Ruijie Networks – Innovation Beyond Networks

RG-Switch (for RGOS 11.X) FAQs V1.1

Copyright Statement

Exemption Statement

This document is provided “as is”. The contents of this document are subject to change without any notice. Please obtain the latest information through the Ruijie Networks website. Ruijie Networks endeavors to ensure content accuracy and will not shoulder any responsibility for losses and damages caused due to content omissions, inaccuracies or error

Revision History

Date	Change contents	Reviser
2016.09.01	Initial Release	Amy & crystal
2017.02	Add new chapter of 4.10 Typical Case on publication V1.1	TAC Oversea

1 Overview

This document describes usage limitations of switches using the RGOS 11.x software platform and problems that frequently arise during deployment, so as to provide guidance for after-sales engineers to deploy and implement products and improve the deployment efficiency and quality.

Audience

- Network Engineers
- Network Administrator

Obtain Technical Assistance

- Ruijie Networks Websites : http://www.ruijienetworks.com
- Ruijie Service Portal : http://case.ruijienetworks.com

Welcome to report error and give advice in any Ruijie manual to Ruijie Service Portal

Related Documents

- RG-Switch (for RGOS 11.X) FAQs V1.0

2 Introduction to the Index

This document collects the frequently asked questions (FAQs) about minimalist networks and provides answers by category. Because the questions are not indexed, to search for a specific question, press the shortcut key **Ctrl**+**F** in the document and enter keywords of your question in the search box.

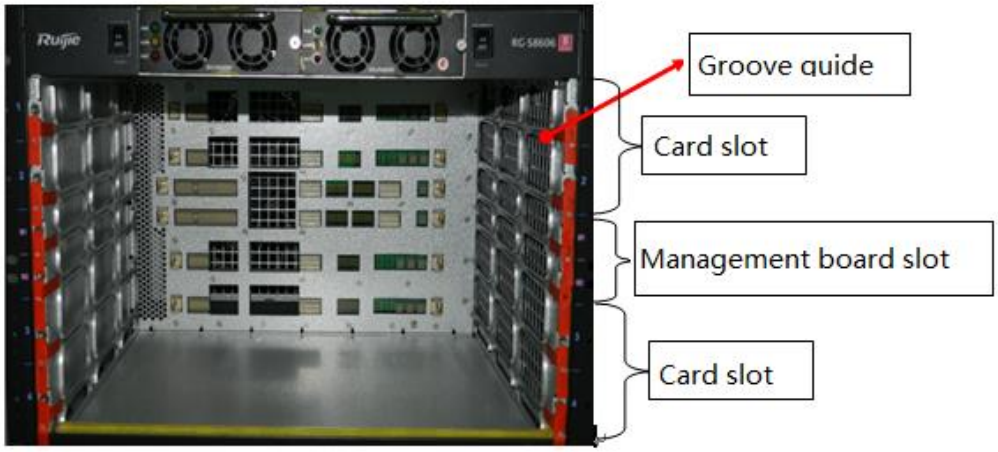
3 Contents

4 FAQ

4.1 Hardware Installation Precautions

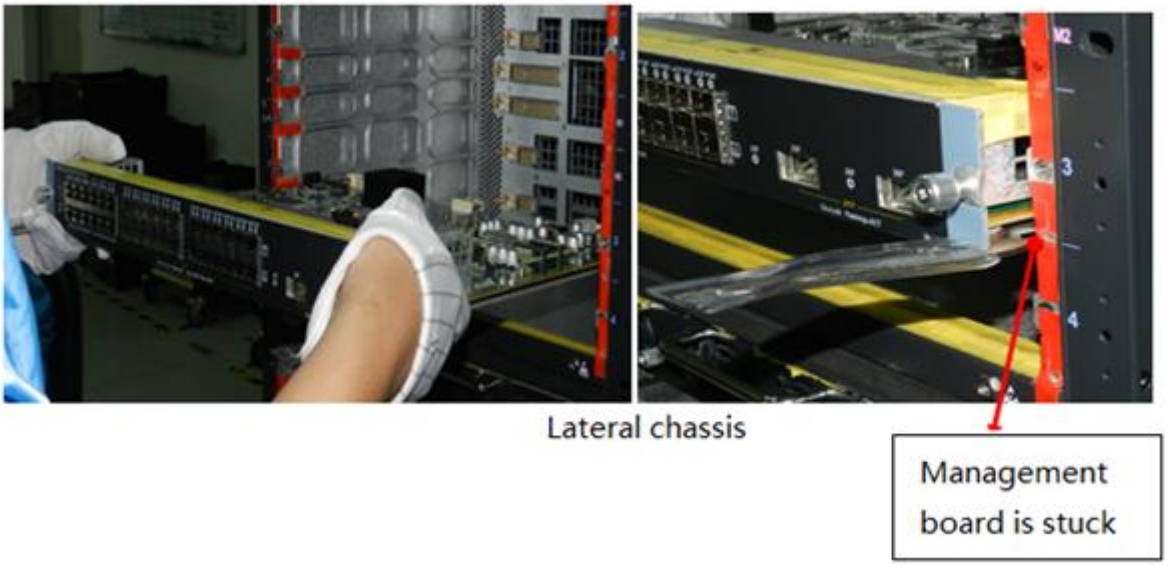
Q1. Card (Supervisor Module) Insertion Operation (Wear ESD Gloves or an ESD Wrist Strap in Daily Operations)

Step 1: Confirm the models and slots of cards and supervisor modules, as well as positions of guide rails.



Step 2: Turn the self-locking lever to a position vertical to the panel of a card (supervisor module).

Step 3: Hold the card (supervisor module) with hands, keep it parallel to the chassis, and insert it into the correct slot till it is locked by the self-locking lever.



Step 4: Hold the self-locking lever, insert the card (supervisor module) along the motion trail of the self-locking lever till the card (supervisor module) is completely inserted into the chassis.

Step 5: Use a screwdriver to tighten screws on the left and right sides of the card (supervisor module).

Q2. Card (Supervisor Module) Removal Operation

Step 1: Turn the self-locking lever to a position vertical to the chassis.

Step 2: Hold the filler panel of the card (supervisor module) with hands and gently pull it out in a direction parallel to the guide rail.

Q3. Precautions in Card (Supervisor Module) Operations

Step1: When a card (supervisor module) cannot be inserted, do not insert it in with strong force. Pull it out and then attempt to insert it into the chassis.

Step 2. Ensure that a card (supervisor module) is in parallel to the guide rail during insertion and removal.

Q4. Post-installation Check

Check Item	Check Result	
1. Ground cables are connected correctly.	Yes	No
2. The fan assembly is installed correctly and connected properly.		
3. Power modules are installed correctly and connected properly.		
4. The power switch is in the off state (the rocker switch is in the OFF position).		
5. Power cables are connected correctly.		
6. Supervisor modules are installed correctly and connected properly.		
7. Service cards are installed correctly and connected properly.		
8. Switch fabric modules are installed correctly and connected properly.		

4.2 Power

Q1: Is the Power Supply Mode of the N18000, 86E, and 78E Redundancy Power Supply or Load Power Supply? Can Their Power Supply Mode Be Changed?

The N18000, 86E, and 78E support two redundancy modes in power supply: non-redundancy mode and N+M redundancy mode. The devices use the non-redundancy power supply mode by default.

Non-redundancy mode: This mode is the default configuration of devices. The total power of the system is the sum of the output powers of all power supplies and each module supplies power according to their actual capability. Assume that a chassis is equipped with four 400 W power supplies. The total system power provided by the power supplies is 1600 W.

N+M redundancy mode: A system has a total of N+M power supplies, M redundant power supplies are configured, and N power supplies are available currently. The total power of the system is the sum of the output power of N power supplies. After power redundancy is configured, the redundant power supplies are used as backup power supplies to prevent power faults and they do not participate in system power distribution. For example, after one redundant power supply is configured, if a power supply of a device malfunctions and cannot supply power, the redundant power supply immediately supplies power and participates in system power distribution. After the faulty power supply is restored, it becomes a redundant power supply, thereby maintaining the system power unchanged.

The number of configured redundant power supplies must be smaller than the number of power supplies that are available currently. Redundancy fails. The command for configuring the power redundancy mode is as follows:

[Command] power redundancy [switch devid] pwrs enable

[Parameter Description] switch devid: Specifies the ID of the chassis, to which the card slot for which the redundancy mode is to be configured belongs. It is supported only in VSU mode. The default value is the local chassis ID.

pwrs: Specifies the number of redundant power supplies.

[Configuration Example] Configure 1+2 power redundancy: The N18010 chassis is equipped with three DC 1600 W power supplies. It can work properly as long as one power supply is available. Therefore, the other two power supplies can be configured as redundant power supplies.

```
Ruijie(config)#power redundancy 2 enable
```

[Verification] Run the show power command to check whether the power redundancy configuration takes effect and the number of redundant power supplies.

```
Ruijie#show power
Chassis-type: RG_N18010
Power-redun: yes
Redun-powers: 1
Energy-saving: off
```

Q2: Which Cards of the N18000 Will Be Powered Off First When the Power Is Insufficient and What Is the Basis?

1. The N18000 is powered by the intelligent power supply, which allows configuring power supply priority for cards, controlling the power-on and power-off of cards, and reading the operating temperature, input voltage, and other information of the power supply.
2. The power supplies of cards have different priorities. A card with a higher priority is powered on prior to that with a lower priority and is powered off later than that with a lower priority. The default power supply priority of cards is as follows: supervisor module > FE card > VSL card > other cards. For cards of the same type, a card with a smaller slot ID has a higher priority than that with a larger slot ID. You can configure the power supply priority in the system running phase. This function ensures that cards with a higher priority are powered on first in the next startup and power-on. The command for configuring the power supply priority of cards is as follows:

   [Command] power priority [switch devid] slot slotid prio

   [Parameter Description] switch devid: Specifies the ID of the chassis, to which the card slot for which the power-on and power-off priority is to be configured belongs. It is supported only in VSU mode. The default value is the local chassis ID.

   slot slotid: Specifies the slot ID of the card to be configured. The value is the range of card slot IDs.

   prio: Specifies the priority of a card to be configured. The value ranges from 1 to 16. 1 indicates the lowest priority and 16 indicates the highest priority.

   [Usage Guide] This command is used to change the default power supply priority of VSL cards and other cards. FE cards can only use the default priority.

[Configuration Example] Change the priority of the card in slot 3 of the N18010 to 10.

```
Ruijie(config)#power priority slot 3 10
```

4.3 Service Cards

Q1: What Are Differences Between CM Cards, Other Cards, and FE Cards Supported by the N18014 and Those Supported by the N18010?

1. The N18010 supports the M18000-WS-ED wireless controller cards, M18000-48GT-P-EDPOE cards, and RG-PA1600I-PPOE power supplies, which are not supported by the N18014.
2. The control engine and FE cards supported by the N18010 and N18014 vary with the model.
3. Other cards and power modules are universal to the N18010 and N18014.

Q2: How to Display the Serial Numbers of the Chassis, Power Supplies, Fans, and Cards by Running Commands on the N18000?

