3onedata

ICP222-1T2F-2CI-TB-P(12-48VDC)
CAN Server
User Manual

Document Version: 01

Release Date: 07/26/2022

Trademark statement

3onedata, 3onedata and 3One data are the registered trademark owned by 3onedata Co., Ltd. And other trademarks mentioned in this manual belong to their corresponding companies.

Notice

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

3onedata Co., Ltd.

Headquarter address:	3/B, Zone 1, Baiwangxin High Technology Industrial park, Nanshan District, Shenzhen, 518108 China
Technology support:	tech-support@3onedata.com
Service hotline:	+86 -880-4496
E-mail:	sales@3onedata.com
Fax:	+86 -0755-26703485
Website:	http://www.3onedata.com

Preface

The user manual has introduced the CAN server:

- Can Port Work Mode
- Network management relative principle overview

Audience

This manual applies to the following engineers:

- Network administrators
- Technical support engineers

Text Format Convention

Format	Description
" "	Words with “” represent the interface words. Such as: “Port No.“.
>	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
 Notice	Remind the announcements in the operation, improper operation may result in data loss or equipment damage.
 Warning	Pay attention to the notes on the mark, improper operation may cause personal injury.

Format	Description
 Note	Conduct a necessary supplements and explanations for the description of operation content.
 Key	Configuration, operation, or tips for device usage.
 Tips	Pay attention to the operation or information to ensure 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	07/26/2022	Manual development

Content

1 Log in the Web Interface

About this chapter

Content	Link
This Chapter	1.1 WEB Browsing System Requirements 1.2 Setting IP Address of PC 1.3 Log in the Web Configuration Interface

1.1 WEB Browsing System Requirements

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

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

1.2 Setting IP Address of PC

The default management of device is as follows:

IP Settings	Default Values
IP address	192.168.1.254
Subnet mask	255.255.255.0

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 CAN server are on the same subnet.

Note

While configuring the device for the first time, if it's the local configuration mode, first confirm the network segment of current PC is 1.

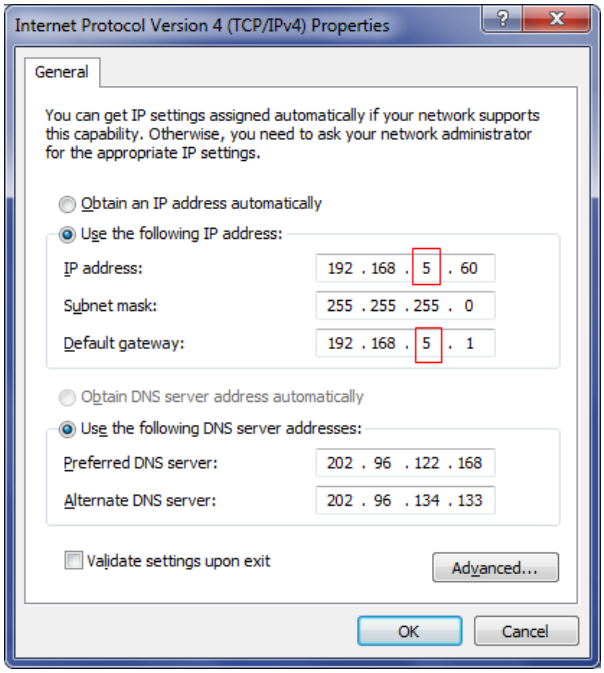
Eg: Assume that the IP address of the current PC is 192.168.5.60, change the network segment "5" of the IP address to "1".

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".



Step 3 Click “OK”, IP address is modified successfully.

Step 4 End.

1.3 Log in the Web Configuration Interface

Operation steps

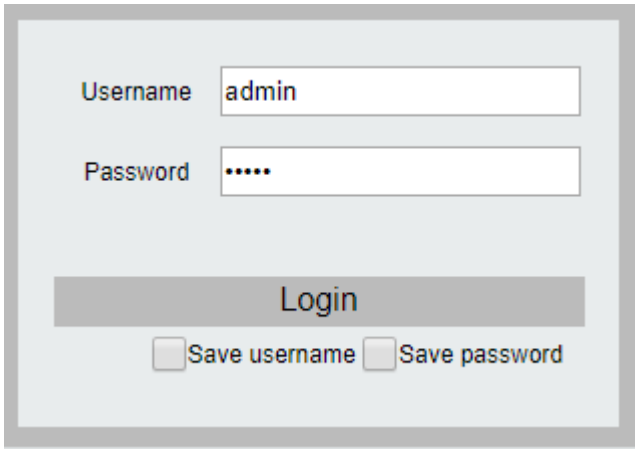
Login in the web configuration interface as follow:

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.



Note:

- The default username and password are “admin”; please strictly distinguish capital and small letter while entering.
- Default user account has the administrator privileges.

Step 5 Click "Login".

Step 6 End.

After successful login, you can configure the relevant parameters and information of the WEB interface as needed.

2 System Information

About this chapter

Content	Link
This Chapter	2.1 Product Information 2.2 Network information

2.1 Product Information

Function Description

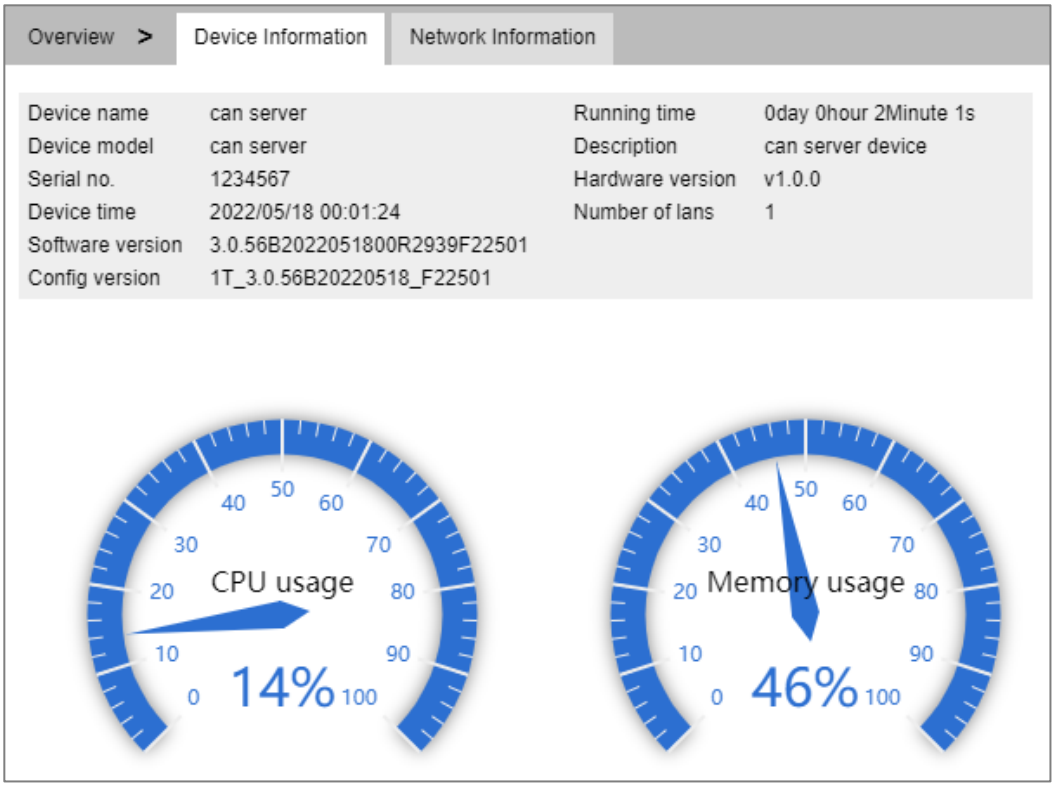
In “Device information” interface, user can check Device name,Device model, CAN No, Firmware Ver, Device time, Description, Number of LAN, CPU Utilization, Memory Utilization and so on.

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. Note: Configure the device name on the "System Management > Device Information Configuration" page.
Device model.	Equipment model or name of the device.
Serial no.	Serial number of the device
Device time	The time display of current device, which can synchronize the time of local PC or NTP server.
Software version	Software version information of the device.
Config version	Software version information of the device.
Running time	Running time of the current device.
Description	Description information of the device. Note: Configure the device information On the "System Management > Device Information Configuration" page.
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

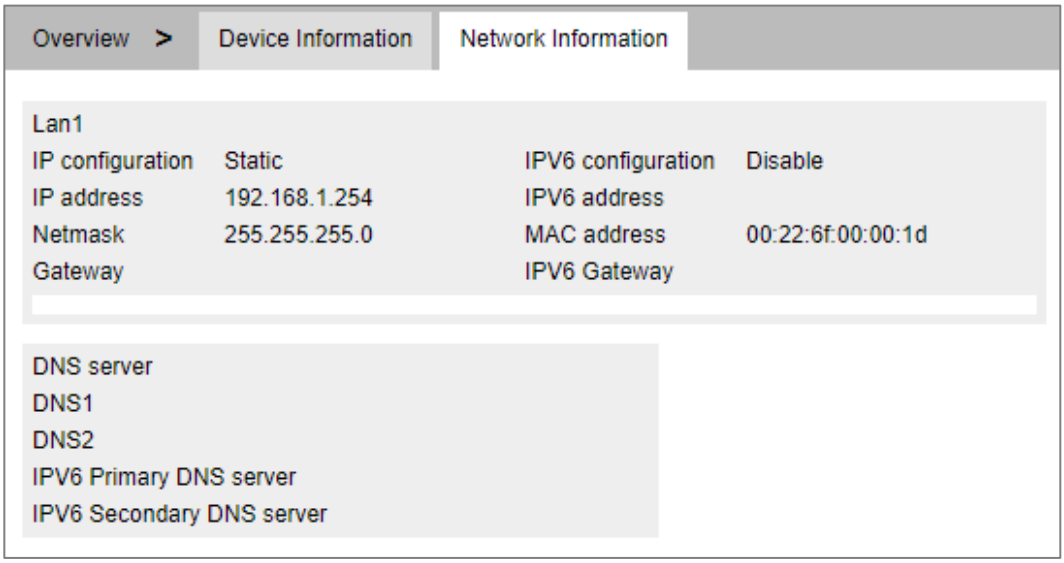
On the page of "Network information", user can check device network address information and DNS server information.

Operation Path

Open in order: “System Information” > Network Information”.

Interface Description

Network information interface as follows:



The main elements configuration description of network information interface.

Interface Element	Description
LAN1	**LAN1 information bar**
IP Configuration	Display how the LAN 1 of the device gets the IP address.
Netmask	Display device subnet mask.
MAC Address	Display the MAC address of device LAN1.
IP Address	Display LAN1 IP address.
Gateway	Display LAN1 gateway address.
IPv6Configuration	Display how the LAN 1 of the device gets the IPv6 address.
IPv6 Address	Display the IPv6 address of device LAN1.
IPv6 Gateway	Display LAN1 IPv6 gateway address.
DNS server	**DNS server information bar**
DNS1	Display device main DNS server address.
DNS2	Display device backup DNS server address.
IPv6 Primary DNS	Display the IPv6 primary DNS server of the device.

Interface Element	Description
Server	
IPv6 Secondary DNS Server	Display the IPv6 secondary DNS server of the device.

3 Network Configuration

Function Description

On the “Network Configuration” page, you can configure the IP address, DNS address and LLDP of the device. The IPv4 address of the device supports dynamic acquisition or manual static configuration through DHCP and BOOTP protocol, and the IPv6 address supports dynamic acquisition or manual static configuration through DHCPv6 protocol, and also supports dynamic acquisition of IPv6 address by SLAAC. The IPv4 and IPv6 addresses of the device support dynamic acquisition of DHCP protocol or manual static configuration, and IPv4 also supports automatic acquisition of BOOTP protocol.

The total length of IPv6 address is 128 bits, and it is usually divided into 8 groups, each of which is in the form of 4 hexadecimal numbers, and each group of hexadecimal numbers is separated by a colon. For the convenience of writing, IPv6 also provides a compression format. The specific compression rules are:

- The leading "0" in each group can be omitted.
- The address contains two or more consecutive groups of 0, which can be replaced by double colons "::".

An IPv6 address can be divided into the following two parts:

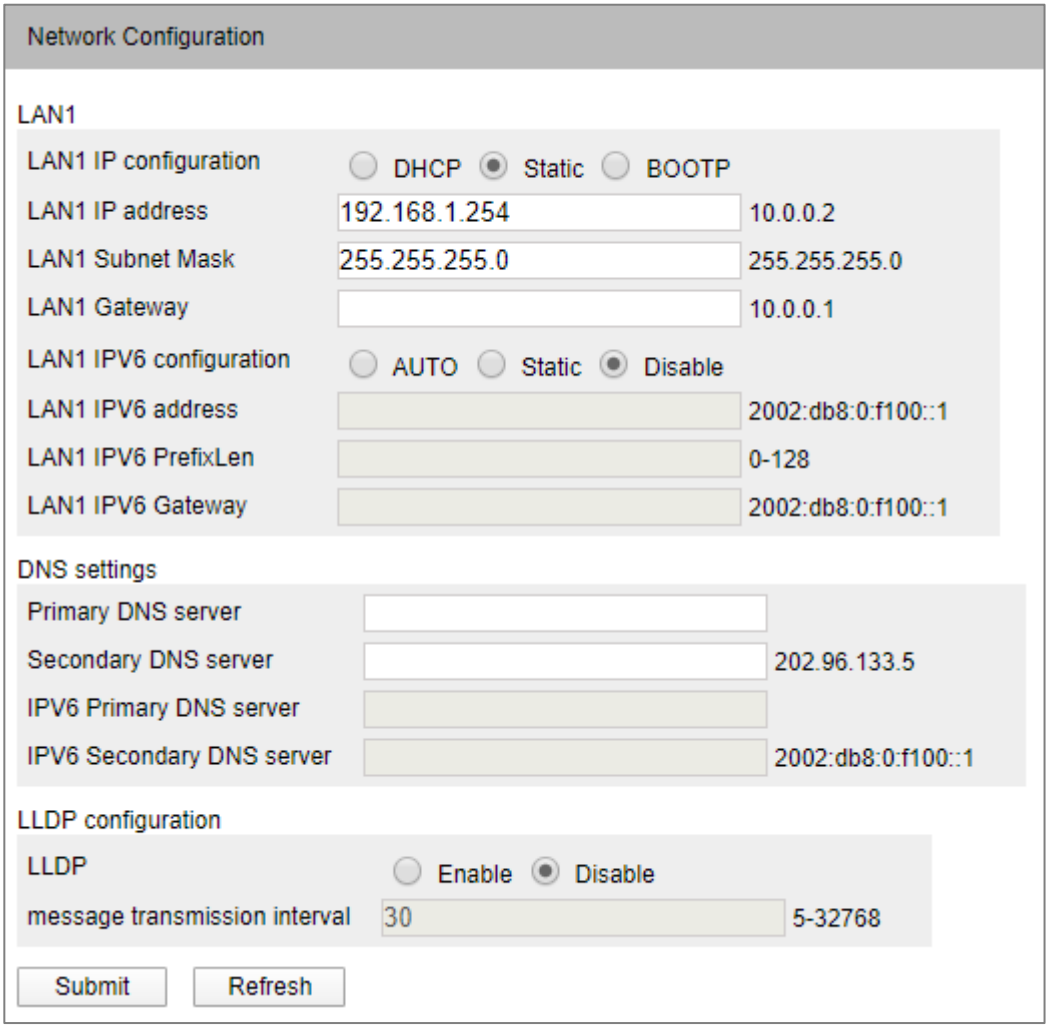
- Network prefix: n bits, equivalent to the network ID in IPv4 address;
- Interface: 128-n bits, equivalent to the host ID in IPv4 address.

Operation Path

Open: “Network Configuration”.

Interface Description

Network configuration interface as follows:



The main element configuration description of network configuration interface:

Interface Element	Description
Network Port 1	**LAN1 Configuration Bar**
LAN1 IP Configuration	Configuration of network address of device LAN 1: • DHCP: Obtain an IP address, subnet mask, and gateway address automatically from DHCP server. • Static: 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	Manually set the IP address of the device LAN1, which is 192.168.1.254 by default.
LAN1 Subnet Mask.	Manually set the subnet mask of the device LAN1, which is 255.255.255.0 by default.
LAN1 Gateway	Manually set the gateway address of the device LAN 1.
LAN1 IPv6	Configuration mode of LAN1 IPv6 network address:

Interface Element	Description
Configuration	• AUTO(DHCPv6): automatically acquire dynamic IP address, network address prefix and gateway address from DHCP server, or acquire network address prefix through SLAAC to finish IPv6 address setting. • Static: manually configure IP address, address prefix length and gateway address. • Disable: IPv6 network address is not enabled by default.
LAN1 IPv6 Address	Under manual setting, the LAN1 IPv6 address of the device, such as 2002:db8:0:f100::1.
LAN1 IPv6 PrefixLen	Under the manual setting, the LAN1 IPv6 network prefix length of the device, which is in the range of 0-128.
LAN1 IPv6 Gateway	Under manual setting, the LAN1 IPv6 gateway address of device.
DNS Settings	**DNS Settings Bar**
Primary DNS Server	DNS Sever IP address, for example: 202.96.133.4.
Secondary DNS Server	DNS Sever backup IP address, for example: 202.96.133.5.
IPv6 Primary DNS Server	IPv6 address of DNS server, such as: 2002:db8:0:f100::4.
IPv6 Secondary DNS Server	Secondary IPv6 address of DNS server, such as: 2002:db8:0:f100::5.
LLDP Configuration	**LLDP Configuration Bar**
LLDP	LLDP function enables radio box, and the options are as follows: • Enable: enable LLDP (link layer discovery protocol). • Disable: Disable LLDP.
Message Transmission Interval	LLDP message transmission interval time, the value range is 5-32768, unit: second. When the LLDP function is enabled, the device will periodically send LLDP messages to neighboring devices.

4 Rapid Ring

About This Chapter

Content	Link
This chapter	4.1 Ring Configuration 4.2 Ring Status

4.1 Ring Configuration

Function Description

On the "Ring Configuration" page, you can configure the device ring network redundancy function of the fiber port.

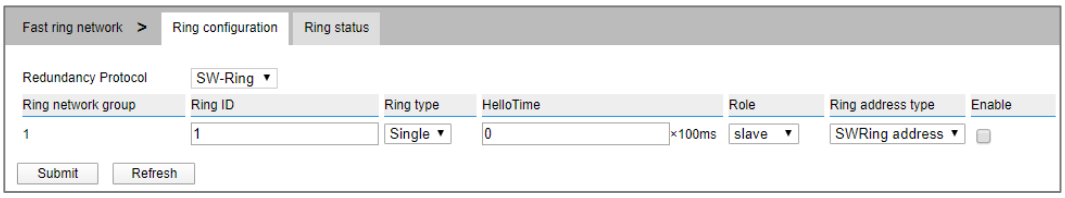
SW-Ring is an Ethernet ring network algorithm independently developed by our company, which is specially developed and designed for high-reliability industrial control network applications that need link redundancy backup. It has Ethernet link redundancy and the ability of fast and automatic fault recovery. SW-Ring adopts no-master station design. In a multi-ring network composed of 250 devices at most, the network disconnection self-recovery time is less than 20ms. The fiber port of the device can be used as a ring network port to connect with other switches. When the network connection is interrupted, the SW-Ring redundancy mechanism enables the backup link to quickly restore the network communication.

Operation Path

Open in order: “Fast Ring Network > Ring Configuration”.

Interface Description

Ring configuration interface as follows:



The main element configuration description of ring configuration interface:

Interface Element	Description
Redundancy Protocol	Select the corresponding redundancy protocol. Options are: • None: indicates that the ring network function is disabled. • SW-Ring V3: support single ring and chain.
Ring Network Group	Support ring network group 1, it means that the device supports at most 1 ring network group.
Ring ID	The current ring network ID of ring network when multiple devices form a ring network. The network ID is different in different ring networks.
Ring Type	According to the requirements of the site environment, different ring network types can be selected. • Single: Single ring, using a continuous ring to connect each device together. • Chain: Chain, through an advanced software technology, enhances the flexibility of users to build any type of redundant network topology.
Hellotime	Hello_time is the interval of hello packet transmission, which is an inquiry packet sent by CPU to adjacent devices through the ring network port to confirm whether the connection is normal.
Role	The single ring type has the options of master and slave devices, and supports the structure of one-master-multiple - slave and no-master. One-master-multi-slave structure is, when the device is the master device, one end of the loop master device is the backup link, and when the loop network fails, the slave master station activates the backup link to ensure the normal operation of the network. When all the ring network devices are slave stations, it is a no-master structure.
Ring Address Type	The destination MAC address type of the ring network protocol, the same ring network address type is used in the same ring network, and the options are as follows: • SWRing Address：SWRing protocol address, this default configuration is recommended. • STP Address: when some device Chain or HelloTime in the ring network are incompatible, all devices in the ring

Interface Element	Description
	network can be switched to STP protocol addresses.
Enable	Enable or disable the corresponding ring network group.

4.2 Ring Status

Function Description

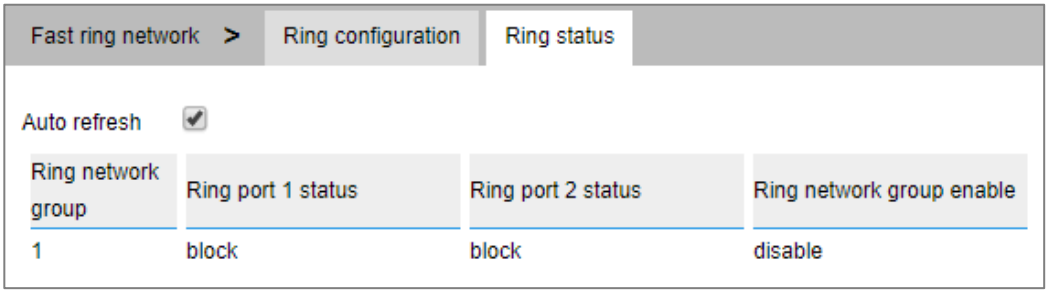
On the “Ring Status” page, you can view the ring network status of the fiber port of the device.

Operation Path

Open in order: “Fast Ring Network > Ring Status”.

Interface Description

Ring status interface as follows:



The main element configuration description of ring status interface:

Interface Element	Description
Auto Refresh	Auto refresh check box. After checking it, the page will be automatically refreshed every 5 seconds.
Ring Network Group	Display the ring network group ID.
Ring Port 1 Status	Communication status of ring network port 1 can be shown as follows: • Block • Forward
Ring Port 2 Status	Communication status of ring network port 2 can be shown as follows: • Block • Forward
Ring Network	The enabled status of the ring group can be displayed as

Interface Element	Description
Group Enable	follows: • Enable • Disable

5 CAN Settings

Function Description

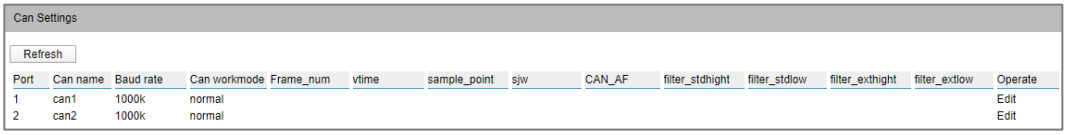
Users can check and configure baud rate, woke mode, subcontract frame number, CAN frame limit and other parameters of each CAN port of the device on “CAN Settings“ page.

Operation Path

Open: "CAN Settings”.

Interface Description

CAN settings interface as follows:



The main element configuration description of CAN settings interface:

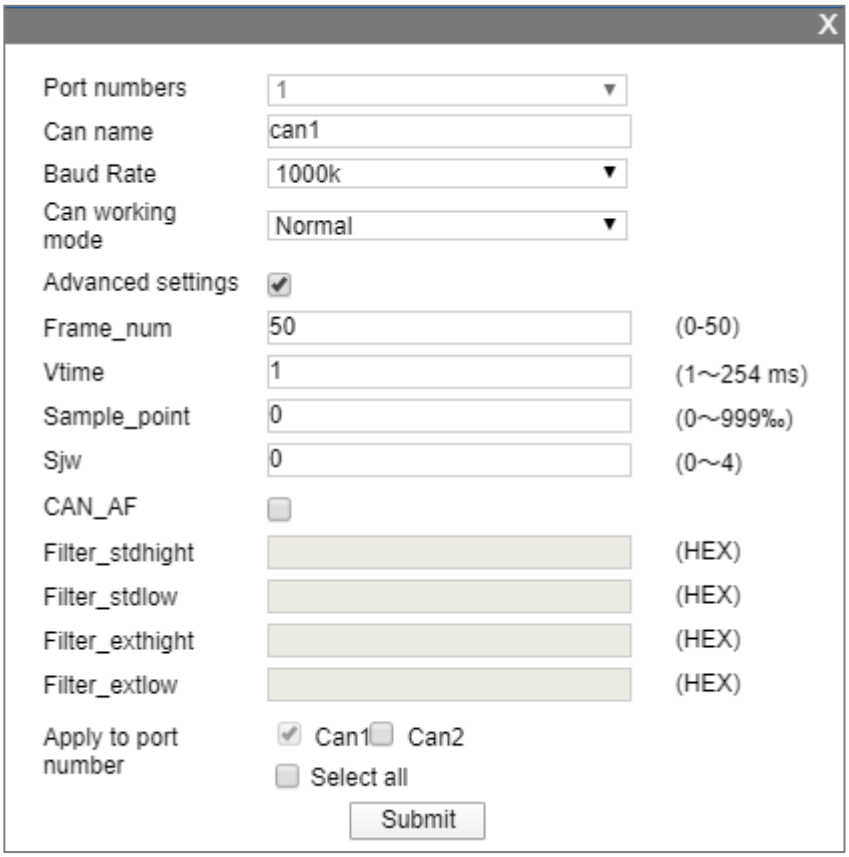
Interface Element	Description
Port	Display the CAN port number of the device.
CAN name	Displays the name of the device’s CAN port.
Baud Rate	Display the baud rate of the device’s CAN port.
Can workMode	Display the work mode of the device‘s CAN port. • Normal: the device is in normal operating status. • Listening: the device is in interception status and can't send data. • Self Test: the device is in the self-transmitting and receiving operation status.
Frame_Num	Display the number of CAN frames received when the device CAN port encapsulates Ethernet packets.
vTime	Display the time interval of CAN frames received when the device CAN port encapsulates Ethernet packets.

Interface Element	Description
Sampling_point	Display the value of sampling point of the device's CAN port, unit is "‰".
Sjw	Display the resynchronized jump width of the device's CAN port.
CAN_AF	Display acceptance and filtering status of the device's CAN port. • Enable • Disable
filter_stdhight	Display the upper limit of standard frame received by the device's CAN port.
filter_stdlow	Display the lower limit of standard frame received by the device's CAN port.
filter_exthight	Display the upper limit of extended frame received by the device's CAN port.
filter_extlow	Display the lower limit of extended frame received by the device's CAN port.
Operate	Click "Edit" to modify the parameters of corresponding CAN port.

Click Edit in the CAN port entry to modify the current CAN port parameters.

Interface Description: Edit

Edit interface is as follows:



Configuration description of main elements of the Edit interface:

Interface Element	Description
Port numbers	The port number of the device's CAN port edited currently.
CAN name	Set the name of the device's CAN port which supports up to 1-32 letters or numbers.
Baud Rate	CAN baud rate drop-down list, options as follows: 5K/10K/20K/50K/100K/125K/250K/500K/800K/1000K
Can Working Mode	The drop-down list of CAN work mode, the options are as follows: • Normal: the device is in normal operating status. • Just Listen: CAN server is in interception status and can't send data. • Self Test: the device is in the self-transmitting and receiving operation status.
Advanced Settings	Advanced Settings Check box, click to configure more function parameters.
Frame—num	When the CAN port continuously receives data and the received CAN frame number reaches "Frame Number", the received data is packaged as an Ethernet packet and sent out, settable value is 0-50.

Interface Element	Description
VTime	When the CAN port doesn't receive the new data frame within defined time of "Frame Wait Time", the received data that hasn't been sent out is packaged to an Ethernet packet sent to the Ethernet port, settable value is 1-254ms.
Sampling point	Sampling point is the sample of bus state at the end of phase buffer section 1 when the bus level is read and converted into the corresponding bit value. The desired value is the percentage of the time from the beginning of a bit to the sampling point to the total time of a complete bit, which ranges from "0-999‰". Note: When there is a phase difference on the bus, you can adjust the sampling point for resynchronization.
Sjw	SJW (reSynchronization Jump Width) specifies the upper limit of the extension or shortening of the phase buffer section. The value ranges from 1 to 4.
CAN_AF	CAN_AF check box, click to enable CAN port acceptance and filtering function. After enabled, the data will be eliminated if the standard frame and the extended frame ID received by CAN port are not in the restricted range.
filter_stdhight	The upper limit of standard frame received by the device's CAN port, which is hexadecimal and the valid value range is 000-7FF.
filter_stdlow	The lower limit of standard frame received by the device's CAN port, which is hexadecimal and the valid value range is 000-7FF.
filter_exthight	The upper limit of extended frame received by the device's CAN port, which is hexadecimal and the valid value range is 00000000-1FFFFFFF.
filter_extlow	The lower limit of extended frame received by the device's CAN port, which is hexadecimal and the valid value range is 00000000-1FFFFFFF.
Apply to the port number	Check the CAN port check box to apply the current settings to the specified CAN port.

