



High-Performance, Enhanced Security Network Time Server

## Manual of NTP Server

High-Performance, Enhanced Security Network Time Server



Contact Us:

**GFClock Yasapersada**

Address:

Jl. Pejaten Raya No.12a Pejaten Barat, Pasar Minggu, Jakarta Selatan 12510

Website: [www.gfclock.com](http://www.gfclock.com) Email: [gfclock.yasapersada@gmail.com](mailto:gfclock.yasapersada@gmail.com) Call: 0821-146 117 32



## Table of Contents

1. Device Appearance.....	1
2. Hardware Installation and Debugging.....	1
2.1. Device Structure.....	1
2.2. Outdoor installation.....	2
2.3. Indoor installation.....	3
3. Device Operation.....	4
3.1. Indicator Light Status.....	4
3.2. Panel Display and Keyboard.....	4
3.2.1. The Main Panel Display.....	4
3.2.2. Panel Login.....	5
3.2.3. Menu Introduction and Operation.....	5
3.2.2.3.1. View and Modify Network Configuration.....	5
3.2.2.3.2. Enabling, Disabling, and Modifying Bonding Configuration.....	8
3.2.2.3.3. Checking the NTP Service Status.....	9
3.2.2.3.4. Checking the Satellite and Antenna Status.....	9
3.2.2.3.5. Viewing and Modifying the Time Zone.....	9
3.2.2.3.6. Modifying the Satellite Receiving Mode.....	10
3.2.2.3.7. Modifying the Device Panel Password.....	10
3.2.2.3.8. Disabling and Enabling the SSH Service.....	10
3.2.2.3.9. Viewing the System Status.....	11
3.2.2.3.10. Viewing Device Information.....	11
3.3. Client Configuration.....	11
3.4. Server Configuration and Debugging.....	13
4. Remote Management and Monitoring.....	14
4.1. Login Information.....	14
4.2. HTTP/HTTPS Login.....	14
4.3. SSH Login.....	19
4.4. SFTP Login.....	19
5. Common Malfunctions and Maintenance.....	20
5.1. Common Malfunctions.....	20
5.1.1. The time displayed on the time server is incorrect after power on.....	20
5.1.2. All indicator lights do not turn on after power on.....	20
5.1.3. The device cannot receive satellites for a long time.....	20
5.1.4. Cannot ping the time server after configuring the network.....	21
5.1.5. Satellite reception is unstable, and sometimes the device enters a hold state.....	21
5.1.6. The client cannot receive time synchronization services.....	21
5.1.7. How to configure network devices to receive time synchronization services.....	21
5.2. Daily Maintenance.....	22

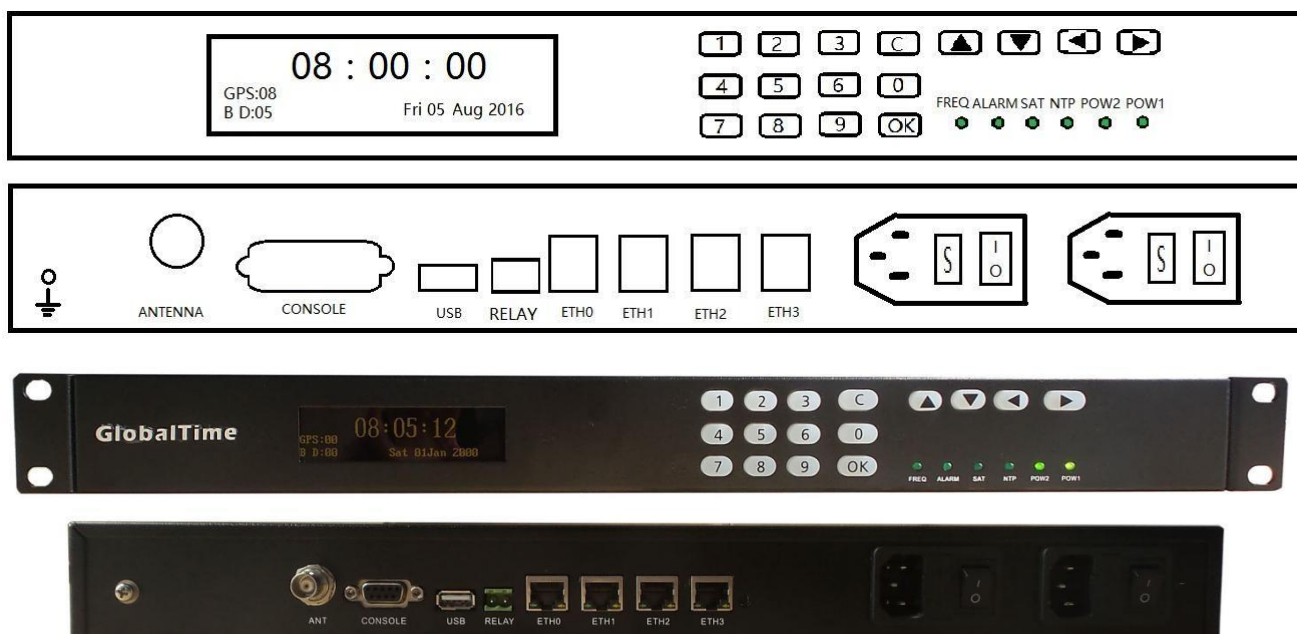


## High-Performance, Enhanced Security Network Time Server

---

5.2.1. Purpose .....	22
5.2.2. Checklist .....	22

## 1. Device Appearance



- OLED display with 64x256 resolution in green, displaying device basic status and current time.
- Sixteen-key keyboard for viewing and modifying system configuration.
- Six status lights indicating satellite, NTP and other service statuses, as well as power supply for two power sources.

The device panel is shown in the above figure. There are two power sockets with fuses on the back panel. After opening the fuse socket, there is one primary and one backup fuse, making it convenient for customers to replace them. The fuse specification is 0.5A.

The antenna socket is a 50-ohm BNC female socket.

There are 4/2/1 10M/100M/1000M adaptive Ethernet ports and one serial port for monitoring.

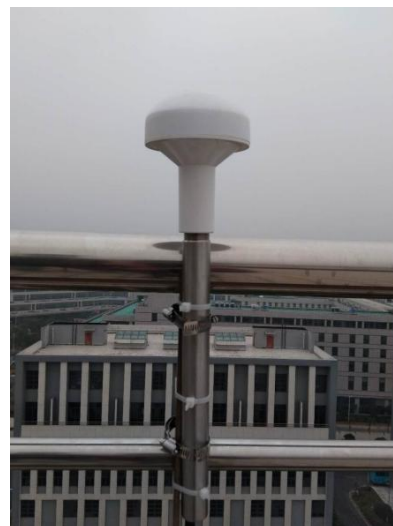
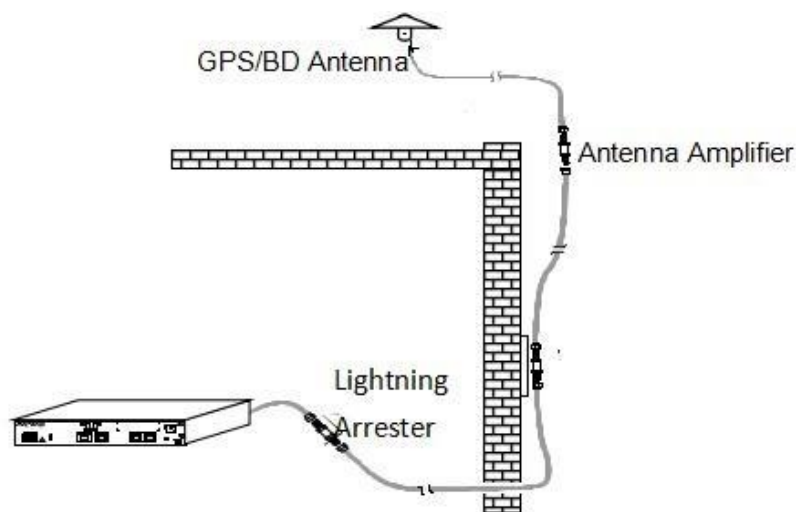
There is an antenna input port and a handheld device input port.

