New Rock Technologies, Inc.

SX3000 Enterprise Session Border Controller (SBC)

Maintenance Guide

Website: http://www.newrocktech.com
Email: gs@newrocktech.com

Document version: 201504

Contents

Contents of Table

1 Routine Maintenance

1.1 Introduction

Routine maintenance, also known as preventive maintenance or periodic maintenance is a proactive mode to periodically maintain devices in the normal status. Routine maintenance helps you understand the running status and changing trend of the device, allowing you to take effective measures to eliminate hidden faults. The recommended maintenance period for SX3000 is one week, which can be adjusted as required.

1.2 Maintenance Preparation

- Ensure that SX3000 can be accessed through Telnet/SSH.
  The Telnet/SSH service is disbled by default. You can enable it and set passoword for accessing in **Advance > Security management**.
- Ensure that SX3000 can be accessed through graphical user interface (GUI).
  The default username is **admin** and password is **SX3000@123**.

1.3 Maintenance Items

1.3.1 Checking the Running Time

Step1 Telnet/SSH into SX3000.

Step2 Run the **uptime** command to check the running time of SX3000.

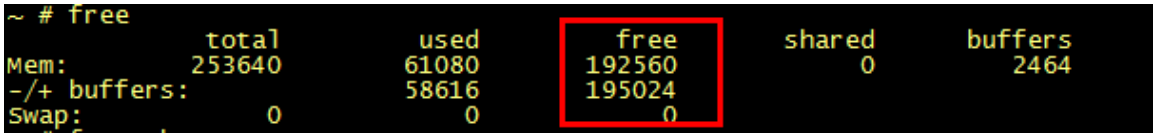
Note

The running time of SX3000 will be accumulated unless it is manually restarted.

1.3.2 Checking the RAM

Step1 Telnet/SSH into SX3000.

Step2 Run the **free** command to check the random-access memory (RAM) of SX3000.



Note

The lower threshold for the RAM of SX3000 is 5000 KB. If the value of column **free** is smaller than 5000, SX3000 will restart.

1.3.3 Checking the Process

Step1 Telnet/SSH into SX3000.

Step2 Run the **ps** command to check the current process message of SX3000.

```
~ # ps
PID   USER     TIME   COMMAND
    1 root       0:03 init
    2 root       0:00 [kthreadd]
    3 root       0:00 [ksoftirqd/0]
    4 root       0:00 [kworker/0:0]
    5 root       0:01 [kworker/u:0]
    6 root       0:05 [rcu_kthread]
    7 root       0:00 [khelper]
    8 root       0:00 [netns]
   42 root       0:00 [irq/72-serial i]
   44 root       0:00 [irq/73-serial i]
   46 root       0:00 [irq/74-serial i]
   48 root       0:00 [irq/44-serial i]
   50 root       0:00 [irq/45-serial i]
   52 root       0:00 [irq/46-serial i]
  225 root       0:00 [sync_supers]
  227 root       0:00 [bdi-default]
  229 root       0:00 [kblockd]
  237 root       0:00 [omap2_mcspi]
  249 root       0:00 [khubd]
  356 root       0:00 [musb-hdrc.0]
  359 root       0:00 [musb-hdrc.1]
  361 root       0:00 [rpciod]
  371 root       0:00 [kswapd0]
  372 root       0:00 [fsnotify_mark]
  373 root       0:00 [nfsiod]
  375 root       0:00 [crypto]
  478 root       0:00 [mtdblock0]
  483 root       0:00 [mtdblock1]
  488 root       0:00 [mtdblock2]
  493 root       0:00 [mtdblock3]
  498 root       0:00 [mtdblock4]
  503 root       0:00 [mtdblock5]
  508 root       0:00 [mtdblock6]
  513 root       0:00 [mtdblock7]
  518 root       0:00 [mtdblock8]
  614 root       0:00 [jffs2_gcd_mtd6]
  619 root       1:02 [kworker/0:2]
  640 root       0:03 /sbin/syslogd -s 300
  642 root       0:00 /sbin/klogd
  662 root       0:00 [kworker/u:2]
  714 root       0:04 /var/run/sshd
  727 root       0:00 /var/run/sntpd -v -P no -r -l /etc/rdated.conf -x 30 -4
  778 root       0:00 /usr/sbin/inetd
  779 root       0:00 init
  780 root       0:00 /var/run/cpe
  782 root     1386:3 /var/run/app
  784 root       0:05 /var/run/boa
 9841 root       0:00 -sh
14721 root       0:00 {sshd} sshd: root@pts/0
14725 root       0:00 -sh
14792 root       0:00 ps
```