6 CAN Mode

About this chapter

Content	Link
This Chapter	6.1 TCP Server Mode 6.2 TCP Client Mode 6.3 TCP Server Mode Configuration Bar 6.4 UDP Client Mode 6.5 UDP Rang Mode 6.6 UDP Multicast Mode

Function Description

Configure the work mode of corresponding device CAN port on "CAN Mode Settings" page.

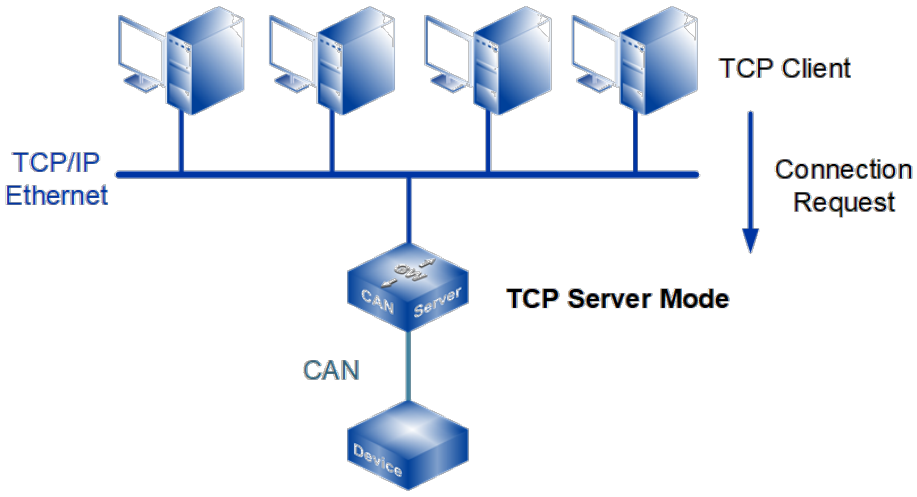
The working modes supported by the device are:

- CAN TCP Server Mode
- CAN TCP Client Mode
- CAN UDP Server Mode
- CAN UDP Client Mode
- CAN UDP Rang Client Mode
- CAN UDP Muliticast Mode

Operation Path

Open in order “CAN Mode > CAN1”. Under the menu of "CAN Mode", the corresponding CAN port information can be configured by entering different CAN ports. The configuration operation mode of all CAN ports' WEB interfaces is the same.

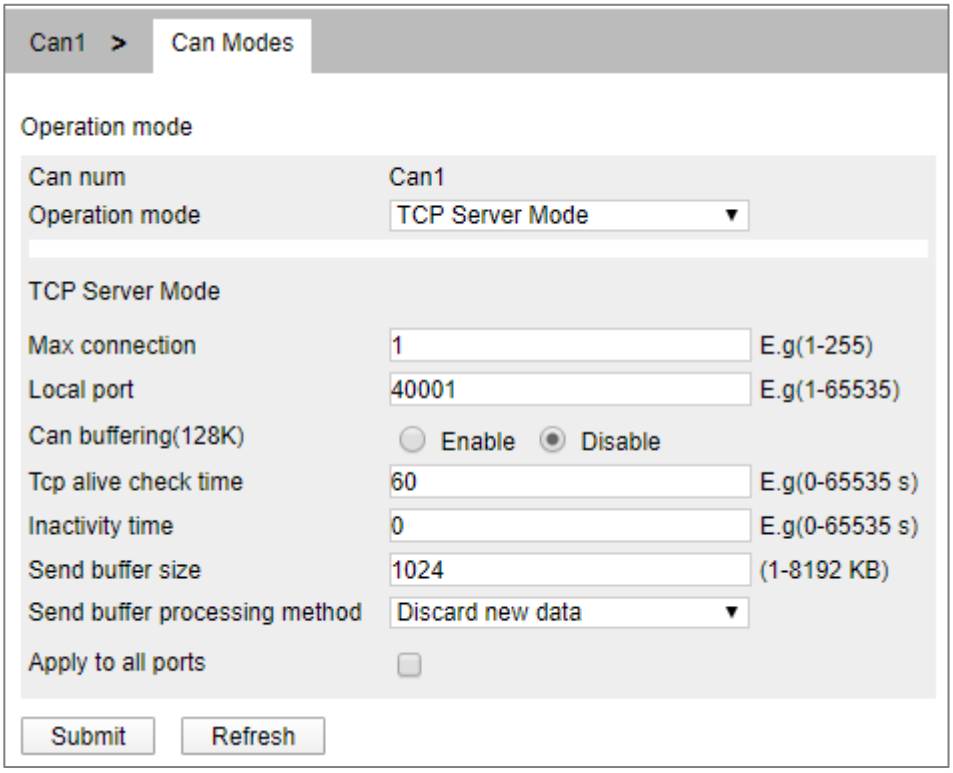
6.1 TCP Server Mode



In CAN TCP server mode, the device is assigned an IP port number and passively waits for the host to connect. After the host initiates connection request and establish connection to the device, the host can realize the data transmission via network connection and CAN port. CAN TCP Server Mode supports multiple session connection at the same time, so that multiple hosts can read or send Ethernet data to a CAN port device at the same time.

Interface Description

TCP server mode interface is as follows:

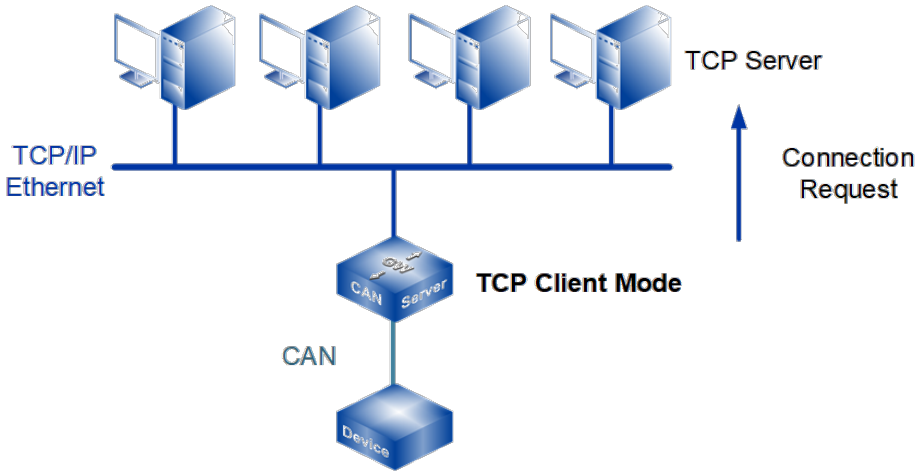


TCP server mode interface main element configuration instructions:

Interface Element	Description
Operation mode	**Operation Mode Configuration Bar**
CAN num	Displays the CAN number of the device currently configured.
Operation mode	The operation modes of CAN port of the device are as follows: • TCP Server Mode • TCP Client Mode • UDP Server Mode • UDP Client Mode • UDP Rang Mode • UDP Multicast Mode
TCP Server Mode	**TCP Server Mode Configuration bar**
Max connection	The maximum session number supported by the device's CAN port. Note: Session refers to the process the device transmits data received from CAN port to Ethernet via socket connection. More than one session number represents the device transmits the data received from CAN port to Ethernet via more than one socket.
Local port	Local port of the device, effective range is 1-65535. Note: TCP port provided by the device that can be connected by other TCP/IP nodes, which is associated with the corresponding CAN port of the device.
CAN buffering(128k)	Port data cache, which can cache CAN port data up to 128K after the network is abnormal. When the network returns to normal, the cached data is forwarded. Options are as follows: • Enable; • Disable.
TCP alive check time	If no TCP activity occurs within the allotted time, the system would send contact-probing message to check the validity of TCP connection. If the reply packet of opposite side hasn't been received after sending probe packet for 3 times, system will regard the opposite side as down and forwardly close the communication connection. If set TCP Alive Time to "0", the function will be disabled. Effective time range 0~65535s.
Inactivity time	The idle time of device's communication link, valid time range 0~65535s. • TCP Timeout > 0: If there is no data communication between the server and client, the server and client will break connection.

Interface Element	Description
	• TCP Timeout = 0: When there is no data communication between the server and client, the server and client will keep in connection status.
Send buffer size	The size of CAN port's cache for sending, range 1-8192KB. If the Ethernet receives too much data, CAN needs to cache the data. If the cache is too large, the real-time data will be affected.
Send buffer processing method	When sending cache data overflows, the data can be processed as follows: • Discard new data; • Discard old data.
Apply to all ports	Apply current setting to all CAN ports.

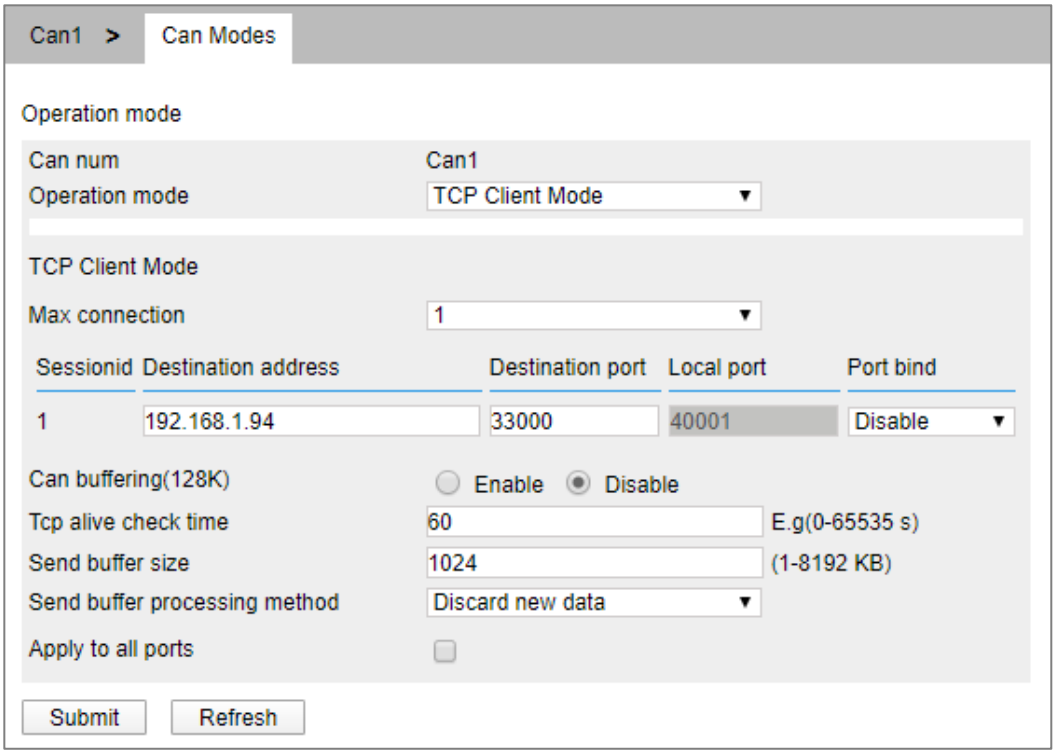
6.2 TCP Client Mode



In CAN TCP client mode, the device can actively establish a network connection with the host specified by the user when the CAN port data arrives. After the data transmission is completed, the device will automatically close the network connection according to TCP keep-alive time/idle timeout and other parameters. CAN TCP Client Mode supports multiple session connection at the same time, so that multiple hosts can read or send Ethernet data to a CAN port device at the same time.

Interface Description

TCP Client mode interface is as follows:

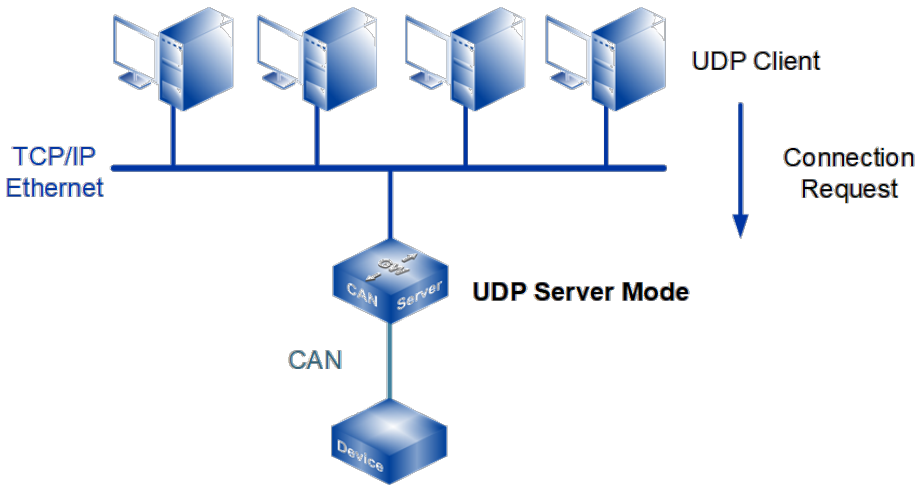


TCP client mode interface main element configuration instructions:

Interface Element	Description
Operation mode	**Operation Mode Configuration Bar**
CAN num	Displays the CAN number of the device currently configured.
Operation mode	The **operation** modes of CAN port of the device are as follows: • TCP Server Mode • TCP Client Mode • UDP Server Mode • UDP Client Mode • UDP Rang Mode • UDP Multicast Mode
TCP Client Mode	**TCP Client Mode Configuration Bar**
Max connection	The session number of the device's CAN port. Note: Session refers to the process the device transmits data received from CAN port to Ethernet via socket connection. More than one session number represents the device transmits the data received from CAN port to Ethernet via more than one socket.
Destination address	The IP address of the server to which the device needs to connect.
Destination port	Enter the TCP port number of the server to which the device needs to connect.

Interface Element	Description
Local port	A local port number assigned by the device for TCP connection, which can provide service or connection to the outside world, is used to connect and communicate with the server.
Port bind	Local port fixed, options are as follows: • Disable: the system automatically selects the idle local port to establish a connection with the server; • Enable: connect to the server using a manually configured local port.
Can buffering (128k)	Port data cache, which can cache CAN port data up to 128K after the network is abnormal. When the network returns to normal, the cached data is forwarded. Options are as follows: • Enable; • Disable.
TCP alive check time	If no TCP activity occurs within the allotted time, the system would send contact-probing message to check the validity of TCP connection. If not receiving any reply packet from the other after sending probing packet three times in succession, it would consider the opposite side as offline and take the initiative to close communication connection. If set TCP Alive Time to "0", the function will be disabled. Effective time range 0~65535s.
Send buffer size	The size of CAN port's cache for sending, value range is 1-8192KB. If the Ethernet receives too much data, CAN needs to cache the data. If the cache is too large, the real-time data will be affected.
Send buffer processing method	When sending cache data overflows, the data can be processed as follows: • Discard new data; • Discard old data.
Apply to all ports	Apply current setting to all CAN ports.

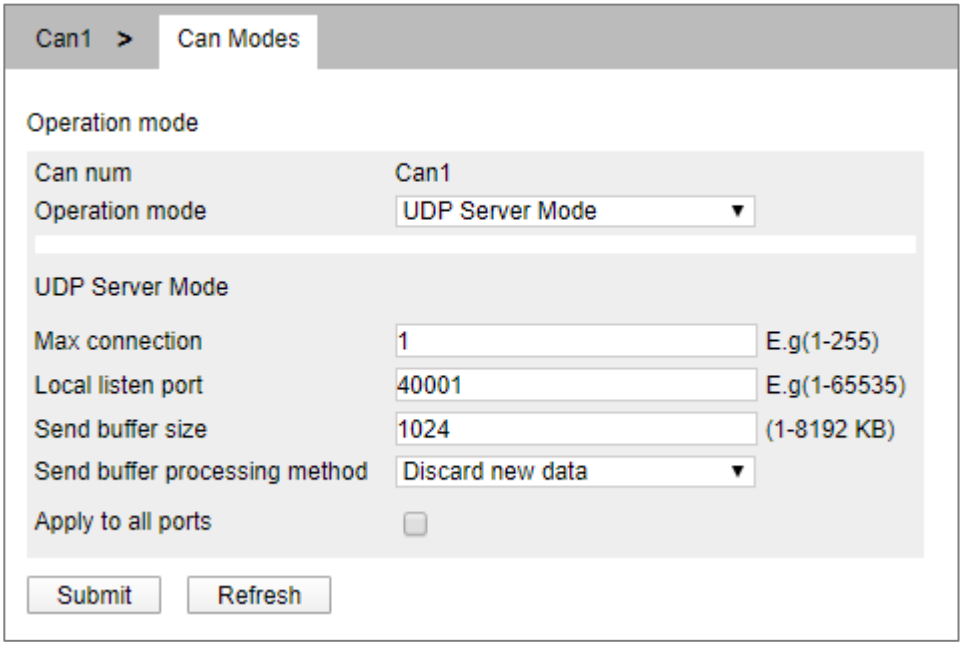
6.3 TCP Server Mode Configuration Bar



Under CAN UDP Server Mode, the device can be a server, and it can transmit data with the host user appointed under the UDP protocol. Under CAN UDP Server Mode, the device can transmit the data from CAN device to one or multiple hosts, and CAN device can also receive the data from one or multiple hosts.

Interface Description

TCP Server Mode interface is as follows:

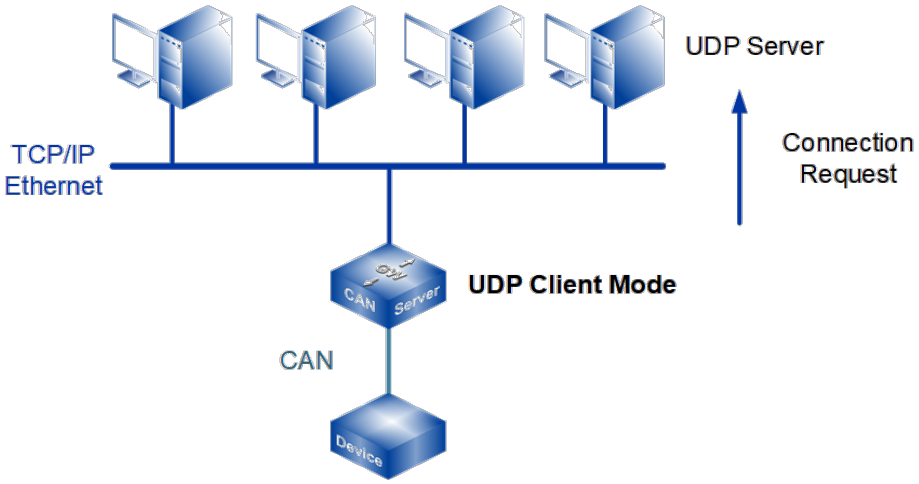


UDP Server Mode interface main element configuration instructions

Interface Element	Description
Operation mode	**Operation Mode Configuration Bar**
CAN num	Displays the CAN number of the device currently configured.

Interface Element	Description
Operation mode	The **operation** modes of CAN port of the device are as follows: • TCP Server Mode • TCP Client Mode • UDP Server Mode • UDP Client Mode • UDP Rang Mode • UDP Multicast Mode
UDP Server Mode	**TCP Server Mode Configuration Bar**
Max connection	The maximum session number supported by the device's CAN port.
Local listen port	The device is used as the listening port of UDP server for receiving UDP data. Note: User must allot the only listening port to each CAN port, then the system can normally receive UDP data.
Send buffer size	The size of CAN port's cache for sending, value range is 1-8192KB. If the Ethernet receives too much data, CAN needs to cache the data. If the cache is too large, the real-time data will be affected.
Send buffer processing method	When sending cache data overflows, the data can be processed as follows: • Discard new data; • Discard old data.
Apply to All Ports	Apply current setting to all CAN ports.

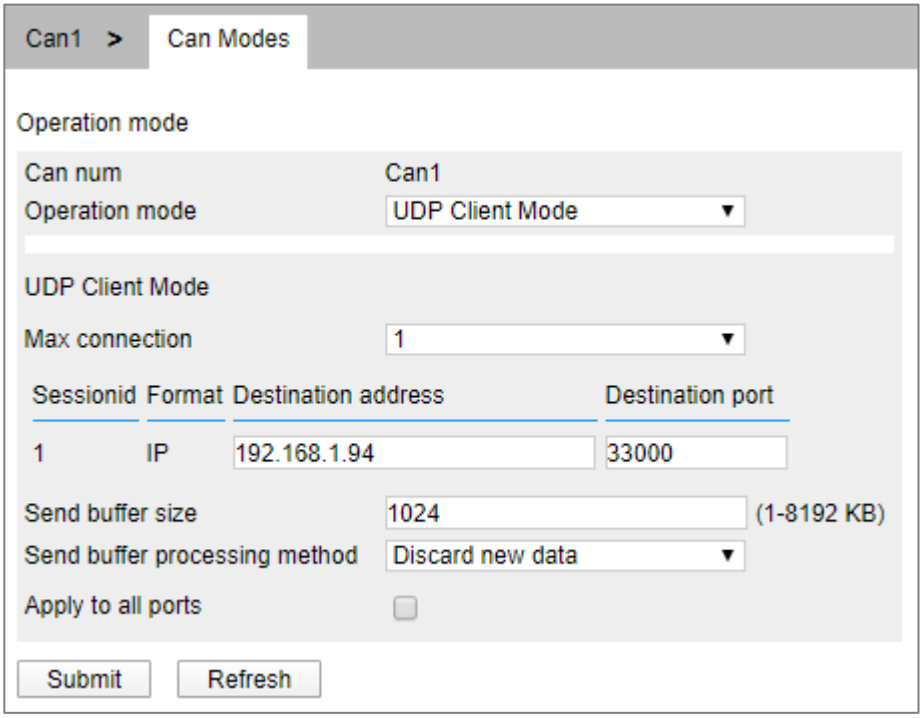
6.4 UDP Client Mode



Under CAN UDP Client Mode, the device can be a client, and it can transmit data with the host user appointed under the UDP protocol. Under CAN UDP Client Mode, the device can transmit the data from CAN device to one or multiple hosts, and CAN device can also receive the data from one or multiple hosts.

Interface Description

UDP Client Mode interface is as follows:

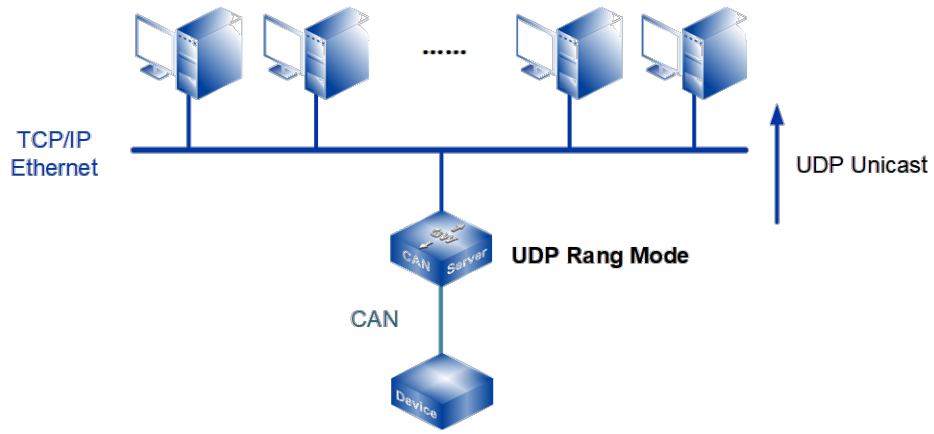


UDP Client Mode interface main element configuration instructions:

Interface Element	Description
Operation mode	**Working Mode Configuration Bar**

Interface Element	Description
CAN num	Displays the CAN number of the device currently configured.
Operation mode	The working modes of CAN port of the device are as follows: • TCP Server Mode • TCP Client Mode • UDP Server Mode • UDP Client Mode • UDP Rang Mode • UDP Multicast Mode
UDP Client Mode	**UDP Client Mode Configuration Bar**
Max connection	The maximum session number of the device's CAN port.
Format	The Server address format that CAN as the UDP client needs to connect: IP: IP address format, eg. 192.168.1.254; also support IPv6 address format, such as 2001:db8:0:f100::1.
Destination IP address	Enter the IP address of the server to which the device needs to connect.
Destination port	The listening port number of the server which the device need for session.
Send buffer size	The size of CAN port's cache for sending, value range is 1-8192KB. If the Ethernet receives too much data, CAN needs to cache the data. If the cache is too large, the real-time data will be affected.
Send buffer processing method	When sending cache data overflows, the data can be processed as follows: • Discard new data; • Discard old data.
Apply to All Ports	Apply current setting to all CAN ports.

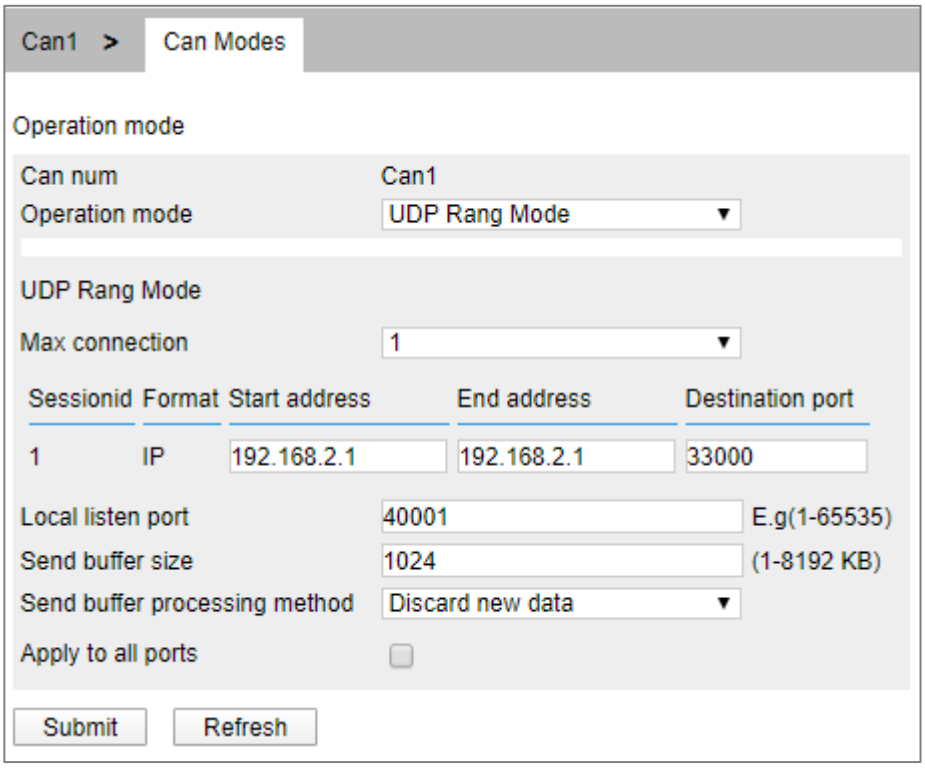
6.5 UDP Rang Mode



When the router, switch and other devices do not support multicast function, the device can realize the multicast function under the CAN UDP Rang Mode. In this mode, the device transmits data with multiple hosts in the same network segment designated by the user through UDP protocol, to achieve point to multipoint data communication. Under CAN UDP Rang Mode, CAN device can receive the data from one or multiple hosts.

Interface Description

UDP Rang Mode interface as follows:



UDP Rang Mode interface main element configuration instructions:

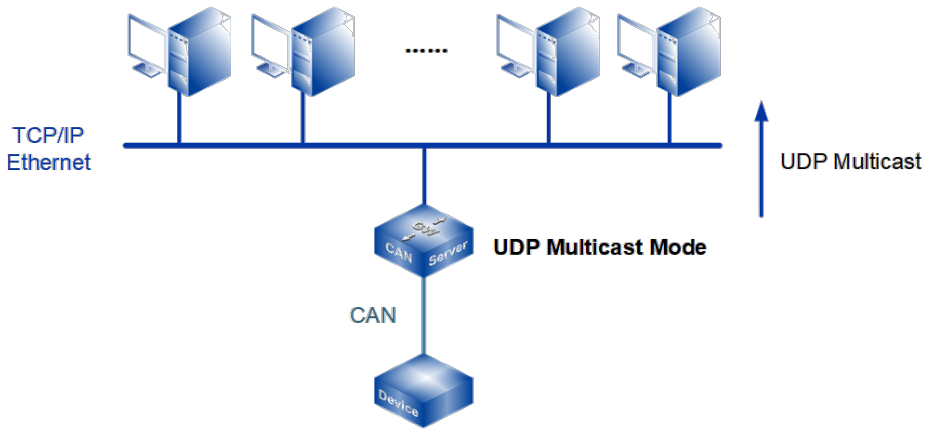
Interface Element	Description
Operation mode	**Operation Mode Configuration Bar**
CAN num	Displays the CAN number of the device currently configured.
Operation mode	The operation modes of CAN port of the device are as follows: • TCP Server Mode • TCP Client Mode • UDP Server Mode • UDP Client Mode • UDP Rang Mode • UDP Multicast Mode
UDP Rang Mode	**UDP Rang Mode Configuration Bar**
Max connection	The maximum session number supported by the device's CAN port, options include: 1/2/3/4
Format	The format of UDP Rang address.
Start Address	Start IP address of UDP Rang destination address.
End address	End IP address of UDP Rang destination address.
Destination port	The listening port number of the server that the device need for session.
Local listen port	The listening port of the device to receive UDP data Note: User must allot the only listening port to each CAN port, then the system can normally receive UDP data.
Send buffer size	The size of CAN port's cache for sending, value range is 1-8192KB. If the Ethernet receives too much data, CAN needs to cache the data. If the cache is too large, the real-time data will be affected.
Send buffer processing method	When sending cache data overflows, the data can be processed as follows: • Discard new data; • Discard old data.
Apply to All Ports	Apply current setting to all CAN ports.