There is a USB host interface for program upgrades and configuration backups.

A dry node relay triggers an alarm.

## 2. Hardware Installation and Debugging

### 2.1. Device Structure



GPS Antenna

The NTP time server consists of an outdoor part and an indoor part.

The outdoor part mainly consists of a GPS/BDS satellite receiving antenna, a lightning arrester, and an antenna amplifier (optional). Its function is to receive satellite signals.

The indoor part is the main device of the NTP time server, which completes satellite signal demodulation, local clock calibration, and implementation of the NTP protocol. It provides NTP time service to other network devices through Ethernet ports.

Below are detailed introductions to the installation of the indoor and outdoor parts.

## 2.2. Outdoor installation

The outdoor part of the NTP time server consists of a GPS/BDS satellite receiving antenna, lightning arrester, and antenna amplifier (optional), which are responsible for receiving satellite signals. The indoor part is the main equipment of the NTP time server, which completes satellite signal demodulation, local clock calibration, NTP protocol implementation, and provides NTP time service to other network devices through the network port.

The following are detailed instructions for the installation of the indoor and outdoor parts.

The outdoor part of the NTP time server consists of a GPS/BDS satellite receiving antenna, transmission cable, and antenna amplifier. The installation precautions are as follows:

Firstly, the installation position of the antenna should be carefully selected as it has a significant impact on the equipment's operation. The antenna should be installed in a high and unobstructed location, such as on the roof, and the sky above should be open. For optimal performance, the elevation angle should be maintained at 15 degrees or more without obstruction. It is useless to install the antenna indoors as GPS/BDS satellite signals are very weak and cannot be received indoors. Tree cover or plastic rain shelter above the antenna generally has little effect, but other obstructions have a significant impact on the signal. In fact, placing a book on the antenna can completely block the satellite signal.

During antenna installation, it should be positioned lower than the lightning rod or other buildings

## High-Performance, Enhanced Security Network Time Server

that attract lightning and at a distance of 10-15 meters from them. GPS/BDS antennas themselves are rarely struck by lightning but are often damaged due to the strong induced electric field from surrounding buildings (lightning rods, towers, etc.) being struck. A lightning arrester can be installed on the cable. The lightning arrester should be installed at the position where the cable enters the wall, making it easier to ground properly. The lightning arrester is installed between the feeder cable and the equipment, and the ground wire is led out from the lightning arrester to the ground pole. The ground resistance of the ground pole should be below 4 ohms, and it must be firmly connected to ensure reliable discharge during lightning strikes.

Sometimes the antenna can be installed outside a window, which requires the building around it to be open and without corners, so at least half of the sky's satellites can be received. However, as an instrument for long-term use, it is strongly recommended that the antenna be installed at a high location, and installation outside a window should only be used for temporary testing.

The area around the GPS/BDS antenna installation position should not have high-power microwave transmitters operating on the same frequency band, and other high-power electromagnetic radiation on other frequency bands should be avoided from directly irradiating the GPS/BDS antenna.

If the length of the feeder cable between the antenna and the equipment is less than 100 meters, it can be connected directly. If it is between 100 and 200 meters, a line amplifier should be added. If it is between 200 and 300 meters, two line amplifiers should be added. For longer feeder cables, please contact the engineering staff as we have a specialized plan. Longer feeder cables usually use the 1/2 inch RF cable from the American Andrew company, and the loss of this cable is 12.8 dB/100 m.

The main precautions during the installation of the feeder cable are:

Do not bend it too much, which can cause the conductor inside the feeder to break.

When the feeder cable enters the room, it should be bent into a U-shape to prevent water from pouring in.

Frequency Range:	1575 +/- 50MHz	RF Connector:	N Type
Polarization Mode:	Right Handed circular polarization	Installation Method:	Screw (M24 x 1.5) Connector
Antenna Gain:	≥3.5dB	Volume:	∅96 x 126mm
Amplifier Gain:	≥37dB	Operating Temperature:	-45°C to 85°C
Noise Figure:	≤1.5dB	Storage Temperature:	-50°C to 90°C
Interference Suppression:	25dB( f0+/- 100MHz)	Humidity:	0 to 100%
Power Consumption:	3V x 20mA		

Technical Index of Antenna

### 2.3. Indoor installation

After connecting the main device to 220V AC power, the "power" indicator light on the front panel of the device should light up, indicating that the power part of the device is working normally. At this time, when measuring the BNC socket of the antenna with a multimeter, there should be a 5V

## High-Performance, Enhanced Security Network Time Server

feeding voltage. Connect the antenna cable to the "antenna" socket. Then configure the IP address and other network settings of the time server through the keyboard and display menu, save and exit, and then restart the NTP time server to make the network settings take effect. After the restart, ping the IP address of the server on another computer to check whether the network settings are correct. Then observe the satellite reception status, server time tracking status and other information. When the server has locked the satellite time (the "NTP" light on the panel turns green), NTP8010 can provide time information for other clients in the network. The specific software configuration process can be found in the next chapter.

### 3. Device Operation

#### 3.1. Indicator Light Status

Indicator	Status	Instruction
Power Supply	ON	The power supply is normal
	OFF	The power supply is abnormal
NTP	OFF	The server is unlock and is searching for time source
	GREEN	The time source is locked
SAT	OFF	The satellite signal is not received
	GREEN	The satellite signal is received
FREQ	OFF	No back-up frequency source or OCXO is not used currently
	GREEN	Back-up frequency source is working
Alarm	OFF	Normal
	GREEN	CPU occupation is beyond the limite (70%)

#### 3.2. Panel Display and Keyboard



##### 3.2.1. The Main Panel Display

<1> The current time and date.

<2> The current number of received satellites.

<3> The current NTP service status.

### 3.2.2 Keyboard Operation

#### 3.2.2.1 Operation Instructions

Press the number keys to enter the corresponding menu and submenu. Press the OK key to enter the menu edit mode or confirm the input. Use the direction keys to adjust the input position or flip through pages. Press the C key to return to the previous menu. When in input mode, use the direction keys to adjust the input position. Press the up key to escape to hexadecimal input, and press the down key to escape to decimal point and colon input. Press the OK key to confirm. After modifying the configuration, restart the device for it to take effect.

#### 3.2.2. Panel Login

Press the OK key on the main interface to enter the login state. Enter the password and press OK to confirm. After a successful login, the main menu will be displayed. The initial password is 123456. After a successful login, the main menu will be as follows:



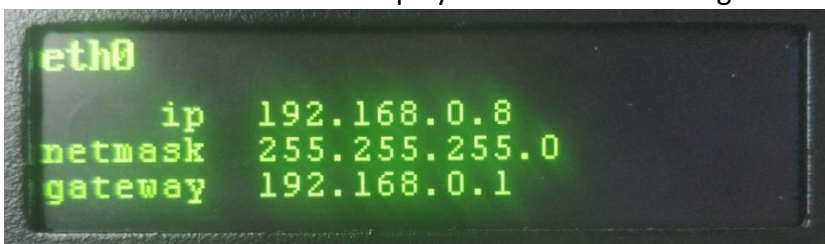
### 3.2.3. Menu Introduction and Operation

#### 3.2.2.3.1. View and Modify Network Configuration

Press the 1 key on the main menu to enter the NETWORK menu, then press 1 key again to enter the ethernet menu, and then press 1 key again to enter the ipv4 menu to configure the ipv4 address. Alternatively, press the 2 key to enter the ipv6 menu to configure the ipv6 address. Finally, press the number key to enter the corresponding network card menu to view the selected network card configuration information. After the configuration is completed, restart the device for the configuration to take effect.