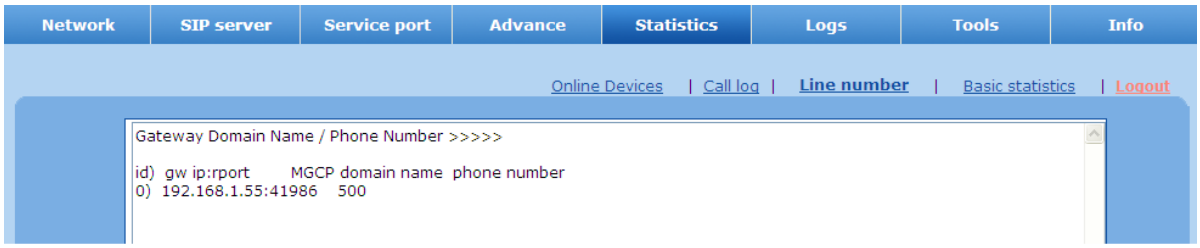
Note

In normal conditions, the status of the app process is displayed.

1.3.4 Checking the Online Terminals

Step1 Log in to the GUI of SX3000.

Step2 Click **Statistics** > **Line number**.



Note

If SX3000 works normally, you can view IP address and number of the registered terminal on this page.

1.3.5 Checking the Link Status of the Ethernet Interface

Step1 Telnet/SSH into SX3000.

Step2 Run the following commands to check the link status of the Ethernet interface.

~ # dmesg -c

~ # switch reg t

~ # dmesg -c

Port 1 Link Up,100 Mbps Full Duplex!
Port 2 Link Up,1000 Mbps Full Duplex!
Port 3 Link Down!
Port 4 Link Down!

Note

Port1/2/3/4 indicates Ethernet interface 1, Ethernet interface 2, and Ethernet interface 3 respectively. If the status of an Ethernet interface is “Link Down”, the Ethernet interface is disconnected.

1.3.6 Checking the SIP server in Usage

Step1 Log in to the GUI of SX3000.

Step2 Click **Statistics** > **Online Devices**.

Note

The last but one field of the entry indicates the SIP server IP address in usage, which can be used to determine whether the current active SIP server is normal.

1.3.7 Backing up Configurations

Step1 Log in to the GUI of SX3000.

Step2 Click **Tools > Export data > Download**.

Note

To avoid unexpected configuration loss, please back up configurations after the initial configuration or configuration change.

1.3.8 Changing Password Periodically

Changing the GUI Password

Step1 Log in to the GUI of SX3000.

Step2 Click **Tools > Change password** and enter the new password.

Changing the Telnet/SSH Password

Step1 Log in to the GUI of SX3000.

Step2 Click **Advance > Security management > Telnet/SSH password** and enter the new password.

Step3 Use the new password for logging after restarting.

Note

To ensure the device security, please change the GUI and Telnet passwords periodically.

2 Troubleshooting

2.1 Troubleshooting Process

A troubleshooting process generally consists of the following stages:

- Collecting information
- Troubleshooting the fault
- Resolving the the fault

2.1.1 Collecting Information

Fault information can be collected from:

- Feedback from the customer
- Alarms generated by the network management system
- Routine maintenance or inspection

Collecting raw information is of great importance during the initial troubleshooting stage. Raw information helps maintenance personnel narrow down the possible causes, ensuring a fast and accurate fault location. In case of faults, especially major faults, take caution that no action is performed until all necessary information is collected.

