LUNA2000B
ESS

Modbus Port Definitions

Issue	01
Date	2023-11-28

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: https://e.huawei.com

Contents

1 ESS Models

This chapter describes the energy storage system (ESS) models that use Modbus protocol and the minimum software versions required.

1.1 ESS Model Description

Table 1-1 ESS models and software versions

Model Series	Model Name	Model ID	Minimum Firmware Version
LUNA2000-200KWH series	LUNA2000-200KWH-2H0	512	FusionSolar V800R021C10
LUNA2000-200KWH series	LUNA2000-200KWH-2H1	513	LUNA2000B V300R023C00

NOTE

Different ESS models vary in the number of ESS subsystems and configuration of commercial & industrial (C&I) cabinet subsystems. Check the information in the point table before use.

2 Introduction

Modbus is a widely used protocol for device communications. This document describes the Modbus protocol used by Huawei ESSs and can be used to regulate subsequent development for third-party integration. Huawei ESSs comply with the standard Modbus protocol, and this document focuses on the information specific to Huawei ESSs. For other information about Modbus, see the standard documents about the Modbus protocol. For details about the interaction modes and examples of the standard protocol and custom part used in Huawei ESSs, see **5 Overview of the Communications Protocol**.

2.1 Terms and Abbreviations

Table 2-1 Terms and abbreviations

Term	Description
Master node	In the master-slave communication, the party that initiates the communication is called the master node.
Slave node	During master-slave communication, the party that responds to a communication request is referred to as the slave node.
Broadcast address	Fixed to **0**.
Register address	Recorded in two bytes.
U16	16-bit unsigned integer
U32	32-bit unsigned integer
U64	64-bit unsigned integer
I16	16-bit signed integer
I32	32-bit signed integer
I64	64-bit signed integer

Term	Description
STR	Character string
MLD	Multiple bytes
Bitfield16	16-bit data
Bitfield32	32-bit data
-	N/A
s	Second
EPOCHTIME	Number of seconds since 1970-01-01 00:00:00
RO	Read-only data
RW	Data that is readable and writable
WO	Write-only data

3 C&I Cabinet Subsystem

3.1 Register Definitions

Table 3-1 C&I cabinet subsystem

No.	Signal	Read/Write	Type	Unit	Gain	Address	Quantity	Scope
1	Container status 1	RO	Bitfield16	N/A	N/A	30000	1	For details about the bit definition, see alarm definitions.
2	Container status 2	RO	Bitfield16	N/A	N/A	30001	1	For details about the bit definition, see alarm definitions.
3	Container status 3	RO	Bitfield16	N/A	N/A	30002	1	For details about the bit definition, see alarm definitions.
4	Battery cabin temperature 1	RO	I16	℃	10	30014	1	
5	Battery cabin humidity 1	RO	I16	%	10	30015	1	
6	Battery cabin dew point temperature	RO	I16	℃	10	30034	1	
7	SOC	RO	U16	%	1	30035	1	[0, 100]

No.	Signal	Read/Write	Type	Unit	Gain	Address	Quantity	Scope
8	Energy charged today	RO	U32	kWh	100	30038	2	
9	Energy discharged today	RO	U32	kWh	100	30040	2	
10	Energy charged this month	RO	U32	kWh	100	30042	2	
11	Energy discharged this month	RO	U32	kWh	100	30044	2	
14	Energy charged this year	RO	I64	kWh	100	30046	4	
15	Energy discharged this year	RO	I64	kWh	100	30050	4	
16	Total auxiliary power consumption	RO	U32	kWh	100	30060	2	
17	Charge/ Discharge power	RO	I32	kW	1000	30062	2	
18	Rated capacity	RO	U32	kWh	1000	30064	2	
19	Rated power	RO	U32	kW	1000	30066	2	
20	Chargeable capacity	RO	U32	kWh	1000	30068	2	
21	Dischargeable capacity	RO	U32	kWh	1000	30070	2	
22	Total energy charged	RO	I64	kWh	100	30076	4	
23	Total energy discharged	RO	I64	kWh	100	30080	4	
24	CO concentration 1	RO	U16	ppm	1	30091	1	
25	CO concentration 2	RO	U16	ppm	1	30092	1	

No.	Signal	Read/Write	Type	Unit	Gain	Address	Quantity	Scope
26	H_2 concentration 1	RO	U16	ppm	1	30104	1	
27	Alarm 1	RO	U16	N/A	1	30118	1	For details about the bit definition, see alarm definitions.
29	Alarm 2	RO	U16	N/A	1	30119	1	For details about the bit definition, see alarm definitions.
30	Fan speed 1	RO	U16	RPM	1	30190	1	
31	Fan speed 2	RO	U16	RPM	1	30191	1	
32	DC bus voltage	RO	U16	V	10	30202	1	[0, 6553]
33	DC bus current	RO	U16	A	10	30203	1	[0, 6553]
34	Phase A voltage	RO	U32	V	100	30300	2	
35	Phase B voltage	RO	U32	V	100	30302	2	
36	Phase C voltage	RO	U32	V	100	30304	2	
37	Phase A active power	RO	I32	kW	1000	30306	2	
38	Phase B active power	RO	I32	kW	1000	30308	2	
39	Phase C active power	RO	I32	kW	1000	30310	2	
40	Active power	RO	I32	kW	1000	30312	2	
41	Reactive power	RO	I32	kVar	1000	30314	2	
42	Power factor	RO	I16	N/A	1000	30316	1	

No.	Signal	Read/Write	Type	Unit	Gain	Address	Quantity	Scope
43	Rectifier fault	RO	U16	N/A	N/A	30499	1	**0**: no **1**: yes
44	Total output voltage of rectifiers	RO	U16	V	10	30500	1	
45	Total output current of rectifiers	RO	U16	A	10	30501	1	
46	Quantity of rectifiers	RO	U16	N/A	1	30502	1	
47	Total output power of rectifiers	RO	U32	kW	1000	30503	2	

