

RIO1000 Series Industrial I/O Server User Manual

Document Version: 02 Release Date: 01/10/2023

Industrial Ethernet communication solutions experts

3onedata Co., Ltd.

Copyright © 2023 3onedata Co., Ltd. All rights reserved.

No company or individual is allowed to duplicate or transmit this manual in any forms without written permission issued by 3onedata Co., Ltd.

Trademark statement



30nedata, **30nedata** and **30ne data** are the registered trademark owned by

3onedata Co., Ltd. And other trademarks mentioned in this manual belong to their corresponding companies.

Note

Purchased product, service or features should be constrained by 3onedata commercial contracts and clauses. The whole or part product, service or features described in this document may beyond purchasing or using range. 3onedata won't make any statement or warranty for this document content unless any other appointment exists.

Due to product version upgrading or other reason, this document content will be upgraded periodically. Unless other appointment exists, this document only for usage guide, all statement, information and suggestion in this document won't constitute any warranty.



3onedata Co., Ltd.

Headquarter address:	3/B, Zone 1, Baiwangxin H District, Shenzhen, 518108 C	ligh Technology hina	Industrial	park,	Nanshan
Technology support:	tech-support@3onedata.com				
Service hotline:	+86-400-880-4496				
E-mail:	sales@3onedata.com				
Fax:	+86 0755-2670-3485				
Website:	http://www.3onedata.com	http://www.3onec	lata.com		



The device user manual describes the following contents:

- Network management method
- Overview of related principles of network management

Audience

This manual applies to the following engineers:

- Network administrators
- Technical support engineers

Text Format Convention

Format	Description	
	Words with "" represent the interface words. Fox example	
	"Port number".	
>	Multi-level path is separated by ">". Such as opening the	
	local connection path description: Open "Control Panel>	
	Network Connection> Local Area Connection".	
Light Blue Font	It represents the words clicked to achieve hyperlink. The font	
	color is as follows: 'Light Blue'.	
About this chapter	The section 'about this chapter' provide links to various	
	sections of this chapter, as well as links to the Principles	
	Operations Section of this chapter.	

Symbols

Format	Description
\land	Remind the announcements in the operation, improper
Notice	operation may result in data loss or equipment damage.

Format	Description
\wedge	Pay attention to the notes on the mark, improper operation
Warning	may cause personal injury.
	Conduct a necessary supplements and explanations for the
Note	description of operation content.
Key	Configuration, operation, or tips for device usage.
	Pay attention to the operation or information to ensure
Tips	success device configuration or normal working.

Port Convention

The port number in this manual is only an example, and does not represent the actual port with this number on the device. In actual use, the port number existing on the device shall prevail.

Revision Record

Version No.	Date	Revision note
01	6/18/2021	Product release
02	1/10/2023	Add point-to-point function

Content

P	REFA	CE	1
С	ONTE	2NT	1
1	LO	OG IN THE WEB INTERFACE	1
	1.1	WEB BROWSING SYSTEM REQUIREMENT	1
	1.2	SETTING IP ADDRESS OF PC	1
	1.3	LOG IN THE WEB CONFIGURATION INTERFACE	2
2	SY	STEM INFO	4
	2.1	PRODUCT INFORMATION	4
	2.2	NETWORK INFORMATION	5
3	NI	TWORK CONFIGURATION	7
4	C	OMMUNICATION SETTINGS	12
5	AI	DDRESS CONFIGURATION	14
	5.1	USER-DEFINED MODBUS ADDRESS	14
	5.2	DEFAULT ADDRESS	17
6	I/C	O CONFIGURATION	19
	6.1	DI SETTINGS	19
	6.2	DO SETTINGS	23
7	PC	DINT-TO-POINT CONFIGURATION	28
	7.1	RULE TABLE	28
	7.2	DO SAFE MODE SETTINGS	30
8	SN	[MP	32
	8.1	SNMP AGENT SETTINGS	32
9	AI	ARM SETTINGS	35
	9.1	E-MAIL ALERT CONFIGURATION	35
	9.2	SNMP TRAP ALARM CONFIGURATION	36
	9.3	IO TRAP SETTINGS	37
	9.4	SYSTEM ALERT SETTINGS	39
1() SY	STEM STATUS	41
	10.1	ROUTING TABLE	41
	10.2	SYSTEM NETWORK STATUS	42
	10.3	System Log	43
11	SY	STEM MANAGEMENT	49
	11.1	DEVICE INFORMATION CONFIGURATION	49

11.2	TIME SETTING	50
11.3	REMOTE MANAGEMENT	51
11.4	USER CONFIGURATION	52
11.5	IP Address Filtering	53
11.6 I	MAC FILTERING	55
11.7	STATIC ROUTING CONFIGURATION	57
11.8	DIAGNOSTIC TEST	60
11.8.1	Ping	60
11.8.2	2 Traceroute	61
11.8.3	Packet Capture Diagnosis	62
11.9	System Maintenance	63
11.9.1	Configure File Management	63
11.9.2	2 Restore Default Settings	64
11.9.3	Software Upgrade	65
12 MAIN	NTENANCE AND SERVICE	67
12.1 I	INTERNET SERVICE	67
12.2	Service Hotline	67
12.3 I	PRODUCT REPAIR OR REPLACEMENT	67



1.1 WEB Browsing System Requirement

Hardware and software	System requirements
CPU	Above Pentium 586
Memory	Above 128MB
Resolution	Above 1024x768
Color	256 color or above
Browser	Internet Explorer 6.0 or above
Operating system	Windows XP/7/8/10

Using this device, the system should meet the following conditions.

1.2 Setting IP Address of PC

The default management of device is as follows:

IP Settings	Default Value
IP address (LINK1)	192.168.1.254
Subnet mask	255.255.255.0

Note

The network configuration of the device supports single IP and double IP modes, and the default is double IP mode.

- In the single IP mode, the default IP address of Ethernet port LINK1/LINK2 is 192.168.1.254.
- In the Dual IP mode, the default IP address of Ethernet port LINK1 is 192.168.1.254, the default IP address of Ethernet port LINK2 is 192.168.8.254.

When configuring a device through the Web:

- Before conducting remote configuration, please confirm the route between computer and device is reachable.
- Before making a local configuration, make sure that the IP address of the computer and the serial server are on the same subnet.

	Note

While configuring the device for the first time, if the device is configured locally and accessed through LINK1, first confirm that the network segment of the current PC is 1.

Eg: Assume that the IP address of the current PC is 192.168.5.60, change the network segment "5" of the IP address to "1".

Operation Steps

Amendment steps as follow:

- Step 1 Open "Control Panel> Network Connection> Local Area Connection> Properties> Internet Protocol Version 4 (TCP / IPv4)> Properties".
- Step 2 Change the selected "5" in red frame of the picture below to "1".

Internet Protocol Version 4 (TCP/IPv4)	Properties		
General			
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.			
Obtain an IP address automatica	ally		
• Use the following IP address: —			
IP address:	192.168.5.60		
S <u>u</u> bnet mask:	255 . 255 . 255 . 0		
Default gateway:	192.168.5.1		
Obtain DNS server address auto	matically		
• Use the following DNS server ad	dresses:		
Preferred DNS server:	202 . 96 . 122 . 168		
Alternate DNS server:	202 . 96 . 134 . 133		
Validate settings upon exit	Ad <u>v</u> anced		
	OK Cancel		

Step 3 Click "OK", IP address is modified successfully.Step 4 End.

1.3 Log in the Web Configuration Interface

Operation Steps

Login in the web configuration interface as follow:

- Step 1 Run the computer browser.
- Step 2 Enter the address of the device "http://192.168.1.254" in the address bar of the browser.
- Step 3 Click the "Enter" key.
- **Step 4** Pop-up dialog box as shown below, enter the user name and password in the login window.

Username	admin
Password	
	Login
Sa	ve username Save password

Note:

- The default username and password are "admin"; please strictly distinguish capital and small letter while entering.
- Default username and password have the administrator privileges.

Step 5 Click "Login".

Step 6 End.

After login in successfully, user can configure relative parameters and information according to demands.



2.1 Product Information

Function Description

In "Device information" interface, user can check Device name,Device model, Serial No, Firmware Ver, Device time, Description, Number of LAN, CPU Utilization, Memory Utilization and so on.

Operation Path

Open in order: "System Maintenance > Device information".

Interface Description

The product information interface is as follows:



The main elements configuration description of device information interface:

Interface Element	Description
Device Name	Network identity or device type of the device.
Device Model.	Equipment model or name of the device.
Serial No.	Serial number of the device
Firmware Version	Software version information of the device.
Device Time	The current device time display, synchronizes the local PC
	or NTP server time.
Running Time	Current device running time after being powered on.
Description	Port information of the device.
Hardware Version	Current hardware version information, pay attention to the
	hardware version limits in software version.
Number of Lans	The network port number of the device.
CPU Usage	CPU usage of the current device.
Memory Usage	Memory usage of the current device.

2.2 Network information

Function Description

On the page of "Network information", user can check device network address information and DNS server information.

Operation Path

Open in order: "System Information" > Network Information".

Interface Description

Network information interface as follows:

Overview >	Device Information	Network Information	
Lan1 IP configuration IP address Netmask Gateway	Static 192.168.1.254 255.255.255.0	IPV6 configuration IPV6 address MAC address IPV6 Gateway	Disable 00:22:6f:85:d2:71
Lan2 IP configuration IP address Netmask Gateway	Static 192.168.8.254 255.255.255.0	IPV6 configuration IPV6 address MAC address IPV6 Gateway	Disable 00:22:6f:85:d2:72
DNS server DNS1 DNS2 IPV6 Primary DN IPV6 Secondary	S server DNS server		

The main elements configuration description of network information interface.

Interface Element	Description
LAN1	LAN1 information bar
IP Configuration	Shows how the LAN 1 of the device gets the IP address.
Netmask	Display device subnet mask.
MAC Address	Display device LAN 1 MAC address.
IP Address	Display LAN1 IP address.
Gateway	Display LAN1 gateway address.
LAN2	LAN2 information bar
IP Configuration	Shows how the LAN 2 of the device gets the IP address.
Netmask	Display device LAN2 subnet mask.
MAC Address	Display device LAN 2 MAC address.
IP Address	Display LAN2 IP address.
Gateway	Display LAN2 IP address.
DNS Server	DNS server information bar
DNS1	Display device main DNS server address.
DNS2	Display device backup DNS server address.



Function Description

On the "Network Settings" page, user can set the IP address and DNS address of this device. The IP address of the device supports DHCP/BOOTP protocol dynamic acquisition or static manual configuration. The device provides two Ethernet ports, which can work in single IP mode (redundant mode/switching mode) and dual IP mode to meet the requirements of various network environments.

Operation Path

Open: "Network Configuration".

Interface Description 1: Single IP

Single IP interface is as below:

Network Configuration		
LAN mode	Single IP V	
Mode configuration	Redundancy mode Switch n	node
LAN1		
LAN1 IP configuration	🔵 DHCP 🖲 Static 🔵 BOOTP	
LAN1 IP address	192.168.1.254	10.0.0.2
LAN1 Subnet Mask	255.255.255.0	255.255.255.0
LAN1 Gateway		10.0.0.1
LAN1 IPV6 configuration	🔵 AUTO 🔵 Static 💿 Disable	
LAN1 IPV6 address		2002:db8:0:f100::1
LAN1 IPV6 PrefixLen		0-128
LAN1 IPV6 Gateway		2002:db8:0:f100::1
DNS settings		
Primary DNS server		
Secondary DNS server		202.96.133.5
IPV6 Primary DNS server		
IPV6 Secondary DNS server		2002:db8:0:f100::1
LLDP configuration		
LLDP	🖲 Enable 🔵 Disable	
message transmission interva	I 30	5-32768
Submit Refresh		

Interface Description 2: Dual IP

Dual IP interface is as below:

Network Configuration		
LAN mode	Dual IP 🔻	
LAN1		
LAN1 IP configuration	OHCP Static BOOTP	
LAN1 IP address	192.168.1.254	10.0.0.2
LAN1 Subnet Mask	255.255.255.0	255.255.255.0
LAN1 Gateway		10.0.0.1
LAN1 IPV6 configuration	🔵 AUTO 🔵 Static 💿 Disable	
LAN1 IPV6 address		2002:db8:0:f100::1
LAN1 IPV6 PrefixLen		0-128
LAN1 IPV6 Gateway		2002:db8:0:f100::1
LAN2		
LAN2 IP configuration		
LAN2 ID address	DHCP Static BOOTP	40.0.0.0
LAN2 Public Mask		10.0.0.2
LAN2 Subhet Mask		255.255.255.0
LANZ Galeway		10.0.0.1
LAN2 IPV6 configuration	AUTO Static Disable	
LAN2 IPV6 address		2002:db8:0:f100::1
LAN2 IPV6 PrefixLen		0-128
LAN2 IPV6 Gateway		2002:db8:0:f100::1
DNS settings		
Primary DNS server		
Secondary DNS server		202.96.133.5
IPV6 Primary DNS server		
IPV6 Secondary DNS server		2002:db8:0:f100::1
	Enable Disable	
message transmission interval	30	5-32768
Submit Refresh]	

The main element configuration description of network configuration interface:

Interface Element	Description					
LAN Mode	The network mode drop-down list of the device can be					
	selected as follows:					
	• Single IP: the device ports LINK1 and LINK2 are in the same network LAN1;					
	• Dual IP: the device has dual IP and dual MAC addresses,					
	with port LINK1 in network LAN1 and port LINK2 in					
	network LAN2.					