Notice

- Rang address only supports IP addresses of Class B and Class C. The start address value and end address value of the Rang address need to be the same network segment. IPv6 segment address requires that the first 112-bit address prefix of the start address and the end address be same.
- The start value of Rang address must be less than or equal to the end address value.

- In order to ensure the normal operation of communication, the rang address range needs to be small as much as possible because each IP will cost 20ms.

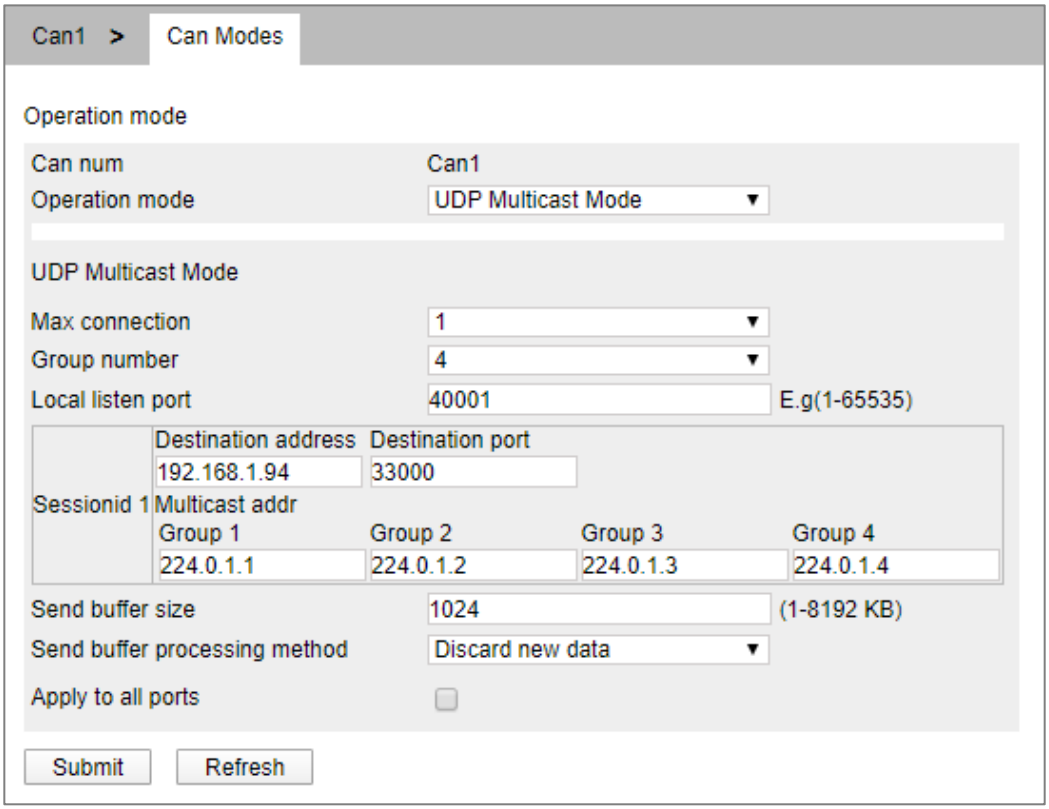
6.6 UDP Multicast Mode



Under CAN UDP multicast mode, devices can unicast or multicast the data of CAN device to one or more hosts designated by users through UDP protocol, and can also receive unicast and multicast data from one or more devices, thus realizing many-to-many communication.

Interface Description

UDP Multicast Mode interface as follows:



UDP Multicast Mode interface main element configuration instructions:

Interface Element	Description
Operation mode	**Operation Mode Configuration Bar**
CAN num	Displays the CAN number of the device currently configured.
Operation mode	The **operation** modes of CAN port of the device are as follows: • TCP Server Mode • TCP Client Mode • UDP Server Mode • UDP Client Mode • UDP Rang Mode • UDP Multicast Mode
UDP Multicast Mode	UDP Multicast Mode Configuration Bar
Max connection	The maximum session number of the device's CAN port.
Group Number	The multicast number supported by one session, it supports maximum 4 multicasts.
Local listen port	The listening port of the device to receive Multicast Note: User must allot the only listen port to each CAN port, and then the system can normally receive the multicast.
Destination address	The IP address of the opposite host that the device needs to connect.
Destination port	Enter the port number of the opposite host that the device needs to connect.
Multicast addr	Group address is used for identifying an IP multicast group, multicast address range is: 224.0.0.0 ~ 239.255.255.255. The address prefix of IPv6 multicast address is: FF02::/16 (Notice: avoid public multicast addresses when using IPv6 multicast address, such as FF02::1, FF02::2, FF02::5, FF02::9, etc.). The device can send or receive multicast data to multiple hosts.
Send buffer size	The size of CAN port's cache for sending, value range is 1-8192KB. If the Ethernet receives too much data, CAN needs to cache the data. If the cache is too large, the real-time data will be affected.
Send buffer processing method	When sending cache data overflows, the data can be processed as follows: • Discard new data;

Interface Element	Description
	• Discard old data.
Apply to All Ports	Apply current setting to all CAN ports.

7 CAN State

About this chapter

Content	Link
This Chapter	7.1 CAN Port Count 7.2 Network Connection state

7.1 CAN Port Count

Function Description

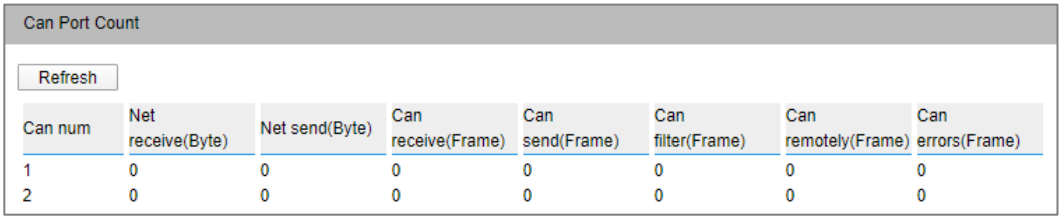
On the "CAN Port Count" page, you can view the statistics of the number of bytes received and sent during the conversion between each CAN port and the network.

Operation Path

Open in order: "CAN Status> CAN Port Count" .

Interface Description

The interface of CAN Port Count is as follows:



The main element configuration description of CAN Port Count interface:

Interface Element	Description
Can num	Display the corresponding CAN port number of the device.
Network receive (Bytes)	Number of bytes received by the device network interface.
Network transmit (Bytes)	Number of bytes sent by the device network interface.
Can receive (Frame)	The number of data frames received by the device CAN port.

Interface Element	Description
Can send (Frame)	The number of data frames transmitted by the device CAN port.
Can filter (Frame)	The number of data frames filtered by the device's CAN port.
Can remotely (Frame)	The number of remotely frames transmitted by the device's CAN port.
Can errors (Frame)	The number of error frames transmitted by the device's CAN port.

7.2 Network Connection state

Function Description

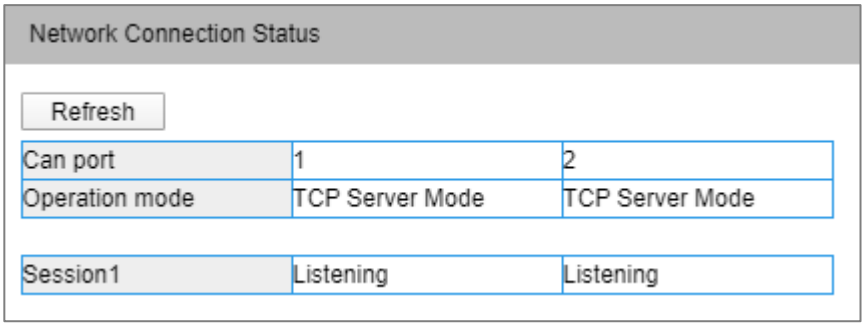
On the "Network Connection Status" page, you can view the working mode and network session connection status of each CAN port of the device.

Operation Path

Open in order: "CAN Status > Network Connection Status".

Interface Description

The network connection status interface is as follows:



The main elements configuration descriptions of the network connection status interface:

Interface Element	Description
CAN num	Display CAN port number corresponding to device.
Operation mode	The operation mode of current CAN port are as follows: • TCP Server Mode • TCP Client Mode • UDP Server Mode • UDP Client Mode

Interface Element	Description
	• UDP Rang Mode • UDP Multicast Mode
Session (1-3)	The current connection state of network connection of the CAN port can be displayed as follows: • Connected • Connecting • Listening • (None): the session is not enabled or UDP is not connected

8 System Status

About this chapter

Content	Link
This Chapter	8.1 Routing Table 8.2 System Network Status 8.3 System Log

8.1 Routing Table

Function Description

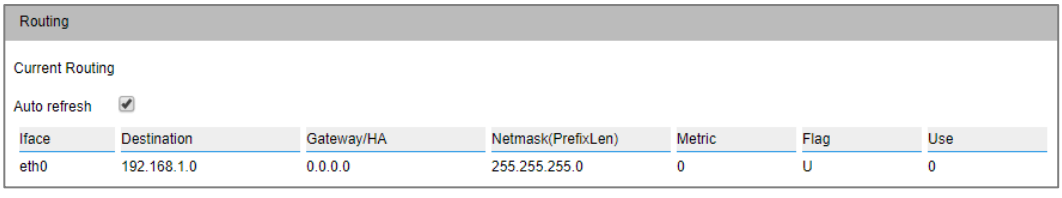
In “Routing” page, you can see the current route information.

Operation Path

Open in order: “System Status > Routing".

Interface Description

Route Table Interface Screenshot:



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.

Interface Element	Description
Gateway/HA	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.
Flag	Display routing status, valid status is: • U：UP • 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.

8.2 System Network Status

Function Description

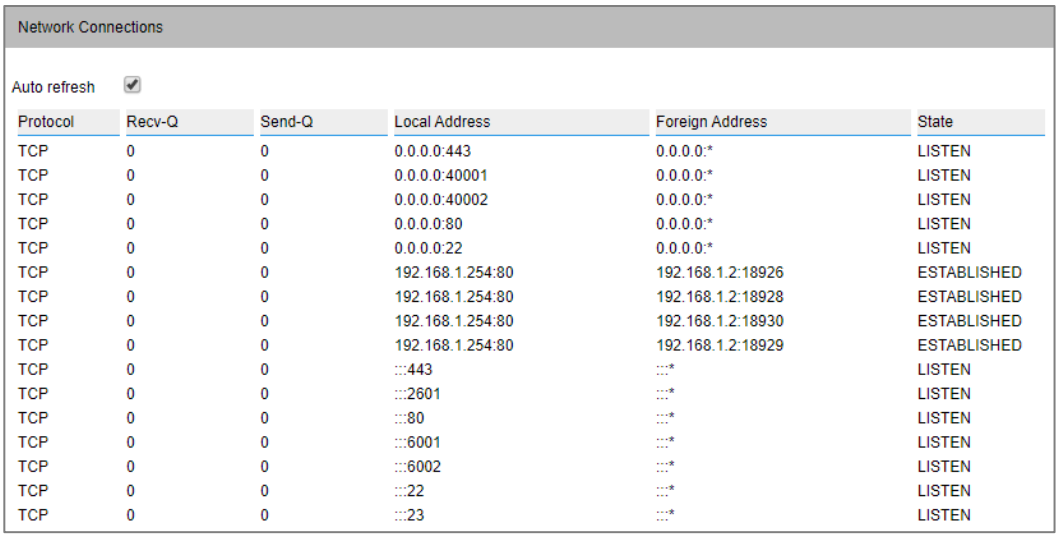
On the page of "System Network Status", user can check TCP connection informationof the device.

Operation Path

Open in order: “System Status > System Network Status”.

Interface Description

The system network status interface is as follows:



The main element configuration description of system network status interface:

Interface Element	Description
Protocol	Network protocol type.
Recv-Q	Number of network receiving queues.
Send-Q	Number of network sending queues.
Local 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. • SYN_SENT: sending connection request. • SYN_RECV: the server should send an ACK to acknowledge the client's SYN and send a SYN of its own to the client. • ESTABLISHEN: represents an open connection, in which two parties can or have data interaction. • FIN_WAIT1: sending FIN actively to request to close connection state. • CLOSE_WAIT: when the passive close terminal receives FIN, it will send ACK to answer FIN request and enter CLOSE_WAIT state. • FIN_WAIT2: when the active close terminal receives ACK, it will enter FIN_WAIT2status. • LAST_ACK: After some time the passive close terminal receives end-of-file character, it will call CLOSE to close connection. Thus it’s TCP also sends a FIN and waits the opposite ACK. It enters LAST-ACK status. • TIME_WAIT: when the active close terminal receives FIN, it will send ACK and enter CLOSE_WAIT state. • CLOSING: wait the remote terminal to confirm the connection interruption. • CLOSED: when the passive close terminal receives ACK package, it will enter CLOSED status. • UNKNOWN: unknown Socket status.

8.3 System Log

Function Description

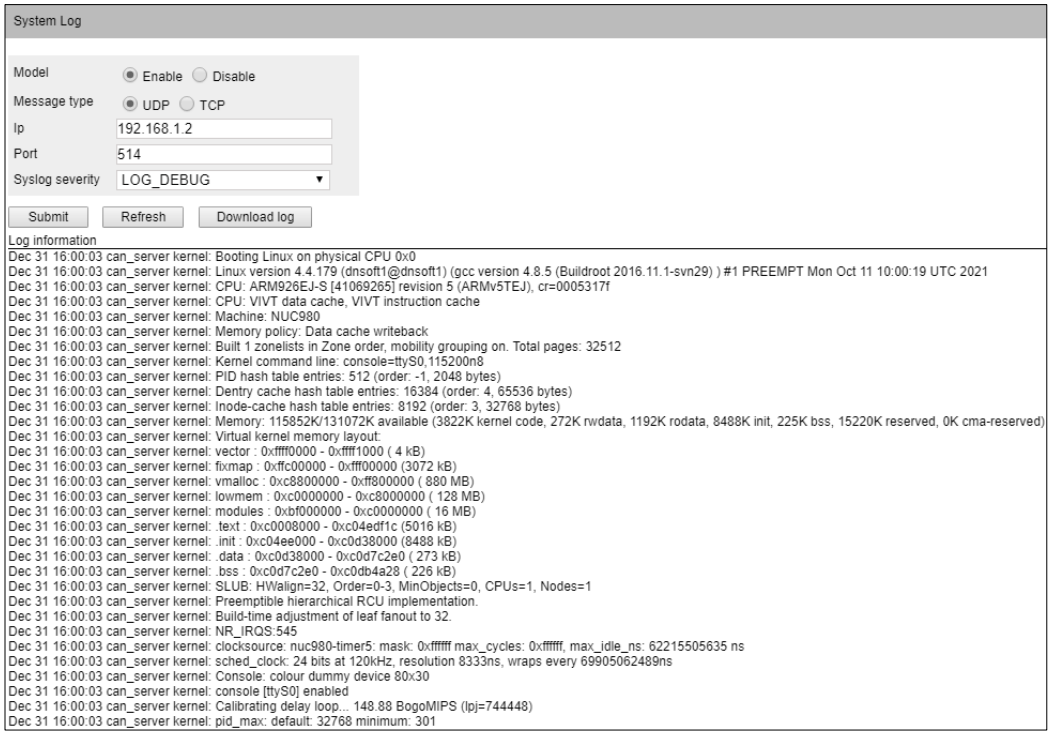
On the "System log" page, you can view the log information of the device and upload the log information to the syslog server. During the operation of the device, the system will record all kinds of situations in operation, thus forming log information. The log information is mainly used to check the 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:



The main elements configuration description of system log interface:

Interface Element	Description
Mode	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.

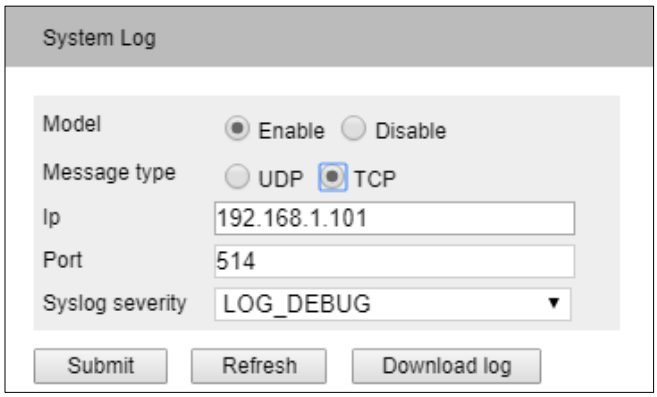
Interface Element	Description
Message Type	System log information transmission protocol, which can be selected as follows: • TCP: system log information is sent to the log server by TCP protocol. TCP (transmission control protocol), connection-oriented and reliable transmission-layer communication protocol; • 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.
Download log	Click the "Download Log" button to export the current log file “messages” locally.

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:



1 Check “Enable” in the “Model” checkbox;

2 Check “TCP“ protocol in “Message Type” checkbox;

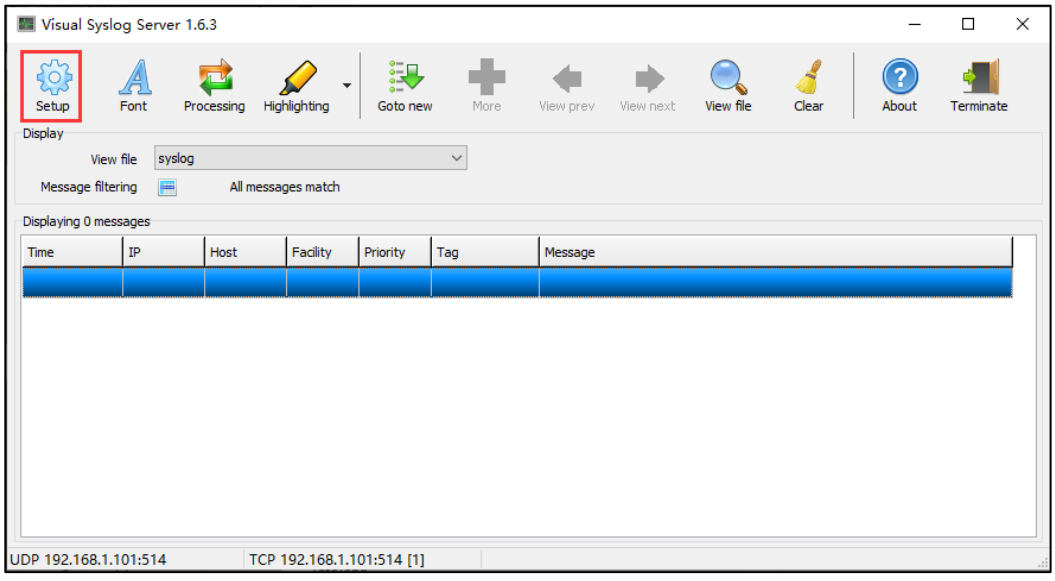
3 In the IP text box, enter the IP address "192.168.1.101" of the server.

4 In the "Port" text box, enter the port number of the server, and the default port of syslog protocol is 514;

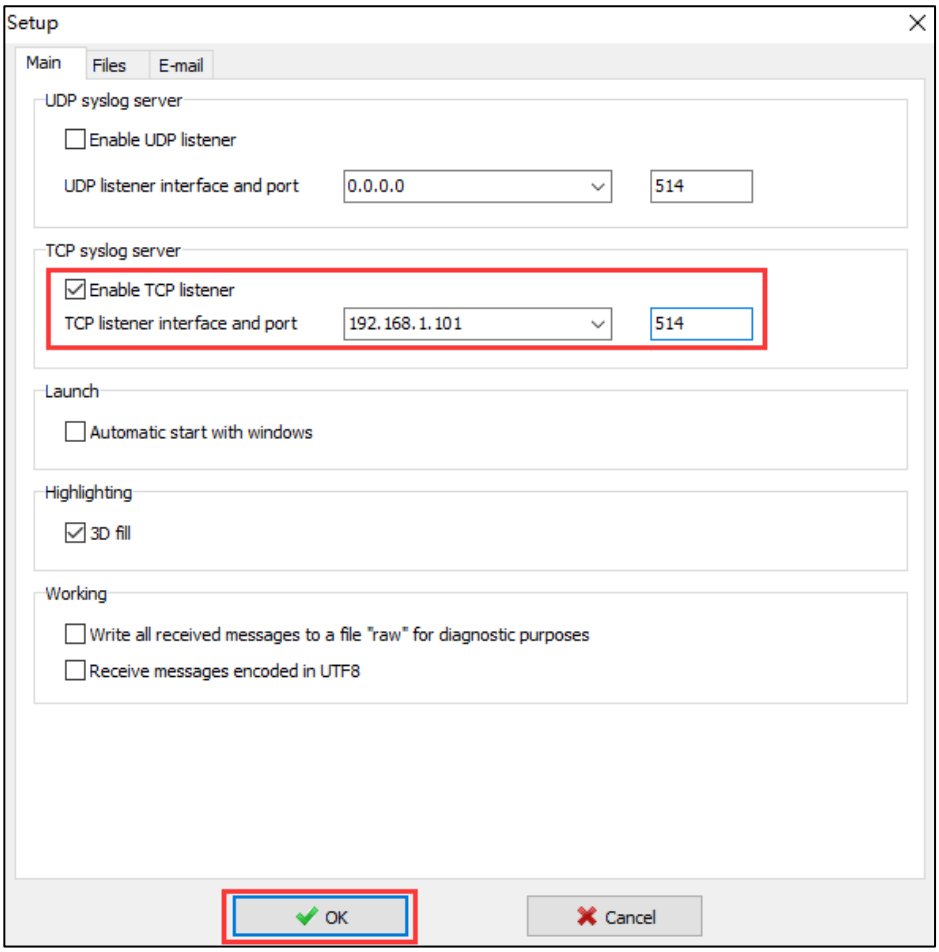
5 In the “Syslog severity” drop-down list, select “LOG_INFO”;

6 Click “Submit” button.

Step 3 Run "Visual Sys log Server" on the host to complete the configuration of relevant parameters, as shown below.



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

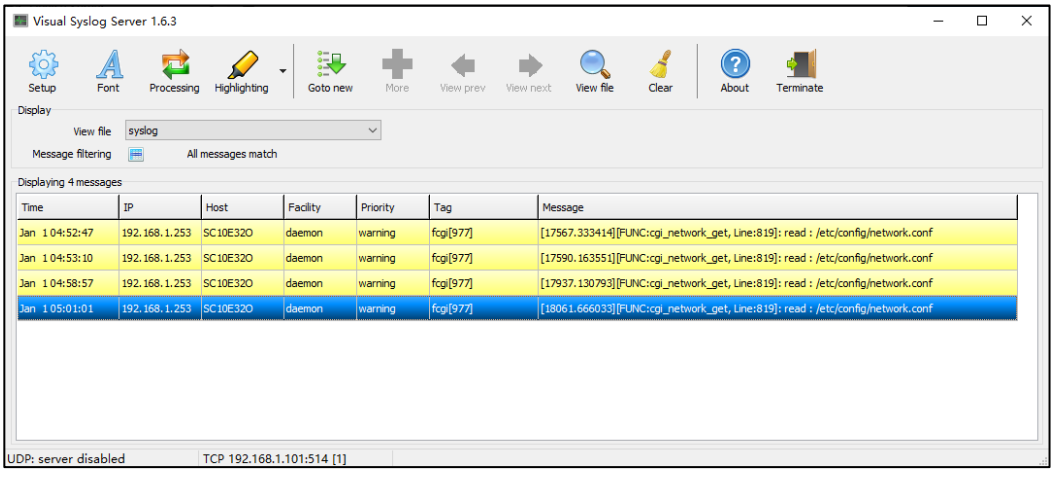


2 On the "Setup" page, in the Main configuration area, check "Enable TCP Listener", as shown in the above figure;

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.



Step 5 End.

9 System Management

About this chapter

Content	Link
This Chapter	9.1 Device Information Configuration 9.2 Time Settings 9.3 Remote Management 9.4 User Configuration 9.5 IP Address Filtering 9.6 Mac Address Filtering 9.7 Static Routing Configuration 9.8 Free ARP 9.9 Diagnostic Test 9.10 System Maintenance

9.1 Device Information Configuration

Function Description

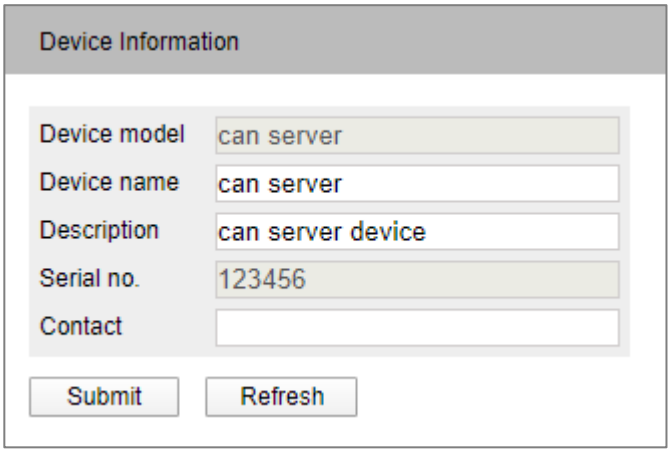
In the “Device Information Configuration” page, you can configure the device name, device description, and maintenance contact information.

Operation Path

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

Interface Description

The screenshot of device information configuration interface:



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.
Serial no.	Device CAN port 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.

9.2 Time Settings

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:

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 automatically synchronize NTP server time.

9.3 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 the security protocol based on the application layer and transport layer. Telnet is transmitted in plaintext, while SSH is transmitted in ciphertext, which is more secure. SSH is a currently reliable protocol that provides security protocol for remote login sessions and other web 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

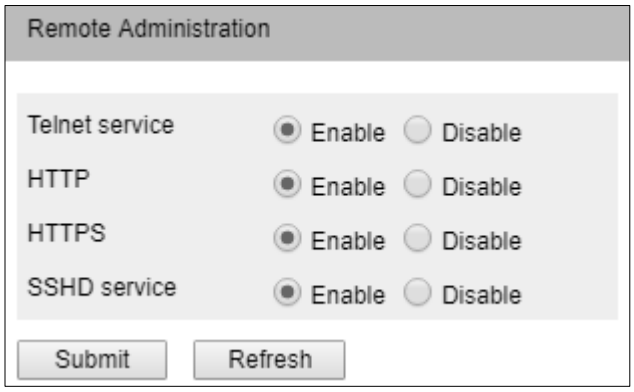
On the "Remote Administration" page, access methods such as TELNET, HTTP, HTTPS and SSHD can be restricted.

Operation Path

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

Interface Description

The Remote management interface is as follows:



The main elements configuration description of Remote management interface:

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

9.4 User Configuration

Function Description

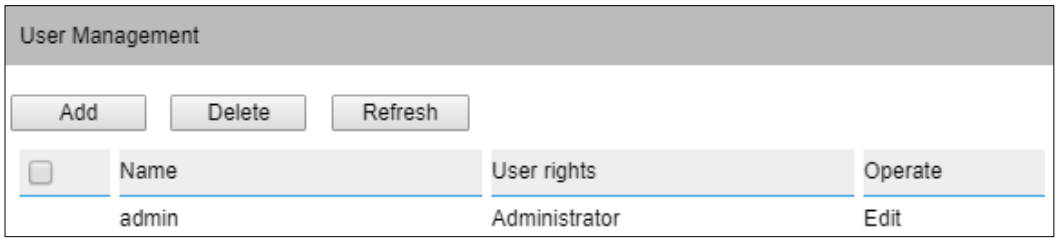
In the "user configuration" page, users can add and delete users freely. Users need to access the device by login with user name and password. The initial user name and password are both: admin.

Operation Path

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

Interface Description

The User Configuration interface is as follows:



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.