#### IPv4 Address Configuration

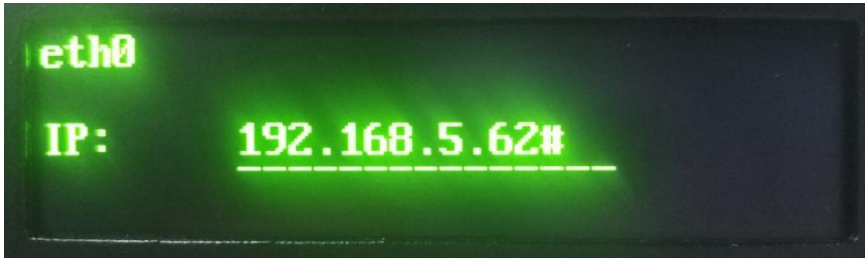
For example, press 1 to enter the NETWORK menu, then press 1 to enter the ethernet menu, then press 1 to enter the ipv4 configuration, and then press 1 to enter the eth0 menu. The configuration information of eth0 will be displayed as shown in the figure below:



## High-Performance, Enhanced Security Network Time Server

Press the OK key to enter the menu edit mode, where you can reset the network configuration. The operation is as follows:

<1> Enter the IP address, and press the down key to escape to the decimal point, as shown in the figure below:



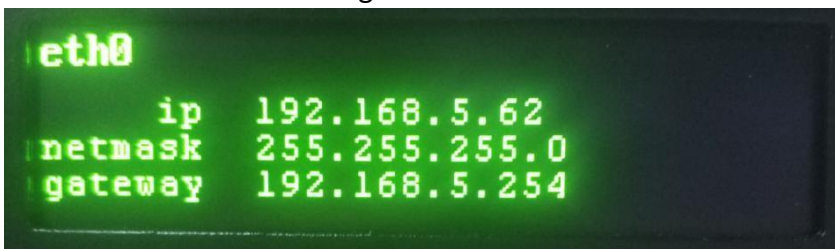
Press the OK key to confirm. If the IP address is entered correctly, you will be prompted to enter the subnet mask. If the input is incorrect, you will be prompted to re-enter the IP address. To enter the subnet mask, follow the steps shown in the figure below:



<3> After confirming the subnet mask input by pressing the OK key, continue to enter the gateway, as shown in the figure below:



<4> After confirming the gateway input by pressing the OK key, the menu will be exited. Press the corresponding number key again to select the network card and check whether the configuration has been successfully modified. When the modification is successful, the screen should display the information shown in the figure below:



### IPv6 address configuration

For example: Press 1 to enter the NETWORK menu, then press 1 to enter the ethernet menu, then press 2 to enter the IPv6 configuration, then press 1 to enter the eth0 menu. If eth0 IPv6 address has already been configured, the eth0 IPv6 configuration information will be displayed. If it hasn't

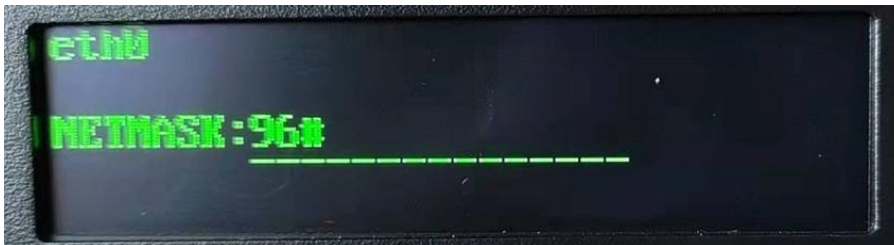
## High-Performance, Enhanced Security Network Time Server

been configured yet, the setting mode will be entered directly, as shown in the figure below:

<1> Enter the IP address. Press the down key to escape to a colon. Press the up key to escape to a hexadecimal number. Use the left and right keys to select the corresponding letter (A/B/C/D/E/F), which will be displayed in capital letters. Press the OK key to confirm the selected character (A/B/C/D/E/F), as shown in the figure below:



<2> Press OK to confirm. If the IP address input is correct, proceed to subnet mask input. If the input is incorrect, a prompt will appear to re-enter the IP address. The number of subnet mask bits can be entered as shown below.



<3> Press OK to confirm the subnet mask input, and then proceed to gateway input as shown below.



<4> After pressing OK to confirm, you will exit the menu. Press the number key again to select the network card and check if the configuration has been successfully modified. The following image indicates that the modification was successful.



### 3.2.2.3.2. Enabling, Disabling, and Modifying Bonding Configuration

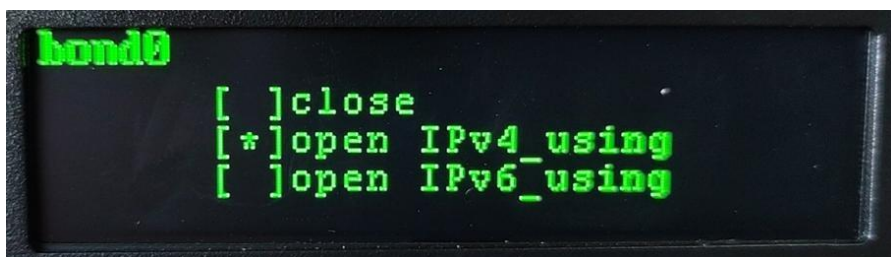
To enable, disable, or modify bonding configuration, first enter the NETWORK menu by pressing 1 in the main menu. Then, press 2 to enter the bond menu, and then press 1 or 2 to enter the bond0 or bond1 menu to configure the bond IP address (bonding mode only supports IPv4 or IPv6, not both at the same time). Then, follow the sub-menu sequence (1->2->3->4) to configure the numeric bond0/bond1.

The following are the steps for each operation:

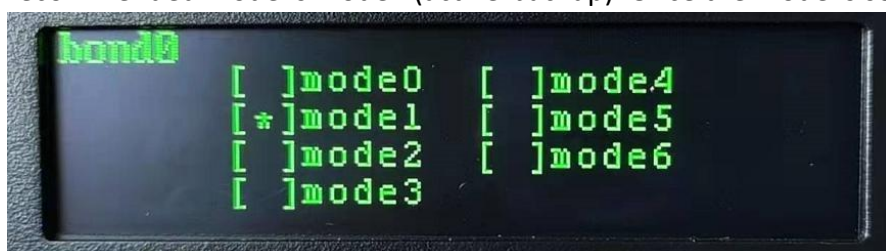
<1> Press 1 to enter the bond (0/1) open/close menu, and use the up and down keys to move the asterisk to select the desired operation.

"close" means closing the bonding function and configuration. "open IPv4\_using" means opening the bonding function while configuring the IPv4 address, and "open IPv6\_using" means opening the bonding function while configuring the IPv6 address.

After completing the configuration, press OK to confirm. If you choose "close," the bond has already been closed and no further action is needed. If you choose "open IPv4\_using" or "open IPv6\_using," please continue with the following operations.



<2> After selecting the bonding to configure, press the 2 key to enter the bond (0/1) mode menu. Use the arrow keys to select the bonding mode, and then press the OK key to confirm. The recommended mode is mode1 (active-backup). Once the mode is set, proceed to the next step.



