Overall analysis KC868-H8&H32 device communication protocol

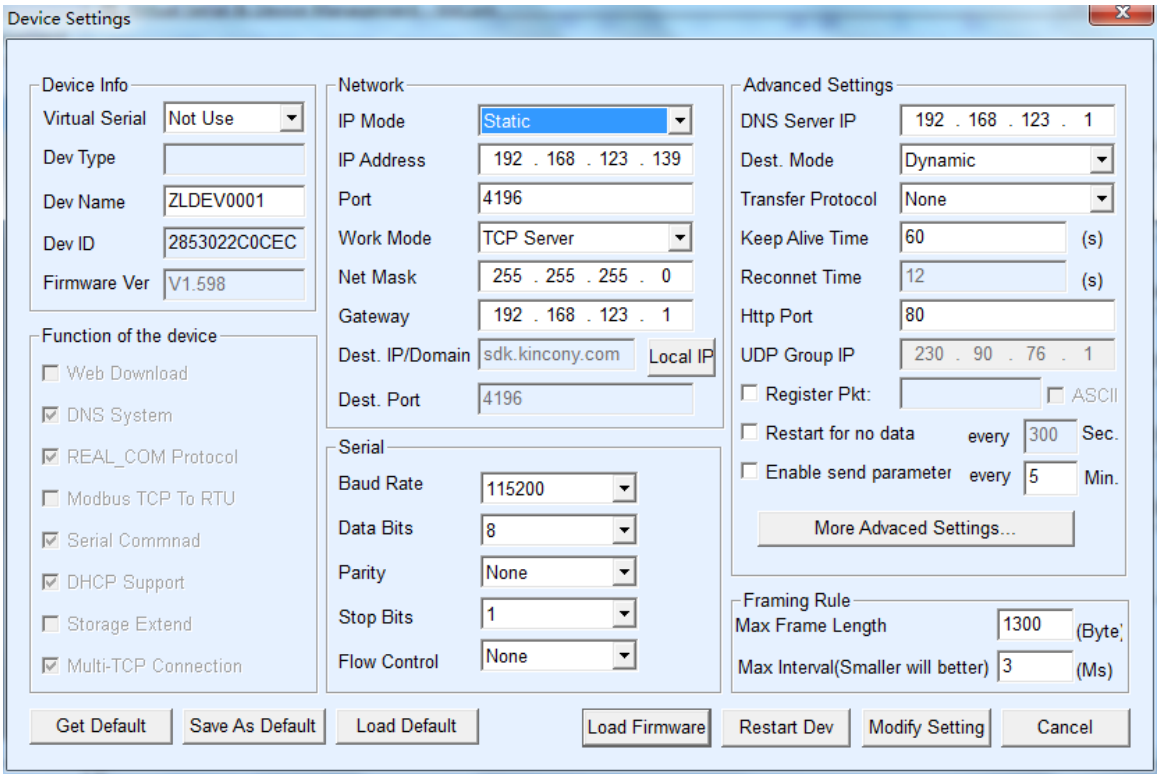
Now, we will start to overall analyze the device communication protocol, and check how it is communicated with the other devices. The KC868-H8 and KC868-H32 are the different models with different quantities relay. The protocol is general used.

KC868-H8

KC868-H32

First, we list all the content of the communication protocol. All of the below, when the device is set into “TCP serve” mode through the Ethernet configuration tool, It can be controlled to communicate by the PC client software. The default IP address and Port number of the device are 192.168.1.200 and 4196.

We can study and debug the protocol via the Ethernet configuration tool, which can be downloaded from Kincony official website: www.kincony.com.