2.1.2 Troubleshooting the Fault

The cause of a fault is unique at each specific circumstance. Through analysis and comparisons, the exact cause of the fault can be identified. A fast and accurate fault diagnosis improves the troubleshooting efficiency, preventing the fault from further deterioration due to aimless troubleshooting. Locating the cause of fault is an important step in the process of technical troubleshooting, which provides guide for determining the means or measures for resolving the fault.

2.1.3 Resolving the Fault

After identifying causes of a fault, you can troubleshoot the fault accordingly.

Fault troubleshooting is a process of taking proper measures or steps (such as changing configurations or restarting the device) to rectify a fault and restore the system.

2.2 Troubleshooting Cases

2.2.1 Terminals Fail to Register to the SIP server through SX3000

Fault Description

The IP terminal can directly register to the SIP server, but cannot register to the SIP server through SX3000.

Cause Analysis

- The network between the terminal and SX3000 or between SX3000 and SIP server fails.
- The registration server and ports of the terminal are improperly configured.
- The registration account and password are incorrectly set.
- The encryption modes on the terminal and SX3000 do not match.
- There are special restrictions.

Troubleshooting and Solution

- Telnet/SSH into SX3000 and run the **ping** command to check the network connection between SX3000 and terminal and between the SX3000 and SIP server. If the network fails, debug the network and try again.
- Check whether the registration address on the terminal is the address of SX3000 and whether the serving port, account, and password are correct.
- Check whether the encryption modes on the terminal and SX3000 match. If not, change the encryption mode on SX3000.
- Check whether there are special restrictions on SIP signaling. For example, Huawei SoftCo will check whether or not there is a field of Huawei in **User-Agent** of the registation message.

In addition, you can capture packets on the network to fast locate the fault:

- If SX3000 does not receive registration messages, the cause may be that the terminal does not send these messages. Check terminal configurations and the network connection between the terminal and SX3000.
- If SX3000 receives messages and obtains no response after sending these messages to the SIP server, check software configurations on SX3000 and the network connection between SX3000 and SIP server.
- If SX3000 forwards registration messages to the SIP server and receives the code 403 in response, check whether the registration password is correct.
- If SX3000 forwards registration messages to the SIP server and receives the code 404 in response, check whether the registration number is correct.

2.2.2 One Side or Both Sides Fail to Hear the Voice of the Far End

Fault Description

During the communication, one side or both sides fail to hear the voice of the far end.

Cause Analysis

- The codes of terminals are different.
- The SDP address in the SIP signaling is incorrect.
- The terminal does not send RTP packets.
- Type-of-Service (TOS) on SX3000 does not match TOS on the terminal.
- The RTP proxy function is disabled on SX3000.

Troubleshooting and Solution

Capture packets on the switch through mirroring or on SX3000 for analysis. For details, see **Q8 How to capture IP packets on the SX3000** in Chapter 3.

- Check whether the SDP address in the SIP signaling is correct. The **200OK** message sent from SX3000 to the terminal needs to carry the address of SX3000.

- Check whether the terminal sends RTP packets. If not, check the terminal configurations.
- Check whether codecs in RTP packets sent by the two terminals are the same. If not, check the terminal configurations.
- Check whether the TOS value is configured for SX3000. If so, check whether the TOS value for SX3000 is identical with TOS values on the terminal and SIP server.
- Log in to the GUI of SX3000, and click **Advance > System** to check the **RTP proxy** parameter. If the value of this parameter is set to **No**, please set to **Yes**.

2.3 Vendor Assistance in Information Analysis

If the on-spot engineer is unable to troubleshoot the fault, New Rock can provide assistance in fault analysis. To ensure a quick and accurate troubleshooting, the on-spot engineer needs to provide the following information:

- Logs when the fault occurs (If the fault can be reproduced, logs with the level of 8 need to be captured. For method of capturing logs, see **Q5 How to download logs** in Chapter 3.)
- Packets captured on the network when the fault occurs (Packets can be captured on the mirroring switch using **wireshark** or on the background of SX3000 using **tcpdump**). For packet capturing on the background of SX3000, see **Q8 How to capture IP packets on the SX3000** in Chapter 3.
- Current configurations of SX3000. For configuration download, see **Q5 How to download logs** in Chapter 3.
- Fault information and on-site environment, including the detailed fault information, network topology, and IP address of the terminal/SX3000/SIP server.