9.5 IP Address Filtering

Function Description

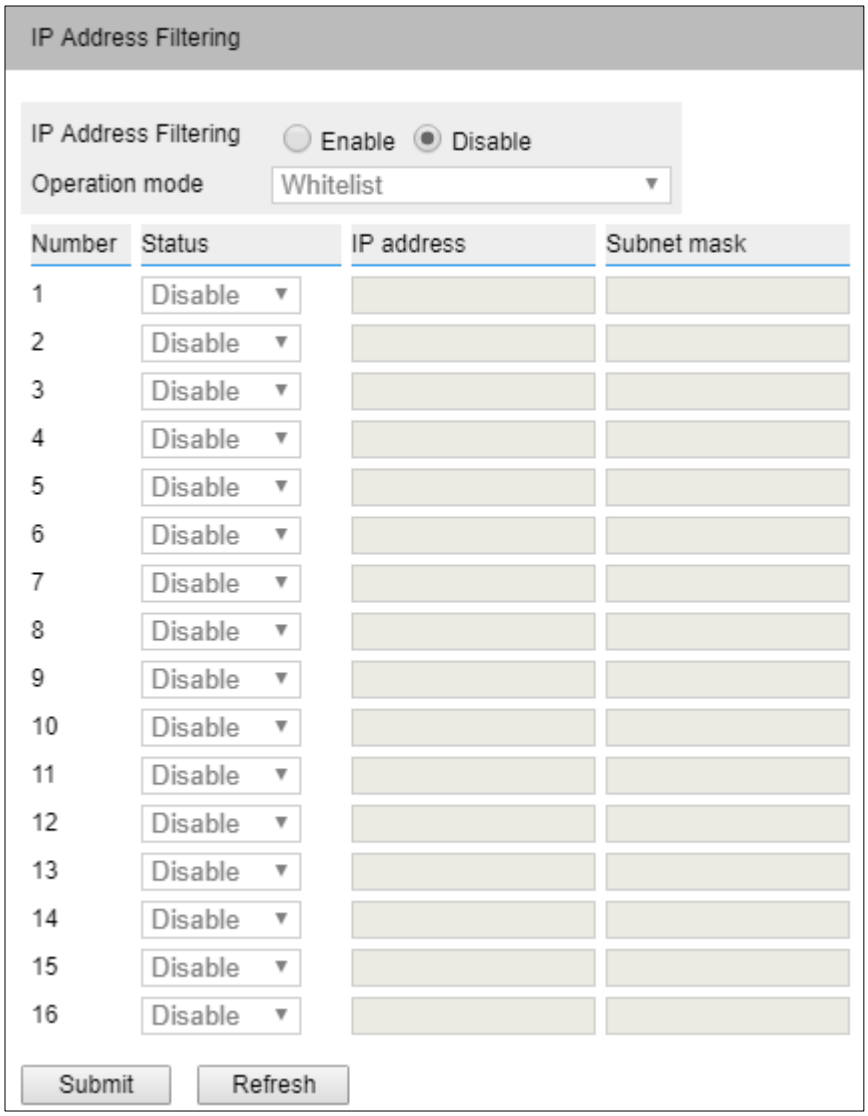
Users can limit the ongoing access or connected host IP address and subnet mask via setting access rules on the "IP Filter" page.

Operation Path

Open in order: “System Management> IP Address Filtering”.

Interface Description

IP Filter interface as follows:



Main elements configuration instructions in IP Address Filtering interface:

Interface Element	Description
IP Address Filtering	Enable or disable IP filtering rules. • 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.

Interface Element	Description
	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 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"; IPv6 is supported at the same time
Subnet mask	Set the subnet mask in dotted decimal format in the filter rule, such as "255.255.255.0". For IPv6, the address prefix length of IPv6 can be set.

9.6 Mac Address Filtering

Function Description

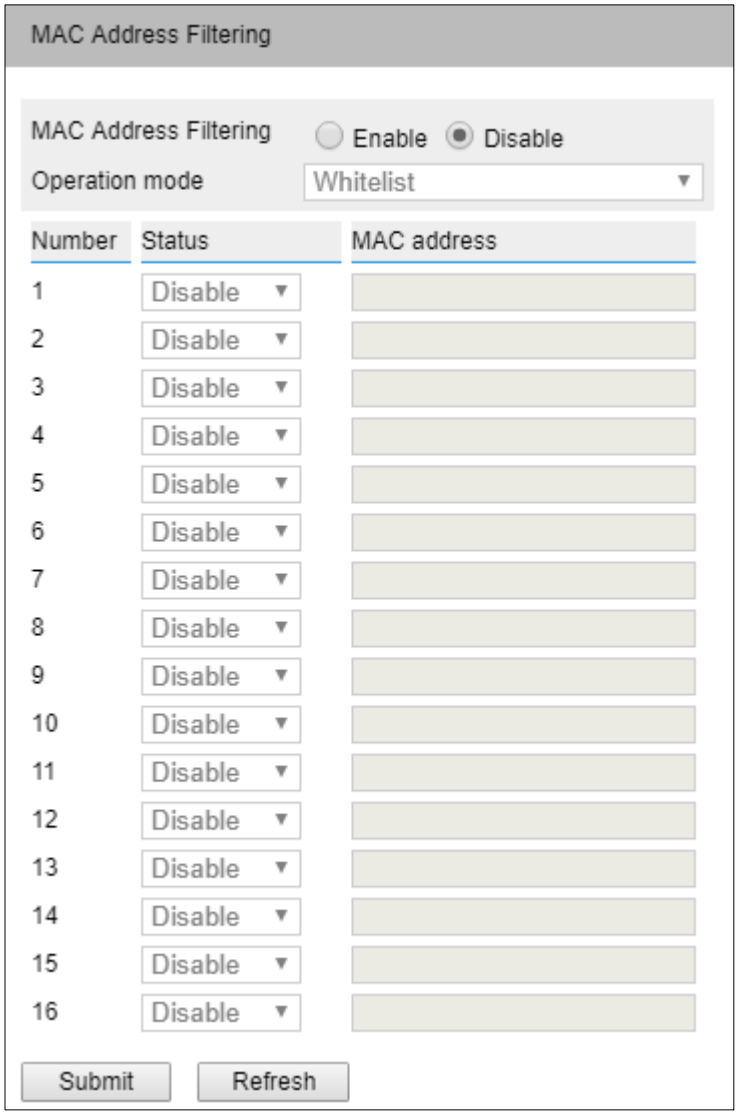
On the "MAC Filter" page, user can restrict the host MAC address to access or connect by setting access rules.

Operation Path

Open in order: “System Management > MAC Address Filtering”.

Interface Description

MAC filter interface shown as follows:



The main elements configuration description of MAC Filter interface:

Interface Element	Description
Mac Address Filtering	Enables or disables MAC address filtering rules. • 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 the MAC address filtering rule number.
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".

9.7 Static Routing Configuration

Function Description

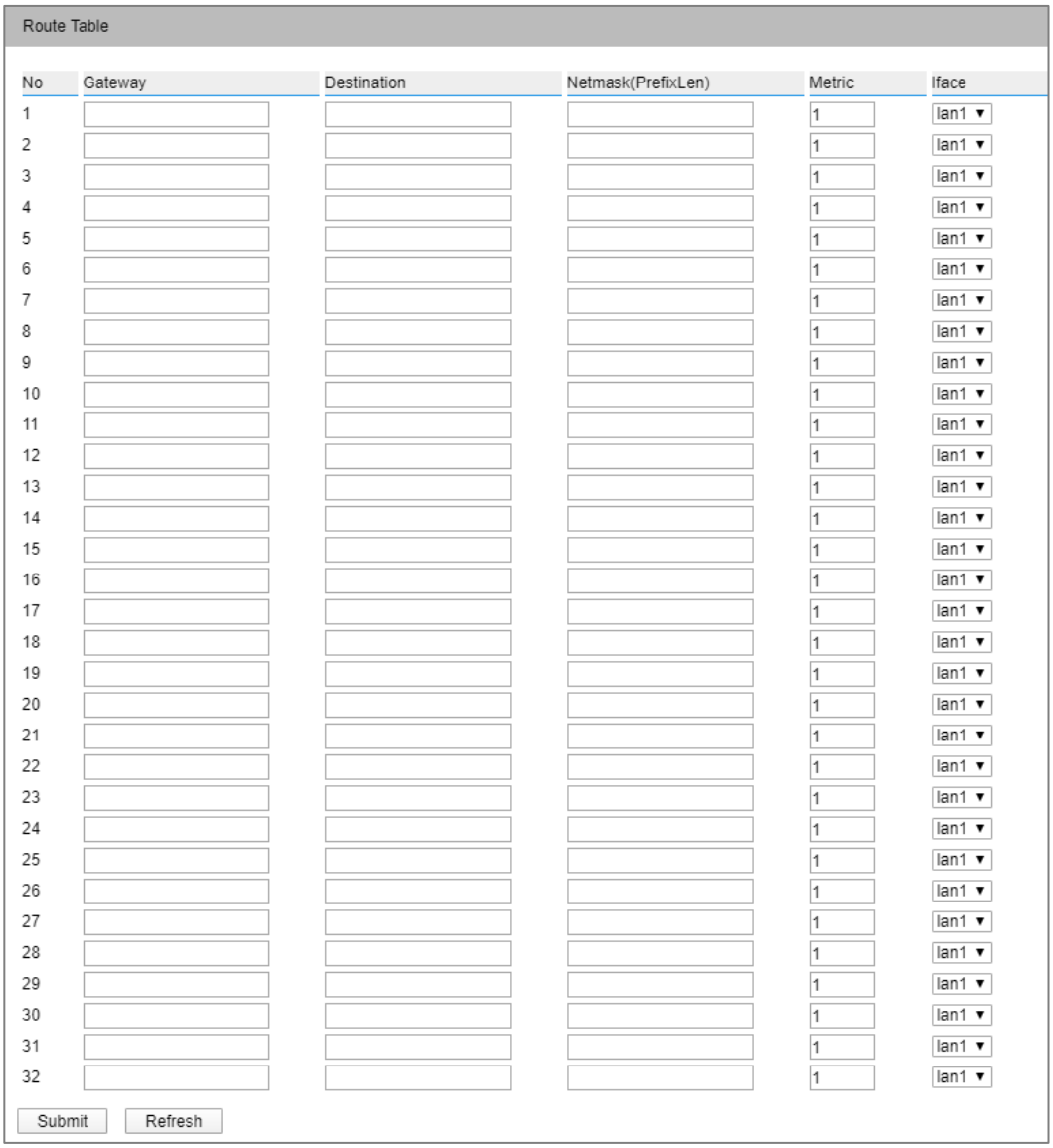
In “Static Routing Configuration“ page, you can configure how to connect device with external network. In the dual IP mode, the data egress interface can be specified via static routing configuration when device is communicating across network segment. Device supports up to 32 routing entries, every 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:



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(PrefixLen)	The prefix length of IPv4 subnet mask or IPv6 network of the 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:

Interface Element	Description
	• lan1

9.8 Free ARP

Function Description

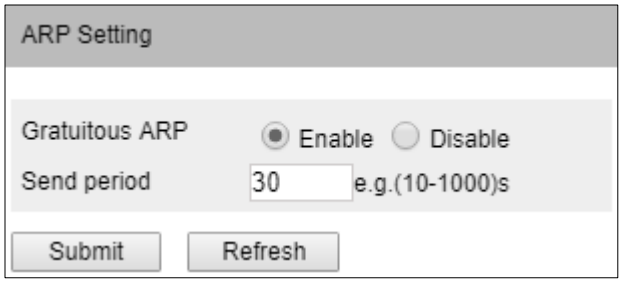
In “Free ARP” page, you can enable free ARP function and set parameter of sending period. Free ARP function can avoid the failure of communication due to device MAC address being aged by switch or router.

Operation Path

Open in order: “System Management > Free ARP”.

Interface Description

Free ARP interface is as below:



Main elements configuration descriptions of free ARP interface:

Interface Element	Description
Gratuitous ARP	Free ARP function status, options as follows: • Enable • Disable
Send period	The interval time of sending Gratuitous ARP network packet, 10 in default, for example:10-1000s.

9.9 Diagnostic Test

9.9.1 Ping

Function Description

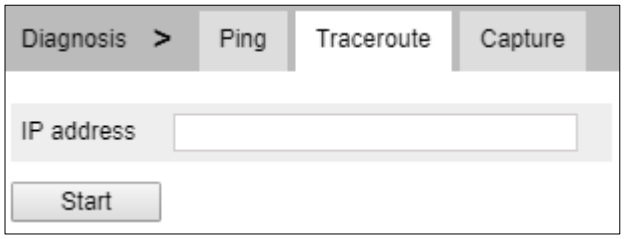
On the "Ping" page, users can use the Ping command to check the network connection or the network connection speed. Ping utilizes the uniqueness of network machine IP address to send a data packet to the target IP address, and then ask the other side to return a similarly sized packet to determine whether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

Operation Path

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

Interface Description

The interface of Ping is as follows:



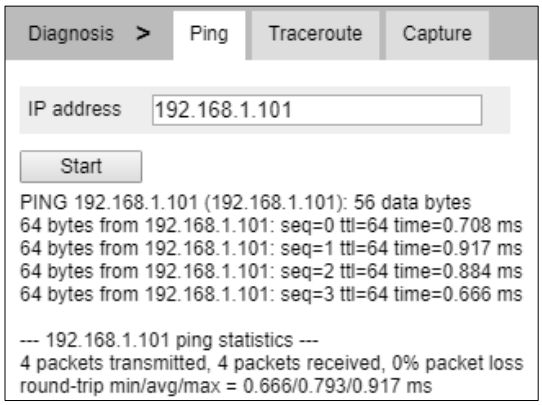
The main elements configuration description of Ping configuration interface:

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.

9.9.2 Traceroute

Function Description

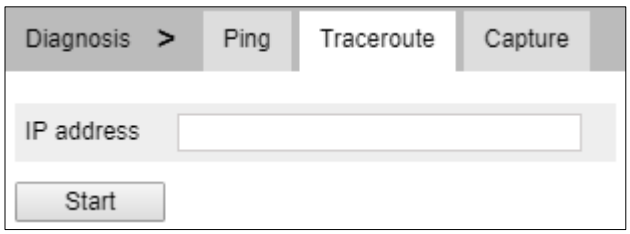
On the "Traceroute" page, users can test the network conditions between the device and the target host. Traceroute measures how long it takes by sending small packets to the destination device until they return. Each device on a path Traceroute returns three test results. Output result includes each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



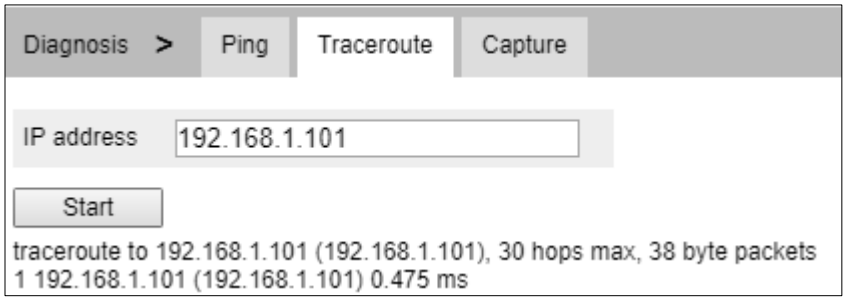
The main element configuration description of Traceroute interfaces:

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:

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

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



Note:

The above figure shows the time from the device to IP address 192.168.1.101, which takes 0.475ms after one hop.

Step 3 End.

9.9.3 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:

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.
Ends.	Click the "End" button, the device stops capturing network packets, and saves the network packets captured during this period to the local client in ".pcap" format. Note: Users can use Wireshark or other third-party software to open the captured packets.

9.10 System Maintenance

9.10.1 Configuration File

Function Description

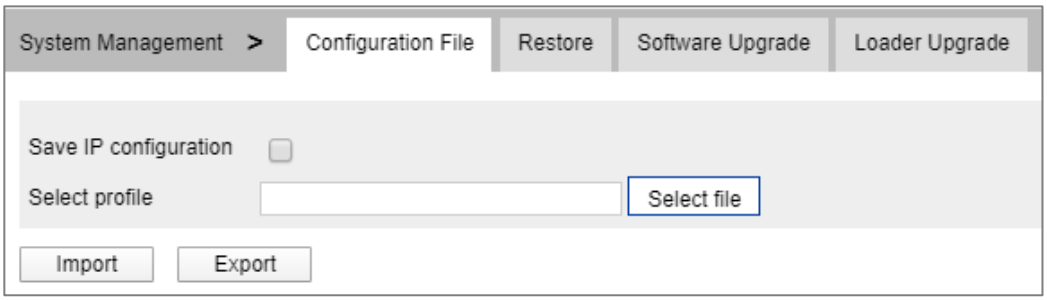
On the "Management File" page, user can download and upload configuration file.

Operation Path

Open in order: “System Management > System Maintenance > Configuration File”.

Interface Description

Configuration file interface is as follows:



The main elements configuration description of configure file interface:

Interface Element	Description
Save IP configuration	When checked, the device can keep the current IP address 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 ".tar", which is encrypted, so please do not decompress or modify it.
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 open.

- 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.

9.10.2 Restore Factory 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:

The main element configuration description of restore factory settings interface:

Interface Element	Description
Save IP configuration	When checked, the device can keep the current IP address after restoring the factory settings.
Restore	Click this button, 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 of the device is the static IP address "192.168.1.253", and the user name and password default to "admin".

9.10.3 Upgrade

Function Description

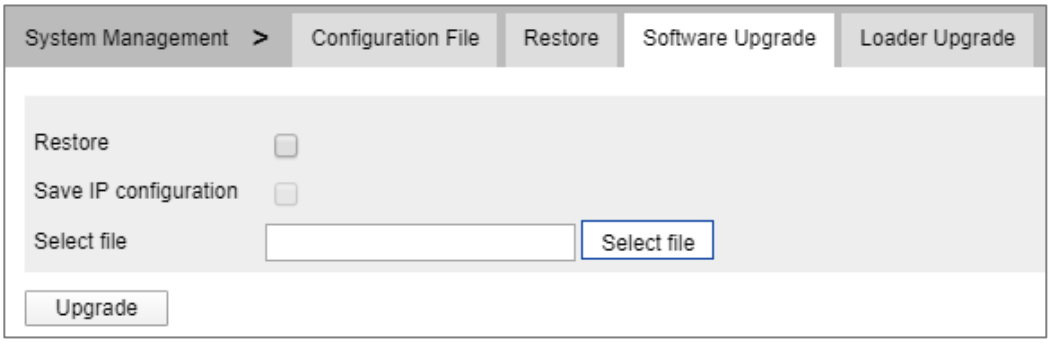
On the Software Upgrade page, you can update and upgrade the device program.

Operation Path

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

Interface Description

The software update interface as follows:



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 configuration	After the software upgrade is checked to restore the factory 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.

9.10.4 Loader Upgrade

Function Description

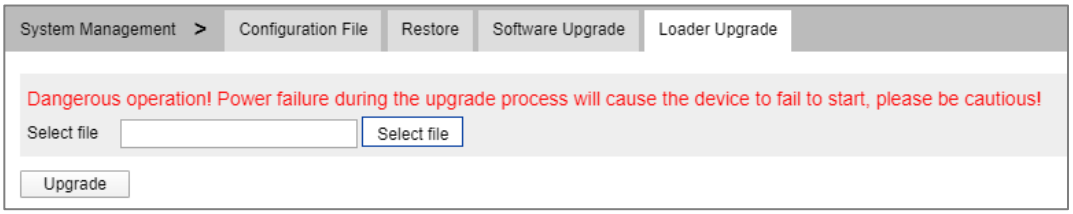
On the Loader Upgrade page, you can update Boot Loader.

Operation Path

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

Interface Description

The Loader update interface as follows:



The main elements configuration description of Loader update interface:

Interface Element	Description
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.

10 CAN Mode Setting Example

About this chapter

Content	Link
This Chapter	10.1 TCP Server Mode 10.2 TCP Client Mode 10.3 TCP Server Mode Configuration Bar 10.4 UDP Client Mode 10.5 UDP Rang Mode 10.6 UDP Multicast Mode

Note

Interface elements, operation paths and some functions involved in the CAN server and test software in the configuration example shall be subject to the actually acquired device and software. Because the software version is not updated or upgraded regularly, the configuration examples are for reference only.

10.1 TCP Server Mode

Background introduction

Under "TCP Server Mode", it's assumed that CAN server port "CAN1" passively waits for the connection of one host PC, meanwhile the host can read or send the Ethernet data to a CAN port device.

CAN server (TCP server mode) parameter information as follow:

- IP address: 192.168.1.254
- Work port: 32000
- Baud rate: 1000K

The parameters of the host PC (TCP client) are as follows:

- IP address: 192.168.1.2

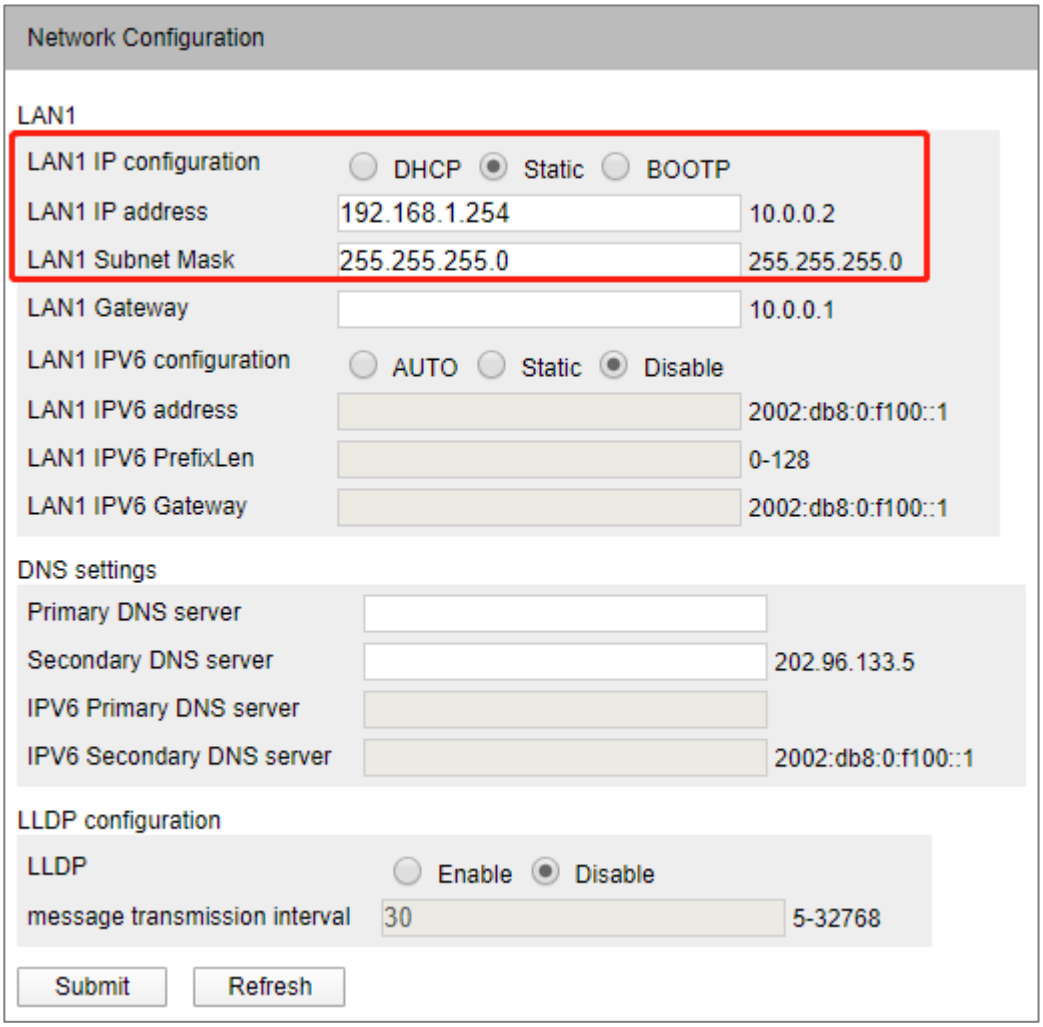
Configuration steps

Step 1 Configure CAN server IP address.

1 Login in the Web configuration interface, choose "Network Configuration".

2 In the "LAN1" area, select "LAN1 Configuration" as "Static", and enter the corresponding network address information such as " LAN1 IP Address", "LAN1 Subnet Mask" and "LAN1 Gateway".

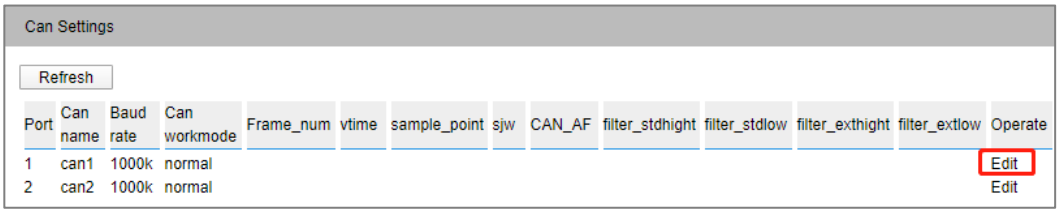
3 Other parameters remain the default, click "Submit".



Step 2 Configure the CAN port parameter information.

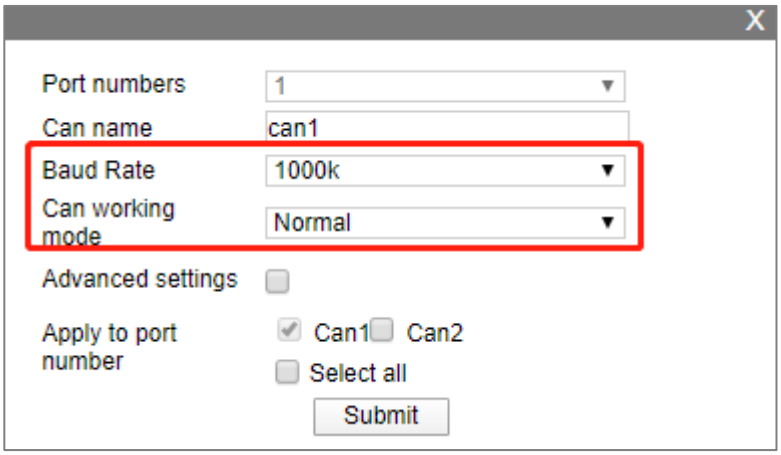
1 Log in to the Web configuration interface and select "CAN Settings".

2 In the CAN1 entry, click the "Edit" button under the operation, as shown in the following figure.



3 In the “Edit” window, set “Baud Rate” and “CAN working mode” respectively, as shown

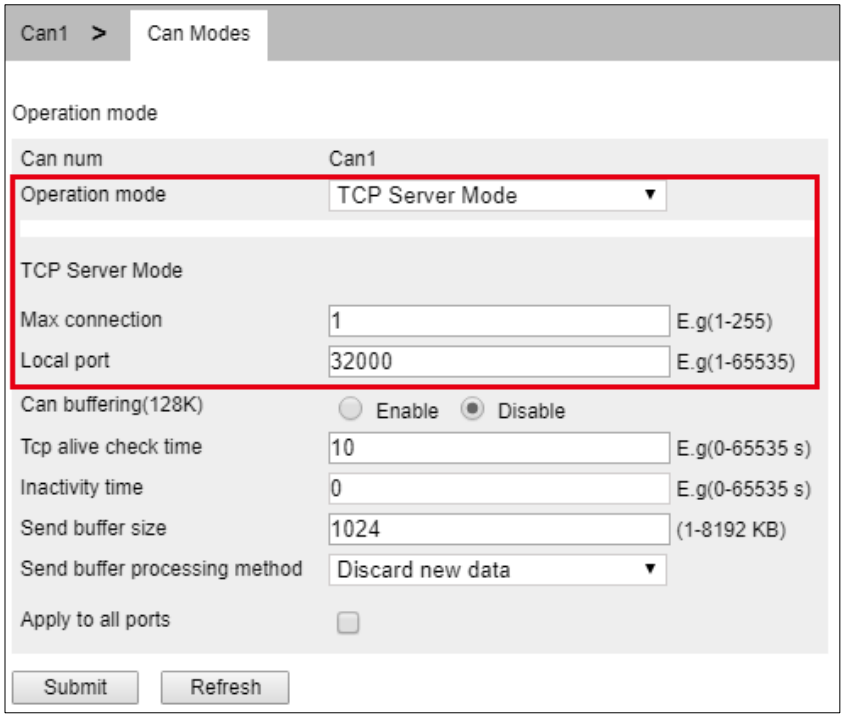
in the following figure.



4 Other parameters remain the default, click "Submit".

Step 3 Configure the work mode of CAN server.

1 Log in to the WEB configuration interface and select "CAN mode > CAN1".



2 Click the "Operation mode" drop-down list box and select "TCP Server Mode".

3 Enter 1 in "Max connection" text box.

4 Enter "32000" on "Local port" text box.

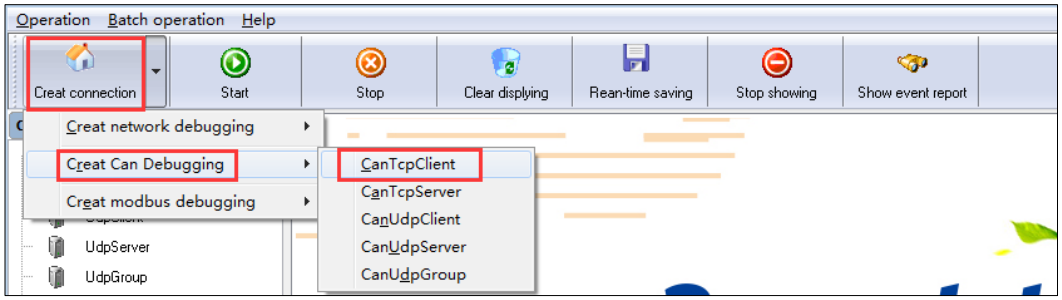
5 Other parameters remain the default, click "Submit".