The show manuinfo command is used to display the serial numbers of the chassis, engine, cards, power supplies, and fans.

```
Ruijie#show manuinfo
Device 1
    Location:                   Chassis
    Device name:                RG-N18010
    Device Serial Number:       G1HL21P000084
    Hardware Version:           1.00
    Mac Address:              14.14.4b.76.1e.c8

Device 2
    Location:              Slot-1
    Device name:           M18000-24GT20SFP4XS-ED
    Device Serial Number:       G1HL20N00006B
    Hardware Version:           1.00
    Software Version:           N18000_RGOS 11.0(1)B2

Device 3
    Location:                   Slot-2
    Device name:                M18000-44SFP4XS-ED
    Device Serial Number:       G1HL20U00026B
```

```
    Hardware Version:           1.00
    Software Version:           N18000_RGOS 11.0(1)B2

Device 4
    Location:                   Slot-FE2
    Device name:                M18010-FE-D I
    Device Serial Number:       G1HL10Y000720
    Hardware Version:           1.00
    Software Version:           N18000_RGOS 11.0(1)B2

Device 5
    Location:                   Slot-FE3
    Device name:                M18010-FE-D I
    Device Serial Number:       G1HL10Y000813
    Hardware Version:           1.00
    Software Version:           N18000_RGOS 11.0(1)B2

Device 6
    Location:                   Slot-M1
    Device name:                M18010-CM
    Device Serial Number:       G1HL20H000325
    Hardware Version:           1.00
    Software Version:           N18000_RGOS 11.0(1)B2
    Mac Address:                14.14.4b.75.bc.96

Device 7
    Location:                   Power 1
    Device name:                RG-PA1600I
    Device Serial Number:       AA74858
    Hardware Version:           2

Device 8
    Location:                   Power 2
    Device name:                RG-PA1600I

Device 9
    Location:                   FAN 1
    Device name:                M10-FAN-R
    Device Serial Number:       9974HL20G0078
    Hardware Version:           V1.00
```

```
Device 10
    Location:                   FAN 2
    Device name:                M10-FAN-R
    Device Serial Number:       9974HL20G0047
    Hardware Version:           V1.00

Device 11
    Location:                   FAN 3
    Device name:                M10-FAN-R
    Device Serial Number:       9974HL20G0051
    Hardware Version:           V1.00

Device 12
    Location:                   FAN 4
    Device name:                M10-FAN-F
    Device Serial Number:       9973HL20F0025
    Hardware Version:           V1.00
```

Q3: What Are the Functions of the Reset Button on the Engine of the N18000?

The **Reset** button implements the reset of the system.

The **Reset** button supports long-press operation and short-press operation. If you press the button for less than 5 seconds, this operation is short-press. If you press the button for five or more seconds, this operation is long-press. Long-press and short-press are described as follows:

1. Status indicator in the case of long-press or short-press: When you press the **Reset** button for a short period of time, the indicator blinks green and the system resets within 5 seconds after the button is released. When you press the **Reset** button for a long period of time, the indicator blinks green for 5 seconds and then blinks red, the system resets within 5 seconds after the button is released.
2. When you press the **Reset** button for a short period of time, the system starts collecting information, the system is not restarted during information collection, and the system is reset after information collection is complete. When you press the **Reset** button for a long period of time, the system is directly restarted within 5 seconds after you release the button.

Q4: Poor Contact of the Obliquely Inserted Memory Module — Troubleshooting Guide

Applicable scope:

All CM cards in high-end switches that use obliquely inserted memory module sockets, as shown in the following figure.

The models include but are not limited to the following:

M18010-CM

M18010-CM II

M18014-CM

M18014-CM II

M18007-CM II

M18007-CM II LITE

M8600E-CM

M7800E-CM

Fault symptom:

The two common fault logs are as follows:

The device is restarted repeatedly and the following exception information is displayed in the case of boot:

Boot 1.2.2-eaf8aaa (Build time: Apr 21 2014 - 10:12:42)

DRAM: 4 GiB

Boot 1.2.2-eaf8aaa (Build time: Apr 21 2014 - 10:12:42)

DRAM: 4 GiB

The device automatically restarts and the following exception information is displayed (the ECC error is reported repeatedly):

```
NAND:  512 MiB
Flash: 8 MiB
```

```
    SETMAC: Setmac operation was performed at 2014-06-16 21:16:11 (version: 11.0)
    Press Ctrl+C to enter Boot Menu
    Bootloader: Done loading app on coremask: 0xf
    [    0.000000] ERROR PBANK_LSB: 4, ROW_LSB: 2, Row bits: 16, Col bits: 10, Row mask: 0xffff, Col
mask: 0x3ff
    [    0.000000] ERROR LMC0 ECC: sec_err:8 ded_err:0
    [    0.000000] LMC0 ECC:        Failing dimm:   0
    [    0.000000] LMC0 ECC:        Failing rank:   0
    [    0.000000] LMC0 ECC:        Failing bank:   7
    [    0.000000] LMC0 ECC:        Failing row:    0xff0b
    [    0.000000] LMC0 ECC:        Failing column: 0x2dbe
    [    0.000000] LMC0 ECC:        syndrome: 0xce
    [    0.000000] Failing  Address: 0x000000010f0b6cf8, Data: 0xc00627d8c006cfec
    [    0.000000] ERROR PBANK_LSB: 4, ROW_LSB: 2, Row bits: 16, Col bits: 10, Row mask: 0xffff, Col
mask: 0x3ff
    [    0.000000] ERROR LMC0 ECC: sec_err:1 ded_err:0
    [    0.000000] LMC0 ECC:        Failing dimm:   0
    [    0.000000] LMC0 ECC:        Failing rank:   0
    [    0.000000] LMC0 ECC:        Failing bank:   5
    [    0.000000] LMC0 ECC:        Failing row:    0x14
    [    0.000000] LMC0 ECC:        Failing column: 0x1110
    [    0.000000] LMC0 ECC:        syndrome: 0xce
    [    0.000000] Failing  Address: 0x0000000000144480, Data: 0x080510000083102d
    [    9.235671] ERROR PBANK_LSB: 4, ROW_LSB: 2, Row bits: 16, Col bits: 10, Row mask: 0xffff, Col
mask: 0x3ff
    [    9.350371] ERROR LMC0 ECC: sec_err:8 ded_err:0
    [    9.350374] LMC0 ECC:        Failing dimm:   0
    [    9.350377] LMC0 ECC:        Failing rank:   0
    [    9.350379] LMC0 ECC:        Failing bank:   6
    [    9.350382] LMC0 ECC:        Failing row:    0xdd
    [    9.350385] LMC0 ECC:        Failing column: 0x379a
    [    9.350388] LMC0 ECC:        syndrome: 0xce
    [    9.350390] Failing  Address: 0x0000000000dde458, Data: 0xcccccccccccccccc
```

Troubleshooting suggestion:

When a faulty card encounters the preceding fault symptoms, the fault may be caused by poor contact between the memory module and the memory module socket. In this case, perform the following operations to attempt to eliminate the poor contact:

Step 1: Remove the faulty card from the chassis and put it on a flat platform.

Step 2: After wearing ESD gloves or an ESD wrist strap, hold the edge in the middle of the memory module where no component resides (as shown in Figure 2), shake the memory module top down along the direction vertical to the memory module plane (as shown in Figure 3), with the amplitude smaller than 5 mm, to prevent damage to the memory module and socket.

Figure 2

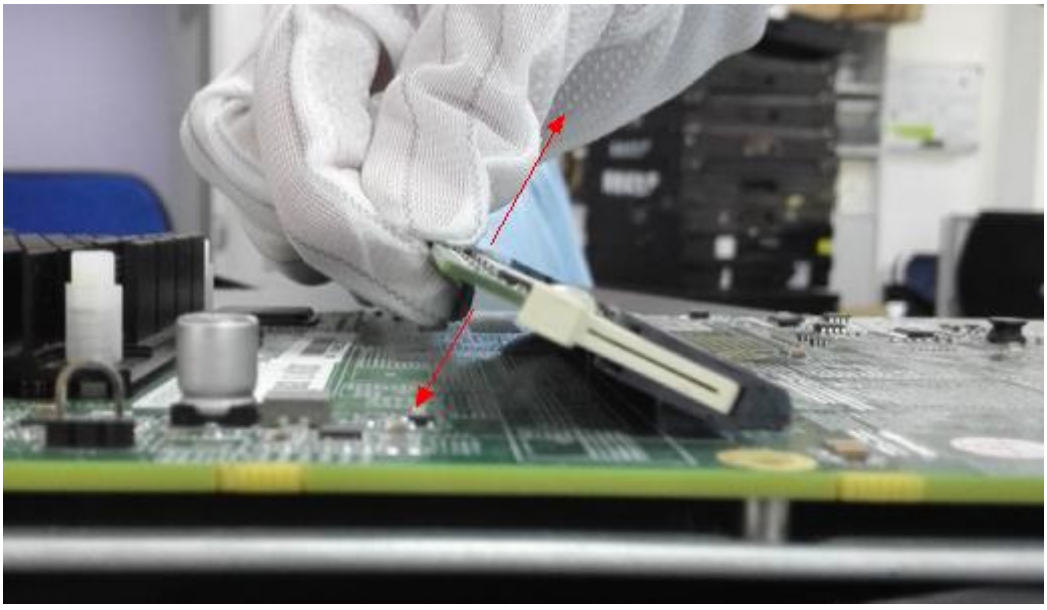


Figure 3

Step 3: Hold both ends of the memory module and socket with index fingers and thumbs, and press the memory module into the socket with force along the direction parallel to the memory module, as shown in Figure 4.

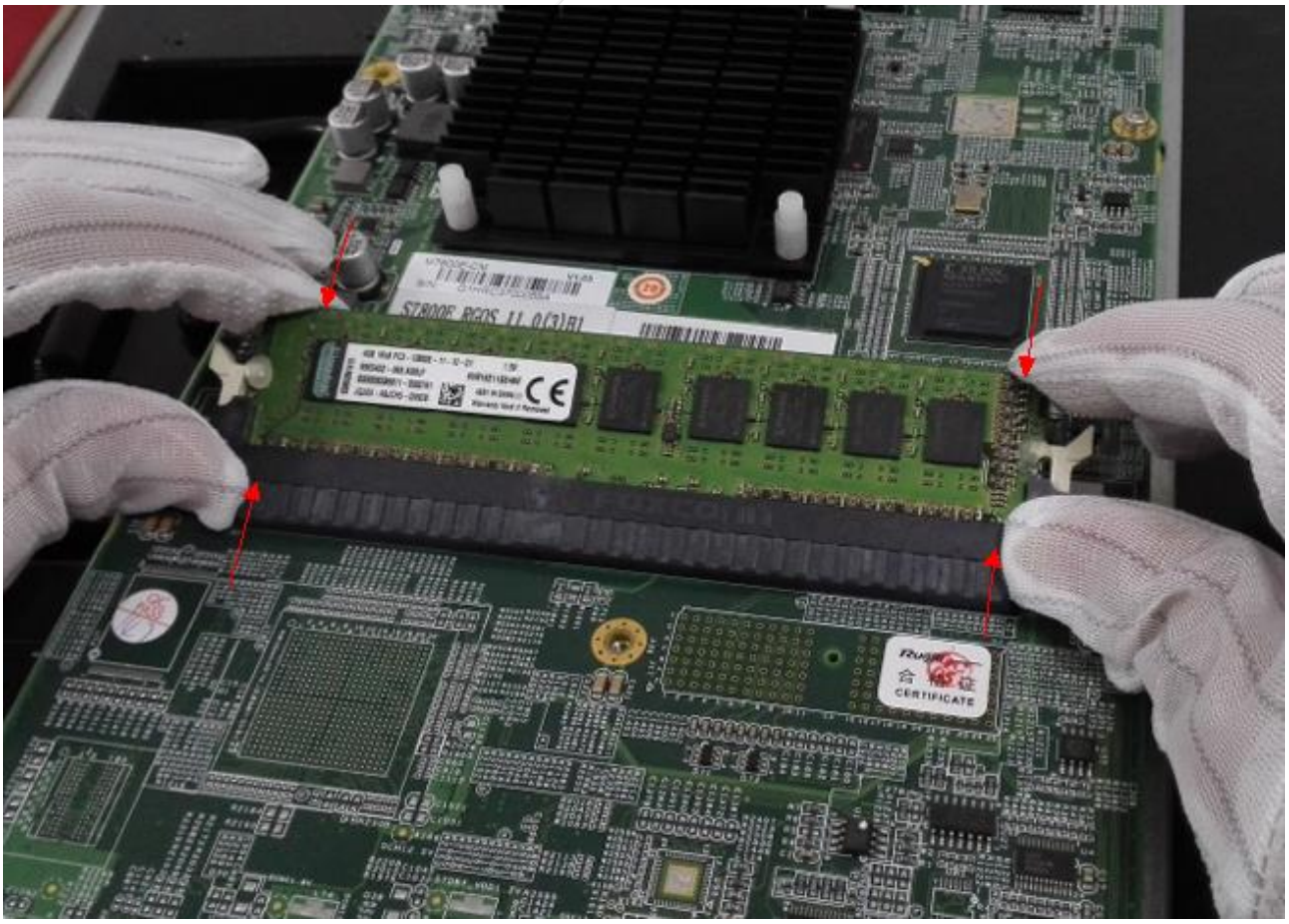


Figure 4

Step 4: Insert the faulty card into the chassis and power on the device.

