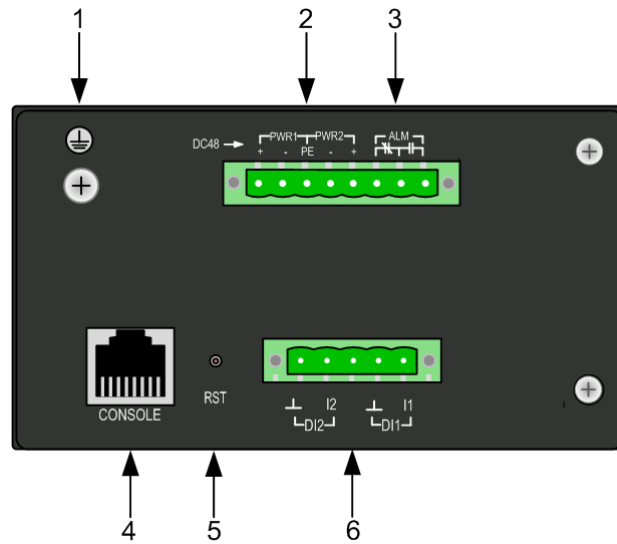


1	LEDs (PWR1, PWR2, ALM, RUN, POE 1–8)
2	Service interfaces 1–8 (1000 Mbit/s RJ45 electrical interfaces) and LEDs (LNK/ACT and SPEED)
3	LEDs 9–12 (1000 Mbit/s SFP optical interface status LED)
4	Service interfaces 9–12 (1000 Mbit/s SFP optical interface)

## 2.1.2 Top appearance

Figure 2-2 shows the top appearance of the Gazelle S1512i-PWR.

Figure 2-2 Top appearance



1	Ground terminal
2	DC power interface (PWR1 and PWR2)
3	Alarm interface (ALM)
4	Console interface
5	RST button
6	DI interface



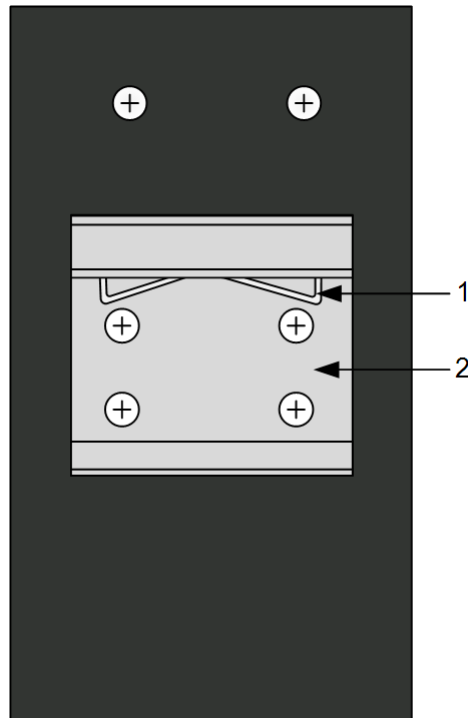
**Note**

The DC power supply of the Gazelle S1512i-PWR supports Redundant Power System (RPS) input.

### 2.1.3 Rear appearance

Figure 2-3 shows the rear appearance of the Gazelle S1512i-PWR.

Figure 2-3 Rear appearance



1	Spring clip
2	Rail clip

## 2.2 Interfaces

### 2.2.1 Service interfaces

The Gazelle S1512i-PWR provides multiple interfaces to transmit services.

Table 2-1 lists interfaces on the Gazelle S1512i-PWR.

Table 2-1 Interfaces

Print	Interface type	Description
1–8	RJ45	10/100/1000BASE-TX auto-negotiation electrical interface, supporting PoE
9–12	SFP optical interface	Support the following optical module: 1000BASE-X

### 2.2.2 RJ45 Console interface

Table 2-2 lists parameters of the RJ45 Console interface.


Table 2-2 Parameters of the RJ45 Console interface

Parameter	Description
Connector type	RJ45
Working mode	Duplex UART
Electrical features	RS232
Baud rate	9600 baud

## 2.2.3 Management and auxiliary interfaces

Table 2-3 lists management and auxiliary interfaces on the Gazelle S1512i-PWR.

Table 2-3 Management and auxiliary interfaces

Interface type	Description
Console interface	RJ45 Console interface, used to connect the Gazelle S1512i-PWR to a PC
Alarm interface	Use 3 PINs of the 8-pin Phoenix connector with spaces of 5.08 mm. It is used to output alarms.   <b>Note</b> Alarms generated on the Gazelle S1512i-PWR are output by the alarm interface to the monitoring device, which records and monitors operations of the Gazelle S1512i-PWR.
DI interface	5-pin Phoenix connector with spaces of 5.08 mm, used to input alarms, supporting 2 way of digital input
Power interface	Use 5 PINs of the 8-pin Phoenix connector with spaces of 5.08 mm. It is used to input power.

## 2.3 Button

Table 2-4 lists the button on the Gazelle S1512i-PWR.

Table 2-4 Button

Button	Description
RST	<ul style="list-style-type: none"> <li>• Short press: press it for less than 3s to restart the Gazelle S1512i-PWR.</li> <li>• Long press: press it for more than 3s to restore factory settings.</li> </ul>

## Caution

- Pressing the RST button will restart the Gazelle S1512i-PWR and interrupt services. Use it with care.
- Long press of the RST button for more than 3s will restore factory settings and clear all current configurations. We recommend exporting configuration files and upload them to the server for backup before restoring factory settings.
- Short press of the RST button for less than 3s will restart the Gazelle S1512i-PWR. To prevent configuration files from being lost, save the current configurations before restarting the Gazelle S1512i-PWR.

## 2.4 LEDs

Table 2-5 lists LEDs on the Gazelle S1512i-PWR.

Table 2-5 LEDs

LED	Print	Color	Description
Electrical interface status LED	LNK/ACT (1–8)	Yellow	<ul style="list-style-type: none"> <li>• Yellow: the electrical interface is in Link Up status.</li> <li>• Blinking yellow: the electrical interface is receiving or sending data.</li> <li>• Off: the electrical interface is in Link Down status.</li> </ul>
PoE remote power supply working status LED	POE	Green	<ul style="list-style-type: none"> <li>• Green: the electrical interface is supplying power to a remote PD.</li> <li>• Off: the electrical interface is not supplying power or disconnected from any remote PD.</li> </ul>
Optical interface status LED (9–12)	9–12	Green	<ul style="list-style-type: none"> <li>• Green: the optical interface is in Link Up status.</li> <li>• Blinking green: the optical interface is receiving or sending data.</li> <li>• Off: the optical interface is in Link Down status.</li> </ul>
Power status LED	PWR1/PWR2	Green	<ul style="list-style-type: none"> <li>• Green: power supply 1 or power supply 2 is normal.</li> <li>• Off: power supply 1 or power supply 2 is abnormal or both are off.</li> </ul>
System status LED	RUN	Green	<ul style="list-style-type: none"> <li>• Green: the system is being started or working improperly.</li> <li>• Blinking green: the system is working properly.</li> <li>• Off: the system is being started or working improperly.</li> </ul>
Alarm output LED	ALM	Red	<ul style="list-style-type: none"> <li>• Red: the system is being started or alarms are generated in the system.</li> <li>• Off: no alarms are generated or alarms are cleared in the system.</li> </ul>



## 2.5 Power supply

### 2.5.1 Introduction

The DC power supply, based on related industrial standards, meets strict specifications.

The DC power supply supports the following functions:

- Support 48 VDC power input.
- Support overload protection and reverse polarity protection.
- Support overvoltage and surge protection.
- Support NMS and electromagnetic relay alarms for power failure.

### 2.5.2 Appearance and interfaces

There is one 8-pin Phoenix connector with spaces of 5.08 mm on the top of the Gazelle S1512i-PWR. The power interface uses 5 PINs of the 8 PINs.

Figure 2-4 shows appearance of the DC power interface.

Figure 2-4 Appearance of the DC power interface

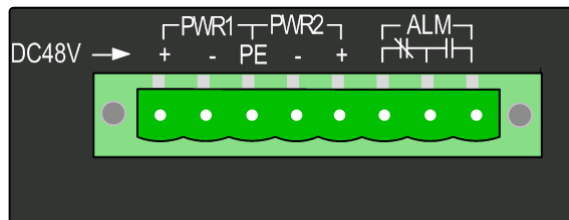


Table 2-6 lists interface type and description of the DC power interface.

Table 2-6 DC power interface

Power supply	Print	Description
DC power supply	+ (PWR1)	Positive input terminal of power supply 1
	- (PWR1)	Negative input terminal of power supply 1
	PE	Ground terminal
	- (PWR2)	Negative input terminal of power supply 2
	+ (PWR2)	Positive input terminal of power supply 2

# 3 Interfaces and modules

This chapter describes parameters of interfaces and modules on the Gazelle S1512i-PWR, including the following sections:

- Interfaces
- SFP modules

## 3.1 Interfaces

### 3.1.1 1000BASE-X SFP optical interface

Table 3-1 lists parameters of the 1000BASE-X SFP optical interface.

Table 3-1 Parameters of the 1000BASE-X SFP optical interface

Parameter	Description
Connector type	LC/PC
Coding scheme	8B/10B
Transmission rate	1000 Mbit/s
Duplex mode	Full duplex

### 3.1.2 1000BASE-T electrical interface

Table 3-2 lists parameters of the 1000BASE-T electrical interface.

Table 3-2 Parameters of the 1000BASE-T electrical interface

Parameter	Description
Connector type	RJ45
Transmission rate	Support 10/100/1000 Mbit/s auto-negotiation.

Parameter	Description
Duplex mode	Support full duplex and half duplex modes.
Specifications	<ul style="list-style-type: none"> <li>• When the transmission rate is 10/100 Mbit/s, we recommend using the Cat 5 or better STP cable.</li> <li>• When the transmission rate is 1000 Mbit/s, we recommend using the Cat 6 or better STP cable.</li> </ul>

### 3.1.3 RJ45 Console interface

Table 3-3 lists parameters of the RJ45 Console interface.

Table 3-3 Parameters of the RJ45 Console interface

Parameter	Description
Connector type	RJ45
Duplex mode	Duplex UART
Electrical feature	RS-232
Baud rate	9600 baud
Data bit	8
Stop bit	1

### 3.1.4 Alarm output interface

The alarm output interface is embedded with an electromagnetic relay. When the Gazelle S1512i-PWR is in abnormal status, it can output alarms by controlling the connection status of PINs, notify on-site maintenance personnel, and send alarms to the NMS.

The alarm output interface and power interface of the DC power model is co-located on an 8-pin Phoenix connector with spaces of 5.08 mm, of which the alarm output interface takes up 3 PINs, as shown in Figure 3-1.

- When an alarm is generated, PIN 1 and PIN 2 are connected, and thus the ALM LED is on.
- When no alarm is generated, PIN 2 and PIN 3 are connected, and thus the ALM LED is off.