Step 4 Run the debug assistant software to create a TCP client for the host.

1 Install and run "Debugging Assistant" software.

2 Click "Create Connection" drop-down list box, choose "Create Can Debugging >

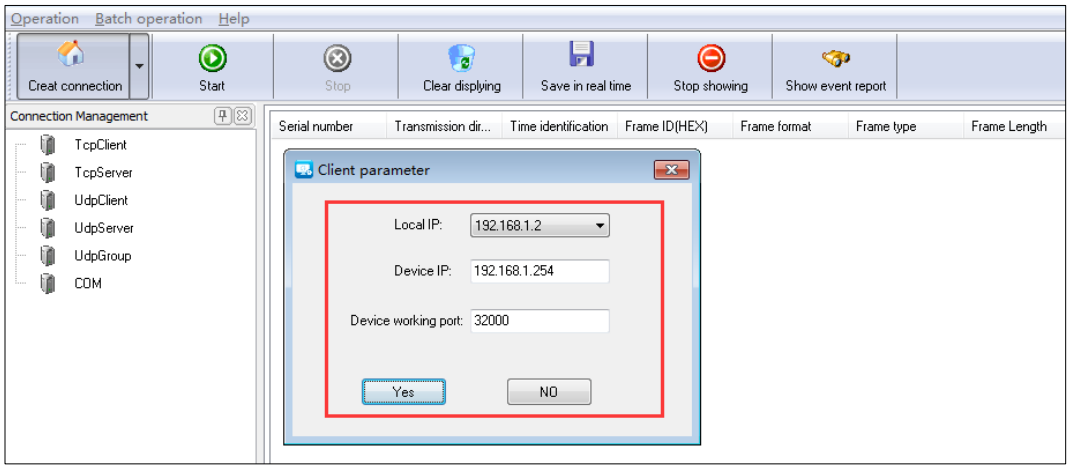
CanTcpClient".



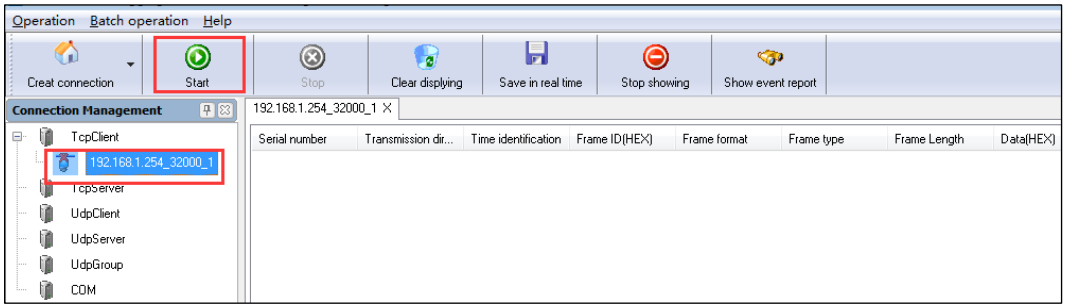
3 On the pop-up "Local IP" drop-down list box, choose the IP address of host PC (TCP client) "192.168.1.2".

4 On the "Device IP" text box, enter the IP address of CAN server (TCP server) "192.168.1.254".

5 On the "Device Working Port" text box, enter the work port of CAN server "32000", click "Yes".



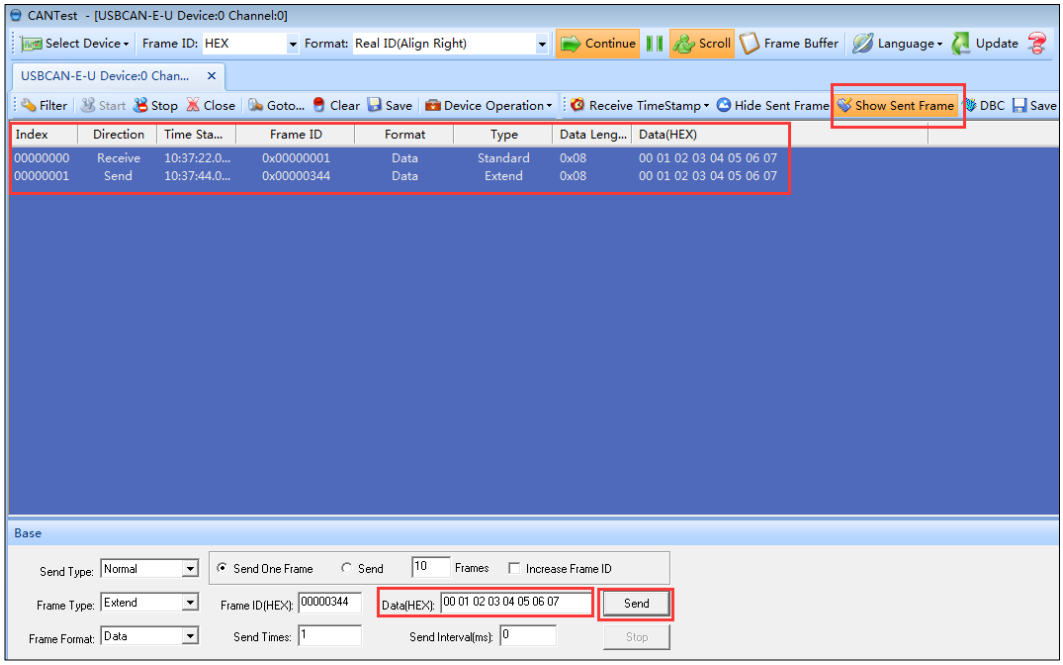
6 Choose the created UdpClient connection, click "Start".



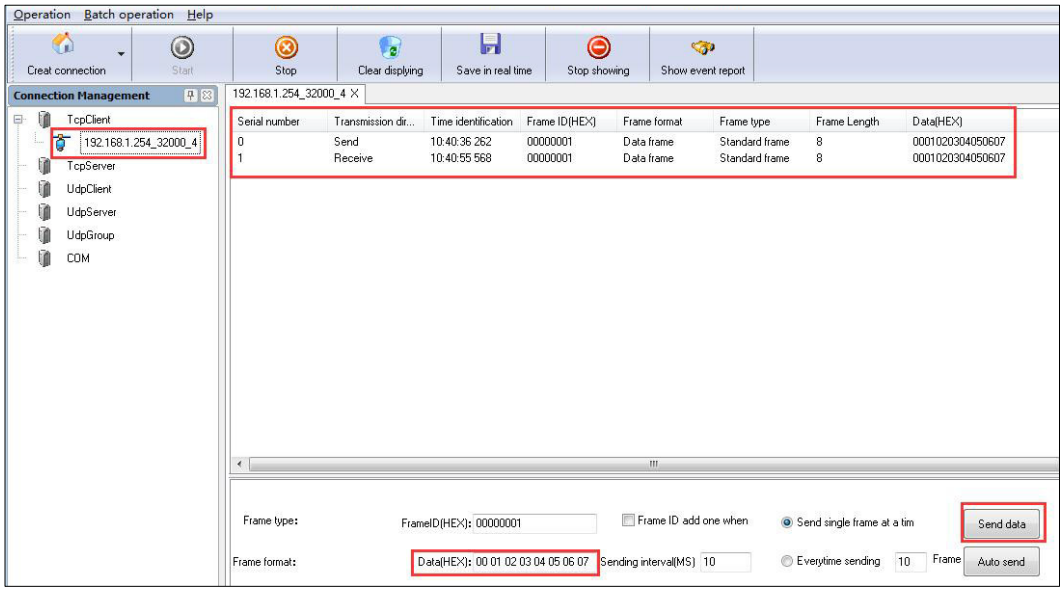
Step 5 Synchronously run "Debugging Assistant" and "CANTest" software, test the intercommunication between CAN server (TCP server) and host PC (TCP client).

1 Install and run "CANTest" software, click "Show Sent Frame" option box.

2 Frame data maintains default "00 01 02 03 04 05 06 07", click "Send".



3 Run "Debugging Assistant" software, check the CAN port information received by host PC on TcpClient option box. In a similar way, host PC can send information to CAN port device.



Step 6 End.

10.2 TCP Client Mode

Background introduction

Under "TCP Client Mode", it's assumed that CAN server port "CAN1" forwardly creates connection with one host PC, meanwhile the host can read or send the Ethernet data to a CAN port device.

CAN server (TCP client mode) parameter information as follow:

- IP address: 192.168.1.254
- Work port: 32000
- Baud rate: 1000K

The parameters of the host PC (TCP server) are as follows:

- IP address: 192.168.1.2
- Local Port:33000

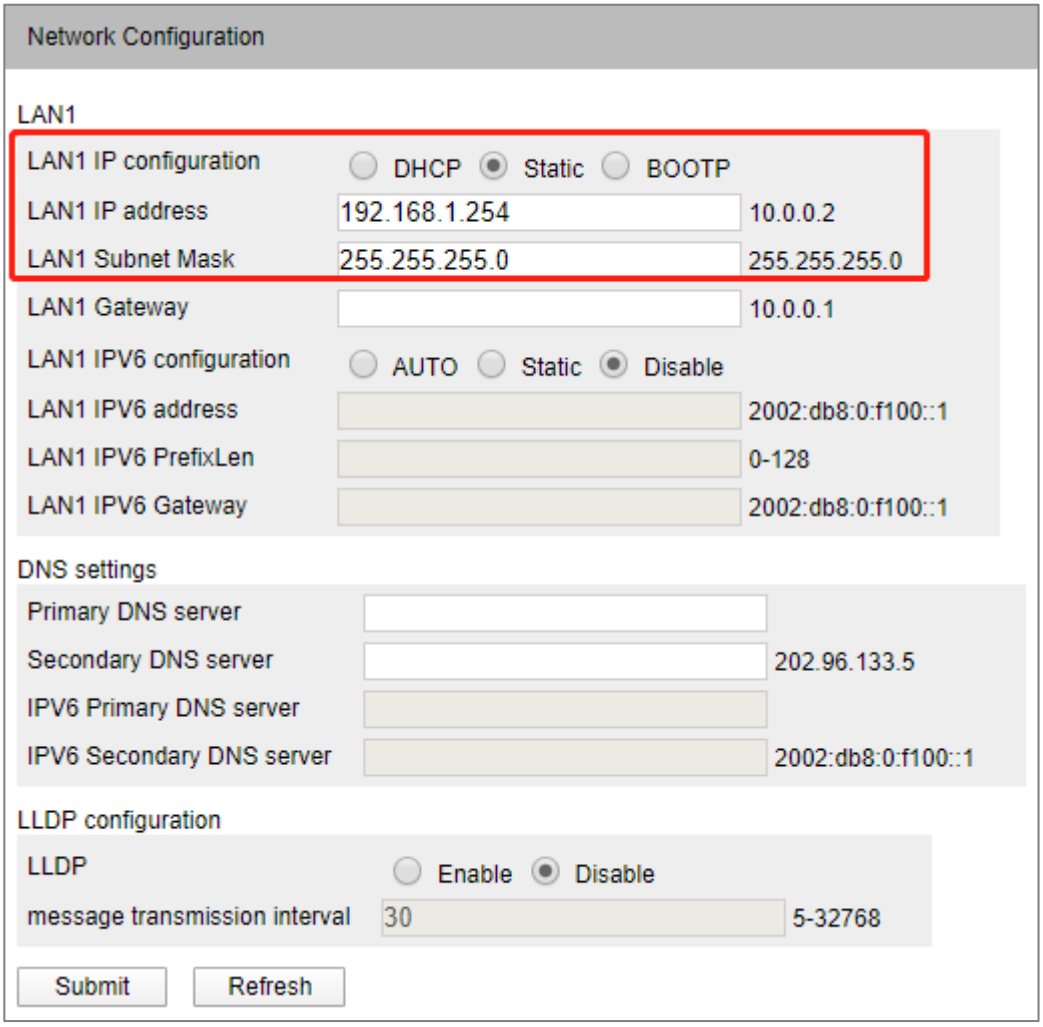
Configuration steps

Step 1 Configure CAN server IP address.

1 Login in the Web configuration interface, choose "Network Configuration".

2 In the "LAN1" area, select "LAN1 IP configuration" as "Static", and enter the corresponding network address information such as "LAN1 IP Address", "LAN1 Subnet Mask" and "LAN1 Gateway".

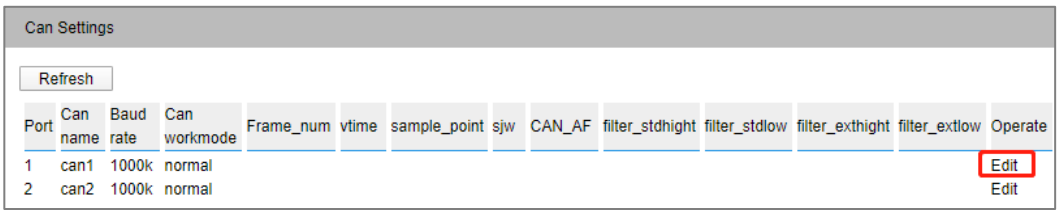
3 Other parameters remain the default, click "Submit".



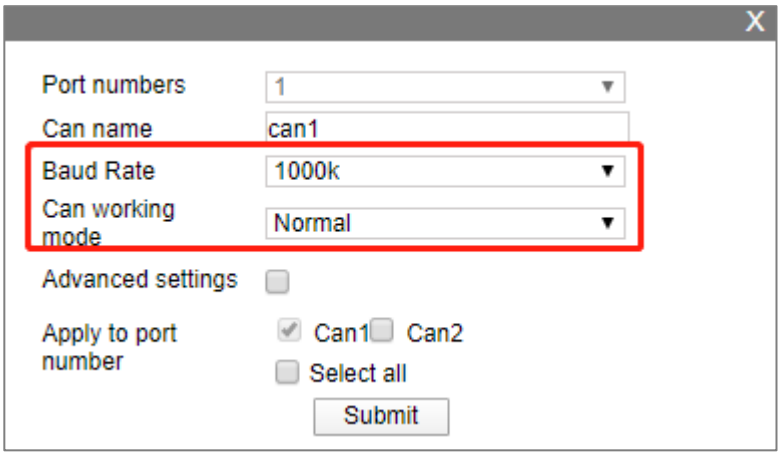
Step 2 Configure the CAN port parameter information.

1 Log in to the Web configuration interface and select "CAN Settings".

2 In the CAN port1 entry, click the "Edit" button under the operation, as shown in the following figure.



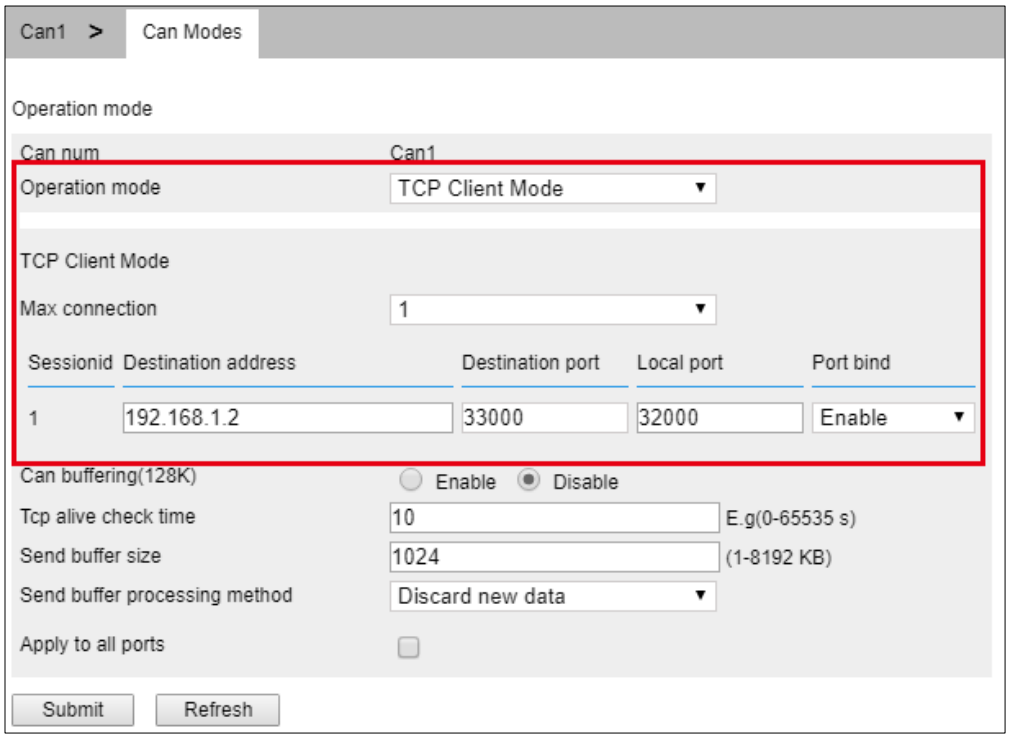
3 In the “Edit” window, set “Baud Rate” and “CAN working mode” respectively, as shown in the following figure.



4 Other parameters remain the default, click "Submit".

Step 3 Configure the work mode of CAN server.

1 Log in to the WEB configuration interface and select "CAN mode > CAN1".



2 Click the "Operation Mode" drop-down list box and select "TCP Client Mode".

3 Click "Max connection" drop-down list box, select "1".

4 Enter the host PC's IP address "192.168.1.2" in the destination address text box.

5 Enter the host PC's local port number, 33000, in the destination port text box.

6 In the “Port bind” drop-down list, select “Enable”.

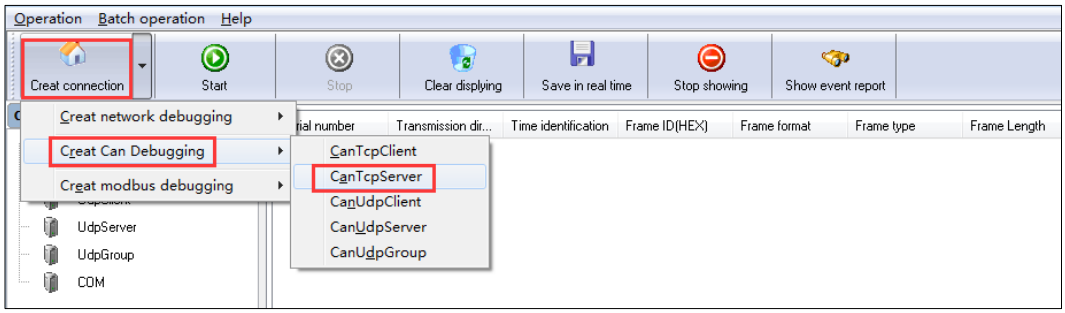
7 Enter the local port number "32000" of the CAN server in the "Local port" text box.

8 Other parameters remain the default, click "Submit".

Step 4 Run the debug assistant software to create a TCP client for the host.

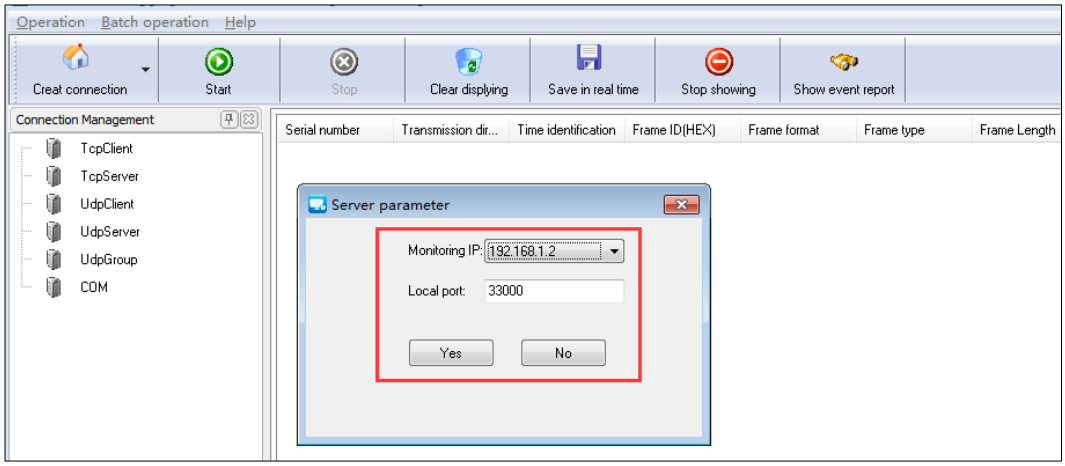
1 Install and run "Debugging Assistant" software.

2 Click "Create Connection" drop-down list box, choose "Create Can Debugging > CanTcpServer".

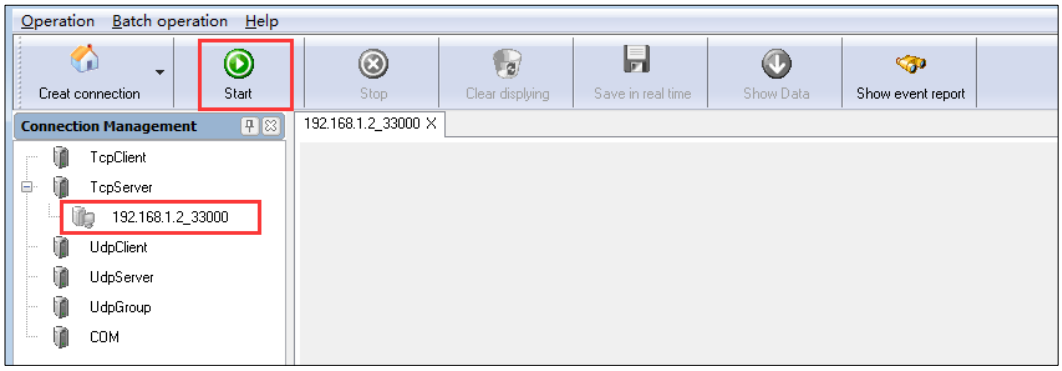


3 On the pop-up "Monitoring IP" drop-down list box, choose the IP address of host PC (TCP server) "192.168.1.2".

4 Enter the host PC (TCP server) local port "33000" on the "Local Port" text box, click "Yes".



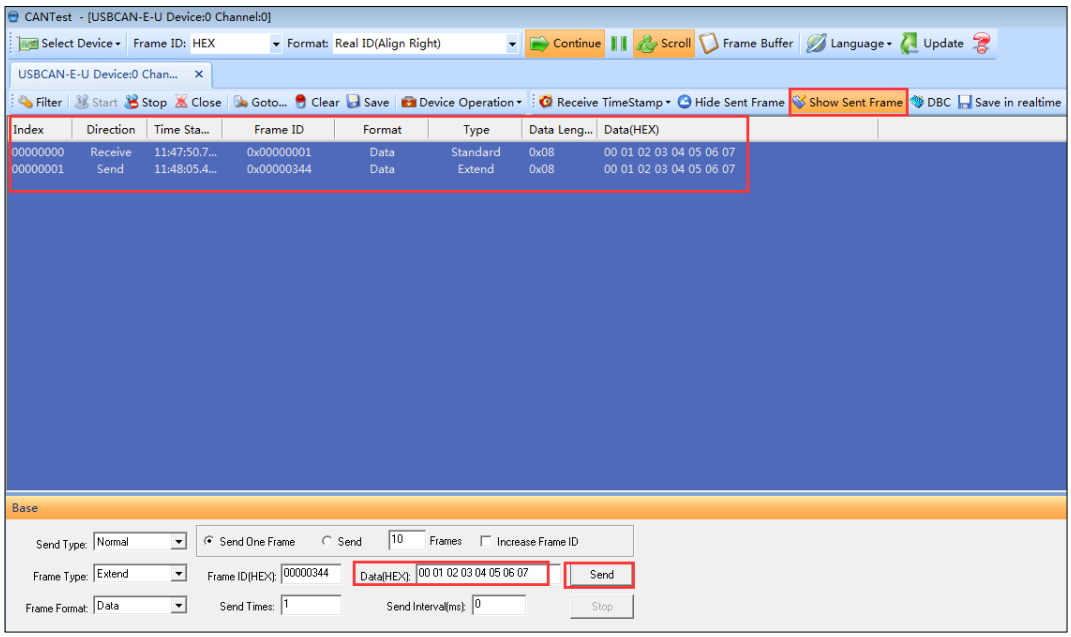
5 Choose the created UdpServer connection, click "Start".



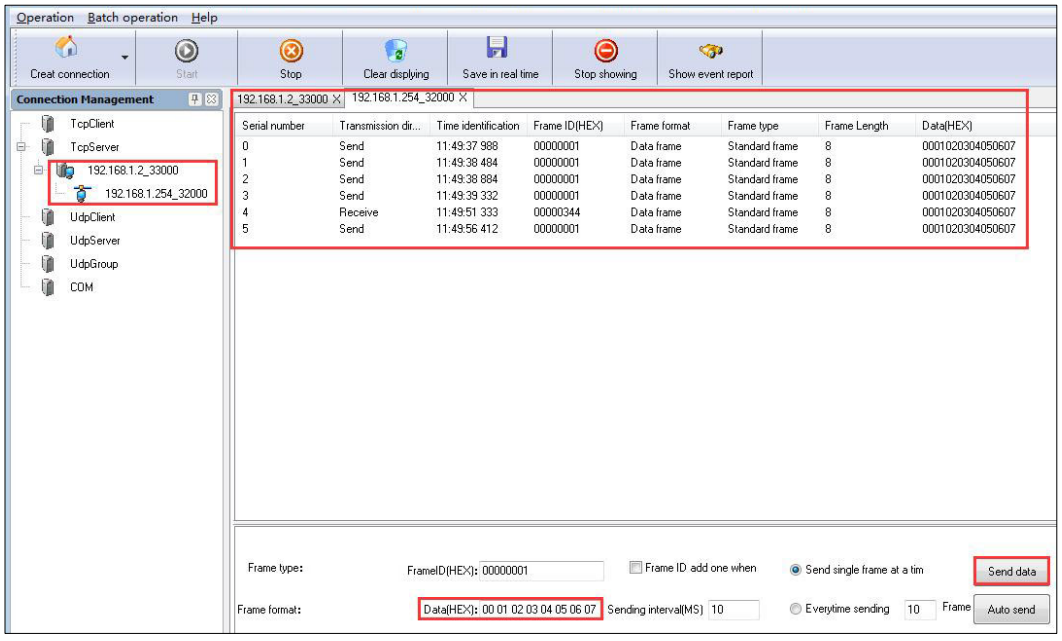
Step 5 Synchronously run "Debugging Assistant" and "CANTest" software, test the intercommunication between CAN server (TCP client) and host PC (TCP server).

1 Install and run "CANTest" software, click "Show Sent Frame" option box.

2 Frame data maintains default "00 01 02 03 04 05 06 07", click "Send".



3 Run "Debugging Assistant" software, check the CAN port information received by host PC on UDPServer option box. In a similar way, host PC can send information to CAN port device.



Step 6 End.

10.3 TCP Server Mode Configuration Bar

Background introduction

Under "UDP Server Mode", it's assumed that CAN server port "CAN1" passively waits for the connection of one host PC, meanwhile the host can read or send the Ethernet data to a CAN device.

CAN server (UDP server) parameter information as follow:

- IP address: 192.168.1.254
- Listen Port: 32000
- Baud rate: 1000K

Host PC (UDP client mode) parameter information as follow:

- IP address: 192.168.1.2
- Local Port:60000

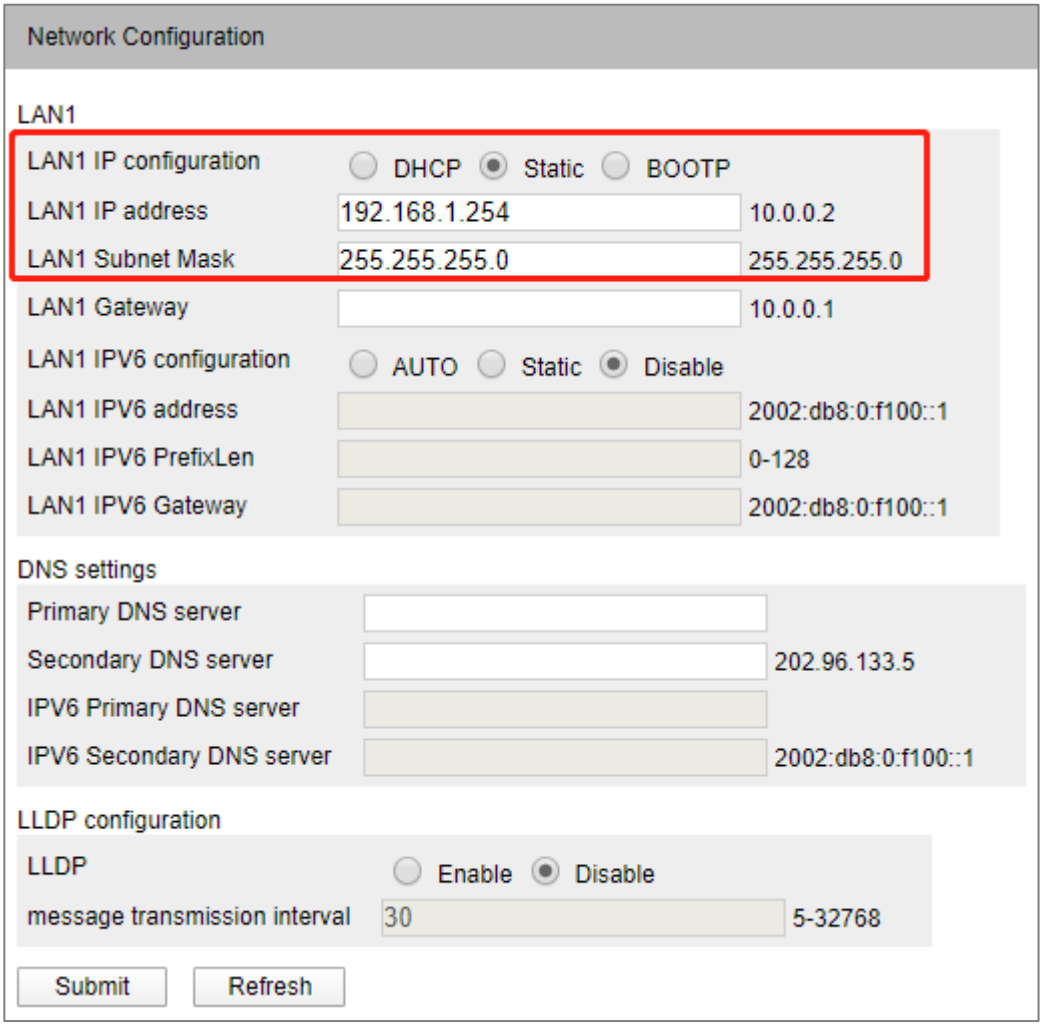
Operating Steps

Step 1 Configure CAN server IP address.