If the fault is rectified and the device runs properly after the preceding operations are performed, the poor contact is eliminated and the sudden poor contact will not occur on the memory module in the subsequent device running.

If the fault persists after the preceding operations are performed, you are recommended to perform the following operations:

Step 1: When the faulty card encounters the repeated restart symptom, press **Ctrl**+**T** till the card resets and enters the memory self-check state. Then, release the buttons. After the memory self-check is complete, record the collected log for future troubleshooting.

Step 2: Record the customer name, device running duration, device serial number, and other common information.

Step 3: Start the DOA or RMA process for the faulty card.

4.4 Software Upgrade

Q1: What Are Meanings of Different States Displayed After the show upgrade status Command Is Executed?

There are five states in total:

Ready, upgrade, success, transfer, and no information displayed, which are described as follows:

Ready: Indicates that nodes can be upgraded. The engine detects these nodes.

Transfer: Indicates that bin files are being transferred to a card.

Upgrade: Indicates that an upgrade is in progress.

Success: Indicates that a card is upgraded successfully.

No information displayed: Indicates that a card cannot be identified.

Q2: When a Device Using the RGOS 11.X Software Platform Is Upgraded in a VSU Environment, Does the Device Need to Be Split for the Upgrade?

The device does not need to be split for upgrade. The software released after August 2014, with uboot later than version 1.2.7 can be directly upgraded in VSU mode.

Q3: What Are Differences Between a Rack Package and a Hot Patch Package?

Rack package:

A rack package version contains the engine, cards, FE cards, FW cards, and other service cards. When a rack package is used for an upgrade, relevant parts are upgraded accordingly. A device needs to be restarted when the device is upgraded using a rack package.

Hot patch package:

A hot patch package contains hot patches of multiple function components. It is often used to fix small bugs. When a device is upgraded using a hot patch package, patches are installed for function components. After the upgrade, the device supports new functions immediately and it does not need to be restarted.

In general, the name of a hot patch package is *xx* patch.bin. For details, see relevant release notes.

Q4: Case — A Card Fails to Be Identified

[Fault Background]

The 78E uses a single engine and one EB card and the EB card cannot be identified. After a console cable is inserted into the card, the card is always restarted. After the console cable is inserted into the engine and the show version detail command is executed, it is found that the version is S7800E_RGOS 11.0(1)B2 (M00532809022014).

```
    Ruijie#show version  detail
    System description      : Ruijie High-density IPv6 100G Core Routing Switch(S7805E) By Ruijie
Networks
    System start time       : 2014-12-28 10:58:48
    System uptime           : 0:00:51:20
    System hardware version : 1.00
    System software version : S7800E_RGOS 11.0(1)B2
    System patch number     : NA
    System software number  : M00532809022014
    System serial number    : G1HL524000127
    System boot version     : 1.2.7.ef4d454(140722)
    System core version     : 2.6.32.dcfcf416d758ea
    System cpu partition    : 2-3
    Module information:
      Slot M1 : M7800E-CM
        Hardware version    : 1.00
        System start time   : 2014-12-28 10:58:48
        Boot version        : 1.2.7.ef4d454(140722)
        Software version    : S7800E_RGOS 11.0(1)B2
        Software number     : M00532809022014
        Serial number       : G1HL524000127
```

[Handling Procedure]

1. Copy the following card program file and main program file to a USB flash drive:

   Card program: main_ca-octeon-lc_RGOS11.0(3)B1_01241813.bin. Rename it main_ca-octeon-lc.bin.

   Main program: S7800E_RGOS11.0(3)B1_CM_01241814_install.bin

   **********Perform the following operations on the CM engine**********

2. Remove the EB card and upgrade the device to 11.0(3)B1. The steps are as follows:

   Step 1: Run dir usb0:/ to check that the two files are in the USB flash drive and the file size is correct.

```
Ruijie#dir usb0:/
Directory of usb0:/
   1 drwx          4096  Thu Jan  1 00:00:00 1970  .
   2 drwx           416  Tue Nov  4 18:58:07 2014  ..
   3 -rwx      67803445  Sun Dec 28 11:39:06 2014  main_ca-octeon-lc.bin
   4 -rwx     226098336  Sun Dec 28 11:42:12 2014  S7800E_RGOS11.0(3)B1_CM_01241814_install.bin
2 files, 2 directories
536870912 bytes total (7,693,602,816 bytes free)
```

Step 2: Run the upgrade usb0:S7800E_RGOS11.0(3)B1_CM_01241814_install.bin command to upgrade the device:

```
Ruijie#upgrade usb0:S7800E_RGOS11.0(3)B1_CM_01241814_install.bin
Ruijie#Ready for release /mnt/usb0/ca-octeon-cm.bin
*Dec 28 11:57:23: %7: Decompress to /mnt/usb0/ca-octeon-cm.bin
*Dec 28 11:57:24: %7: Release completed 10%
*Dec 28 11:57:24: %7: Release completed 20%
*Dec 28 11:57:25: %7: Release completed 30%
*Dec 28 11:57:25: %7: Release completed 40%
*Dec 28 11:57:26: %7: Release completed 50%
*Dec 28 11:57:26: %7: Release completed 60%
*Dec 28 11:57:27: %7: Release completed 70%
*Dec 28 11:57:27: %7: Release completed 80%
*Dec 28 11:57:28: %7: Release completed 90%
*Dec 28 11:57:28: %7: Release completed 100%
*Dec 28 11:58:00: %7: [Slot M1]:Upgrade processing is 10%
*Dec 28 11:58:21: %7: [Slot M1]:Upgrade processing is 60%
*Dec 28 12:00:23: %7: [Slot M1]:Upgrade processing is 90%
*Dec 28 12:00:25: %7: [Slot M1]:
*Dec 28 12:00:25: %7: Upgrade info [OK]
*Dec 28 12:00:25: %7:   Kernel version[2.6.32.dcfcf416d758ea->2.6.32.4fbb9cc8be12f6]
*Dec 28 12:00:25: %7:   Rootfsversion[1.0.0.09da5efa->1.0.0.5e842dee]
*Dec 28 12:00:25: %7: [Slot M1]:Reload system to take effect!
*Dec 28 12:00:28: %7: [Slot M1]:Upgrade processing is 100%
*Dec 28 12:00:29: %7: %PKG_MGMT:auto-syncconfig synchronization, Please wait for a moment....
*Dec 28 12:00:29: %7: [Slot M1]
*Dec 28 12:00:29: %7:   device_name: ca-octeon-cm
*Dec 28 12:00:30: %7:   status:      SUCCESS
```

Step 3: Run the **show upgrade status** command to check whether all cards except the EB card are upgraded successfully.

Step 4: After confirming that the upgrade is successful, restart the device:

```
S7805E#reload
Reload system?(y/N)y
```

Step 5: After restart, insert the EB card and check whether the EB card can be automatically synchronized. If yes, restart the device and check that the card is upgraded successfully. If no, proceed with the following steps.

Step 6: Upgrade the EB card.

Copy the upgrade package to the **tmp** directory of the main supervisor module.

(Note: Ensure that the card program is renamed **main_ca-octeon-lc.bin**. Otherwise, the file cannot be copied successfully.)

- Run the **run-system-shell** command in global configuration mode to enter the shell screen.
- Restart the tftp process:

```
cd /mnt/usb0
pkill recover_server
uboot-tftp-srv          //Restart the tftp process.
ps -e | grep tftp   //Check whether the tftp process is normal.
```

An example of the preceding commands is as follows:

```
Ruijie#run-system-shell
~ #cd /mnt/usb0
/mnt/usb0 # pkill recover_server
/mnt/usb0 # uboot-tftp-srv
killall: upgrade_inotify_path: no process killed
killall: in.tftpd: no process killed
/mnt/usb0 # sh: turning off NDELAY mode
/mnt/usb0 # ps -e | grep tftp
 1864 ?        00:00:00 tftp_tipc_serve
 3837 ?        00:00:00 in.tftpd
```

*****************************Perform the following operations on the EB card*******************************

Step 7: Erase the original bin file in the EB card (format the card). The operations are as follows:

1) Insert the console port into the EB card and insert the card into the device.

A. Press Ctrl+C to enter the uboot state.

```
====== BootLoaderMenu("Ctrl+Z" to upper level) ======
       TOP menu items.
  ************************************************
      0. Tftp utilities.
       1. XModem utilities.
```

```
          2. Run main.
         3. SetMac utilities.
          4. Scattered utilities.
   ************************************************
             Press a key to run the command:
```

B. Enter 4 (that is, select 4. Scattered utilities)

```
   ====== BootLoaderMenu("Ctrl+Z" to upper level) ======
          Scattered utilities.
     ************************************************
        0. Show the bootloader version.
       1. Reload system.
        2. Set baudrate.
        3. Advanced settings.
     ************************************************
     Press a key to run the command:
```

C. Enter 3 (that is, select 3. Advanced settings).

```
   ====== BootLoaderMenu("Ctrl+Z" to upper level) ======
          Advanced settings.
   ************************************************
           0. Set isolatecpus.
           1. Set Fast boot.
           2. Set Support Shell.
           3. Open/Close debug switch.
           4. Format flash filesystem.
           5. Set default environment.
   ************************************************
     Press a key to run the command:
```

D. Enter 4 (that is, select 4. Format flash filesystem) to format the file system of the EB card.

2) After formatting the file system of the EB card, remove and then insert the EB card, and wait one minute.

If multiple number signs (####) are displayed, the upgrade is successful. Enter **y** when a prompt requesting you to enter y or n.

******************************Perform the following operations on the engine**********************************

Step 8: After the EB card is upgraded successfully, power off and then restart the device, and run the **show version detail** command to check whether the version is correct.

Note: If a firewall card fails to be identified or the one-click upgrade is unsuccessful, the card program package cannot be used for upgrade. In this case, use the firewall card upgrade package of a relevant version for the upgrade.

If the uboot of the card is earlier than version 1.2.9, the uboot of the card needs to be upgraded. The procedure is as follows:

1. Connect the EB card to a serial cable and upgrade the uboot of the EB card over the XMODEM protocol as follows:

Step 1: Restart the EB card, press Ctrl+C during startup to enter the uboot screen:

```
====== BootLoader Menu("Ctrl+Z" to upper level) ======
    TOP menu items.
***********************************************
      0. Tftp utilities.
      1. XModem utilities.
      2. Run main.
      3. SetMac utilities.
      4. Scattered utilities.
 ***********************************************
     Press a key to run the command:
```

Step 2: Enter 1 (that is, select 1. XModem utilities)

```
====== BootLoader Menu("Ctrl+Z" to upper level) ======
      XModem utilities.
***********************************************
      0. Upgrade bootloader.
      1. Upgrade kernel and rootfs by install package.
      2. Upgrade the entire device by distribute package.
  ***********************************************
Press a key to run the command:
```

Step 3: Enter 0 (that is, select 0. Upgrade bootloader). Then, choose Transmission > Send Xmodem on the SecureCRT, and select the uboot file for the upgrade.

Step 4: Enter y when a prompt requesting you to enter y or n.

4.5 Layer-2 Switching Technology

Q1: What Are Functions of Proxy ARP in a Sub VLAN of a Super VLAN?

The proxy ARP function of a Sub VLAN is used in combination with the proxy ARP function of a Super VLAN. If the proxy ARP function of a Sub VLAN is disabled, the inter-Sub VLAN access is not supported.