Interface Element	Description
Mode	In the single IP mode, the operation mode of the equipment
Configuration	network port can be checked as follows:
_	 Redundancy mode: Ports LINK1 and LINK2 are
	redundant ports, which support link backup. One port is in
	active state and one port is in backup state;
	Switch mode: ports LINK1 and LINK2 are normal
	Ethernet ports.
LAN1	LAN1 Configuration Bar
LAN1 IP	Configuration of network address of device LAN 1:
Configuration	Obtain an IP address automatically(DHCP): Obtain an IP
	address, subnet mask, and gateway address
	automatically from DHCP server.
	• Manual setting: manually configure the IP address,
	subnet mask, and gateway address.
	BOOTP: Automatically obtain IP address, subnet mask
	and default gateway address from BOOTP(Bootstrap
	Protocol) server.
LAN1 IP Address	The IP address of the device LAN1 is 192.168.1.254 by
	default in manual setting mode.
LAN1 Subnet	The subnet mask of the device LAN1 is 255.255.255.0 by
Mask.	default in manual setting mode.
LAN1 Gateway	The gateway address of the device LAN 1 in manual setting
	mode.
LAN2	LAN2 configuration bar
LAN2 IP	Configuration of network address of device LAN 2:
Configuration	Obtain an IP address automatically(DHCP): Obtain an IP
	address, subnet mask, and gateway address
	automatically from DHCP server.
	Manual setting: manually configure the IP address,
	subnet mask, and gateway address.
	BOOTP: Automatically obtain IP address, subnet mask
	and default gateway address from BOOTP(Bootstrap
	Protocol) server.
LAN2 IP Address	The IP address of the device LAN2 is 192.168.8.254 by
	default in manual setting mode.
LAN2 Subnet	The subnet mask of the device LAN2 is 255.255.255.0 by
Mask.	default in manual setting mode.
LAN2 Gateway	The gateway address of the device LAN 2 in manual setting
	mode.

Interface Element		Description		
DNS Settings		DNS Settings Bar		
Primary	DNS	IP address of DNS server, for example: 202.96.133.4.		
Server				
Secondary	DNS	DNS Sever backup IP address, for example: 202.96.133.5.		
Server				



Function Description

On the "Communication Settings" page, you can configure the Modbus TCP connection timeout and communication watchdog time.

Operation Path

Open: "Communication Settings".

Interface Description

The Communication Settings interface as follows:

Communication Settings	
Enable Server Socket Idle Connection Timeout Interval	
60	sec(1-65535, default = 60, disable = 0)
Enable communication watchdog	
0	sec(1-65535, default = 0, disable = 0)
Auto clear alarm for Safe Mode	
Submit Refresh	

The main element configuration description of Communication Settings interface:

Interface Element	Description	
Enable Server Socket	Modbus TCP idle connection timeout, value range:	
Idle Connection	1-65535, unit: seconds. When the Modbus TCP idle	
Timedout Interval connection time exceeds the specified value, the de		
	will disconnect the corresponding Modbus TCP	
	connection.	
Enable Communication	Communication watchdog time in safe mode, value	
Watchdog	range: 1-65535, unit: s. When the Modbus TCP	

Interface Element	Description
	connection is lost or the interruption time exceeds the
	specified value, the system will enter the safe mode and
	the DO state will change to the set safe value.
Auto Clear Alarm for	When the Modbus TCP connection returns to normal, the
Safe Mode	system will exit the safe mode and automatically clear the
	safe mode alarm.



5.1 User-Defined Modbus Address

Function Description

On the "User-Defined Modbus Address" page, you can enable the Modbus TCP Slave protocol to customize the starting address and function code of the slave station.

Operation Path

Open in order: "Address Configuration > User-Defined Modbus Address ".

Interface Description

The Customize Address interface is as follow:

User-defined Modbus Addressing						
Patrach						
Enat	e Modbus/TCP Slave Protocol					
No.	Description	User-defined Start Address(DEC)	Function Code	Read/Write	Total Channels	Data Type
1	DO Value	0	01:COIL STATUS	RW	8	1bit
2	DO Pulse Status	16	01:COIL STATUS	RW	8	1bit
3	DO Value All Channel	32	03:HOLDING REGISTER •	RW	1	1WORD
4	DI Value	0	02:INPUT STATUS	R	8	1bit
5	DI Counter Value (Double Word)	16	04:INPUT REGISTER	R	8	2WORD
6	DI Value All Channel	48	04:INPUT REGISTER	R	1	1WORD
7	DI Counter Start/Stop	256	01:COIL STATUS	RW	8	1bit
8	DI Counter Reset	272	01:COIL STATUS	RW	8	1bit
9	P2P Connect Status	4096	02:INPUT STATUS	R	8	1bit
10	P2P Output Safe Flag	4112	02:INPUT STATUS	R	8	1bit
11	Clear P2P Output Safe Flag	4128	01:COIL STATUS	RW	8	1bit
12	Clear Watchdog Alarm	4144	01:COIL STATUS	RW	1	1bit
13	DO PulseCount	36	03:HOLDING REGISTER •	RW	8	1WORD
14	DO PulseOnWidth	52	03:HOLDING REGISTER •	RW	8	1WORD
15	DO PulseOffWidth	68	03:HOLDING REGISTER •	RW	8	1WORD
16	DI Counter Overflow Flag	1000	02:INPUT STATUS	R	8	1bit
17	Model Name	5000	04:INPUT REGISTER •	R	10	1WORD
18	Device Name	5040	04:INPUT REGISTER	R	30	1WORD
19	Device Up Time	5020	04:INPUT REGISTER	R	2	1WORD
20	Firmware Version	5029	04:INPUT REGISTER •	R	2	1WORD
21	Firmware Build Date	5031	04:INPUT REGISTER •	R	2	1WORD
22	Mac Address	5024	04:INPUT REGISTER	R	3	1WORD
23	IP Address	5027	04:INPUT REGISTER	R	2	1WORD
Subm	it Load Default					

The main elements configuration description of Customize Address interface:

Interface Element Description

Interface Element	Description		
Enable	When the Modbus/TCP Slave protocol is enabled, the device		
Modbus/TCP	will act as a Modbus TCP slave station, and the DI/DO,		
Slave Protocol	system information and other parameters of the device can be		
	read or configured through the Modbus TCP master station.		
SN.	Serial number.		
Description	DI/DO and system information parameter name of the device.		
User-Defined Start	The starting address of the parameter in the device register is		
Address (DEC)	the slave station address, and the value range is 0-65535.		
Function Code	The category of Modbus slave function code has the following		
	options:		
	01: COIL STATUS. Read/write coil, support Modbus		
	function codes 01, 05 and 15.		
	02: INPUT STATUS. Read input discrete quantity,		
	support Modbus function code 02.		
	• 03: HOLDING REGISTER. Read/write holding register,		
	support Modbus function codes 03, 06 and 16.		
	• 04: INPUT REGISTER. Read input register, support		
	Modbus function code 04.		
Read/write	Read and write privileges of the slave coil/register.		
Total Channels	The number of channels occupied by the slave station		
	address.		
Data Type	The unit size of the data type of the slave station.		
Load Default	The slave station address will load the factory configuration in		
	the "Default Address" page.		

The default address information table of Modbus slave station register:

Parameter	Description	Start	Function	Privilege	Length	Unit
name		Address	Code			
DO Value	DO channel status:	0	01	Read/writ	8	1 bit
	• 0: OFF			е		
	• 1: ON Status					
DO Pulse	DO pulse status:	16	01	Read/writ	8	1 bit
Status	• 0: stop			е		
	• 1: Enable					
DO Value All	DO channel status,	32	03	Read/writ	1	1WO
Channel	8bit corresponds to 8			е		RD
(Ch0-Ch7)	channels:					

Parameter	Description	Start	Function	Privilege	Length	Unit
name		Address	Code			
	• 0: OFF					
	1: ON Status					
DI Value	DI channel status:	0	02	Read	8	1 bit
	• 0: OFF					
	1: ON Status					
DI Counter	DI counter value,	16	04	Read	8	2WO
Value (Double	double word (high/low					RD
Word)	word).					
DI Value All	DI channel status,	48	04	Read	1	1WO
Channel	8bit corresponds to 8					RD
(Ch0-Ch7)	channels:					
	• 0: OFF					
DI Osumbar	1: ON Status	050	01	De e d/e mit	0	4 1-14
DI Counter	DI counter status:	256	01	Read/writ	8	1 DIT
Start/Stop	 0. stop 1: enable 			е		
DI Counter	1: recount and clear	272	01	Read/writ	8	1 bit
Reset	overflow.			е		
Clear	• 1: Watchdog	4144	01	Read/writ	1	1 bit
Watchdog	alarm triggered			е		
Alarm	• 0: clear					
	watchdog alarm					
DO	DO pulse counting.	36	03	Read/writ	8	1WO
PulseCount				е		RD
DO	DO pulse ON width,	52	03	Read/writ	8	1WO
PulseOnWidth	unit: ms.			е		RD
DO	DO pulse OFF width,	68	03	Read/writ	8	1WO
PulseOffWidth	unit: ms.			е		RD
DI Counter	DI Counter Overflow	1000	02	Read	8	1 bit
Overflow Flag	identification:					
	• 0: normal					
	• 1: overflow					
Model Name	Device model, ASCII	5000	04	Read	10	1WO
	code display.					RD
Device Name	Device name, ASCII	5040	04	Read	30	1WO
	code display.					RD

Parameter	Description	Start	Function	Privilege	Length	Unit
name		Address	Code			
Device Up	Running time, unit:	5020	04	Read	2	1WO
Time	seconds.					RD
Firmware	Software Version	5029	04	Read	2	1WO
Version						RD
Firmware Build	Software date, such	5031	04	Read	2	1WO
Date	as B20210526, the					RD
	first word is 2021, and					
	the last two bytes are					
	5 and 26.					
Mac Address	MAC Address, HEX	5024	04	Read	3	1WO
	display.					RD
IP Address	IP Address	5027	04	Read	2	1WO
						RD

5.2 Default Address

Function Description

On the "Default Address" page, you can view the default address information of Modbus TCP Slave register.

Operation Path

Open in order: "Address Configuration > Default Address".