3.2 Alarm Definitions

Table 3-2 Alarm definition table

ID	Alarm Name	Alarm Cause	Severity	Register Address	Bit
3804	AC SPD Fault	AC SPD fault	Major	30000	0
3825	UPS Alarm	A UPS alarm has been generated.	Major	30000	3
3832	Fire Alarm	A fire has been detected in the battery cabin.	Major	30000	7
3826	Combustible Gas Alarm	1. The safety valve of the lithium battery is open, and combustible gas is leaked. 2. Lithium battery thermal runaway has occurred.	Major	30000	11

ID	Alarm Name	Alarm Cause	Severity	Register Address	Bit
3831	Built-in Fire Suppression Module Pressure Low	1. Check whether the pressure gauge pointer is in the green area. If yes, check whether the network cable from the fire suppression module is securely connected to the DI port on the CMU. 2. If not, replace the fire suppression module as soon as possible by referring to the maintenance manual. Otherwise, the system will automatically shut down three days later.	Major	30000	12
3800	Battery Cabin Water Alarm	Water is detected in the battery cabin.	Major	30001	0
3801	Battery Cabin Door 1 Status Alarm	Battery cabin door 1 is open.	Major	30002	1
3827	Battery Cabin Temperature High	The ambient temperature in the battery cabin is too high, which triggers system shutdown.	Major	30118	0
3828	Battery Cabin Condensation Risk	Condensation risk exists in the battery cabin.	Minor	30118	2
3829	Battery Cabin T/H Sensor Malfunction	There are too many faulty temperature and humidity sensors in the battery cabin.	Minor	30118	4
3830	Battery Cabin T/H Control Malfunction	Too many air conditioners in the battery cabin are faulty. As a result, the temperature and humidity in the battery cabin cannot be controlled properly.	Major	30118	6
3833	Rectifier Fault	The rectifier is faulty.	Major	30119	0
3833	Rectifier Fault	The rectifier is faulty.	Major	30119	1
3833	Rectifier Fault	The rectifier is faulty.	Major	30119	2
3833	Rectifier Fault	The rectifier is faulty.	Major	30119	3
3833	Rectifier Fault	The rectifier is faulty.	Major	30119	4
3833	Rectifier Fault	The rectifier is faulty.	Major	30119	5

4 ESS Subsystem

4.1 Register Definitions

Table 4-1 ESS subsystem

No.	Signal Name	Read / Write	Data Type	Unit	Gain	Register Address	Number of Registers	Scope
1	Quantity of working packs	RO	U16	N/A	1	30101	1	N/A
2	Device status	RO	U16	N/A	1	30102	1	[0,9]
3	Rack voltage	RO	I16	V	10	30103	1	N/A
4	Rack current	RO	I16	A	10	30104	1	N/A
5	SOC	RO	U16	%	1	30105	1	[0,100]
6	SOH	RO	U16	%	1	30106	1	[0,100]
7	Charge/ Discharge power	RO	I32	kW	1000	30107	2	N/A
8	SOE	RO	U16	%	1	30164	1	[0,100]
9	DOD	RO	U16	%	1	30167	1	[0,100]

No.	Signal Name	Read / Write	Data Type	Unit	Gain	Register Address	Number of Registers	Scope
10	Chargeable capacity	RO	U32	kWh	1000	30168	2	N/A
11	Dischargeable capacity	RO	U32	kWh	1000	30170	2	N/A
14	Highest pack temperature	RO	I16	℃	100	30176	1	N/A
15	Pack with highest temperature	RO	U16	N/A	1	30177	1	N/A
16	Lowest pack temperature	RO	I16	℃	100	30178	1	N/A
17	Pack with lowest temperature	RO	U16	N/A	1	30179	1	N/A
18	Lowest pack voltage	RO	U16	V	10	30180	1	N/A
19	Pack with lowest voltage	RO	U16	N/A	1	30181	1	N/A
20	Highest pack voltage	RO	U16	V	10	30182	1	N/A
21	Pack with highest voltage	RO	U16	N/A	1	30183	1	N/A
22	Energy charged today	RO	U32	kWh	100	30192	2	N/A
23	Energy charged this month	RO	U32	kWh	100	30194	2	N/A
24	Energy charged this year	RO	U32	kWh	100	30196	2	N/A
25	Energy discharged today	RO	U32	kWh	100	30202	2	N/A
26	Energy discharged this month	RO	U32	kWh	100	30204	2	N/A
27	Energy discharged this year	RO	U32	kWh	100	30206	2	N/A

No.	Signal Name	Read / Write	Data Type	Unit	Gain	Register Address	Number of Registers	Scope
29	DCDC - Battery-side voltage	RO	I16	V	10	31561	1	N/A
30	DCDC - Bus-side voltage	RO	I16	V	10	31562	1	N/A
31	DCDC - Battery-side current	RO	I16	A	10	31563	1	N/A
32	DCDC - Bus-side current	RO	I16	A	10	31564	1	N/A
33	DCDC - Cabinet temperature	RO	I16	℃	10	31565	1	N/A
34	DCDC - ISO insulation resistance	RO	U16	MΩ	1000	31571	1	N/A

No.	Signal Name	Read / Write	Data Type	Unit	Gain	Register Address	Number of Registers	Scope
35	DCDC - Running status	RO	U16	N/A	1	31614	1	0x0000: Standby; 0x0001: Standby: safe mode; 0x0002: Standby: cable connection detection; 0x0100: Soft start; 0x0200: Running; 0x0201: Operating: limited power; 0x0202: Operating: self-derating;

No.	Signal Name	Read / Write	Data Type	Unit	Gain	Register Address	Number of Registers	Scope
								0x0203: running (current limiting); 0x0300: Unexpected shutdown; 0x0301: Commanded shutdown; 0x0302: Emergency power off; 0x0303: Charge/Discharge disabled; 0x0304: Battery pack rapid shutdown;

No.	Signal Name	Read / Write	Data Type	Unit	Gain	Register Address	Number of Registers	Scope
								0xB000: off-line; 0xC000: Loading
36	Teleindication alarm 1	RO	U16	N/A	1	39014	1	For details about the bit definition, see alarm definitions.
37	Teleindication alarm 2	RO	U16	N/A	1	39015	1	For details about the bit definition, see alarm definitions.