Figure 3-1 Alarm output interface on the DC power model

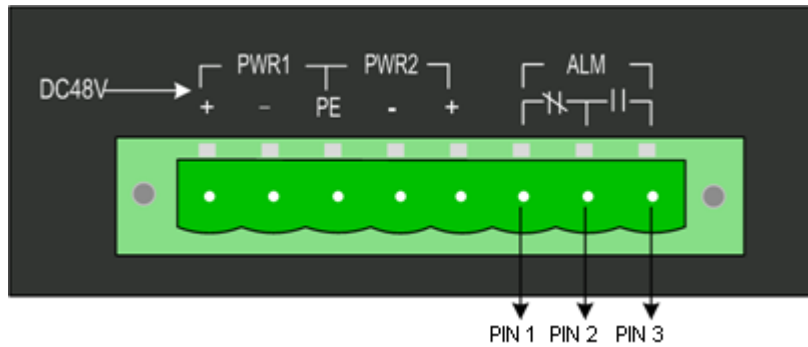


Table 3-4 lists parameters of the alarm output interface.

Table 3-4 Parameters of the alarm output interface

Parameter	Description
Connector type	5.08 mm × 8-pin Phoenix connector
Working mode	Electromagnetic relay
Electrical feature	Connected/Disconnected

### 3.1.5 DI interface

The DI interface uses 4 PINs of 5-pin Phoenix connector with spaces of 5.08 mm and is used to input digital signals from an external device for monitoring external environment alarms, as shown in Figure 3-2.

Figure 3-2 DI interface

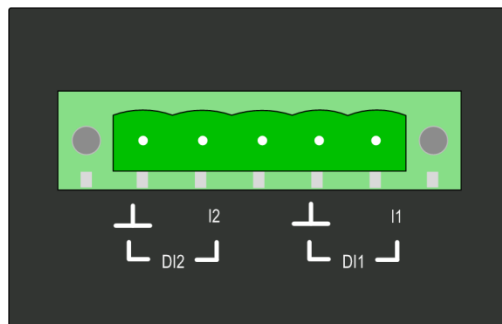


Table 3-5 lists PINs of the DI interface.

Table 3-5 PINs of the DI interface

PIN	Description
1	Positive terminal of No. 1 way of external digital input
2	Positive terminal of No. 2 way of external digital input

PIN	Description
⊥	Negative terminal

The DI interface supports 2 ways of DI and up to 8 mA input current. Each way of DI supports the following two statuses:

- High level: the input voltage is 13–30 VDC.
- Low level: the input voltage is -30 to 1 VDC.

After login, you can configure the triggering condition of an external alarm to high level or low level in global configuration mode as required, as described in Table 3-6.

Table 3-6 Configuring triggering condition


Step	Command	Description
1	<code>Raisecom#config</code>	Enter global configuration mode.
2	<code>Raisecom(config)#alarm outside-alarm num { high   low }</code>	<p>Configure the triggering condition of an external alarm to high level or low level.</p> <ul style="list-style-type: none"> <li>• <i>Num</i>: being 1 or 2, DI ID</li> <li>• High: configure the triggering condition to high level.</li> <li>• Low: configure the triggering condition to low level.</li> </ul> <p> <b>Note</b> By default, each external alarm is triggered by high level.</p>

Table 3-7 lists parameters of the DI interface.

Table 3-7 Parameters of the DI interface

Parameter	Description
Connector type	5.08 mm × 5-pin Phoenix connector
Input voltage range	-30 to +30 VDC
High level	+13 to +30 VDC
Low level	-30 to +1 VDC
Maximum input current	8 mA

## 3.2 SFP modules

All Raisecom modules comply with RoHS and all Raisecom optical modules support DDM.

### 3.2.1 Dual-fiber bidirectional (LC/PC)

Table 3-8 Parameters of GE (1250 Mbit/s) dual-fiber bidirectional optical modules

Model	Tx wavelength (nm)	Rx wavelength (nm)	Tx optical power (EOL) (dBm)	Overloading point (dBm)	Extinction ratio (dB)	Rx sensitivity (dBm)	Mode	Transmission distance (km)
USFP-Gb/M-I	850	830–870	-9.5 to -3	> 0	> 9	< -17	MM	0.55
USFP-Gb/S1-I	1310	1260–1620	-10 to -3	> -3	> 9	< -21	SM	15
USFP-Gb/S2-I	1310	1260–1620	-2 to 3	> -3	> 9	< -21	SM	40
USFP-Gb/S3-I	1550	1260–1620	0–5	> -3	> 9	< -22	SM	80

### 3.2.2 Single-fiber bidirectional (LC/PC)

Table 3-9 Parameters of GE (1250 Mbit/s) single-fiber bidirectional optical modules

Model	Tx wavelength (nm)	Rx wavelength (nm)	Tx optical power (EOL) (dBm)	Overloading point (dBm)	Extinction ratio (dB)	Rx sensitivity (dBm)	Mode	Transmission distance (km)
USFP-Gb/SS13-I	1310	1500–1610	-10 to -3	> -3	> 9	< -21	SM	15
USFP-Gb/SS15-I	1550	1260–1360	-10 to -3	> -3	> 9	< -21	SM	15
USFP-Gb/SS24-I	1490	1530–1580	-3 to 2	> -3	> 9	< -21	SM	40
USFP-Gb/SS25-I	1550	1450–1530	-3 to 2	> -3	> 9	< -21	SM	40
USFP-Gb/SS34-I	1490	1530–1580	-2 to 3	> -3	> 9	< -26	SM	80
USFP-Gb/SS35-I	1550	1450–1510	-2 to 3	> -3	> 9	< -26	SM	80

# 4 Cables

---

This chapter describes cables used by the Gazelle S1512i-PWR, including the following sections:

- Ground cable
- DC power cable
- Ethernet cable
- Fiber
- Digital input cable
- Alarm cable

## 4.1 Ground cable

### 4.1.1 Introduction



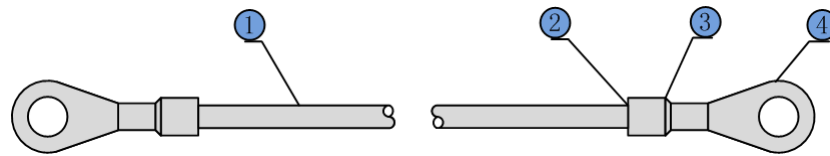
Connecting the ground cable properly is an important guarantee for lightning protection, shock proof, and anti-interference. When installing and using the device, ensure that the ground cable is properly connected; otherwise, personnel injury or equipment damage may occur.

The ground cable is used to connect the Gazelle S1512i-PWR to the ground.

### 4.1.2 Appearance

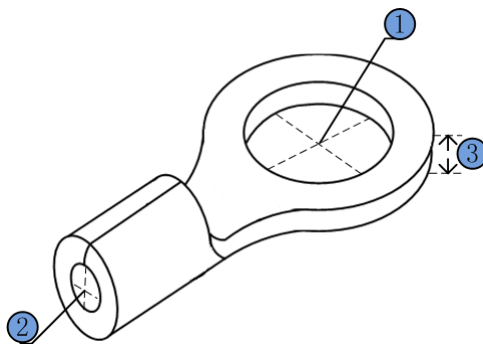
The ground cable is composed of ground terminals and the coaxial cable. The ground terminal is usually an OT non-insulated terminal. The coaxial cable is a yellow/green copper soft flame-retardant conducting wire. Figure 4-1 and 0 show the ground cable and OT terminal.

Figure 4-1 Ground cable



1	Conducting wire	2	Stripped end (connected to the OT terminal)
3	Insulating sheath	4	OT terminal

Figure 4-2 OT terminal



1	Inner diameter of soldering lug	2	Inner diameter of sheath	3	Thickness of soldering terminal
---	---------------------------------	---	--------------------------	---	---------------------------------

### 4.1.3 Technical specifications

Table 4-1 lists technical specifications of the ground cable.

Table 4-1 Technical specifications of the ground cable

Parameter	Description
Model (recommended)	PIL-ground cable-Φ4-D. Φ4 indicates a diameter of 4 mm. The letter D is the length, which can be customized. For example, the customer requires a 2-m cable, and you can name it PIL-ground cable-Φ4-2m.
Standard	Comply with the UL standard and meet RoHS requirements.
Conducting wire	Yellow/Green multi-strand copper-core conducting wire 16AWG (1.25 mm <sup>2</sup> ) Electronic wire UL1007 or UL1015 is used.
Stripped end	10 mm long, tinned
Insulating sheath	3.5/1.75 black heat-shrink tubing. It is a 20 mm plastic tube which shrinks when being heated.



Parameter	Description
Welding technology	The conducting wire and OT terminals adopt solderless pressed connection.
Error in length of conducting wire	±5 mm

Table 4-2 lists technical specifications of the OT terminal.

Table 4-2 Technical specifications of the OT terminal

Parameter	Description
Model	Ground round-pressed terminal (M4)
Compliant standard	JB2436-78
Technical specifications	<ul style="list-style-type: none"> <li>• 4.3 soldering lug</li> <li>• Inner diameter of soldering lug: 4 mm</li> <li>• Outer diameter of soldering lug: ≤ 8 mm</li> <li>• Inner diameter of sheath: 2.1 mm</li> <li>• Thickness of soldering lug: ≥ 0.6 mm</li> </ul>
Cross-sectional area of the conducting wire	16–15 AWG (1.2–1.5 mm <sup>2</sup> )



### Note

- The Gazelle S1512i-PWR is delivered without the ground cable. If required, make the ground cable on site according to technical specifications.
- The ground cable cannot be longer than 30 m and should be as short as possible; otherwise, a ground bar should be used instead.

## 4.2 DC power cable

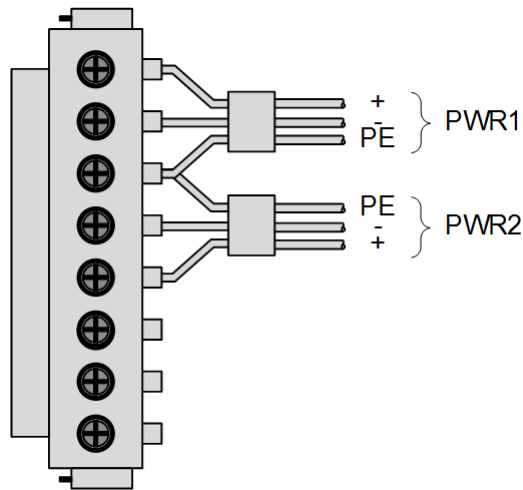
### 4.2.1 Introduction

The DC power cable transmits 48 VDC power from the power sourcing equipment to the power interface of the Gazelle S1512i-PWR, and then transmits power to the entire device.

### 4.2.2 Appearance

The DC power cable is composed of the plug and conducting wire, as shown in Figure 4-3.

Figure 4-3 DC power cable



## 4.2.3 Technical specifications

Table 4-3 lists technical specifications of the DC power cable.

Table 4-3 Technical specifications of the DC power cable

Parameter	Description
Connector	5.08-8pin-head/RoHS
Type	Copper core multi-strand power cable 18AWG (0.75 mm <sup>2</sup> )



### Note

The Gazelle S1512i-PWR is delivered without the power cable but with power connector only. If required, make the power cable on site according to technical specifications.