<3> Press the number 3 key to enter the bond (0/1) network menu for network configuration. The configuration setting for this item is the same as the configuration for a regular network interface. For details, please refer to section 3.2.2.3.1 IP configuration instructions.

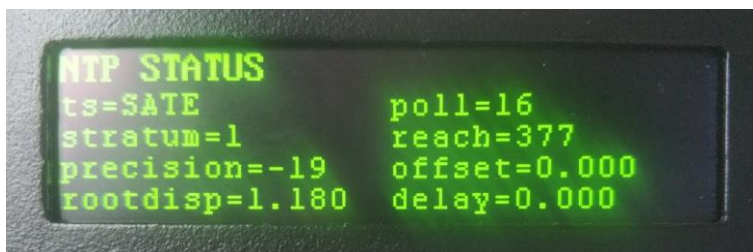
<4> Press the number 4 key to enter the bond (0/1) slaves menu. Use the up and down arrow keys to select the network interfaces that need to be added to the bonding group. Press the OK key to indicate the selection with an asterisk (\*). The number of network interfaces selected for slaves cannot be less than 2, and network interfaces that are already used by another bond cannot be selected again. After completing the selection, move the > symbol to the confirm option and press OK to confirm the bonding configuration.



<5> After completing the configuration, it is necessary to restart the device for the changes to take effect.

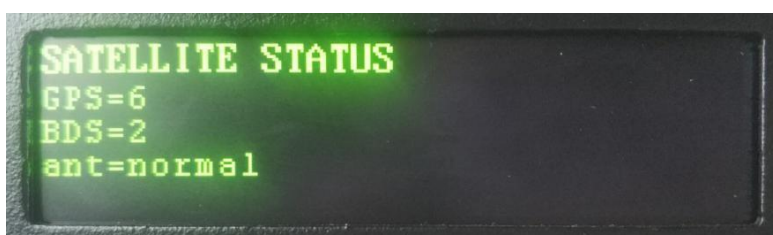
### 3.2.2.3.3. Checking the NTP Service Status

Press the number 2 key in the main menu to enter the NTP STATUS menu and check the status of the NTP service.



### 3.2.2.3.4. Checking the Satellite and Antenna Status

Press the number 3 key in the main menu to enter the SATELLITE STATUS menu and check the status information of the satellite and antenna.



### 3.2.2.3.5. Viewing and Modifying the Time Zone

Press the number 4 key to enter the SYSTEM INFORMATION menu, then press the number 1 key to enter the timezone menu. The arrow points to the current time zone, as shown in the figure below:



If you need to modify the time zone, use the up and down arrow keys to select the corresponding time zone, and then press the OK key to confirm the modification of the time zone.

### 3.2.2.3.6. Modifying the Satellite Receiving Mode

Press the number 4 key to enter the SYSTEM INFORMATION menu, then press the number 2 key to enter the sat mode menu. The asterisk indicates the current satellite receiving mode, as shown in the figure below:



If you need to modify the satellite receiving mode, use the up and down arrow keys to select the mode, press the OK key to confirm, and the system needs to be restarted for the changes to take effect.

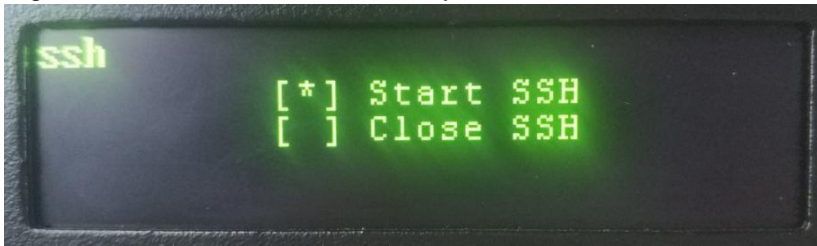
### 3.2.2.3.7. Modifying the Device Panel Password

Press the number 4 key to enter the SYSTEM INFORMATION menu, then press the number 3 key to enter the new password menu. Modify the device panel password, which is a combination of numbers of less than 8 digits.



### 3.2.2.3.8. Disabling and Enabling the SSH Service

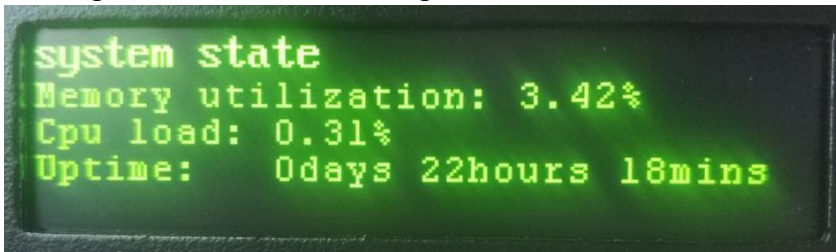
Press the number 4 key to enter the SYSTEM INFORMATION menu, then press the number 4 key to enter the ssh menu, and disable or enable the ssh service. The asterisk indicates the current status of the ssh service, as shown in the figure below:



If you need to enable or disable the ssh service, use the up and down arrow keys to select the corresponding function, and press the OK key to confirm.

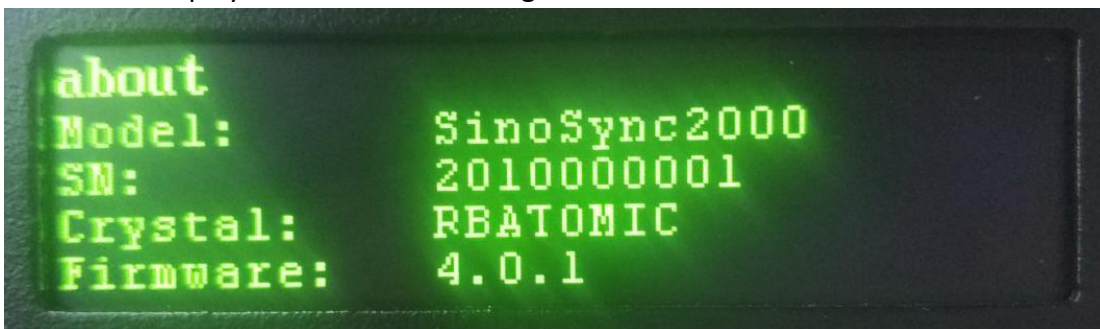
### 3.2.2.3.9. Viewing the System Status

Press the number 4 key to enter the SYSTEM INFORMATION menu, then press the number 5 key to enter the system state menu. It can display the current memory usage, CPU load, and system running time. As shown in the figure below:



### 3.2.2.3.10. Viewing Device Information

Press the number 4 key to enter the SYSTEM INFORMATION menu, then press the number 6 key to enter the about menu. The device model, serial number, crystal oscillator type, firmware version, etc. will be displayed. As shown in the figure below:



## 3.3. Client Configuration

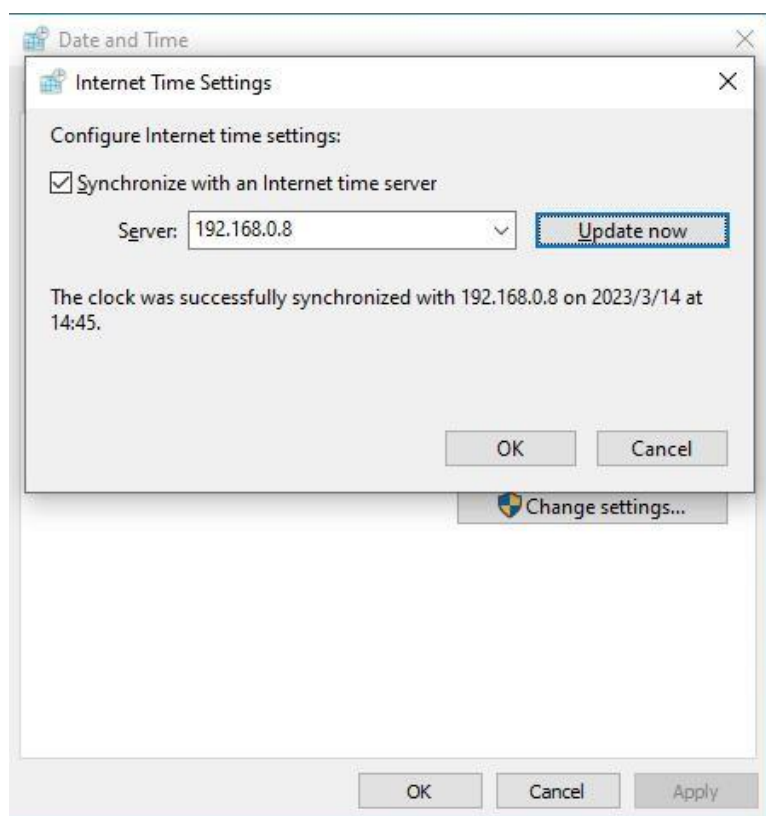
For WinXP/2003, the system includes the NTP service, which can be set directly. The specific method is as follows:

Step 1: Double-click on the time mark on the right side of the Windows taskbar to bring up the date and time properties interface. Select the Internet Time interface, as shown in the image below.

## High-Performance, Enhanced Security Network Time Server

Step 2: Modify the default time server for Windows, such as changing it to 192.168.2.8.

Step 3: Click "Apply", and then click "Update Now". After synchronization is successful, it will display "Succeeded to synchronize time with \*\*\*\*\* at year/month/day, hour:minute. Next synchronization: year/month/day, hour:minute". By default, Windows synchronizes once a week. If the interface displays "RPC not available", open the control panel, select Administrative Tools/Services, search for "Windows Time" from the list of services, and select "Start service automatically and start service".



Step 4: If you think that synchronizing once a week is too long, you can modify the registry to shorten the synchronization interval. The specific registry item is located at: `\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpClient\SpecialPollInterval`. The default value is 604800 = 60 × 60 × 24 × 7, which is one week. To synchronize once a day: 86400 To synchronize once an hour: 3600 To synchronize every ten minutes: 600

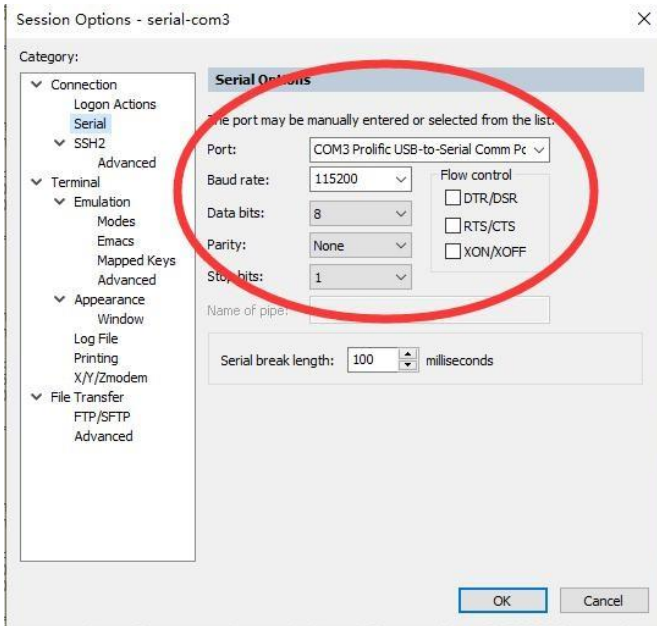
Step 5: After modifying the registry, you need to stop the Windows Time service and then restart it so that the time interval can be updated. If you have previously installed other time synchronization software, you need to uninstall the software and then restart the computer to ensure that the Windows time service works properly.

For Windows 2000/98 operating systems, use our company's time synchronization software or third-party time synchronization software. Refer to the respective user manual for specific settings. For UNIX systems, there is usually an `ntpd` or `xntpd` daemon process. Create an `ntp.conf` configuration file in the `/etc` directory and write "server \*\*\*\*\*" (time server IP) into the file. Then, start the daemon process to synchronize the time.

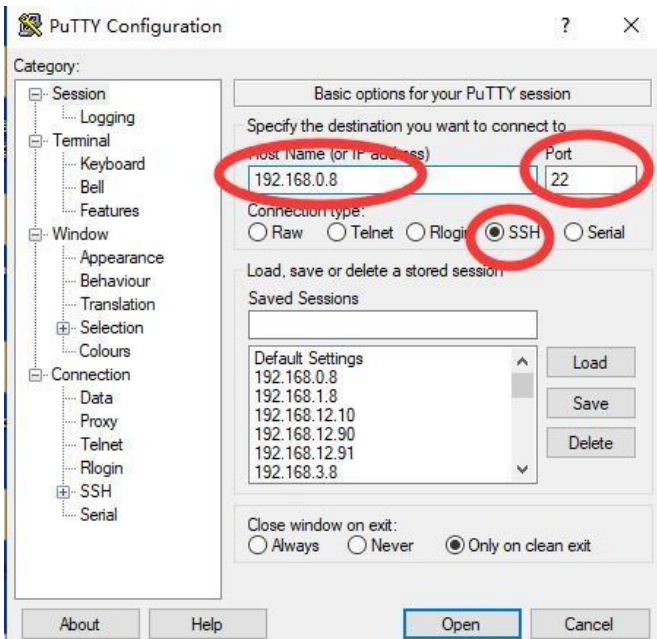
### 3.4. Server Configuration and Debugging

<1> Default Login Information Username: ntpuser Password: ntpuser2016 Username: root Password: globaltime

<2> Console Port Login Use a serial cable to connect the server console port to the USB port on a computer. Choose the Port port based on the actual situation, and configure it as shown in the figure below:



<3> SSH Login The SSH service version on the server is relatively new, please use a new version of SSH client software to log in. For example, putty0.73, SecureCRT8.5.0 or above. The SSH connection configuration is as shown in the figure below:



High-Performance, Enhanced Security Network Time Server

Enter the server IP address, select port 22, and choose the SSH protocol.

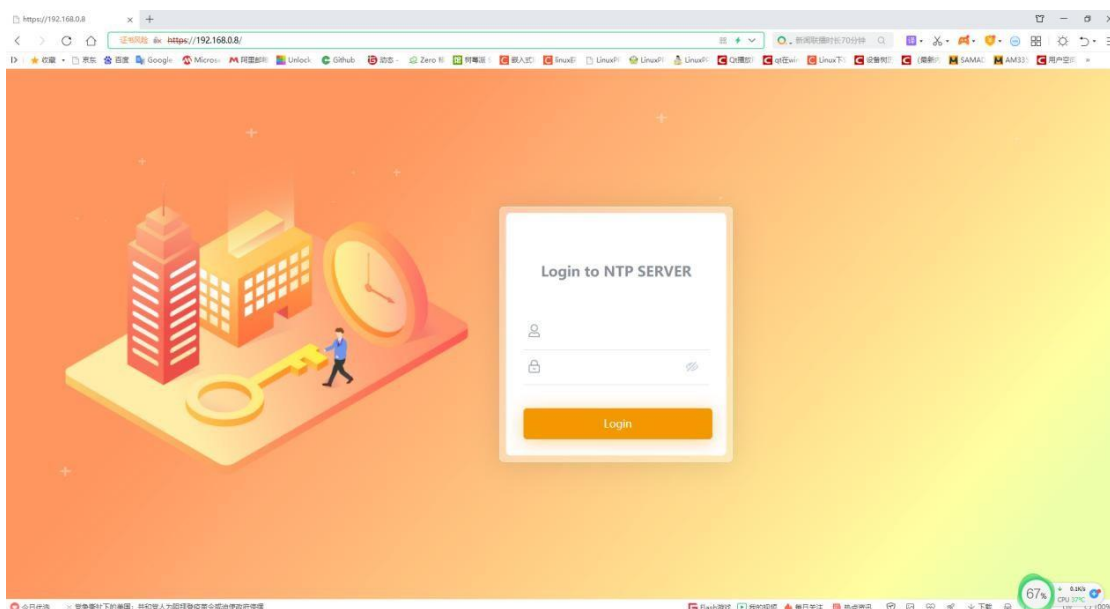
## 4. Remote Management and Monitoring

### 4.1. Login Information

The username and password are the same as the system, and only the root or ntpuser user can log in.