No.	Signal Name	Read / Write	Data Type	Unit	Gain	Register Address	Number of Registers	Scope
38	Teleindication alarm 3	RO	U16	N/A	1	39016	1	For details about the bit definition, see alarm definitions.
39	Teleindication alarm 4	RO	U16	N/A	1	39017	1	For details about the bit definition, see alarm definitions.

4.2 Alarm Definitions

Table 4-2 Alarm definition table

ID	Alarm Name	Alarm Cause	Severity	Register Address	Bit
3013	Controller-Pack Communication Error	The rack controller fails to communicate with the battery pack.	Major	39014	13
3014	Rack Controller Abnormal	A major fault has occurred on the internal circuit of the rack controller.	Major	39014	14

ID	Alarm Name	Alarm Cause	Severity	Register Address	Bit
3015	Controller Battery Side Overvoltage	The battery side voltage exceeds the maximum operating voltage of the power module.	Major	39014	15
3016	Controller Battery Side Undervoltage	The battery is not securely connected or is abnormal.	Major	39015	0
3017	Controller Battery Side Short-Circuit	The battery cable is incorrectly connected.	Major	39015	1
3018	Controller Battery Side Reverse Polarity	The battery cable is reversely connected.	Major	39015	2
3019	Controller Bus Side Overvoltage	The bus cable is not correctly connected, or the bus voltage exceeds the maximum operating voltage of the power module.	Major	39015	3
3020	Controller Bus Side Reverse Polarity	The bus is connected in reverse polarity.	Major	39015	4
3021	Controller Insulation Resistance Abnormal	1. The battery is short-circuited to the ground. 2. The battery is in a humid environment and the insulation between the circuit and ground is poor.	Major	39015	5
3022	Controller Temperature High	1. The installation position of the battery power control module is not well ventilated. 2. The ambient temperature is too high. 3. The battery power control module is abnormal. 4. The fan in the battery power control module is abnormal.	Minor	39015	6
3023	Controller Battery Terminal Temperature High	The battery terminal is not securely connected.	Major	39015	7
3024	Controller Bus Terminal Temperature High	The bus terminal is not securely connected.	Major	39015	8

ID	Alarm Name	Alarm Cause	Severity	Register Address	Bit
3025	Controller Version Mismatch	The upgrade fails.	Minor	39015	9
3026	Controller Internal Fan Faulty	The internal fan is short-circuited, the power supply is insufficient, or the fan is damaged.	Warning	39015	10
3027	Pack Monitoring Board Error	A major fault has occurred on the internal circuit of the battery pack monitoring device.	Major	39015	11
3028	Pack Internal Error	A major fault occurred on the battery pack.	Major	39015	12
3029	Pack Lockout	A failure recurs many times in the battery pack.	Major	39015	13
3030	Pack Fan Fault	1. The fan is short-circuited. 2. The power supply is insufficient. 3. The fan is damaged. 4. The fan is blocked.	Major	39015	14
3031	Pack Temperature Imbalance	The temperatures of cells in a battery pack are unbalanced.	Minor	39015	15
3032	Pack Overvoltage	The voltage of the battery pack or its cell is too high.	Major	39016	0
3033	Controller Power Control Unit Communication Error	The internal communication of the rack controller has failed.	Major	39016	1
3034	Controller Connection Detection Error	The battery rack and its power module are connected incorrectly.	Major	39016	2
3035	Battery Pack Positions of Rack Controller Abnormal	1. The actual quantity of the battery packs is inconsistent with the setting value. 2. The system has not identified the address of the battery pack. 3. The address of the battery pack is not identified after changing. 4. The connection of the battery pack is incorrect.	Major	39016	3

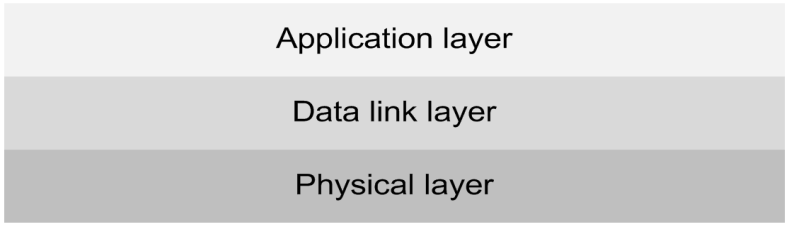
ID	Alarm Name	Alarm Cause	Severity	Register Address	Bit
3036	Optimizer Error	A major fault has occurred in the circuit inside the optimization unit of the battery pack.	Major	39016	4
3037	Optimizer Temperature High	1. The installation position of the battery pack is not well ventilated. 2. The ambient temperature is too high. 3. The battery power control module is abnormal. 4. The optimization unit is abnormal.	Minor	39016	5
3038	Optimizer Terminal Temperature High	The terminal is not securely connected.	Major	39016	6
3039	Optimizer Version Mismatch	The upgrade fails.	Minor	39016	7
3040	Incorrect Controller Bus Connection	The output buses are not connected in parallel in the 1C scenario.	Major	39016	8
3041	Loose Connection on Copper Bar	The copper bar of the battery pack is loosely connected.	Major	39016	9
3042	Controller Rapid Shutdown Connection Detection Error	The rapid shutdown cabling between battery racks is incorrect.	Major	39016	10
3043	Pack SOH Low	The SOH of the battery pack is low.	Warning	39016	11
3044	Pack Overcurrent	The battery pack current exceeds the maximum operating current for long.	Major	39016	12
3045	Pack Temperature High	1. The installation position of the battery pack is not well ventilated. 2. The air conditioner/fan is not running properly.	Major	39016	13
3046	Pack Temperature Low	The ambient temperature is too low that it activates the charge/discharge protection.	Major	39016	14