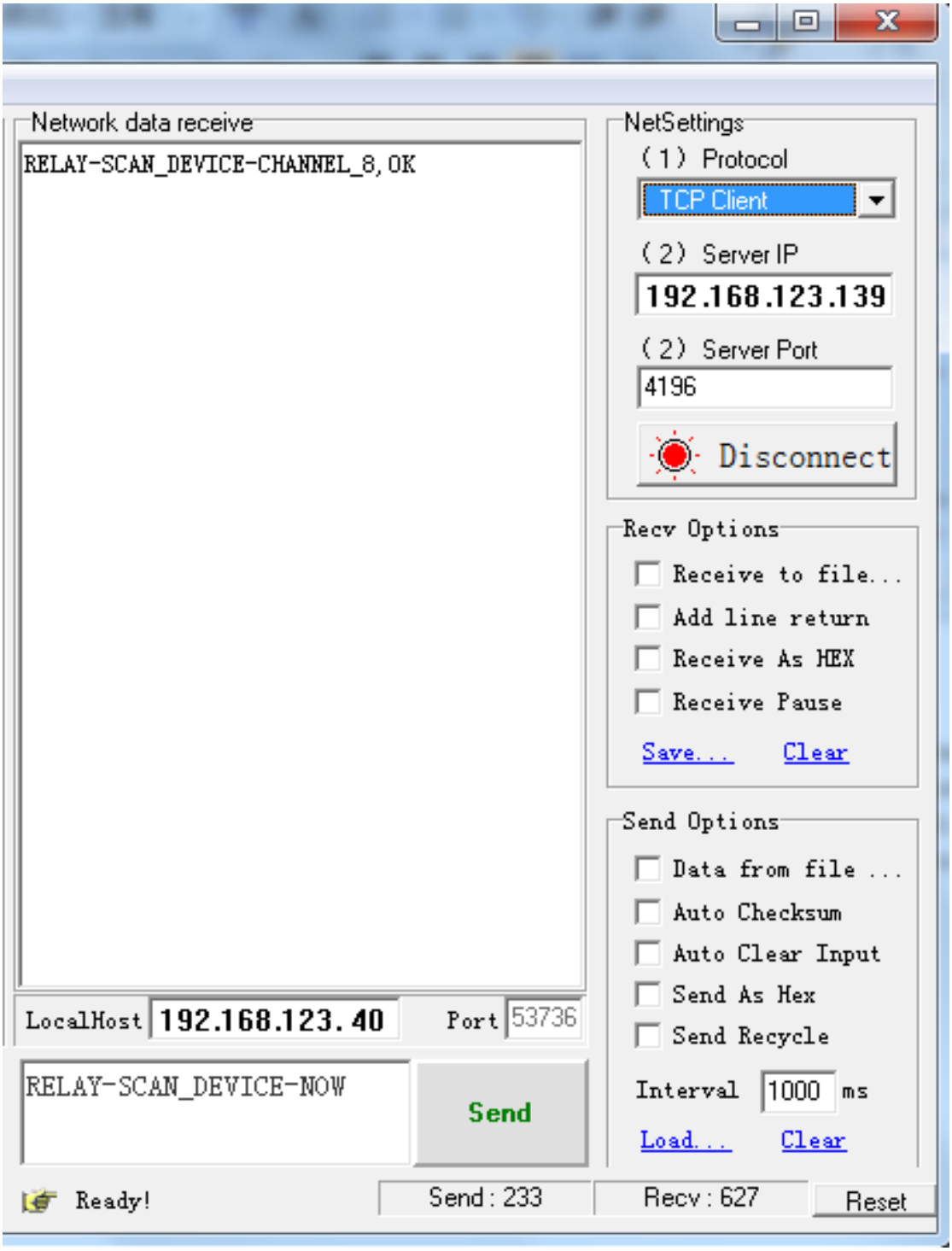


1. Check the device model (as below picture)

Send: RELAY-SCAN_DEVICE-NOW

Return: RELAY-SCAN_DEVICE-CHANNEL_8/CHANNEL_32, OK/ERROR

This is an instruction for checking the device type. When we want to get the type of the current connecting device, we can send the above instruction. And if the connecting device is KC868-H8, it will return “RELAY-SCAN_DEVICE-CHANNEL_8, OK”, if the connecting device is KC868-H32, it will return “RELAY-SCAN_DEVICE-CHANNEL_32, OK, when the command is received successfully