The preceding information can be sent to gs@newrocktech.com through e-mail for instant help.

3 FAQs

Q1. What to do if I forget the IP address of SX3000 and how to change the IP address?

Log in to SX3000 through the console interface (the username is **root**, the password is the same as the password of the Telnet/SSH) and run the **ifconfig** command to check the IP address of each Ethernet interface. Set the IP address of the computer in the same network segment as the IP address of one of the Ethernet interfaces and then log in to the GUI of SX3000 to change the IP address.

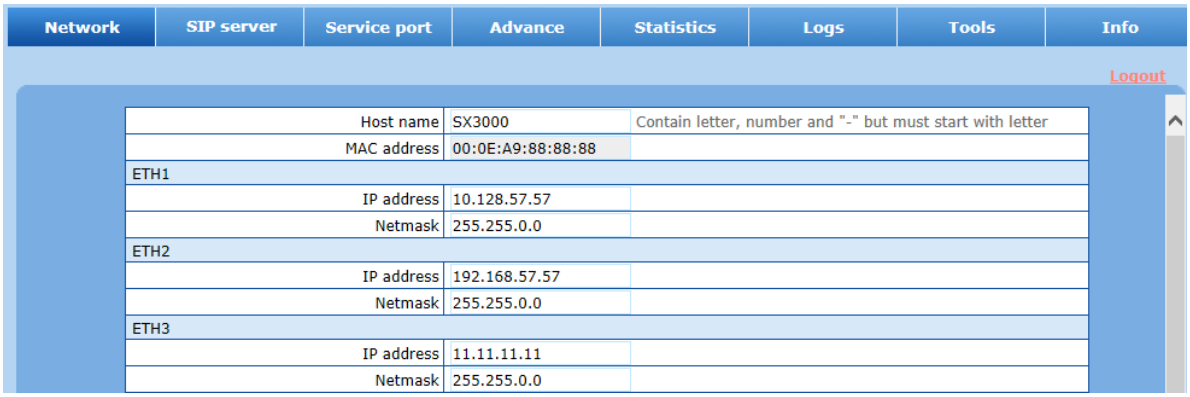
Note

Communication parameters for the console interface on SX3000 include 115200 bit/s, eight data bits, one stop bit, no parity, and no flow control.

Q2. After logging in to the GUI as the administrator, I can neither change configurations nor find the submit button. What's wrong?

Multiple users can concurrently log in to the GUI of SX3000, but only the first login user has the authority as an administrator. Other users have only the read rights. The rights of the current user can be queried at the upper left corner of the GUI, as shown in the following diagram.

Figure 3-1 GUI of SX3000



Q3. How to forward messages if the IP address of the SIP server and addresses of Ethernet interfaces on SX3000 are in different network segments?

Forward the messages through a network port that is in the same network segment as the default gateway address.

Q4. How to set QoS?

Quality of Service (QoS) can be set by setting TOS values. TOS values are set in the **Advance** tag of the GUI. TOS values are in hexadecimal, which can be converted from DSCP binary value by adding two bits 00 at the left side. For example, if the DSCP value is 46(101110), the converted TOS value is 0xB8 (10111000).

The following information is used as reference:

IP precedence (IP TOS)

There are eight IP precedence values, ranging from 0 to 7. The larger the value is, the higher the precedence. By default, values 6 and 7 are reserved for internetwork and network control. You are not recommended to use these two values.

DSCP precedence

There are 64 IP precedence values, ranging from 0 to 63. The larger the value is, the higher the precedence. Under the current definition, the default DSCP value is 0.

For class selectors that are defined as being backward-compatible with IP precedence, the DSCP value can be 8, 16, 24, 32, 40, 48, or 56. For Expedited Forwarding (EF) that is commonly used for low-latency services, the recommended DSCP value is 46 (101110). For Assured Forwarding (AF), four service levels are defined and each service level is assigned with three DSCP values, namely (10, 12, 14), (18, 20, 22), (26, 28, 30), and (34, 36, 38).