Such a design aims at facilitating operations. If the proxy ARP function of a single Sub VLAN is disabled, it takes effect only on the Sub VLAN. Therefore, the proxy ARP function of a Sub VLAN can be disabled as required. To disable the proxy ARP function of all Sub VLANs in a Super VLAN, disable the proxy ARP function of the Super VLAN.

```
Ruijie#show supervlan
supervlan id  supervlan arp-proxy  subvlan id  subvlan arp-proxy  subvlan ip range
------------  -------------------  ----------  -----------------  ------------------------
          10                  OFF          11                 ON
                                           12                 ON
                                           13                 ON
                                           14                 ON
                                           15                 ON
                                           16                 ON
                                           17                 ON
                                           18                 ON
                                           19                 ON
                                           20                 ON
```

Q2: How Does the N18000 Process Data with the Destination MAC Address of All 0's?

When the data is used for Layer-2 communication:

1. If the destination MAC address is all 0's and the source MAC address is normal, the device floods the data.
2. If the source MAC address is all 0's and the destination MAC address is normal, the device does not learn the MAC address and normally forwards the data.

When the data is used for Layer-3 communication:

1) If the destination MAC address is all 0's and the source MAC address is normal, the device does not forward the data at Layer 3 because the destination MAC address is not the MAC address of the device.

2) If the source MAC address is all 0's and the destination MAC address is normal, the device normally forwards the data.

Q3: Can Load Balancing of AP Interfaces Be Configured in Interface Configuration Mode Rather Than in Global Configuration Mode for the N18000, S86E, and S78E?

Currently, the load balancing of AP interfaces can be configured in interface configuration mode for the N18000, S86E, and S78E and the configuration takes effect on AP interfaces. Therefore, different load balancing methods can be adopted for AP interfaces based on their traffic characteristics.

The configuration commands are as follows:

```
Ruijie(config)#interface aggregateport 1
Ruijie(config-if-AggregatePort 1)#aggregateport load-balance src-dst-ip
```

Q4: After Interfaces of the N18000 Are Aggregated, Why Does the Speed Displayed After the show interface status Command Is Executed Keep Unchanged?

The speed displayed after the show interface status command is executed is the speed of a member interface rather than the speed of the aggregate port. If the speeds of member interfaces that are statistically aggregated are different, the speed of the last member interface in the up state is displayed after this command is executed.

The details are as follows:

```
Ruijie(config)#int range g1/21 - 22
Ruijie(config-if-range)#port-group 1
Ruijie#show interface status | in up
InterfaceStatus    Vlan   Duplex   Speed     Type
GigabitEthernet 1/21up1Full1000Mcopper
GigabitEthernet 1/22up1Full1000Mcopper
AggregatePort 1     up1Full     1000M     copper
```

To display the speed of AP Port 1, run the **show interface aggregateport** *X* command**:**

```
Ruijie#show interface aggregateport 1
Index(dec):97 (hex):61
AggregatePort 1 is UP  , line protocol is UP
  Hardware is AggregateLink AggregatePort, address is 1414.4b75.bc96 (bia 1414.4b75.bc96)
  MTU 1500 bytes, BW 2000000 Kbit
  Aggregate Port Informations:
Aggregate Number: 1
Name: "AggregatePort 1"
Members: (count=2)
GigabitEthernet 1/21Link Status: Up
GigabitEthernet 1/22Link Status: Up
```

Q5: After a Member Interface of the N18000 Exits from an AP Aggregate Port, Why Cannot the Member Interface Be in the Up State If No Configuration Is Performed?

After a member interface exits from an AP aggregate port, the shutdown command is automatically executed on the member interface to prevent loops.

4.6 Layer-3 Switching Technology

Q1: When a Device Functions as a DHCP Server, How to Set Option Fields?

The following uses a case to answer this question. A customer's DHCP server is configured on a Ruijie switch. A client needs to acquire the server file startup path from the switch through DHCP Option 66. The server file startup path is 10.0.1.4:/var/tmp/rootfs. The configuration is as follows:

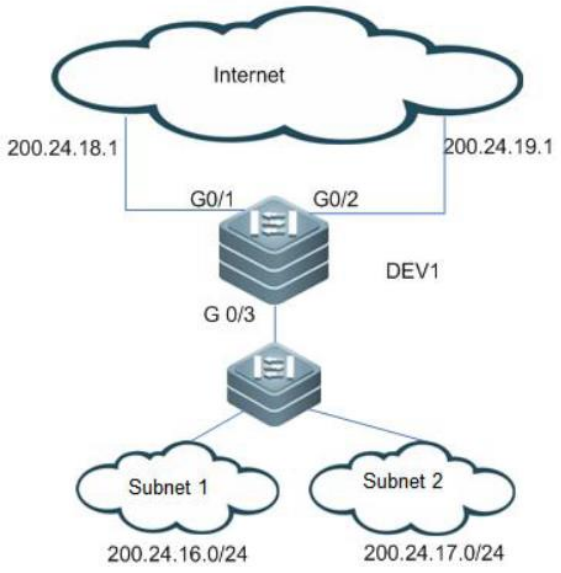
```
ip dhcp pool ruijie
 option 66 ascii 10.0.1.4:/var/tmp/rootfs
```

Notes: In the configuration:

```
Ruijie(dhcp-config)#option 66 ?
  ascii  Data is an NVT ASCII string     //Common string
  hex    Data is a hexadecimal string   //String in hexadecimal notation, that is, characters ranging from 0 to F
  ip     Data is one or more IP addresses  /IP address
```

In the test: The switch replies with the Option 66 field only when the client requests the Option 66 field.

Q2: When PBR Is Configured for a Device Using the RGOS 11.X Software Platform, Can the Device Be Correlated to Monitor the Next-Hop Reachability Based on the PBR and Perform Operations Based on the Up/Down State of Interfaces?



As shown in the Figure-1, DEV1 connects to subnets 1 and 2 through G0/3, and connects to the Internet through G0/1 and G0/2 with the next hop of 200.24.18.1 and 200.24.19.1, respectively. Subnet 1's segment is 200.24.16/20 and subnet 2's segment is 200.25.19.1.

Correlation with DLDP

PBR part:

```
Ruijie(config)#ip access-list standard network_1
Ruijie(config-std-nacl)# 10 permit 200.24.16.0 0.0.0.255
Ruijie(config)#ip access-list standard network_2
Ruijie(config-std-nacl)# 10 permit 200.24.17.0 0.0.0.255
Ruijie(config)#route-map PBR permit 10
Ruijie(config-route-map)# match ip address network_1
Ruijie(config-route-map)# set ip next-hop 200.24.18.1
Ruijie(config-route-map)# set ip next-hop 200.24.19.1
Ruijie(config-route-map)#!
Ruijie(config-route-map)#route-map PBR permit 20
Ruijie(config-route-map)# match ip address network_2
Ruijie(config-route-map)# set ip next-hop 200.24.19.1
Ruijie(config-route-map)# set ip next-hop 200.24.18.1
Ruijie(config)#ip policy redundance //Change the mode to redundancy backup mode.
Ruijie(config)#int g0/3
Ruijie(config-if-GigabitEthernet 0/3)#ip policy route-map PBR //Interface calling
```

DLDP part:

```
Ruijie(config)#int g0/1
```

```
Ruijie(config-if-GigabitEthernet 0/1)#dldp 200.24.18.1
Ruijie(config)#int g0/2
Ruijie(config-if-GigabitEthernet 0/1)#dldp 200.24.19.1
```

Principle introduction:

By default, PBR selects the next hop based on the common routing before the next-hop interface becomes down. In redundancy backup mode, PBR selects the next hop in polling mode. Therefore, DLDP can be used to detect the reachability of the next-hop address. If the DLDP detection result is unreachable, PBR actively changes the next-hop Layer-3 interface to the down state, thereby resolving connectivity detection of indirectly connected devices. In the preceding figure, DEV1 is directly connected to a carrier device and therefore DLDP is not required. If DEV1 is connected to a carrier device through a Layer-2 device or an optical-to-electrical converter, DLDP needs to be configured to implement switching.

4.7 Security Technology

Q1: The Client Authentication Fails and a Prompt Indicating Server Unregistered Is Displayed.

Common Causes

1. The NAS device encapsulates its IP address into a redirection packet and sends the packet to the portal device for check during Web authentication. If the IP address is inconsistent with the IP address stored on the portal device, a prompt indicating server unregistered is displayed.
2. The portal key is configured incorrectly on the NAS device.

Solution

For the first cause:

1. For a device using the RGOS 11.X software platform, run the ip portal source-interface command to change the IP address.
2. The default IP address sent by the NAS device is the latest IP address encapsulated and sent to the portal device that is contained in the routing table. Therefore, change the IP address on the portal device to rectify the fault.

For the Second Cause:

Check whether the key on the portal device and the key on the NAS device are configured correctly.

Q2: 2nd-generation Web Authentication Needs to Be Configured on the N18000 and a User Gateway Is Connected to the N18000. How to Configure Web Authentication in a Layer-3 Architecture?

When a user passes Web authentication and goes online successfully, the device needs to write the user entry into forwarding rules and specify a binding mode. The matching mode of forwarding rules can be adjusted to change the Internet access rules of users. For example, when only IP binding is adopted, packets that match the IP address are forwarded and the user can access the Internet. When IP+MAC binding is adopted, only users whose packets match both the IP address and MAC address can access the Internet.

In a Layer-3 authentication scenario, MAC addresses contained in packets received by the device are the address of the user gateway rather than the MAC addresses of users. Therefore, the IP binding mode should be adopted. Web authentication is based on IP+MAC binding by default. Users can determine the binding mode according to the accurate user information that can be obtained by the device. When both the IP addresses and MAC addresses of users are accurate, for example, in Layer-2 network deployment, IP+MAC binding is preferred. Otherwise, IP binding is preferred.

The configuration reference is as follows:

```
Ruijie(config)#web-auth template eportalv2   //Access the template.
Ruijie(config.tmplt.eportalv2)#bindmode ip-only-mode   //Change the binding mode to IP binding.
```

Note: IP binding needs to be enabled in the Web template and is not applicable to large gateway scenarios. If the authentication mode is gateway mode, the error "%Error: ip-only-mode can not be used in gateway mode." is displayed after the preceding command is executed. Change the command to the following:

```
Ruijie(config.tmplt.eportalv2)#bindmode ip-mac-mode  //Change the binding mode to IP+MAC binding.
```

Q3: In a N18000+WS Environment, Web Authentication Needs to Be Enabled for Users Connected to an AP. How to Perform Deployment on the N18000?

If the AP uses centralized forwarding mode, when Web authentication is enabled for wireless users on the N18000, the Web controlled function needs to be enabled on the internal connection port of the WS connected to the N18000 and the management VLAN of the AP needs to be configured as a free-authenticated VLAN.

If the AP uses local forwarding mode, when Web authentication is enabled for wireless users on the N18000, the Web controlled function needs to be enabled on the port of the N18000 that is directly connected to the AP and the management VLAN of the AP needs to be configured as a free-authenticated VLAN.

Q4: What Is Web Authentication Noise?

HTTP packets transmitted by a terminal are first processed by Newton switch that functions as a NAS device. When the NAS device redirects the terminal, the pushed message contains a script that allows only the standard browser to be identified and redirected, preventing software such as QQ and Xunlei from sending a large number of HTTP requests and overloading the server. The standard browser terminal will be redirected to interact with the ePortal service.

Q5: Both the http redirect direct-site 1.1.1.1 and the web-auth direct-host 1.1.1.1 Commands Are Used to Configure IP Free-authentication Access. What Are Their Differences?

direct-site allows passing of packets whose destination IP address matches the access destination IP address. For example, if direct-site is set to the IP address of a SAM server, users do not need to be authenticated to access this destination IP address.

direct-host allows passing of packets whose source IP address matches the access source IP address. For example, if direct-host is set to the IP address of a printer, the printer does not need to be authenticated to access user terminals. If users need to access the printer without authentication,

direct-site can be configured to the same IP address of direct-host.