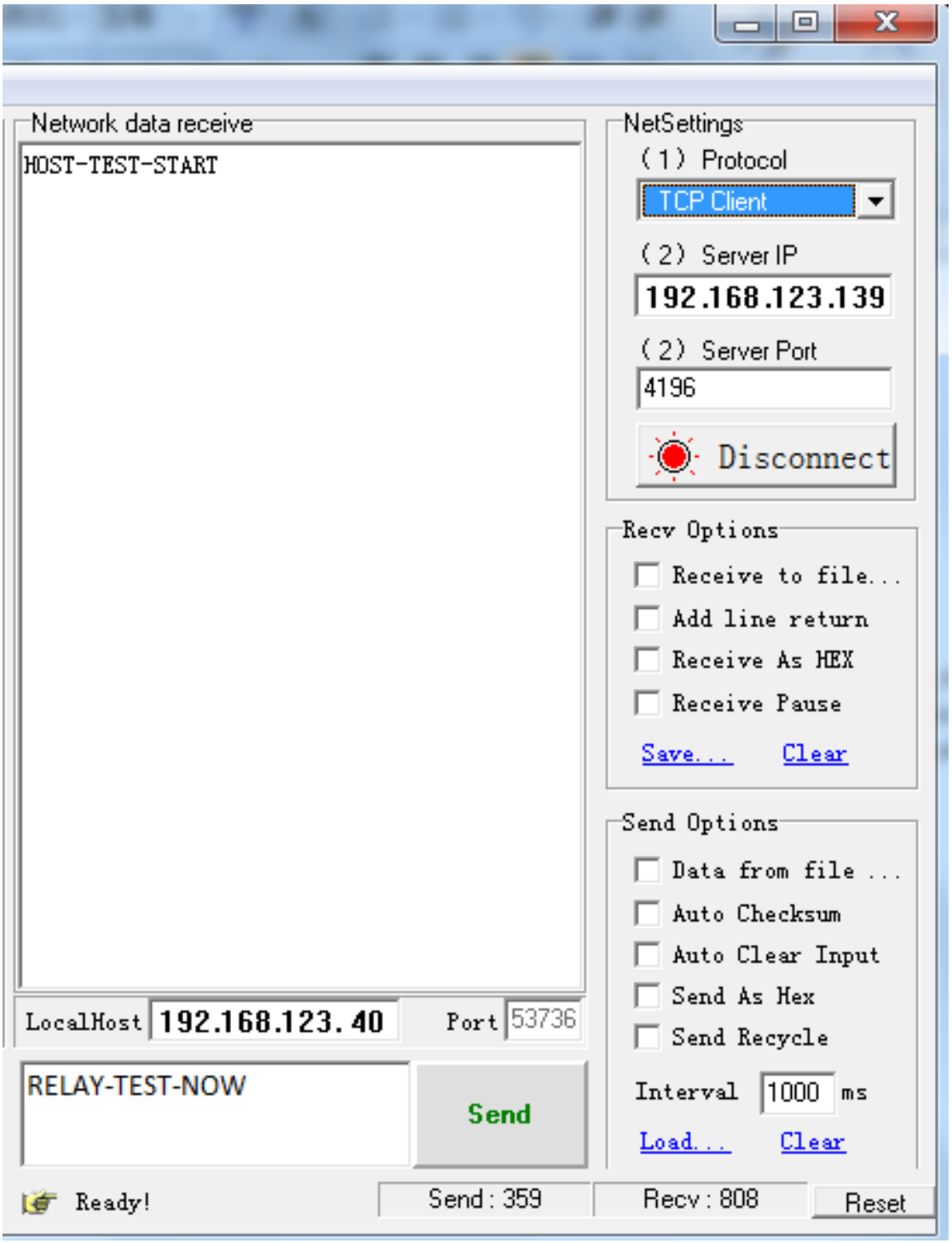


2. Open the working mode of the device server (as below picture):

Send: RELAY-TEST-NOW

Return: HOST-TEST-START

This is the initialization command of the device, when the device is in “TCP Server” mode, this initialization command is required to send to get the device into working mode. After opening the working mode, the “package number” parameter in all subsequent protocols can be used with a fixed number, we will describe again in the following protocol resolution.



3. Command set of device initialization:

Send: RELAY–SCAN_DEVICE–NOW

Send: RELAY-TEST-NOW

This is the initialization command set. After each power up for the device, these two commands must be sent firstly to initialize the device. The return value of the commands had been described above. Once the “relay-test-now” command is sent and the “host-test-start” string is returned, the device can be controlled freely.

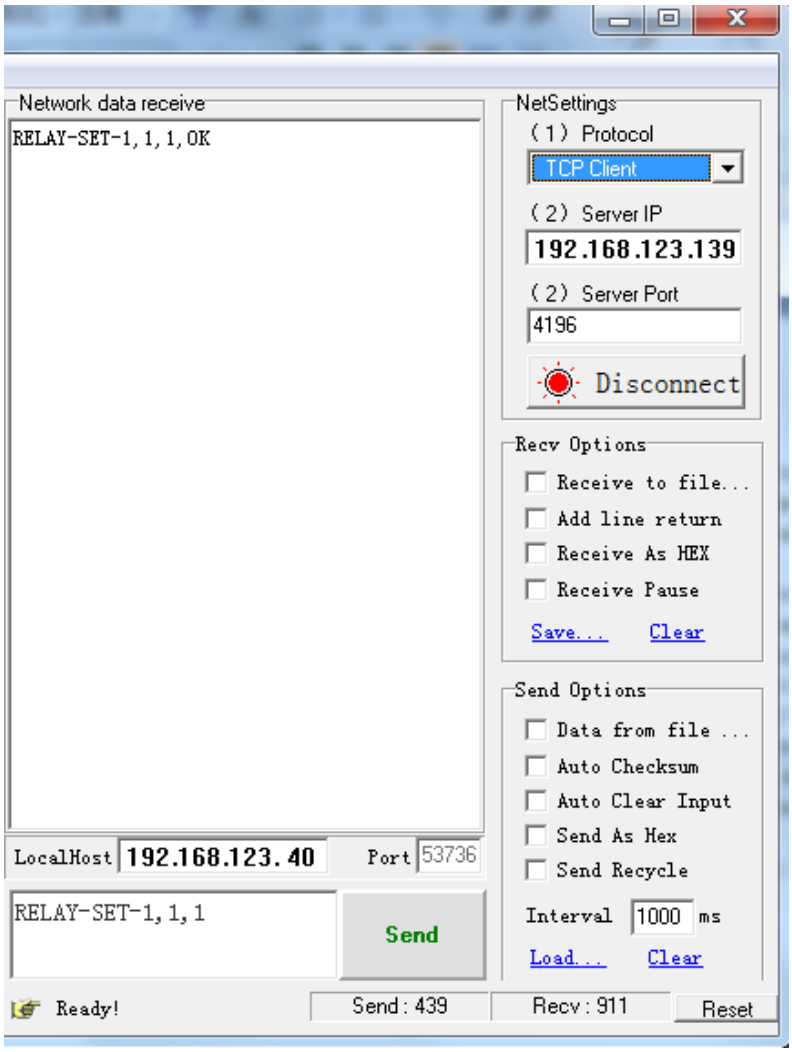
4. Separately control one relay to be on and off:

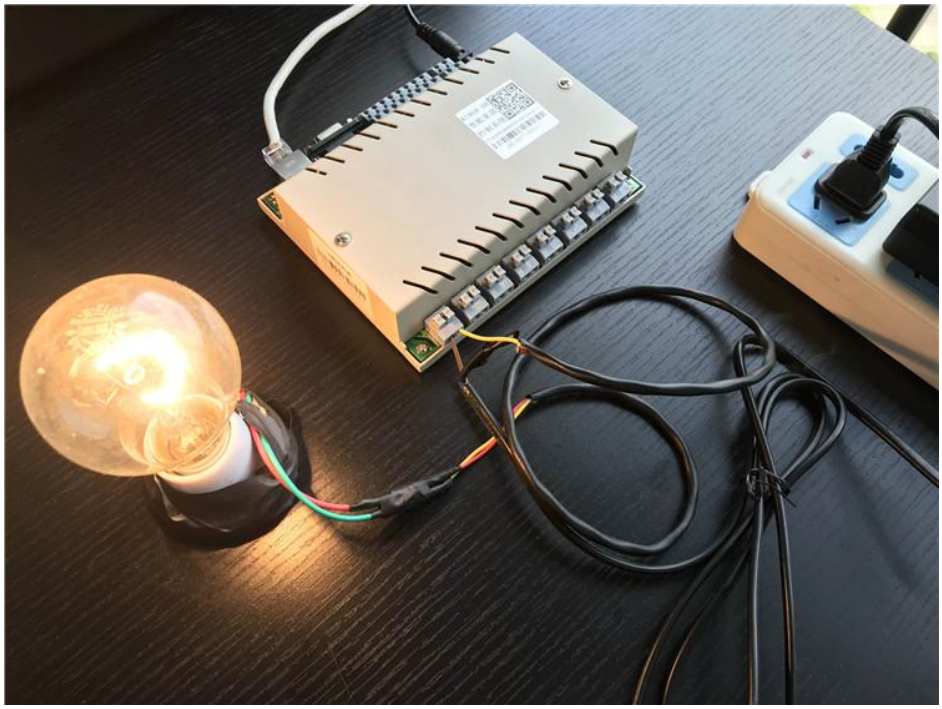
Send: RELAY-SET-x (1 byte pack_num), x (1 byte relay serial number), x (1 byte action 0 / 1) Return: RELAY-SET-x (1 byte pack_num), X (1 byte relay serial number), x (1 byte action 0 / 1), OK/ERROR