ID	Alarm Name	Alarm Cause	Severity	Register Address	Bit
3047	Pack Undervoltage	1. The voltage of the battery pack or its cell is too low. 2. Battery pack stores the energy for long when off-grid. 3. Battery pack does not work for long after getting on-grid.	Major	39016	15
3048	Pack Aux. Power Supply Faulty	The relay control of the black start auxiliary power supply is faulty.	Warning	39017	0
3052	DC Aux. Power Supply of Controller Faulty	1. The DC circuit breaker is OFF. 2. The PSU is faulty.	Major	39017	4
3053	External Fan of Rack Controller Faulty	The external fan is short-circuited or damaged, the power supply is insufficient, or the air channel is blocked.	Warning	39017	5
3054	Rack Controller Temperature Abnormal	The NTC is short-circuited or open-circuited.	Warning	39017	6
3055	Optimizer Temperature Low	The ambient temperature is too low.	Major	39017	7
3056	Emergency Power-Off	The EPO button is pressed down.	Major	39017	8
3057	Controller-Pack Version Inconsistency	1. The versions of the rack controller and battery packs are inconsistent. 2. The upgrade fails. 3. The battery packs have been replaced.	Warning	39017	9
3058	Controller-Pack Version Mismatch	1. The versions of the rack controller and battery packs are inconsistent. 2. The upgrade fails. 3. The battery packs have been replaced.	Major	39017	10
3059	Communication Error Between Controller and PCS	1. The communications cable between the CMU and SmartLogger is abnormal. 2. The communications cable between the PCS and SmartLogger is abnormal.	Major	39017	11

5 Overview of the Communications Protocol

The Modbus communications protocol consists of the following layers.

Figure 5-1 Modbus protocol layers



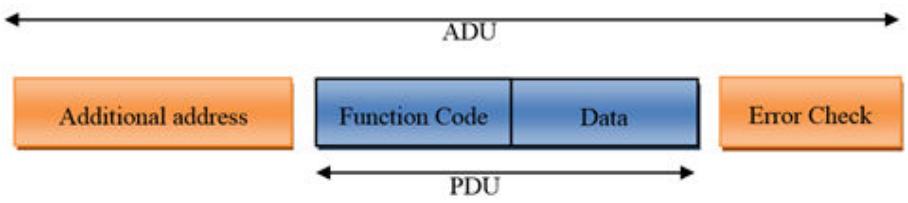
5.1 Physical Layer

Huawei ESS containers provide Modbus communication based on FE physical media. The communication is based on the TCP link and complies with the Modbus-TCP format.

5.2 Data Link Layer

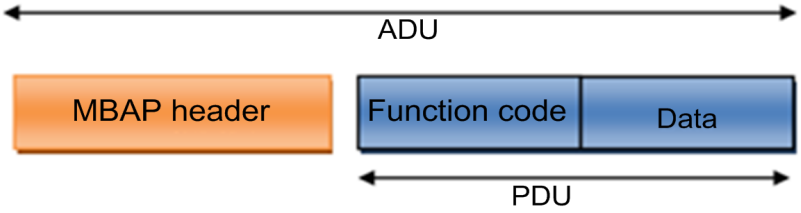
The following figure shows the generic frame structure of the Modbus protocol.

Figure 5-2 Modbus generic frame format



5.2.1 Modbus-TCP

Figure 5-3 Modbus-TCP frame format



5.2.1.1 ADU Length

The recommended frame length is 260 bytes based on the standard. When some extended functions are applied, the data service provider may extend the ADU to a proper length based on available resources to improve network transmission efficiency. The ADU length is indicated by the length field in the MBAP header.

5.2.1.2 MBAP Header

When Modbus runs on top of TCP/IP, a dedicated MBAP header (Modbus application protocol header) is used to identify the Modbus ADU. The Modbus header consists of four fields and seven bytes, which are defined as follows.

Table 5-1 MBAP definition

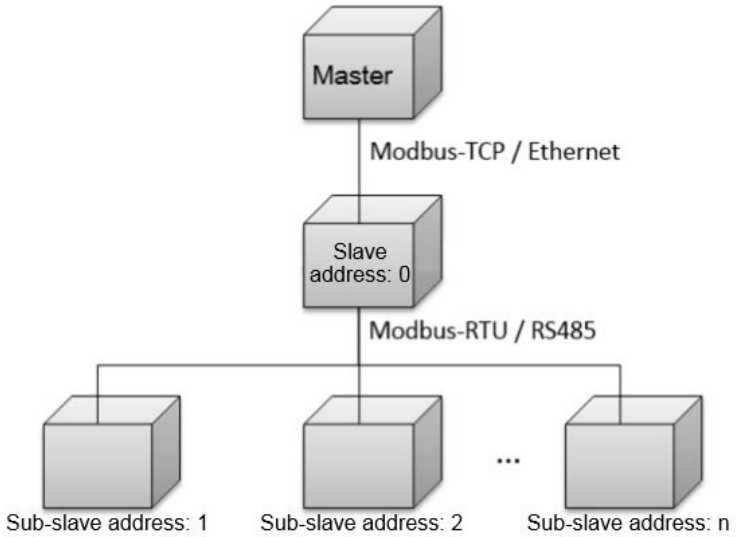
Data Field	Length (Byte)	Description	Client	Server
Transmission identifier	2	Matching identifier between a request frame and a response frame	Assigned by the client. It is recommended that each frame be assigned a unique identifier.	The identifier of the response frame from the server must be the same as that of the corresponding request frame.
Protocol	2	0 = Modbus protocol	Assigned by the client; 0 by default	The identifier of the response frame from the server must be the same as that of the corresponding request frame.