Interface Description

The default address interface is as follow:

Default Modules Address Refrest No. Description User-defined Start Address(DEC) runction Code Read/Write Total Channels Data Type 1 DO Value 0 1 RV 8 1bit 2 DO Value All Channel 32 3 RV 8 1bit 3 DO Value All Channel 32 3 RV 1 1WORD 4 DI Value 0 2 R 8 1bit 5 Di Counter Value 16 4 R 8 1bit 6 U Value All Channel 4 R R 1 1WORD 6 DI Value All Channel 4 R R 1 1WORD 7 DI Counter Start/Stop 256 1 RW 8 1bit 8 DI Counter Start/Stop 256 1 RW 8 1bit 10 P2P Output Stafe Flag 412 RW 8 <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>							
Refresh Vertresh User-defined Address(DEC) Sunction Code Address(DEC) Read/Write Total Channels Data Type 1 DO Value 0 1 Read/Write 8 1bit 2 DO Value All Channel 1 RW 8 1bit 3 DO Value All Channel 1 RW 8 1bit 4 DI Value All Channel 3 Adverse(DEC) RW 8 1bit 5 DO Cunter Value (Double Word) 16 4 R 8 1bit 6 DI Value All Channel 4 R 8 1bit 6 DI Value All Channel 4 R 1 1WORD 6 DI Value All Channel 4 R 8 1bit 7 DI Counter Status 406 2 RW 8 1bit 8 DI Counter Status 406 2 R 8 1bit 10 P2P Connect Status 4144 1 RW	Default Modbus Address						
Refrest Vesc-defined Address User-defined Start Address Function Code Address Read/Write Total Channels Data Type 1 DO Value 0 1 RW 8 1bit 2 DO Value All Channel 32 3 RW 8 1bit 3 DO Value All Channel 32 3 RW 1 1WORD 4 DI Value 0 2 R 8 1bit 5 DI Counter Value (Double Word) 16 4 R 1 1WORD 6 DI Value All Channel 48 4 R 1 1WORD 7 DI Counter Start/Stop 256 1 RW 8 1bit 8 DI Counter Start/Stop 272 1 RW 8 1bit 10 P2P Output SteFlag 4112 2 R 1bit 11 Clear P2P Output SteFlag 4128 RW 8 1bit 12 Clear Watching Alarm							
No.DescriptionUser-defined Adress(DEC)Function CodeRead/WriteTotal ChannelsData Type1DO Value01RW81bit2DO Pulse Status161RW81bit3DO Value All Channel323RW11WORD4DI Value02R81bit5DI Counter Value (Double Word)164R82WORD6DI Value All Channel484R11WORD7DI Counter Stat/Stop2561RW81bit8DI Counter Stat/Stop2561RW81bit9P2P Connect Status41122R81bit9P2P Output Staf Flag41122R81bit10Clear P2P Output Staf Flag41122R11bit11Sclear P2P Output363RW81bit13DO PulseComt363RW81WORD14DO PulseComt683RW81WORD14DO PulseComt5404R301WORD16DI Cunter Overflow Flag10002R301WORD17Model Name Flag50004R301WORD18Device Name Flag50204R21WORD19Device Name <br< td=""><td>Refres</td><td>1</td><td></td><td></td><td></td><td></td><td></td></br<>	Refres	1					
No.DescriptionStart Address(DEC)Function CodeRead/WriteTotal ChannelsData Type1DO Value01RW81bit2DO Pulse Status161RW81bit3DO Value Al Channel323RW11WORD4DI Value Al Channel323RW11WORD5DI Counter Value (Double Word)164R81bit5DI Counter Start/Stop2561RW81bit6DI Counter Start/Stop2561RW81bit9P2P Connect Status40962R81bit9P2P Connect Status4128RW81bit10P2P Cuptul Stafe Flag stafe Flag4128RW81bit11Stafe Flag4128RW81bit12Alarm4144RW81bit13DO PulseOnWidth523RW81WORD14DO PulseOnWidth523RW81WORD15DO PulseOfWidth683RW81WORD16Di Counter Overflow relag1002R301WORD15DO PulseOfWidth523RW301WORD16Di Counter Overflow relag5004R301WORD17Model Name5004 <td< td=""><td></td><td></td><td>User-defined</td><td></td><td></td><td></td><td></td></td<>			User-defined				
Address(DEC)Address(DEC)Address(DEC)Address(DEC)Address(DEC)1DO Value01RW81bit2DO Value All Channel323RW11WORD3DO Value All Channel323RW11WORD4DI Value02R81bit5DI Counter Value164R82WORD6DI Counter Start/Stop2561RW81bit8DI Counter Reset2721RW81bit9P2P Connect Status40962R81bit10P2P Connect Status41281RW81bit11Clear P2P Output Stafe Flag41281RW81bit12Clear Witchdog Alam41441RW81bit13DO PulseCount363RW81WORD14DO PulseGonWitd523RW81WORD15DO PulseGonWitd523RW81WORD16DI Counter Overflow Flag50004R3001WORD18Device Name50404R21WORD19Device Name50404R21WORD19Device Name50214R21WORD10Firmware Build Date50244R21WORD<	No.	Description	Start	Function Code	Read/Write	Total Channels	Data Type
IDO Value01RW8Ibit2DO Pulse Status161RW8Ibit3DO Value All Channel323RW1WORD4DI Value02R8Ibit5Di Counter Value (Double Word)164R82WORD6DI Value All Channel484R1WWORD6DI Value All Channel484R1IWORD7DI Counter Start/Stop2561RW8Ibit8DI Counter Reset2721RW8Ibit9P2P Connect Status40962R8Ibit10P2P Couput Stafe Flag41122R8Ibit11Clear P2P Output1122R8Ibit12Clear Valcholog Alarm41441RW8Ibit13DO PulseOrtWidth533RW8IWORD14DO PulseOrtWidth683RW8IWORD14DO PulseOrtWidth683RW8IWORD15DO PulseOrtWidth683RW8IWORD16DI Counter Overflow Flag10002R3Ibit17Model Name50004R30IWORD18Device Name50404R2IWORD			Address(DEC)				
1Do Value01NW5Init2Do Value All Channel323RW11WORD3Do Value All Channel323RW11WORD4DI Value02R81bit5DI Counter Value (Double Word)164R82WORD6DI Value All Channel484R11WORD7DI Counter Start/Stop2561RW81bit8DI Counter Reset2721RW81bit9P2P Connect Status40962R81bit10P2P Output Safe Flag41281RW81bit11Clear P2P Output Alarm41441RW81bit12Clear Watchdog Alarm41441RW81bit13DO PulseContri363RW81WORD14DO PulseContrivetflow Flag10002R81bit15DO PulseContri 04683RW81bit16DI Counter Overflow Flag10002R3001WORD18Device Up Time50204R21WORD19Device Up Time50244R21WORD21Firmware Build Date50314R21WORD22Mac Address50244 <t< td=""><td>1</td><td>DO Value</td><td>0</td><td>1</td><td>PW/</td><td>0</td><td>1bit</td></t<>	1	DO Value	0	1	PW/	0	1bit
2Do Fulse Status101RW31MW RD4Di Value02R81bit5Di Counter Value (Duble Word)164R82WORD6Di Value Ali Channel484R11WORD7Di Counter Stat/Stop2561RW81bit8Di Counter Stat/Stop2561RW81bit9P2P Connect Status4062R81bit10P2P Output41281RW81bit11Clear P2P Output Stafe Flag41281RW81bit12Clear P2P Output Alarm41441RW81WORD13DO PulseCount363RW81WORD14DO PulseCount363RW81WORD15DO PulseCount363RW81WORD16DI Counter Overflow Flag10002R301WORD18Device Up Time Stope44R301WORD19Device Up Time Stope50244R21WORD21Firmware Build Date Stope50244R31WORD22Mac Address Stope50244R31WORD23Wardenses Stope50244R31WORD24Mac Address Stope<	2	DO Value DO Pulco Statuc	16	1	PW/	0	161
3Do Value Al Channel 323RW1INCRD4D1 Value02R81015D1 Counter Value (Double Word)164R82WORD6D1 Value Al Channel (Double Word)484R11WORD7D1 Counter Start/Stop 2561RW81018D1 Counter Reset 	2	DO Value All Channel	22	3	PW/	1	1000
10102R001005Di Value164R82WORD6Di Value Al Channel484R11WORD7Di Counter Start/Stop2561RW81bit8Di Counter Start/Stop2561RW81bit9P2P Connect Status40962R81bit10P2P Output Sate Flag41122R81bit11Clear P2P Output Sate Flag41281RW81bit12Clear Watchdog Alam41441RW81bit13D O PulseCount363RW81WORD14D O PulseOnWidth523RW81WORD15D O PulseOnWidth523RW81bit16PI counter Overflow Flag10002R301WORD17Model Name50004R301WORD18Device Up Time50204R21WORD19Device Up Time50214R21WORD19Device Up Time50244R21WORD21Firmware Build Date50314R31WORD22Mac Address50244R31WORD23Ib Vidtress50244R31WORD<	3	DU Value All Chariner	0	2	P	0	1WORD
5Drouble Word (Double Word)164R82WORD6Di Value Al Channel 484R11WORD7Di Counter Start/Stop 2561RW81bit8Di Counter Start/Stop 2561RW81bit9P2P Connect Status 40962R81bit10P2P Output Safe Flag 41122R81bit11Clear P2P Output Alarm41281RW81bit12Clear Watchdog Alarm41441RW81bit13Do PulseCount Alarm363RW81WORD14Do PulseCount Flag363RW81WORD15Do PulseCount 063RW81bit16Di OuseOrtWidth 523RW81bit17Model Name50004R101WORD18Device Up Time Flag50294R21WORD19Device Up Time Funware Build Date S0314R21WORD21Firmware Build Date S0314R31WORD22Mac Address S024AR21WORD23Wickdress S024AR31WORD24Mac Address S024R31WORD25Mac Address S024AR31WORD26Mac Address S024 <td>4</td> <td>DI Value</td> <td>0</td> <td>2</td> <td>IX</td> <td>0</td> <td>IDIL</td>	4	DI Value	0	2	IX	0	IDIL
6DI Value All Channel484R11WORD7DI Counter Start/Stop2561RW81bit8DI Counter Reset2721RW81bit9P2P Connect Status40962R81bit10P2P Output Safe Flag41122R81bit11Clear P2P Output Alarm41281RW81bit12Clear Watchdog Alarm41441RW11bit13DO PulseContr363RW81WORD14DO PulseContr363RW81WORD15DO PulseContr/Width523RW81WORD16DI Counter Overflow Flag10002R301WORD17Model Name50004R301WORD18Device Up Time Timware Parison50294R21WORD19Device Up Time Timware Build Date 50314R21WORD22Mac Address So244R31WORD23Id Address Futor50244R31WORD24Mac Address Futor50244R31WORD23Id Address Futor50244R31WORD	5	(Double Word)	16	4	R	8	2WORD
7DI Counter Start/Stop 2561RW8Ibit8DI Counter Reset2721RW81bit9P2P Connect Status40962R81bit10P2P Output Stafe Flag41122R81bit11Clear P2P Output Stafe Flag41281RW81bit12Clear Valchdog Alarm41441RW11bit13DO PulseCount363RW81WORD14DO PulseCont/Vidth523RW81WORD15DO PulseOrtWidth683RW81WORD16DI Counter Overflow Flag10002R301WORD18Device Up Time Funder Stord50004R301WORD19Device Up Time Funder Stord50294R21WORD21Firmware Build Date Stord50314R21WORD22Mac Address Stord60244R31WORD23Id Address Stord60244R31WORD	6	DI Value All Channel	48	4	R	1	1WORD
8DI Counter Reset2721RW81bit9P2P Connet Status40962R81bit10P2P Output Status40962R81bit11Clear P2P Output41281RW81bit12Clear V2trohutA1281RW81bit13D O PulseCount363RW81WORD14D O PulseContVidth523RW81WORD15D O PulseOntVidth683RW81WORD16DI Counter Overflow Flag10002R81bit17Model Name50004R301WORD18Device Up Time50204R21WORD19Device Up Time50294R21WORD21Firmware Build Date50314R21WORD22Mac Adfress50244R21WORD23IP Adfress50244R21WORD	7	DI Counter Start/Stop	256	1	RW	8	1bit
9P2P Connect Status40962R81bit10P2P Output Safe Flag41122R81bit11Clear P2P Output Safe Flag41281RW81bit12Clear Watchdog Alarm41441RW11bit13D O PulseCount363RW81WORD14D O PulseOnWidth523RW81WORD15D O PulseOtWidth683RW81WORD16DI Counter Overflow Flag10002R301bit17Model Name50004R101WORD18Device Up Time Flag50204R21WORD19Device Up Time Firmware Wersion50294R21WORD21Firmware Build Date Flag50314R31WORD22Mac Address Firmware Stores50244R31WORD	8	DI Counter Reset	272	1	RW	8	1bit
10P2P Output Safe Flag41122R81bit11 $\begin{array}{c} Clear P2P Output Safe Flag Safe Safe Safe Safe Safe Safe Safe Safe$	9	P2P Connect Status	4096	2	R	8	1bit
11Clear P2P Output Safe Flag41281RW81bit12Clear Watchdog Alarm1441RW11bit13D P Ulse Count363RW81WORD14D O Pulse OnVidth523RW81WORD15D O Pulse OnVidth683RW81WORD16D Counter Overflow Flag10002R81bit17Model Name50004R101WORD18Device Up Time50404R301WORD19Device Up Time50294R21WORD21Firmware Build Date50314R21WORD22Mac Address50244R31WORD23IP Address50244R21WORD	10	P2P Output Safe Flag	4112	2	R	8	1bit
12Clear Watchdog Alam41441RW1Ibit13Do PulseCount363RW81WORD14Do PulseOnWidth523RW81WORD15Do PulseOnWidth683RW81WORD16Di Counter Overflow Flag10002R101WORD17Model Name50004R101WORD18Device Up Time Filer Stold50204R21WORD19Device Up Time Filer Stold50294R21WORD21Firmware Build Date Filer Stold50314R21WORD22Mac Address Folder Stold50244R31WORD	11	Clear P2P Output Safe Flag	4128	1	RW	8	1bit
13DO PulseCount363RW81WORD14DO PulseOnWidth523RW81WORD15DO PulseOnWidth683RW81WORD16D Counter Overflow Flag10002R81bit17Model Name50004R101WORD18Device Name50404R301WORD19Device Unime50204R21WORD20Firmware Version50294R21WORD21Firmware Build Date50314R21WORD22Mac Address50244R31WORD	12	Clear Watchdog Alarm	4144	1	RW	1	1bit
14DO PulseOnWidth523RW81WORD15DO PulseOnWidth683RW81WORD16DI Counter Overflow Flag10002R81bit17Model Name50004R101WORD18Device Up Time Solon50404R301WORD19Device Up Time Firmware Version50294R21WORD21Firmware Solo14R21WORD22Mac Address50244R31WORD23IP Address50244R31WORD	13	DO PulseCount	36	3	RW	8	1WORD
15DO PulseOffWidth683RW81WORD16DI Counter Overflow Flag10002R81bit17Model Name50004R101WORD18Device Name50404R301WORD19Device Up Time50204R21WORD20Firmware Version50294R21WORD21Firmware Build Date50314R21WORD22Mac Address50244R31WORD	14	DO PulseOnWidth	52	3	RW	8	1WORD
16 DI Counter Overflow Flag 1000 2 R 8 1bit 17 Model Name 5000 4 R 10 1WORD 18 Device Name 5040 4 R 30 1WORD 19 Device Up Time 5020 4 R 2 1WORD 20 Firmware Version 5029 4 R 2 1WORD 21 Firmware Build Date 5031 4 R 2 1WORD 22 Mac Address 5024 4 R 3 1WORD	15	DO PulseOffWidth	68	3	RW	8	1WORD
17 Model Name 5000 4 R 10 1WORD 18 Device Name 5040 4 R 30 1WORD 19 Device Up Time 5020 4 R 2 1WORD 20 Firmware Version 5029 4 R 2 1WORD 21 Firmware Build Date 5031 4 R 2 1WORD 22 Mac Address 5024 4 R 3 1WORD	16	DI Counter Overflow Flag	1000	2	R	8	1bit
18 Device Name 5040 4 R 30 1WORD 19 Device Up Time 5020 4 R 2 1WORD 20 Firmware Version 5029 4 R 2 1WORD 21 Firmware Build Date 5011 4 R 2 1WORD 22 Mac Address 5024 4 R 3 1WORD 23 IP Address 5027 4 R 2 1WORD	17	Model Name	5000	4	R	10	1WORD
19 Device Up Time 5020 4 R 2 1WORD 20 Firmware Version 5029 4 R 2 1WORD 21 Firmware Build Date 5031 4 R 2 1WORD 22 Mac Address 5024 4 R 3 1WORD 23 IP Address 5027 4 R 2 1WORD	18	Device Name	5040	4	R	30	1WORD
20 Firmware Version 5029 4 R 2 1WORD 21 Firmware Build Date 5031 4 R 2 1WORD 22 Mac Address 5024 4 R 3 1WORD 23 IP Address 5027 4 R 2 1WORD	19	Device Up Time	5020	4	R	2	1WORD
21 Firmware Build Date 5031 4 R 2 1WORD 22 Mac Address 5024 4 R 3 1WORD 23 I/A Address 5027 4 R 2 1WORD	20	Firmware Version	5029	4	R	2	1WORD
22 Mac Address 5024 4 R 3 1WORD	21	Firmware Build Date	5031	4	R	2	1WORD
23 IP Address 5027 4 P 2 1WOPD	22	Mac Address	5024	4	R	3	1WORD
	23	IP Address	5027	4	R	2	1WORD