Q6: When DOT1X Is Configured on the N18000, What Are Differences Between Gateway Mode and Access Mode?

1. Resources are more optimized in gateway mode. Devices have larger authentication entries in comparison with the access mode.
2. If access control-relevant application is deployed on a core device, the authentication mode needs to be switched to gateway authentication mode on the core device. Otherwise, no configuration is required.
3. After the authentication mode is switched, the new mode takes effect only after the device is restarted. Save the configuration before restarting the device.
4. Configuration method:

Method	authentication.
Switch A	SwitchA(config)#auth-mode gateway Please save config and reload system. SwitchA(config)#exit *Nov 7 10:13:27: %SYS-5-CONFIG_I: Configured from console by console SwitchA#reload Reload system?(Y/N)y SwitchA#
Verification	Use the **show running** command to check whether the configuration has taken effect.
Switch A	SwitchA(config)#show running-config | include auth-mode auth-mode gateway SwitchA(config)#

Q7: How to Implement Free Authentication for a Single VLAN in DOT1X/Web Environment?

A free-authenticated VLAN can be configured so that users in the specified VLAN can access the Internet without passing the DOT1X authentication or Web authentication. A device on which free-authenticated VLANs are configured directly skips the access control detection when receiving packets from VLANs contained in the free-authenticated VLAN list, thereby allowing users in free-authenticated VLANs to access the Internet without authentication. The free-authenticated VLAN function can be considered as one application of the secure channel. No free-authenticated VLAN is configured by default. The configuration command is as follows:

[Command] Global mode: [no] direct-vlan vlanlist //no: Indicates that free–authenticated VLANs are deleted if this option is configured. vlanlist: Indicates the configured or deleted free-authenticated VLAN list.

Example: Configure VLAN 100 and VLAN 200 as free-authenticated VLANs and display configured free-authenticated VLANs.

```
Ruijie(config)#direct-vlan 100,200 //Configure VLAN 100 and VLAN 200 as free-authenticated VLANs.
Ruijie#show direct-vlan//Check free-authenticated VLANs configured on the device.
direct-vlan 100,200
```

Notes:

1. The N18000, 86E, and 78E support a maximum of 100 free-authenticated VLANs currently.
2. Free-authenticated VLANs occupy hardware entries. If authentication and other access control functions are disabled, the effects are the same regardless of whether free-authenticated VLANs are configured. It is recommended that free-authenticated VLANs be configured for special users who request to access the Internet without authentication only when relevant access control functions are enabled.
3. Free-authenticated VLANs do not participate in the access authentication detection but must pass the security ACL check. If specified users or VLANs that are not allowed to pass are configured in the ACL, the users cannot access the Internet

even though free-authenticated VLANs are configured for them. Therefore, when configuring the ACL, do not add a specified VLAN or users in a specified VLAN to the ACL so that users in the free-authenticated VLAN can truly access the Internet without authentication.

4.8 Reliability

Q1: Does the Device Using the RGOS 11.X Software Platform Needs to Be Restarted When a VSL Is Added in VSU Mode?

The device does not need to be restarted.

A new VSL takes effect immediately after the configuration is complete, the VSU or the card where the VSL is configured does not need to be restarted. Likewise, users can also delete an existing VSL. The deletion takes effect immediately after the configuration is complete.

Q2: A VSU Cannot Be Created After the VSL Between Two Devices Passes Through An Intermediate Device.

Principle Analysis

When a VSU is created, data packets that pass through the VSL are HG packets for internal communication rather than common Ethernet packets. If the intermediate device of the VSL does not support non-Ethernet packets, the VSU cannot be created.

Q3: Three Devices Using the RGOS 11.X Software Platform Are Used to Create a VSU. What Are Differences Between the VSL Configuration and That on Devices Using the RGOS 10.X Software Platform?

Configuration Differences

11.x

```
vsl-port
port-member interface tenGigabitEthernet 1/1
port-member interface tenGigabitEthernet 1/2
```

10.x

```
vsl-aggregateport 1
port-member interface tenGigabitEthernet 1/1  fiber
```

```
    vsl-aggregateport 2   //Add the link used for interconnecting to another device to another aggregate group.
    port-member interface tenGigabitEthernet 1/2  fiber
```

Principle Analysis

For devices using the RGOS 10.X software platform, specified ports of different devices need to be added to an aggregate group, and connection errors may occur in this case. Improvements are made to devices using the RGOS 11.X software platform and only ports need to be added to one resource pool. Then, the software automatically negotiates to add them to an aggregate group, without manual intervention.

Q4: When Two Devices Are Used to Create a VSU, vsl-ap1 and vsl-ap2 Are Displayed After the show switch virtual link Command Is Executed, Why vsl-ap2 Is Down?

When two devices using the RGOS 11.X software platform are used to create a VSU, they are added to vsl-ap1 by default and therefore, vsl-ap2 is down.

VSLs between devices using the RGOS 11.X software platform are automatically added to different vsl-aps, which is applied when more than two devices are used to create a VSU. Ports only need to be configured as VSL ports. Then, the devices automatically add these VSL ports to different APs, so as to differentiate VSLs between different devices.

Q5: What Are Hardware Requirements for VSLs When the S7800E, N18000, or S8600E Is Used to Create VSUs?

Cards with 10G interfaces or 40G ports are required when the S7800E, N18000, or S8600E is used to create VSUs. The N18000, S8600E, and S7800E support the CB, DB, ED, EF, and EB cards currently. Pay attention to the following rules when creating VSUs:

1. CB cards can be used only with CB cards to create VSUs.
2. The DB, ED, EF, and EB cards can be used alone or in combination to create VSUs.

4.9 NMS and Monitoring

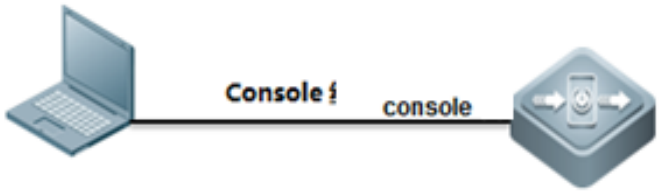
Q1: How to Restore the Password of Mid-range and Low-end Box-type Switches?

Notes

1. Get a configuration cable ready when restoring the password.
2. Password restoration is performed at the CTRL layer during device restart. The network needs to be disconnected. Perform password restoration operation when the network can be disconnected.
3. Strictly follow the operation steps. Improper operations may cause configuration loss.
4. Passwords of switches using the RGOS 11.X software platform are restored by saving the configuration.

Password Restoration Steps

Step 1: If an administrator forgets the login password and fails to enter the configuration mode. Use a configuration cable to enter the CTRL layer to restore the password.



Step 2: Configure the network device by using HyperTerminal.

1) Manually power off the device and then restart it.

2) When the Ctrl+C prompt is displayed, press Ctrl+C to access the BootLoader menu.

```
====== BootLoader Menu("Ctrl+Z" to upper level) ======
    TOP menu items.
***********************************************
    0. Tftp utilities.
    1. XModem utilities.
    2. Run main.
    3. SetMac utilities.
    4. Scattered utilities.
    5. Set Module Serial
***********************************************
Press a key to run the command:
```

3) Press **Ctrl**+**Q**.

Enter **ubootui**, press **Enter**, and then press **Ctrl**+**P** immediately

```
s29xs#ubootui
Leaving simple UI....
s29xs#
```

4) Run the following commands:

```
s29xs#setenv runlevel 2
s29xs#run linux
Creating 1 MTD partitions on "nand0":
0x000001000000-0x000002e00000 : "mtd=6"
UBI: attaching mtd1 to ubi0
UBI: physical eraseblock size:   131072 bytes (128 KiB)
UBI: logical eraseblock size:    126976 bytes
UBI: smallest flash I/O unit:    2048
UBI: VID header offset:          2048 (aligned 2048)
UBI: data offset:                4096
UBI: attached mtd1 to ubi0
UBI: MTD device name:            "mtd=6"
UBI: MTD device size:            30 MiB
UBI: number of good PEBs:        240
UBI: number of bad PEBs:         0
UBI: max. allowed volumes:       128
UBI: wear-leveling threshold:    4096
UBI: number of internal volumes: 1
UBI: number of user volumes:     1
UBI: available PEBs:             19
UBI: total number of reserved PEBs: 221
UBI: number of PEBs reserved for bad PEB handling: 2
UBI: max/mean erase counter: 2/0
UBIFS: recovery needed
UBIFS: recovery deferred
UBIFS: mounted UBI device 0, volume 0, name "kernel"
UBIFS: mounted read-only
UBIFS: file system size:   26030080 bytes (25420 KiB, 24 MiB, 205 LEBs)
UBIFS: journal size:       3682304 bytes (3596 KiB, 3 MiB, 29 LEBs)
UBIFS: media format:       w4/r0 (latest is w4/r0)
UBIFS: default compressor: LZO
UBIFS: reserved for root:  0 bytes (0 KiB)
Unmounting UBIFS volume kernel!
   Uncompressing Kernel Image ... OK
   Loading Device Tree to 823fc000, end 823ff593 ... OK
Starting kernel ...
5) Run the following commands:
~ #
~ # cd /data/
/data # ls
```

```
/data # mv config.text config_backup.text
/data # sync
/data # reboot
```

Q2: How to Restore Passwords of Case-type Switches?

Notes

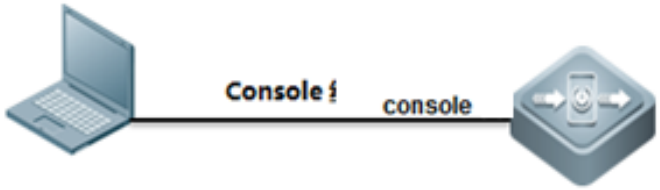
1. Get a configuration cable ready when restoring the password.
2. Password restoration is performed at the CTRL layer during device restart. The network needs to be disconnected. Perform password restoration operation when the network can be disconnected.
3. Strictly follow the operation steps. Improper operations may cause configuration loss.
4. Passwords of switches using the RGOS 11.X software platform are restored by saving the configuration.

Configuration Key Points

1. Get a configuration cable (console cable) ready for password restoration. The device needs to be restarted and password restoration needs to be completed at the CTRL layer.
2. The password restoration of switches using the RGOS 11.X software platform takes effect only at the current time. That is, if there is no input within 10 minutes after the CLI is displayed. A password still needs to be entered after timeout occurs. If the password is not changed after the CLI is displayed, the previous password is still required at the next restart of the device.

Password Restoration Steps

Step 1: If an administrator forgets the login password and fails to enter the configuration mode. Use a configuration cable to enter the CTRL layer to restore the password.



1. Manually power off the device and then restart it.
2. When the Ctrl+C prompt is displayed, press Ctrl+C to access the BootLoader menu.

```
System bootstrap ...
Nor Flash ID: 0xC2CB0000, SIZE: 8388608Bytes
Press Ctrl+B to enter Boot Menu .....
Load Ctrl Program ...

Executing program, launch at: 0x00010000


Self decompressing the image :
#################################################################
Ctrl Version: RGOS 10.4(2b2) Release(102500)
MTD_DRIVER-5-MTD_NAND_FOUND: 1 NAND chips(chip size : 134217728
1 nand chip(s) found on the target.
Press Ctrl+C to enter Ctrl ...  ---->  Press constantly
                                        :
Hot Commands:
-------------------------------------------------------------
F1. tftp 192.168.0.2 192.168.0.1 rgos.bin -main
-------------------------------------------------------------
Ctrl>^C
Ctrl>  ---->  Ctrl mode
```

3. rename config.text ---->config.bak

```
Ctrl>
Ctrl>rename config.text config.bak
Ctrl>
```

4. load firmware

```
Ctrl>load
```

5. recovery the previous config file

```
Ruijie#rename flash:config.bak flash:config.text
Ruijie#copy startup-config running-config
```

```
Ruijie#copy flash:config.bak flash:config.text
Ruijie#copy startup-config running-config
```

6. Set new password

```
Ruijie(config)#
Ruijie(config)#enable secret ruijie ──► New password
Ruijie(config)#line vty 0 4
Ruijie(config-line)#password ruijie ──► New telnet pwd
Ruijie(config-line)#login
Ruijie(config-line)#end
Ruijie#*Feb 27 19:35:14: %SYS-5-CONFIG_I: Configured from conso

Ruijie#wr ──► Save config file

Building configuration...

[OK]
```

Q3: How to Copy Information Collected in One-click Mode over TFTP When No USB Flash Drive Is Available?