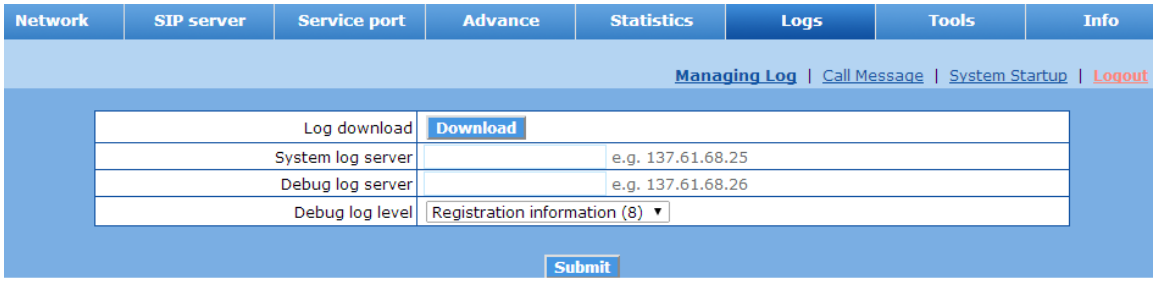
Q5. How to download logs?

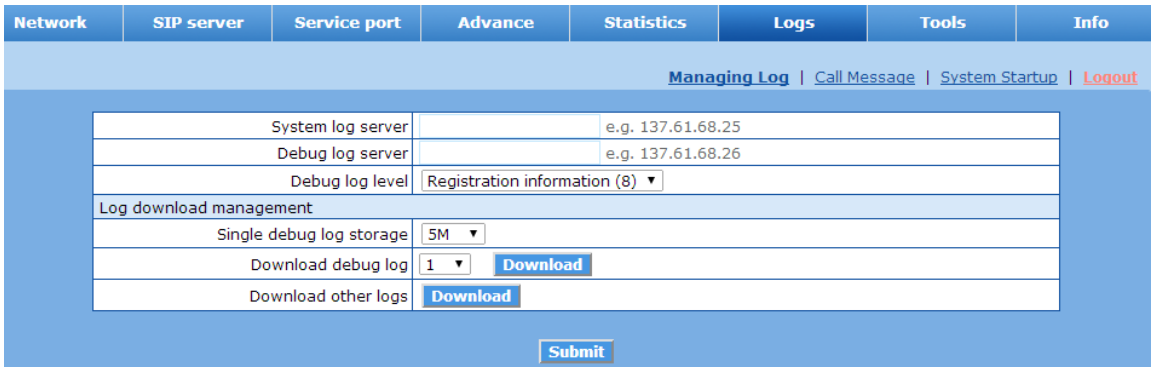
Click **Logs > Managing Log** to download logs of SX3000.

Logs are downloaded for fault analysis on SX3000. If the fault occurred on SX3000 can be reproduced, you are recommended to change the value of **Log level** to **Registration information(8)** so that more detailed information can be obtained.

During normal operation of SX3000, set the value of **Log level** to **3** or a value smaller than 3.

The debugging log entries are stored on the SD card if there is one in the slot otherwise in the flash memory. The download interfaces are shown below.





Q6. Does SX3000 support the TR069 protocol?

Yes. You can configure TR069-related parameters such as the server URL, username, and password in

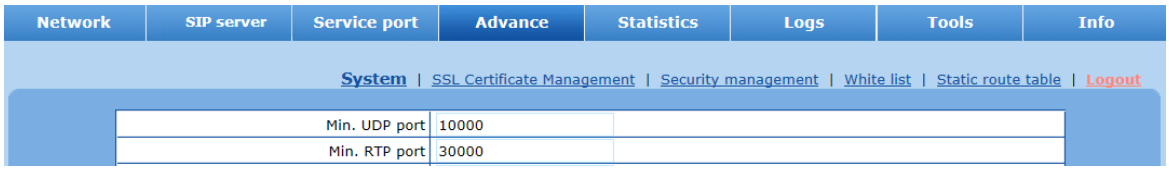
the **Advance** tag of the GUI. In addition, SX3000 has passed the interoperability testing with Huawei network management system.