1 Login in the Web configuration interface, choose "Network Setting".

2 In the "LAN1" area, select " LAN1 IP Configuration" as "Static", and enter the corresponding network address information such as " LAN1 IP Address", " LAN1 Subnet Mask" and " LAN1 Gateway".

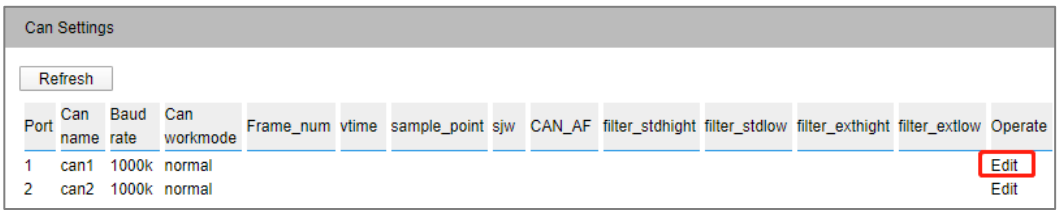
3 Other parameters remain the default, click "Submit".



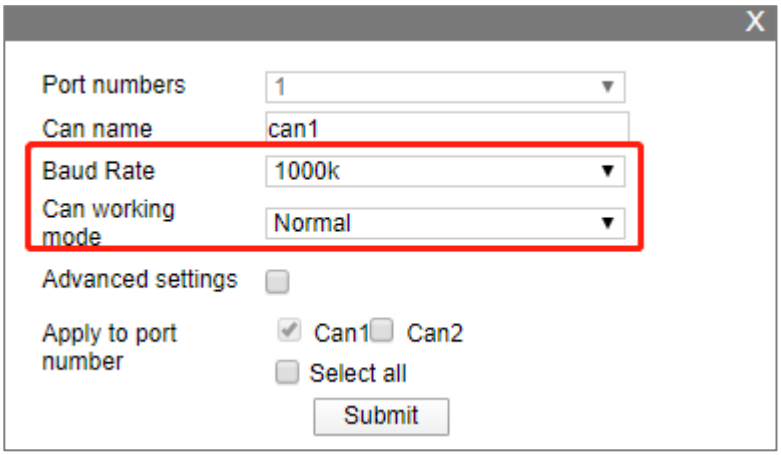
Step 2 Configure the CAN port parameter information.

1 Log in to the Web configuration interface and select "CAN Settings".

2 In the CAN1 entry, click the "Edit" button under the operation, as shown in the following figure.



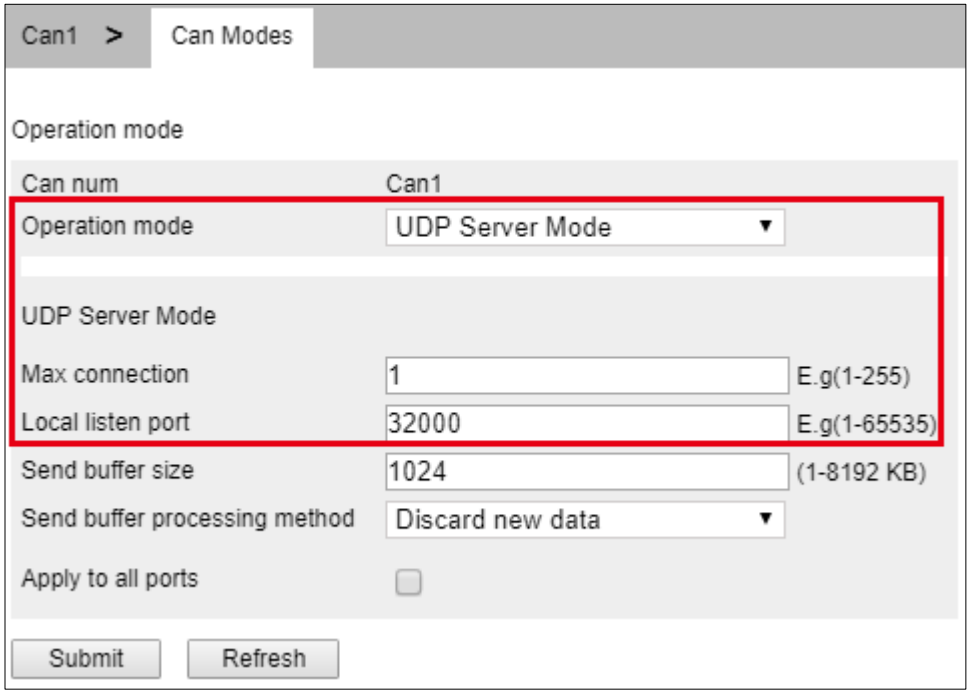
3 In the “Edit” window, set “Baud Rate” and “CAN working mode” respectively, as shown in the following figure.



4 Other parameters remain the default, click "Submit".

Step 3 Configure the work mode of CAN server.

1 Log in to the WEB configuration interface and select "CAN mode > CAN1".



2 Click the "Operation Mode" drop-down list box and select "UDP Server Mode".

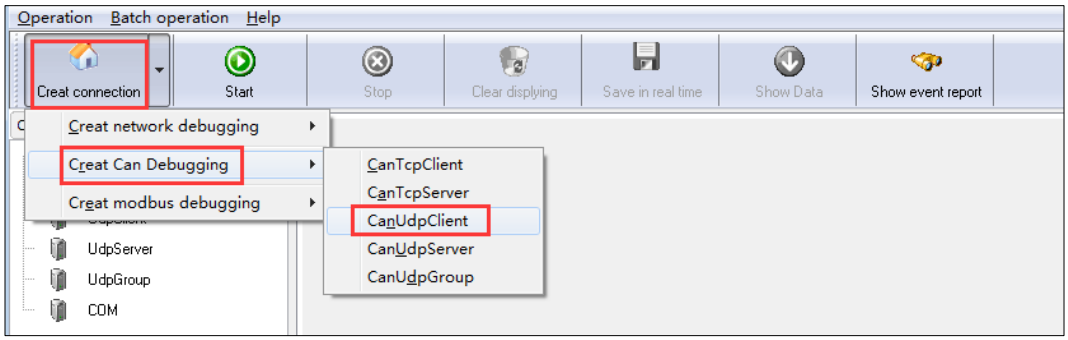
3 Enter 1 in "Max connection" text box.

4 Enter "32000" on "Local listen port" text box.

5 Other parameters remain the default, click "Submit".

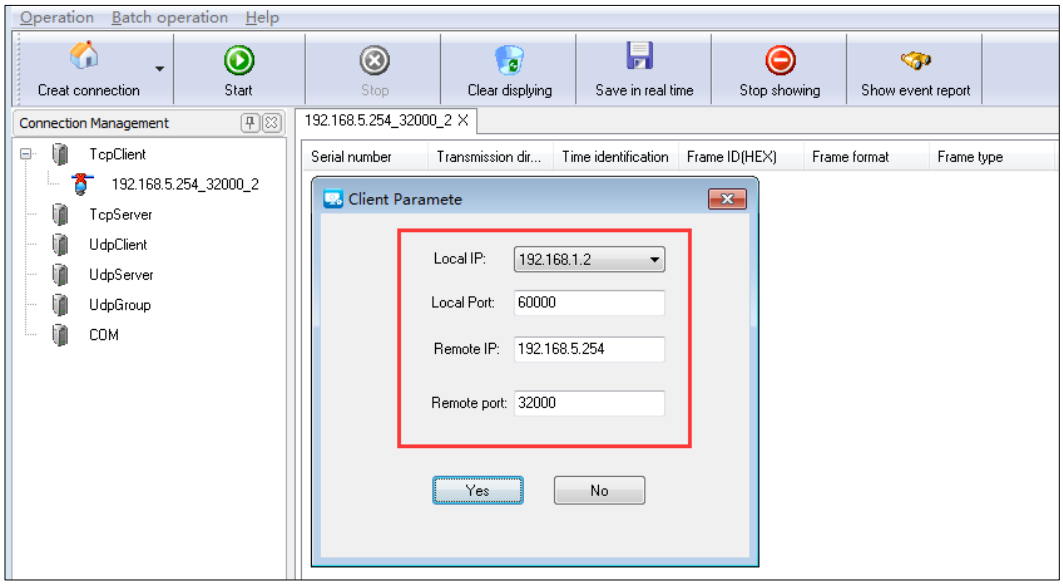
Step 4 Run the "DebugTool" software, create UDP client for the host.

1 Install and run "Debugging Assistant" software, Click "Create Connection" drop-down list box, choose "Create Can Debugging > CanUdpClient".



2 On the pop-up "Local IP" drop-down list box, choose the IP address of host PC (Udp client) "192.168.1.2".

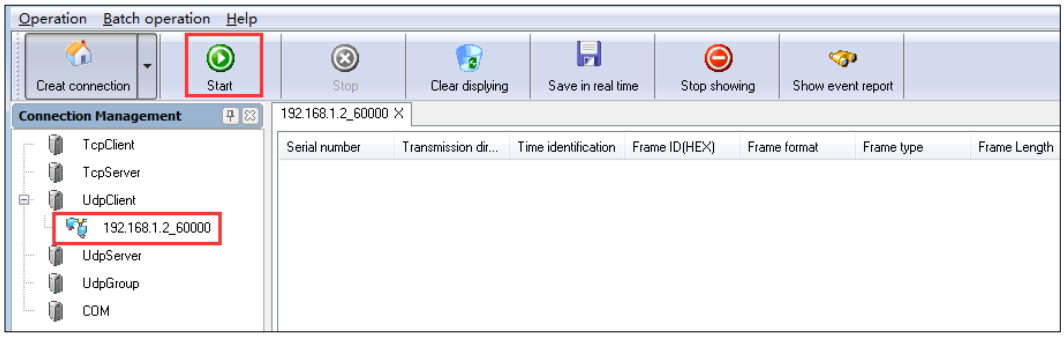
3 Enter the host PC (Udp client) port "60000" on the "Local Port" text box.



4 On the "Remote IP" text box, enter the IP address of CAN server (Udp server) "192.168.1.254".

5 On the "Remote Port" text box, enter the port of CAN server (Udp server) "32000", click "Yes".

6 Choose the created Udpclient connection, click "Start".

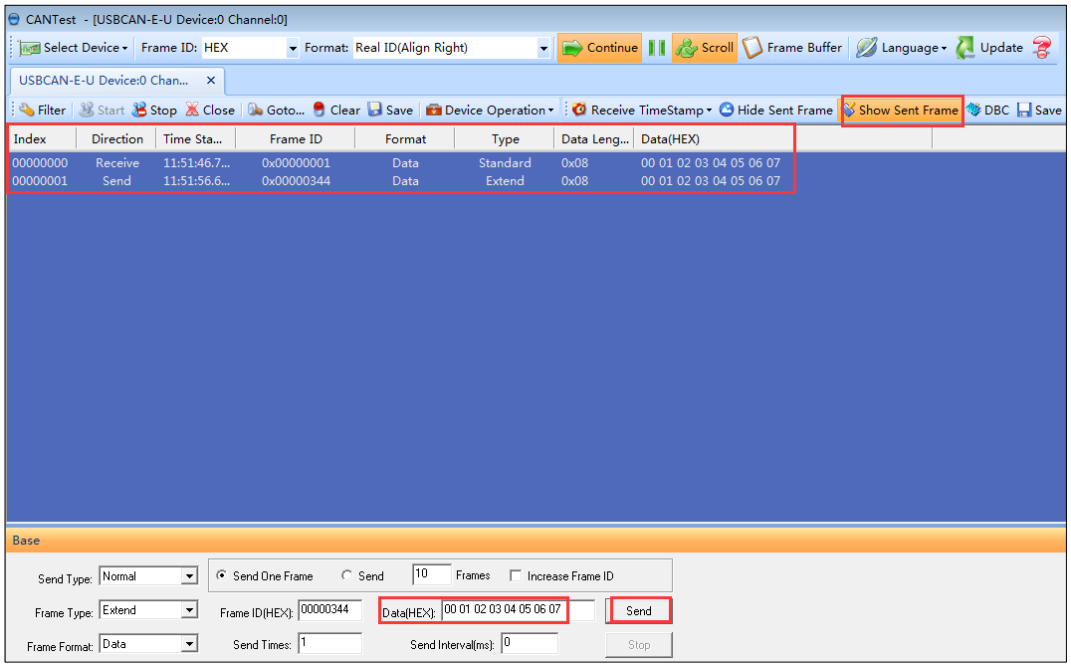


Step 5 Synchronously run "Debugging Assistant" and "CANTest" software, test the

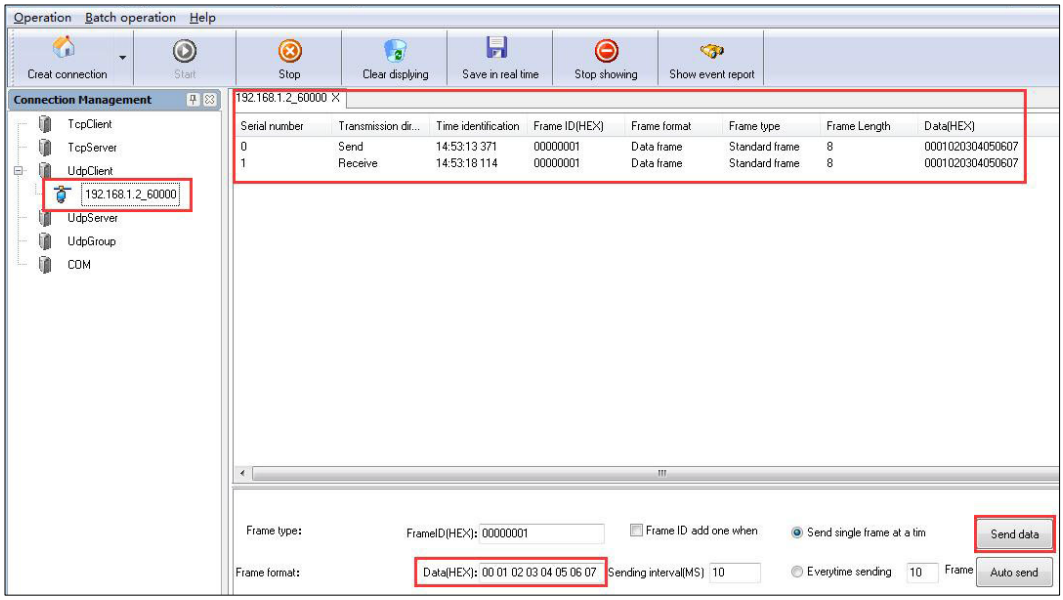
intercommunication between CAN server (UDP server) and host PC (UDP client).

1 Install and run "CANTest" software, click "Show Sent Frame" option box.

2 Frame data maintains default "00 01 02 03 04 05 06 07", click "Send".



3 Run "Debugging Assistant" software, check the CAN port information received by host PC on UDPClient option box. In a similar way, host PC can send information to CAN port device.



Step 6 End.

10.4 UDP Client Mode

Background introduction

Under "UDP Client Mode", it's assumed that CAN server port "CAN1" forwardly waits for the connection of one host PC, meanwhile the host can read or send the Ethernet data to a CAN device.

CAN server (UDP client mode) parameter information as follow:

- IP address: 192.168.1.254
- Listening Port: 60001
- Baud rate: 1000K

The parameters of the host PC (UDP server) are as follows:

- IP address: 192.168.1.2
- Local Port:33000

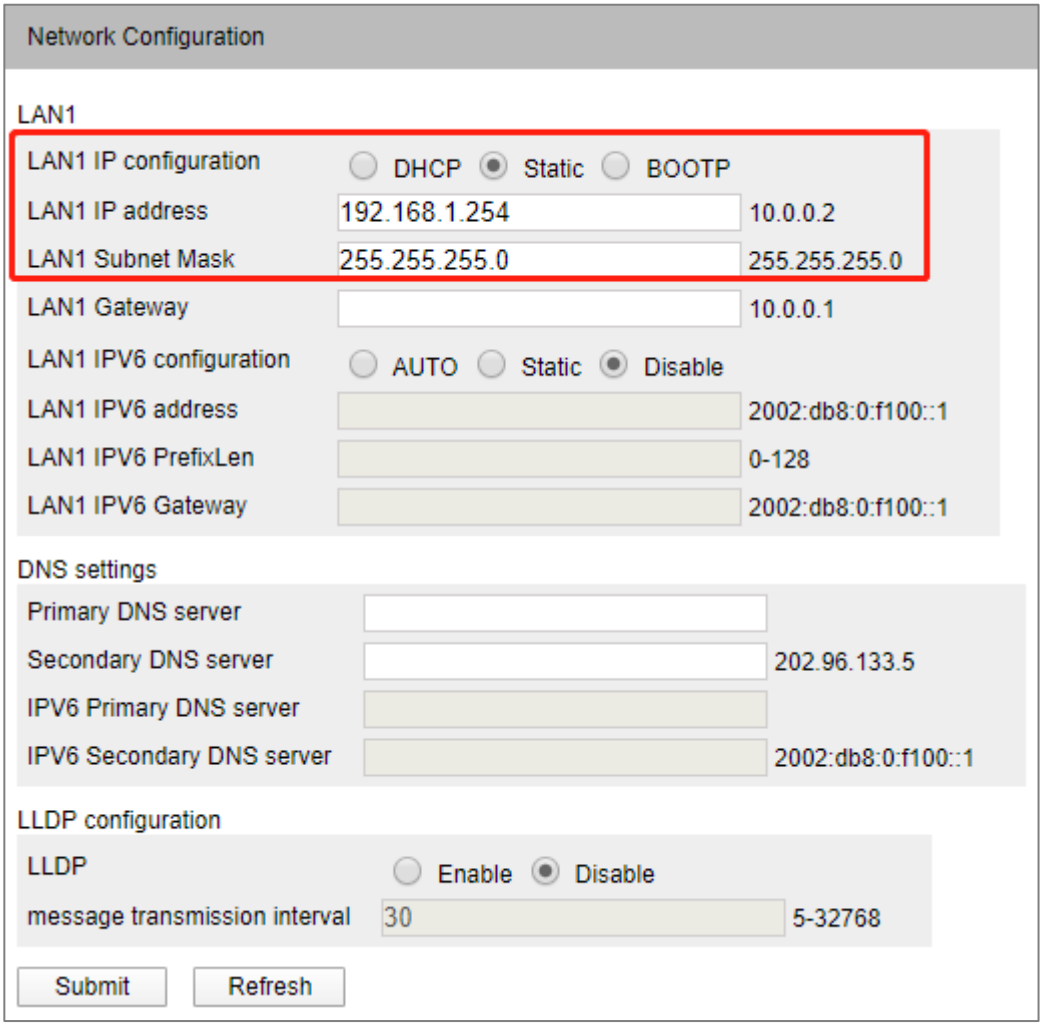
Operating Steps

Step 1 Configure CAN server IP address.

1 Login in the Web configuration interface, choose "Network Configuration".

2 In the "LAN1" area, select "LAN1 IP Configuration" as "Static", and enter the corresponding network address information such as " LAN1 IP Address", " LAN1 Subnet Mask" and "LAN1 Gateway".

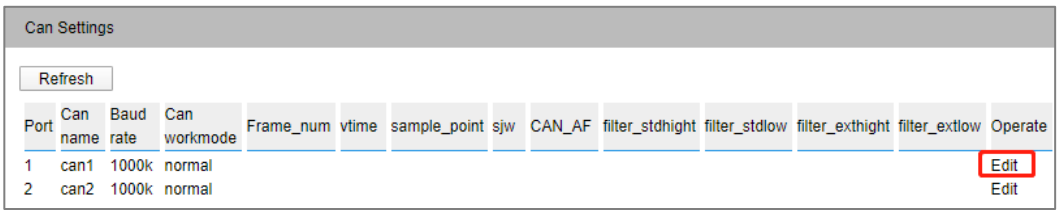
3 Other parameters remain the default, click "Submit".



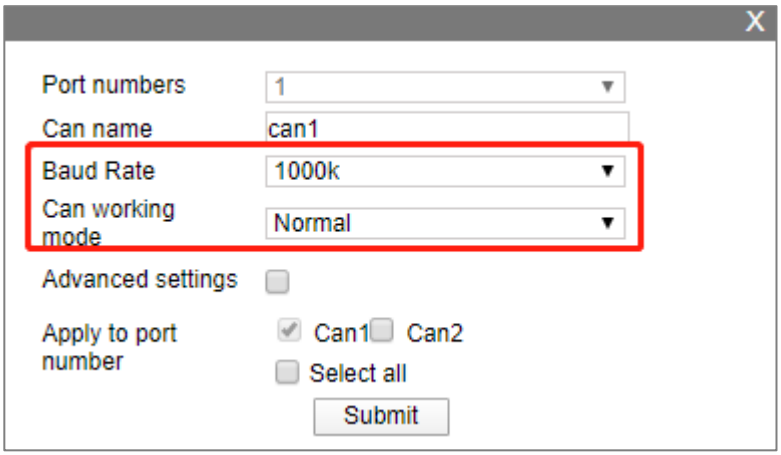
Step 2 Configure the CAN port parameter information.

1 Log in to the Web configuration interface and select "CAN Settings".

2 In the CAN1 entry, click the "Edit" button under the operation, as shown in the following figure.



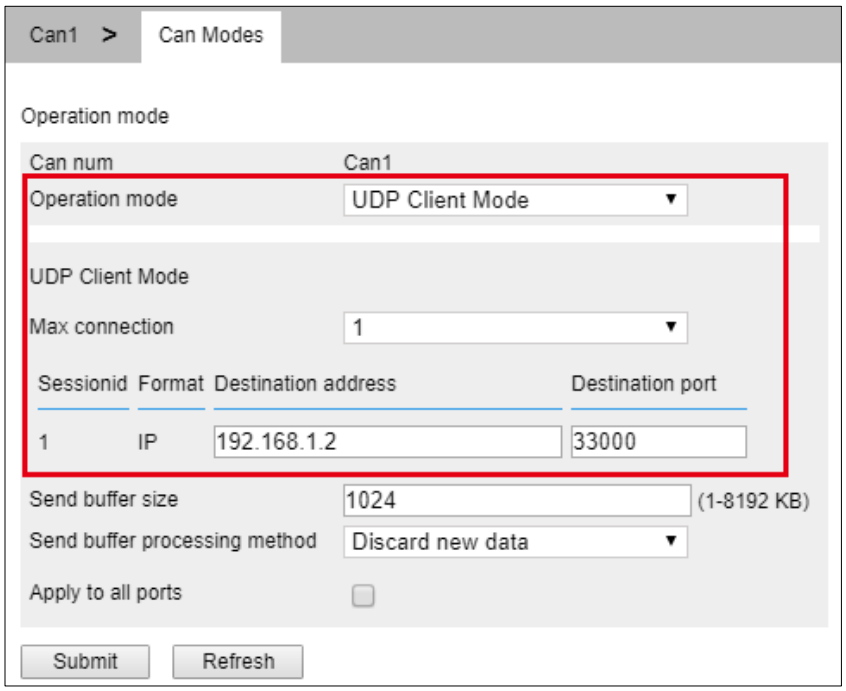
3 In the “Edit” window, set “Baud Rate” and “CAN working mode” respectively, as shown in the following figure.



4 Other parameters remain the default, click "Submit".

Step 3 Configure the work mode of CAN server.

1 Log in to the WEB configuration interface and select "CAN mode > CAN1".



2 Click the "Operation Mode" drop-down list box and select "UDP Client Mode".

3 Click "Max connection" drop-down list box, select "1".

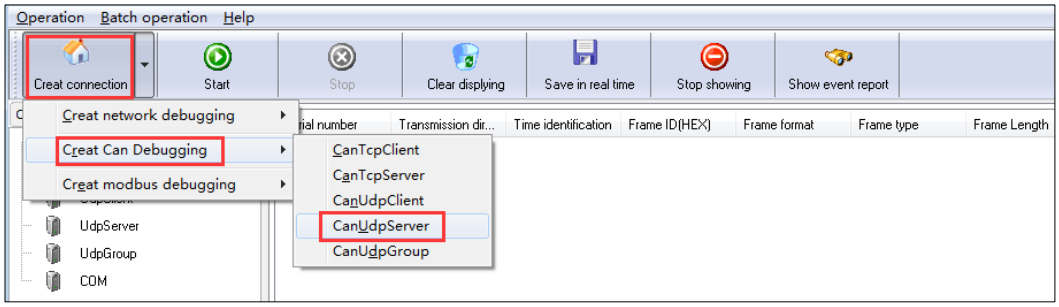
4 Enter the host PC's IP address "192.168.1.2" in the destination address text box.

5 Enter the host PC's local port number, 33000, in the destination port text box.

6 Other parameters remain the default, click "Submit".

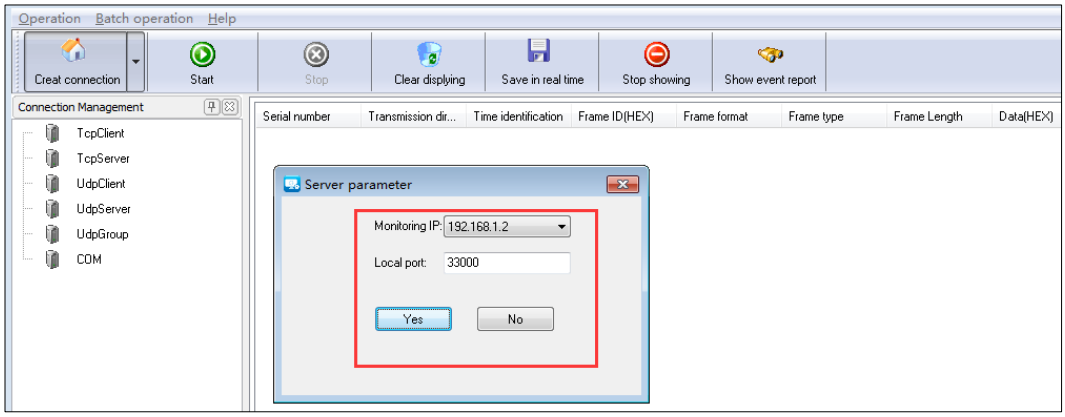
Step 4 Run the “Debug Assistant” software to create a UDP server for the host.

1 Install and run "Debugging Assistant" software, Click "Create Connection" drop-down list box, choose "Create Can Debugging > CanUDPServer".