## 4.3 Ethernet cable

### 4.3.1 Introduction

For the Gazelle S1512i-PWR, the Ethernet cable connects the Ethernet electrical interface and other devices.

The Ethernet interface on the Gazelle S1512i-PWR is self-adaptive to straight-through cable mode and crossover cable mode.



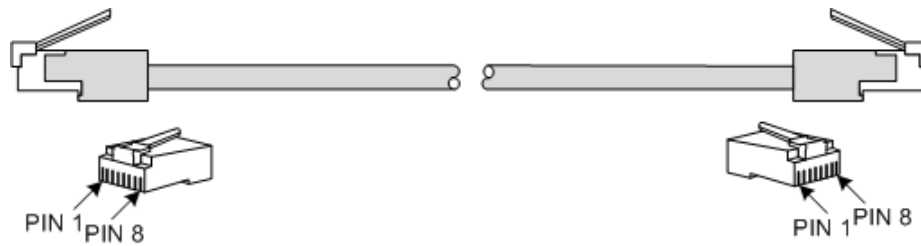
### Note

If required, make the Ethernet cable on site according to technical specifications.

### 4.3.2 Appearance

Figure 4-4 shows the Ethernet cable.

Figure 4-4 Ethernet cable



### 4.3.3 Technical specifications

The Ethernet cables have two types:

- Straight-through cable: used to connect devices of different type, such as between a PC and a switch, between a switch and a router
- Crossover cable: used to connect devices of the same type, such as between PCs, between switches, between routers, between a PC and a router (they are of the same type)

Table 4-4 lists the wiring of EIA/TIA 568A and EIA/TIA 568B standards.

Table 4-4 Wiring of EIA/TIA 568A and EIA/TIA 568B standards

Connector (RJ45)	EIA/TIA 568A	EIA/TIA 568B
PIN 1	White/Green	White/Orange
PIN 2	Green	Orange
PIN 3	White/Orange	White/Green
PIN 4	Blue	Blue
PIN 5	White/Blue	White/Blue
PIN 6	Orange	Green
PIN 7	White/Brown	White/Brown
PIN 8	Brown	Brown

Table 4-5 lists technical specifications of the Ethernet cable.

Table 4-5 Technical specifications of the Ethernet cable

Parameter	Description
Name	CBL-ETH-RJ45/RJ45-D-RoHS
Connector	RJ45 crystal head
Model	Cat 5 or better STP cable

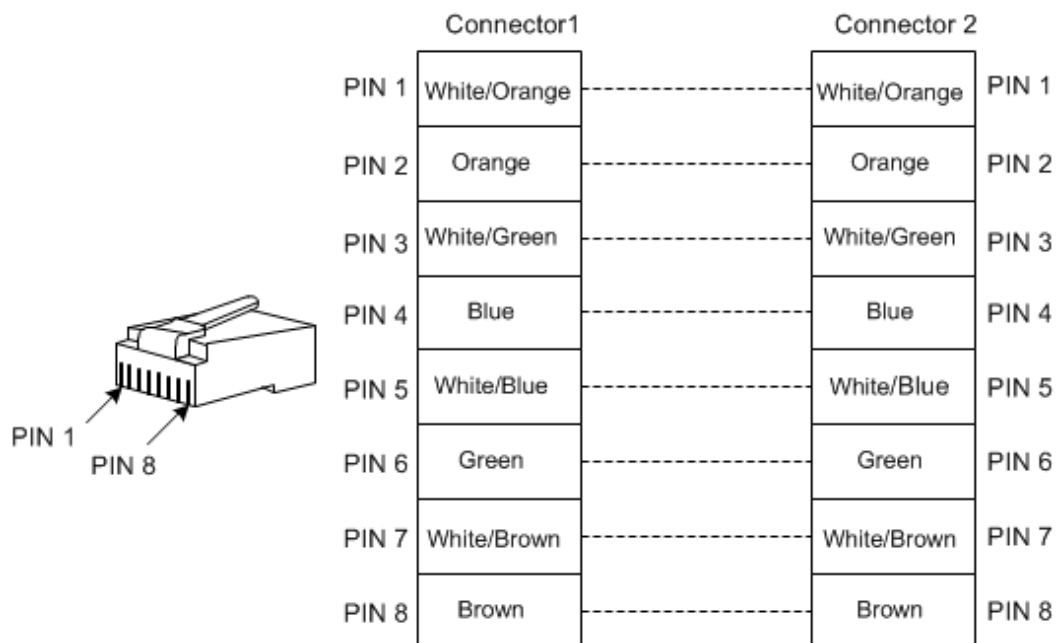
Parameter	Description
Number of cores	8
Length	The letter D is the length, which can be customized. For example, if the customer requires a 2-meter cable, you can name it CBL-ETH-RJ45/RJ45-2m-RoHS.

## Straight-through cable

Both two RJ45 connectors of the straight-through cable follow EIA/TIA 568B standard wiring.

Figure 4-5 shows the wiring of the straight-through cable.

Figure 4-5 Wiring of the straight-through cable



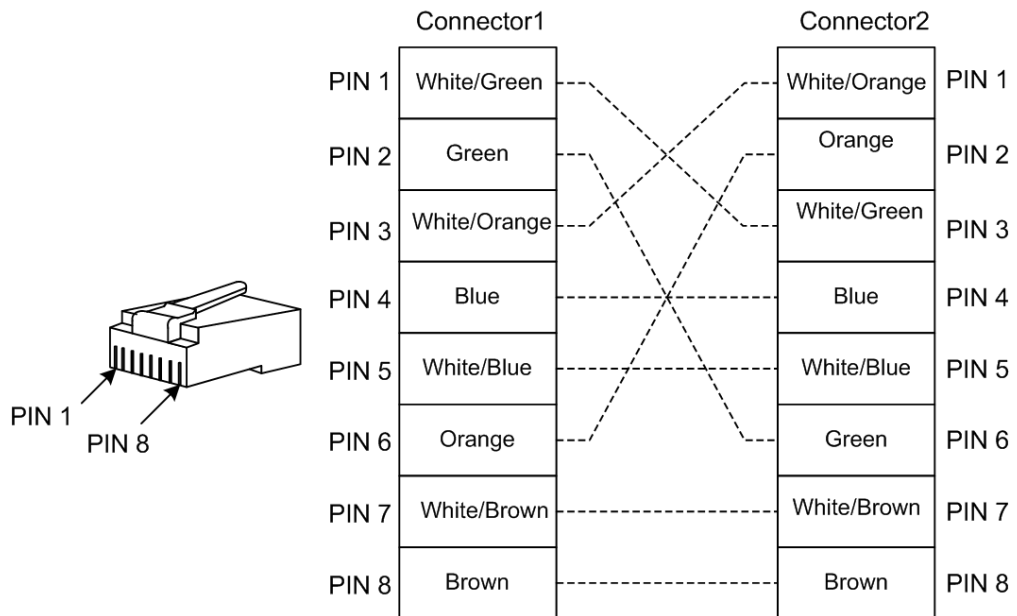
## Crossover cable

The wiring of the 100 Mbit/s crossover cable is different from that of the 1000 Mbit/s crossover cable.

One RJ45 connector of the 100 Mbit/s crossover cable follows EIA/TIA 568A standard wiring; the other RJ45 connector follows EIA/TIA 568B standard wiring.

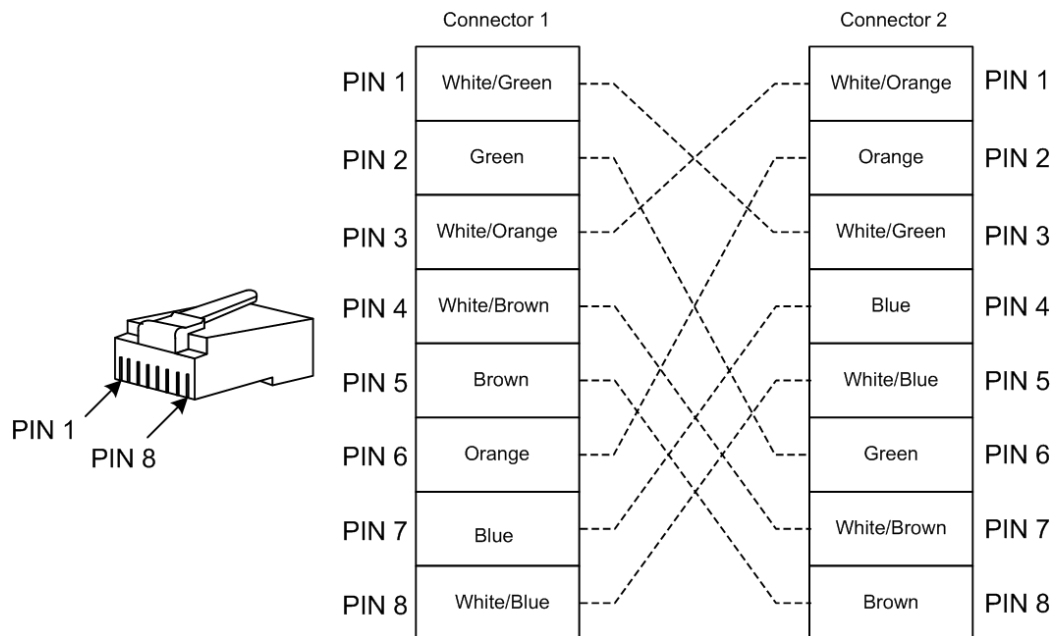
Figure 4-6 shows the wiring of the 100 Mbit/s crossover cable.

Figure 4-6 Wiring of the 100 Mbit/s crossover cable



The 1000 Mbit/s crossover cable uses all 8 pins. The crossover is PIN 1 to PIN 3, PIN 2 to PIN 6, PIN 4 to PIN 7, and PIN 5 to PIN 8, as shown in Figure 4-7.

Figure 4-7 Wiring of the 1000 Mbit/s crossover cable



## 4.4 Fiber

### 4.4.1 Introduction

The Gazelle S1512i-PWR supports the Single-Mode Fiber (SMF) and Multi-Mode Fiber (MMF). These two kinds of fiber are same in appearance while different in color. The yellow one is the SMF and the orange one is the MMF.

The Gazelle S1512i-PWR can be connected to the Optical Distribution Frame (ODF) or optical interfaces of other devices through the fiber.

Table 4-6 lists the type and usage of the fiber.