Q7. What are the UDP and RTP ports in the advance tag of the GUI and what are value ranges of these two ports?

The User Datagram Protocol (UDP) port is the source port used by SX3000 to forward Session Initiation Protocol (SIP) messages to the SIP server. For example, the IP terminal sends registration messages to the service port 5060 of SX3000. Then, SX3000 forwards the registration messages to the SIP server from the port 20010. The port 20010 is the UDP port. It ranges between the min. UDP port number and (min. RTP port number -1).

The range of UDP ports is from a minimum UDP port number to (a minimum RTP port - 1).

The port on the SX3000 that is used to send and receive RTP messages. RTP port is used to send and receive RTP packets. It ranges between the min. RTP port number to (min. RTP port number +4799).



Q8. How to capture IP packets on SX3000?

The tcpdump (a Linux network data capturing and analysis tool) is available on the device. It can be used to capture packets (excluding RTP packets) transferred through a device port for analysis.

Procedures of using **Tcpdump** at the background are as follows:

Step1 Telnet/SSH into SX3000.

Step2 Run the **cd /tmp** command to enter the directory **/tmp**.

Step3 Run the **./tcpdump -i any -s 0 -w sbc.cap** command to capture packets.

Step4 Reproduce the fault. After that, the **sbc.cap** file will be generated in the directory **/tmp** after pressing **Ctrl+C**.

Step5 Run the **tar -cvzf log.tar.gz sbc.pcap /var/config /var/log** command to generate the **log.tar.gz** file.

Step6 Install the SFTP server on the computer and do as follows on the background of SX3000 to upload files to the computer:

- Run the **sftp *username@X.X.X.X*** command. X.X.X.X is the IP address of the SFTP server.
- Enter the SFTP password.
- Run the **put log.tar.gz** command to upload the file to the local computer. The **log.tar.gz** file contains packets captured by SX3000 on the network.
- Run the **exit** command to quit SFTP.

Step7 Run the **rm log.tar.gz** command to delete the **log.tar.gz** file and release the occupied memory.

Note

Capturing of packets on the background is used only when the packet capturing cannot be performed in the on-site environment. The recommended packet capturing duration is two minutes. If the packet capturing process lasts for a long period of time, excessive memory will be occupied, leading to the restart of SX3000. During packet capturing, you can open another Telnet/SSH window and run the **free** command to check the remaining memory. Ensure that the memory of SX3000 is greater than 5M bytes.

Q9. How to capture media stream packets on the device?

To capture RTP packets, follow these steps:

Step1 Copy the tcpdump to the SFTP server.

Step2 Log in to the device using a telnet/SSH session, and then type **cd tmp** to enter the **tmp** folder.

Step3 Run the **sftp username@X.X.X.X** command to enter directory **sftp**.

Step4 Browse the directory that stores the tcpdump, then run the **get tcpdump** command to download the tcpdump to directory **tmp**.

Step5 When the download is complete, run the **exit** command.

Step6 Run the **./tcpdump -i any -s 0 -w sbc.pcap** command to capture packets.

Step7 Press **Ctrl+C** to finish capturing, and then repeat Steps 5 to 7 shown in Q8.

Q10. If I forget the Telnet/SSH password, how can I restore it?

The missing Telnet/SSH password can be restored by logging in to the SX3000 through the GUI.

Choose **Advanced > Security > Management** > **Telnet/SSH Service Password**. Then set a new password. After restarting the device, the new Telnet/SSH password can be used to log in to the device.

4 Acronyms and Abbreviations

Table 4-1 Acronyms and Abbreviations

Terms	Full Spelling
SBC	Session Border Controller
RTP	Real-time Transport Protocol
SIP	Session Initiation Protocol
TR069	CPE WAN Management Protocol
TOS	Type-Of-Service
DSCP	Differentiated Services Code Point
QoS	Quality of Service
UDP	User Datagram Protocol
URL	Uniform Resource Locator
EF	Expedited Forwarding
AF	Assured Forwarding