6.1 DI Settings

Function Description

On the "DI Settings" page, you can configure the working mode and view the status of DI channel.

Operation Path

Open in order: "I/O Configuration > DI Settings".

Interface Description

DI configuration interface as follows:

DI Setting					
Refres	h				
DI Channel	Mode	Status	Filter	Counter Trigger	Operate
DI-00	DI	OFF	100.0 ms		Edit
DI-01	DI	OFF	100.0 ms		Edit
DI-02	DI	OFF	100.0 ms		Edit
DI-03	DI	OFF	100.0 ms		Edit
DI-04	DI	OFF	100.0 ms		Edit
DI-05	DI	OFF	100.0 ms		Edit
DI-06	DI	OFF	100.0 ms		Edit
DI-07	DI	OFF	100.0 ms		Edit

The main element configuration description of DI configuration interface:

Interface Element	Description

Interface Element	Description			
DI Channel	DI channel name.			
Mode	The current operation mode of DI channel displays as follows:			
	• DI: DI mode, it detects the status of DI channel.			
	Counter: Counter mode, it detects the change of DI			
	channel status.			
Status	The current status of DI channel is shown as follows:			
	OFF (OFF alias): DI mode status;			
	ON (ON alias): DI mode status;			
	STOP: Counter mode status;			
	In Counter mode, trigger counting.			
	Note: DI channel supports dry contact and wet contact (NPN or PNP) and other connection modes:			
	• When used as a dry contact, OFF indicates open circuit and ON			
	indicates short circuit with GND;			
	• When used as a wet contact NPN, OFF indicates 10~30V and			
	ON indicates 0~3V;			
	• When used as wet contact PNP, OFF indicates $0 \sim 3V$ and ON			
	indicates 10~30V.			
Filter	The filtering time of DI channel, unit: Ms. Within the specified			
	filtering time, the DI channel state changes and recovers, and			
	the generated trigger count or state change will be filtered out.			
Counter Trigger	Trigger mode of DI counter, as shown below:			
	• Lo to Hi: DI channel changes from high level to low level;			
	• Hi to Lo: DI channel changes from low level to high level;			
	• Both: "Lo to Hi"和"Hi to Lo".			
Operate	Click "Edit" button to modify the mode and parameter of			
	current DI channel.			

On the DI settings page, click "Edit" to enter the mode settings page.

Interface description: Edit-DI Mode

The Edit-DI mode interface is as follows:

			Х
Curre	nt Setting		
	Model	DI 🔹	
	Filter	100	
Apply	to all DI channels		
Alias	Name		
	Alias name of channel	DI-00	
	Alias name of 'OFF' status	OFF	
	Alias name of 'ON' status	ON	
	Submit Close		

The configuration description of main elements of the Edit-DI Mode interface:

Interface Element	Description
Current setting	The configuration bar of mode settings.
Model	The drop-down list of DI channel work mode, the options are
	as follows:
	• DI
	Counter
Filter	The filtering time of DI channel, unit: Ms. Within the specified
	filtering time, the DI channel state changes and recovers, and
	the generated trigger count or state change will be filtered out.
Apply to all DI	Check the "Apply to all" check box to apply the mode setting
channels	parameters to all DI channels.
Alias Name	The configuration bar of alias settings.
Alias Name of	DI channel name, which can be customized.
Channel	Note:
	Aliases do not support Chinese and characters as "&";'/\:".
Alias Name of	DI channel OFF status name.
OFF Status	Note:
-	Aliases do not support Chinese and characters as "&";'/\:".
Alias Name of ON	DI channel ON status name.
Status	Note:
	Aliases do not support Chinese and characters as "&";' / \:".

On the mode setting page, select the "Counter" mode.

Interface Description: Edit—Counter Mode

The Edit-Counter mode interface is as follows:

	Х
Current Setting	
Model	Counter •
Filter	100
Counter Trigger	Lo to Hi 🔻
Counter Start/Enable	
Power On Setting	
Initial Counter Value Setting	
value	0
Reset Counter	
Count Transformation	
Enable Counter Scaling	
Result=Count Difference* 1 + 0	
Update every 5 sec	
Apply to all DI channels	
Alias Name	
Alias name of channel	DI-00
Alias name of 'OFF' status	OFF
Alias name of 'ON' status	ON
Submit Close	

The configuration description of main elements of the Edit—Counter interface:

Interface Element	Description			
Current Setting	The configuration bar of mode settings.			
Model	The drop-down list of DI channel work mode, the options are			
	as follows:			
	• DI			
	Counter			
Filter	The filtering time of DI channel, unit: Ms. Within the specified			
	filtering time, the DI channel state changes and recovers, and			
	the generated trigger count or state change will be filtered out.			
Counter Trigger	The drop-down list of DI counter trigger method, the options			
	are as follows:			
	• Lo to Hi: DI channel changes from high level to low level;			
	• Hi to Lo: DI channel changes from low level to high level;			
	• Both: "Lo to Hi"和"Hi to Lo".			
Counter	The start counting check box, check it to start the DI channel			
Start/Enable	trigger counting.			

Interface Element	Description			
Power On Settings	The boot setting check box, check it to start counting			
	immediately after the device is powered on. If unchecked,			
	after the device is powered on again, the DI count will be			
	cleared and the count will be turned off by default.			
Initial Counter	The initial setting check box, check it to define the initial count			
Value Setting	value.			
Value	When counting is started, the count value starts counting on			
	the initial value.			
Reset Counter	The recount check box. When checked, the count will be			
	cleared and the count will start again on the initial value.			
Count	The configuration bar of count conversion			
Transformation				
Enable Counter	The start count conversion check box. Check it to start the			
Scaling	count value conversion function. The transformation formula			
	is: Result=Count Difference * Gain + Offset. Count Difference			
	is the difference of the collected count value during the update			
	time. The value range of gain and offset is 0-4294967294.			
Update time	The update time of count conversion, value range:			
	0-4294967294, unit: s.			
Apply to all DI	Check the "Apply to all" check box to apply the mode setting			
Channels	parameters to all DI channels.			
Alias Name	The configuration bar of alias settings.			
Alias Name of	DI channel name, which can be customized.			
Channel	Note: Aliases do not support Chinese and characters as "&":'/\:".			
Alias Name of	DI channel OFF status name.			
OFF Status	Note:			
	Aliases do not support Chinese and characters as "&";'/\:".			
Alias Name of ON	DI channel ON status name.			
Status	Aliases do not support Chinese and characters as "&";' / \:".			

6.2 DO Settings

Function Description

On the "DO Settings" page, you can configure the working mode and control the status of DO channel.

Operation Path

Open in order: "I/O Configuration > DO Settings".

Interface Description

DO configuration interface is as follows:

DO Setting						
Refresh						
DO Channel	Mode	Status	ON Width	OFF Width	Operate	
DO-00	DO	OFF	-	-	Edit	
DO-01	DO	OFF			Edit	
DO-02	DO	OFF			Edit	
DO-03	DO	OFF			Edit	
DO-04	DO	OFF			Edit	
DO-05	DO	OFF			Edit	
DO-06	DO	OFF			Edit	
DO-07	DO	OFF			Edit	

The main element configuration description of DO configuration interface:

Interface Element	Description			
DO channel	DO channel name.			
Mode	The current operation mode of DO channel displays as			
	follows:			
	• DO: DO mode, it controls the status of DO channel.			
	Pulse Output: Pulse Output mode, pulse signal output.			
Status	The current status of DO channel is shown as follows:			
	OFF (OFF alias): DO mode status;			
	ON (ON alias): DO mode status;			
	STOP: Pulse Output mode status;			
	Pulse signal frequency under Pulse Output mode.			
ON Width	Time width of ON state under pulse mode, unit:ms.			
OFF Width	Time width of OFF state under pulse mode, unit:ms.			
Operate	Click "Edit" button to modify the mode and parameter of			
	current DO channel.			

On the DO settings page, click "Edit" to enter the mode settings page.

Interface Description: DO Mode

The Edit-DO mode interface is as follows:

	X
Current Setting	
Model	DO 🔻
DO Status	OFF 🔻
Power On Setting	OFF 🔻
Safe Status Setting	OFF 🔻
Power On Delay	0 Sec(Max:65535)
Apply to all DO channels	
Alias Name	
Alias name of channel	DO-00
Alias name of 'OFF' status	OFF
Alias name of 'ON' status	ON
Submit	Close

Interface Element	t Description				
Current setting	The configuration bar of current settings.				
Model	The drop-down list of DO channel work mode, the options are				
	as follows:				
	• DO				
	Pulse Output				
DO Status	The drop-down list of DO status. The options are as follows:				
	ON Status				
	• OFF				
Power On Settings	The drop-down list of boot settings, options as follows:				
	• ON: after the device is powered on, restore the DO state				
	or pulse count.				
	OFF				
Safe Status	The drop-down list of Security Status of DO channel. The				
Setting	options are as follows:				
	• ON: after entering the safe mode, the state of DO				
	channel is ON.				
	• OFF: after entering the safe mode, the state of DO				
	channel is OFF.				
	Hold LAST: after entering the safe mode, the state of DO				
	channel is the last hold state.				
	Note:				

The configuration description of main elements of the Edit-DO Mode interface:

Interface Element	Description			
	The "Communication Watchdog Time" needs to be enabled in the safe mode.			
Power On Delay	After the device is powered on, the delay time of DO channel			
	status, with a value range of 0-65535, unit: seconds.			
Apply to all DO	Check the "Apply to all" check box to apply the mode setting			
Channels	parameters to all DO channels.			
Alias Name	The configuration bar of alias settings.			
Alias Name of	DO channel name, which can be customized.			
Channel	Note: Aliases do not support Chinese and characters as "&";' / \:".			
Alias Name of	DO channel OFF status name.			
OFF Status	Note: Aliases do not support Chinese and characters as "&";' / \:".			
Alias Name of ON	DO channel ON status name.			
Status	Note: Aliases do not support Chinese and characters as "&";'/\:".			