Table 4-6 Type and usage of the fiber

Usage	Local connector	Remote connector	Type	Standard
<ul style="list-style-type: none"> <li>Connect the Gazelle S1512i-PWR to the ODF through the Ethernet optical interface.</li> <li>Connect the Ethernet optical interface on the Gazelle S1512i-PWR to optical interfaces on other devices.</li> </ul>	LC/PC	LC/PC	2-mm SMF	ITU-T G.652
			2-mm MMF	
	LC/PC	FC/PC	2-mm SMF	
			2-mm MMF	
	LC/PC	SC/PC	2-mm SMF	
			2-mm MMF	

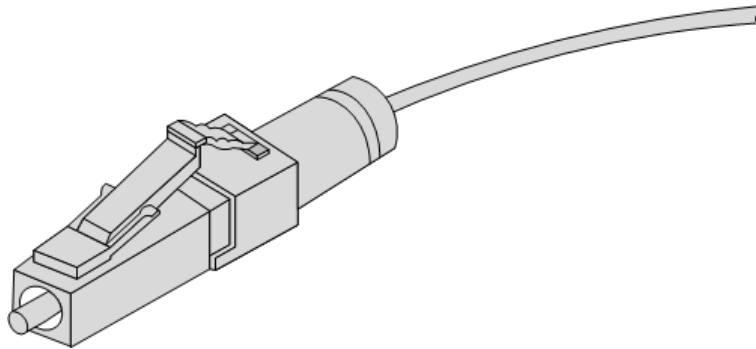
#### Note

- Choose the connector type and jumper cable length reasonably based on the on-site requirements.
- Choose a connector suitable for the optical interface. Otherwise, it may increase additional loss of fiber links, reduce transmission quality of services, or even damage the connector and optical interface.

### 4.4.2 Appearance

Figure 4-8 shows the appearance of the LC/PC fiber connector.

Figure 4-8 LC/PC fiber connector



When connecting or removing the LC/PC fiber connector, align the connector with the optical interface, and do not rotate the fiber. Operate the fiber as below:

- To connect the fiber, align the head of the fiber with the optical interface and insert the fiber into the interface gently.
- To remove the fiber, press down the clamping connector, and push the fiber head inwards, and then pull the fiber out.

### 4.4.3 Wiring

Table 4-7 lists the wiring of the fiber.

Table 4-7 Wiring of the fiber

Wiring	Local optical interface	Direction of optical signals	Peer optical interface
Single-fiber connection	Optical interface	<->	Optical interface
Dual-fiber connection	Optical interface Tx	->	Optical interface Rx
	Optical interface Rx	<-	Optical interface Tx

## 4.5 Digital input cable

### 4.5.1 Introduction

The digital input interface on the Gazelle S1512i-PWR uses 4 pins of the 5-pin Phoenix connector (with spaces of 5.08 mm) to input external alarms from an external device.

The digital input interface supports 2 ways of DI. Each way supports two statuses:

- Status 1: the input voltage is 13–30 V.
- Status 2: the input voltage is -30 to 1 V.

The condition for triggering alarms can be configured as required. By default, it is status 1.

- If status 1 is configured as the alarm status, status 2 is the normal status.

- If status 2 is configured as the alarm status, status 1 is the normal status.

## 4.5.2 Appearance

The digital input cable is composed of the connector and alarm conducting wire, as shown in Figure 4-9.

Figure 4-9 Alarm interface

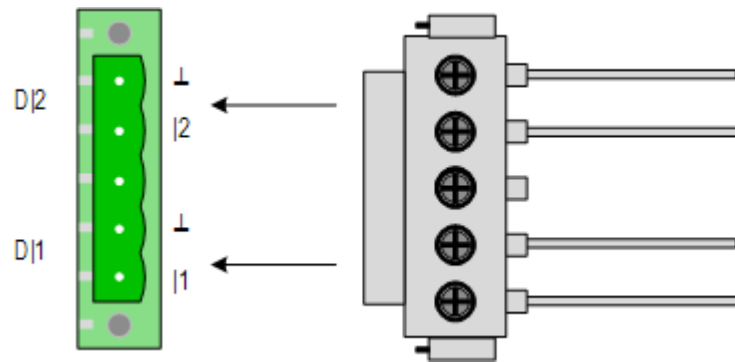


Table 4-8 describes the digital input interface.

Table 4-8 Digital input interface

Terminal	Description
1	Positive terminal of No. 1 way of external digital input
2	Positive terminal of No. 2 way of external digital input
⊥	Negative terminal

## 4.5.3 Technical specifications

Table 4-9 lists technical specifications of the digital input cable.

Table 4-9 Technical specifications of the digital input cable

Parameter	Description
Connector	5.08-8pin-head/RoHS
Specifications	Copper core multi-strand conducting wire 18AWG (0.75 mm <sup>2</sup> )



The digital input cable is not delivered with the Gazelle S1512i-PWR. If required, make it on site according to technical specifications.



## 4.6 Alarm cable

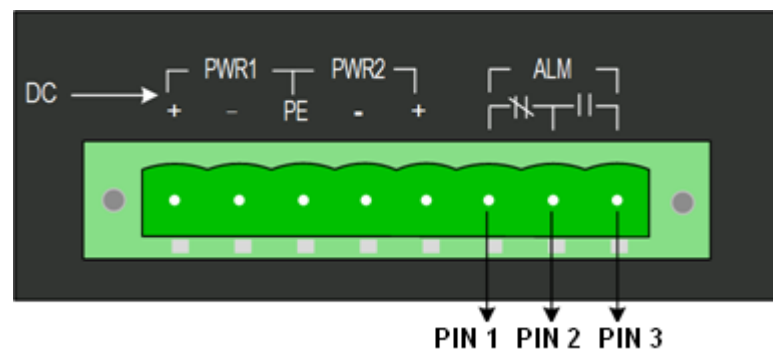
### 4.6.1 Introduction

The alarm interface on the switch is a 3-pin Phoenix connector interface (with spaces of 5.08 mm). When the Gazelle S1512i-PWR is in abnormal status (temperature and voltage), it can output alarms by controlling the connection status of PINs, notify on-site maintenance personnel, and send alarms to the NMS.

### 4.6.2 Appearance

The alarm cable is composed of the connector and the alarm conducting wire, as shown in Figure 4-10.

Figure 4-10 Alarm output interface



- When an alarm is generated, PIN 1 and PIN 2 are connected, and thus the alarm LED is on.
- When no alarm is generated, PIN 3 and PIN 2 are connected, and thus the alarm LED is off.

### 4.6.3 Technical specifications

Table 4-10 lists technical specifications of the alarm cable.

Table 4-10 Technical specifications of the alarm cable

Parameter	Description
Connector type	5.08 mm × 3-pin Phoenix connector
Specifications	Copper core multi-strand conducting wire 16AWG (1.25 mm <sup>2</sup> )



Only the Phoenix connector is delivered with the Gazelle S1512i-PWR. If required, make the alarm cable on site according to technical specifications.

# 5 Technical specifications

This chapter describes technical specifications of the Gazelle S1512i-PWR, including the following sections:

- Overall parameters
- Protocols and standards

## 5.1 Overall parameters

Table 5-1 lists overall parameters of the Gazelle S1512i-PWR.

Table 5-1 Overall parameters

Parameter			Description
Dimensions			<ul style="list-style-type: none"> <li>• 80 mm (Width) × 121 mm (Depth) × 150 mm (Height) (without cooling fins)</li> <li>• 105 mm (Width) × 121 mm (Depth) × 150 mm (Height) (with cooling fins)</li> </ul>
Maximum power consumption			<ul style="list-style-type: none"> <li>• &lt; 240 W (with PoE power supply)</li> <li>• &lt; 11 W (without PoE power supply)</li> </ul>
Weight (without guide rail)			≤ 1.61 kg
Operating temperature (altitude: 0–1800 m)			-40 to +75 °C
Storage temperature			-40 to +85 °C
Operating Humidity			5%–95% RH (non-condensing)
Protection level			IP30
Power	DC power	Rated voltage	48 VDC
		Voltage range	<ul style="list-style-type: none"> <li>• 36–60 VDC (without PoE power supply)</li> <li>• 44–57 VDC (with PoE power supply)</li> </ul>
	–	Overload protection	Supported

Parameter		Description
	Reverse polarity protection	Supported

## 5.2 Protocols and standards

### 5.2.1 Compliant communication protocols and standard

- IEEE 802.1Q VLAN
- IEEE 802.3ad Link Aggregation
- IEEE 802.1ad QinQ
- IEEE 802.1D Spanning Tree Protocol
- IEEE 802.1w RSTP
- IEEE 802.1s MSTP
- IEEE 802.1x Security
- IEEE 802.1p CoS Prioritization
- IEEE 802.3x Flow Control
- IEEE 802.1ab LLDP
- IEC 62351 Power systems management and associated information exchange - Data and communications security
- IEEE 802.3 Information Technology

### 5.2.2 Laser safety class



#### Warning

The laser inside fiber may hurt your eyes. Do not stare into the optical interface directly during installation and maintenance.

According to the Tx power of Laser, the Gazelle S1512i-PWR laser belongs to Class 1 in safety class.

In Class 1, the maximum Tx power on the optical interface is smaller than 10 dBm (10 mW).

### 5.2.3 Reliability indexes

Table 5-2 lists reliability indexes of the Gazelle S1512i-PWR.

Table 5-2 Reliability indexes

Parameter	Description
System availability	99.999%. The annual failure time for the Gazelle S1512i-PWR should be no longer than 5 minutes.
Annually system mean repair rate	< 1.5%

Parameter	Description
MTTR	< 2 hours
MTBF	35 years

## 5.2.4 EMC standards

The Gazelle S1512i-PWR complies with the following EMC standards when cooperating with an external power:

- Electro Magnetic Interference (EMI) meets CISPR 22 CLASS A related requirements.
- Static electricity meets IEC 61000-4-2 level 3 requirements.
- Radiated Immunity Test (RIT) meets IEC 61000-4-3 level 3 requirements.
- Electrical Fast Transient (EFT) meets IEC 61000-4-4 level 3 requirements.
- Surge (impact) meets IEC 61000-4-5 level 4 requirements.
- RF Conducted Immunity (CI) meets IEC 61000-4-6 level 3 requirements.
- Power Frequency Magnetic Field meets IEC 61000-4-8 level 3 requirements.
- Pulse Magnetic Field meets IEC 61000-4-9 level 3 requirements.
- Damped oscillation meets IEC 61000-4-12 level 3 requirements.
- Damped Oscillation Wave Magnetic Field meets IEC 61000-4-10 level 5 requirements.
- DC power voltage falling and interruption meet IEC 61000-4-29 requirements.

## 5.2.5 Environmental standards

The Gazelle S1512i-PWR is applicable to the industrial environment and should meet environmental requirements shown in Table 5-3.

Table 5-3 Environmental requirements

Parameter	Description
Air pressure	86–106 kPa
Operating temperature (altitude: 0–1800 m)	-40 to +75 °C
Storage temperature	-40 to +85 °C
Operating humidity	5%–95% RH (non-condensing)
Protection level	IP40
Environmental authentication	Comply with EU RoHS standard.

# 6 Hardware installation

This chapter describes hardware installation of the Gazelle S1512i-PWR, including the following sections:

- Preparing for installation
- Installing device
- Grounding device
- Connecting cables
- Powering on device
- Checking installation

## 6.1 Preparing for installation

### 6.1.1 Environmental conditions

The Gazelle S1512i-PWR can be installed in the following scenarios:

- Guide rail
- Wall



#### Note

Before installation, ensure that the location for installing the Gazelle S1512i-PWR meets operating environment requirements. For details, see section 5.2.5 Environmental standards.