When no USB flash drive is available, case-type devices using the RGOS 11.X software platform (78E/86E/N18000) store information that is collected in one-click in the temporary directory TMP/VSD/0. Files in this directory need to be copied to the flash memory and hen copied to another position over TFTP.

The operation steps are as follows:

Step 1: Enter the debug su mode and start one-click information collection (no USB flash drive needs to be inserted):

```
Ruijie#debug su
Ruijie(support)#tech-support package
```

Step 2: Copy files that are collected in one-click mode in the temporary directory TMP/VSD/0 to the flash memory.

```
run-system-shell
cp /tmp/vsd/0/tech_support* /data
sync
exit
```

Step 3: Copy the files to another position over TFTP.

Q4: How to Handle When the USB Flash Drive Inserted into the N18000 Is Not Displayed on the Configuration Screen?

Symptom:

```
N18010#
N18010#
N18010#*Jul  7 10:06:36: %7: usb 1-1: USB disconnect, address 3
USB-5-USB_DISK_REMOVED: USB Disk [sda] has been removed from USB port[0].
*Jul  7 10:06:41: %7: usb 1-1: new high speed USB device using octeon-ehci and address 4
*Jul  7 10:06:41: %7: usb 1-1: configuration #1 chosen from 1 choice
*Jul  7 10:06:41: %7: usb stor probe1 register led cpu-usb1
*Jul  7 10:06:41: %7: scsi2 : SCSI emulation for USB Mass Storage devices
*Jul  7 10:06:41: %7: usb-storage: device found at 4
*Jul  7 10:06:41: %7: usb-storage: waiting for device to settle before scanning
[ 1439.787120] scsi 2:0:0:0: Direct-Access     Teclast  CoolFlash        8.07 PQ: 0 ANSI: 4
[ 1439.892717] sd 2:0:0:0: [sda] 30720000 512-byte logical blocks: (15.7 GB/14.6 GiB)
[ 1439.985483] sd 2:0:0:0: [sda] Write Protect is off
*Jul  7 10:06:47: %7: usb-storage: device scan complete[ 1440.043104] sd 2:0:0:0: [sda] Assuming drive cache: write through

[ 1440.176987] sd 2:0:0:0: [sda] Assuming drive cache: write through

[ 1440.331490] sd 2:0:0:0: [sda] Assuming drive cache: write through
[ 1440.404763] sd 2:0:0:0: [sda] Attached SCSI removable disk
*Jul  7 10:06:47: %7:  sda: sda4
USB-5-USB_DISK_FOUND: USB Disk [sda] has been inserted to USB port[0].

N18010#dir us
N18010#dir usb0:
Dir failed. No such file or directory
N18010#
```

```
N18010#dir
Directory of flash:/
   1 drw-          288  Sat Apr 19 12:27:33 2014  at
   2 drwx          296  Fri Jan 11 19:55:14 2008  dm
   3 drwx          160  Thu Jan  3 06:24:34 2008  rep
   4 drwx          232  Fri Mar 14 13:29:37 2014  scc
   5 drwx          160  Thu Jan  3 06:24:45 2008  ssh
   6 drwx          224  Thu Jan  3 06:24:35 2008  var
   7 d---          288  Fri Jan 11 19:55:20 2008  web
   8 -rw-            4  Wed Jun  4 12:15:17 2014  .rbcnt
   9 drwx          160  Thu Jan  3 06:24:44 2008  addr
  10 drwx          160  Fri Jan 11 19:55:21 2008  dcb0
  11 drwx          232  Thu Jan  1 00:01:04 1970  cwmp
  12 -rw-          216  Mon Jul  7 10:05:05 2014  config.text.stat
  13 drwx          872  Fri Jan 11 19:55:34 2008  sync
  14 --w-           82  Mon Jul  7 10:05:04 2014  config_vsu.dat
  15 drwx          296  Sat Apr 19 12:27:11 2014  .rgos
  16 -rw-         2136  Mon Jul  7 10:05:05 2014  config.text
  17 -rw-            0  Fri Jan 11 19:55:24 2008  ss_ds_debug.txt
  18 -rwx         8448  Mon Jul  7 10:05:04 2014  .shadow
  19 -rwx          277  Mon Jul  7 10:05:04 2014  .pswdinfo
  20 -rwx          696  Wed Jun  4 11:56:13 2014  httpd_cert.crt
  21 drwx          232  Fri Jan 11 19:55:21 2008  l2gre
  22 -rw-            4  Sun Jul  6 17:22:40 2014  reload
  23 drwx          160  Thu Jan  3 19:46:28 2008  dm_tipc
  24 -rw-        85572  Wed Apr 30 15:51:07 2014  .cap_vsu_file.tar.bz2
  25 drwx          232  Fri Jan 11 19:55:23 2008  snpv4
  26 drwx          232  Thu Jan  1 00:01:03 1970  trill
  27 drwx         5808  Wed Jun  4 12:21:11 2014  .config
  28 -rw-          256  Wed Jun  4 11:56:08 2014  mpsp.txt
  29 drwx          232  Sat Apr 19 12:27:24 2014  rg_licns
  30 drwx          160  Fri Jan 11 19:55:18 2008  syslog
  31 drwx          160  Thu Apr 24 10:05:08 2014  upgrade_ram
  32 drwx          160  Fri Jan 11 19:55:21 2008  vmsup0
  33 drw-          296  Mon Jul  7 10:04:31 2014  cap_file
  34 drwx          296  Fri Jan 11 16:34:14 2008  dm_vdu
  35 drwx          224  Fri Jan 11 19:55:14 2008  dm_vsd
  36 -rwx           16  Sat Mar 22 08:35:39 2014  .username.data
  37 -rwx          887  Wed Jun  4 11:56:13 2014  httpd_key.pem
  38 -rwx         2426  Sat Apr 19 12:53:24 2014  standalone.text
14 files, 24 directories
536870912 bytes total (3,624,960 bytes free)
N18010#
```

When partitions of the USB flash drive adopt the sda4 format, the partitions cannot be automatically mounted on the device. Use a USB flash drive formatting tool to format the USB flash drive and select the FAT32 format for partitions.

After rectification:

```
N18010#dir usb0:
Directory of usb0:/
0 files, 0 directories
536870912 bytes total (7,987,490,816 bytes free)
N18010#
N18010#
N18010#
```

4.10 Typical Case

Q1: What Do I Do When the Device Is Suspended After the M8600-MPLS Card Is Inserted?

Fault Symptom:

Try to insert the ASE3 module into slot 4 and the chassis will be blocked, then we installed into module 8, check the output.

The console is suspended after the M8600-MPLS card is inserted and the displayed status is "resetting".

```
CORE-REMI#  sho version slots
  Dev Slot Port Configured Module            Online Module                User Status  Software St
atus
  --- ---- ---- --------------------------- --------------------------- ------------ -----------
----
  1   1    2    7200-2XG                    7200-2XG                    installed    ok

  1   2    4    7200-4XG                    7200-4XG                    installed    ok

  1   3    4    7200-4XG                    7200-4XG                    installed    ok

  1   4    0    none                        none                        none         none

  1   5    24   7200-24G                    7200-24G                    installed    ok

  1   6    24   7200-24                     7200-24                     installed    ok

  1   7    0    none                        none                        none         none

  1   8    0    7200-ASE3                   7200-ASE3                   installed    resetting

  1   M1   0    N/A                         7200-CM4                    N/A          master

  1   M2   0    N/A                         7200-CM4                    N/A          backup
```

Solution:

1. Check the version.

```
Ctrl>version
Module information:
  Slot-1 : 7200-2XG
    Hardware version : A3.0
    Original main file version : Firmware10.4(3) Release(118208)
    BOOT version     : 10.4  Release (118208)
    CTRL version     : 10.4  Release (118208)
  Slot-2 : 7200-4XG
    Hardware version : A3.0
    Original main file version : Firmware10.4(3) Release(118208)
    BOOT version     : 10.3  Release (76833)
    CTRL version     : 10.4  Release (118208)
  Slot-3 : 7200-4XG
    Hardware version : A3.0
    Original main file version : Firmware10.4(3) Release(118208)
    BOOT version     : 10.3  Release (76833)
    CTRL version     : 10.4  Release (118208)
  Slot-5 : 7200-24G
    Hardware version : A3.0
    Original main file version : Firmware10.4(3) Release(118208)
    BOOT version     : 10.4  Release (118208)
    CTRL version     : 10.4  Release (118208)
  Slot-6 : 7200-24
    Hardware version : A3.0
    Original main file version : Firmware10.4(3) Release(118208)
    BOOT version     : 10.4  Release (118208)
    CTRL version     : 10.4  Release (118208)
  Slot-8 : 7200-ASE3
    Hardware version : A1.0
    Original main file version : FirmwareRGNOS 10.3.00(3b12), Release(40793)
    BOOT version     : 10.3  Release (40793)
    CTRL version     : 10.3  Release (40793)
```

2. It is preliminarily judged that the version is too old and not compatible with the device. Attempt to upgrade cards in CTRL mode.

```
Ctrl>upgrade -slot 8
These images in linecard will be updated:
     Slot     image    linecard
    ------    -----    ------------------------
```

```
          8     CTRL                    7200-ASE3
                MAIN                    7200-ASE3
-----------------------------------------------
(Slot 8): Installing MAIN
(Slot 8): Download imageVerify the image .[ok]

Upgrade file to Module(s) in slot: [8]
Please wait......
Upgrade file to Module in slot [8] OK!
(Slot 8): MAIN installed.
(Slot 8): Install finish in slot 8 (7200-ASE3).
```

3. Restart the device.

Note: Restart the entire device and check whether the version is successfully upgraded under the main program. Otherwise, the version is still the earlier version in CTRL mode.

```
Ctrl>reload
Do you still want to reload system?(y/N):
SYS-5-RESTART: The device is restarting. Reason: Restart the whole system!.
```

4. After checking that the version is upgraded successfully under the main program, the fault is rectified and the device is restored to the normal state.

```
Slot-8 : 7200-ASE3
  Hardware version : A1.0
  Software version : v10.4(3) Release(118208)
  BOOT version     : 10.3 Release(40793)
  CTRL version     : 10.4(3) Release(118208)
Slot-M1 : 7200-CM4
  Hardware version : A2.0
  Software version : v10.4(3) Release(118208)
  BOOT version     : 10.4(3) Release(118208)
  CTRL version     : 10.4(3) Release(118208)
Slot-M2 : 7200-CM4
  Hardware version : A2.0
  Software version : v10.4(3) Release(118208)
  BOOT version     : 10.4(3) Release(118208)
  CTRL version     : 10.4(3) Release(118208)
```

Q2: What Do I Do If the Error "Did not find xxx in xxx.mib" Is Reported When a MIB Node Is Read?

The error log is as follows:

Did not find 'ospfAreaNssaTranslatorState' in module OSPF-MIB (/home/snmp/mibs/RuijieDCN_OSPF-TRAP-MIB-4750.mib)

Did not find 'ospfRestartStatus' in module OSPF-MIB (/home/snmp/mibs/RuijieDCN_OSPF-TRAP-MIB-4750.mib)

In the internal test, locate the OSPF-TRAP-MIB-4750.mib file and the ospfAreaNssaTranslatorState node. The code shows that the OSPF-MIB-4750.mib file must be called to read the node.