On the mode setting page, select the "Pulse Output" mode.

Interface Description: Edit-Pulse Output Mode

The Edit-Pulse Output mode interface is as follows:

	Х
Current Setting	
Model	Pulse O V
ON Width	100
OFF Width	100
Pulse Count	0
Pulse Start	
Power On Setting	
Safe Status Setting	
Power On Delay	0 Sec(Max:65535)
Apply to all DO channels	
Alias Name	
Alias name of channel	DO-00
Alias name of 'OFF' status	OFF
Alias name of 'ON' status	ON
Submit	Close

The configuration description of main elements of the Edit-Pulse Output interface:

Interface Element	Description				
Current Settings	The configuration bar of mode settings.				
Model	In the drop-down list of DO channel work mode, the options				
	are as follows:				
	• DO				
	Pulse Output				
ON Width	ON state time width, value range: 1-65535, unit: ms.				
OFF Width	OFF state time width, value range: 1-65535, unit: ms.				
Pulse Count	Pulse number, the value range is 1-65535.				
Pulse Start	The start pulse check box, check it to start pulse counting.				
Power On Settings	The boot settings check box. After checking it, the device is				
	powered on to start pulse counting. If not checked, the pulse				
	counting will be turned off by default after the device is				
	powered on again.				
Safe Status	The safe state check box. After checking it, if you enter the				
Setting	safe mode, the DO channel will restart pulse counting. If				
	unchecked, there is no safe mode status.				
	Note: The "Communication Watchdog Time" needs to be suchlad in sofe				
	mode.				
Power On Delay	After the device is powered on, the delay time of pulse				
	counting, with a value range of 0-65535, unit: seconds.				
Apply to all DO	Check the "Apply to all" check box to apply the mode setting				
channels	parameters to all DO channels.				
Alias Name	The configuration bar of alias settings.				
Alias Name of	DO channel name, which can be customized.				
Channel	Note:				
Alias Namo of	Anases do not support Chinese and characters as \mathcal{X}^{*} , \mathcal{X}^{*} .				
OFF Status	Aliases do not support Chinese and characters as "&";' / \:".				
Alias Name of ON	DO channel ON status name.				
Status	Note:				
	Aliases do not support Chinese and characters as "&";'/\:".				

7 Point-to-Point Configuration

In some remote automation implementations, the control room and field sensors may be far away from each other, and usually only one remote I/O module collects data from all sensors. Point-to-point communication is almost unlimited, because it transmits input to output control by integrating multiple I/O signals on one network line, without the help of PLC or controller. This device has point-to-point communication and channel-to-channel mapping support, allowing simultaneous transmission of multiple targets. In addition, this device supports up to 16 channels of Ethernet transmission (based on transmitter and receiver I/O pair).

7.1 Rule Table

Function Description

In the rule table, I/O pairs for point-to-point communication can be configured.

Operation Path

Open in turn: "Address Configuration > Point-to-Point Configuration > Rule Table".

Interface Description

Rule Table									
Apply to No.									
1-10	11-20	21-30 31-4	0 41-50						
Enable	No.	Local Channel	Remote IP	Remote Port(1-65535)	Remote Channel	Interval Time(500-6	5535 ms)	On Change	Direction
	1	DO-05 *	192.168.1.253	9020	DI-06 V	≤ 500	ms		DO <- DI (Peer From)
	2	DI-01 *	0.0.0.0	9020	Ŧ	✓ 500	ms		DI -> DO (Peer to)
	3	DI-01 *	0.0.0.0	9020	v	✓ 500	ms		DI -> DO (Peer to)
	4	DI-01 *	0.0.0.0	9020		✓ 500	ms		DI -> DO (Peer to)
	5	DI-01 *	0.0.0.0	9020	Ŧ	✓ 500	ms		DI -> DO (Peer to)
	6	DI-01 *	0.0.0.0	9020	Ŧ	✓ 500	ms		DI -> DO (Peer to)
	7	DI-01 *	0.0.0.0	9020	V	✓ 500	ms		DI -> DO (Peer to)
	8	DI-01 *	0.0.0.0	9020	v	✓ 500	ms		DI -> DO (Peer to)
	9	DI-01 *	0.0.0.0	9020	Ŧ	✓ 500	ms		DI -> DO (Peer to)
	10	DI-01 *	0.0.0.0	9020	Ŧ	✓ 500	ms		DI -> DO (Peer to)
	11	DI-01 *	0.0.0.0	9020	Ŧ	✓ 500	ms		DI -> DO (Peer to)
	12	DI-01 *	0.0.0.0	9020	v	✓ 500	ms		DI -> DO (Peer to)
	13	DI-01 *	0.0.0.0	9020	T	✓ 500	ms		DI -> DO (Peer to)
	14	DI-01 *	0.0.0.0	9020	v	✓ 500	ms		DI -> DO (Peer to)
	15	DI-01 *	0.0.0.0	9020	v	✓ 500	ms		DI -> DO (Peer to)
	16	DI-01 *	0.0.0.0	9020	v	✓ 500	ms		DI -> DO (Peer to)
17 DI-01 ▼ 0.0.0.0 9020 ▼ 🕑 500 ms DI -> DO (Peer to)									
Local Listen Port 9020 (1-65535,Default:9020)									
Heart beat Interval time 60 sec(0-65535,default=60,disable=0)									
Subm	Submit Refresh								

The configuration description of main elements of the Edit-DI Mode interface:

Interface Element	Description		
Enable	If checked, a channel rule is enabled.		
Num	The serial number of the channel, which supports editing up		
	to 50 channel rules.		
Local channel	Configure local channel, DI or DO channel can be chosen.		
	After point-to-point configuration, the DO channel device will		
	act as a server and the DI channel device as a client.		
Destination	Address of peer device of point-to-point connection.		
Address			
Destination Port	Communication port set by the peer device.		
Destination	Connection channel of peer device.		
channel	This item needs to be configured only when the local		
	channel is configured as a DO channel;		
	• When the local channel is configured as DI channel, this		
	item cannot be configured.		
Interval Elapsed	Inform the peer device of the connection status of DI at		
	intervals.		
Change synapse	When checked, the peer device will be informed when t		
	connection status of DI changes.		
Direction	Display communication control direction.		
<u>3onedata</u>

Interface Element	Description
	• DO <- DI (Peer From);
	• DI -> DO (Peer to)。

7.2 DO Safe Mode Settings

Function Description

Configure the security sign of DO port, and display the connection status and security status.

Operation Path

Open in turn: "Address Configuration > Point-to-Point Configuration > DO Security Mode Settings".

Interface Description

DO Safe Mode Settings				
DO Channels	Mode	Sate Mode Flag	Connection Status	Safe Status
DO-01	DO	ON 🔻	OFF LINE	OFF
DO-02	DO	OFF 🔻	OFF LINE	OFF
DO-03	DO	OFF •	OFF LINE	OFF
DO-04	DO	OFF 🔻	OFF LINE	OFF
DO-05	DO	OFF 🔻	OFF LINE	OFF
DO-06	DO	OFF 🔻	OFF LINE	OFF
DO-07	DO	OFF 🔻	OFF LINE	OFF
DO-08	DO	OFF 🔻	OFF LINE	OFF
Submit	Clear_Safe_Flag	Refresh		

	c				
The main element	configuration	description	of DO	sate r	node interface:

Interface Element	Description	
DO channel	DO channel No.	
Mode	According to DO channel working mode, DO or Plusoutput.	
Safety sign	Safety sign is the output state of DO channel after triggering	
	safety state. Note: Whether DO is ON or OFF before triggering the safety state, after triggering the safety state, the safety state will change according to the value ON/OFF/HOLDLAST configured by DO.	
Connection status	Is there a DI to control the DO?	
	• ONLINE means connecting to the peer DI through TCP;	
	OFFLINE indicates that the TCP connection is	
	disconnected, and there is no DI to control the DO.	

<u>3onedata</u>

Interface Element	Description			
Security Status	It is a flag, which is determined by the "connection status". It is			
	OFF by default, and turns to ON when TCP connection is			
	successful and unexpected disconnection occurs. ON means			
	that the security state is triggered. If the flag is not cleared, the			
	security state will remain ON, indicating that the TCP			
	connection was accidentally disconnected.			
Apply	Click "Apply" to save current configuration.			
Clear mark	Reset all ON of the safe state to OFF.			
Refresh	Refresh the interface display.			



SNMP (Simple Network Management Protocol) is a network management standard protocol widely used in TCP/IP networks. SNMP provides a way to manage devices by running network management software on a central computer (or network management workstation).

SNMP System consists of NMS (Network Management System), Agent Process, Management Object and MIB (Management Information Base) four parts. Agent: Agent is an agent process in the managed device, which is used to maintain the information data of the managed device and respond to the request from the NMS, and report the administration data to the NMS that sending the request.

8.1 SNMP Agent Settings

Function Description

In the "SNMP Agent Settings" page, the SNMP function can be enabled and disabled, and other related parameters such as SNMP community name, version and user information can be configured.

Operation Path

Open in order: "SNMP > SNMP Agent Settings".

Interface Description

SNMP agent settings interface as follows:

SNMP Agent Settings	
SNMP	🔵 Enable 💿 Disable
Read community string	
Write community string	
Contact name	
Location	
SNMP agent version	✓ v1 ✓ v2 ✓ v3
Read only user name	
Read only authentication mode	Disable •
Read only password	
Read only privacy mode	Disable •
Read only privacy	
Read/write user name	
Read/write authentication mode	Disable •
Read/write password	
Read/write privacy mode	Disable •
Read/write privacy	
Submit Refresh	

Main elements configuration description of SNMP agent settings interface:

Interface Element	Description
SNMP	The radio box of enable/disable SNMP function, the
	options are as follows:
	Enable
	Disable
Read Community	The text box of readable community name, supporting
String	0-32bit character string input. The readable community
	name is used for authentication of Get operation between
	Agent and NMS.
Write Community	The text box of writable community name, supporting
String	0-32bit character string input. The writable community
	name is used to complete Set operation authentication
	between Agent and NMS.
Contact Name	The text box of SNMP contact information, supporting
	0-32bit character string input.
Location	The text box of position information, supporting 0-32bit

<u>3onedata</u>

Interface Element	Description
	character string input.
SNMP Agent Version	The check box of the SNMP agent version, which supports
	optional v1, v2 and v3 versions. Compared with v1/v2,
	version v3 mainly adds authentication and encryption.
Read-only User	The text box of read-only user name, supporting 0-32bit
Name	character string input.
Read-only	The drop-down list of read-only user authentication mode,
Authentication Mode	the options are as follows:
	• Disable
	MD5: message digest algorithm 5;
	SHA: Secure Hash Standard.
Read-only Password	The text box of read-only user authentication key,
	supporting 0-32bit character string input.
Read-only Privacy	The drop-down list of read-only user data encryption mode,
Mode	the options are as follows:
	Disable
	• DES_CBC: The system encrypts the data by using the
Deed only Driveov	cipner group link code of the data encryption standard.
Read-only Phyacy	Read-only user data encryption key text box, supporting
	U-32bit character string input.
Read/write User	The text box of read/write user name, supporting 0-32bit
Name	character string input.
Read/Write	The drop-down list of read/write user authentication mode,
Authentication Mode	the options are as follows:
	Disable MDE (massage direct algorithm 5);
	 MD5 (message digest algorithm 5), SHA: Secure Hash Standard
Read/Write Password	The text box of read/write user authentication key
	supporting 0-32bit character string input.
Read/Write Privacy	The drop-down list of read/write user data encryption
Mode	mode, the options are as follows:
	Disable
	• DES_CBC: The system encrypts the data by using the
	cipher group link code of the data encryption standard.
Read/Write Privacy	The text box of read/write user data encryption key,
	supporting 0-32bit character string input.



9.1 E-Mail Alert Configuration

Function Description

On the "E-Mail Alert configuration" page, user can configure the sender, recipient, mailbox server and other parameters. The system can inform the change information of power connection, warm start, cold start, LAN port connection, serial DCD and DSR signals of the device by mail.