### 6.1.2 Power conditions

Table 6-1 lists power conditions of the Gazelle S1512i-PWR.

Table 6-1 Power conditions

Parameter	Description
DC	<ul style="list-style-type: none"><li>• Rated voltage: 48 VDC</li><li>• Voltage range: 36–60 VDC</li></ul>

Parameter	Description
RPS	We recommend preparing a Redundant Power System (RPS) to ensure that the Gazelle S1512i-PWR can work properly when the main power supply fails.
Power	The power supply for the Gazelle S1512i-PWR must be greater than the maximum power consumption.

### 6.1.3 Electrostatic conditions

To prevent human electrostatic from damaging the Gazelle S1512i-PWR, you must wear an Electrostatic Discharge (ESD) wrist strap before contacting the Gazelle S1512i-PWR. The ESD wrist strap should contact your skin properly. Ensure that the other end of the ESD wrist strap is properly grounded.

### 6.1.4 Grounding conditions

The Gazelle S1512i-PWR must be grounded and the ground resistance should be no more than 1  $\Omega$ . Grounding properly is a necessity for lightning protection and anti-interference.

### 6.1.5 Other conditions

Before installation, you should ensure that auxiliary components are ready. For example, cables and supporting facilities are correctly installed.

### 6.1.6 Precautions for unpacking

The Gazelle S1512i-PWR is packed in a dedicated box. When you unpack it, pay attention to the following matters:

- Lay the box facing up.
- According to the Packing List, check whether the device and auxiliary parts are complete.

## 6.2 Installing device

### 6.2.1 Installing device on guide rail



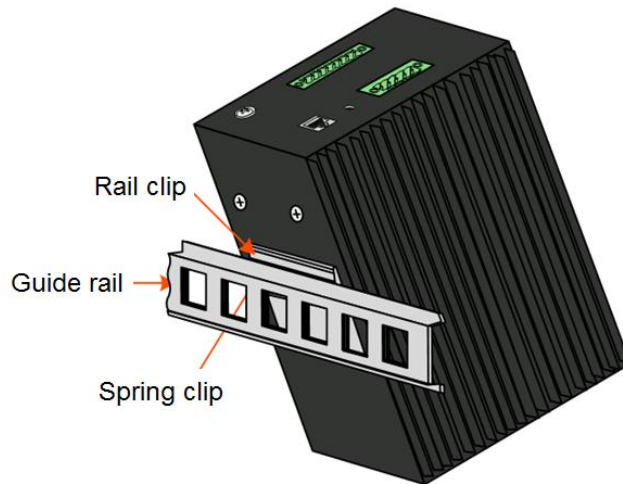
#### Note

When the Gazelle S1512i-PWR is taken out of the packing box, it is installed with the rail clip on the rear panel.

Install the Gazelle S1512i-PWR on the guide rail as below:

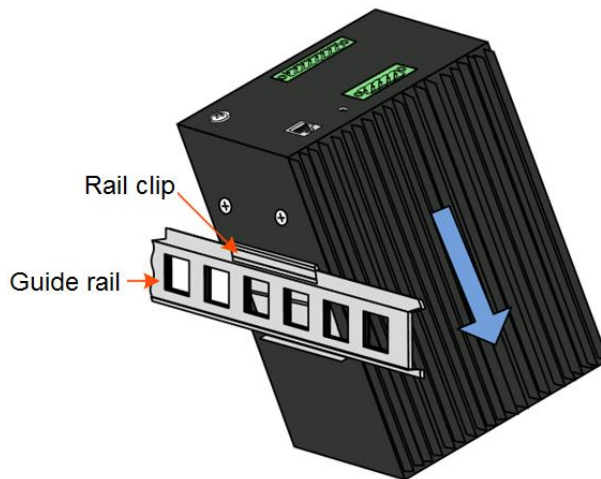
- Step 1 Connect the rail clip to the guide rail, as shown in Figure 6-1.

Figure 6-1 Connecting the rail clip to the guide rail



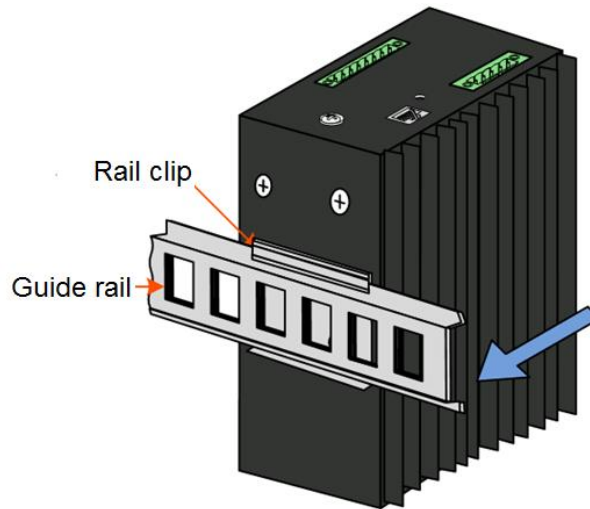
Step 2 Press the Gazelle S1512i-PWR downward to fix the spring clip to the guide rail tightly, as shown in Figure 6-2.

Figure 6-2 Installing the rail clip to the guide rail



Step 3 Press the Gazelle S1512i-PWR downward to fix the Gazelle S1512i-PWR on the guide rail, as shown in Figure 6-3.

Figure 6-3 Installing the device on the guide rail



Step 4 Ensure that the rail clip is connected to the guide rail tightly.

## 6.2.2 Installing device on wall



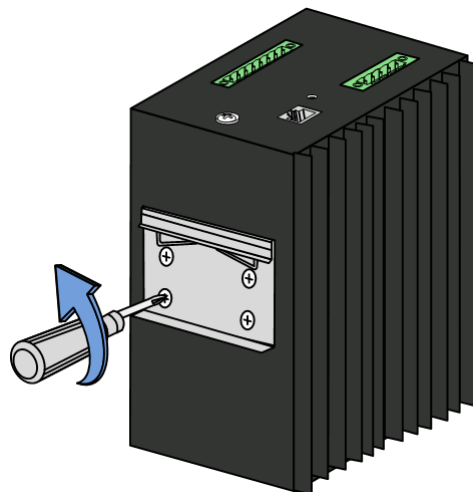
### Note

- You can choose either guide-rail installation or wall-mount installation as required. You need to remove the rail clip on the rear panel before the wall-mount installation.
- The Gazelle S1512i-PWR is not delivered with the wall-mount bracket. You can purchase it separately if required.

Install the Gazelle S1512i-PWR on the wall as below:

Step 1 Anticlockwise unscrew the rail clip to remove it, as shown in Figure 6-4.

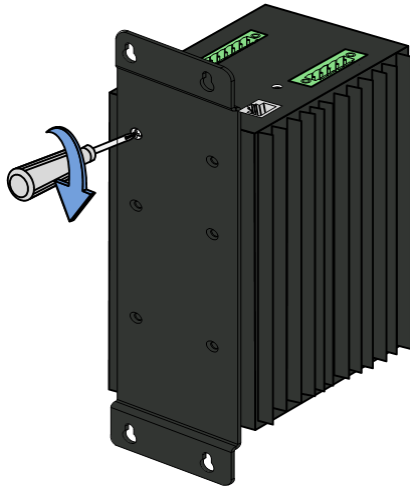
Figure 6-4 Removing the rail clip



Step 2 Install the wall-mount bracket to the rear panel of the Gazelle S1512i-PWR and clockwise screw the wall-mount bracket tightly, as shown in Figure 6-5.

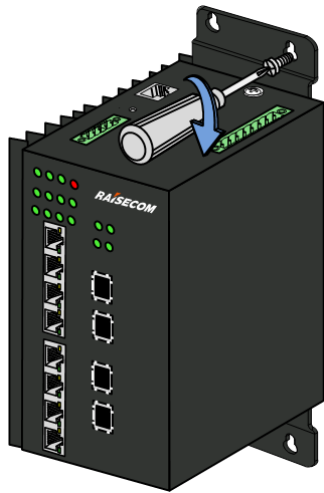


Figure 6-5 Installing the wall-mount bracket to the rear panel of the device



Step 3 Install the wall-mount bracket to the wall and clockwise screw the wall-mount bracket tightly, as shown in Figure 6-6.

Figure 6-6 Installing the wall-mount bracket on the wall



## 6.3 Grounding device

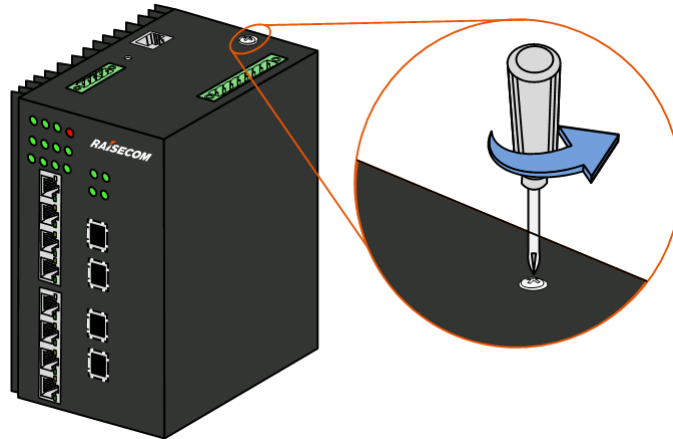
### Warning

Connecting the ground cable properly is an important guarantee for lightning protection, anti-electric shock, and anti-interference. The Gazelle S1512i-PWR must be connected to the ground cable correctly during installation, which helps avoid personal injury and equipment damage.

Connect the ground cable as below:

Step 1 Anticlockwise unfasten the screw of the ground terminal and properly keep the screw and washers, as shown in Figure 6-7.

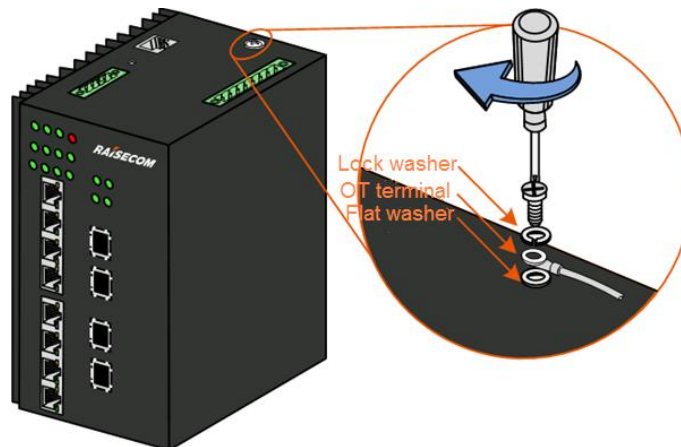
Figure 6-7 Unfastening the screw of the ground terminal



Step 2 Fit the OT terminal of the ground cable and washers to the screw in order.

Step 3 Install the screw to the ground terminal again and clockwise tighten the screw, as shown in Figure 6-8.

Figure 6-8 Connecting the ground cable



## 6.4 Connecting cables

### 6.4.1 Connecting LC/PC fiber

#### Caution

When the Gazelle S1512i-PWR is not used, you should put a dustproof cover on the optical interface to prevent dust and dirt from entering it to ensure that the Gazelle S1512i-PWR works normally.