Data Field	Length (Byte)	Description	Client	Server
Data length	2	Follow-up data length	Assigned by the client based on the actual data frame	Assigned by the server based on the actual frame length
Logical device ID	1	0	Assigned by the client based on the actual data frame request	The identifier of the response frame from the server must be the same as that of the corresponding request frame.

5.2.1.3 Communications Address

Based on the TCP communications host, unit 0 is used by default to access the directly connected slave node, and other addresses are used to access the downstream devices of the slave node. The default address of the slave node is 0. The address is configurable.

Figure 5-4 Three-layer communications addresses



5.2.1.4 TCP Port

In a local area network or VPN environment, the master node may initiate a TCP socket connection to the slave node. The master node can use port 502 to request data services from the slave node.

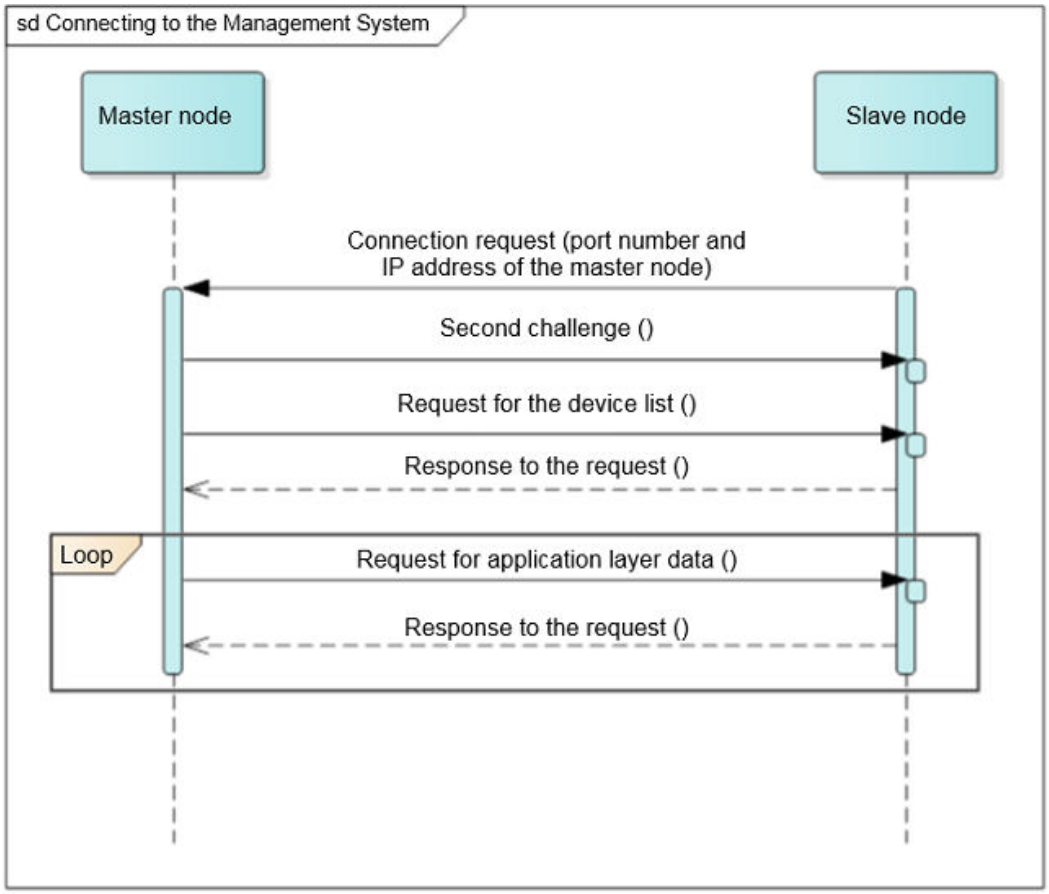
In a non-VPN environment across the public network, the device deployed on the internal network needs to initiate TCP socket link establishment to the master node exposed on the public network. In this case, you need to specify the port number of the master node on the slave node. To ensure security and minimize traffic, the master node must provide at least one encrypted port and one non-encrypted port.

5.2.1.5 TCP Link Establishment Process

This section focuses on the cross-public network application.

The following figure shows the process of connecting a slave node.

Figure 5-5 Process of establishing a secure TCP connection



5.3 Application Layer

5.3.1 Function Code

Table 5-2 Function code

Function Code	Description	Remarks
0x03	Reads registers.	Supports continuous reading of a single register or multiple registers.
0x06	Writes a single register.	Supports writing into a single register.
0x10	Writes multiple registers.	Supports continuous writing into multiple registers.

5.3.2 Exception Code

Exception codes must be unique for each network element (NE) type. The names and descriptions should be provided in the NE interface document. Different versions of the same NE type must be backward compatible. Exception codes in use cannot be assigned to other exceptions.