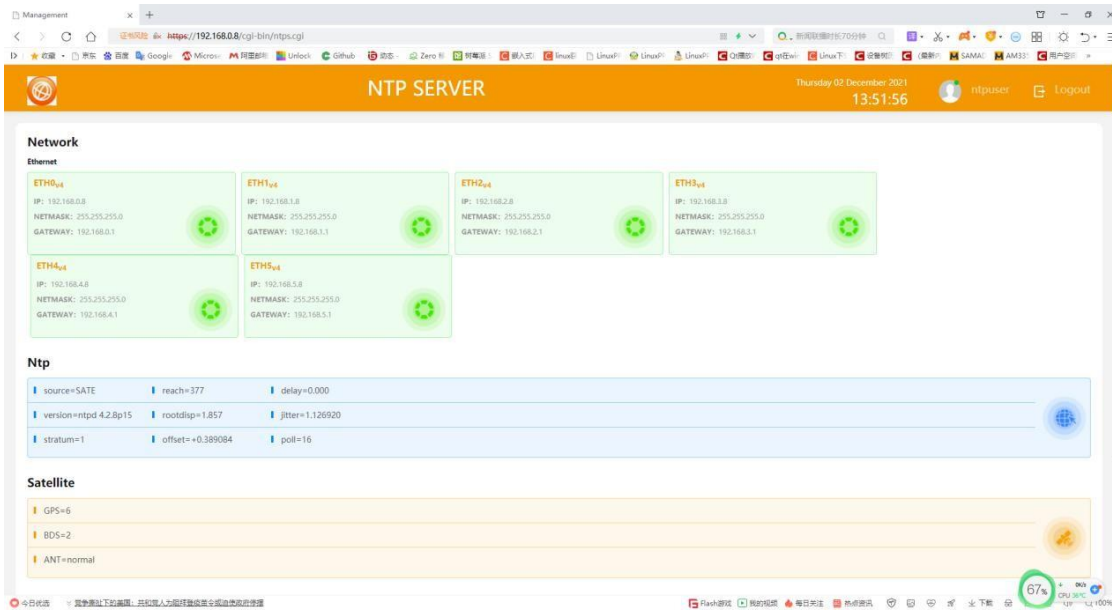
### 4.2. HTTP/HTTPS Login

<1> In the address bar of the browser, enter the server's IP address, for example: `http://192.168.0.8`



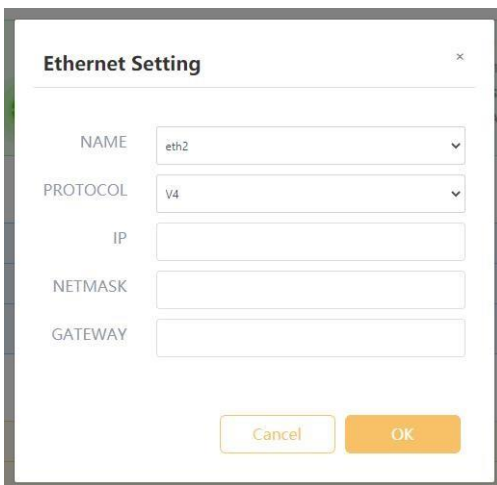
<2> Enter the username and password. After successfully logging in, you can view information about the server's login user, time, configuration, status, and other information.

## High-Performance, Enhanced Security Network Time Server

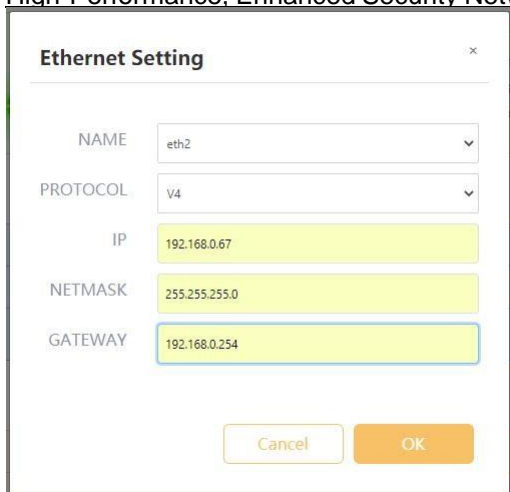


You can view the current network configuration, NTP service status, satellite status, system status, and device information.

<3> Configure the Server Basic Network Configuration Click on the Ethernet button to enter the settings page, and select and fill in the information as shown in the figure below:



In the NAME drop-down menu, select the network interface card that needs to be reconfigured. Choose the IPv4/6 protocol for PROTOCOL, and then enter the IP address, subnet mask, and gateway in order. For example, enter the IPv4 configuration as follows:



**Ethernet Setting** [Close]

NAME: eth2

PROTOCOL: V4

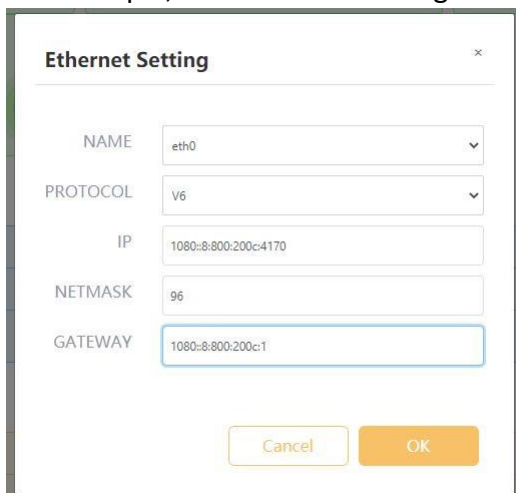
IP: 192.168.0.67

NETMASK: 255.255.255.0

GATEWAY: 192.168.0.254

Buttons: Cancel, OK

For example, enter the IPv6 configuration as follows:



**Ethernet Setting** [Close]

NAME: eth0

PROTOCOL: V6

IP: 1080::8:800:200c:4170

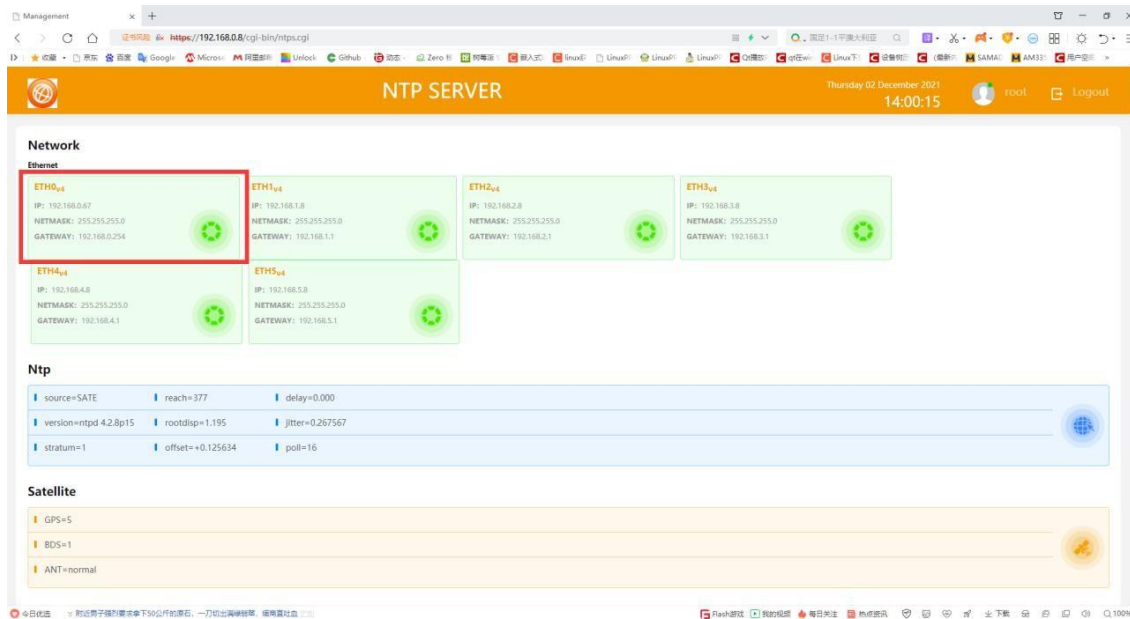
NETMASK: 96

GATEWAY: 1080::8:800:200c:1

Buttons: Cancel, OK

Finally, click the OK button to complete the configuration operation. After the configuration is completed, the page will be automatically refreshed to check whether the configuration information has been successfully modified. If the modification fails, it may be due to incorrect input information, please reconfigure it. The updated configuration is shown in the figure below, and the configuration information has been updated:

## High-Performance, Enhanced Security Network Time Server



After successfully modifying the configuration, the device needs to be restarted to take effect.

Bonding Configuration Click on the Bonding button to enter the bonding configuration page, which looks like this:

### Bonding Setting

NAME:

SWITCH:  enable  disable

SLAVES:  eth0  eth1  eth2  eth3  eth4  eth5

MODE:

IP:

NETMASK:

GATEWAY:

Select bond0 or bond1 in the NAME field.

In the SWITCH field, select the enable/disable radio button to turn on or off the corresponding bonding function.

In the SLAVES field, select at least 2 network cards that need bonding.

In the MODE field, select the bonding mode. Modes 0-6 are available, with mode 1 (active-backup mode) being the most commonly used.

### High-Performance, Enhanced Security Network Time Server

Enter the IP address, subnet mask, and gateway information. IPv6 address/subnet mask/gateway configuration is also supported.

For example, enter the following configuration:

**Bonding Setting**

NAME: bond0

SWITCH:  enable  disable

SLAVES:  eth0  eth1  eth2  eth3  eth4  eth5

MODE: mode1

IP: 192.168.1.199

NETMASK: 255.255.255.0

GATEWAY: 192.168.1.254

Buttons: Cancel, OK

Click the OK button to complete the configuration of bond0. The status page is refreshed as follows, and the configuration has been updated:

**NTP SERVER** Thursday 02 December 2021 14:08:51 root Logout

**Network**

**Bonding**

**BOND0<sub>04</sub>**  
IP: 192.168.5.66  
NETMASK: 255.255.255.0  
GATEWAY: 192.168.5.1  
MODE: balance-rr  
SLAVES: eth0 eth1

**Ethernet**

**ETH2<sub>04</sub>**  
IP: 192.168.2.8  
NETMASK: 255.255.255.0  
GATEWAY: 192.168.2.1

**ETH3<sub>04</sub>**  
IP: 192.168.3.8  
NETMASK: 255.255.255.0  
GATEWAY: 192.168.3.1

**ETH4<sub>04</sub>**  
IP: 192.168.4.8  
NETMASK: 255.255.255.0  
GATEWAY: 192.168.4.1

**ETH5<sub>04</sub>**  
IP: 192.168.5.8  
NETMASK: 255.255.255.0  
GATEWAY: 192.168.5.1

**Ntp**

source=SATE reach=377 delay=0.000  
version=ntpd 4.2.8p15 rootdisp=1.135 jitter=0.326496  
stratum=1 offset=+0.231555 poll=16

**Satellite**

GPS=5  
BDS=1

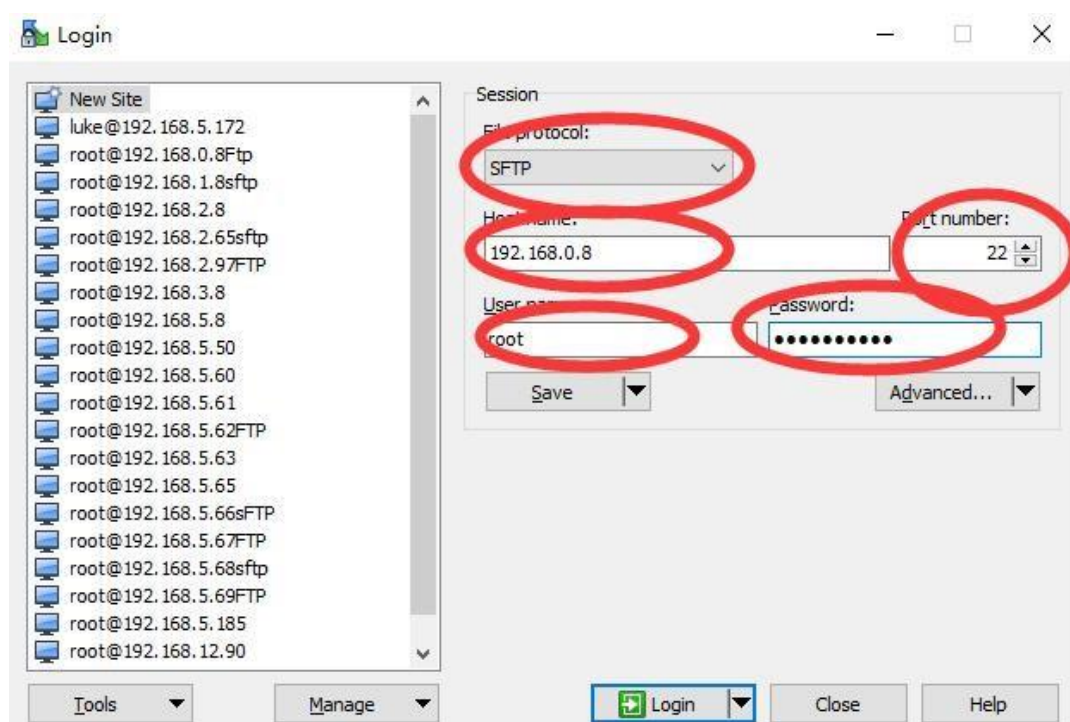
After modifying the configuration, the device needs to be restarted for the changes to take effect.

### 4.3. SSH Login

Use “ntpuser” to remotely log in to the system to view and configure device information. For specific operations, please refer to the CLI operation instructions.