#### Warning

There is invisible laser in the Gazelle S1512i-PWR, which may cause eye injury. Therefore, you should not look directly at the optical interface, head of the optical connector, or breakage of the fiber.

Connect the LC/PC fiber as below:

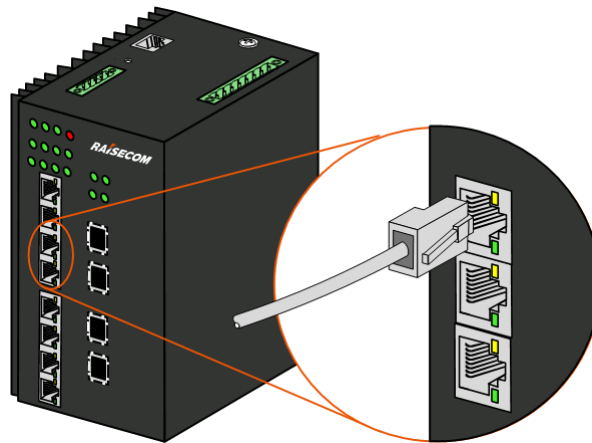
- Step 1 Insert the SFP optical module into the optical interface on the Gazelle S1512i-PWR.
- Step 2 Remove the dustproof covers of the optical module and fiber, and keep it for later use.
- Step 3 Align the connector with the optical interface to insert the fiber into the optical interface gently.
- Step 4 To remove the fiber, push the fiber connector inwards slightly, and pull out the fiber.

## 6.4.2 Connecting Ethernet cable

Connect the Ethernet cable as below:

- Step 1 Make the Ethernet cable according to specifications.
- Step 2 Align the Ethernet cable head with the Ethernet interface of the Gazelle S1512i-PWR and insert the Ethernet cable into the Ethernet interface gently, as shown in Figure 6-9.

Figure 6-9 Connecting the Ethernet cable



## 6.4.3 Connecting power cable

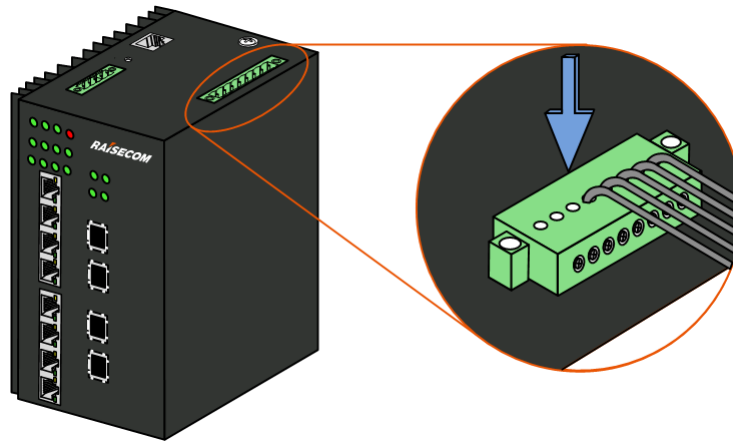
### Caution

- Ensure that the ground cable is grounded correctly before connecting the power cable.
- Disconnect all power supplies before connecting or removing the power cable.
- Use the power cable which meets the technical specifications.

The DC power interface on the Gazelle S1512i-PWR uses 5 PINs of the 8-pin Phoenix connector with spaces of 5.08 mm. Connect the power cable as below:

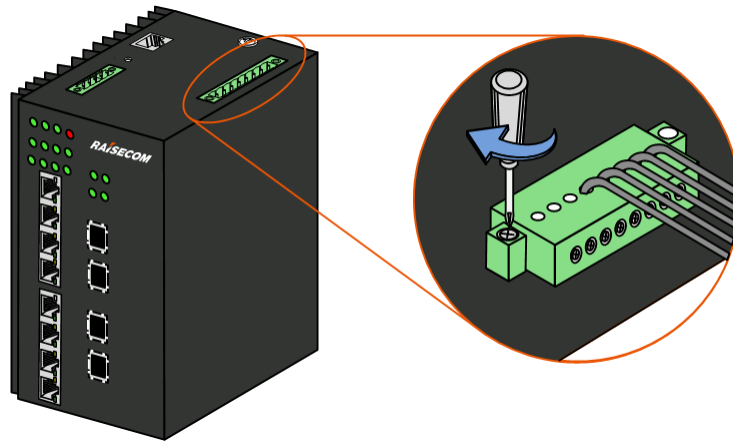
- Step 1 Make the DC power cable according to technical specifications.
- Step 2 Insert the DC power cable plug into the power interface on the Gazelle S1512i-PWR properly, as shown in Figure 6-10.

Figure 6-10 Connecting the connector of the DC power cable



Step 3 Fasten screws of the DC power cable tightly, as shown in Figure 6-11.

Figure 6-11 Fastening screws of the DC power cable



Step 4 Connect the other end of the DC power cable to the cabinet or the powering equipment in the equipment room.

## 6.5 Powering on device

Power on the Gazelle S1512i-PWR as below:

- Step 1 After the Gazelle S1512i-PWR is properly installed, connect the power cable to it.
- Step 2 After powering on it, the PWR LED is on, which means that the power is supplied to the Gazelle S1512i-PWR.
- Step 3 The Gazelle S1512i-PWR begins to operate properly after self-check and initialization. Interface LEDs indicate the working status of the interface (on, off, or blinking).

## 6.6 Checking installation

Table 6-2 lists items to be checked after installation.

Table 6-2 Items to be checked after installation

No.	Item	Method
1	Components of the Gazelle S1512i-PWR are installed properly and do not loose or fall off.	Check
2	All screws are tightened properly.	Check
3	Cables are connected correctly without looseness or virtual connection.	Check
4	Wiring of signal cables is compliant with the engineering design documents.	Check
5	Signal cables are not damaged, disconnected, or intermediately connected.	Check
6	Labels on the two ends of the signal cable are correct, distinct, and neat.	Check
7	Pigtail of fiber should be fit into a pipe sleeve or groove for protection and it should not be extruded by other cables or objects when it is placed outside the cabinet.	Check
8	The curvature radius of the fiber should be greater than 20 times of the diameter of the fiber. In general, the curvature radius of the fiber is greater than 40 mm.	Check
9	The power cable and ground cable are compliant with the engineering design documents for convenience of dilatation.	Check
10	The power cable and signal cable should be laid out separately.	Check
11	No stains or scratches on the Gazelle S1512i-PWR.	Check
12	The insurance capacity of the power can support the Gazelle S1512i-PWR to work normally as the maximum power consumption.	Use a tester.
13	When making the nose of the power cable or ground cable, you should ensure that it is welded or crimped firmly.	Check
14	The power cable and ground cable are connected reliably and the lock washer of the ground terminal is placed upon the flat washer.	Check
15	There is enough room for heat dissipation around the Gazelle S1512i-PWR and no heavy object is placed on it.	Check

# 7 Management and maintenance

---

This chapter describes management and maintenance of the Gazelle S1512i-PWR, including the following sections:

- Management modes
- Maintenance methods
- Troubleshooting strategy
- NView NNM system

## 7.1 Management modes

You can use the following methods to access the Gazelle S1512i-PWR for management and maintenance:

- CLI
- Web

### 7.1.1 CLI

#### Telnet management

The Telnet protocol is one of TCP/IP protocols and the standard protocol for Internet remote login. You can transfer the PC used by the local user to a terminal in remote host system through the Telnet protocol. Using the Telnet program on the terminal user's PC, you can log in to and manage the Gazelle S1512i-PWR.

#### SSH management

Secure Shell (SSH) is a protocol for secure remote login and other secure network services over an insecure network. When users undergo remote logins, SSH will automatically encrypt the data before transmission and decrypt them when the data arrive at the destination. By this way, SSH protects network devices from various attacks, such as plaintext password interception.

Moreover, SSH can replace Telnet to manage the remote device or provide a secure channel for FTP, and so on.

## 7.1.2 Web

The Gazelle S1512i-PWR provides Web management feature. You can log in to, manage, and maintain the Gazelle S1512i-PWR through the Web browser.

Web management employs the graphic management interface and is more easily to access compared with the CLI mode.

## 7.1.3 SNMP

Simple Network Management Protocol (SNMP) is designed by the Internet Engineering Task Force (IETF) to resolve problems in managing network devices connected to the Internet. Through SNMP, a network management system can manage all network devices that support SNMP, including monitoring network status, modifying configurations of a network device, and receiving network alarms. SNMP is the most widely used network management protocol in TCP/IP networks.

Till now, SNMP has three versions: v1, v2c, and v3, described as below.

- SNMPv1 uses community name authentication mechanism. The community name, a string defined by an agent, acts like a password. The network management system can visit the agent only by specifying its community name correctly. If the community name carried in a SNMP packet is not authorized by the Gazelle S1512i-PWR, the packet will be discarded.
- Compatible with SNMPv1, SNMPv2c also uses community name authentication mechanism. SNMPv2c supports more operation types, data types, and error codes, and thus better identifying errors.
- SNMPv3 uses User-based Security Model (USM) and View-based Access Control Model (VACM) security mechanism. You can configure whether USM authentication is enabled and whether encryption is enabled to provide higher security. USM authentication mechanism allows authenticated senders and prevents unauthenticated senders. Encryption is to encrypt packets transmitted between the network management system and agents, thus preventing interception.

The Gazelle S1512i-PWR supports v1, v2c, and v3 of SNMP.

## 7.2 Maintenance methods

The Gazelle S1512i-PWR caters to users' requirements on operation and maintenance in the aspects of hardware design and function configuration, thus providing users with powerful maintenance performance.

The Gazelle S1512i-PWR supports diagnosing and testing failures regarding software and hardware.

### 7.2.1 Ping

Packet Internet Grope (Ping) is the most widely used command for fault diagnosis and troubleshooting. It is usually used to detect whether two hosts are connected or not. Ping is achieved with ICMP echo packets. If an Echo Reply packet is sent back to the source address during a valid period after the Echo Request packet is sent to the destination address, it indicates the route between source and destination address is reachable.

## 7.2.2 Traceroute

Traceroute is used to discover the real route followed by the packet to transmit to the destination. Although the Ping feature can test the connectivity, it cannot record all network devices on the route limited by the IP head. Traceroute can be used to test routing information from the source host to the destination host.

## 7.2.3 Enviromental monitoring

Environmental monitoring is to monitor key parameters of the device, including temperature and voltage. When those parameters are abnormal, you can take corresponding measurements to prevent failures.

## 7.2.4 RMON management

Remote Network Monitoring (RMON) is a standard developed by the Internet Engineering Task Force (IETF). RMON is used to monitor network data through different Agents and NMS, and it mainly realizes statistical and alarm reporting functions. RMON is an extension of SNMP. However, compared with SNMP, ROMN is more active and efficient for monitoring remote devices. The administrator can quickly trace faults generated on the network, network segment, or device.

At present, RMON implements four function groups: statistic group, historical group, alarm group, and event group.