This command is the core directive we have introduced in the first part of the article, and is also the most exciting hardware version command of the “hello world”, which can control the opening or closing of one relay, and is very simple and easy to understand.

The first parameter, pack_num, as we mentioned earlier, is meaningless when the device is under "TCP server"

mode, For example: we can set the number "1" to fix. You might wonder, if it is a useless parameter, why it is still kept in the instruction as a parameter that is meaningless. Well, the real meaning of "package number" will be reflected in the remote control mode, our tutorial is not covered yet, we will use it in the later "remote control mode" tutorial.
The third byte parameter in the protocol-"action 0/1": "0" means "off" and "1" means "on". For example: if we want to turn on the first relay, we can send the command "relay-set-1,1,1", the first parameter "1" is a fixed package number, The "1" of the second parameter represents the first relay, and the third parameter "1" means "on".
If we want to turn off the first relay, we can send the command "relay-set-1,1,0", the first parameter "1" is a fixed package number; The second parameter "1" indicates the first relay and the third parameter "0" means "off". If we want to turn on the second relay, we can send the command "relay-set-1,2,1", the first parameter "1" is a fixed package number; The second parameter "2" indicates the second relay and the third parameter "1" means "on".
Now, you should feel how easy it is to control the relay. A little bit of accomplishment :)





5. Separately check the current switch status of one relay (as below picture):

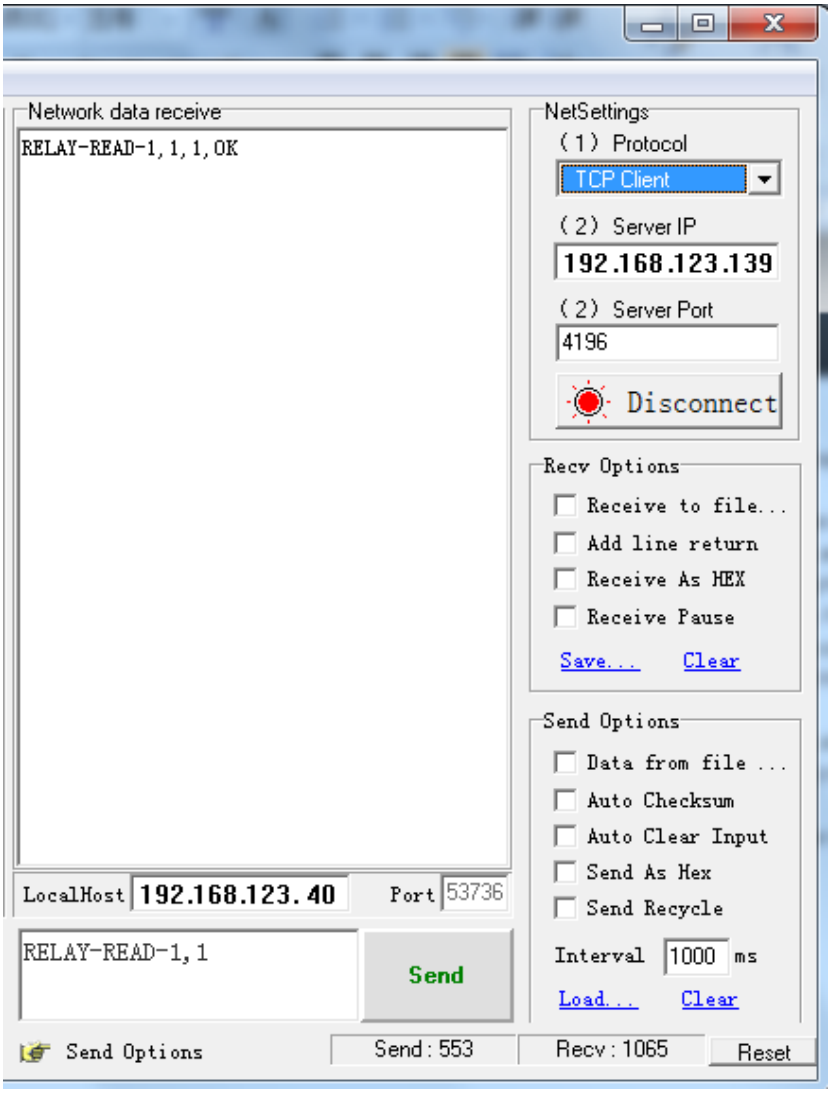
Send: RELAY-READ-x (1 byte pack_num), x (1 byte relay sequence number)

Return: RELAY-READ-x (1 byte pack_num), x (1 byte relay sequence number), x (1 byte status 0 / 1), OK/ERROR

When we control the device to open and close, then open and close again, and then…. we may already have no idea of the current state of the relay after long time, and sometimes we need to know their current status with “open” or “close” before doing the control, . At this time, we can use the relay's checking command to make a query. For example, if we want to know whether the first relay is in "open" or "close" state, we can send: "relay-read-1,1", the first parameter "1" represents the fixed pack number, and the second parameter "1" represents the number of the relay to be queried.