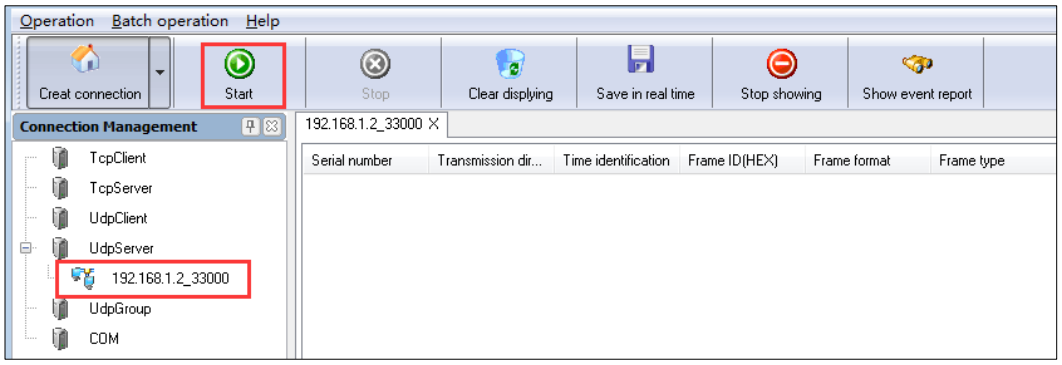


2 On the "Monitoring IP" drop-down list box, choose the IP address of host PC (UDP server) "192.168.1.2".

3 Enter the host PC (UDP server) local port "33000" on the "Local Port" text box, click "Yes".



4 Choose the created UdpServer connection, click "Start".



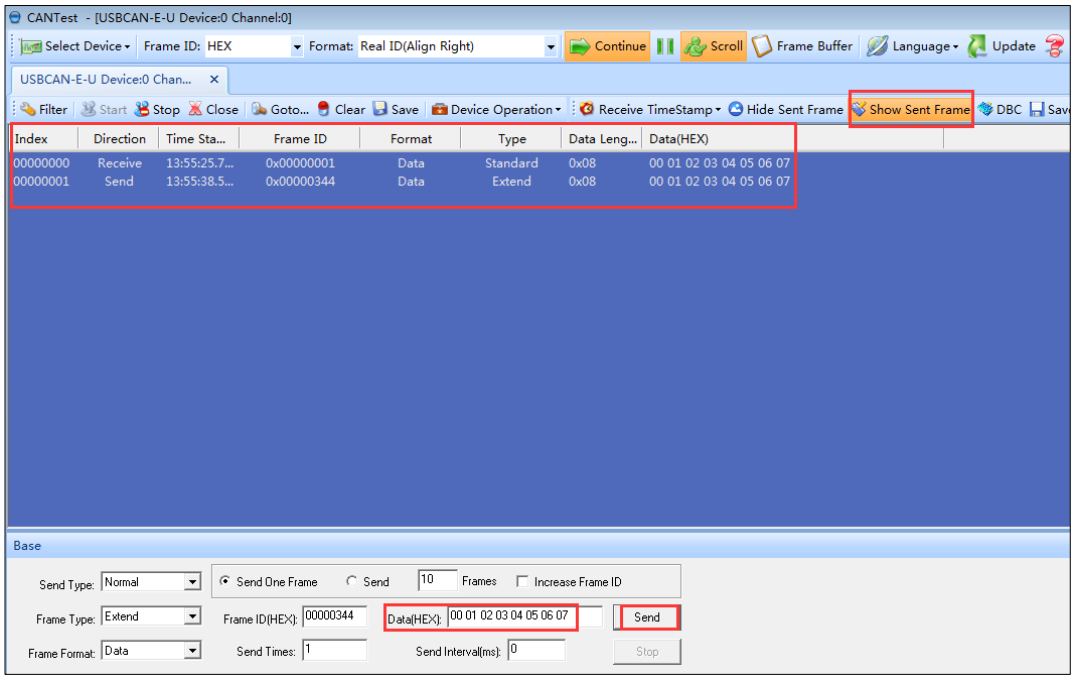
Notice

UDP (User Datagram Protocol), it's a connectionless protocol. Therefore, after successfully creating UdpClient connection, user doesn't need to click "Start".

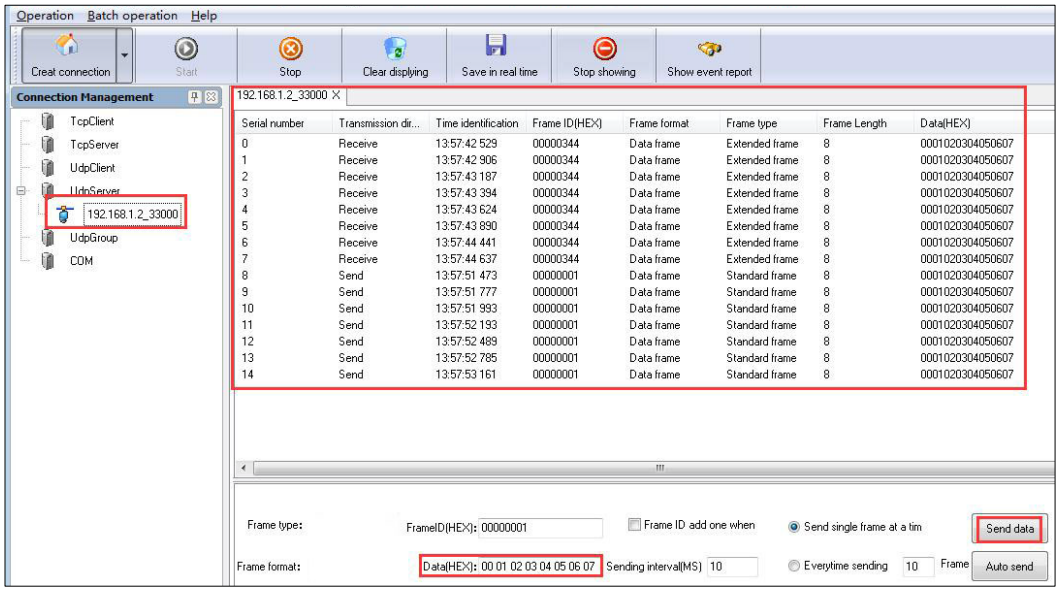
Step 5 Synchronously run "Debugging Assistant" and "CANTest" software, test the intercommunication between CAN server (UDP client) and host PC (UDP server).

1 Install and run "CANTest" software, click "Show Sent Frame" option box.

2 Frame data maintains default "00 01 02 03 04 05 06 07", click "Send".



3 Run "Debugging Assistant" software, check the CAN port information received by host PC on UDPServer option box. In a similar way, host PC can send information to CAN port device.



Step 6 End.

10.5 UDP Rang Mode

Background introduction

When the router, switch and other devices do not support multicast function, CAN server can realize the multicast function under the CAN UDP Rang Mode. It's assumed

that the CAN port of CAN server corresponding to the computer is "CAN1", CAN server can transmit data with two hosts in the same network segment "192.168.1.2" ~ "192.168.1.3" via UDP protocol.

CAN server (UDP server) parameter information as follow:

- IP address: 192.168.1.254
- Listen Port: 32000
- Baud rate: 1000K

The parameters of the host PC A (UDP client A) are as follows:

- IP address: 192.168.1.2
- Local Port:33000

Host B (UDP client B) parameter information as follow:

- IP address: 192.168.1.3
- Local Port:33000

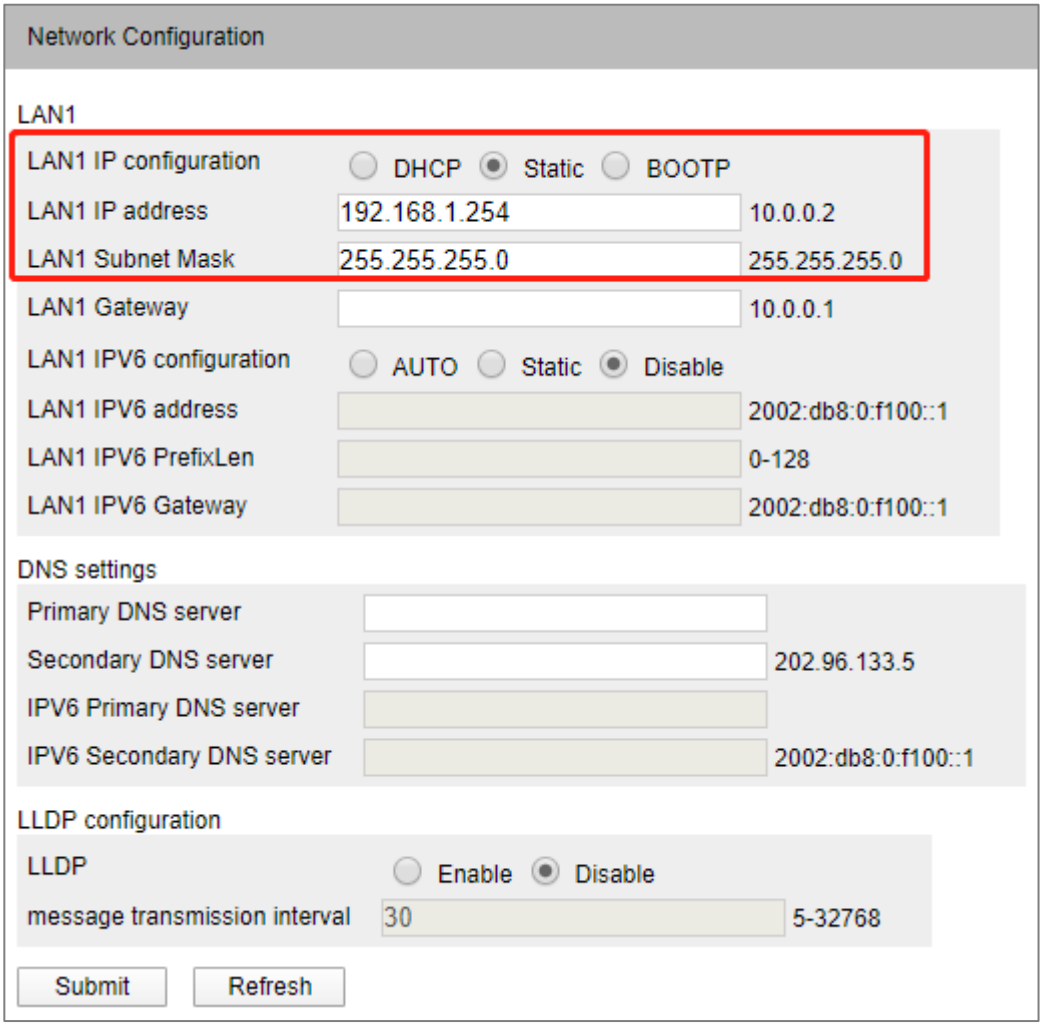
Operating Steps

Step 1 Configure CAN server IP address.

1 Login in the Web configuration interface, choose "Network Setting".

2 In the "LAN1" area, select "LAN1 IP Configuration" as "Static", and enter the corresponding network address information such as " LAN1 IP Address", " LAN1 Subnet Mask" and " LAN1 Gateway".

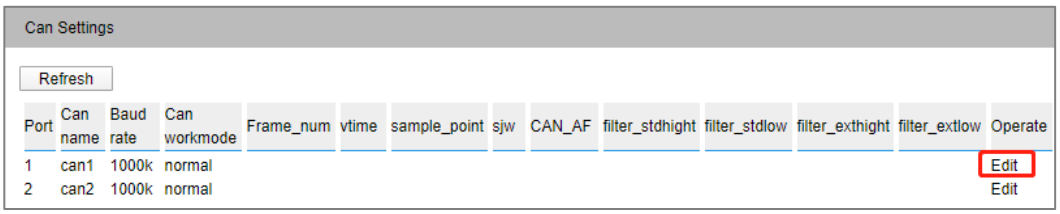
3 Other parameters remain the default, click "Submit".



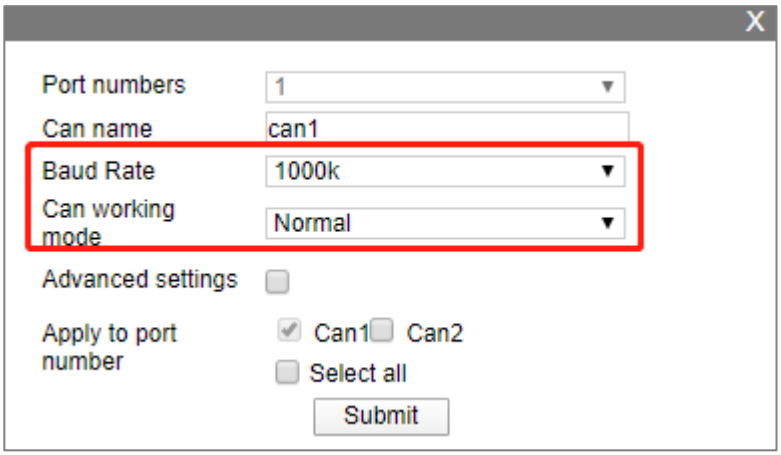
Step 2 Configure the CAN port parameter information.

1 Log in to the Web configuration interface and select "CAN Settings".

2 In the CAN1 entry, click the "Edit" button under the operation, as shown in the following figure.



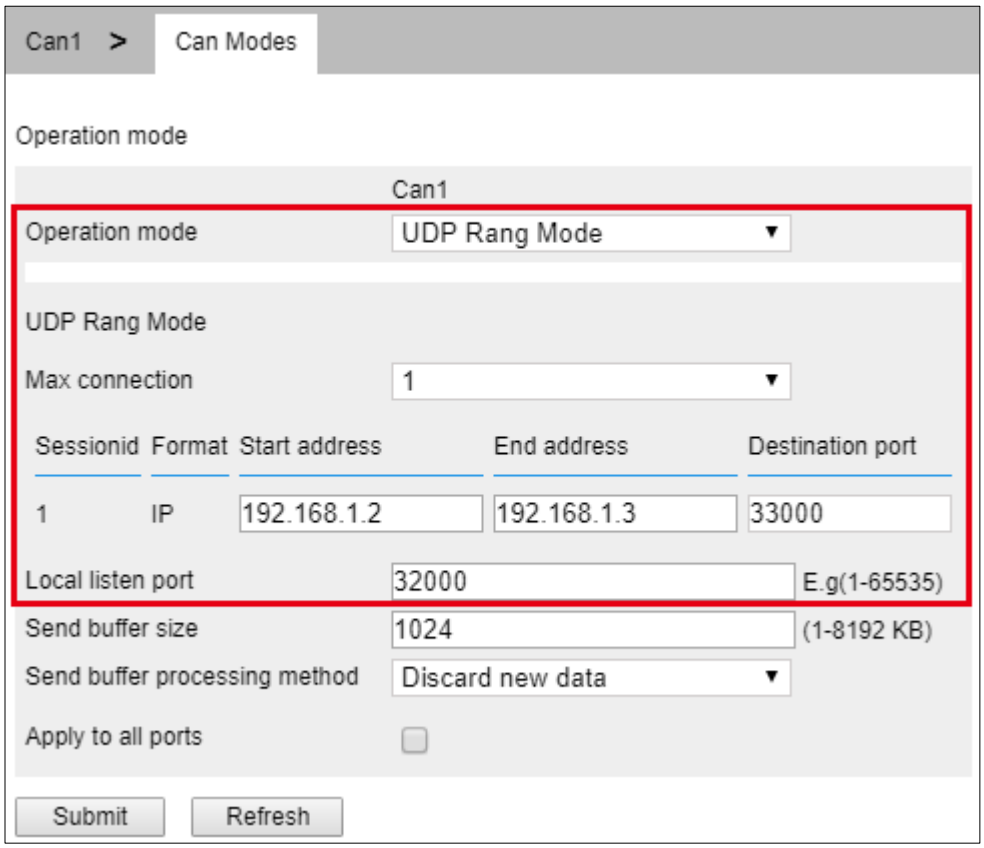
3 In the “Edit” window, set “Baud Rate” and “CAN working mode” respectively, as shown in the following figure.



4 Other parameters remain the default, click "Submit".

Step 3 Configure the work mode of CAN server.

1 Log in to the WEB configuration interface and select "CAN mode > CAN1".



2 Click the “Operation mode” drop-down list box and select “UDP Rang Mode”.

3 Click "Max connection" drop-down list box, select "1".

4 Enter "192.168.1.2" on the "Start Address" text box.

5 Enter "192.168.1.3" on the "End Address" text box.

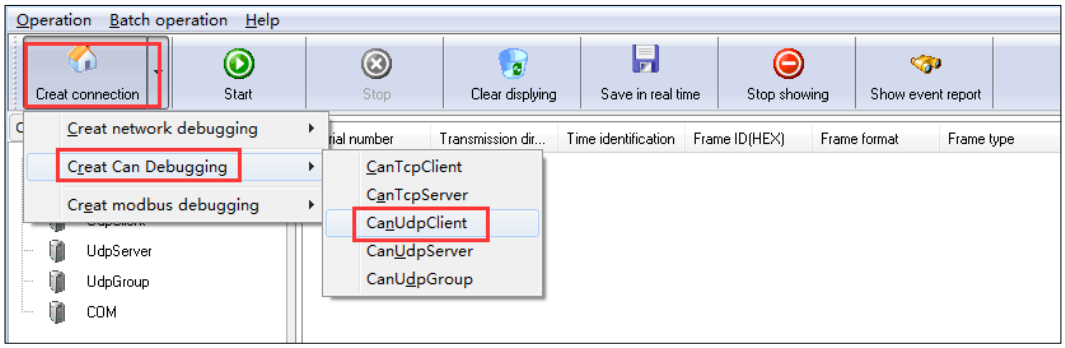
6 Enter "33000" on the "Destination Port" text box.

7 Enter "32000" on "Local listen Port" text box.

8 Other parameters maintain the default, click "Submit".

Step 4 Run the debug assistant software on host A to create Udp client A.

1 Install and run "Debugging Assistant" software, Click "Create Connection" drop-down list box, choose "Create Can Debugging > CanUDPClient".

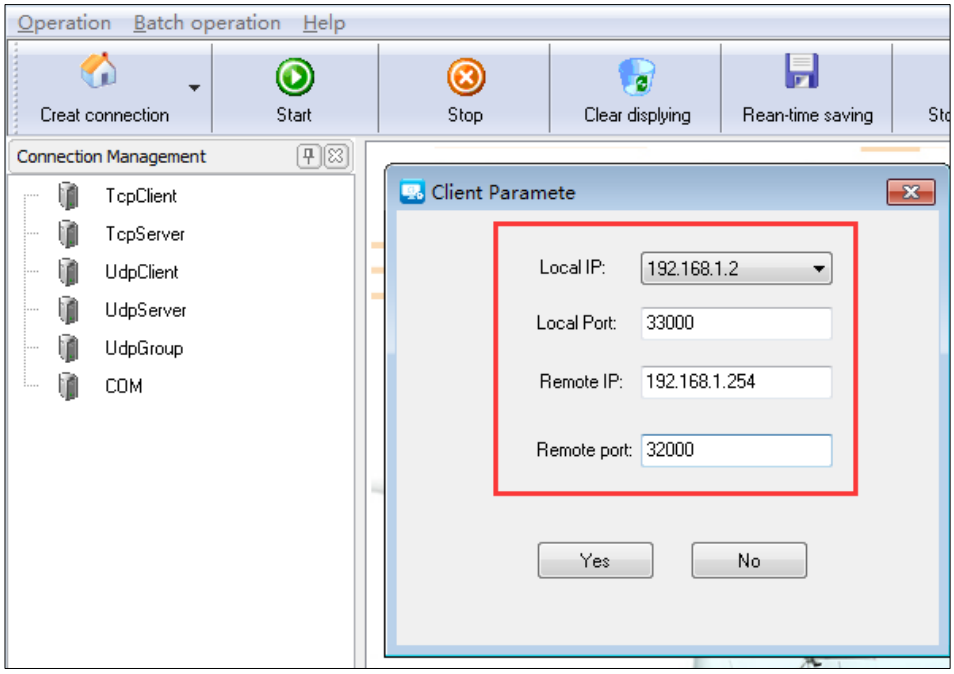


2 On the "Local IP" drop-down list box, choose the IP address of host A (Udp client A) "192.168.1.2".

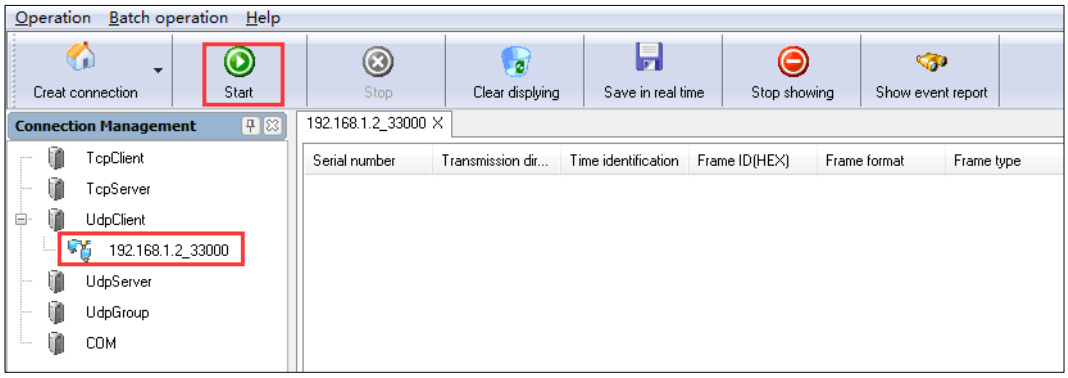
3 Enter the host A (Udp client A) port "60000" on the "Local Port" text box.

4 On the "Remote IP" text box, enter the IP address of CAN server (Udp server) "192.168.1.254".

5 On the "Remote Port" text box, enter the port of CAN server (Udp server) "33000", click "Yes".

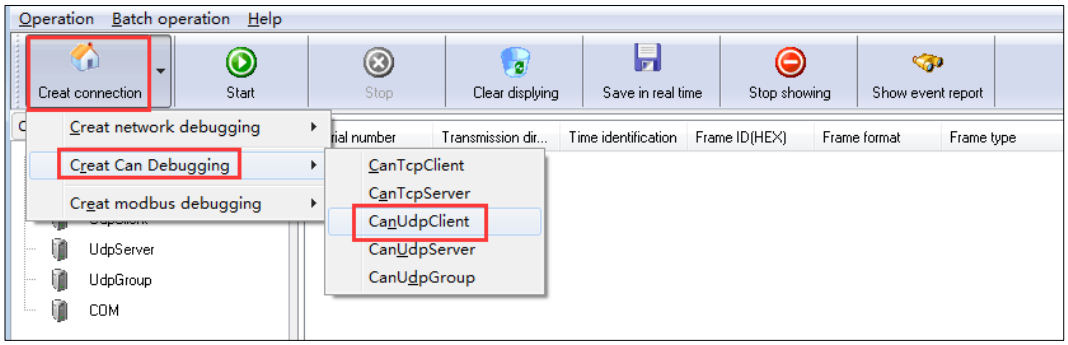


6 Choose the created UdpClient connection, click "Start".



Step 5 Run the debug "Debugging Assistant" on host B to create UDP client B.

1 Install and run "Debugging Assistant" software, Click "Create Connection" drop-down list box, choose "Create CAN Debugging > CANUDPClient".

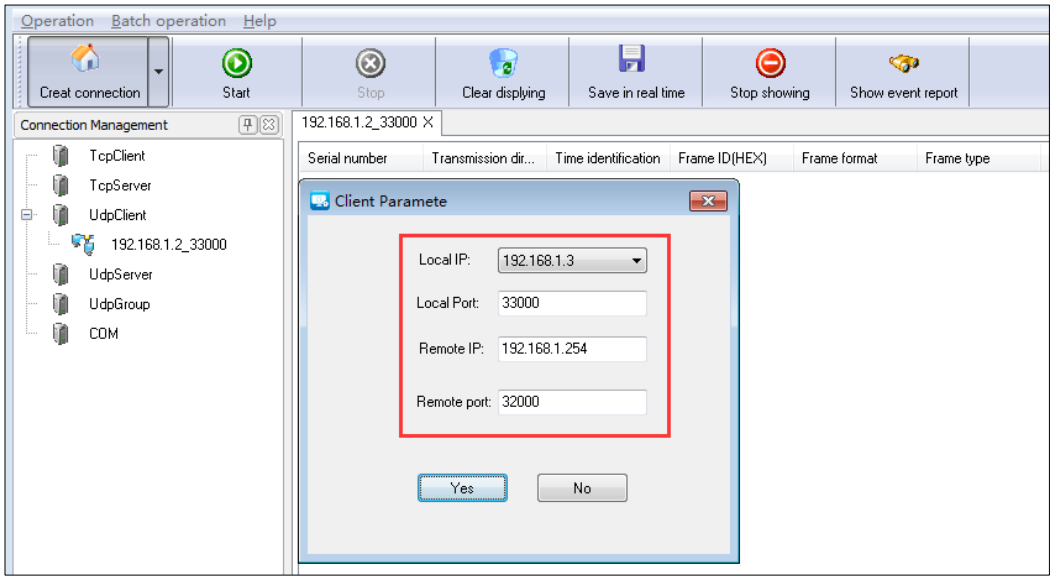


2 In the “Monitoring IP” drop-down list box, select the IP address "192.168.1.3" of the host B (that is, the UDP client B).

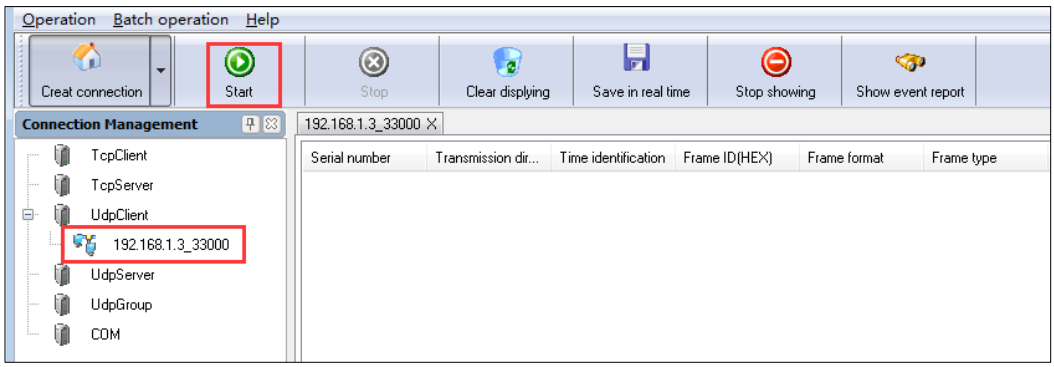
3 Enter the host B (UDP client B) port "60000" on the "Local Port" text box.

4 On the "Remote IP" text box, enter the IP address of CAN server (Udp server) "192.168.1.254".

5 On the "Remote Port" text box, enter the port of CAN server (Udp server) "33000", click "Yes".



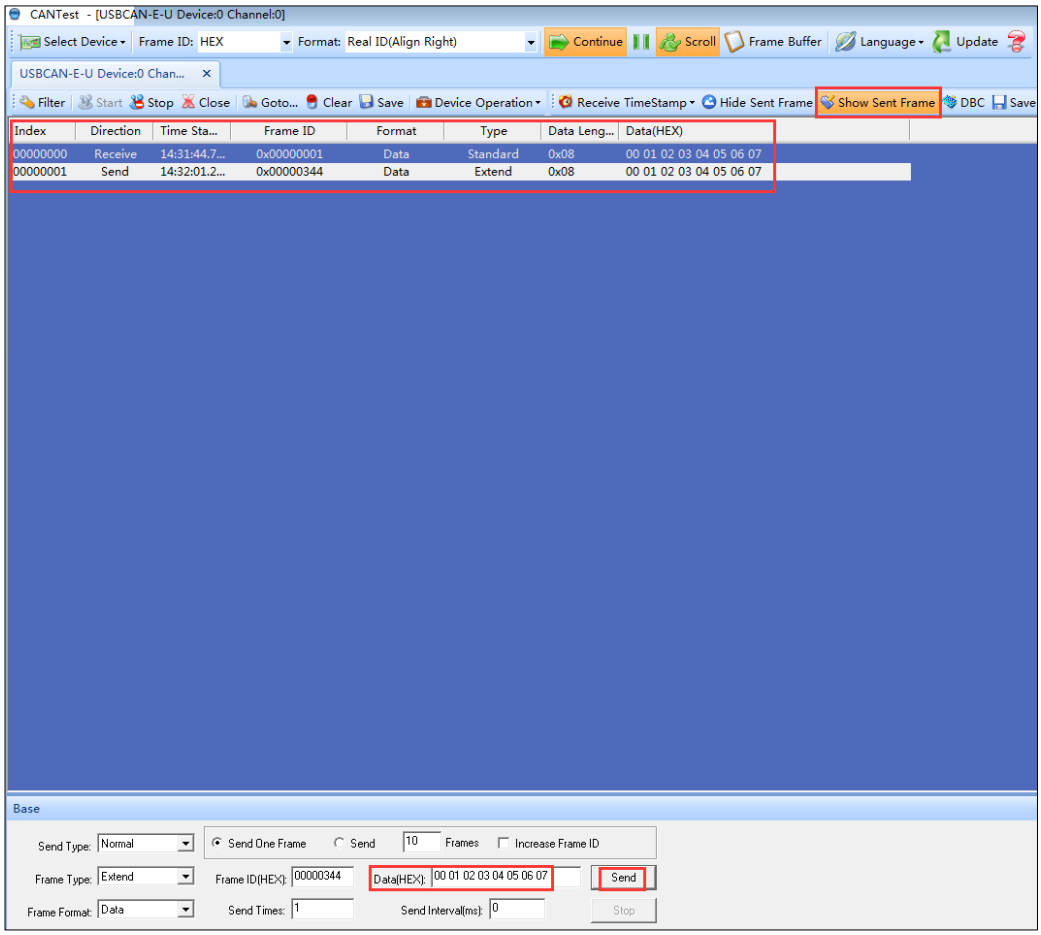
6 Choose the created UdpClient connection, click "Start".