Table 5-3 Exception codes returned by an NE (0x00–0x8F used for common exception codes)

Code	Term	Description
0x01	Invalid function	The function code received in the query is not an allowable action for the server (or slave node). This may be because the function code is only applicable to newer devices, and cannot be implemented in the unit selected. It also indicates that the server (or slave node) is in the wrong state to process a request of this type, for example because it is not configured and is being asked to return register values.

Code	Term	Description
0x02	Invalid data address	The data address received in the query is not an allowable address for the server. More specifically, the combination of the starting register address and register quantity is invalid. For a controller with 100 registers, the PDU addresses the first register as 0 and the last one as 99. If the starting register address in a request is 96 and the register quantity is 4, the request can obtain the return values of registers 96, 97, 98, and 99. If the starting register address of a request is 96 and the register quantity is 5, the request fails and the exception code 0x02 "Invalid data address" is returned because the request attempts to read registers 96, 97, 98, 99, and 100, among which 100 is not a defined address.
0x03	Invalid data value	The value contained in the query data field is not an allowable value for the server (or slave node). The value indicates a fault in the structure of the remainder of a complex request, such as an incorrectly implied length. It does not mean that a data item submitted for storage in a register has a value outside the expectation of the application program since the Modbus protocol is unaware of the significance of any particular value of any particular register.
0x04	Slave node failure	An error occurs while the server attempts to perform the requested action.
0x06	Slave node busy	The server cannot accept a Modbus request PDU. The client application determines whether and when to retransmit the request.
0x80	No permission	An operation is not allowed because of a permission authentication failure or permission expiration.
0x90	Southbound access device response timeout	The response from the southbound device times out or the communication is disconnected.
0x91	Internal unit response timeout	The response from the internal unit times out or the communication is disconnected.

5.3.3 Read Registers (0x03)

5.3.3.1 Frame Format of a Master Node Request

Data Field	Length	Description
Function Code	1 byte	0x03
Starting Register Address	2 bytes	0x0000–0xFFFF
Number of Registers	2 bytes	1–125

5.3.3.2 Frame Format of a Normal Response from a Slave Node

Data Field	Length	Description
Function Code	1 byte	0x03
Byte Count	1 byte	2 x *N*
Register Value	2 x *N* bytes	N/A

NOTE

N refers to the number of registers.

5.3.3.3 Frame Format of an Abnormal Response from a Slave Node

Data Field	Length	Description
Function Code	1 byte	0x83
Exception Code	1 byte	See **5.3.2 Exception Code**.

5.3.3.4 Examples

This section takes the Modbus-TCP communications frames as an example. The differences between Modbus-RTU and Modbus-TCP lie in the additional address field and the CRC. Pay attention to the differences when using the Modbus-RTU frames. This also works for the follow-up examples.

The master node sends a query request (register address: 32306/0X7E32) to the slave node (logical device ID: 00).

Description		Frame Data
MBAP Header	Protocol identifier	00
		01
	Protocol	00

Description		Frame Data
		00
	Data length	00
		06
	Logical device ID	00
Function Code		03
Data	Register address	7E
		32
	Number of registers	00
		02

Normal response from a slave node

Description		Frame Data
MBAP Header	Protocol identifier	00
		01
	Protocol	00
		00
	Data length	00
		07
	Logical device ID	00
Function Code		03
Data	Byte count	04
	Register data	00
		00
		00
		01

Abnormal response from a slave node

Description		Frame Data
MBAP Header	Protocol identifier	00

Description		Frame Data
		01
	Protocol	00
		00
	Data length	00
		03
	Logical device ID	00
Function Code		83
Data	Error code	03

5.3.4 Writing a Single Register (0x06)

5.3.4.1 Frame Format of a Master Node Request

Data Field	Length	Description
Function Code	1 byte	0x06
Register Address	2 bytes	0x0000–0xFFFF
Register Value	2 bytes	0x0000–0xFFFF

5.3.4.2 Frame Format of a Normal Response from a Slave Node

Data Field	Length	Description
Function Code	1 byte	0x06
Register Address	2 bytes	0x0000–0xFFFF
Register Value	2 bytes	0x0000–0xFFFF

5.3.4.3 Frame Format of an Abnormal Response from a Slave Node

Data Field	Length	Description
Function Code	1 byte	0x86
Exception Code	1 byte	See **5.3.2 Exception Code**.

5.3.4.4 Examples

A master node sends a command (register address: 40200/0X9D08) to a slave node (address: 00).

Description		Frame Data
MBAP Header	Protocol identifier	00
		01
	Protocol	00
		00
	Data length	00
		06
	Logical device ID	00
Function Code		06
Data	Register address	9D
		08
	Register data	00
		00

Normal response from a slave node

Description		Frame Data
MBAP Header	Protocol identifier	00
		01
	Protocol	00
		00
	Data length	00
		06
	Logical device ID	00
Function Code		06
Data	Register address	9D
		08
	Register data	00
		00

Abnormal response from a slave node

Description		Frame Data
MBAP Header	Protocol identifier	00
		01
	Protocol	00
		00
	Data length	00
		03
	Logical device ID	00
Function Code		86
Data	Error code	04

5.3.5 Writing Multiple Registers (0x10)

5.3.5.1 Frame Format of a Master Node Request

Data Field	Length	Description
Function Code	1 byte	0x10
Starting Register Address	2 bytes	0x0000–0xFFFF
Number of Registers	2 bytes	0x0000–0x007b
Byte Count	1 byte	2 x *N*
Register Value	2 x *N* bytes	Value

NOTE

N refers to the number of registers.

5.3.5.2 Frame Format of a Normal Response from a Slave Node

Data Field	Length	Description
Function Code	1 byte	0x10
Register Address	2 bytes	0x0000–0xFFFF

Data Field	Length	Description
Number of Registers	2 bytes	0x0000–0x007b

5.3.5.3 Frame Format of an Abnormal Response from a Slave Node

Data Field	Length	Description
Function Code	1 byte	0x90
Exception Code	1 byte	See **5.3.2 Exception Code**.