At this time, after the query is successful, the device returns the "relay-read-1, 1, ok", and the second parameter "1" represents the current state as the "open" state, and if it is the "0", the current state is the "close" state.

If you want to check the other relays, you can directly change the sequence number of the relays.



6. Checking trigger input status:

Send: RELAY-GET_INPUT-x (1 byte pack_num)

Return: RELAY-GET_INPUT-x (1 byte pack_num), x (1 byte state), OK/ERROR

Note: when the input terminal of the device is triggered, it will proactively report a command in the format: RELAY-ALARM-X, X represents the number of the input terminal triggered.

The input terminals of the device are used to connect the switching value signals. See the parts on the below picture, the high and lower terminals combine into a set of switching value inputs.

It has a wide range of practical applications. You can define that the outputs relay will do what actions when there is triggered signal inputting. You can connect one switch or one switching value sensor. This is what we usually call intelligent linkage. It is also one of the most widely used methods in smart home.

In the automated control process, the first step is to obtain the state of the trigger event, that is, when it is triggered and which input terminal is triggered. Then we can use the trigger input checking command to check, for example: send "RELAY-GET_INPUT-1" to the device KC868-H8, when sending successfully, the device will return: "RELAY-GET_INPUT-1, 255, OK". The parameter of "255" is the state byte of the all 8 input terminals. We use 8-bit binary to represent the state of the 8 inputs. "0" is for "triggered" and "1" is for "not triggered".

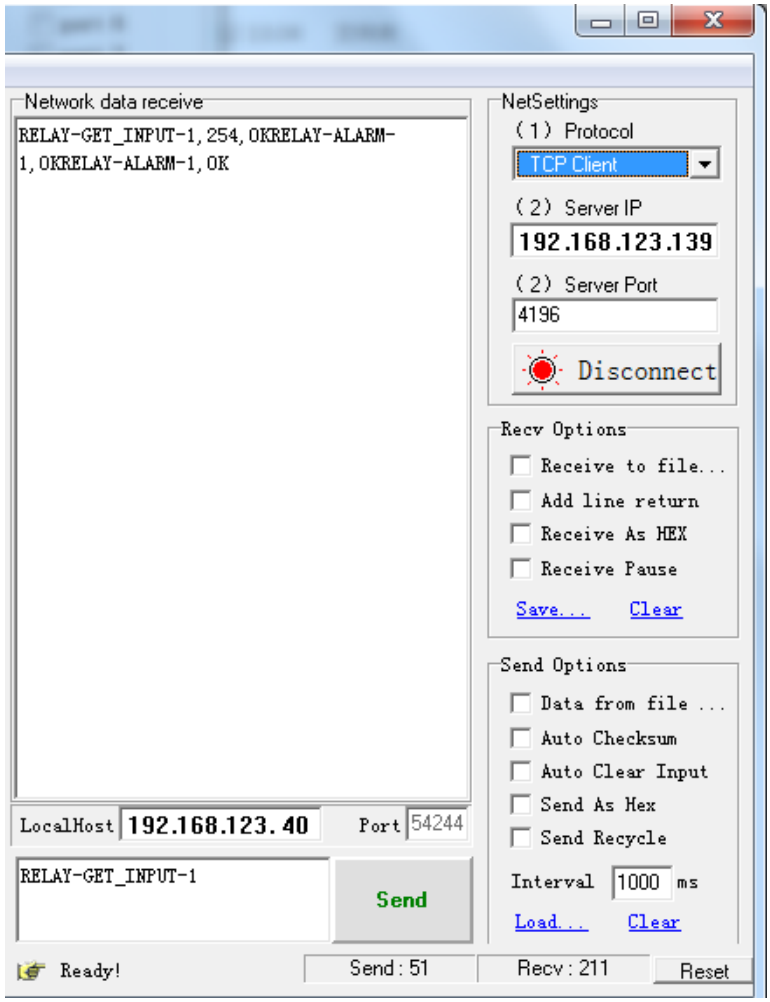
If the states of all the 8 inputs are "not triggered," then the input state is 11111111, note that the number "1" is under the binary, and then we convert the 8-bit “1” to a decimal number, which is the number "255".

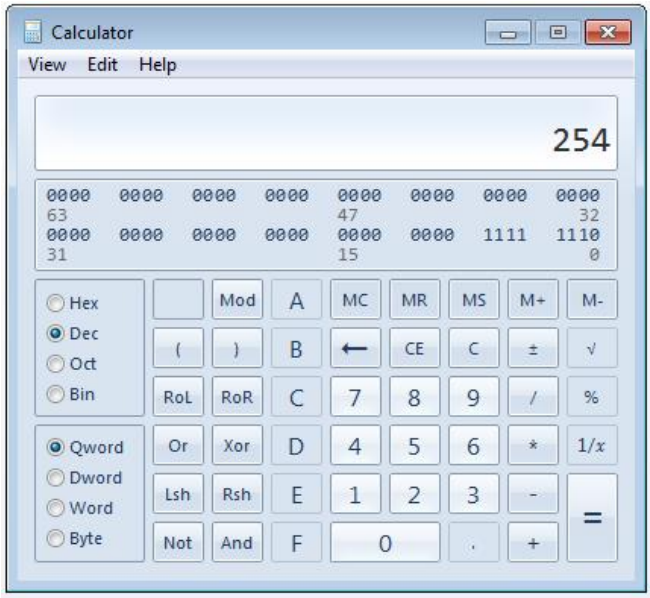
If the state of all the 8 inputs is all "triggered," then the input state is 00000000. As the same, the number "0" is under the binary, and we convert the 8-bit “0” to a decimal number, which the number is also "0".