## 7.2.5 System log

The system log means that the device records the system information and debugging information in a log and sends the log to the specified destination. When the device fails, you can check and locate the fault easily.

The system information and some debugging output will be sent to the system log to process. According to the configuration, the system will send the log to various destinations. The destinations that receive the system log are divided into:

- Host: send the log message to the host.
- Monitor: send the log information to the monitor, such as Telnet terminal.
- File: send the log information to the Flash of the device.
- Buffer: send the log information to the buffer.
- SNMP server: transfer the log information into Trap and send it to the SNMP server.

## 7.2.6 Watchdog

Through configuring the watchdog feature, you can prevent the system program from endless loop caused by uncertain faults to improve the stability of system.

## 7.2.7 Port mirroring

Port mirroring refers to mirroring some packets of a specified source interface to the destination interface, namely, the monitor port, without affecting forwarding of normal packets. You can monitor packets sending and receiving on one interface by this function and analyze the relevant network status or fault conditions.



The Gazelle S1512i-PWR is in support of data stream mirroring on the ingress interface, egress interface, and both the ingress and egress interfaces. Packets received and sent by the mirroring port will be copied to the monitor port for analysis and monitoring after port mirroring is enabled. The monitor port and mirroring port cannot be the same one.

## 7.3 Troubleshooting strategy

Common switch faults include physical layer faults, MAC link layer faults, and data configuration faults, as listed in Table 7-1.

Table 7-1 Troubleshooting strategy

No.	Fault analysis	Troubleshooting method
1	Physical layer analyses	<ul style="list-style-type: none"> <li>• Check the operation status and environment of the device. Ensure that the device is installed properly and runs properly.</li> <li>• Check link status and LED status. Use the replacement method to confirm the fault point or section.</li> </ul>
2	Switch system analyses	<ul style="list-style-type: none"> <li>• Check the networking topology. Ensure that the network topology complies with device features.</li> <li>• Check alarms on the device or the NMS. Ensure that the device is configured correctly and versions of different devices are compatible.</li> </ul>
3	MAC link layer analyses	<ul style="list-style-type: none"> <li>• Check MAC address learning and VLAN partition to locate the faulty MAC address learning point or section.</li> <li>• Check whether MAC address learning on the device interface or chip is correct. Analyze network conditions, and rule out impact from viruses, attacks, and loops.</li> <li>• Check statistics on MAC addresses and VLANs on each interface to locate the fault.</li> </ul>
4	Data configuration analyses	<ul style="list-style-type: none"> <li>• Check whether data configurations comply with the customer's services and networking requirements. If no, correct data configurations.</li> <li>• Check whether data configurations are consistent with those of the interconnected devices. If no, correct data configurations.</li> </ul>
5	Protocol internetworking analyses	<ul style="list-style-type: none"> <li>• Check statistics on protocol packets, learn the interconnected device and its parameters, and analyze whether protocol parameters are correct.</li> <li>• Master the usage and analysis method of the packet capture tool and packet capture protocols, and analyze protocol error codes.</li> </ul>

## 7.4 NView NNM system

### 7.4.1 Functions

"Comprehensive Access, Overall Network Management" is a vision that Raisecom has been in pursuit of. The NView NNM system is developed to meet overall and efficient OAM

requirements. It is of complete functions, friendly User Interface (UI), and easy operations, and can meet requirements by service activation and daily maintenance.

The NView NNM system, based on SNMP, can perform centralized configurations and fault detection over all manageable devices of Raisecom. It has the following functions:

- Topology management: display network topology graphically, organize and manages nodes of various types and links between these nodes, and support automatic or manual planning of network functions.
- Alarm management: collect, classify, display, and manage all alarms reported by managed devices. It supports query, sorting, filtering, statistics, forwarding, and voice prompt.
- Performance management: enable you to view realtime or historical performance metrics, such as interfaces, traffic, and bandwidth utilization.
- Inventory management: manage physical inventory, such as devices, chassis, and interfaces.
- Customer management: manage information about all connected users, and allow the mapping between customer information and device/interface. This function helps quickly locate affected customers.
- Security management: support user account and password rules according to security management features in network management; control authorized access from a client according to the *Client Access Control List*; provide the Invalid Login Verification function, which will lock a user if the times of typing incorrect user name and password exceeds the configured number; provide security control policies based on level, authority, and domain; provide detailed system/device operation logs to facilitate you to control operation authorities.
- Service management: manage predefined system services through the application service management framework, such as Trap receiving service, alarm storm prevention service, and alarm forwarding service.
- Data center: enable you to manage devices, such as backing up, restoring, rolling back, and activating; enable you to manage upgradable files, backup files, operations, and logs for backup. The backup operation is easy, simple and with high security.
- Data downloading: download logs, historical alarms, and performance data from database as viewable files and then delete these data from database. This ensures efficient operation of database in the NView NNM system.

## 7.4.2 Features

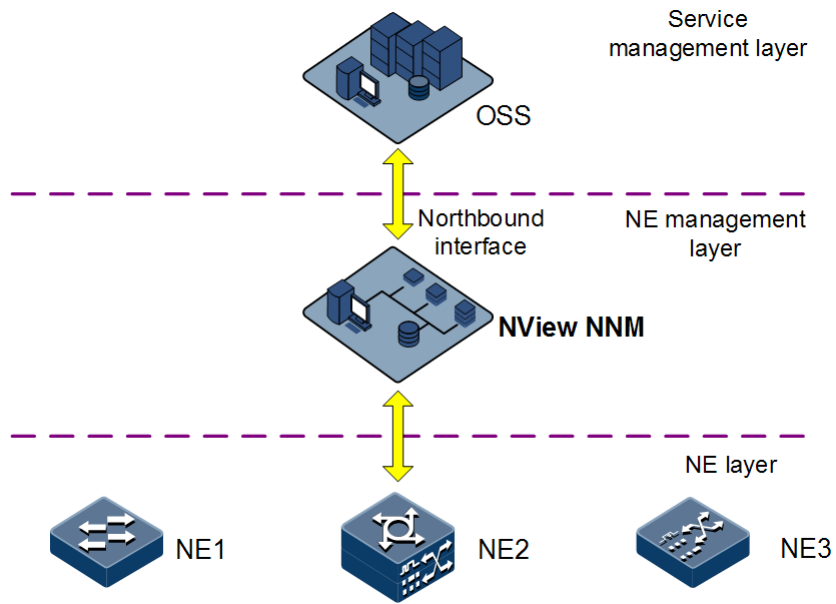
The NView NNM system has the following features:

- Work as the uniform platform for all manageable devices of Raisecom.
- Uniformly manage data network and transport network.
- Provide strong NE-level management and subnet-level management.
- Provide northbound interfaces for integration with the OAM system, such as COBRA, SNMP, JDBC, and SOCKET interfaces.
- Communicate with NE-level devices through SNMP in southbound. With module design, it supports flexible deployment according to actual situation.

Able to be interconnected to the Operation Support System (OSS), the NView NNM system implements OAM functions between the OSS and NEs through the northbound interface, such as service activation, alarm reporting, alarm synchronization, fault diagnosis, and periodical inspection.

Figure 7-1 shows the orientation of the NView NNM system.

Figure 7-1 Orientation of the NView NNM system



# 8 Appendix

---

This chapter lists terms, acronyms, and abbreviations involved in this document, including and following sections:

- Terms
- Acronyms and abbreviations

## 8.1 Terms

### A

Access Control List (ACL)	A series of ordered rules composed of permit   deny sentences. These rules are based on the source MAC address, destination MAC address, source IP address, destination IP address, interface ID, and so on. The device decides to receive or refuse the packets based on these rules.
Automatic Laser Shutdown (ALS)	The technology that is used for automatically shutting down the laser to avoid the maintenance and operation risks when the fiber is pulled out or the output power is over great.
Auto-negotiation	The interface automatically chooses the rate and duplex mode according to the result of negotiation. The auto-negotiation process is: the interface adapts its rate and duplex mode to the highest performance according to the peer interface, that is, both ends of the link adopt the highest rate and duplex mode they both support after auto-negotiation.
Automatic Protection Switching (APS)	APS is used to monitor transport lines in real time and automatically analyze alarms to discover faults. When a critical fault occurs, through APS, services on the working line can be automatically switched to the protection line, thus the communication is recovered in a short period.

### B

Bracket	Small parts at both sides of the chassis, used to install the chassis into the cabinet
---------	--

## C

**Challenge Handshake Authentication Protocol (CHAP)** CHAP is a widely supported authentication method in which a representation of the user's password, rather than the password itself, is sent during the authentication process. With CHAP, the remote access server sends a challenge to the remote access client. The remote access client uses a hash algorithm (also known as a hash function) to compute a Message Digest-5 (MD5) hash result based on the challenge and a hash result computed from the user's password. The remote access client sends the MD5 hash result to the remote access server. The remote access server, which also has access to the hash result of the user's password, performs the same calculation using the hash algorithm and compares the result to the one sent by the client. If the results match, the credentials of the remote access client are considered authentic. A hash algorithm provides one-way encryption, which means that calculating the hash result for a data block is easy, but determining the original data block from the hash result is mathematically infeasible.

## D

**Dynamic ARP Inspection (DAI)** A security feature that can be used to verify the ARP data packets in the network. With DAI, the administrator can intercept, record, and discard ARP packets with invalid MAC address/IP address to prevent common ARP attacks.

**Dynamic Host Configuration Protocol (DHCP)** A technology used for assigning IP address dynamically. It can automatically assign IP addresses for all clients in the network to reduce workload of the administrator. In addition, it can realize centralized management of IP addresses.

## E

**Ethernet in the First Mile (EFM)** Complying with IEEE 802.3ah protocol, EFM is a link-level Ethernet OAM technology. It provides the link connectivity detection, link fault monitoring, and remote fault notification for a link between two directly-connected devices. EFM is mainly used for the Ethernet link on edges of the network accessed by users.

**Ethernet Ring Protection Switching (ERPS)** It is an APS protocol based on ITU-T G.8032 standard, which is a link-layer protocol specially used for the Ethernet ring. In normal conditions, it can avoid broadcast storm caused by the data loop on the Ethernet ring. When the link or device on the Ethernet ring fails, services can be quickly switched to the backup line to enable services to be recovered in time.

## F

**Full duplex** In a communication link, both parties can receive and send data concurrently.

## G

**GFP encapsulation** Generic Framing Procedure (GFP) is a generic mapping technology. It can group variable-length or fixed-length data for unified adaption, making data services transmitted through multiple high-speed physical transmission channels.

**Ground cable** The cable to connect the device to ground, usually a yellow/green coaxial cable. Connecting the ground cable properly is an important guarantee for lightning protection, anti-electric shock, and anti-interference.

## H

**Half duplex** In a communication link, both parties can receive or send data at a time.

## I

**Institute of Electrical and Electronics Engineers (IEEE)** A professional society serving electrical engineers through its publications, conferences, and standards development activities. The body responsible for the Ethernet 802.3 and wireless LAN 802.11 specifications.