Operation Path

Open in order: "Alarm Configuration > E-Mail Alert Settings".

Interface Description

Mail Alarm Settings configuration interface is as follows:

E-mail Alert	
Mail server (SMTP)	
Port numbers	
Auth type	Plaintext •
My server requires authentication	
User name	
Password	
From e-mail address	
To e-mail address 1	
To e-mail address 2	
To e-mail address 3	
To e-mail address 4	
Submit Refresh	

5	
Interface Element	Description
Mail Server (SMTP)	Mailbox server address using SMTP simple mail transfer
	protocol provided by mailbox service provider, and mailbox
	server address used by sender when sending mail.
Port number	Port number of mailbox server.
Auth type	The drop-down list of authentication method, the options are
	as follows:
	Plaintext;
	SSL: encryption protocol of Secure Sockets Layer;
	• TLS: encryption protocol of Transport Layer Security.
My server requires	The check box of mailbox server authentication. Check the
authentication	configuration according to the authentication requirements
	of mailbox server.
User name	The user name of the sender's mailbox server.
Password	Login password or authorization code of sender's mailbox
	server.
From E-mail	The email address from which the sender sends a warning
address	message.
To e-mail address 1	The input text box of Address 1, which is used to fill in the
	email address of receiving alarm mails.
To e-mail address 2	The input text box of Address 2, which is used to fill in the
	email address of receiving alarm mails.
To e-mail address 3	The input text box of Address 3, which is used to fill in the
	email address of receiving alarm mails.
To e-mail address 4	The input text box of Address 4, which is used to fill in the
	email address of receiving alarm mails.

Main element configuration instructions in Disable Mode interface

9.2 SNMP Trap Alarm Configuration

Function Description

In the SNMP Trap Alarm page, you can configure the IP address or domain name of the server that receives SNMP Trap information.

Operation Path

Open in order: "Advanced Config > SNMP Trap Alarm Configuration".

Interface Description

The SNMP Trap Alarm Configuration interface as follows:

SNMP Trap	
SNMP trap server IP or domain name	
Trap version	● v1 ○ v2c
Trap community	
Submit Refresh	

The main elements configuration description of SNMP Trap alarm interface:

Interface Element	Description
SNMP Trap server IP	The text box of IP address or domain name of SNMP Trap
or domain name	server. The server is used to receive SNMP Trap
	information sent by devices.
Trap version	The radio box of SNMP Trap version, which supports
	optional v1 and v2c versions.
Trap community	The text box of SNMP Trap community name, which
	specifies SNMP community name.

9.3 IO Trap Settings

Function Description

On the "IO Trap Settings" page, IO Trap alarms can be configured.

Operation Path

Open in order: "Alarm Settings > IO Trap Settings".

Interface Description

The IO Trap settings interface as follows:

IO Trap Setting				
Channel	Mode		Specific ID(1.20)	Triggor
Channel	wode		Specific ID(1-20)	rngger
DI-00	DI		1	On Change
DI-01	DI		1	On Change
DI-02	DI		1	On Change
DI-03	DI		1	On Change
DI-04	DI		1	On Change
DI-05	DI		1	On Change
DI-06	DI		1	On Change
DI-07	DI		1	On Change
DO-00	DO		1	On Change
DO-01	DO		1	On Change
DO-02	DO		1	On Change
DO-03	DO		1	On Change
DO-04	DO		1	On Change
DO-05	DO		1	On Change
DO-06	DO		1	On Change
DO-07	DO		1	On Change
Submit Refresh				

The main element configuration description of IO Trap Settings interface:

Interface Element	Description		
Channel	The name of DI and DO channels.		
Mode	The working modes of DI and do channels are shown as		
	follows:		
	• DI		
	Counter		
	• DO		
	Pulse Output		
SNMP Trap	The enable Trap check box. After checking it, when the DI or		
	DO status changes, the device sends Trap information to the		
	SNMP server through SNMP.		
	Note:		
	The Counter and Pulse Output modes do not support Irap alarms.		
Special ID (1-20)	Trap special ID, the value range is 1-20, and different ID event		
	types can be customized.		
Trigger	Trap trigger mode, as shown below:		
	• On Change: when the channel status changes, the Trap		
	message will be triggered.		
	: no trigger mode.		

9.4 System Alert Settings

Function Description

In the "System Alert Settings" page, the alarm type of system events can be configured.

Operation Path

Open in order: "Alarm Configuration >System Alarm Settings".

Interface Description

System Alert Settings interface is as follows:

Event Settings	
System event	
Event	System event alarm
Cold start	🗌 trap 🔲 mail 🔲 syslog
Warm start	🗌 trap 🔲 mail 🔲 syslog
Ethernet 1 link down	🗌 trap 🔲 mail 🔲 syslog
Ethernet 2 link down	🗌 trap 🔲 mail 🔲 syslog
Console(web/text) login auth fail	🗌 trap 🔲 mail 🔲 syslog
IP changed	🗌 mail 🔲 syslog
Password changed	🗌 mail 🔲 syslog
Time synchronization	syslog
Ntp connection failure	syslog
E-mail sending failure	syslog
Firmware upgrade	syslog
Configuration changed	syslog
Configuration import	syslog
Configuration export	syslog
Submit Refresh	

Main elements configuration description of system alarm interface:

Interface Element	Description	
System Event	System event alert configuration bar	
Event	System event alert types, shown as follows:	
	• Cold start: device will send alarm after it is powered of	
	and restarted.	

Interface Element	Description
	 Warm start: In the case of uninterrupted power supply, the device will send alarm after restarting the device via the Web or CLI configuration. Network card1: device will send alarm when lan1 loses connection. Network card2: device will send alarm when lan2 loses connection. Login Failed: device will send alarm when web login password authentication fails. Modify Static IP: device will send alarm when "Network Configuration" is modified. Modify Password: device will send alarm when "User Configuration" is modified. Timing: device will send alarm when "Time Setting" is modified. NTP Connection Failed: device will send alarm when much modified. NTP Connection Failed: device will send alarm when mail sending fails due to network or other problems. Firmware Upgrade: device will send alarm when the firmware is upgraded. Modify Configuration: device will send alarm when part of webpage configuration: device will send alarm when
System Event	System alert mode check box, the options are as follows:
Alarm	 Trap: after checked, device will send SNMP Trap message for alarm according to "SNMP Trap Alarm Configuration" information when the corresponding system event sends an alarm. Mail: after checked, device will send mail for alarm according to "Mail Alarm Configuration" information when the corresponding system event sends an alarm. Sys log: after checked, device will record alarm message in "System Log" information when the corresponding system event sends an alarm; device will send log message for alarm to remote syslog if it is enabled.



10.1 Routing Table

Function Description

In "Routing" page, you can see the current route information.

Operation Path

Open in order: "System Status > Routing".

Interface Description

Route Table Interface Screenshot:

Routing						
Current Ro	outing					
Auto refres	sh 🕑					
lface	Destination	Gateway/HA	Netmask	Metric	Flag	Use
eth0.1	192.168.1.0	0.0.0.0	255.255.255.0	0	U	0
eth0.2	192.168.8.0	0.0.0.0	255.255.255.0	0	U	0

The main elements configuration description of routing interface:

Interface Element	Description	
Iface	Display the interface name of physical network.	
Destination	Display the IP address of destination host or the network	
	address of destination routing.	
Gateway	Display gateway IP address or next hop router IP address of.	
Netmask	Display destination network subnet mask.	
Metric	Display the router hops from source terminal to destination	
	terminal.	
Flags	Display routing status, valid status is:	
	• U: UP	

Interface Element	Description	
	D: DOWN	
	G: Route to gateway	
	H: Route to host computer	
	T: Routing settings	
	R: RIP is dynamic	
Use	The quantity of data packet which is sent correctly via the	
	router.	

10.2 System Network Status

Function Description

On the page of "System Network Status", user can check TCP connection information of the device.

Operation Path

Open in order: "System Status > System Network Status".

Interface Description

The system network status interface is as follows:

Network Connections					
Auto refresh					
Protocol	Recv-Q	Send-Q	Local Address	Foreign Address	State
TCP	0	0	127.0.0.1:6666	0.0.0.0:*	LISTEN
TCP	0	0	0.0.0.80	0.0.0.0:*	LISTEN
TCP	0	0	127.0.0.1:5555	0.0.0.0:*	LISTEN
TCP	0	0	0.0.0.0:502	0.0.0.0:*	LISTEN
TCP	0	0	0.0.0.22	0.0.0.0:*	LISTEN
TCP	0	0	0.0.0.23	0.0.0.0:*	LISTEN
TCP	0	0	0.0.0.0:443	0.0.0.0:*	LISTEN
TCP	0	0	192.168.1.254:443	192.168.1.161:13987	ESTABLISHED
TCP	0	0	127.0.0.1:45290	127.0.0.1:6666	ESTABLISHED
TCP	0	0	127.0.0.1:6666	127.0.0.1:45290	ESTABLISHED
TCP	0	0	192.168.1.254:443	192.168.1.161:13989	ESTABLISHED
TCP	0	0	127.0.0.1:57636	127.0.0.1:5555	ESTABLISHED
TCP	0	0	192.168.1.254:443	192.168.1.161:13988	ESTABLISHED
TCP	0	0	127.0.0.1:5555	127.0.0.1:57636	ESTABLISHED
TCP	0	0	192.168.1.254:443	192.168.1.161:13991	ESTABLISHED

The main element configuration description of system network status interface:

Interface Element	Description
Protocol	Network protocol type.
Receiv-Q	Number of network receiving queues.
Send-Q	Number of network sending queues.

Interface Element	Description	
Local IP address	Device IP address and network port number.	
Foreign Address	IP address and network port number of remote host.	
State	The status of the network socket is as follows:	
	LISTEN: listening state.	
	• ESTABLISHEN: the connection has been established.	

10.3 System Log

Function Description

On the "System log" page, you can view the log information of the device and upload the log information to the syslog server. During the operation of the device, the system will record all kinds of situations in operation, thus forming log information. The log information is mainly used to check the running status of device, analyze the status of network and locate the causes of problems, and provide basis for system diagnosis and maintenance. The generated log information can be saved on the device, and the log information can be output to the log server by using syslog protocol.

Operation Path

Open in order: "System Management > System Log".

Interface Description

System log interface as follows:

<u>3onedata</u>

System Log	
Model	O Enable Disable
Message type	● UDP ○ TCP
lp	192.168.1.2
Port	514
Syslog severity	LOG_EMERG
Submit	Refresh Download log
Log information	
Log information Dec 31 16:00:03 IC 2016.11.1-svn29)) Dec 31 16:00:03 IC Dec 31 16	Derver kernel: Booting Linux on physical CPU 0x0 Derver kernel: Linux version 4.4.179 (dnsoft1@dnsoft1) (gcc version 4.8.5 (Buildroot #1 PREEMPT Wed May 26 08:44:48 UTC 2021 Derver kernel: CPU: ARM926EJ-S [41069265] revision 5 (ARMv5TEJ), cr=0005317f Derver kernel: CPU: VIVT data cache, VIVT instruction cache Derver kernel: Machine: NUC980 Derver kernel: Memory policy: Data cache writeback Derver kernel: Built 1 zonelists in Zone order, mobility grouping on. Total pages: 32512 Derver kernel: Kernel command line: console=ttyS0,115200n8 Derver kernel: PID hash table entries: 512 (order: -1, 2048 bytes) Derver kernel: Dentry cache hash table entries: 16384 (order: 4, 65536 bytes) Derver kernel: Indde-cache hash table entries: 8192 (order: 3, 32768 bytes) Derver kernel: Indde-cache hash table entries: 8192 (order: 3, 32768 bytes) Derver kernel: Wemory: 110120K/131072K available (3874K kernel code, 273K rwdata, 72K init, 213K bss, 20952K reserved, 0K cma-reserved) Derver kernel: Virtual kernel memory layout: Derver kernel: fixmap : 0xffc00000 - 0xfff00000 (3072 kB) Derver kernel: fixmap : 0xffc00000 - 0xc8000000 (128 MB) Derver kernel: modules : 0xbf000000 - 0xc0000000 (128 MB) Derver kernel: init : 0xc0008000 - 0xc0000000 (16 MB) Derver kernel: init : 0xc0008000 - 0xc1318520 (274 kB) Derver kernel: .init : 0xc04fd000 - 0xc1318520 (274 kB) Derver kernel: .init : 0xc12d4000 - 0xc1318520 (274 kB) Derver kernel: .init : 0xc12d4000 - 0xc1318520 (274 kB) Derver kernel: .init : 0xc212d4000 - 0xc1318520 (274 kB) Derver kernel: .init : 0xc212d4000 - 0xc1318520 (274 kB) Derver kernel: .init : 0xc212d4000 - 0xc1318520 (274 kB) Derver kernel: .init : 0xc212d4000 - 0xc1318520 (274 kB) Derver kernel: .init : 0xc212d4000 - 0xc1318520 (274 kB) Derver kernel: .init : 0xc212d4000 - 0xc1318520 (274 kB) Derver kernel: .init : 0xc212d4000 - 0xc1318520 (274 kB) Derver kernel: .init : 0xc212d4000 - 0xc1318520 (274 kB) Derver kernel: .init : 0xc212d4000 - 0xc1318520 (274 kB) Derver kernel: .
Dec 31 16:00:03 IC Dec 31 16:00:03 IC	Dserver kernel: SLUB: HWalign=32, Order=0-3, MinObjects=0, CPUs=1, Nodes=1 Dserver kernel: Preemotible hierarchical RCU implementation
Dec 31 16:00:03 IC Dec 31 16:00:03 IC Dec 31 16:00:03 IC	Dserver kernel: Build-time adjustment of leaf fanout to 32. Dserver kernel: NR_IRQS:545 Dserver kernel: clocksource: nuc980-timer5: mask: 0xffffff max_cycles: 0xffffff.
max_idle_ns: 6221 Dec 31 16:00:03 IC 69905062489ns	5505635 ns Oserver kernel: sched_clock: 24 bits at 120kHz, resolution 8333ns, wraps every