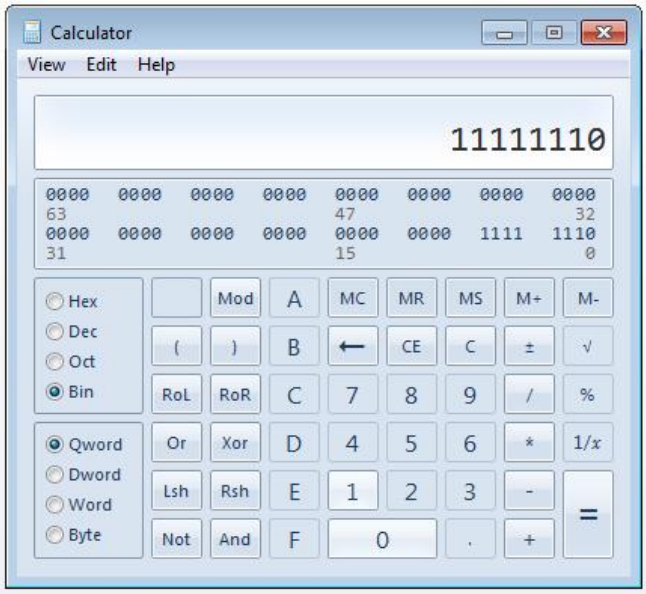
If the state is "not triggered" for the inputs 1 to 4 and "triggered" for the inputs 5 to 8, then the input state is 00001111, note that the number of "00001111" is under binary and should be read from right to left. Then we convert

the 8-bit “00001111” to a decimal number, which the number is "15". It means the device will return “RELAY-GET_INPUT-1, 15, OK” for this inputting state.

Actually, we do not need to constantly loop to check the status; we can use the trigger active reporting command to check the status. When the trigger signal is generated, the client receives the “RELAY-ALARM-x” instruction string, and then sends another instruction string "RELAY-GET_INPUT-x" for checking the status. As shown in the following figure, when we manually short the input of the first input terminal with tweezers, the device KC868-H8 proactively reports the string "RELAY-ALARM-1", at this time, we send the state checking command”RELAY-GET_INPUT-1”, the device will return the string”RELAY-GET_INPUT-1,254,OK”, as told above, the number “254” is a decimal number, we convert it into the binary, which is “11111110”, the binary numbers “1” and “0” represent “not triggered” and “triggered”. So we know the first input is status of “0”, which is triggered.







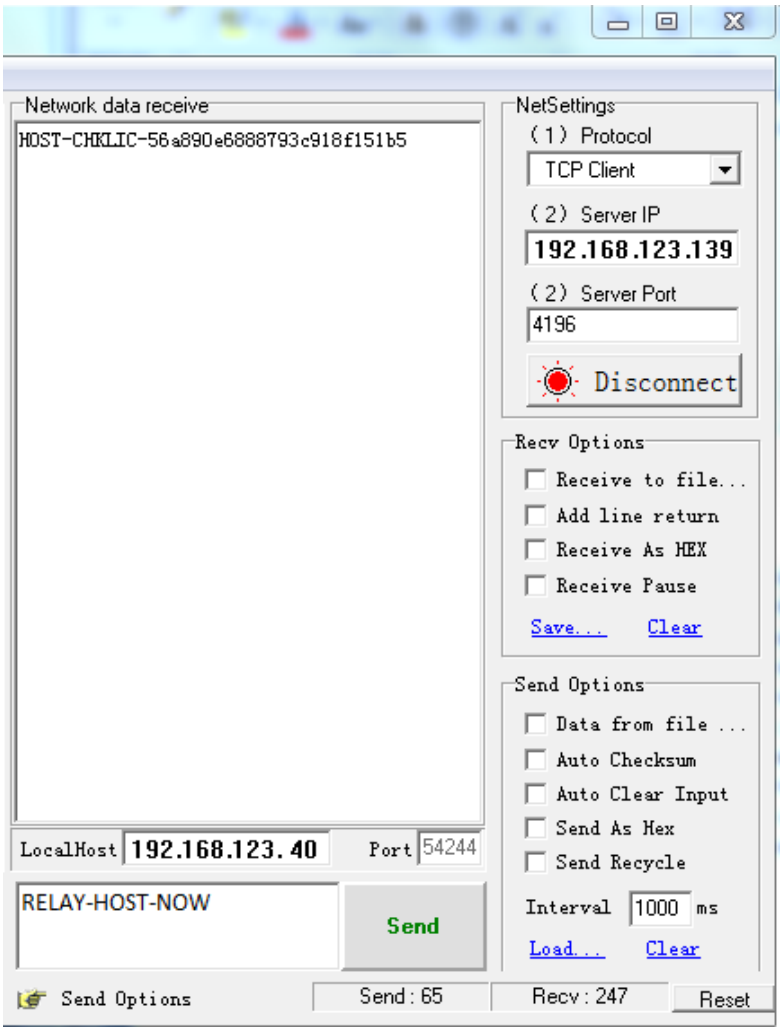
7. Checking the serial number of the device:

Send: RELAY-HOST-NOW

Return: HOST-CHKLIC-56a890e6888793c918f151b5 (return the serial number).