**Internet Assigned Numbers Authority (IANA)** The organization operated under the IAB. IANA delegates authority for IP address-space allocation and domain-name assignment to the NIC and other organizations. IANA also maintains a database of assigned protocol identifiers used in the TCP/IP suite, including autonomous system numbers.

**Internet Engineering Task Force (IETF)** A worldwide organization of individuals interested in networking and the Internet. Managed by the Internet Engineering Steering Group (IESG), the IETF is charged with studying technical problems facing the Internet and proposing solutions to the Internet Architecture Board (IAB). The work of the IETF is carried out by various working groups that concentrate on specific topics, such as routing and security. The IETF is the publisher of the specifications that led to the TCP/IP protocol standard.

## L

**Label** Symbols for cable, chassis, and warnings

**Link Aggregation** With link aggregation, multiple physical Ethernet interfaces are combined to form a logical aggregation group. Multiple physical links in one aggregation group are taken as a logical link. Link aggregation helps share traffic among member interfaces in an aggregation group. In addition to effectively improving the reliability on links between devices, link aggregation can help gain greater bandwidth without upgrading hardware.

Link Aggregation Control Protocol (LACP)	A protocol used for realizing link dynamic aggregation. The LACPDU is used to exchange information with the peer device.
Link-state tracking	Link-state tracking provides an interface linkage scheme, extending the range of link backup. Through monitoring upstream links and synchronizing downstream links, faults of the upstream device can be transferred quickly to the downstream device, and primary/backup switching is triggered. In this way, it avoids traffic loss because the downstream device does not sense faults of the upstream link.
<b>M</b>	
Multi-mode fiber (MMF)	In this fiber, multi-mode optical signals are transmitted.
<b>N</b>	
Network Time Protocol (NTP)	A time synchronization protocol defined by RFC1305. It is used to synchronize time between distributed time server and clients. NTP is used to perform clock synchronization on all devices that have clocks in the network. Therefore, the devices can provide different applications based on a unified time. In addition, NTP can ensure a very high accuracy with an error of 10ms or so.
<b>O</b>	
Open Shortest Path First (OSPF)	An internal gateway dynamic routing protocol, which is used to decide the route in an Autonomous System (AS)
Optical Distribution Frame (ODF)	A distribution connection device between the fiber and a communication device. It is an important part of the optical transmission system. It is mainly used for fiber splicing, optical connector installation, fiber adjustment, additional pigtail storage, and fiber protection.
<b>P</b>	
Password Authentication Protocol (PAP)	PAP is an authentication protocol that uses a password in Point-to-Point Protocol (PPP). It is a twice handshake protocol and transmits unencrypted user names and passwords over the network. Therefore, it is considered insecure.
Point-to-point Protocol over Ethernet (PPPoE)	PPPoE is a network protocol for encapsulating PPP frames in Ethernet frames. With PPPoE, the remote access device can control and account each access user.

**Private VLAN (PVLAN)** PVLAN adopts Layer 2 isolation technology. Only the upper VLAN is visible globally. The lower VLANs are isolated from each other. If you partition each interface of the switch or IP DSLAM device into a lower VLAN, all interfaces are isolated from each other.

## Q

**QinQ** 802.1Q in 802.1Q (QinQ), also called Stacked VLAN or Double VLAN, is extended from 802.1Q and defined by IEEE 802.1ad recommendation. This VLAN feature allows the equipment to add a VLAN tag to a tagged packet. The implementation of QinQ is to add a public VLAN tag to a packet with a private VLAN tag, making the packet encapsulated with two layers of VLAN tags. The packet is forwarded over the ISP's backbone network based on the public VLAN tag and the private VLAN tag is transmitted as the data part of the packet. In this way, the QinQ feature enables the transmission of the private VLANs to the peer end transparently. There are two QinQ types: basic QinQ and selective QinQ.

**Quality of Service (QoS)** A network security mechanism, used to solve problems of network delay and congestion. When the network is overloaded or congested, QoS can ensure that packets of important services are not delayed or discarded and the network runs high efficiently. Depending on the specific system and service, it may relate to jitter, delay, packet loss ratio, bit error ratio, and signal-to-noise ratio.

## R

**Rapid Spanning Tree Protocol (RSTP)** Evolution of the Spanning Tree Protocol (STP), which provides improvements in the speed of convergence for bridged networks

**Remote Authentication Dial In User Service (RADIUS)** RADIUS refers to a protocol used to authenticate and account users in the network. RADIUS works in client/server mode. The RADIUS server is responsible for receiving users' connection requests, authenticating users, and replying configurations required by all clients to provide services for users.

## S

**Simple Network Management Protocol (SNMP)** A network management protocol defined by Internet Engineering Task Force (IETF) used to manage devices in the Internet. SNMP can make the network management system to remotely manage all network devices that support SNMP, including monitoring network status, modifying network device configurations, and receiving network event alarms. At present, SNMP is the most widely-used network management protocol in the TCP/IP network.



Simple Network Time Protocol (SNTP)	SNTP is mainly used for synchronizing time of devices in the network.
Single-Mode Fiber (SMF)	In this fiber, single-mode optical signals are transmitted.
Spanning Tree Protocol (STP)	STP can be used to eliminate network loops and back up link data. It blocks loops in logic to prevent broadcast storms. When the unblocked link fails, the blocked link is re-activated to act as the backup link.
<b>V</b>	
Virtual Local Area Network (VLAN)	VLAN is a protocol proposed to solve broadcast and security issues for Ethernet. It divides devices in a LAN into different segments logically rather than physically, thus implementing multiple virtual work groups which are based on Layer 2 isolation and do not affect each other.
VLAN mapping	VLAN mapping is mainly used to replace the private VLAN Tag of the Ethernet service packet with the ISP's VLAN Tag, making the packet transmitted according to ISP's VLAN forwarding rules. When the packet is sent to the peer private network from the ISP network, the VLAN Tag is restored to the original private VLAN Tag according to the same VLAN forwarding rules. Thus, the packet is sent to the destination correctly.

## 8.2 Acronyms and abbreviations

<b>A</b>	
AAA	Authentication, Authorization, and Accounting
ABR	Area Border Router
AC	Alternating Current
ACL	Access Control List
ANSI	American National Standards Institute
APS	Automatic Protection Switching
ARP	Address Resolution Protocol
AS	Autonomous System
ASE	Autonomous System External
AWG	American Wire Gauge

### **B**

---

BC	Boundary Clock
BDR	Backup Designated Router
BITS	Building Integrated Timing Supply System
BOOTP	Bootstrap Protocol
BPDU	Bridge Protocol Data Unit
BTS	Base Transceiver Station
<b>C</b>	
CAR	Committed Access Rate
CAS	Channel Associated Signaling
CBS	Committed Burst Size
CE	Customer Edge
CHAP	Challenge Handshake Authentication Protocol
CIDR	Classless Inter-Domain Routing
CIR	Committed Information Rate
CIST	Common Internal Spanning Tree
CLI	Command Line Interface
CoS	Class of Service
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
CST	Common Spanning Tree
<b>D</b>	
DAI	Dynamic ARP Inspection
DBA	Dynamic Bandwidth Allocation
DiffServ	Differentiated Service
DNS	Domain Name System
DRR	Deficit Round Robin
DS	Differentiated Services
DSL	Digital Subscriber Line
<b>E</b>	
EAP	Extensible Authentication Protocol

---

EAPoL	EAP over LAN
EFM	Ethernet in the First Mile
EMC	Electro Magnetic Compatibility
EMI	Electro Magnetic Interference
EMS	Electro Magnetic Susceptibility
ERPS	Ethernet Ring Protection Switching
ESD	Electro Static Discharge
<b>F</b>	
FCS	Frame Check Sequence
<b>G</b>	
GARP	Generic Attribute Registration Protocol
GE	Gigabit Ethernet
GMRP	GARP Multicast Registration Protocol
GPS	Global Positioning System
GVRP	Generic VLAN Registration Protocol
<b>H</b>	
HDLC	High-level Data Link Control
HTTP	Hyper Text Transfer Protocol
<b>I</b>	
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
IE	Internet Explorer
IEC	International Electro technical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IS-IS	Intermediate System to Intermediate System Routing Protocol
ISP	Internet Service Provider

ITU-T International Telecommunications Union - Telecommunication  
Standardization Sector

## L

LACP Link Aggregation Control Protocol  
LACPDU Link Aggregation Control Protocol Data Unit  
LAN Local Area Network  
LCAS Link Capacity Adjustment Scheme  
LLDP Link Layer Discovery Protocol  
LLDPDU Link Layer Discovery Protocol Data Unit

## M

MAC Medium Access Control  
MDI Medium Dependent Interface  
MDI-X Medium Dependent Interface cross-over  
MIB Management Information Base  
MSTI Multiple Spanning Tree Instance  
MSTP Multiple Spanning Tree Protocol  
MTBF Mean Time Between Failure  
MTU Maximum Transmission Unit  
MVR Multicast VLAN Registration

## N

NMS Network Management System  
NNM Network Node Management  
NTP Network Time Protocol  
NView NNM NView Network Node Management

## O

OAM Operation, Administration, and Management  
OC Ordinary Clock  
ODF Optical Distribution Frame  
OID Object Identifiers

Option 82 DHCP Relay Agent Information Option

## **P**

P2MP Point to Multipoint  
P2P Point-to-Point  
PADI PPPoE Active Discovery Initiation  
PADO PPPoE Active Discovery Offer  
PADS PPPoE Active Discovery Session-confirmation  
PAP Password Authentication Protocol  
PDU Protocol Data Unit  
PE Provider Edge  
PIM-DM Protocol Independent Multicast-Dense Mode  
PIM-SM Protocol Independent Multicast-Sparse Mode  
Ping Packet Internet Grope  
PPP Point to Point Protocol  
PPPoE PPP over Ethernet  
PTP Precision Time Protocol

## **Q**

QoS Quality of Service

## **R**

RADIUS Remote Authentication Dial In User Service  
RCMP Raisecom Cluster Management Protocol  
RED Random Early Detection  
RH Relative Humidity  
RIP Routing Information Protocol  
RMON Remote Network Monitoring  
RNDP Raisecom Neighbor Discover Protocol  
ROS Raisecom Operating System  
RPL Ring Protection Link  
RRPS Raisecom Ring Protection Switching  
RSTP Rapid Spanning Tree Protocol

---

RSVP	Resource Reservation Protocol
RTDP	Raisecom Topology Discover Protocol
<b>S</b>	
SCADA	Supervisory Control And Data Acquisition
SF	Signal Fail
SFP	Small Form-factor Pluggable
SFTP	Secure File Transfer Protocol
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SP	Strict-Priority
SPF	Shortest Path First
SSH	Secure Shell
STP	Spanning Tree Protocol
<b>T</b>	
TACACS+	Terminal Access Controller Access Control System
TC	Transparent Clock
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLV	Type Length Value
ToS	Type of Service
TPID	Tag Protocol Identifier
<b>U</b>	
UDP	User Datagram Protocol
USM	User-Based Security Model
<b>V</b>	
VLAN	Virtual Local Area Network
VRRP	Virtual Router Redundancy Protocol

**W**

WAN Wide Area Network

WRR Weight Round Robin