Interface Element	Description
Model	System log server configuration type, which can be checked
	as follows:
	• Enable: when enabled, the system log will be saved to
	the remote system log server.
	Disable: Disable the syslog server function.
Message Type	System log information transmission protocol, which can be
	selected as follows:
	• TCP: system log information is sent to the log server by
	TCP protocol. TCP (transmission control protocol),
	connection-oriented and reliable transmission-layer
	communication protocol;

The main elements configuration description of system log interface:

Interface Element	Description				
	 UDP: the system log information is sent to the log server by UDP protocol. UDP (user datagram protocol), connectionless-oriented transmission-layer communication protocol. 				
IP	IP address of the syslog server.				
Port	The port number of syslog server, and the default port of syslog protocol is 514.				
Syslog Severity	 The level of system log can be selected as follows: LOG_EMERG: extremely urgent error; LOG_ALERT: an error that needs to be corrected immediately; LOG_CRIT: a more serious error; LOG_ERR: An error occurred; LOG_WARNING: warning, there may be some error; LOG_NOTICE: information to be noticed; LOG_INFO: general prompt information; LOG_DEBUG: debug information. 				

Configuration Instance

"Visual Sys log Server" is a free open source software for receiving and viewing syslog messages. At present, the host with "Visual Sys log Server" installed is used as the system log server, and the IP address of the host is 192.168.1.101. The device transmits log information to the host server through TCP protocol. The configuration steps are as follows:

- **Step 1** Log in to the device WEB interface.
- **Step 2** On the "System log" page, configure relevant parameters, as shown in the following figure:

System Log	
Model	Enable Disable
Message type	UDP • TCP
lp	192.168.1.101
Port	514
Syslog severity	LOG_EMERG V
Submit	Refresh Download log

1 Check "Enable" in the "Model" checkbox;

- 2 Check "TCP" protocol in "Message Type" checkbox;
- 3 In the IP text box, enter the IP address "192.168.1.101" of the server.
- 4 In the "Port" text box, enter the port number of the server, and the default port of syslog protocol is 514;
- 5 In the "Log Level" drop-down list, select "LOG_INFO";
- 6 Click "Apply" button.
- **Step 3** Run "Visual Sys log Server" on the host to complete the configuration of relevant parameters, as shown below.

🔤 Visual Sysl	log Server 1	1.6.3								_		×
Setup	A Font F	Processing High	nlighting	Goto nev	More	View prev	View next	View file	d Clear	? About	Terminate	:
View	w file syslo	3			\sim							
Message filte	ering 📕	All messag	ges match									
Displaying 0 mes	ssages											
Time	IP	Host	Facility	Priority	Tag	Message						
UDP 192.168.1.	.101:514	TCP 1	192.168.1.1	01:514 [1]								

1 Click the "Setup" button, as shown in the above figure;

Setup			×
Main Files E-mail			
UDP syslog server			
Enable UDP listener			
UDP listener interface and port	0.0.0.0 ~	514	
TCP syslog server			
Enable TCP listener			
TCP listener interface and port	192.168.1.101 ~	514	
Automatic start with windows Highlighting			
Working	file "raw" for diagnostic purposes IF8		
✓ ○	К	Cancel	

- 2 On the "Setup" page, in the Main configuration area, check "Enable TCP Listener", as shown in the above figure;
- 3 Select the IP address "192.168.1.101" and port number "514" of the server from the "TCP listener interface and port" drop-down list;
- 4 Click "OK" button.
- **Step 4** Check the log information in the "Visual Sys log Server" configuration interface, as shown in the following figure.

Visual Syslog S	erver 1.6.3									-	×
Setup Font	Processing	J Highlighting	Goto new	More	View prev View I	next View file	of Clear	? About	Terminate		
Display											
View file		messages match		~							
Dicolaving 4 message	· · · ·	measuges mater									
Time	IP	Host	Facility	Priority	Tag	Message					
Jan 104:52:47	192.168.1.253	SC10E32O	daemon	warning	fcgi[977]	[17567.333414][FU	JNC:cgi_network_	get, Line:81	19]: read : /etc/config/network.	conf	
Jan 104:53:10	192.168.1.253	SC10E32O	daemon	warning	fcgi[977]	[17590.163551][FU	JNC:cgi_network_	get, Line:81	19]: read : /etc/config/network.	conf	
Jan 104:58:57	192.168.1.253	SC10E32O	daemon	warning	fcgi[977]	[17937.130793][FU	JNC:cgi_network_	get, Line:81	19]: read : /etc/config/network.	conf	
Jan 105:01:01	192.168.1.253	SC10E32O	daemon	warning	fcgi[977]	[18061.666033][FU	JNC:cgi_network_	get, Line:81	19]: read : /etc/config/network.	conf	
UDP: server disable	d	TCP 192.168.1	.101:514 [1]								

Step 5 End.



11.1 Device Information Configuration

Function Description

In the "Device Information Configuration" page, you can configure the device name, device description, and maintenance contact information.

Operation Path

Open in order: "System Management > Device Information Settings".

Interface Description

The screenshot of device information configuration interface:

Device Information				
Device model	io server			
Device name	IO Server			
Description	io server device			
Serial no.	1234567			
Contact				
Submit	Refresh			

The main elements configuration description of device information interface:

Interface Element	Description
Device model	Device model information, the input box is grayed and cannot
	be entered by default.
Device name	Enter the device name in the "Name" text box. To identify
	each device in the network, give the device a different name.
Description	Enter the device description in the "Description" text box.

Interface Element	Description
Serial no.	Device serial information, the input box is grayed and cannot
	be entered by default.
Contact	Enter the contact information of the equipment maintenance
	personnel in the "Contact information" text box.

11.2 Time Setting

The full name of NTP protocol is Network Time Protocol. Its destination is to transmit uniform and standard time in international Internet. Specific implementation scheme is appointing several clock source websites in the network to provide user with timing service, and these websites should be able to mutually compare to improve the accuracy. It can provide millisecond time correction, and is confirmed by the encrypted way to prevent malicious protocol attacks.

Function Description

On the "Time Settings" page, user can configure the device time and NTP server information.

Operation Path

Open in order: "System manage > Time setting".

Interface Description

Time setting interface as follows:

Time Setting	
Time zone	(GMT+08:00)Beijing, Chongqing, Hong Kong, Urumqi ▼
Local time	2005 / 01 / 01 00 : 19 : 14 Changed
Time server	ntp.aliyun.com
Submit	Refresh

The main elements configuration description of time settings interface:

Interface Element	Description
Time Zone	Time standard of different global regions.
local Time	The device's own time. Click the "Change" button to manually
	modify the device time or synchronize it to the current
	computer time.
Time Server	IP address or domain name of NTP server. The device will

Interface Element	Description
	automatically synchronize NTP server time.

11.3 Remote Management

HTTPS (full name: Hypertext Transfer Protocol over Secure Socket Layer) is an HTTP channel targeted for security, which in short is a Secure version of HTTP. HTTPS provides data encryption services to prevent the attacker to intercept the transmitted message between the Web browser and web server, obtain some sensitive information, such as credit card numbers, passwords, etc.

The full English name of SSH is Secure Shell. SSH is a security protocol based on application layer and transmission layer. Telnet is transmitted in plaintext, while SSH is transmitted in ciphertext, which is more secure. SSH is a reliable protocol which provides security for remote login sessions and other network services. Using SSH protocol can effectively prevent information leakage in the process of remote management, and can also prevent DNS and IP spoofing. In addition, the transmitted data is compressed so that the transmission speed can be increased.

Function Description

On the "Remote Administration" page, access methods such as TELNET, HTTP, HTTPS and SSHD can be restricted.

Operation Path

Open in order: "System Management > Remote Management".

Interface Description

The Remote management interface is as follows:

Remote Administration					
Telnet service	Enable Disable				
HTTP	Enable Disable				
HTTPS	Enable Disable				
SSHD service	Enable Disable				
Submit	Refresh				

The main elements configuration description of Remote management interface:

Interface Element	Description		
TELNET Service	TELNET service function status, the options are as follows:		
	Enable;		

Interface Element	Description
	• Disable. Note: When enabled, the TELNET client can access the CLI interface of the device.
HTTP	Device HTTP protocol function status, options are as follows:
	Enable;Disable.
	Note: When enabled, when using HTTP to access the WEB interface, the format is HTTP://192.168.1.254, and the address is the IP address of the corresponding device.
HTTPS	Device HTTPS protocol function status, options are as
	follows:
	• Enable;
	• Disable.
	Note: When enabled, when using HTTPS to access the WEB interface, the format is HTTPS://192.168.1.254, and the address is the IP address of the corresponding device.
SSHD service	SSH service function status, the options are as follows:
	• Enable;
	• Disable.
	Note: When enabled, the SSH client can access the CLI interface of the device

11.4 User Configuration

Function Description

In the "user configuration" page, users can add and delete users freely. Users need to access the device by login with user name and password. The initial user name and password are both: admin.

Operation Path

Open in order: "System Management > User Configuration".

Interface Description

User configuration interface as follows:

<u>3onedata</u>

User Management				
Add	Delete Refresh			
	Name	User rights	Operate	
	admin	Administrator	Edit	

The main elements configuration description of user configuration interface:

Interface Element	Description			
Name	Identification of the visitor. Note: User names and passwords can support up to 32 characters.			
User Rights	 The user's access rights are shown as follows: Administrator: has administrator authority and can configure parameters of device; General user: has viewing authority, and can view device configuration parameters and network diagnosis operations. 			
Operate	Click Edit to modify the password and user rights of the current user.			

11.5 IP Address Filtering

Function Description

Users can limit the ongoing access or connected host IP address and subnet mask via setting access rules on the "IP Filter" page.

Operation Path

Open in order: "System Management> IP Address Filtering".

Interface Description

IP filter interface shown as follows:

IP Address Filtering					
IP Addres	ss Filtering n mode	C Enable Disable Whitelist			
Number	Status	IP address Subnet mask			
1	Disable	Y			
2	Disable	Y			
3	Disable	▼			
4	Disable	Y			
5	Disable	Y			
6	Disable	v			
7	Disable	Y			
8	Disable	v			
9	Disable	▼			
10	Disable	▼			
11	Disable	v			
12	Disable	Y			
13	Disable	v			
14	Disable	Y			
15	Disable	Y			
16	Disable	Y			
Submit Refresh					

Main element configuration instructions in IP Filtering interface

Interface Element	Description
IP Address	Enable or disable IP filtering rules.
Filtering	Enable
	Disable
Operation Mode	Set filtering rules for IP addresses.
	• White list: the IP address set in the filtering rule is allowed
	to access the device.
	• Blacklist: IP addresses set in filtering rules are prohibited
	from accessing devices.
	Notice:
	• When the white list is enabled, IP addresses outside the white
	list will not be able to access the device.
	• If the IP address in the white list cannot access the device,
	please clean the browser cache and access it again.
	• When the blacklist is enabled, the IP addresses covered by the

Interface Element	Description		
	blacklist will not be able to access the device.		
Number	Displays the IP address filtering rule number.		
Status	Enable or disable Filtering rules.		
	Enable		
	Disable		
IP Address	Set the IP address in dotted decimal format in the filter rule,		
	such as "192.168.1.61".		
Subnet Mask	Set the subnet mask in dotted decimal format in the filter rule,		
	such as "255.255.255.0".		