For the maintenance and management, each device has a unique identifier, similar to the ID number of each person.

For example: after sending the command "RELAY-HOST-NOW", the device returns the string " HOST-CHKLIC-56a890e6888793c918f151b5" , the "56a890e6888793c918f151b5" is the serial number of the device, which is combined of letter and number. The serial number will also be used in the later tutorial on remote control. At the same time, this is also a test command for the device relay. If this command is sent to the device, all the relays of the device will be opened in turn automatically, and then all relays will be closed in turn.



8. One-time control of multiple relay on and off:

KC868-H8:

Send: RELAY-SET_ALL-x (1 byte pack_num), D0

Return: RELAY-SET_ALL-x (1 byte pack_num), D0, OK/ERROR

KC868-H32:

Send: RELAY-SET_ALL-x (1 byte pack_num), D3, D2, D1, D0

Return: RELAY-SET_ALL-x (1 byte pack_num), D3,D2,D1,D0,OK/ERROR

In the communication protocol described earlier, we have been able to open and close each relay separately. Here, we introduce a command to control multiple relays at the same time. What's the difference between them?

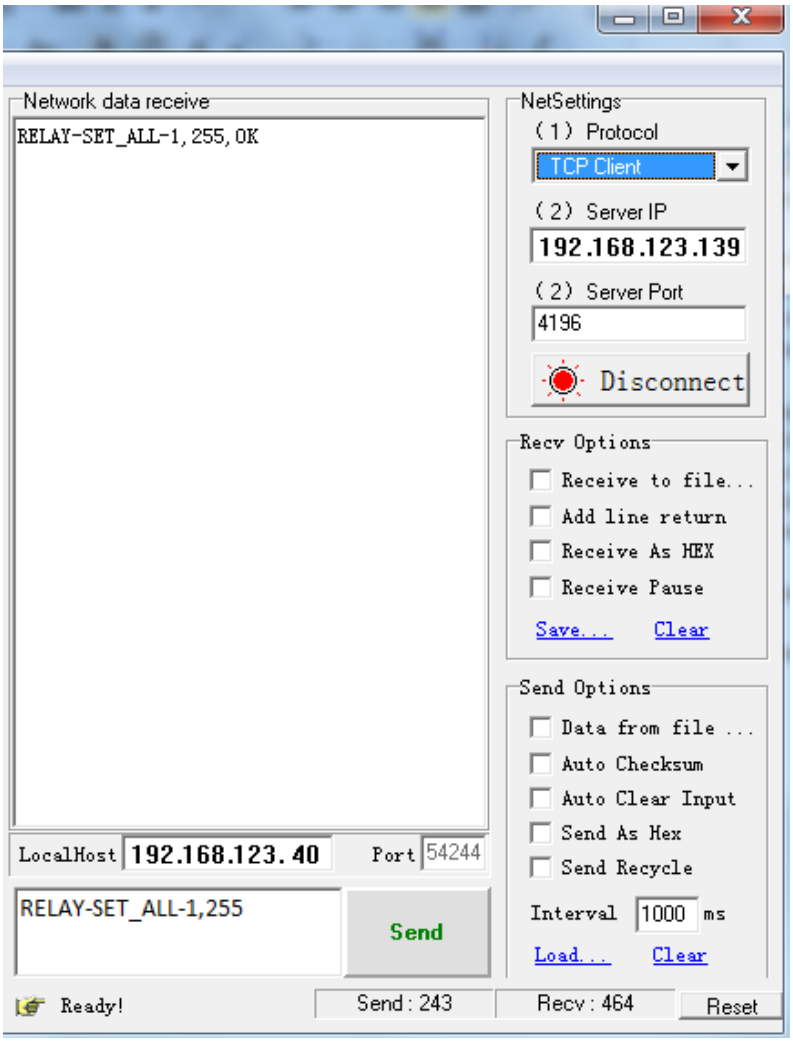
The controlling we mentioned above is for one relay. If we want to control multiple relays together, we need to send multiple control commands and take some time to execute.

Here, the instructions we introduce can achieve a one-time control of multiple relays, such as "all on", "all off," or some "on", some "off", only one command can get them controlled. And the speed of multiplex control is also fast. We can see that in the command, except the "package number" parameter, there is only one parameter left, this byte represents the states of the outputs of the device which will be required to set, and now the "1" for "on," "0" means "off", as the same it is 8-bit binary to indicate the state of each relay, then converted to decimal numbers.