5.3.5.4 Examples

The master node sets the register address 40118/0X9CB6 to 2 and the register address 40119/0X9CB7 to 50 for the slave node (address: 00). The request frame format is as follows.

Description		Frame Data
MBAP Header	Protocol identifier	00
		01
	Protocol	00
		00
	Data length	00
		0B
	Logical device ID	00
Function Code		10
Data	Register address	9C
		B6
	Number of registers	00
		02
	Byte count	04
	Register data	00
		02
		00
		32

Normal response from a slave node

Description		Frame Data
MBAP Header	Protocol identifier	00
		01
	Protocol	00
		00
	Data length	00
		06
	Logical device ID	00
Function Code		10
Data	Register address	9C
		B6
	Number of registers	00
		02

Abnormal response from a slave node

Description		Frame Data
MBAP Header	Protocol identifier	00
		01
	Protocol	00
		00
	Data length	00
		03
	Logical device ID	00
Function Code		90
Data	Error code	04

5.3.6 Reading Device Identifiers (0x2B)

This command code allows reading identifiers and added packets that are relevant to the physical and function description of the remote devices.

Simulate the interface of the read device identifier as an address space. This address space consists of a set of addressable data elements. Data elements are objects to be read, and the object IDs determine these data elements.

A data element consists of three objects:

1. Basic device identifier: All objects of this type are mandatory, such as the vendor name, product code, and revision version.
2. Regular device identifier: In addition to the basic data objects, the device provides additional and optional identifiers and data object description. Define all types of objects according to definitions in the standard, but the execution of this type of objects is optional.
3. Extended device identifier: In addition to regular data objects, the device provides additional and optional identifiers and private data object description. All the data is related to the device.

Table 5-4 Read device identifiers

Object ID	Object Name/ Description	Type	Mandatory/ Optional	Type
0x00	Vendor	ASCII string	Mandatory	Basic
0x01	Product code	ASCII string	Mandatory	
0x02	Main revision version	ASCII string	Mandatory	
0x03–0x7F	--	--	--	Regular
0x80–0xFF	--	--	--	Extended

5.3.6.1 Command for Querying Device Identifiers

Table 5-5 Request frame format

Data Field	Length	Description
Function Code	1 byte	0x2B
MEI Type	1 byte	0x0E
ReadDevId Code	1 byte	01
Object ID	1 byte	0x00

Table 5-6 Frame format for a normal response

Data Field			Length	Description
Function Code			1 byte	0x2B
MEI Type			1 byte	0x0E
ReadDevId Code			1 byte	01
Conformity Level			1 byte	01
More			1 byte	--
Next Object ID			1 byte	--
Object Quantity			1 byte	--
Object List	First object	Object ID	1 byte	0x00
		Object length	1 byte	N
		Object value	*N* bytes	--
	...	...	...	...

Table 5-7 Object list

Object ID	Object Name/ Description	Description	Type
0x00	Vendor	"HUAWEI"	Basic
0x01	Product code	"SUN2000" or "LUNA2000-P"	
0x02	Main revision version	ASCII string, software version	

Table 5-8 Frame format for an abnormal response

Data Field	Length	Description
Function Code	1 byte	0xAB
Exception Code	1 byte	See **5.3.2 Exception Code**.

5.3.6.2 Command for Querying a Device List

Table 5-9 Request frame format

Data Field	Length	Description
Function Code	1 byte	0x2B
MEI Type	1 byte	0x0E
ReadDevId Code	1 byte	03
Object ID	1 byte	0x87

Table 5-10 Frame format for a normal response

Data Field			Length	Description
Function Code			1 byte	0x2B
MEI Type			1 byte	0x0E
ReadDevId Code			1 byte	03
Conformity Level			1 byte	03
More			1 byte	--
Next Object ID			1 byte	--
Object Quantity			1 byte	--
Object List	First object	Object ID	1 byte	0x87
		Object length	1 byte	N
		Object value	*N* bytes	--
	...	...	...	...

Table 5-11 Object list

Object ID	Object Name	Type	Description
0x80–0x86	Retained	--	Returns a null object with a length of 0.

Object ID	Object Name	Type	Description
0x87	Number of devices	int	Returns the number of devices connected to this address.
0x88	Description about the first device	ASCII string See the device description definitions.	Returns only description about the first device if an NE allows only one device to be connected to each address.
0x8A	Description about the second device	--	--
--	--	--	--
0xFF	Description about the 120th device	--	--

5.3.6.3 Device Description Definition

Each device description consists of all "attribute=value" character strings.

"Attribute ID=%s;attribute ID=%s;... attribute ID=%s"

Example: "1= LUNA2000-200KTL-H0; 2=V800R021C10; 3=P1.0-D5.0; 4=123456789ABC; 5=1; 6=1.0; 8=LUNA2000-P"

Table 5-12 Definition of attributes

Attribute ID	Attribute	Type	Description
1	Device model	ASCII string	--
2	Device software version	ASCII string	--
3	Interface protocol version	ASCII string	See the interface protocol version definitions.
4	ESN	ASCII string	--
5	Device ID	int	0, 1, 2, 3,... (assigned by NEs; 0 indicates the master device into which the Modbus card is inserted)
6	Feature version	ASCII string	--

Attribute ID	Attribute	Type	Description
8	Device type	ASCII string	LUNA2000-P or SUN2000