11.6 MAC Filtering

Function Description

On the "MAC Filter" page, user can restrict the host MAC address to access or connect by setting access rules.

Operation Path

Open in order: "System Management > MAC Address Filtering".

Interface Description

MAC filter interface shown as follows:

MAC Address Filtering					
MAC Address Filtering O Enable O Disable					
Operation mode Whitelist •					
Number	Status		MAC address		
1	Disable	Ŧ			
2	Disable	•			
3	Disable	•			
4	Disable	•			
5	Disable	•			
6	Disable	•			
7	Disable	•			
8	Disable	•			
9	Disable	•			
10	Disable	•			
11	Disable	•			
12	Disable	Ŧ			
13	Disable	•			
14	Disable	•			
15	Disable	•			
16	Disable	Ψ.			
Submit Refresh					

The main elements configuration description of MAC Filter interface:

Interface Element	Description		
MAC Address	Enables or disables MAC address filtering rules.		
Filtering	Enable		
	Disable		
Operation Mode	Set filtering rules for MAC addresses.		
	• White list: the MAC address set in the filtering rule is		
	allowed to access the device.		
	Blacklist: MAC addresses set in filtering rules are		
	prohibited from accessing devices.		
	Notice:		
	• When the white list is enabled, MAC addresses outside the		
	white list will not be able to access the device.		
	• When the blacklist is enabled, the MAC addresses covered by		
	the blacklist will not be able to access the device.		

Interface Element	Description		
Number	Display MAC address of the filtering rule		
Status	Enable or disable Filtering rules.		
	Enable		
	Disable		
MAC Address	Set the six-byte hexadecimal format MAC address in the filter		
	rule, such as "00-22-6F-03-BD-52".		

11.7 Static Routing Configuration

Function Description

In "Static Routing Configuration" page, you can configure how to connect device with external network. In the dual IP mode, the data egress interface can be specified via static routing configuration when device is communicating across network segment. Device supports up to 32 routing entries, every entry must provide gateway, destination address, subnet mask, egress interface and other information.

Operation Path

Open in order: "System Management > Static Routing Configuration".

Interface Description

The static routing configuration interface as follows:

Route Table					
No	Gateway	Destination	Netmask	Metric	Iface
1				1	lan1 ▼
2				1	lan1 ▼
3				1	lan1 ▼
4				1	lan1 ▼
5				1	lan1 ▼
6				1	lan1 ▼
7				1	lan1 ▼
8				1	lan1 ▼
9				1	lan1 ▼
10				1	lan1 ▼
11				1	lan1 ▼
12				1	lan1 ▼
13				1	lan1 ▼
14				1	lan1 ▼
15				1	lan1 ▼
16				1	lan1 ▼
17				1	lan1 ▼
18				1	lan1 ▼
19				1	lan1 ▼
20				1	lan1 ▼
21				1	lan1 ▼
22				1	lan1 ▼
23				1	lan1 ▼
24				1	lan1 ▼
25				1	lan1 ▼
26				1	lan1 ▼
27				1	lan1 ▼
28				1	lan1 ▼
29				1	lan1 ▼
30				1	lan1 ▼
31				1	lan1 ▼
32				1	lan1 ▼
Subm	it Refresh				

The main elements configuration description of static routing configuration interface:

Interface Element	Description
No	The entry number of static routing table.
Gateway	Gateway IP address or IP address of next hop router.
Destination	The IP address of destination host or the network address of
	destination routing.
Netmask	Subnet mask of destination network.
Metric	The number of routers from source terminal to destination
	terminal is hop. Device will prioritize the routing of data
	packets if more than one router is available to reach a given
	destination.
Iface	Network data egress, options are as follows:
	• lan1

Interface Element	Description
	• lan2

Configuration Instance

Configure the static routing of the device to communicate with PC A, PC B and PC C. Suppose device LAN1 connects to router1, and communicates with PC A; device LNA2 connects to router2, and communicates with PC B/PC C via router3, as the picture below.



Note:

The device picture mentioned in above figure is only an example, and the actual appearance of the device is subject to the device obtained.

The device communicates with PC A, the network parameters are as follows:

- IP address of device network port 1(LAN 1): 10.10.10.10
- Router1 IP address (LAN 1) : 10.10.10.100
- PC A IP address: 192.168.100.100

The device communicates with PC B/C, and the network parameters are as follows:

- IP address of device network port 2(LAN 2) : 20.20.20.20
- Router2 IP address (LAN 2) : 20.20.20.200
- PC B IP address 192.168.200.200
- PC C IP address 192.168.200.200

When the device communicates with PC A, it passes through a router, and the hop count is 1, so a static routing table needs to be added, as shown in item 1 in the following figure. When the device communicates with PC B or PC C, it passes through two routers with a hop count of 2, so a static routing table needs to be added, as shown in item 2 in the following figure.

<u>3onedata</u>

Route	e Table				
No	Gateway	Destination	Netmask	Metric	lface
1	10.10.10.100	192.168.100.100	255.255.255.255	1	lan1 ▼
2	20.20.20.200	192.168.200.0	255.255.255.0	2	lan2 ▼
3				1	lan1 ▼
4				1	lan1 ▼
5				1	lan1 ▼
6				1	lan1 ▼

11.8 Diagnostic Test

11.8.1 Ping

Function Description

On the "Ping" page, users can use the Ping command to check whether the network is clear or the network connection speed. Ping utilizes the uniqueness of network machine IP address to send a data packet to the target IP address, and then ask the other side to return a similarly sized packet to determine whether two network machines are connected and communicated, and confirm the time delay.

Operation Path

Open in order: "System Management > Diagnosis > Ping".

Interface Description

Ping information interface as follows:

Diagnosis	>	Ping	Traceroute	Capture
IP address				
Start				

The main elements configuration description of Ping configuration interface:

Interface Element	Description
IP Address	The IP address of the detected device, that is, the destination
	address. The device can check the network intercommunity
	to other devices via the ping command.

Ping Configuration:

Step 1 Fill in the IP address that needs ping in the IP address text box;

Step 2 Click the "Start" button to check the ping results;



Step 3 End.

11.8.2 Traceroute

Function Description

On the "Traceroute" page, users can test the network conditions between the device and the target host. Traceroute measures how long it takes by sending small packets to the destination device until they return. Each device on a path Traceroute returns three test results. Output result includes each test time (ms), device name (if exists) and the IP address.

Operation Path

Open in order: "System Management > Diagnose Test > Traceroute".

Interface Description

TRACEROUTE interface as follows:

Diagnosis >	Ping	Traceroute	Capture	
IP address				
Start				

The main element configuration description of Traceroute interfaces:

Interface Element	Description
IP Address	IP address of the destination device, fill in the IP address of
	the opposite device that needs to be detected.

TRACEROUTE Configuration Steps:

Step 1 Fill in the destination IP address in the "IP address" text box;

Step 2 Click the "Start" button to check the results, as the picture below.

Diagnosis >	Ping Traceroute	Capture
IP address 19	2.168.1.161	
Start traceroute to 192. 1 192.168.1.161 (168.1.161 (192.168.1.1 192.168.1.161) 0.433 r	161), 30 hops max, 38 byte packets ms

Step 3 End.

11.8.3 Packet Capture Diagnosis

Function Description

On the "Packet Capture Diagnosis" page, the user can obtain the data packets sent and received by the Ethernet port of the device for network debugging and data analysis.

Operation Path

Open in order: "System Management > Diagnose Test > Packet Capture Diagnosis".

Interface Description

The Packet Capture Diagnosis interface screenshot is as follows:

Diagnosis >	Ping	Traceroute	Capture
Start	Stop		

Main elements configuration description of Packet Capture Diagnosis interface:

Interface Element	Description
Start	Click the "Start" button, and the device will start capturing
	network packets.
Stop	Click the "Stop" button, the device stops capturing network
	packets, and saves the network packets captured during this
	period to the local client in ".pcap" format.
	Note:

Interface Element	Description
	Users can use Wireshark or other third-party software to open the captured packets.

11.9 System Maintenance

11.9.1 Configure File Management

Function Description

On the "Management File" page, user can download and upload configuration file.

Operation Path

Open in order: "System Management > System Maintenance > Configuration File Management".

Interface Description

Configuration file management interface is as follows:

System Management >	Configuration File	Restore	Software Upgrade
Save IP configuration)		Select file
Import Export			

The main elements configuration description of configure file management interface:

Interface Element	Description
Save IP	When checked, the device can keep the current IP address
configuration	after importing the configuration file.
Select profile	Select the path to uploadconfiguration file locally , click
	"Select File" to select required configuration file.
	Note: Uploaded configuration files need to be exported by devices of the same model.
Export	Download the configuration file of the current device in the
	format of. tar.
	Note:
	The downloaded configuration file will be saved in the format of
	it.

<u>3onedata</u>

Interface Element	Description
Import	Upload configuration file.

Note

- After finishing update, the device will automatically open a new page to "System Information", and the uploaded configuration file will be valid after the device is reset.
- After uploading the configuration file, if the static IP in the configuration file and the computer IP are not in the same network segment, the webpage cannot be opened.
- While uploading configuration file, if dynamic IP is used in the configuration file and there is no DHCP server in the network segment, relative IP portion won't be updated.
- Do not click on or configure other WEB pages of the device or restart the device when uploading configuration files or upgrading software. Otherwise, the configuration file upload or software update will fail, or the device system will crash.

11.9.2 Restore Default Settings

Function Description

On the "Restore Factory Settings" page, user can restore the device to default setting.

Operation Path

Open in order: "System management > System Maintenance > Restore".

Interface Description

Restore Factory Settings interface is as follows:

System Management	>	Configuration File	Restore	Software Upgrade
Save IP configuration)		
Restore				

The main elements configuration description of Restore Factory settings interface:

Interface Element	Description
Save IP	When checked, the device can keep the current IP address
configuration	after restoring the factory settings.
Restore	Click this button and the device will lose all existing
	configurations and reverts to factory settings.

Note

Restoring factory value settings will cause all configurations to be in the factory state, where the IP address is the static IP address "192.168.1.254", and the user name and password default to "admin".

11.9.3 Software Upgrade

Function Description

On the Software Upgrade page, you can update and upgrade the device program.

Operation Path

Open in order: "System management > System Maintenance > Software Upgrade".

Interface Description

The software update interface as follows:

System Management	>	Configuration File	Restore	Software Upgrade	
Restore)			
Save IP configuration					
Select file			Se	elect file	
Upgrade					

The main elements configuration description of software update interface:

Interface Element	Description
Restore	When checked, the device will be restored to the factory
	settings after upgrading. After unchecking, the configuration
	parameters will be kept after the device software is upgraded.
Save IP	After the software upgrade is checked to restore the factory
configuration	configuration, the IP configuration can be checked to keep the
	current IP address and other parameters will be restored to
	the factory configuration.
Select file	Select the path of the local upgrade file, and click "Select file"
	to select the required configuration file.
Upgrade	Click "Upgrade" button to start the program upgrade.
Note

- Do not click on or configure other WEB pages of the device or restart the device or power off the device when upgrading software. Otherwise, the software update will fail, or the device system will crash.
- Maintain a reliable wired connection when upgrading.
- When the online upgrade is complete, the device will restart automatically.

12 Maintenance and Service

Since the date of product delivery, our company provides 3-year product warranty. According to our company's product specification, during the warranty period, if the product exists any failure or functional operation fails, our company will repair or replace the product for users free of charge. However, the commitments above do not cover damage caused by improper usage, accident, natural disaster, incorrect operation or improper installation.

In order to ensure that consumers benefit from our company's managed switch products, consumers can get help and solutions in the following ways:

- Internet Service;
- Service Hotline;
- Product repair or replacement;

12.1 Internet Service

More useful information and tips are available via our company website. Website: http://www.3onedata.com

12.2 Service Hotline

Users using our company products can call technical support office. Our company has professional technical engineers to answer the questions and help solve the products or usage problems ASAP. Free service hotline: +86-4008804496

12.3 Product Repair or Replacement

As for the product repair, replacement or return, customers should firstly confirm with the company's technical staff, and then contact the salesmen to solve the problem. According to the company's handling procedure, customers should negotiate with our

<u>3onedata</u>

company's technical staff and salesmen to complete the product maintenance, replacement or return.

3onedata



3onedata Co., Ltd.

Headquarter Address:3/B, Zone 1, Baiwangxin High Technology Industrial Park, Song Bai
Road, Nanshan District, Shenzhen, 518108, ChinaTechnology Support:tech-support@3onedata.comService Hotline:4008804496Official Website:http://www.3onedata.com