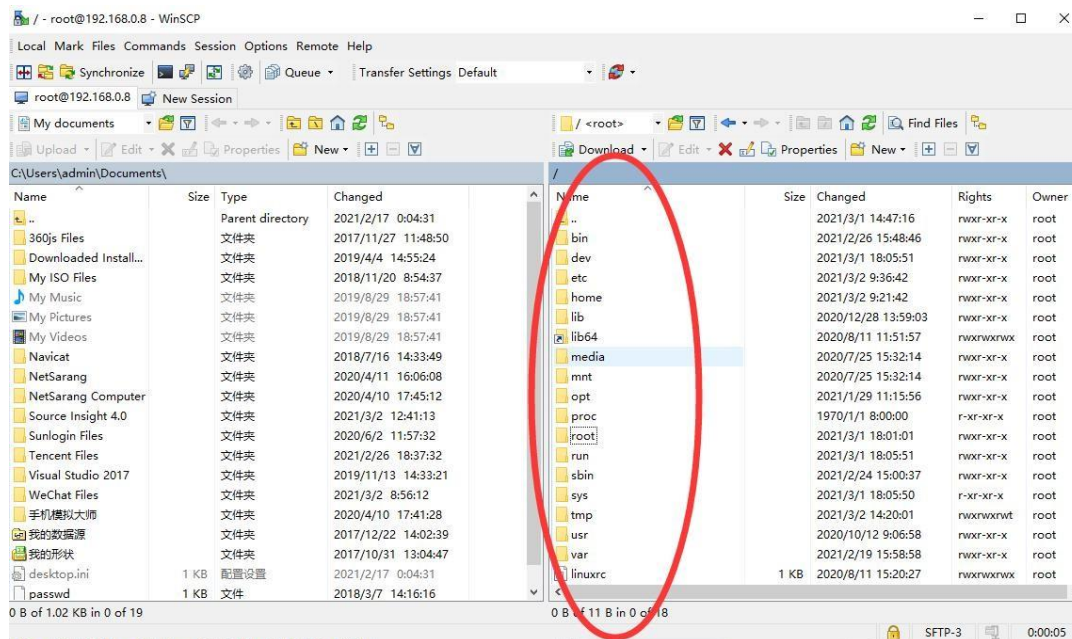
### 4.4. SFTP Login

On Windows, you can use the winscp tool to securely transfer files between the client and the server. The configuration for Winscp is as follows:



After clicking the Login button, you can log in to the server as shown below:

## High-Performance, Enhanced Security Network Time Server



You can switch between the directories on the Windows side and the server side, then drag and drop or copy and paste files to the destination directory.

## 5. Common Malfunctions and Maintenance

### 5.1. Common Malfunctions

#### 5.1.1. The time displayed on the time server is incorrect after power on

The time displayed on the time server after startup is the system default time, which is generally January 1, 2000. The correct time will only be displayed after the satellite is received and locked. Therefore, first ensure that the antenna is installed correctly and the cable is connected properly.

#### 5.1.2. All indicator lights do not turn on after power on

Please check if the power socket has power. In addition, there is a fuse holder on the device socket, please remove and check whether the fuse is intact.

#### 5.1.3. The device cannot receive satellites for a long time

In this case, the feed line system should be the focus of consideration. First, unplug the feed line on the device side and measure the BNC connector with a multimeter. There should be a 5V antenna feed voltage, otherwise the equipment is damaged. Then check whether the outdoor antenna part is connected properly, such as whether the outdoor connector is tightened, whether the waterproof measures for the connector are in place, whether the antenna leaks water, etc.,

#### High-Performance, Enhanced Security Network Time Server

and eliminate these obvious faults one by one. Then disconnect the antenna connector and measure the resistance on the feed line. When the far end is open, the resistance measured at the near end should be infinite; when the far end is short-circuited, the resistance measured at the near end should be only a few ohms. If it is abnormal, check whether the feed line and its connectors are intact. Common faults include quality problems with the line, poorly made connectors, scratched or bitten wires by small animals, etc. If surge protectors or antenna amplifiers are installed in the middle of the feed line, check whether these two components are intact. After eliminating the above faults, if the device still cannot receive satellites, please contact customer service, and our engineers will further process it.

#### **5.1.4. Cannot ping the time server after configuring the network**

First, confirm whether there is a physical connection problem in the network, observe the connection status indicator corresponding to the HUB or switch connected to the time server to see if it is normal. Then check whether there are errors in the network settings. You can first use a crossover cable to directly connect the server to a computer to see if it can be pinged, and then test it on the same network segment using a HUB, and finally test it on different network segments. In short, step by step eliminate faults from easy to difficult. Some firewall software on some computers will block ping operations, so it is best to turn off the firewall before checking the network status.

#### **5.1.5. Satellite reception is unstable, and sometimes the device enters a hold state**

Usually, this is caused by improper positioning of the satellite receiving antenna. If it happens frequently, consider installing the antenna in another location, avoiding obstacles and microwave interference around it.

#### **5.1.6. The client cannot receive time synchronization services**

The NTP protocol uses port 123 for time synchronization services, usually using the UDP protocol, and sometimes using the TCP protocol for transmission. Therefore, the 123 port service should be allowed to pass through the gateway and firewall in the internal network, and the configuration of the gateway and firewall should be checked.

#### **5.1.7. How to configure network devices to receive time synchronization services**

The NTP protocol is an international standard protocol, and many manufacturers' network devices can also receive NTP protocol to adjust their own time. For example, Cisco and Huawei routers can accept NTP services, and some series of switches also support NTP protocol. The setting command for Cisco router is: ntp server <IP address>

## 5.2. Daily Maintenance

### 5.2.1. Purpose

Check for faults in the time synchronization system, accurately locate any issues, and promptly resolve them.

### 5.2.2. Checklist

#### (1) Main panel Check



Check the main panel for time jumping, satellite numbers, and synchronization status. Check if the panel time is jumping normally, check if the satellite number is normal, and check if the synchronization status indicator in the upper right corner is "sync."

#### LED light check

When satellite timing is established, the FREQ light goes out and the SAT light comes on. If there is no antenna connected (rubidium atomic clock or crystal timing), the FREQ light is on and the SAT light is off.

If the ALARM light is on, it indicates that the CPU load is too heavy and has exceeded 75%.

If the NTP light is not on, it indicates that the NTP service status is abnormal and cannot provide NTP timing service.

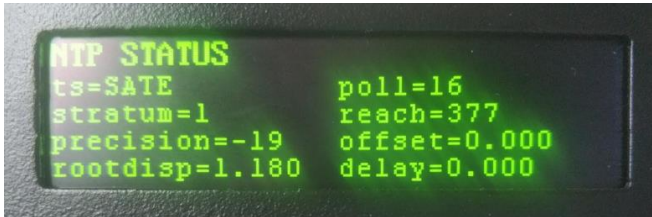
If power1 and power2 are not on, it indicates that the corresponding power supply has failed.



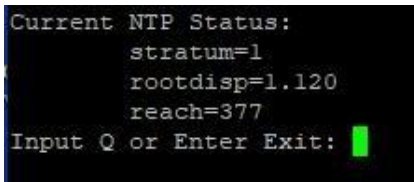
(3) NTP Status Check The NTP service status can be checked using the panel buttons or by logging in remotely through web/ssh. The Stratum of the primary time server must be 1. The Rootdisp value should be less than 10. A value too high indicates an unstable time source. The Reach value should be 377. If it's not 377, it indicates packet loss.

Panel display:

## High-Performance, Enhanced Security Network Time Server



### Remote SSH:



### Remote web:

Ntp

source=SATE	reach=377	delay=0.000
version=ntpd 4.2.8p15	rootdisp=1.135	jitter=0.326496
stratum=1	offset=+0.231555	poll=16

(4) Network Check Check if the network port indicator lights are flashing normally.

We reserve the right to changes at any time.

Local Support - Indonesia

**GFClock Yasapersada**

Address:

Jl. Pejaten Raya No.12a Pejaten Barat, Pasar Minggu, Jakarta Selatan 12510

Website: [www.gfclock.com](http://www.gfclock.com) Email: [gfclock.yasapersada@gmail.com](mailto:gfclock.yasapersada@gmail.com) Call: 0821-146 117 32