For example: if we want to turn on all the 8-way relays, we can send the command "RELAY-SET_ALL-1,255", we want to turn off all the 8-way relays, then we can send the command "RELAY-SET_ALL-1,0". If you want to turn on the relays of 1 to 4 and turn off the relays of 5 to 8, the parameter is defined as "00001111, converted to the decimal number of" 15 ", and the command is finally sent as" RELAY-SET_ALL-1,15"

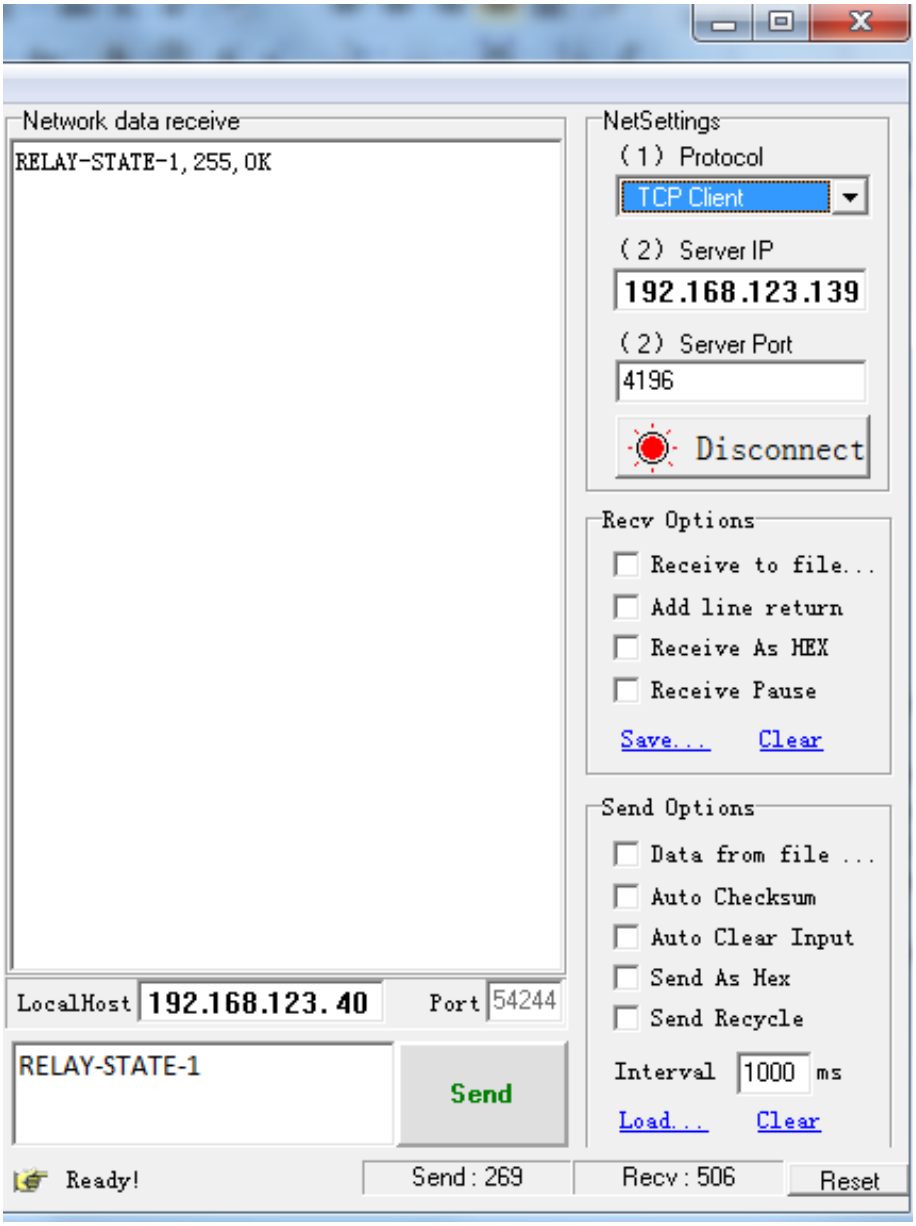
In the content of the protocol, we also see the device KC868-H32, as told above; there are 32-way relays with this model. Similar as the device KC868-H8, just the quantity of the relay is up to 32. In order to operate conveniently,

every 8 relays are controlled with 4 bytes to indicate the status.
It means “D0” is for 8 relays of KC868-H8, but for KC868-H32, “D0” is for the first 8 relays(1 to 8), “D1” is for the second 8 relays(9 to 16) , “D2” is for the third 8 relays(17 to 24), and “D3” is for the forth relays(25 to 32)
The “D0”, “D1”, “D2” and “D3” are with the same meaning for the states of the relays; just the position of the relays is different.
To explain more, for example: “D1” must be a decimal number, which can be converted to the 8-bit binary with “0” and “1”. As told above, the “1” is for “on”, and “0” is for “off”



9. Read multiple relays current switch status at a time:
    Send: RELAY-STATE-x (1 byte pack_num)
    Return:
        DC868-H8: RELAY-STATE-x (1 byte pack_num), D0, OK/ERROR
        KC868-H32: RELAY-STATE-x (1 byte pack_num), D3, D2, D1, D0, OK/ERROR

As similar, we have looked at the communication protocol for checking relay status above, which is checking one relay one time.
Actually, we can also check the states for multiple relays once time. For example: send "RELAY-STATE-1", when the controlling device is KC868-H8, then it will return “RELAY-STATE-1,255,OK”, the number “255” can be converted into the 8-bit binary “11111111”. We already know that the “1” represents the status of “open”. So the return means all the relays of the KC868-H8 are opening.
As the same, when the decimal number from the return is converted into the 8-bit binary with “0”, it means the relay is on “close” state.


Network data receive
RELAY-STATE-1, 255, OK
NetSettings
(1) Protocol
TCP Client
(2) Server IP
192.168.123.139
(2) Server Port
4196
Disconnect
Recv Options
Receive to file...
Add line return
Receive As HEX
Receive Pause
Save...
Clear
Send Options
Data from file ...
Auto Checksum
Auto Clear Input
Send As Hex
Send Recycle
Interval 1000 ms
Load...
Clear
LocalHost 192.168.123.40
Port 54244
RELAY-STATE-1
Send
Ready!
Send : 269
Recv : 506
Reset