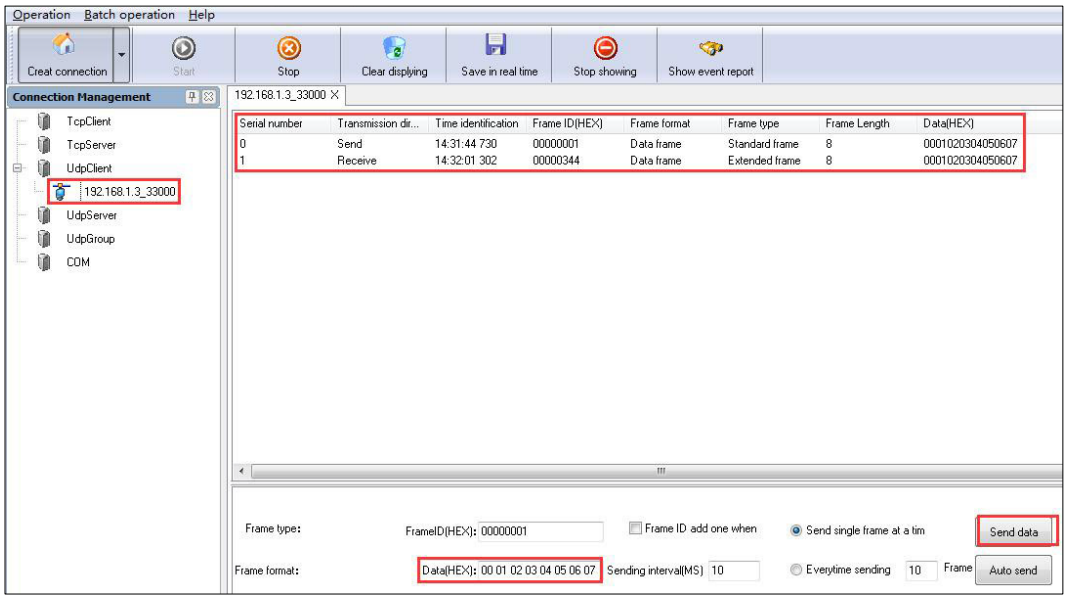
Step 6 Synchronously run "Debugging Assistant" and "CANTest" software, test the intercommunication between CAN server (UDP server) and host PC (UDP client).

1 Install and run "CANTest" software, click "Show Sent Frame" option box.

2 Frame data maintains default "00 01 02 03 04 05 06 07", click "Send".



3 Run "Debugging Assistant" software, check the CAN port information received by host A and B on UDPClient option box. In a similar way, host A and B can send information to CAN port device.



10.6 UDP Multicast Mode

Background introduction

It's assumed that CAN server IP address is "192.168.1.254", user needs to add the CAN server to the multicast address "239.0.0.0". Therefore CAN server can send the unicast or multicast data to one or more appointed hosts via UDP protocol, meanwhile it can receive the unicast or multicast data from one or more devices and achieve many-to-many communication.

CAN server parameter information as follow:

- IP address: 192.168.1.254
- Group Address: 239.0.0.0
- Listen Port: 32000
- Baud rate: 1000K

The parameters of the host PC B are as follows:

- IP address: 192.168.1.2
- Local Port:33000
- Group Address: 239.0.0.1

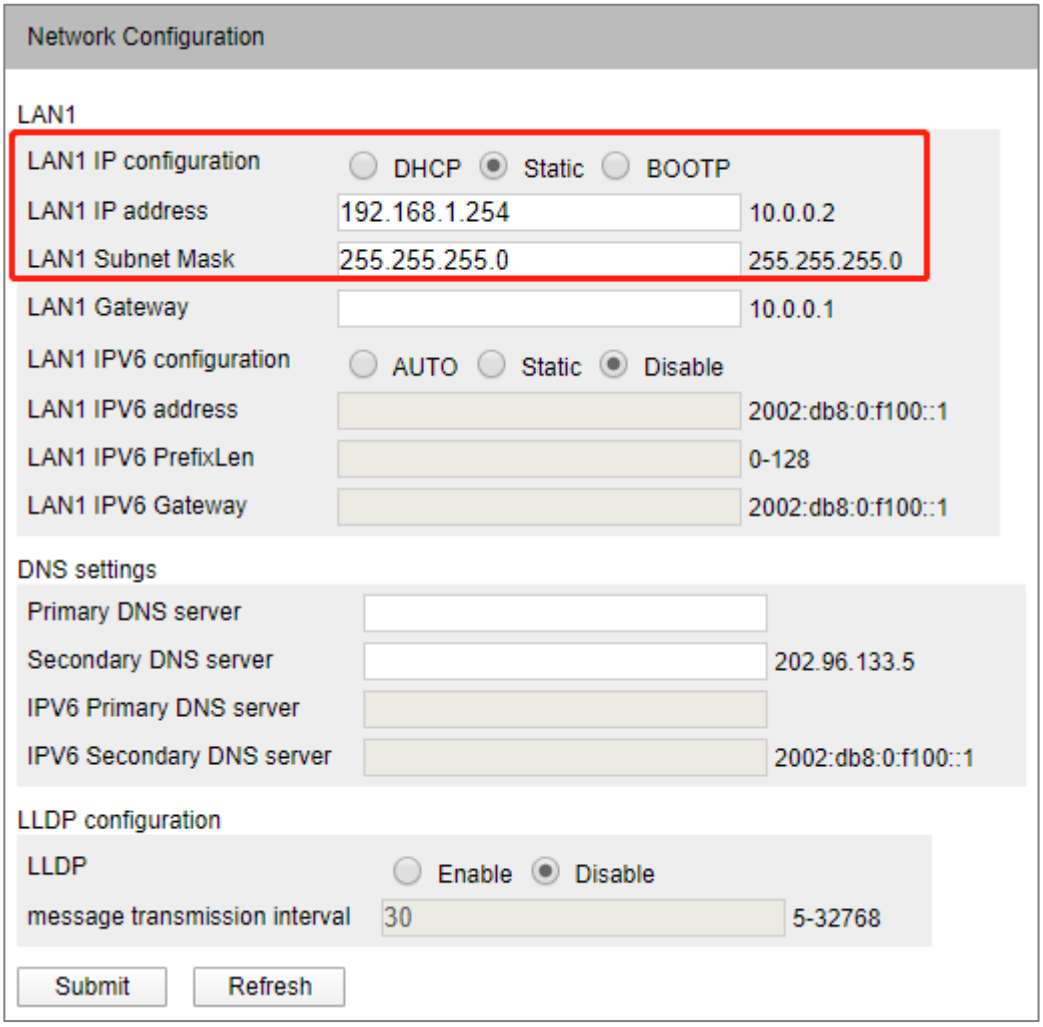
Operation steps

Step 1 Configure CAN server IP address.

1 Login in the Web configuration interface, choose "Network Setting".

2 In the " LAN1" area, select " LAN1 IP Configuration" as "Static", and enter the corresponding network address information such as "LAN1 IPAddress", " LAN1 Subnet Mask" and " LAN1 Gateway".

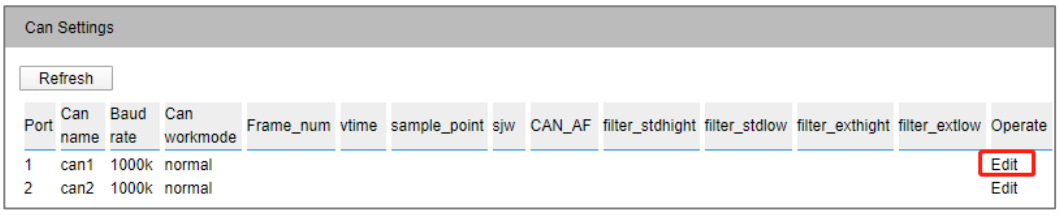
3 Other parameters remain the default, click "Submit".



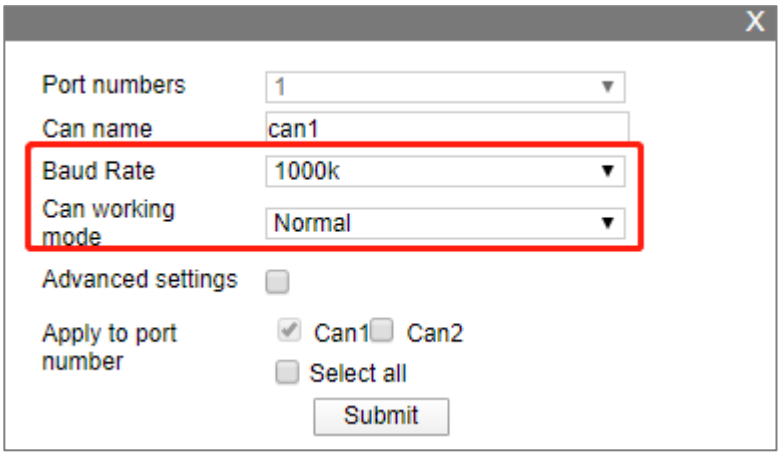
Configure the CAN port parameter information.

1 Log in to the Web configuration interface and select "CAN Settings".

2 In the CAN1 entry, click the "Edit" button under the operation, as shown in the following figure.



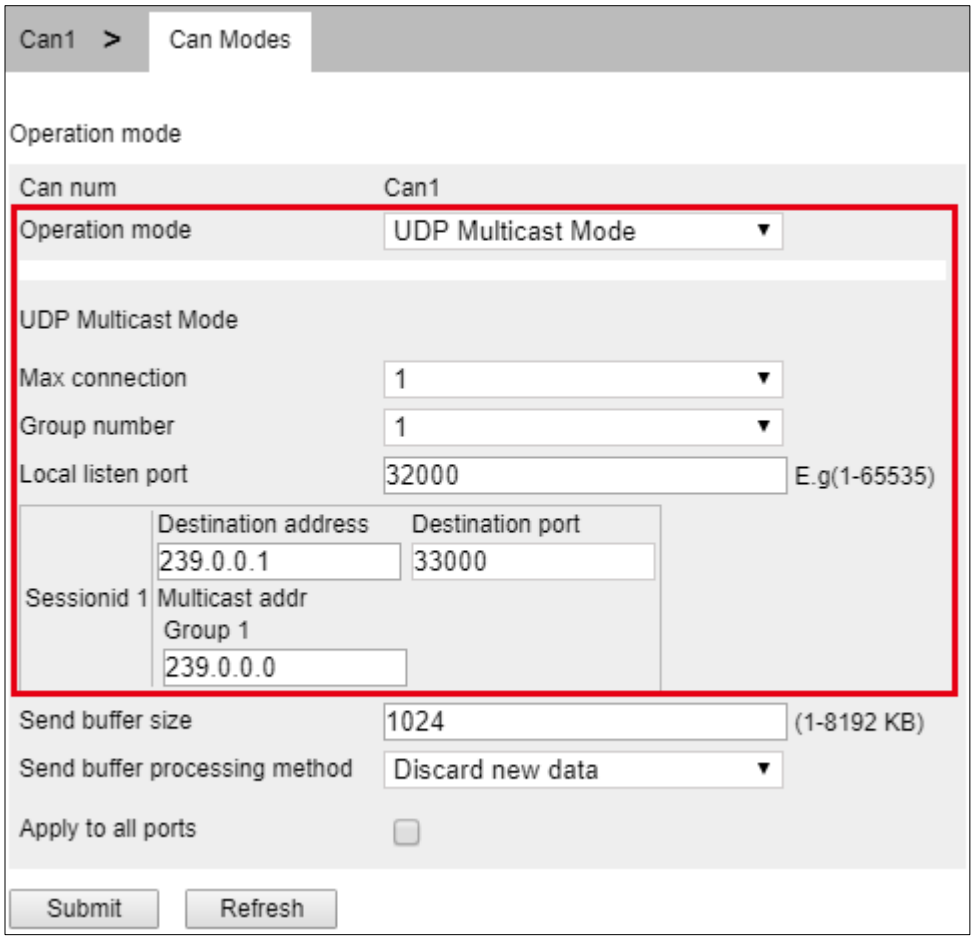
3 In the “Edit” window, set “Baud Rate” and “CAN working mode” respectively, as shown in the following figure.



4 Other parameters remain the default, click "Submit".

Step 2 Configure the work mode of CAN server.

1 Log in to the WEB configuration interface and select "CAN mode > CAN1".



2 Click the “Operation Mode” drop-down list box and select “UDP Multicast Mode”.

3 Click "Max connection" drop-down list box, select "1".

4 Enter "32000" on "Local listen Port" text box.

5 Enter "239.0.0.1" on the "Destination address" text box of "Sessionid 1".

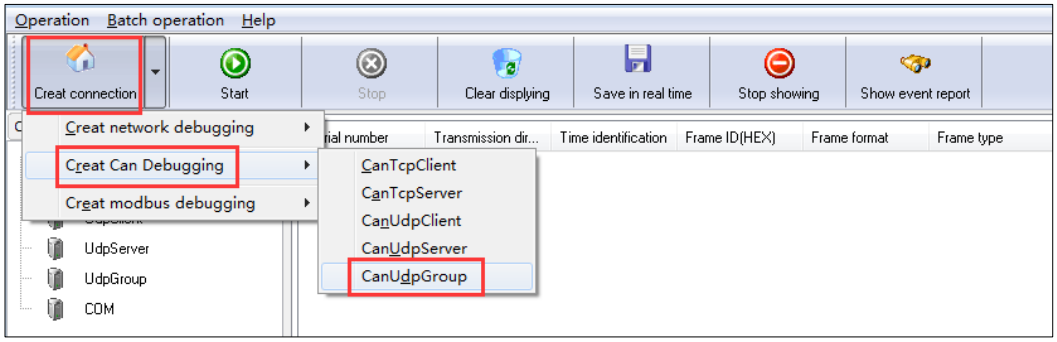
6 Enter "33000" on the "Destination Port" text box of "Sessionid 1".

7 Enter "239.0.0.0" on the "Multicast addr Group 1" text box of "Sessionid 1".

8 Other parameters remain the default, click "Submit".

Step 3 Run the “Debug Assistant” software to create a UDP multicast server for the host.

1 Install and run "Debugging Assistant" software, click "Create Connection" drop-down list box, choose "Create CAN Debugging > CANUDPGroup".



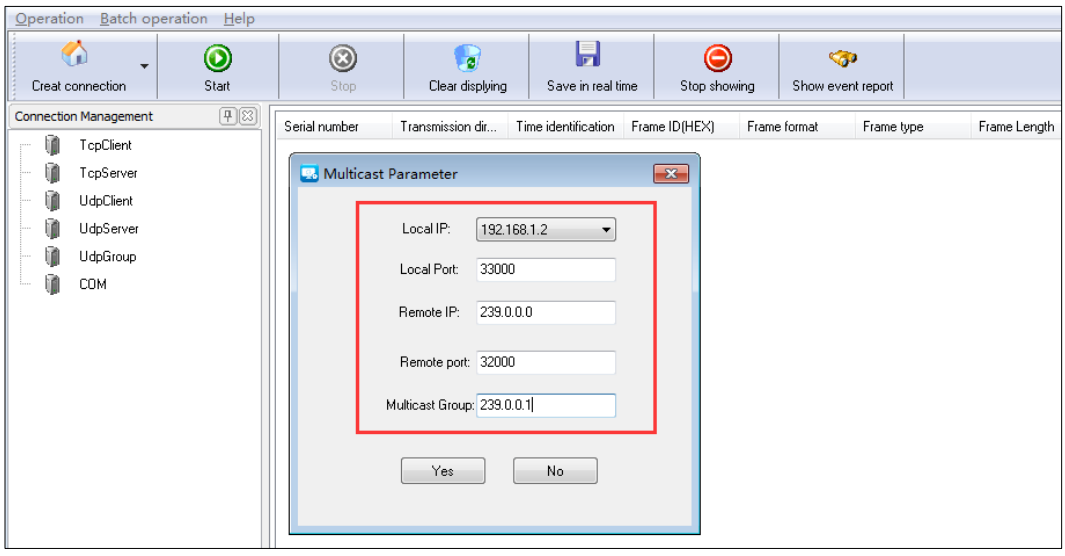
2 On the "Local IP" drop-down list box, choose the IP address of host PC "192.168.1.2".

3 Enter the host PC local port "33000" on the "Local Port" text box.

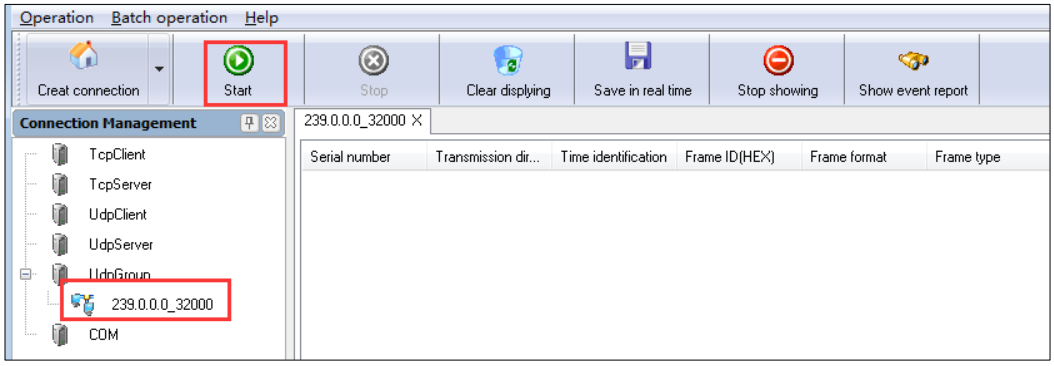
4 On the "Remote IP" text box, enter the IP address of CAN server "239.0.0.0".

5 On the "Remote Port" text box, enter the CAN server local port "32000".

6 Enter multicast group address "239.0.0.1" on the "Multicast Group" text box.



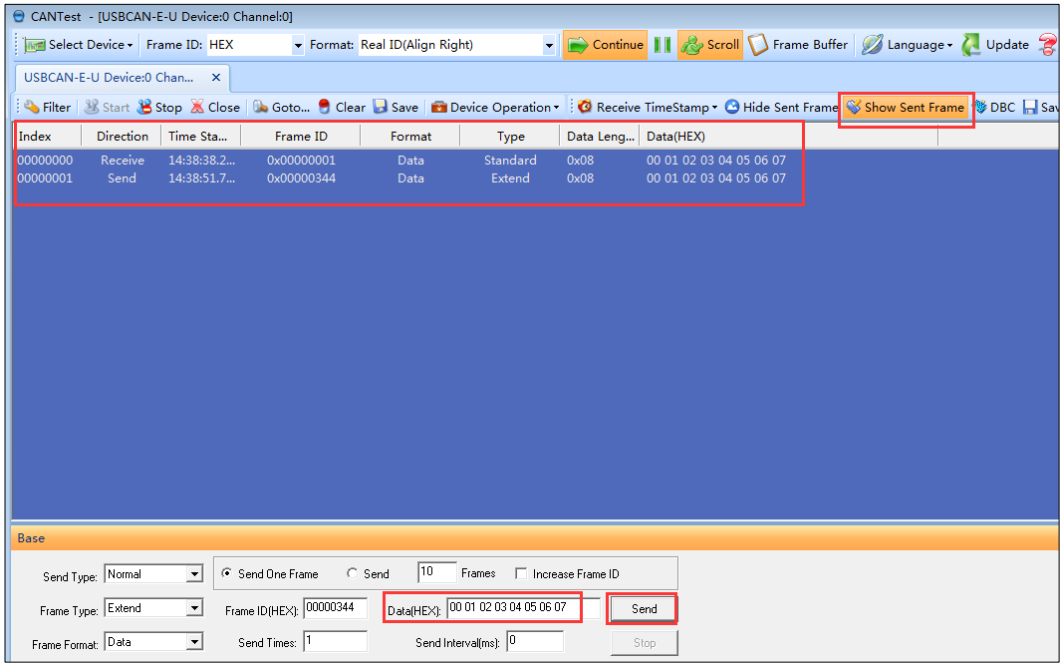
7 Choose the created UdpGroup connection, click "Start".



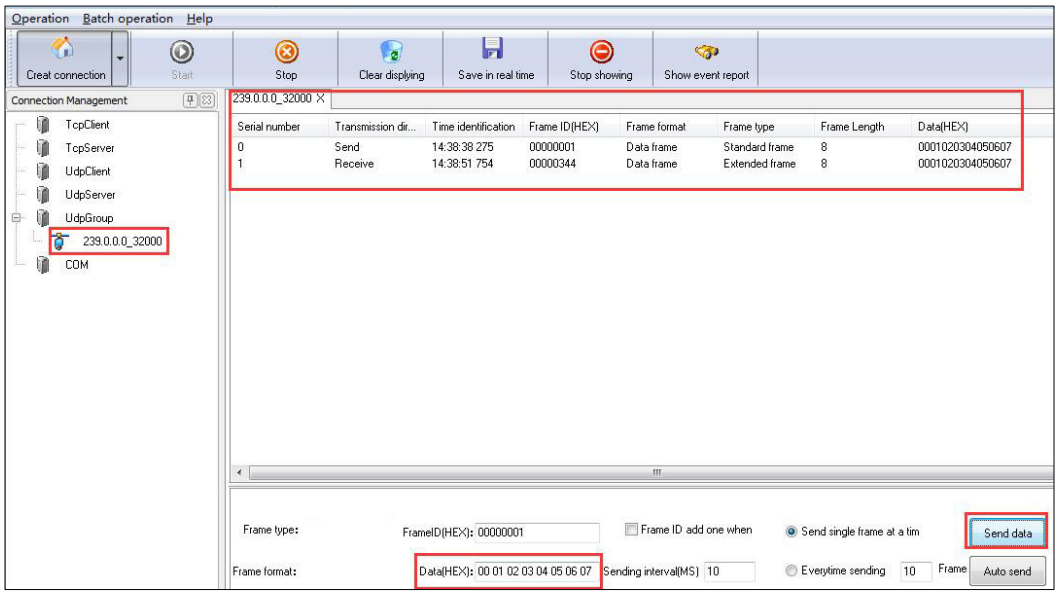
Step 4 Synchronously run "Debugging Assistant" and "CANTest" software, test the intercommunication between CAN server multicast address and host PC multicast address.

1 Install and run "CANTest" software, click "Show Sent Frame" option box.

2 Frame data maintains default "00 01 02 03 04 05 06 07", click "Send".



3 Run "Debugging Assistant" software, check the CAN port information received by host PC on UDPGroup option box. In a similar way, host PC can send information to CAN port device.



Step 5 End.

11 Maintenance and Service

Since the date of product delivery, our company will provide three years 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 product, consumers can get help and solutions in the following ways:

- Internet Service;
- Call technical support office;
- Product repair or replacement;

11.1 Internet Service

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

11.2 Service Hotline

Users of our company's products could call technical support office for help. Our company has professional technical engineers to answer your questions and help you to solve the product or usage problems ASAP.
Free service hotline: +86-400-880-4496

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

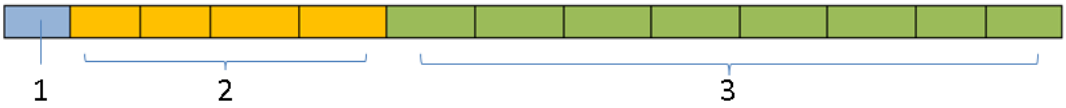
12 Appendix 1: CAN Data Transformation Format

CAN Data Transformation Format

One TCP or UDP frame contains several CAN frames, maximum 50 frames, minimum 1 CAN frame.

Frame	CAN Frame	CAN Frame	CAN Frame	...	CAN Frame

One CAN frame contains 13 bytes, as the picture bellow:



Frame Structure of the Frame Information

In the CAN frame structure picture, "1" represents the frame information: The length is 1 byte, and it's used for identifying some information of the CAN frame, such as type, length and so on.

Frame structure of the frame information as follow:

Bit7 Bit0

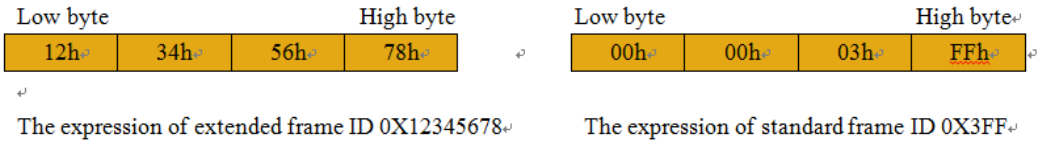
FF	RTR	Reserved	Reserved	D3	D2	D1	D0

- FF: Identification of standard frames and extend frame, 1 is extend frame, and 0 is standard frame.
- RTR: Identification of remote frame and data frame, 1 is remote frame, 0 is data frame.
- Reserved value is 0, don't enter 1.
- D3~D0: Identify the data length of CAN frame.

Frame structure description of the frame ID

In the CAN frame structure picture, "1" represents the frame ID: the length is 4 bytes, the valid bit of standard frame is 11 bits, and the valid bit of extend frame is 29 bits.

Frame structure of the frame ID as follow:

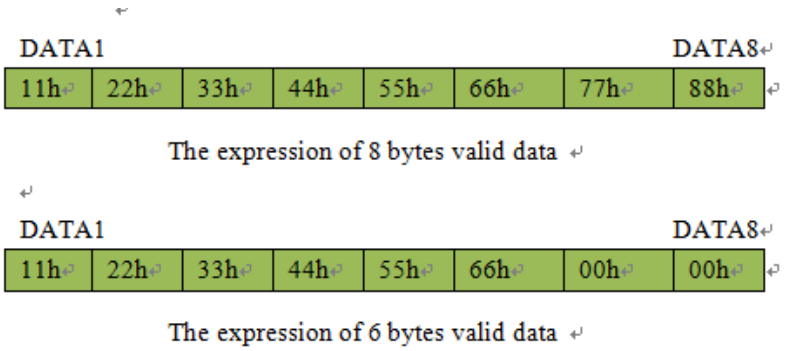


The expression of extended frame ID 0X12345678

The expression of standard frame ID 0X3FF

Frame structure description of the frame data

In the CAN frame structure picture, "3" represents frame data: the length is 8bytes, and the valid length depends on the D3~D0 value of the frame information.



The expression of 8 bytes valid data

The expression of 6 bytes valid data

Following example is an extended data frame, ID is 0X12345678, and it includes the frame expression of 8 bytes data (11h, 22h, 33h, 44h, 55h, 66h, 77h, 88h):

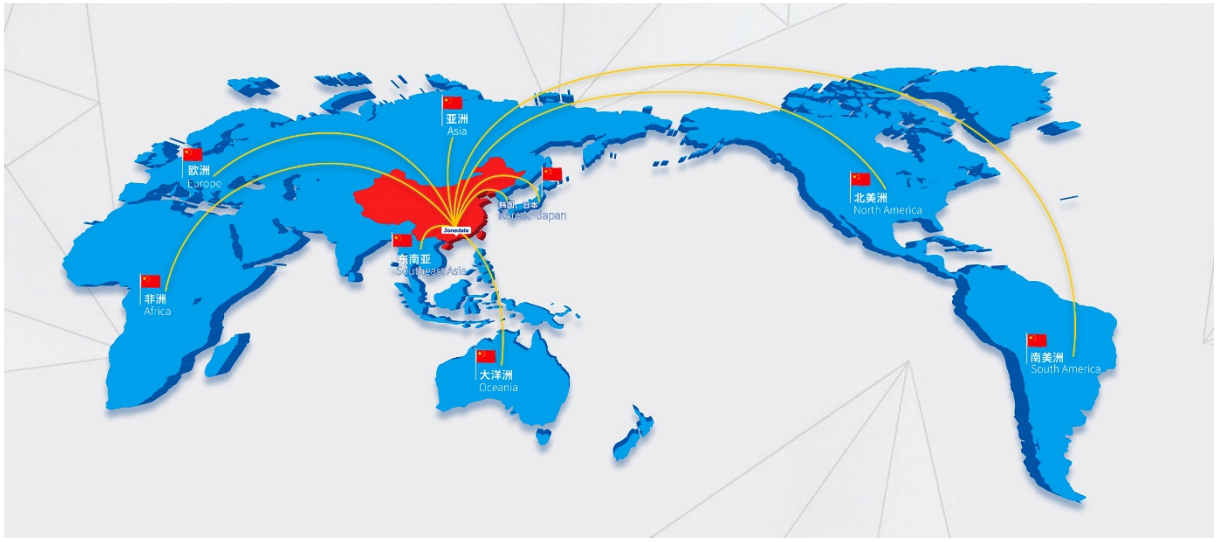
88h	12h	34h	56h	78h	11h	22h	33h	44h	55h	66h	77h	88h

Following example is a standard data frame, ID is 0X3FF, and it includes the frame expression of 6 bytes data (11h, 22h, 33h, 44h, 55h, 66h):

06h	00h	00h	03h	FFh	11h	22h	33h	44h	55h	66h	00h	00h

When the user adopts PC host to send UDP frame, the frame number that each UDP frame includes can't surpass 50 frames. And the UDP frame sending speed is supposed not to surpass 400 frames per second. In addition, it's assumed that user sends 400 UDP frames per second, and each UDP frame contains 50 CAN frames, the frame sending speed is 20000 CAN frames per second, CAN server can't send data in such a speed even in 1000Kbps baud rate. so the sending UDP frame number per second is advised not to surpass 400 frames, and the speed of UDP frame transferred to CAN frame not to surpass 4000 frames per second.

3onedata



3onedata Co., Ltd.

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