Table 5-13 Frame format for an abnormal response

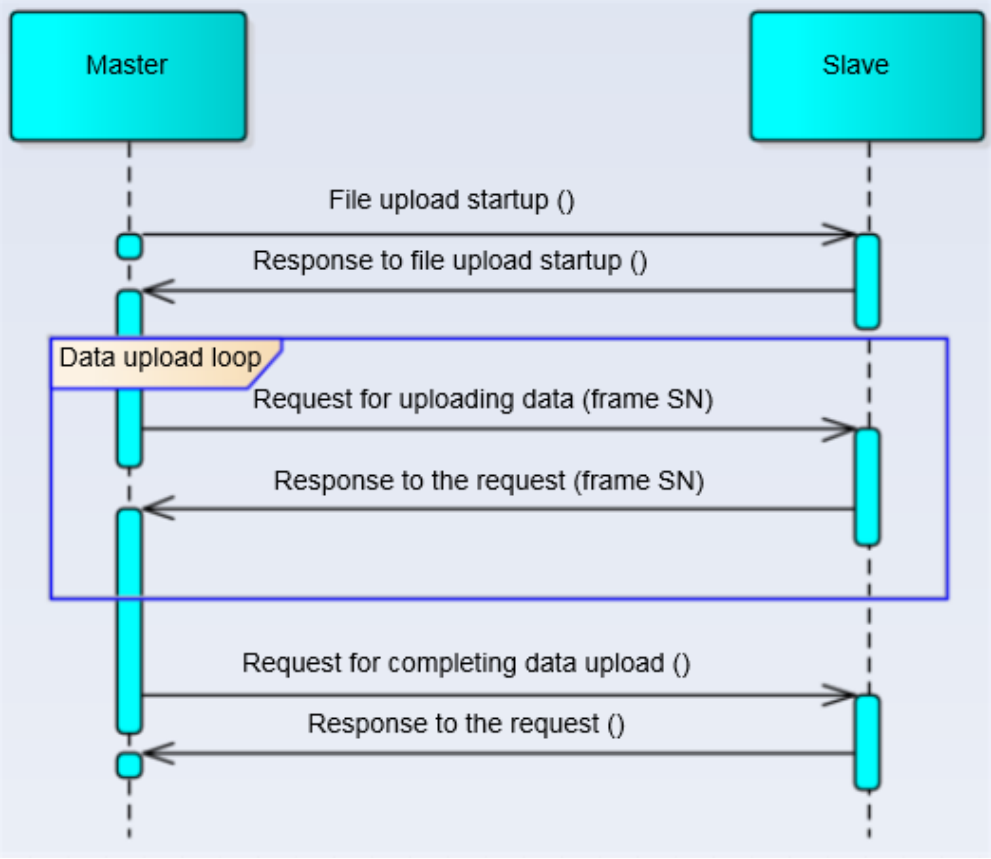
Data Field	Length	Description
Function Code	1 byte	0xAB
Exception Code	1 byte	See **5.3.2 Exception Code**.

5.3.7 Huawei-defined Functions (0x41)

5.3.7.1 Uploading Files

Uploading files means uploading from a slave node to a master node through stream access. The following figure shows the file uploading process.

Figure 5-6 File uploading process



5.3.7.1.1 Starting the Upload

Frame format of a request from a master node

Table 5-14 PDU data field of the request frame for starting upload (0x05)

PDU Data Field	Length (Byte)	Description
Function Code	1	0x41
Sub-function Code	1	0x05
Data Length	1	1+N
File Type	1	Unique ID of a file
Customized Data	N	-

Table 5-15 PDU data field of the response frame for starting the upload (0x05)

Data Field	Length (Byte)	Description
Function Code	1	0x41
Sub-function Code	1	0x05
Data Length	1	6 + N
File Type	1	Unique ID of a file
File Length	4	-
Data Frame Length	1	-
Customized Data	N	-

Table 5-16 PDU data field in the abnormal response frame of the slave node

PDU Data Field	Length	Description
Error Code	1	0xC1
Exception Code	1	See **5.3.2 Exception Code**.

NOTE

If the exception code is 0x06, the request will be retransmitted in 10 seconds. A maximum of six attempts are supported.

5.3.7.1.2 Uploading Data

Table 5-17 Request frame for uploading data (0x06)

PDU Data Field	Length (Byte)	Description
Function Code	1	0x41
Sub-function Code	1	0x06
Data Length	1	3
File Type	1	Unique ID of a file
Frame No.	2	0x0000–0xFFFF

Table 5-18 Response frame for uploading data (0x06)

PDU Data Field	Length (Byte)	Description
Function Code	1	0x41
Sub-function Code	1	0x06
Data Length	1	3 + N
File Type	1	-
Frame No.	2	0x0000–0xFFFF
Frame Data	N	-

Table 5-19 Abnormal response frame for uploading data

PDU Data Field	Length (Byte)	Description
Error Code	1	0xC1
Exception Code	1	See **5.3.2 Exception Code**.

5.3.7.1.3 Completing the Data Upload

Table 5-20 Request frame for completing the data upload

PDU Data Field	Length (Byte)	Description
Function Code	1	0x41
Sub-function Code	1	0x0c
Data Length	1	1
File Type	1	-

Table 5-21 Response frame for completing the data upload

PDU Data Field	Length (Byte)	Description
Function Code	1	0x41
Sub-function Code	1	0x0c
Data Length	1	3
File Type	1	-
File CRC	2	-

Table 5-22 Abnormal response frame for completing the data upload

Data Field	Length	Description
Error Code	1	0xC1
Exception Code	1	See **5.3.2 Exception Code**.

5.3.7.1.4 Timeout Processing

Table 5-23 Processing specifications for sub-process timeout

Item	Constraint
Response timeout period for starting an upload	10s
Response timeout period for uploading data	10s
Maximum retransmission attempts for data upload command	6
Response timeout period for completing a data upload	10s