Solution: Import the complete MIB files and do not select a separate MIB file for importing.

Q3: What Do I Do When PoE Is Not Disabled After the Shutdown Command Is Executed on a Switch Port?

Description:

The shutdown command executed on a switch port will not disable PoE of the port but disable data communication.

To disable PoE on a switch port, run the no poe enable on the port.

Q4: What Do I Do When the Web Page of the S2900 Cannot Be Opened?

Symptom: When a user logs in to the S2928G-12P from the Web page, a prompt, indicating the username and password are incorrect, is displayed.

Solution:

1. Check the username and password and ensure that the user level is set to 15.

```
    username admin password ruijie
    username admin privilege 15
```

2. Configure the HTTP service and authentication mode.

```
enable service web-server http
enable service web-server https
ip http authentication local
```

3. If the user still fails to log in, the fault may be caused by browser incompatibility. Upgrade the firmware or enable the compatibility mode of the Internet Explorer.

Problem firmware：RGOS 10.4(2b12)p2 Release(180357)

Fixed firmware：RGOS 10.4(2b12)p6 Release(196987)

Q5: What Is the VSU Mechanism of the S2910?

1. When you log in to the slave device of the VSU composed of the S2910H through the console port, how can you log in to the master device?

You can run the session master command to log in to the master device and configure the master device.

2. The election mechanism of the master device, slave device, and candidate devices in the VSU is described as follows:

S29_1 (priority 200, master)------S29_2 (priority 190, backup) -----S29_3 (Priority 180, candidate)----S29_4 (priority 170, candidate)

When the S29_1 is down, the member roles of the VSU are as follows:

S29_1 (down)------S29_2 (priority 190, master) -----S29_3 (Priority 180, backup)----S29_4 (priority 170, candidate)

When the S29_1 recovers, the member roles of the VSU are as follows:

S29_1 (priority 200, candidate)------S29_2 (priority 190, master) -----S29_3 (Priority 180, backup)----S29_4 (priority 170, candidate)

When the S29_2 is down, the member roles of the VSU are as follows:

S29_1(priority 200, backup)------S29_2(priority 190, down)-----S29_3(Priority 180, master)----S29_4(priority 170, candidate)

The slave device of the VSU is the candidate device with the highest priority.

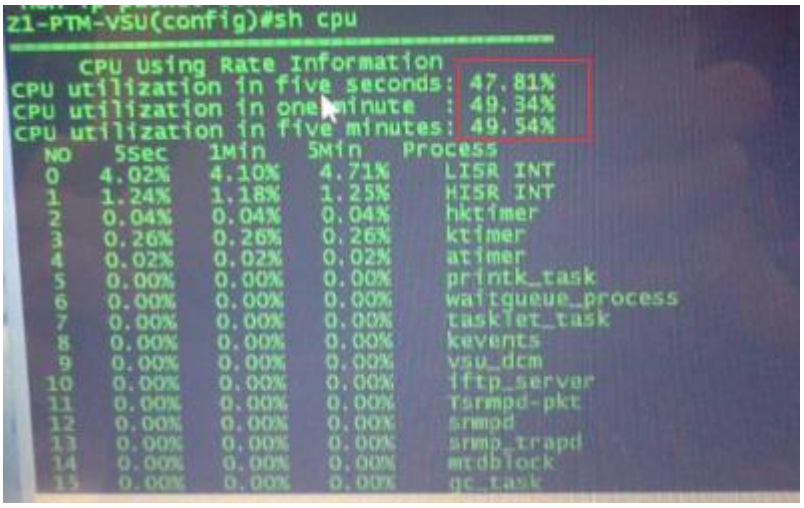
Q6: How Can I View the SN of Optical Transceivers?

Solution: Run the show interface transceiver and show interface transceiver diagnostic commands to display the SN and model information of the optical transceivers.

Q7: When the Device Encounters an OSPF Attack, How Can I Find the Attack Source Rapidly and Take Anti-attack Measures?

Fault Symptom

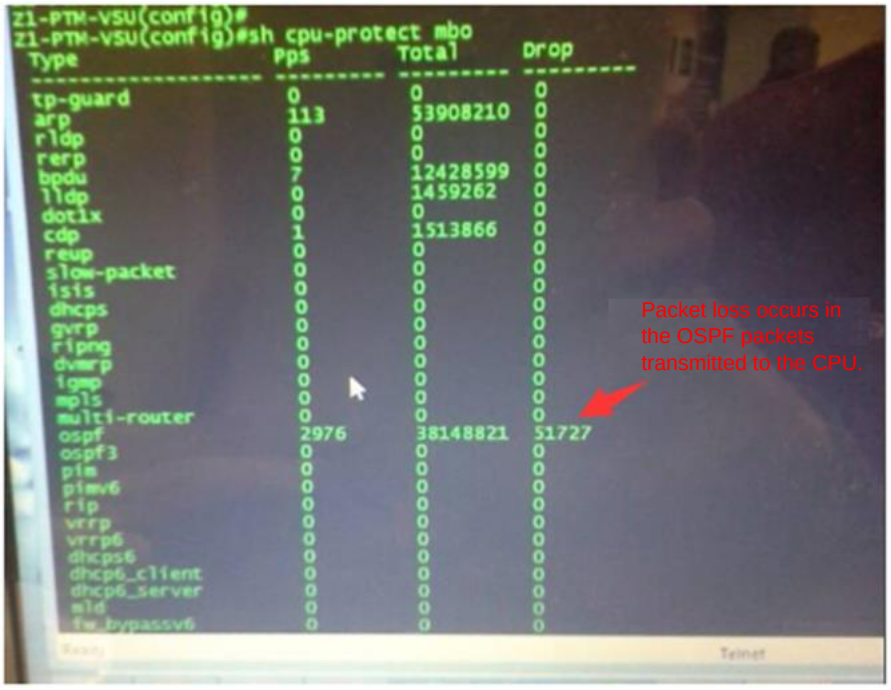
The S12000 encounters an OSPF attack, the CPU usage of the device is very high, and a large number of OSPF packets transmitted to the CPU for processing are lost. As a result, the device fails to establish OSPF neighbor relationships normally.



```
Z1-PTM-VSU(config)#sh cpu
CPU using Rate Information
CPU utilization in five seconds: 47.81%
CPU utilization in one minute  : 49.34%
CPU utilization in five minutes: 49.54%
 NO   5Sec   1Min   5Min   Process
 0   4.02%  4.10%  4.71%   LISR INT
 1   1.24%  1.18%  1.25%   HISR INT
 2   0.04%  0.04%  0.04%   hktimer
 3   0.26%  0.26%  0.26%   ktimer
 4   0.02%  0.02%  0.02%   atimer
 5   0.00%  0.00%  0.00%   printk_task
 6   0.00%  0.00%  0.00%   waitqueue_process
 7   0.00%  0.00%  0.00%   tasklet_task
 8   0.00%  0.00%  0.00%   kevents
 9   0.00%  0.00%  0.00%   vsu_dcm
10   0.00%  0.00%  0.00%   iftp_server
11   0.00%  0.00%  0.00%   tsrmpd-pkt
12   0.00%  0.00%  0.00%   snmpd
13   0.00%  0.00%  0.00%   snmp_trapd
14   0.00%  0.00%  0.00%   mtdblock
15   0.00%  0.00%  0.00%   gc_task
```

2. Possible Causes

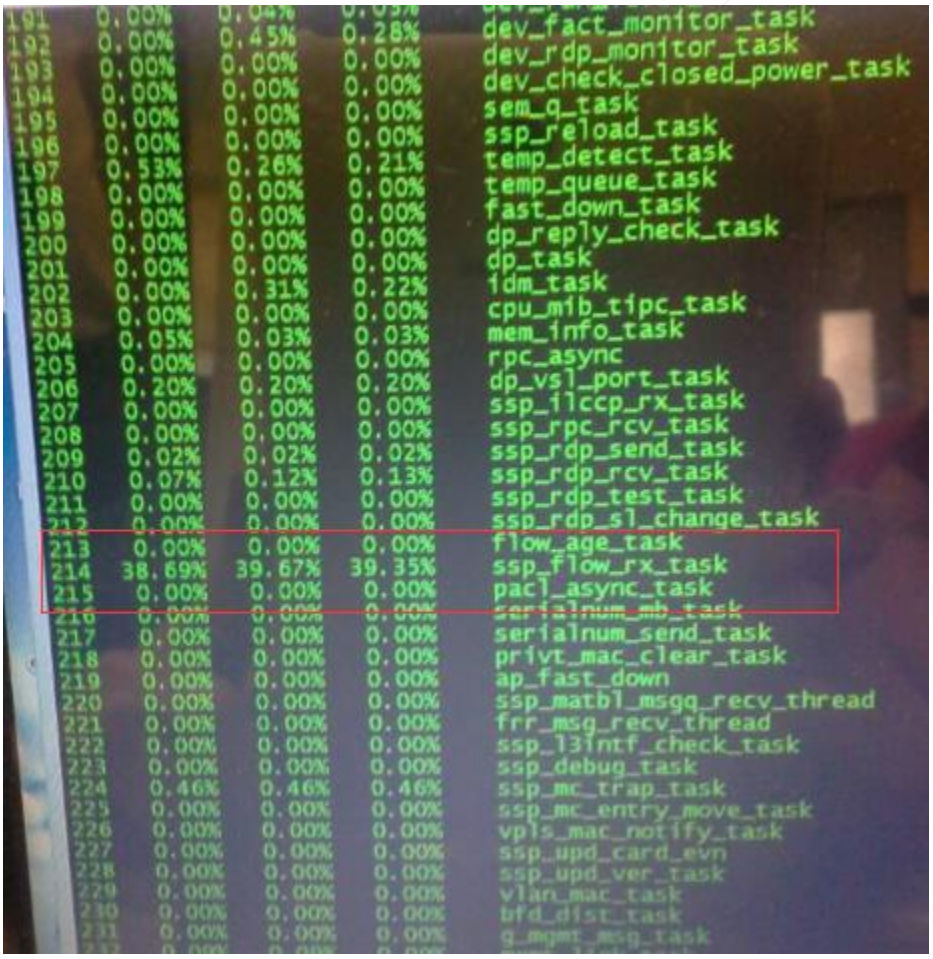
1. OSPF packets transmitted to the CPU are beyond the processing capability of the CPU. As a result, packet loss occurs. Run the show cpu-protect mboard command to check whether packet loss occurs.



```
Z1-PTM-VSU(config)#
Z1-PTM-VSU(config)#sh cpu-protect mbo
Type                Pps      Total     Drop
------------------  -------  --------  -------
tp-guard            0        0         0
arp                 113      53908210  0
rldp                0        0         0
rerp                0        0         0
bpdu                7        12428599  0
lldp                0        1459262   0
dot1x               0        0         0
cdp                 1        1513866   0
reup                0        0         0
slow-packet         0        0         0
isis                0        0         0
dhcps               0        0         0
gvrp                0        0         0
ripng               0        0         0
dvmrp               0        0         0
igmp                0        0         0
mpls                0        0         0
multi-router        0        0         0
ospf                2976     38148821  51727
ospf3               0        0         0
pim                 0        0         0
pimv6               0        0         0
rip                 0        0         0
vrrp                0        0         0
vrrp6               0        0         0
dhcps6              0        0         0
dhcp6_client        0        0         0
dhcp6_server        0        0         0
mld                 0        0         0
fw_bypassv6         0        0         0
```

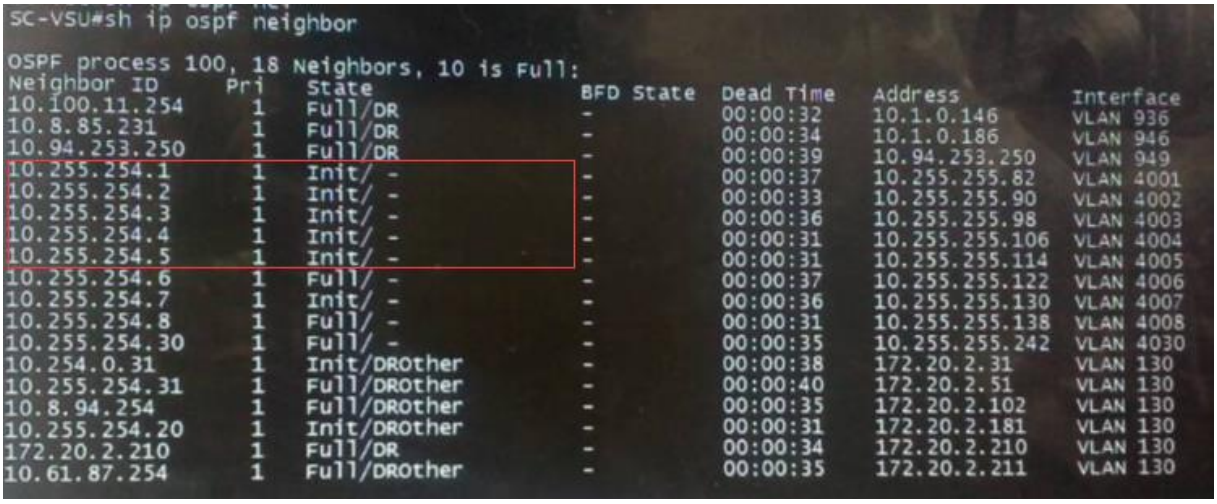
Packet loss occurs in the OSPF packets transmitted to the CPU.

2. Run the show cpu command to identify the processes with high CPU usage.



191	0.00%	0.04%	0.05%	[illegible]
192	0.00%	0.45%	0.28%	dev_fact_monitor_task
193	0.00%	0.00%	0.00%	dev_rdp_monitor_task
194	0.00%	0.00%	0.00%	dev_check_closed_power_task
195	0.00%	0.00%	0.00%	sem_q_task
196	0.00%	0.00%	0.00%	ssp_reload_task
197	0.53%	0.26%	0.21%	temp_detect_task
198	0.00%	0.00%	0.00%	temp_queue_task
199	0.00%	0.00%	0.00%	fast_down_task
200	0.00%	0.00%	0.00%	dp_reply_check_task
201	0.00%	0.00%	0.00%	dp_task
202	0.00%	0.31%	0.22%	idm_task
203	0.00%	0.00%	0.00%	cpu_mib_tipc_task
204	0.05%	0.03%	0.03%	mem_info_task
205	0.00%	0.00%	0.00%	rpc_async
206	0.20%	0.20%	0.20%	dp_vsl_port_task
207	0.00%	0.00%	0.00%	ssp_ilccp_rx_task
208	0.00%	0.00%	0.00%	ssp_rpc_rcv_task
209	0.02%	0.02%	0.02%	ssp_rdp_send_task
210	0.07%	0.12%	0.13%	ssp_rdp_rcv_task
211	0.00%	0.00%	0.00%	ssp_rdp_test_task
212	0.00%	0.00%	0.00%	ssp_rdp_sl_change_task
213	0.00%	0.00%	0.00%	flow_age_task
214	38.69%	39.67%	39.35%	ssp_flow_rx_task
215	0.00%	0.00%	0.00%	pacl_async_task
216	0.00%	0.00%	0.00%	serialnum_mb_task
217	0.00%	0.00%	0.00%	serialnum_send_task
218	0.00%	0.00%	0.00%	privt_mac_clear_task
219	0.00%	0.00%	0.00%	ap_fast_down
220	0.00%	0.00%	0.00%	ssp_matbl_msgq_recv_thread
221	0.00%	0.00%	0.00%	frr_msg_recv_thread
222	0.00%	0.00%	0.00%	ssp_l3intf_check_task
223	0.00%	0.00%	0.00%	ssp_debug_task
224	0.46%	0.46%	0.46%	ssp_mc_trap_task
225	0.00%	0.00%	0.00%	ssp_mc_entry_move_task
226	0.00%	0.00%	0.00%	vpls_mac_notify_task
227	0.00%	0.00%	0.00%	ssp_upd_card_evn
228	0.00%	0.00%	0.00%	ssp_upd_ver_task
229	0.00%	0.00%	0.00%	vlan_mac_task
230	0.00%	0.00%	0.00%	bfd_dist_task
231	0.00%	0.00%	0.00%	g_mgmt_msg_task
232	0.00%	0.00%	0.00%	[illegible]

3. The OSPF neighbor relationships cannot be established.



```
SC-VSU#sh ip ospf neighbor

OSPF process 100, 18 Neighbors, 10 is Full:
Neighbor ID     Pri   State           BFD State  Dead Time   Address         Interface
10.100.11.254     1   Full/DR         -          00:00:32    10.1.0.146      VLAN 936
10.8.85.231       1   Full/DR         -          00:00:34    10.1.0.186      VLAN 946
10.94.253.250     1   Full/DR         -          00:00:39    10.94.253.250   VLAN 949
10.255.254.1      1   Init/ -         -          00:00:37    10.255.255.82   VLAN 4001
10.255.254.2      1   Init/ -         -          00:00:33    10.255.255.90   VLAN 4002
10.255.254.3      1   Init/ -         -          00:00:36    10.255.255.98   VLAN 4003
10.255.254.4      1   Init/ -         -          00:00:31    10.255.255.106  VLAN 4004
10.255.254.5      1   Init/ -         -          00:00:31    10.255.255.114  VLAN 4005
10.255.254.6      1   Full/ -         -          00:00:37    10.255.255.122  VLAN 4006
10.255.254.7      1   Init/ -         -          00:00:36    10.255.255.130  VLAN 4007
10.255.254.8      1   Full/ -         -          00:00:31    10.255.255.138  VLAN 4008
10.255.254.30     1   Full/ -         -          00:00:35    10.255.255.242  VLAN 4030
10.254.0.31       1   Init/DROther    -          00:00:38    172.20.2.31     VLAN 130
10.255.254.31     1   Full/DROther    -          00:00:40    172.20.2.51     VLAN 130
10.8.94.254       1   Full/DROther    -          00:00:35    172.20.2.102    VLAN 130
10.255.254.20     1   Init/DROther    -          00:00:31    172.20.2.181    VLAN 130
172.20.2.210      1   Full/DR         -          00:00:34    172.20.2.210    VLAN 130
10.61.87.254      1   Full/DROther    -          00:00:35    172.20.2.211    VLAN 130
```

It can be judged that the OSPF process is attacked. Based on this conclusion, find out the attack source and take anti-attack measures accordingly.

3. Troubleshooting

1. Find out the attack source.

Method 1: Run the **show interface counter summary** command on the device to locate ports with excessive multicast/broadcast packets, shut down the ports, and then check whether the fault is rectified.

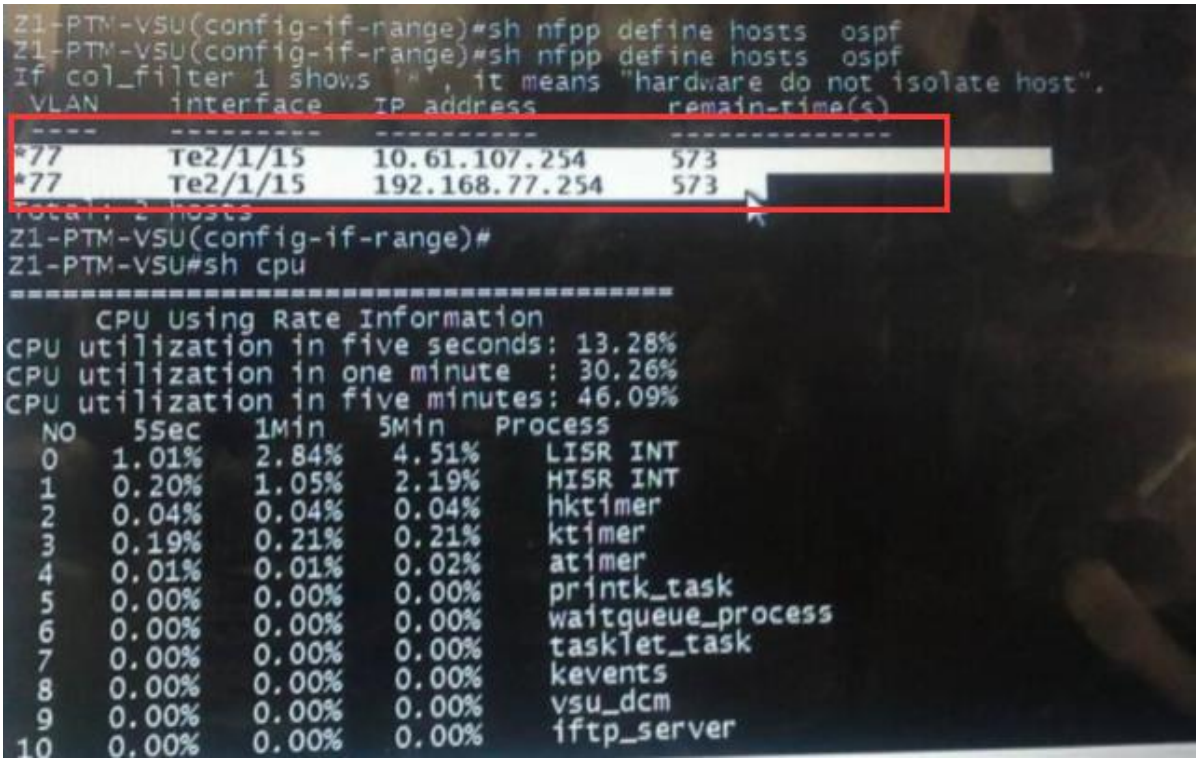
Method 2: Enable the NFPP anti-attack function. If the device encounters ARP attacks, enable the ARP attack prevention policy. In this fault case, the OSPF process is attacked. Therefore, use a defined NFPP policy for restriction. The configuration commands are as follows:

```
nfpp
 define ospf
  match etype 0x800 protocol 89
  global-policy per-src-ip 100 200
```

(The former is used to limit the rate, the latter is used to set the attack threshold, and the values here can be adjusted.)

```
isolate-period 30 //Set hardware isolation.
 interface GigabitEthernet 1/0/1//Apply the policy to all ports.
 nfpp define ospf enable
```

2. After the preceding commands are configured, check whether the CPU attacks of the device are eliminated and check information about the attack source isolated by NFPP. It is found that attacks are initiated in VLAN 77. Perform the shutdown operation on SVI 77, find out the attack source further, and take actions accordingly.



3. Fault Information Collection

```
show cpu
show cpu-protect mboard
show interface counter summary
show interfaces counters rate
show ip ospf neighbor
show ip ospf interface
show nfpp define hosts ospf
```

4. Fault Summary and Precautions

N/A

Q8: Descriptions of the Security Function of the Switch

IP Source Guard + DHCP Snooping:

DHCP Snooping maintains a database of user IP address, and provides data in the database to the IP Source Guard function for filtering so that only users who obtain IP addresses over DHCP can access the network. In this way, IP Source Guard + DHCP Snooping prevent users from setting static IP addresses at discretion.

The IP Source Guard function maintains an source IP address database, and sets user information (VLAN, MAC address, IP address, and port) in the database as hardware filtering entries so that only users whose information match the database can access the network.

The IP Source Guard conducts effective security control in DHCP according to the bound source IP address database. The IP Source Guard automatically synchronizes data of valid users in the database bound to the DHCP Snooping to the source IP address database bound to the IP Source Guard. In this way, the IP Source Guard can stringently filter client packets on the device where DHCP Snooping is enabled. ------Note: You can run the show ip source binding command to display the user IP addresses + MAC addresses bound to ip verify source.

In DHCP Snooping, the IP Source Guard must be enabled if ARP-check needs to be enabled. The configuration is as follows:

```
ip dhcp snooping
interface 0/x
ip verify source
arp-check
```